FortiOS - Microsoft Hyper-V Cookbook

Version 6.4

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/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

November 03, 2020
FortiOS 6.4 Microsoft Hyper-V Cookbook
01-640-619592-20201103

TABLE OF CONTENTS

About FortiGate-VM on Microsoft Hyper-V

FortiGate-VMs allow you to mitigate blind spots by implementing critical security controls within your virtual infrastructure. They also allow you to rapidly provision security infrastructure whenever and wherever it is needed. FortiGate-VMs feature all the security and networking services common to hardware-based FortiGate appliances. You can deploy a mix of FortiGate hardware and VMs, operating together and managed from a common centralized management platform.

This document describes how to deploy a FortiGate-VM in a Microsoft Hyper-V environment.

FortiGate-VM models and licensing

FortiGate-VM offers perpetual licensing (normal series and V-series) and annual subscription licensing (S-series, available starting Q4 2019). The differences are as follows:

	Normal series	V-series	S-series
Licensing term	VM base is perpetual. You must separately contract support services on an annual basis.		Single annually contracted SKU that contains VM base and a FortiCare service bundle.
Support services	Each VM base type is associated with over a dozen SKUs. See the pricelist for details.		Four support service bundle types: • Only FortiCare • UTM • Enterprise • 360 protection
License level	SKUs are based on the number of virtual CPUs (vcPU) (1, 2, 4, 8, 16, 32, or unlimited). The RAM/memory restriction no longer applies for FortiOS 6.2.2 and later versions. FortiOS 6.2.1 and earlier versions have RAM/memory restrictions.		
vCPU number upgrade during contracted term	Not supported.		Supported. You can also upgrade the support service bundle. For details about upgrading, contact a Fortinet sales correspondent.
vCPU number downgrade during contracted term	Not supported.		

	Normal series	V-series	S-series
Virtual domain (VDOM) support	By default, each CPU level supports up to a certain number of VDOMs. See the FortiGate-VM datasheet for the default limits.	By default, all CPU levels do not support adding VDOMs.	

After you submit an order for a FortiGate-VM, Fortinet sends a license registration code to the email address that you entered on the order form. Use this code to register the FortiGate-VM with Customer Service & Support, and then download the license file. After you upload the license to the FortiGate-VM and validate it, your FortiGate-VM is fully functional.

FortiGate-VM evaluation license

The FortiGate-VM includes a limited, 15-day evaluation license that supports:

- 1 CPU maximum
- 1024 MB memory maximum
- Low encryption only (no HTTPS administrative access)
- Security protection:
  - With the built-in signatures that the evaluation license includes, you can use the following features:
    - IPS
    - AntiVirus
    - Industrial DB
  - The following features do not have built-in signatures:
    - Security rating
    - Antispam
    - Web Filter
- Features related to FortiGuard access are not available. Go to *System* > *FortiGuard* in FortiOS for details.
- VDOM:
  - You can enable split-task VDOM in the CLI.
  - You cannot enable multi-VDOM.

Note the following:

- Attempting to upgrade the FortiGate firmware locks the GUI until you upload a full license.
- The evaluation license does not include technical support. The trial period begins the first time that you start the FortiGate-VM.
- After the trial license expires, functionality is disabled until you upload a full license file.
- Features available in the evaluation state may change without prior notice.

FortiGate-VM virtual licenses and resources

The primary requirement for provisioning a FortiGate-VM may be the number of interfaces it can accommodate rather than its processing capabilities. In some cloud environments, the options with a high number of interfaces tend to have high numbers of vCPUs.

FortiGate-VM licensing does not restrict whether the FortiGate can work on a VM instance in a public cloud that uses more vCPUs than the license allows. The number of vCPUs that the license indicates does not restrict the FortiGate from working, regardless of how many vCPUs the virtual instance includes. However, only the licensed number of vCPUs process traffic and management tasks. The FortiGate-VM does not use the rest of the vCPUs.

License	1 vCPU	2 vCPU	4 vCPU	8 vCPU	16 vCPU	32 vCPU
FGT-VM08	OK	OK	OK	OK	The FortiGate-VM uses 8 vCPUs for traffic and management and does not use the rest.	The FortiGate-VM uses 8 vCPUs for traffic and management and does not use the rest.

You can provision a VM instance based on the number of interfaces you need and license the FortiGate-VM for only the processors you need.

Public compared to private clouds

The behavior differs between private and public clouds:

- Private clouds (ESXi/KVM/Xen/Hyper-V): Both licensed vCPUs and RAM are affected. FortiOS 6.4 does not have licensed RAM size restrictions. However, the minimum recommended RAM size is 2 GB for all versions.
- Public clouds (AWS/Azure/GCP/OCI/Aliyun): Only licensed vCPU is affected.

For example, you can activate FG-VM02 on a FGT-VM with 4vCPUs with 16 GB of RAM, running on a private VM platform. Only 2 vCPU and 4 GB of RAM, as licensed, is consumable.

Likewise, you can activate FG-VM02 on a FGT-VM c5.2xlarge EC2 instance with 8 vCPUs running on AWS. Only 2 vCPU is consumable, and there is no limit on the RAM size. You can refer to licenses for public clouds as bring your own license.

Preparing for deployment

This documentation assumes that before deploying the FortiGate-VM on the Microsoft Hyper-V virtual platform, you have addressed the following requirements:

Virtual environment

You have installed the Microsoft Hyper-V software on a physical server with sufficient resources to support the FortiGate-VM and all other VMs deployed on the platform.

If you configure the FortiGate-VM to operate in transparent mode, or include it in a FortiGate clustering protocol (FGCP) high availability (HA) cluster, configure any virtual switches to support the FortiGate-VM's operation before you create the FortiGate-VM.

Management software

If you plan to use the GUI to manage the Hyper-V server remotely, make sure that the management software is installed on a computer with network access to the Hyper-V server.

Options for remote management of Microsoft Hyper-V include:

- Hyper-V Manager
- Virtual Machine Manager

Connectivity

An Internet connection is required for the FortiGate-VM to contact FortiGuard to validate its license. If the FortiGate-VM is in a closed environment, it must be able to connect to a FortiManager to validate the FortiGate-VM license. See Validating the FortiGate-VM license with FortiManager on page 22.

Configuring resources

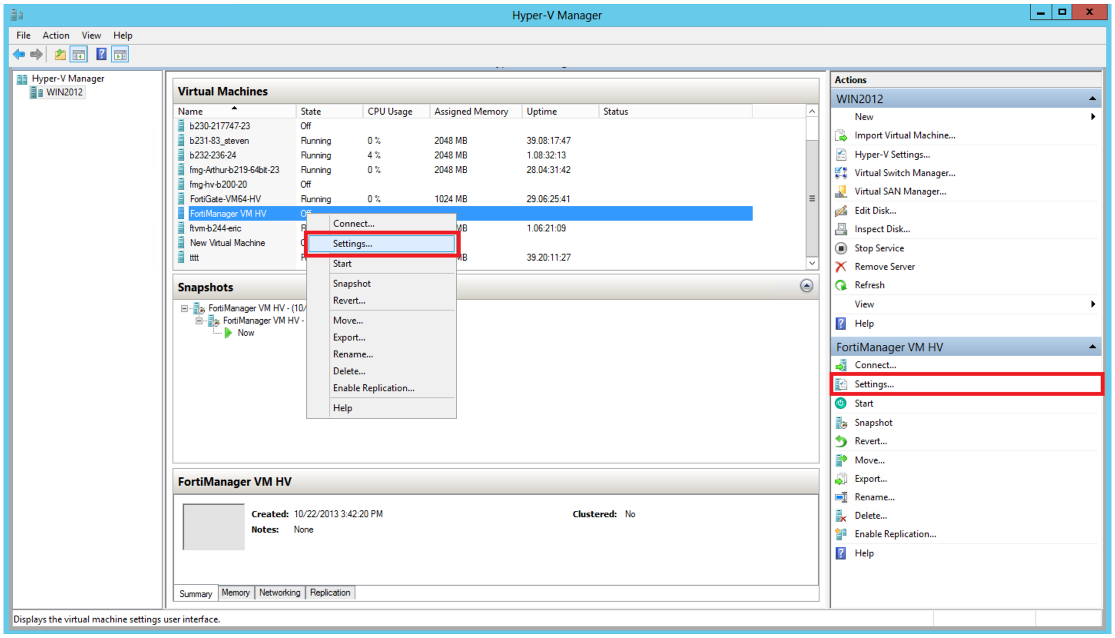
Before you start the FortiGate-VM for the first time, ensure that you have configured the following resources as the FortiGate-VM license specifies:

- Disk sizes
- CPUs

- RAM
- Network settings

To configure settings through Hyper-V Manager:

1. In the Hyper-V Manager, locate the VM name, right-click the entry, and select *Settings* from the menu. Optionally, you can select the VM and select *Settings* in the *Actions* menu.



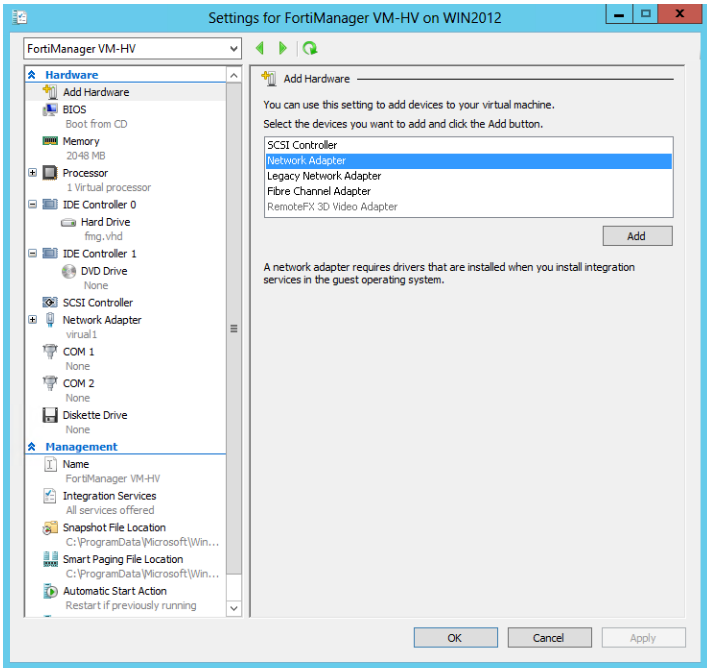
Name	State	CPU Usage	Assigned Memory	Uptime	Status
b230-217747-23	Off				
b231-83_steven	Running	0 %	2048 MB	39.08:17:47	
b232-236-24	Running	4 %	2048 MB	1.08:32:13	
fmg-Arthur-b219-64bit-23	Running	0 %	2048 MB	28.04:31:42	
fmg-hv-b200-20	Off				
FortiGate-VM64-HV	Running	0 %	1024 MB	29.06:25:41	
FortiManager VM HV	Off				
ftvm-b244-eric	R		MB	1.06:21:09	
New Virtual Machine	O				
tttt	R		MB	39.20:11:27	

FortiManager VM HV

Created: 10/22/2013 3:42:20 PM
Clustered: No
Notes: None

Displays the virtual machine settings user interface.

The *Settings* page is displayed.



You can use this setting to add devices to your virtual machine.

Select the devices you want to add and click the Add button.

A network adapter requires drivers that are installed when you install integration services in the guest operating system.

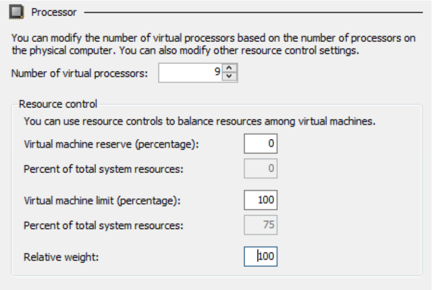
2. Configure virtual processors, network adapters, and virtual hard drive settings.
3. Select *Apply* to save the settings and then select *OK* to close the settings page.

FortiGate-VM virtual processors

You must configure FortiGate-VM virtual processors. The number of processors is dependent on your server environment.

To configure FortiGate-VM virtual processors:

1. In the *Settings* page, select *Processor* from the *Hardware* menu. The *Processor* page is displayed.



Processor

You can modify the number of virtual processors based on the number of processors on the physical computer. You can also modify other resource control settings.

Number of virtual processors: 9

Resource control

You can use resource controls to balance resources among virtual machines.

Virtual machine reserve (percentage): 0

Percent of total system resources: 0

Virtual machine limit (percentage): 100

Percent of total system resources: 75

Relative weight: 100

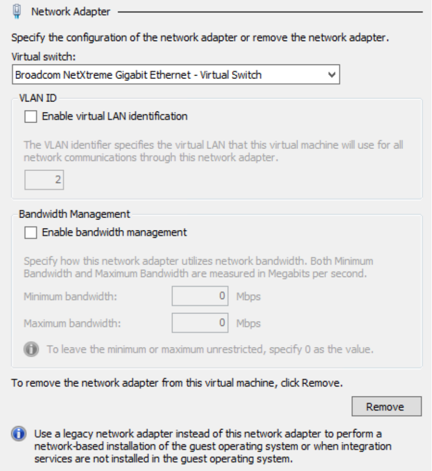
2. Configure the number of virtual processors for the FortiGate-VM. Optionally, you can use resource controls to balance resources among VMs.
3. Select *Apply* to save the settings.

FortiGate-VM network adapters

You must configure FortiGate-VM network adapters. FortiGate-VM supports four network adapters.

To configure FortiGate-VM network adapters:

1. In the *Settings* page, select *Add Hardware* from the *Hardware* menu, select *Network Adapter* in the device list, and select the *Add* button. The *Network Adapter* page is displayed.



Network Adapter

Specify the configuration of the network adapter or remove the network adapter.

Virtual switch:

Broadcom NetXtreme Gigabit Ethernet - Virtual Switch

VLAN ID

☐ Enable virtual LAN identification

The VLAN identifier specifies the virtual LAN that this virtual machine will use for all network communications through this network adapter.

2

Bandwidth Management

☐ Enable bandwidth management

Specify how this network adapter utilizes network bandwidth. Both Minimum Bandwidth and Maximum Bandwidth are measured in Megabits per second.

Minimum bandwidth: 0 Mbps

Maximum bandwidth: 0 Mbps

To leave the minimum or maximum unrestricted, specify 0 as the value.

To remove the network adapter from this virtual machine, click Remove.

Use a legacy network adapter instead of this network adapter to perform a network-based installation of the guest operating system or when integration services are not installed in the guest operating system.

2. In the settings page manually configure four network adapters for FortiGate-VM. For each network adapter, select the virtual switch from the drop-down list.
3. Select *Apply* to save the settings.

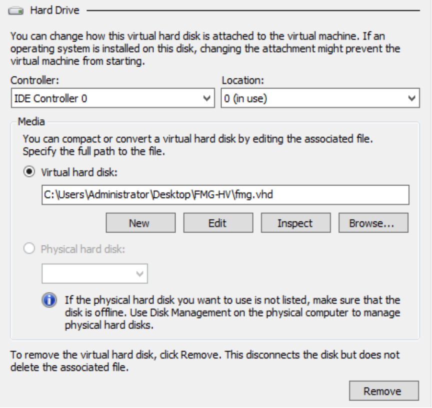
FortiGate-VM virtual hard disk

You can use the DATADRIVE.vhd file in the *-FORTINET.out.hyperv.zip file as the log/data disk. See Deployment package contents on page 14. Alternatively, you can create a new virtual hard drive to use as a log/data disk using the following instructions.

If you know your environment will expand in the future, it is recommended to increase the hard disk size beyond 30 GB. The VM license limit is 2 TB.

To configure a FortiGate-VM virtual hard drive:

1. In the *Settings* page, select *IDE Controller 0 > Hard Drive* from the *Hardware* menu. The *Hard Drive* page displays.



Hard Drive

You can change how this virtual hard disk is attached to the virtual machine. If an operating system is installed on this disk, changing the attachment might prevent the virtual machine from starting.

Controller: IDE Controller 0

Location: 0 (in use)

Media

You can compact or convert a virtual hard disk by editing the associated file. Specify the full path to the file.

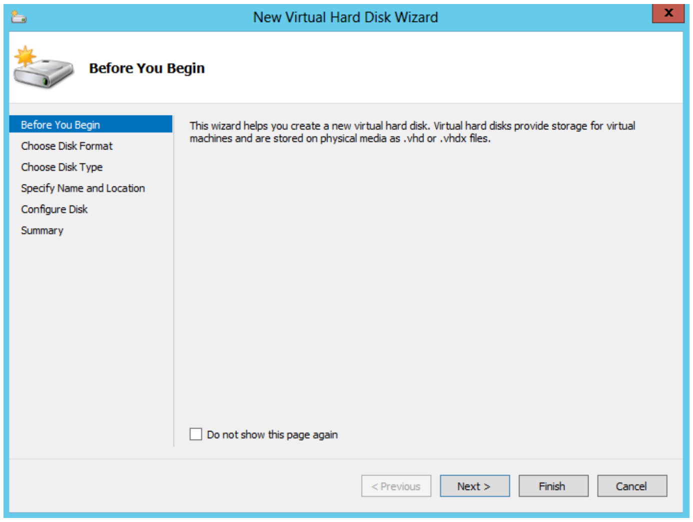
● Virtual hard disk: C:\Users\Administrator\Desktop\FMG-HV\fmg.vhd

○ Physical hard disk:

If the physical hard disk you want to use is not listed, make sure that the disk is offline. Use Disk Management on the physical computer to manage physical hard disks.

To remove the virtual hard disk, click Remove. This disconnects the disk but does not delete the associated file.

2. Select *New* to create a new virtual hard disk. The *New Virtual Hard Disk Wizard* opens.



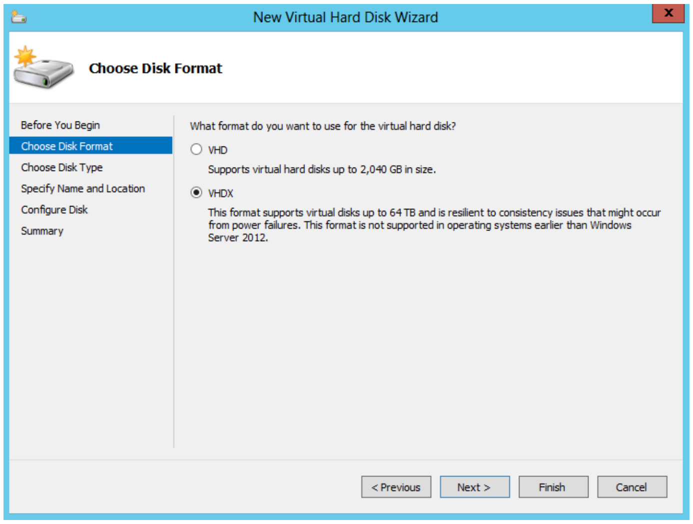
New Virtual Hard Disk Wizard

Before You Begin

This wizard helps you create a new virtual hard disk. Virtual hard disks provide storage for virtual machines and are stored on physical media as .vhd or .vhdx files.

□ Do not show this page again

3. This wizard helps you to create a new virtual hard disk. Select *Next* to continue. The *Choose Disk Format* page opens.



What format do you want to use for the virtual hard disk?

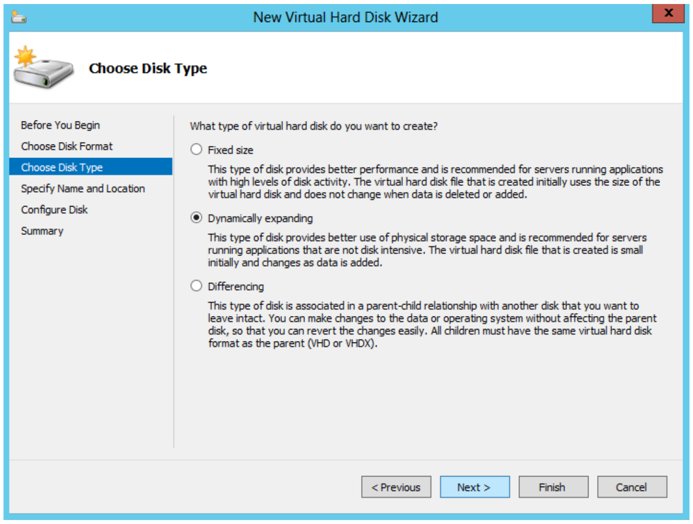
○ VHD

Supports virtual hard disks up to 2,040 GB in size.

● VHDX

This format supports virtual disks up to 64 TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012.

4. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64TB and is resilient to consistency issues that might occur from power failures. This format is not supported in operating systems earlier than Windows Server 2012. Note that FortiGate-VM does not support hard disks larger than 2TB.
5. Select *Next* to continue. The *Choose Disk Type* page opens.



What type of virtual hard disk do you want to create?

○ Fixed size

This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.

● Dynamically expanding

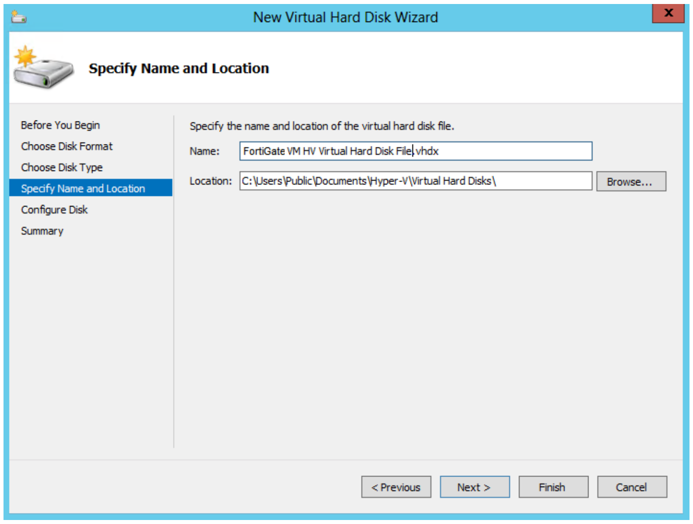
This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual hard disk file that is created is small initially and changes as data is added.

○ Differencing

This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

6. Select the type of virtual disk that you want to use. Select one of the following disk types:
   - Fixed size: This type of disk provides better performance and is recommended for servers running applications with high levels of disk activity. The virtual hard disk file that is created initially uses the size of the virtual hard disk and does not change when data is deleted or added.
   - Dynamic expanding: This type of disk provides better use of physical storage space and is recommended for servers running applications that are not disk intensive. The virtual disk file that is created is small initially and changes as data is added.
   - Differencing: This type of disk is associated in a parent-child relationship with another disk that you want to leave intact. You can make changes to the data or operating system without affecting the parent disk, so that you can revert the changes easily. All children must have the same virtual hard disk format as the parent (VHD or VHDX).

7. Select *Next* to continue. The *Specify Name and Location* page opens.



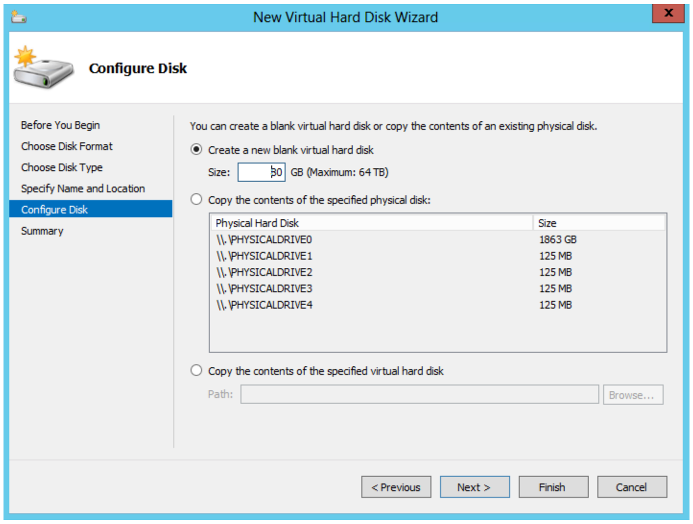
Specify the name and location of the virtual hard disk file.

Name: FortiGate VM HV Virtual Hard Disk File.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

8. Specify the name and location of the virtual hard disk file. Use the *Browse* button to select a specific file folder on your server.

9. Select *Next* to continue. The *Configure Disk* page opens.



You can create a blank virtual hard disk or copy the contents of an existing physical disk.

● Create a new blank virtual hard disk

Size: 30 GB (Maximum: 64 TB)

○ Copy the contents of the specified physical disk:

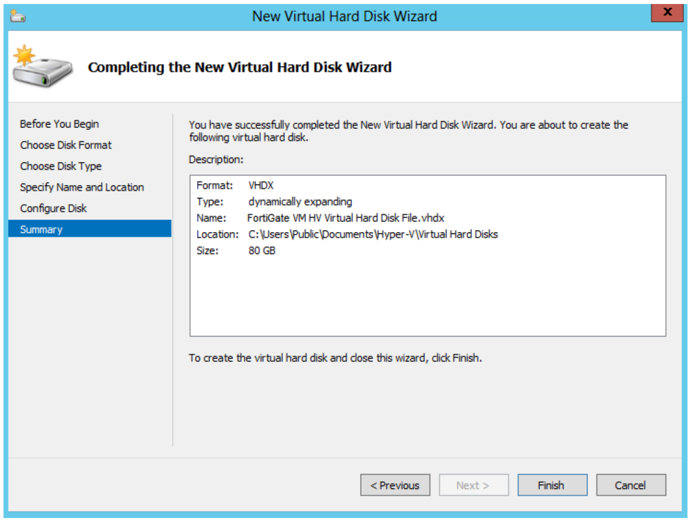
Physical Hard Disk	Size
\\.\PHYSICALDRIVE0	1863 GB
\\.\PHYSICALDRIVE1	125 MB
\\.\PHYSICALDRIVE2	125 MB
\\.\PHYSICALDRIVE3	125 MB
\\.\PHYSICALDRIVE4	125 MB

○ Copy the contents of the specified virtual hard disk

Path:

10. Select to *Create a new blank virtual hard disk* and enter the size of the disk in GB. The maximum size is dependent on your server environment.

11. Select *Next* to continue. The *Summary* page opens.



You have successfully completed the New Virtual Hard Disk Wizard. You are about to create the following virtual hard disk.

Description:

Format: VHDX
Type: dynamically expanding
Name: FortiGate VM HV Virtual Hard Disk File.vhdx
Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks
Size: 80 GB

To create the virtual hard disk and close this wizard, click Finish.

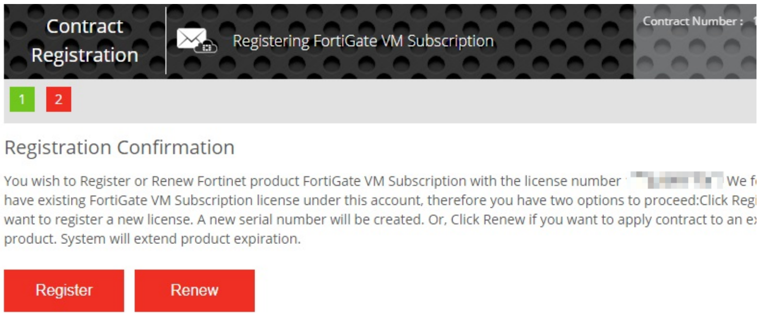
12. The summary page provides details of the virtual hard disk. Select *Finish* to create the virtual hard disk.
13. Select *Apply* to save the settings and select *OK* to exit the settings page.

Registering the FortiGate-VM

Registering the FortiGate-VM with Customer Service & Support allows you to obtain the FortiGate-VM license file.

To register the FortiGate-VM:

1. Log in to the Customer Service & Support site using a support account, or select *Sign Up* to create an account.
2. In the main page, under *Asset*, select *Register/Activate*.
3. In the *Registration* page, enter the registration code that you received via email, and select *Register* to access the registration form.
4. If you register the S-series subscription model, the site prompts you to select one of the following:
    a. Click *Register* to newly register the code to acquire a new serial number with a new license file.
    b. Click *Renew* to renew and extend the licensed period on top of the existing serial number, so that all features on the VM node continue working uninterrupted upon license renewal.



Registration Confirmation

You wish to Register or Renew Fortinet product FortiGate VM Subscription with the license number [redacted] We f
have existing FortiGate VM Subscription license under this account, therefore you have two options to proceed:Click Regi
want to register a new license. A new serial number will be created. Or, Click Renew if you want to apply contract to an e
product. System will extend product expiration.

5. Complete and submit the registration form.
6. In the registration acknowledgment page, click the *License File Download* link.

7. Save the license file (`.lic`) to your local computer. See Uploading the FortiGate-VM license on page 21 or Validating the FortiGate-VM license with FortiManager on page 22 for information about uploading the license file to your FortiGate-VM via the GUI.

Downloading the FortiGate-VM deployment package

FortiGate-VM deployment packages are found on the Customer Service & Support site. In the *Download* drop-down menu, select *VM Images* to access the available VM deployment packages.

1. In the *Select Product* drop-down menu, select *FortiGate*.
2. In the Select Platform drop-down menu, select Microsoft Hyper-V.
3. Select the FortiOS version you want to download.
   There are two files available for download: the file required to upgrade from an earlier version and the file required for a new deployment.
4. Click the *Download* button and save the file.

For more information, see the FortiGate datasheet.

You can also download the following resources for the firmware version:

- FortiOS Release Notes
- FORTINET-FORTIGATE MIB file
- FSSO images
- SSL VPN client

Deployment package contents

The *-FORTINET.out.hyperv.zip file contains:

- In the Virtual Hard Disks folder:
  - fortios.vhd: the FortiGate-VM system hard disk in VHD format
  - DATADRIVE.vhd: the FortiGate-VM log disk in VHD format
- In the Virtual Machines folder:
  - fortios.xml: XML file containing virtual hardware configuration settings for Hyper-V. This is compatible with Windows Server 2012.
- Snapshots folder: optionally, Hyper-V stores snapshots of the FortiGate-VM state here.

Deployment

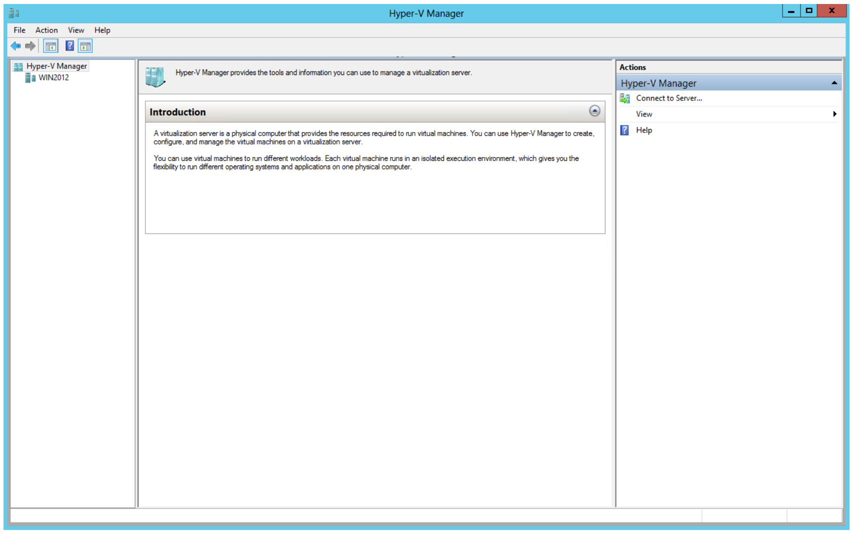
Before you deploy a FortiGate-VM, ensure that you have met the requirements described in Preparing for deployment on page 7 and that the correct deployment package is extracted to a folder on the local computer (see Downloading the FortiGate-VM deployment package on page 14).

After you deploy a FortiGate-VM and upload a full license to replace the default evaluation license, you can power on the FortiGate-VM and test connectivity.

Deploying the FortiGate-VM

To create the FortiGate-VM:

1. Launch the Hyper-V Manager on your Microsoft server. The Hyper-V Manager homepage opens.



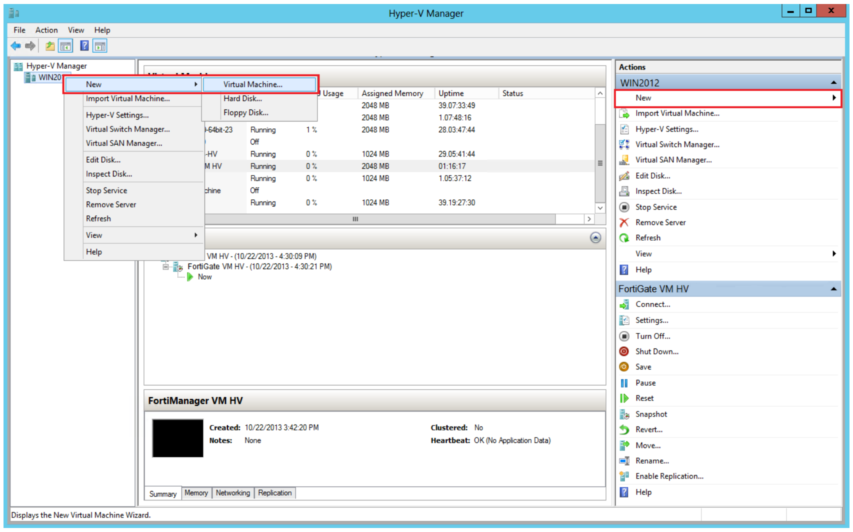
Hyper-V Manager provides the tools and information you can use to manage a virtualization server.

Introduction

A virtualization server is a physical computer that provides the resources required to run virtual machines. You can use Hyper-V Manager to create, configure, and manage the virtual machines on a virtualization server.

You can use virtual machines to run different workloads. Each virtual machine runs in an isolated execution environment, which gives you the flexibility to run different operating systems and applications on one physical computer.

2. Select the server in the right-tree menu. The server details page is displayed.

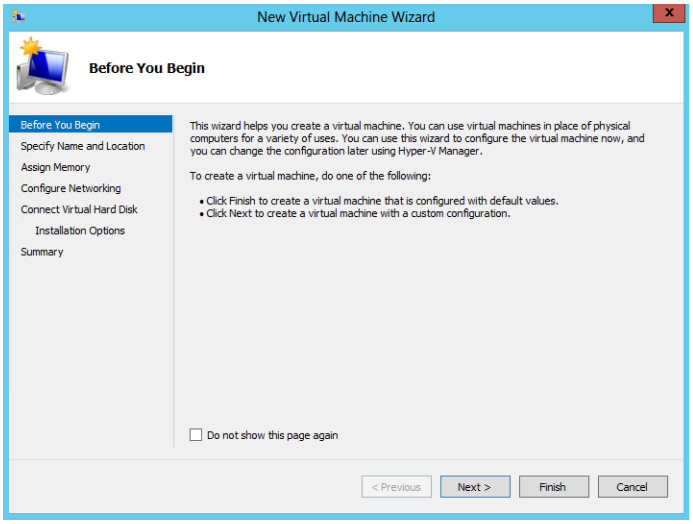


FortiManager VM HV

Created: 10/22/2013 3:42:20 PM
Notes: None
Clustered: No
Heartbeat: OK (No Application Data)

Displays the New Virtual Machine Wizard.

3. Right-click the server and select *New* > *Virtual Machine* from the menu. Optionally, in the *Actions* menu, select *New* and select *Virtual Machine* from the menu. The *New Virtual Machine Wizard* opens.



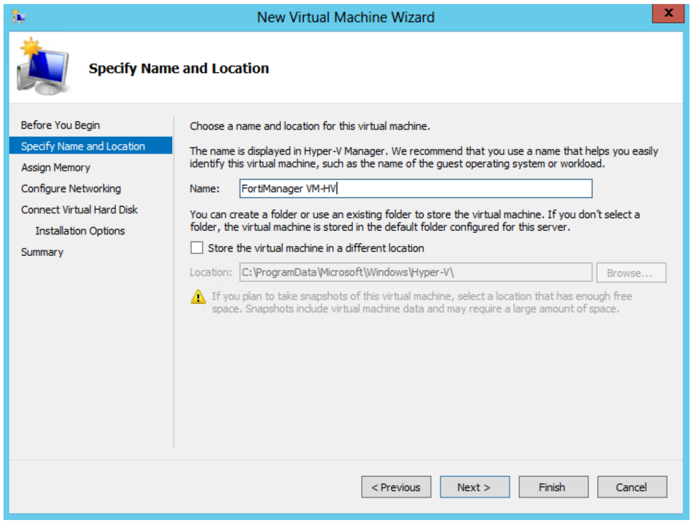
This wizard helps you create a virtual machine. You can use virtual machines in place of physical computers for a variety of uses. You can use this wizard to configure the virtual machine now, and you can change the configuration later using Hyper-V Manager.

To create a virtual machine, do one of the following:

- Click Finish to create a virtual machine that is configured with default values.
- Click Next to create a virtual machine with a custom configuration.

□ Do not show this page again

4. Select *Next* to create a VM with a custom configuration. The *Specify Name and Location* page is displayed.



Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

Name: FortiManager VM-HV

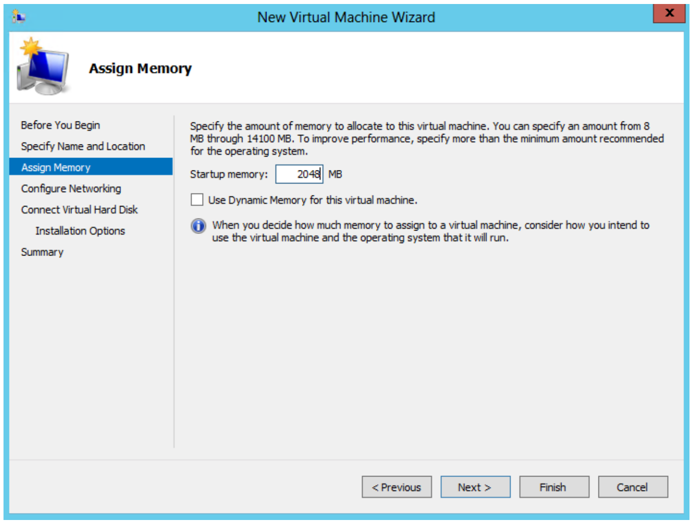
You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

□ Store the virtual machine in a different location

Location: C:\ProgramData\Microsoft\Windows\Hyper-V\

If you plan to take snapshots of this virtual machine, select a location that has enough free space. Snapshots include virtual machine data and may require a large amount of space.

5. Enter a name for this VM. Hyper-V Manager displays the name.
6. Select *Next* to continue. The *Assign Memory* page opens.



Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 8 MB through 14100 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

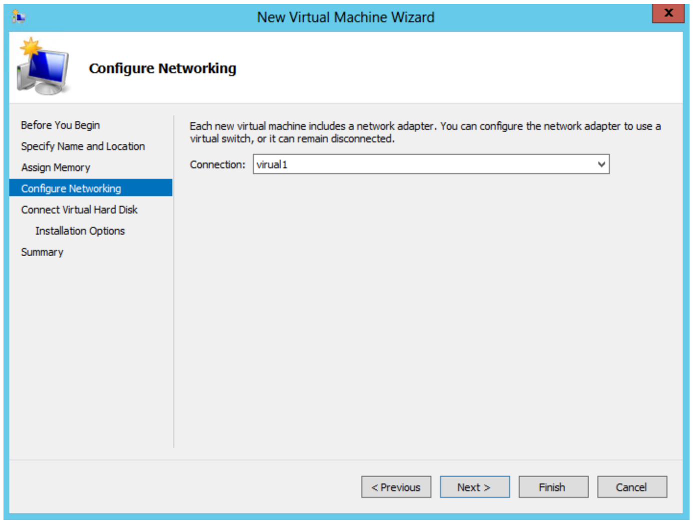
Startup memory: 2048 MB

□ Use Dynamic Memory for this virtual machine.

When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.

7. Specify the amount of memory to allocate to this VM. The default memory for FortiGate-VM is 1GB (1024MB).

8. Select *Next* to continue. The *Configure Networking* page is displayed.



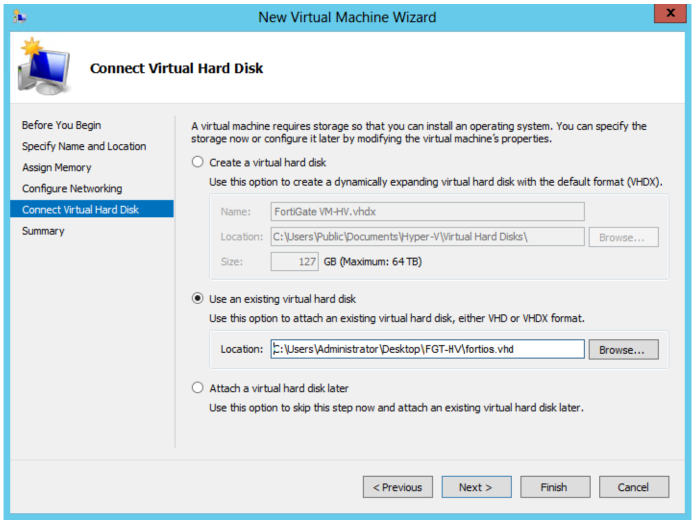
Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: virual1

9. Each new VM includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiGate-VM requires four network adapters. You must configure network adapters in the *Settings* page.

10. Select *Next* to continue. The *Connect Virtual Hard Disk* page is displayed.



Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a dynamically expanding virtual hard disk with the default format (VHDX).

Name: FortiGate VM-HV.vhdx

Location: C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

● Use an existing virtual hard disk

Use this option to attach an existing virtual hard disk, either VHD or VHDX format.

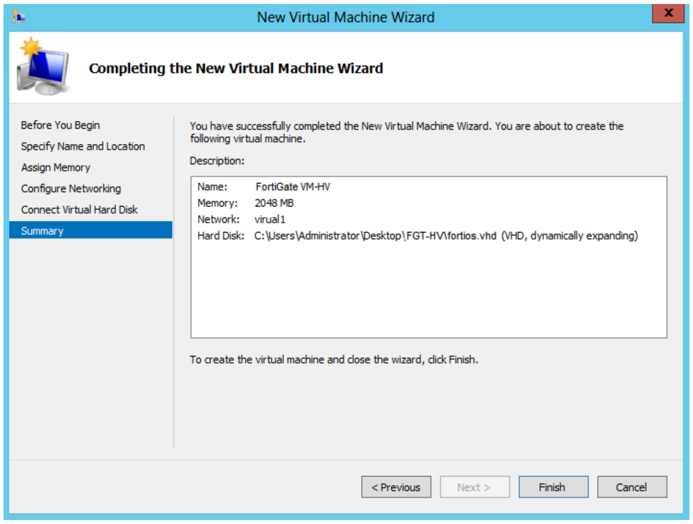
Location: C:\Users\Administrator\Desktop\FGT-HV\fortios.vhd

○ Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.

11. Select to use an existing virtual hard disk and browse for the `fortios.vhd` file that you downloaded from the Fortinet Customer Service & Support portal.

12. Select *Next* to continue. The *Summary* page is displayed.



Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

```
Name:      FortiGate VM-HV
Memory:    2048 MB
Network:   virual1
Hard Disk: C:\Users\Administrator\Desktop\FGT-HV\fortios.vhd (VHD, dynamically expanding)
```

To create the virtual machine and close the wizard, click Finish.

13. To create the VM and close the wizard, select *Finish*.

Initial settings

After you deploy a FortiGate-VM on the Microsoft Hyper-V server, perform the following tasks:

- Connect the FortiGate-VM to the network so that it can process network traffic and maintain license validity.
- Connect to FortiGate-VM GUI via a web browser for easier administration.
- Ensure that the full license file is uploaded to the FortiGate-VM.
- If you are in a closed environment, enable validation of the FortiGate-VM license against a FortiManager on your network.

Network configuration

The first time you start the FortiGate-VM, you will have access only through the console window of your Microsoft Hyper-V server environment. After you configure one FortiGate network interface with an IP address and administrative access, you can access the FortiGate-VM GUI.

Configuring port 1

VM platform or hypervisor management environments include a guest console window. On the FortiGate-VM, this provides access to the FortiGate console, equivalent to the console port on a hardware FortiGate unit. Before you can access the GUI, you must configure FortiGate-VM port1 with an IP address and administrative access.

To configure the port1 IP address:

1. In your hypervisor manager, start the FortiGate-VM and access the console window. You may need to press *Enter* to see a login prompt.
2. At the FortiGate-VM login prompt enter the username `admin`. By default there is no password. Press Enter.

3. Using CLI commands, configure the port1 IP address and netmask:

```
config system interface
   edit port1
      set mode static
      set ip 192.168.0.100 255.255.255.0
   next
end
```

4. To configure the default gateway, enter the following CLI commands:

```
config router static
   edit 1
      set device port1
      set gateway <class_ip>
   next
end
```

You must configure the default gateway with an IPv4 address. FortiGate-VM needs to access the Internet to contact the FortiGuard Distribution Network (FDN) to validate its license.

5. To configure your DNS servers, enter the following CLI commands:

```
config system dns
   set primary <Primary DNS server>
   set secondary <Secondary DNS server>
end
```

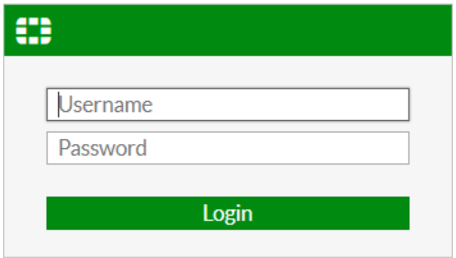
The default DNS servers are `208.91.112.53` and `208.91.112.52`.

Connecting to the FortiGate-VM GUI

You connect to the FortiGate-VM GUI via a web browser by entering the IP address assigned to the port 1 interface (see Configuring port 1 on page 19) in the browser location field. You must enable HTTP and/or HTTPS access and administrative access on the interface to ensure that you can connect to the GUI. If you only enabled HTTPS access, enter "https://" before the IP address.

When you use HTTP rather than HTTPS to access the GUI, certain web browsers may display a warning that the connection is not private.

On the FortiGate-VM GUI login screen, enter the default username "admin" and then select *Login*. FortiOS does not assign a default password to the admin user.



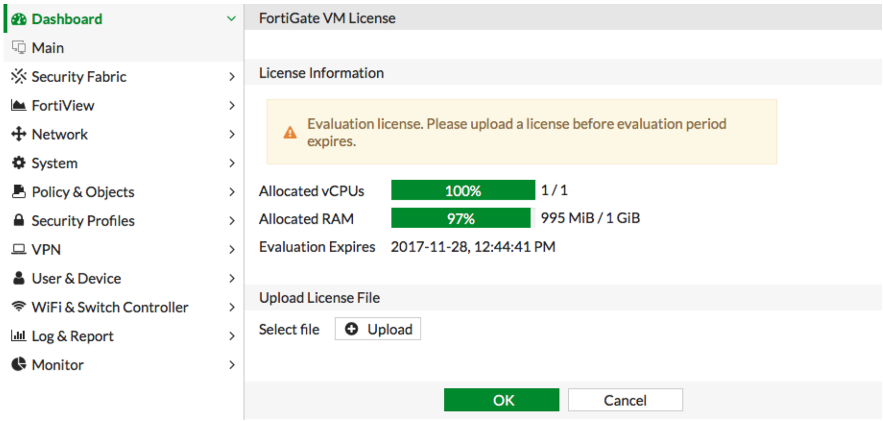
Fortinet recommends that you configure a password for the admin user as soon as you log in to the FortiGate-VM GUI for the first time.

Uploading the FortiGate-VM license

Every Fortinet VM includes a 15-day trial license. During this time the FortiGate-VM operates in evaluation mode. Before using the FortiGate-VM, you must enter the license file that you downloaded from Customer Service & Support upon registration.

To upload the FortiGate-VM license file via the GUI:

1. Do one of the following to access the license upload window:
   - In *Dashboard > Status* window, in the *Virtual Machine* widget, click the *FGVMEV* (FortiGate-VM Evaluation) *License* icon. This reveals a menu of selections to take you directly to the *FortiGate VM License* window or to the *FortiGuard Details* window.
   - Go to *System > FortiGuard*. In the *License Information* section, go to the *Virtual Machine* row and click *FortiGate VM License*.
2. In the *Evaluation License* dialog, select *Enter License*. The license upload page opens.



Evaluation license. Please upload a license before evaluation period expires.

Allocated vCPUs 100% 1 / 1

Allocated RAM 97% 995 MiB / 1 GiB

Evaluation Expires 2017-11-28, 12:44:41 PM

3. Select *Upload* and locate the license file (`.lic`) on your computer.
4. Select *OK* to upload the license file.
5. Refresh the browser to log in.
6. Enter `admin` in the Name field and select *Login*.
   The VM registration status appears as valid in the License Information widget after the license is validated by the FortiGuard Distribution Network (FDN) or FortiManager for closed networks.

Modern browsers can have an issue with allowing connecting to a FortiGate if the encryption on the device is too low. If this happens, use an FTP/TFTP server to apply the license.

To upload the FortiGate-VM license file via the CLI:

You can also upload the license file using the following CLI command:

```
execute restore vmlicense {ftp | tftp} <filenmame string> <ftp server>[:ftp port]
```

Example:

The following is an example output when using a TFTP server to install a license:

```
execute restore vmlicense tftp license.lic 10.0.1.2
   This operation will overwrite the current VM license!Do you want to continue? (y/n)y
   Please wait...Connect to tftp server 10.0.1.2 ...
   Get VM license from tftp server OK.
   VM license install succeeded.
   Rebooting firewall.
```

This command automatically reboots the firewall without giving you a chance to back out or delay the reboot.

Validating the FortiGate-VM license with FortiManager

You can validate your FortiGate-VM license with some FortiManager models. To determine whether your FortiManager has the VM activation feature, see the FortiManager datasheet's Features section.

To validate your FortiGate-VM with your FortiManager:

1. To configure your FortiManager as a closed network, enter the following CLI command on your FortiManager:
```
config fmupdate publicnetwork
   set status disable
end
```
2. To configure FortiGate-VM to use FortiManager as its override server, enter the following CLI commands on your FortiGate-VM:
```
config system central-management
   set mode normal
   set type fortimanager
   set fmg <FortiManager IPv4 address>
   config server-list
      edit 1
         set server-type update
         set server-address <FortiManager IPv4 address>
      end
   end
   set fmg-source-ip <Source IPv4 address when connecting to the FortiManager>
   set include-default-servers disable
   set vdom <Enter the VDOM name to use when communicating with the FortiManager>
```

```
end
```

3. Load the FortiGate-VM license file in the GUI:
   a. Go to *System > Dashboard > Status*.
   b. In the *License Information* widget, in the *Registration Status* field, select *Update*.
   c. Browse for the `.lic` license file and select *OK*.
4. To activate the FortiGate-VM license, enter the `execute update-now` command on your FortiGate-VM.
5. To check the FortiGate-VM license status, enter the following CLI commands on your FortiGate-VM:

```
get system status
   Version: Fortigate-VM v5.0,build0099,120910 (Interim)
   Virus-DB: 15.00361(2011-08-24 17:17)
   Extended DB: 15.00000(2011-08-24 17:09)
   Extreme DB: 14.00000(2011-08-24 17:10)
   IPS-DB: 3.00224(2011-10-28 16:39)
   FortiClient application signature package: 1.456(2012-01-17 18:27)
   Serial-Number: FGVM02Q105060000
   License Status: Valid
   BIOS version: 04000002
   Log hard disk: Available
   Hostname: Fortigate-VM
   Operation Mode: NAT
   Current virtual domain: root
   Max number of virtual domains: 10
   Virtual domains status: 1 in NAT mode, 0 in TP mode
   Virtual domain configuration: disable
   FIPS-CC mode: disable
   Current HA mode: standalone
   Distribution: International
   Branch point: 511
   Release Version Information: MR3 Patch 4
   System time: Wed Jan 18 11:24:34 2012

diagnose hardware sysinfo vm full
   UUID: 564db33a29519f6b1025bf8539a41e92
   valid: 1
   status: 1
   code: 200 (If the license is a duplicate, code 401 displays)
   warn: 0
   copy: 0
   received: 45438
   warning: 0
   recv: 201201201918
   dup:
```

Licensing timeout

In closed environments without Internet access, you must license the FortiGate-VM offline using a FortiManager as a license server. If the FortiGate-VM cannot validate its license within the 30-day license timeout period, the FortiGate discards all packets, effectively ceasing operation as a firewall.

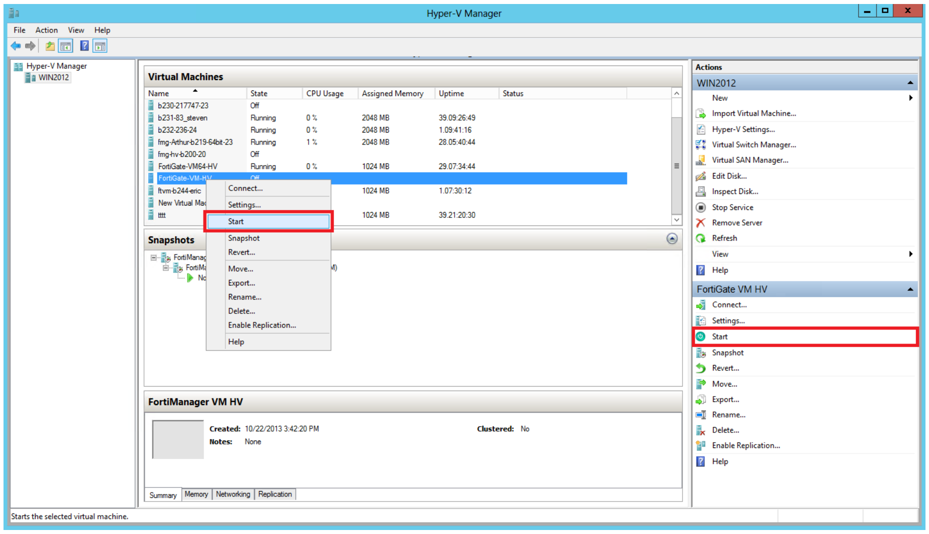
The license status goes through some changes before it times out:

Status	Description
Valid	The FortiGate can connect and validate against a FortiManager or FDS.
Warning	The FortiGate cannot connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is less than 30 days the status does not change.
Invalid	The FortiGate cannot connect and validate against a FortiManager or FDS. A check is made against how many days the Warning status has been continuous. If the number is 30 days or more, the status changes to Invalid. The firewall ceases to function properly.

There is only a single log entry after the FortiGate-VM cannot access the license server for the license expiration period. When you search the logs for the reason that the FortiGate is offline, there is not a long error log list that draws attention to the issue. There is only one entry.

Testing connectivity

You can now proceed to power on your FortiGate-VM. Select the FortiGate-VM in the VM list, right-click, and select *Start*. Optionally, you can select the FortiGate-VM in the VM list and select *Start* in the *Actions* menu.



Name	State	CPU Usage	Assigned Memory	Uptime	Status
b230-217747-23	Off				
b231-83_steven	Running	0 %	2048 MB	39.09:26:49	
b232-236-24	Running	0 %	2048 MB	1.09:41:16	
fmg-Arthur-b219-64bit-23	Running	1 %	2048 MB	28.05:40:44	
fmg-hv-b200-20	Off				
FortiGate-VM64-HV	Running	0 %	1024 MB	29.07:34:44	
FortiGate-VM-HV	Off				
ftvm-b244-eric			1024 MB	1.07:30:12	
New Virtual Mac					
tttt			1024 MB	39.21:20:30	

FortiManager VM HV

Created: 10/22/2013 3:42:20 PM **Clustered:** No
Notes: None

Starts the selected virtual machine.

The PING utility is the usual method to test connectivity to other devices. For this, you need the console on the FortiGate-VM.

In FortiOS, the command for the PING utility is `execute ping` followed by the IP address you want to connect to.

Before you configure the FortiGate-VM for use in production, ensure that connections between it and all required resources can be established.

- If the FortiGate-VM will provide firewall protection between your network and the internet, verify that it can connect to your Internet access point and to resources on the Internet.
- If the FortiGate-VM is part of a Fortinet Security Fabric, verify that it can connect to all devices in the Fabric.
- Verify that each node on your network can connect to the FortiGate-VM.

Configuring your FortiGate-VM

For information about configuring and operating the FortiGate-VM after successful deployment and startup on the hypervisor, see the *FortiOS Administration Guide*.

High availability

FortiGate-VM HA supports having two VMs in an HA cluster on the same physical platform or different platforms. The primary consideration is that all interfaces involved can communicate efficiently over TCP/IP connection sessions.

Heartbeat

There are two options for setting up the HA heartbeat: unicast and broadcast. Broadcast is the default HA heartbeat configuration. However, the broadcast configuration may not be ideal for FortiGate-VM because it may require special settings on the host. In most cases, the unicast configuration is preferable.

Differences between the unicast and broadcast heartbeat setups are:

- The unicast method does not change the FortiGate-VM interface MAC addresses to virtual MAC addresses.
- Unicast HA only supports two FortiGate-VMs.
- Unicast HA heartbeat interfaces must be connected to the same network and you must add IP addresses to these interfaces.

Unicast

You can configure the unicast settings in the FortiOS CLI:

```
config system ha
   set unicast-hb {enable/disable}
   set unicast-hb-peerip {Peer heartbeat interface IP address}
end
```

Setting	Description
`unicast-hb`	Enable or disable default unicast HA heartbeat.
`unicast-hb-peerip`	IP address of the HA heartbeat interface of the other FortiGate-VM in the HA cluster.

Broadcast

Broadcast HA heartbeat packets are non-TCP packets that use Ethertype values 0x8890, 0x8891, and 0x8890. These packets use automatically assigned link-local IPv4 addresses in the 169.254.0.x range for HA heartbeat interface IP addresses.

For FortiGate-VMs to support a broadcast HA heartbeat configuration, you must configure the virtual switches that connect heartbeat interfaces to support MAC address spoofing.

In addition, you must configure the VM platform to allow MAC address spoofing for the FortiGate-VM data interfaces. This is required because in broadcast mode, the FGCP applies virtual MAC addresses to FortiGate data interfaces, and these virtual MAC addresses mean that matching interfaces of the FortiGate-VM instances in the cluster have the same virtual MAC addresses.

With the correct MAC spoofing settings, you can configure HA between two or more FortiGate-VM for Hyper-V instances.

Optimizing FortiGate-VM performance

You can optimize FortiGate-VM performance by configuring interrupt-affinity and packet-distribution-affinity attributes to improve efficiency and resource utilization.

SR-IOV

FortiGate-VMs installed on Microsoft Hyper-V platforms support Single Root I/O virtualization (SR-IOV) to provide FortiGate-VMs with direct access to physical network cards. Enabling SR-IOV means that one PCIe network card or CPU can function for a FortiGate-VM as multiple separate physical devices. SR-IOV reduces latency and improves CPU efficiency by allowing network traffic to pass directly between a FortiGate-VM and a network card, bypassing Microsoft Hyper-V host software and without using virtual switching.

FortiGate-VMs benefit from SR-IOV because SR-IOV optimizes network performance and reduces latency and CPU usage. FortiGate-VMs do not use Microsoft Hyper-V features that are incompatible with SR-IOV, so you can enable SR-IOV without negatively affecting your FortiGate-VM. SR-IOV implements an I/O memory management unit (IOMMU) to differentiate between different traffic streams and apply memory and interrupt translations between the physical functions (PF) and virtual functions (VF).

Setting up SR-IOV on Microsoft Hyper-V involves creating a PF for each physical network card in the hardware platform. Then, you create VFs that allow FortiGate-VMs to communicate through the PF to the physical network card. VFs are actual PCIe hardware resources and only a limited number of VFs are available for each PF.

SR-IOV hardware compatibility

SR-IOV requires that the hardware and operating system on which your Microsoft Hyper-V host is running has BIOS, physical NIC, and network driver support for SR-IOV.

To enable SR-IOV, your Microsoft Hyper-V platform must be running on hardware that is compatible with SR-IOV and with FortiGate-VMs. FortiGate-VMs require network cards that are compatible with ixgbevf or i40evf drivers. As well, the host hardware CPUs must support second level address translation (SLAT).

For optimal SR-IOV support, install the most up to date ixgbevf or i40e/i40evf network drivers. Fortinet recommends i40e/i40evf drivers because they provide four TxRx queues for each VF and ixgbevf only provides two TxRx queues.

Creating an SR-IOV virtual switch

Begin configuring SR-IOV by creating a Microsoft Hyper-V external virtual switch with SR-IOV support. You can use the Microsoft Hyper-V Manager or PowerShell command line.

You can only add SR-IOV to a new virtual switch. You cannot modify an existing virtual switch to enable SR-IOV and you cannot disable SR-IOV for a virtual switch that was already added. To add or remove SR-IOV from a virtual switch you must delete it and then readd it.

From the Microsoft Hyper-V Manager:

1. Open the Virtual Switch Manager.
2. Create a new virtual switch.
3. Add a name and other settings as required.
4. Set the *Connection type* to *External network* and select *Enable single-root I/O virtualization (SR-IOV)*.

From PowerShell:

1. Enter the `Get-NetAdapter` command to view the list of available network adapters.
2. Enter the following command to add a new virtual switch:
   ```
   New-VMSwitch <virtual-switch-name> -netadaptername <network-adapter-name> -EnableIov
         $true
   ```
   Where `<virtual-switch-name>` is the name of the virtual switch that you are creating, and `<network-adapter-name>` is the name of the network adapter that you are binding the virtual switch to.

Enabling SR-IOV for a FortiGate-VM

The following procedure requires shutting down and restarting the FortiGate-VM. Therefore, you should perform it during a quiet time or maintenance window when the network is not busy.

From the Microsoft Hyper-V Manager:

1. Open the FortiGate-VM settings, expand the *Network Adapter* node, and select *Hardware Acceleration*.
2. On the *Hardware Acceleration* page, select *Enable SR-IOV*.

From PowerShell:

```
Set-VMNetworkAdapter IOV8250 -IovWeight 50 -Passthru | fl "iov", "status", "virtualfunction"
```

Interrupt affinity

In addition to enabling SR-IOV in the VM host, to fully take advantage of SR-IOV performance improvements you must configure interrupt affinity for your FortiGate-VM. Interrupt affinity (also called CPU affinity) maps FortiGate-VM interrupts to the CPUs that are assigned to your FortiGate-VM. You use a CPU affinity mask to define the CPUs that the interrupts are assigned to.

A common use of this feature is to improve your FortiGate-VM's networking performance by:

- On the VM host, add multiple host CPUs to your FortiGate-VM.
- On the VM host, configure CPU affinity to specify the CPUs that the FortiGate-VM can use.
- On the VM host, configure other VM clients on the VM host to use other CPUs.
- On the FortiGate-VM, assign network interface interrupts to a CPU affinity mask that includes the CPUs that the FortiGate-VM can use.

In this way, all available CPU interrupts for the configured host CPUs are used to process traffic on your FortiGate interfaces. This configuration could lead to improve FortiGate-VM network performance because you have dedicated VM host CPU cycles to processing your FortiGate-VM's network traffic.

You can use the following CLI command to configure interrupt affinity for your FortiGate-VM:

```
config system affinity-interrupt
   edit <index>
      set interrupt <interrupt-name>
      set affinity-cpumask <cpu-affinity-mask>
   next
end
```

Where:

- `<interrupt-name>` is the name of the interrupt to associate with a CPU affinity mask. You can view your FortiGate-VM interrupts using the `diagnose hardware sysinfo interrupts` command. Usually you associate all of the interrupts for a given interface with the same CPU affinity mask.
- `<cpu-affinity-mask>` is the CPU affinity mask for the CPUs that will process the associated interrupt.

For example, consider the following configuration:

- The port2 and port3 interfaces of a FortiGate-VM send and receive most of the traffic.
- On the VM host you have set up CPU affinity between your FortiGate-VM and four CPUs (CPU 0, 1 , 2, and 3).
- SR-IOV is enabled and SR-IOV interfaces use the i40evf interface driver.

The output from the `diagnose hardware sysinfo interrupts` command shows that port2 has the following transmit and receive interrupts:

```
i40evf-port2-TxRx-0
i40evf-port2-TxRx-1
i40evf-port2-TxRx-2
i40evf-port2-TxRx-3
```

The output from the `diagnose hardware sysinfo interrupts` command shows that port3 has the following transmit and receive interrupts:

```
i40evf-port3-TxRx-0
i40evf-port3-TxRx-1
i40evf-port3-TxRx-2
i40evf-port3-TxRx-3
```

Use the following command to associate the port2 and port3 interrupts with CPU 0, 1 , 2, and 3.

```
config system affinity-interrupt
   edit 1
      set interrupt "i40evf-port2-TxRx-0"
      set affinity-cpumask "0x0000000000000001"
   next
   edit 2
      set interrupt "i40evf-port2-TxRx-1"
      set affinity-cpumask "0x0000000000000002"
   next
   edit 3
      set interrupt "i40evf-port2-TxRx-2"
      set affinity-cpumask "0x0000000000000004"
   next
   edit 4
      set interrupt "i40evf-port2-TxRx-3"
      set affinity-cpumask "0x0000000000000008"
   next
   edit 1
      set interrupt "i40evf-port3-TxRx-0"
      set affinity-cpumask "0x0000000000000001"
   next
   edit 2
      set interrupt "i40evf-port3-TxRx-1"
      set affinity-cpumask "0x0000000000000002"
   next
   edit 3
      set interrupt "i40evf-port3-TxRx-2"
      set affinity-cpumask "0x0000000000000004"
   next
   edit 4
      set interrupt "i40evf-port3-TxRx-3"
      set affinity-cpumask "0x0000000000000008"
   next
end
```

Packet-distribution affinity

With SR-IOV enabled on the VM host and interrupt affinity configured on your FortiGate-VM there is one additional configuration you can add that may improve performance. Most common network interface hardware has restrictions on the number of RX/TX queues that it can process. This can result in some CPUs being much busier than others and the busy CPUs may develop extensive queues.

You can get around this potential bottleneck by configuring affinity packet redistribution to allow overloaded CPUs to redistribute packets they receive to other less busy CPUs. The may result in a more even distribution of packet processing to all available CPUs.

You configure packet redistribution for interfaces by associating an interface with an affinity CPU mask. This configuration distributes packets set and received by that interface to the CPUs defined by the CPU affinity mask associated with the interface.

You can use the following CLI command to configure affinity packet redistribution for your FortiGate-VM:

```
config system affinity-packet-redistribution
   edit <index>
      set interface <interface-name>
      set affinity-cpumask <cpu-affinity-mask>
   next
end
```

Where:

- `<interface-name>` the name of the interface to associate with a CPU affinity mast.
- `<cpu-affinity-mask>` the CPU affinity mask for the CPUs that will process packets to and from the associated interface.

For example, you can improve the performance of the interrupt affinity example shown in the following command to allow packets sent and received by the port3 interface to be redistributed to CPUs according to the 0xE CPU affinity mask.

```
config system affinity-packet-redistribution
   edit 1
      set interface port3
      set affinity-cpumask "0xE"
   next
end
```

Setting up FortiGate-VM HA for a Microsoft Hyper-V Live Migration environment

This guide provides sample configuration of Live Migration FortiGate-VM HA in a Microsoft Hyper-V environment. This feature enables the live migration of a running FortiGate-VM from one physical server to another with zero downtime, continuous service availability, and complete transaction integrity. It also provides transparency to users.

In VM environments that do not support broadcast communication, you can set up a unicast HA heartbeat when configuring HA. Setting up a unicast HA heartbeat consists of enabling the feature and adding a peer IP address. The peer IP address is the IP address of the HA heartbeat interface of the other FortiGate-VM in the HA cluster.

This configuration consists of the following components:

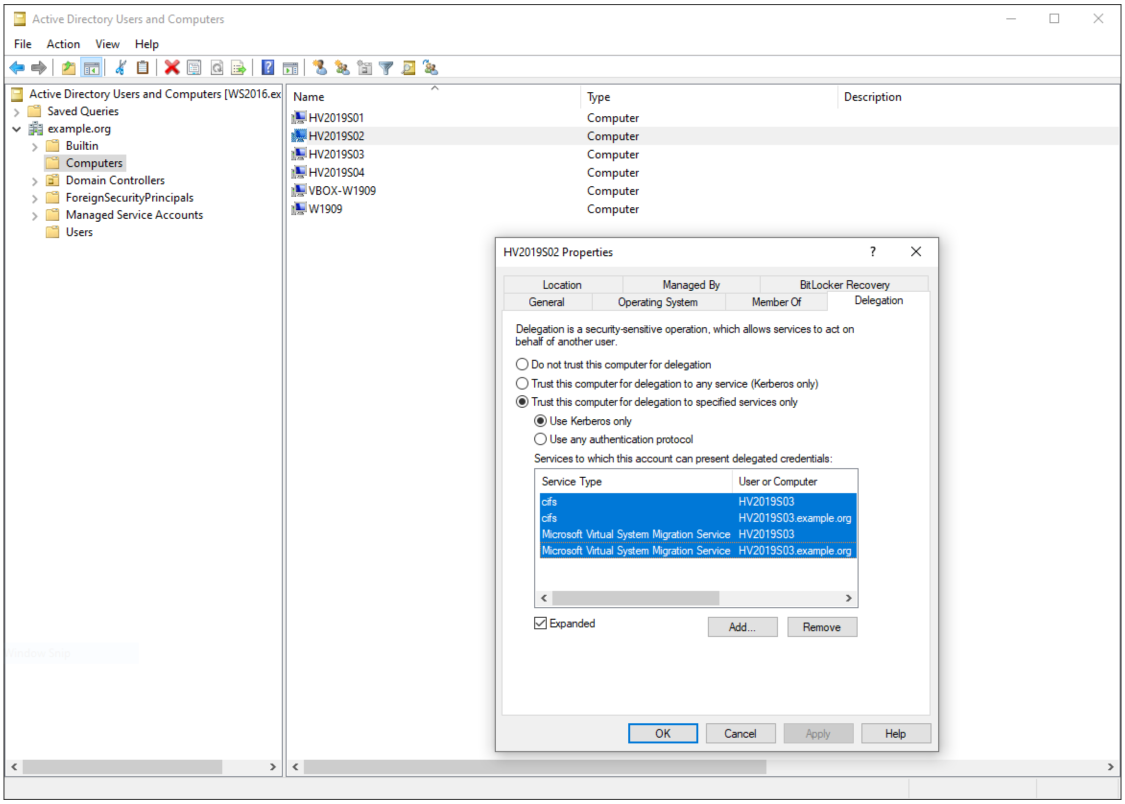
- Two Windows Server 2019 machines, each with four network adapters installed and with Hyper-V role. This guide assumes that you have installed and set up these machines as per Microsoft documentation, and that they have joined a domain. In this example, the machines are HV2019S02 and HV2019S03 and have joined domain example.org.
- Two FortiGate-VM64-HVs deployed on HV2019S02 with FortiOS 6.4.3

To set up FortiGate-VM HA for a Microsoft Hyper-V Live Migration environment:

1. Set up hosts for live migration without failover clustering. See Set up hosts for live migration without Failover Clustering.
2. Use live migration without failover clustering to move a virtual machine. See Use live migration without Failover Clustering to move a virtual machine.
3. In Active Directory Users and Computers, configure the following for HV2019S02 and HV2019S03. See Live Migration via Constrained Delegation with Kerberos in Windows Server 2016 for details:

a. Configure constrained delegation.

b. On the *Delegation* tab, add cifs and Microsoft Virtual System Migration Service.


Active Directory Users and Computers
File
Action
View
Help
Active Directory Users and Computers [WS2016.ex
Saved Queries
example.org
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Managed Service Accounts
Users

Name	Type	Description
HV2019S01	Computer	
HV2019S02	Computer	
HV2019S03	Computer	
HV2019S04	Computer	
VBOX-W1909	Computer	
W1909	Computer	

HV2019S02 Properties

Delegation is a security-sensitive operation, which allows services to act on behalf of another user.

○ Do not trust this computer for delegation
○ Trust this computer for delegation to any service (Kerberos only)
● Trust this computer for delegation to specified services only
● Use Kerberos only
○ Use any authentication protocol

Services to which this account can present delegated credentials:

Service Type	User or Computer
cifs	HV2019S03
cifs	HV2019S03.example.org
Microsoft Virtual System Migration Service	HV2019S03
Microsoft Virtual System Migration Service	HV2019S03.example.org

☑ Expanded

4. Configure HV2019S02 settings:

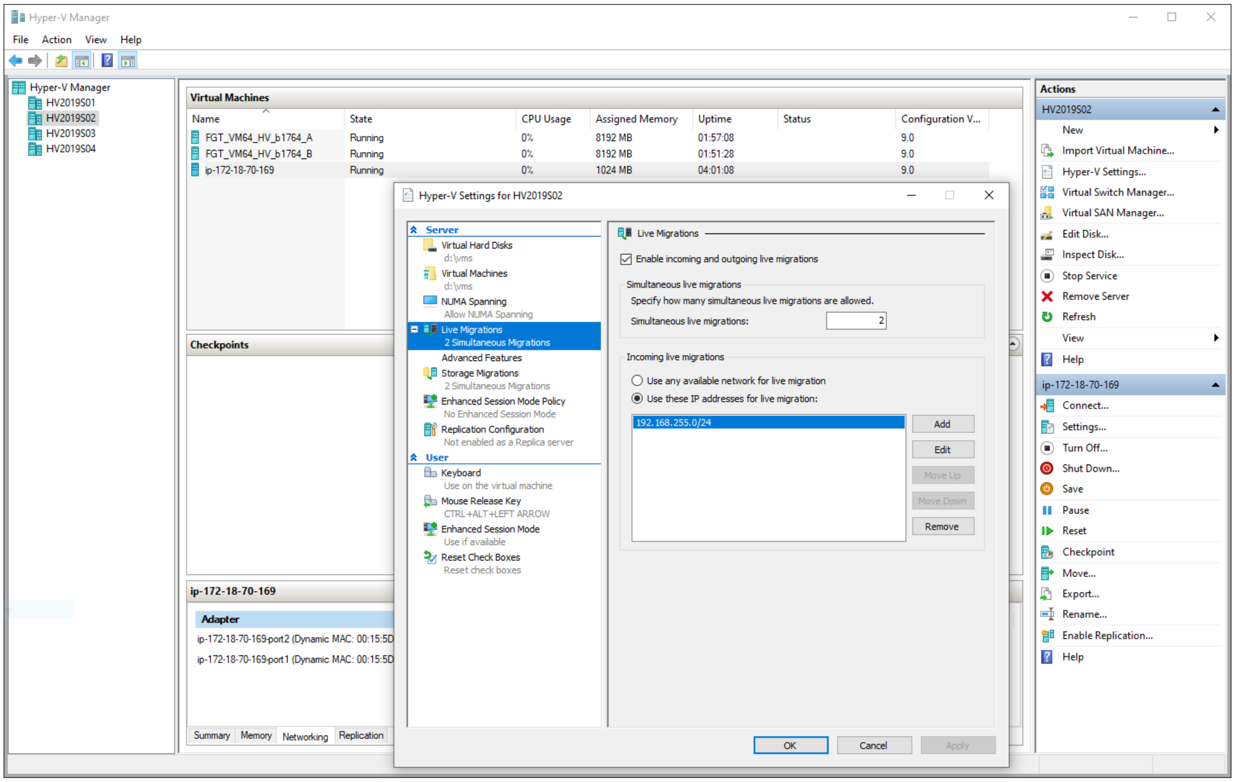
```
PS C:\Users\exampleuser> Add-VMMigrationNetwork 192.168.255.0/24
PS C:\Users\exampleuser> Get-VMMigrationNetwork | fl *

Subnet       : 192.168.255.0/24
Priority     : 0
CimSession   : CimSession: .
ComputerName : HV2019S02
IsDeleted    : False


PS C:\Users\exampleuser>
PS C:\Users\exampleuser> Get-VMHost | fl *

ComputerName                                 : HV2019S02
LogicalProcessorCount                        : 24
ResourceMeteringSaveInterval                 : 01:00:00
HostNumaStatus                               : {HV2019S02}
NumaStatus                                   : {ip-172-18-70-169}
IovSupport                                   : True
IovSupportReasons                            :
InternalNetworkAdapters                      : {MGMT, VSW-port3, VSW-port2,
                                            VSW-port4}
ExternalNetworkAdapters                   : {SRIOV-X710-p1_External,
                                            MGMT_External, VSW-port1_External,
                                            SRIOV-X710-p2_External}
SupportedVmVersions                       : {5.0, 6.2, 7.0, 7.1…}
SecureBootTemplates                       : {MicrosoftWindows,
                                            MicrosoftUEFICertificateAuthority,
                                            OpenSourceShieldedVM}
EnableEnhancedSessionMode                 : False
FibreChannelWwnn                          : C003FF0000FFFF00
FibreChannelWwpnMaximum                   : C003FF105350FFFF
FibreChannelWwpnMinimum                   : C003FF1053500000
MacAddressMaximum                         : 00155DD775FF
MacAddressMinimum                         : 00155DD77500
NumaSpanningEnabled                       : True
VirtualHardDiskPath                       : E:\vms\
VirtualMachinePath                        : E:\vms\
FullyQualifiedDomainName                  : example.org
MemoryCapacity                            : 68185321472
Name                                      : HV2019S02
MaximumStorageMigrations                  : 2
MaximumVirtualMachineMigrations           : 2
UseAnyNetworkForMigration                 : False
VirtualMachineMigrationAuthenticationType : Kerberos
VirtualMachineMigrationEnabled            : True
VirtualMachineMigrationPerformanceOption  : SMB
CimSession                                : CimSession: .
IsDeleted                                 : False


PS C:\Users\exampleuser>
```



Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configuration V...
FGT_VM64_HV_b1764_A	Running	0%	8192 MB	01:57:08		9.0
FGT_VM64_HV_b1764_B	Running	0%	8192 MB	01:51:28		9.0
ip-172-18-70-169	Running	0%	1024 MB	04:01:08		9.0

Live Migrations

☑ Enable incoming and outgoing live migrations

Simultaneous live migrations

Specify how many simultaneous live migrations are allowed.

Simultaneous live migrations: 2

Incoming live migrations

○ Use any available network for live migration

● Use these IP addresses for live migration:

192.168.255.0/24

5. Configure HV2019S03 settings:

```
PS C:\Users\exampleuser> Add-VMMigrationNetwork 192.168.255.0/24
PS C:\Users\exampleuser> Get-VMMigrationNetwork | fl *

Subnet       : 192.168.255.0/24
Priority     : 0
CimSession   : CimSession: .
ComputerName : HV2019S03
IsDeleted    : False


PS C:\Users\exampleuser>
PS C:\Users\exampleuser> Get-VMHost | fl *

ComputerName                              : HV2019S03
LogicalProcessorCount                     : 24
ResourceMeteringSaveInterval              : 01:00:00
HostNumaStatus                            : {HV2019S03}
NumaStatus                                : {ip-172-18-70-170,
                                            FGT_VM64_HV_b1723_B,
                                            FGT_VM64_HV_b1723_A}
IovSupport                                : True
IovSupportReasons                         :
InternalNetworkAdapters                   : {VSW-port4, VSW-port2, VSW-port3,
                                            MGMT}
```

```
ExternalNetworkAdapters                     : {VSW-port1_External,
                                              SRIOV-X710-p2_External,
                                              MGMT_External,
                                              SRIOV-X710-p1_External}
SupportedVmVersions                         : {5.0, 6.2, 7.0, 7.1…}
SecureBootTemplates                         : {MicrosoftWindows,
                                              MicrosoftUEFICertificateAuthority,
                                              OpenSourceShieldedVM}
EnableEnhancedSessionMode                   : False
FibreChannelWwnn                            : C003FF0000FFFF00
FibreChannelWwpnMaximum                     : C003FF06263EFFFF
FibreChannelWwpnMinimum                     : C003FF06263E0000
MacAddressMaximum                           : 00155D8B30FF
MacAddressMinimum                           : 00155D8B3000
NumaSpanningEnabled                         : True
VirtualHardDiskPath                         : E:\vms\
VirtualMachinePath                          : E:\vms\
FullyQualifiedDomainName                    : example.org
MemoryCapacity                              : 68185321472
Name                                        : HV2019S03
MaximumStorageMigrations                    : 2
MaximumVirtualMachineMigrations             : 2
UseAnyNetworkForMigration                   : False
VirtualMachineMigrationAuthenticationType : Kerberos
VirtualMachineMigrationEnabled              : True
VirtualMachineMigrationPerformanceOption   : SMB
CimSession                                  : CimSession: .
IsDeleted                                   : False


PS C:\Users\exampleuser>
```

6. There are several virtual switches created on each Microsoft Hyper-V server for FortiGate-VMs to connect to physical networks and those VMs on protected networks:

Switch	Connection
VSW-port1	External network to Internet.
MGMT	External network to management network.
SRIOV-X710-p1	External network to a closed network.
SRIOV-X710-p2	External network to protected networks.

Ensure that each FortiGate-VM's interfaces are connected to the virtual switches per the following and that you have enabled MAC address spoofing to all interfaces:

Port	Switch
port1	VSW-port1

Port	Switch
port2	MGMT
port3	SRIOV-X710-p1
port4	SRIOV-X710-p2

7. Configure the FortiGate-VMs for high availability (HA). For more details on HA, see High availability on page 25:
   a. Configure FortiGate A:

```
config router static
    edit 100
        set gateway 172.31.250.1
        set device port1
    next
end
config system interface
    edit "port1"
        set vdom "root"
        set mode static
        set ip 172.31.250.11/24
        set allowaccess ping
        set alias "to_Internet"
    next
end
config system interface
    edit "port2"
        set vdom "root"
        set mode static
        set ip 172.18.70.181/24
        set allowaccess ping https ssh
        set alias "ha-mgmt"
    next
end
config system interface
    edit "port3"
        set vdom "root"
        set mode static
        set ip 192.168.30.11/24
        set allowaccess ping
        set alias "HA-Sync"
    next
end
config system interface
    edit "port4"
        set vdom "root"
        set ip 192.168.40.1 255.255.255.0
        set allowaccess ping ssh https
        set type physical
```

```
            set snmp-index 4
            config ipv6
                set ip6-address 2001:db8:c0a8:2800::1/64
                set ip6-allowaccess ping ssh https
                set ip6-send-adv enable
                set ip6-manage-flag enable
                set ip6-other-flag enable
                config ip6-prefix-list
                    edit 2001:db8:c0a8:2800::/64
                        set valid-life-time 600
                        set preferred-life-time 600
                    next
                end
            end
        next
    end
    config system ha
        set group-name "FGVM-HA-DEMO"
        set mode a-p
        set hbdev "port3" 100
        set session-pickup enable
        set session-pickup-connectionless enable
        set ha-mgmt-status enable
        config ha-mgmt-interfaces
            edit 1
                set interface "port2"
                set gateway 172.18.70.1
            next
        end
        set override disable
        set ha-direct enable
    end
```

b. Configure FortiGate B:

```
    config system ha
        set group-name "FGVM-HA-DEMO"
        set mode a-p
        set hbdev "port3" 100
        set session-pickup enable
        set session-pickup-connectionless enable
        set ha-mgmt-status enable
        config ha-mgmt-interfaces
            edit 1
                set interface "port2"
                set gateway 172.18.70.1
            next
        end
        set override disable
        set ha-direct enable
```

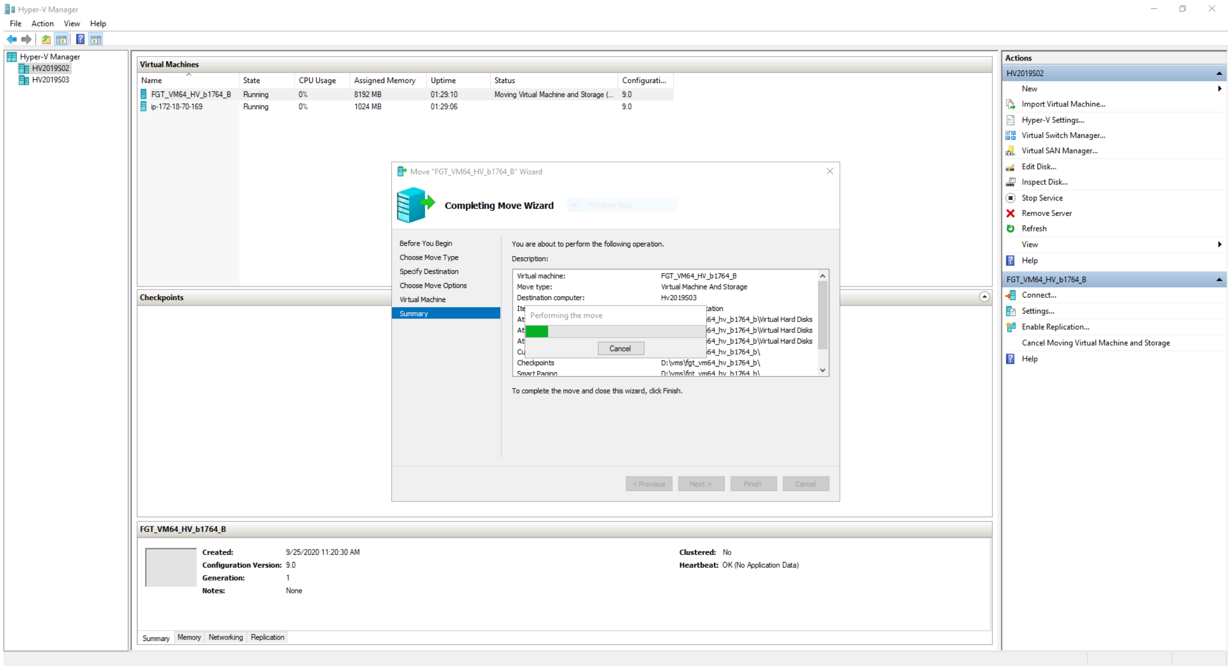
```
end
```

c. Verify HA status:

```
FGT_VM64_HV_A # get system ha status
HA Health Status: OK
Model: FortiGate-VM64-HV
Mode: HA A-P
Group: 0
Debug: 0
Cluster Uptime: 0 days 0:20:0
Cluster state change time: 2020-09-25 13:32:14
Primary selected using:
    <2020/09/25 13:32:14> FGVM08TM20004598 is selected as the primary
because it has the largest value of uptime.
    <2020/09/25 13:31:37> FGVM08TM20004598 is selected as the primary
because it's the only member in the cluster.
    <2020/09/25 13:31:28> FGVM08TM20004598 is selected as the primary
because the peer member FGVM08TM20003583 has SET_AS_SECONDARY flag set.
    <2020/09/25 13:27:43> FGVM08TM20003583 is selected as the primary
because it has the largest value of uptime.
ses_pickup: enable, ses_pickup_delay=disable
override: disable
Configuration Status:
    FGVM08TM20004598(updated 3 seconds ago): in-sync
    FGVM08TM20003583(updated 0 seconds ago): in-sync
System Usage stats:
    FGVM08TM20004598(updated 3 seconds ago):
        sessions=6, average-cpu-user/nice/system/idle=0%/0%/0%/100%,
memory=16%
    FGVM08TM20003583(updated 0 seconds ago):
        sessions=1, average-cpu-user/nice/system/idle=0%/0%/0%/100%,
memory=16%
HBDEV stats:
    FGVM08TM20004598(updated 3 seconds ago):
        port3: physical/10000full, up, rx-
bytes/packets/dropped/errors=3863085/10517/0/0, tx=4211732/11429/0/0
    FGVM08TM20003583(updated 0 seconds ago):
        port3: physical/10000full, up, rx-
bytes/packets/dropped/errors=2583600/6499/0/0, tx=2054873/6169/0/0
Primary     : FGT_VM64_HV_A   , FGVM08TM20004598, HA cluster index = 0
Secondary   : FGT_VM64_HV_B   , FGVM08TM20003583, HA cluster index = 1
number of vcluster: 1
vcluster 1: work 169.254.0.1
Primary: FGVM08TM20004598, HA operating index = 0
Secondary: FGVM08TM20003583, HA operating index = 1

FGT_VM64_HV_A #
```

8. Migrate the FortiGate-VMs from HV2019S02 to HV2019S03:
   - **a.** On HV2019S02, in Hyper-V Manager, right-click FGT_VM64_HV_A and select *Move*.
   - **b.** Select *Move the virtual machine*, then click *Next*.
   - **c.** Browse and select HV2019S03 for the destination computer, then click *Next*.
   - **d.** Select *Move all of the virtual machines data to a single location*, then click *Next*.
   - **e.** For the destination location, enter *D:\vms\fgt_vm64_hv_b1764_a\*, then click *Next*.
   - **f.** Verify the summary, then click *Finish*.
   - **g.** Repeat steps a-f to move FGT_VM64_HA_B.



Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
FGT_VM64_HV_b1764_B	Running	0%	8192 MB	01:29:10	Moving Virtual Machine and Storage (...	9.0
ip-172-18-70-169	Running	0%	1024 MB	01:29:06		9.0

You are about to perform the following operation.

Description:

Virtual machine:	FGT_VM64_HV_b1764_B
Move type:	Virtual Machine And Storage
Destination computer:	Hv2019S03
Ite	ation
At	64_hv_b1764_b\Virtual Hard Disks
At	64_hv_b1764_b\Virtual Hard Disks
At	64_hv_b1764_b\Virtual Hard Disks
Cu	64_hv_b1764_b\
Checkpoints	D:\vms\fgt_vm64_hv_b1764_b\
Smart Paging	D:\vms\fgt_vm64_hv_b1764_b\

To complete the move and close this wizard, click Finish.

FGT_VM64_HV_b1764_B

Created: 9/25/2020 11:20:30 AM
Configuration Version: 9.0
Generation: 1
Notes: None

Clustered: No
Heartbeat: OK (No Application Data)

Both FortiGate-VMs move to HV2019S03 and continue running.

Change log

Date	Change Description
2020-03-31	Initial release.
2020-04-08	Updated Public compared to private clouds on page 6.
2020-04-23	Updated FortiGate-VM evaluation license on page 5.
2020-05-05	Updated Registering the FortiGate-VM on page 13.
2020-11-03	Added Setting up FortiGate-VM HA for a Microsoft Hyper-V Live Migration environment on page 31.

Copyright© 2020 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., in the U.S. and other jurisdictions, and other Fortinet names herein may also be registered and/or common law trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance and other metrics contained herein were attained in internal lab tests under ideal conditions, and actual performance and other results may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to certain expressly-identified performance metrics and, in such event, only the specific performance metrics expressly identified in such binding written contract shall be binding on Fortinet. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. In no event does Fortinet make any commitment related to future deliverables, features or development, and circumstances may change such that any forward-looking statements herein are not accurate. Fortinet disclaims in full any covenants, representations, and guarantees pursuant hereto, whether express or implied. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.