FortiSIEM - Hyper-V Installation Guide

Version 5.3.3

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

09/15/2021
FortiSIEM 5.3.3 Hyper-V Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
05/09/2018	Initial version of FortiSIEM - Hyper-V Installation Guide
03/29/2019	Revision 1: updated instructions for registering on a Supervisor node.
08/20/2019	Revision 2: Updated the location of the image download site.
09/13/2019	Revision 3: FortiSIEM now supports Hyper-V on Microsoft Windows 2012 R2.
11/20/2019	Release of FortiSIEM - Hyper-V Installation Guide for 5.2.6.
03/30/2020	Release of FortiSIEM - Hyper-V Installation Guide for 5.3.0.
09/15/2021	Updated Supported Version for 5.4.0, 5.3.x, and 5.2.x guides.

Installing FortiSIEM on Hyper-V

The document provides instructions to install FortiSIEM on Hyper-V.

- Supported Version
- Pre-installation check-list
- Installing FortiSIEM Virtual Appliance on Hyper-V
- Installing FortiSIEM Report Server on Hyper-V

Supported Version

FortiSIEM supports Hyper-V on Microsoft Windows 2012 R2 and newer.

Pre-installation check-list

Step A: Determine your FortiSIEM hardware needs and deployment type

Before you begin, check the following:

1. Number of Workers needed, if any.
2. Number of Collectors needed, if any.
3. Hardware specification of Supervisor, Worker and Collectors (CPU, RAM, Local Storage)

   If Elasticsearch is chosen as the Event Database, the Supervisor needs an additional 8 GB RAM - in this case, the minimum requirement of the Supervisor is 32 GB RAM.

4. Event Database Storage – Local or Remote (For Remote - NFS or Elasticsearch)
   Note: The Remote option is required if you are deploying Workers. If you are going to add Workers in the future, it is recommended to choose a Remote database option to avoid data migration.
5. Deployment type – Enterprise or Service Provider

Step B: Deploy Remote Storage

Before you install FortiSIEM virtual appliance in Hyper-V, you should decide whether to use NFS storage, local or Elasticsearch storage to store event information in EventDB. If you decide to use a 'Local' disk, you can add a data disk of appropriate size. Typically, this will be named as `/dev/sdd` if it is the 4th disk. While using a 'Local' disk, choose the type 'Dynamically expanding' (VHDX) format so that you are able to resize the disk if your EventDB will grow beyond the initial capacity.

If required, install and configure NFS or Elasticsearch before beginning the installation below:

- *For NFS deployment, see FortiSIEM - NFS Storage Guide.*
- *For Elasticsearch deployment, see FortiSIEM - Elasticsearch Storage Guide.*

Installing FortiSIEM Virtual Appliance on Hyper-V

Step 1: Configure Disk Formats for Data Storage

FortiSIEM virtual appliances in Hyper-V use dynamically expanding VHD disks for the root and CMDB partitions, and a dynamically expanding VHDX disk for EventDB. Dynamically expanding disks are used to keep the exported Hyper-V image within reasonable limits. See the Microsoft documentation topic Performance Tuning Guidelines for Windows Server 2012 (or R2) for more information.

1. Go to the Fortinet Support website https://support.fortinet.com to download the Hyper-V package. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Download and uncompress the packages for Super/Worker, Collector and Report Server (using 7-Zip tool) to the location where you want to install the image.
3. Open Hyper-V Manager.
4. On the **Action** menu, select **Import Virtual Machine**.
   The **Import Virtual Machine Wizard** will launch.
5. Click **Next**.
6. Browse to the folder containing Hyper-V VM, and click **Next**.
7. Select the FortiSIEM image, and click **Next**.
8. For **Import Type**, select **Copy the virtual machine** and click **Next.**
9. Select the storage folders for your virtual machine files and click **Next**.
10. Select the storage folder for your virtual machine's hard disks and click **Next**.
11. Verify the installation configuration and click **Finish**.
12. In Hyper-V Manager, connect to the FortiSIEM virtual appliance and power it on.

Step 2: Configure the Supervisor, Worker, or Collector from the VM Console

Do not press any control keys (for example - **Ctrl**-C or **Ctrl**-Z) while configuring the virtual appliances, as this may cause the installation process to stop. If this happens, you must erase the virtual appliance and start the installation process again.

1. In the Hyper-V Manager, select the Supervisor, Worker, or Collector virtual appliance
2. Right-click to open the **Virtual Appliance Options** menu, and select **Power > Power On**.
3. On the **Virtual Appliance Options** menu, select **Open Console**
   Network Failure Message: When the console starts up for the first time you may see a `Network eth0 Failed` message, but this is an expected behavior.
4. In the VM console, select **Set Timezone** and press **Enter**.
5. Select your **Location** and press **Enter**.
6. Select your **Country** and press **Enter**.
7. Select your **Timezone** and press **Enter**.

8. Review your Timezone information, select **1**, and press **Enter**.
9. When the **Configuration** screen reloads, select **Login**, and press **Enter**.
10. Enter the default login credentials:
    - Login: `root`
    - Password: `ProspectHills`
11. Run the `vami_config_net` script to configure the network:

    ```
    /opt/vmware/share/vami/vami_config_net
    ```

12. Based on your network type, enter one of the options below:
    - **1** for **IPv6 Network Only**
        - When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, and IPv6 DNS Server(s).
    - **2** for **IPv4 Network Only**
        - When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Netmask, IPv4 Gateway, and IPv4 DNS Server(s).
    - **3** for **Both Networks**
        i. When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, IPv6 DNS Server(s).
        ii. Follow Step 13 below to turn off the proxy server and continue with step c.
        iii. When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Prefix, IPv4 Gateway, IPv4 DNS Server(s).
13. Enter **n**. **Note**: The authenticated proxy server is not supported in this version of FortiSIEM. You must turn off the proxy server authentication or completely disable the proxy for the Hyper-V host.
14. Press **Y** to accept the network configuration settings.
15. Enter the **Host name,** and then press **Enter**.
16. For Supervisor and Worker: You will be prompted to choose Supervisor [s] or Worker [w].
    Choose accordingly:
    a. For Supervisor, the system will initialize the PostGreSQL database which will take around 20 minutes and then reboot the system. A few minutes after reboot, the system GUI will be ready to upload license and configure the Event Database Storage option. For a Worker node, the system will reboot quickly and a few minutes after reboot, it will be ready to be added as a Worker from the Supervisor GUI.
    b. For a Worker node, the system will reboot quickly and a few minutes after reboot, it will be ready to be added as a Worker from the Supervisor GUI.
17. For Collector, the system will reboot and after a few minutes it will be ready.

Step 3: Upload the FortiSIEM License on Supervisor

You will now be asked to input a license.

1. Click **Browse** and upload the license file.
   Make sure that the 'Hardware ID' shown in the **License Upload** page matches the license.
2. For **User ID** and **Password**, choose any 'Full Admin' credentials.
   For the first time, install by choosing user as 'admin' and password as 'admin*1'
3. Choose **License type** as 'Enterprise' or 'Service Provider'.
   This option is available only on first install. Once the database is configured, this option will not be available.

Step 4: Choose FortiSIEM Event Database Storage

For fresh installation, you will be taken to the Event Database Storage page. Based on Step-B, you will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options.

For more details, see here.

Step 5: (Optional) Install Workers and Add to Supervisor Node

1. Follow Step 1: Configure Disk Formats for Data Storage and Step 2: Configure the Supervisor, Worker, or Collector from the VM Console to configure a Worker.
2. Add the Worker node to the Supervisor by visiting **ADMIN** > **License** > **Nodes** > **Add**.
3. See **ADMIN** > **Health** > **Cloud Health** to ensure that the Workers are up, healthy and properly added to the system.

Step 6: (Optional) Install Collectors

Collectors can be installed as Virtual Appliances or Hardware appliances (FSM-500F).

Step 7: (Optional) Register Collectors to Supervisor Node

For Enterprise deployments, follow these steps:

1. Login to Supervisor with 'Admin' privileges.
2. Go to **ADMIN** > **Setup** > **Collectors** and add a Collector by entering:
   a. **Name** – Collector Name
   b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time** and **End Time** – set 'Unlimited'.
3. SSH to the Collector and run following script to register Collectors:
   ```
   phProvisionCollector --add <user> <password> <Super IP or Host> <Organization>
   <CollectorName>
   ```
   a. Set **User** and **Password** use the admin User Name and password for the Supervisor
   b. Set **IP Address** as 'Supervisor IP'.
   c. Set **Organization** as 'Super'.
   d. Set **CollectorName** from Step 2a.
   The Collector will reboot during the Registration
4. Go to **ADMIN** > **Health** > **Collector Health** and see the status.

Installing FortiSIEM Report Server on Hyper-V

Follow the steps below to install the FortiSIEM Report Server on Hyper-V:

Step 1: Launch FortiSIEM Supervisor from Hyper-V

- Follow the steps in Step 1 using Report Server image.

Step 2: Start and Configure FortiSIEM

Do not press any control keys (for example - **Ctrl**-C or **Ctrl**-Z) while configuring the virtual appliances, as this may cause the installation process to stop. If this happens, you must erase the virtual appliance and start the installation process again.

1. SSH into the Supervisor console.
2. For Local storage, you can add the data disk. Use the command `fdisk -l` to get the disk name.
3. Run the script `/opt/vmware/share/vami/vami_set_timezone` to set the time zone.
4. Run the script `/opt/vmware/share/vami/vami_config_net` to configure the network.
5. Based on your network type, enter one of the options below:
   - **1** for **IPv6 Network Only**
     - When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, and IPv6 DNS Server(s).
   - **2** for **IPv4 Network Only**
     - When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Netmask, IPv4 Gateway, and IPv4 DNS Server(s).
   - **3** for **Both Networks**
     i. When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, IPv6 DNS Server(s).
     ii. Follow Step 6 below to turn off the proxy server and continue with step c.
     iii. When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Prefix, IPv4 Gateway, IPv4 DNS Server(s).
6. Enter **n**. **Note**: The authenticated proxy server is not supported in this version of FortiSIEM. You must turn off the proxy server authentication or completely disable the proxy for the Hyper-V host.
7. Enter **y** to accept the network configuration settings.
8. Enter the **Host name**, and then press **Enter**.
9. Enter the mount point for your data. Set one of the following:
   - 'Local' (`/dev/<disk_name>`)
     Use the 'disk_name' from Step #2 above.
   - 'NFS' storage mount point
     Note: Do not use the same mount point as EventDB on Supervisor. This should be a different mount point/storage path.

   After you set the mount point, the Report Server will automatically reboot, and in 10 to 15 minutes the Report Server will be successfully configured.

Step 3: Register FortiSIEM Report Server to Supervisor

1. Log in to your Supervisor node.
2. Open the 'License Management' page on:
   - Flash GUI: Go to **Admin** > **License Management**. Under 'Report Server Information', click **Add**.
   - HTML5 GUI: Go to **ADMIN** > **License** > **Nodes** tab. Click **Add** and select '**Report Server**' from the **Type** drop-down.
3. Enter the **Report Server IP Address**, **Database Username** and **Database Password** of the Report Server you want to use to administer.
   Use the same credentials to set up the Visual Analytics Server for reading data from the Report Server.
4. Click **Run in Background** if you want Report Server registration to run in the background for larger installations. When CMDB size is below 1 GB, registration takes approximately three minutes to complete.
5. When the registration is complete, click **OK** in the confirmation dialog.
6. Make sure the Report Server is up and running by navigating to:
   - Flash GUI: **Admin** > **Cloud Health**
   - HTML5 GUI: **ADMIN** > **Health** > **Cloud Health**

Step 4: Sync Reports from FortiSIEM Supervisor to the Report Server

1. Log in to your Supervisor node.
2. Select **Synced Reports** from:
   - Flash GUI: **RESOURCE > Reports** > **Synced Reports**
   - HTML5 GUI: **RESOURCES** > **Reports** > **Synced Reports**
3. Select a Report.
   Currently, only reports that contain a 'Group By' condition can be synced. Both system and user-created reports can be synched as long as it contains a 'Group By' condition.
4. Select **Sync**.
   When the sync process initiates, the Supervisor node dynamically creates a table within the Report Server reportdb database. When the sync is established, it will run every five minutes, and the last five minutes of data in the synced report will be pushed to the corresponding table. This lets you run Visual Analytics on event data stored in the Report Server reportdb database.