FortiAnalyzer - 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 COOKBOOK
http://cookbook.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: techdocs@fortinet.com

April 5, 2024
FortiAnalyzer 6.4 Microsoft Hyper-V Cookbook
05-640-620530-20240405

TABLE OF CONTENTS

Change log

Date	Change description
2020-04-09	Initial release.
2021-03-09	Updated Minimum system requirements on page 7.
2021-03-12	Updated About FortiAnalyzer on Microsoft Hyper-V on page 5.
2021-05-13	Updated About FortiAnalyzer on Microsoft Hyper-V on page 5.
2021-05-28	Updated information about trial licenses and add-on licenses.
2022-11-18	Updated "Minimum system requirements" on page 7.
2023-02-01	Updated "About FortiAnalyzer on Microsoft Hyper-V" on page 5.
2024-04-05	Updated "About FortiAnalyzer on Microsoft Hyper-V" on page 5.

About FortiAnalyzer on Microsoft Hyper-V

This document provides information about deploying a FortiAnalyzer virtual appliance in Microsoft Hyper-V server environments.

This includes how to configure the virtual appliance's virtual hardware settings. This guide presumes that the reader has a thorough understanding of virtualization servers.

This document does not cover configuring and operating the virtual appliance after successfully installing and starting it. For that information, see the *FortiAnalyzer Administration Guide*.

Licensing

Fortinet offers the FortiAnalyzer-VM with a limited, free trial license. Stackable licenses can be purchased, letting you expand your VM solution as your environment expands. You can purchase perpetual or subscription-based licenses. Perpetual licenses never expire.

For information on purchasing a FortiAnalyzer-VM license, contact your Fortinet-authorized reseller, or visit How To Buy.

When configuring your FortiAnalyzer-VM, ensure that you configure hardware settings as the following table outlines and consider future expansion. Contact your Fortinet-authorized reseller for more information.

License	GB/day of logs
Trial License	1
VM-GB1	+1
VM-GB5	+5
VM-GB25	+25
VM-GB100	+100
VM-GB500	+500
VM-GB2000	+2000

See Minimum system requirements on page 7.

See also the FortiAnalyzer product datasheet.

Trial license

With a FortiCare account and FortiAnalyzer 6.4.1 or later, FortiAnalyzer-VM includes a free limited non-expiring trial license.

The free trial license includes support for 3 ADOMs and 1 GB/day of logs.

The free trial license does not include services or support.

You can activate the trial license when you connect to the GUI for the FortiAnalyzer-VM. Full-feature products and services are available for purchase with an add-on license. See Connecting to the GUI and enabling a trial license on page 16.

Add-on license

You must activate a trial license before you can upgrade FortiAnalyzer-VM to a purchased add-on license.

See also FortiAnalyzer 6.4 Trial License Guide.

Preparing for deployment

You can prepare for deployment by reviewing the following information:

- Minimum system requirements
- Deployment package for Microsoft Hyper-V
- Downloading a deployment package

Minimum system requirements

FortiAnalyzer-VM has a minimum requirement of 4 CPU, 8 GB of RAM, and 500 GB of disk storage.

The following table lists the minimum system requirements for your VM hardware, based on your VM's analytic sustained rate.

Analytic sustained rate (logs/sec)	VM hardware requirements		
	RAM (GB)	CPU cores	IOPS
3000	8	4	300
4000	8	4	400
5000	8	4	500
6000	16	8	600
7000	16	8	700
8000	16	8	800
9000	16	8	900
10000	16	8	1000
20000	32	16	2000
30000	32	16	3000
40000	64	32	4000
50000	64	32	5000

You can calculate the collector sustained rate by multiplying the analytic sustained rate by 1.5.

This table does not take into account other hardware specifications, such as bus speed, CPU model, or storage type.

Enabling FortiManager Management Extension Applications (MEA) requires more resources. For details, see the FortiManager Release Notes.

Deployment package for Microsoft Hyper-V

FortiAnalyzer deployment packages are included with firmware images on the Customer Service & Support site. The following table list the available VM deployment package.

VM Platform	Deployment File
Microsoft Hyper-V Server 2012 and 2016	`FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip`

The `.out.hyperv.zip` file contains:

- `FAZ.vhd`: The FortiAnalyzer system hard disk in VHD format.
  The log disk and virtual hardware settings have to be configured manually.

For more information FortiAnalyzer, see the FortiAnalyzer datasheet.

Downloading a deployment package

Firmware image FTP directories are organized by firmware version, major release, and patch release. The firmware images in the directories follow a specific naming convention. Each firmware image is specific to the device model. For example, the `FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip` image, found in the 5.6.0 directory, is specific to the 64-bit Microsoft Hyper-V Server virtualization environment.

You can download the *FortiAnalyzer Release Notes* and MIB file from this directory. The Fortinet Core MIB file is located in the *FortiAnalyzer* > *Download* tab.

Download the `.out` file to upgrade your existing FortiAnalyzer installation.

To download deployment packages:

1. Log in to the Fortinet Customer Service & Support portal then, from the toolbar select *Download* > *Firmware Images*. The *Firmware Images* page opens.
2. Select *FortiAnalyzer* from the *Select Product* dropdown list, then select *Download*.
3. Browse to the appropriate directory for the version that you would like to download.
4. Download the appropriate firmware image and release notes to your management computer.
5. Extract the contents of the package to a new folder on your management computer.

Compatibility for VM hardware versions

FortiAnalyzer-VM supports ESXi 6.5 and later versions. Using corresponding hardware versions 13 and later is highly recommended, as mentioned in Virtual machine hardware versions.

It is recommended to upgrade hardware versions incrementally with only one delta at a time. For example, upgrading from 10 to 11, 11 to 12, 12 to 13, then 13 to 14 is recommended, although directly upgrading from 10 to 14 generally has no issues.

To upgrade hardware versions:

1. Log in to vSphere Client web console.
2. In the left pane tree-menu, right-click the FortiAnalyzer-VM.
3. From the shortcut menu, select *Compatibility* > *Schedule VM Compatibility Upgrade*.
4. Click *YES*.
5. From the *Compatible with* dropdown, select the desired compatibility.
6. Click *OK*.
7. Reboot the FortiAnalyzer-VM.

Deployment

Prior to deploying the FortiAnalyzer, the VM platform must be installed and configured so that it is ready to create virtual machines. The installation instructions for FortiAnalyzer presume that you are familiar with the management software and terminology of your VM platform.

You might also need to refer to the documentation provided with your VM server. The deployment information in this guide is provided as an example because, for any particular VM server, there are multiple ways of creating a virtual machine - command line tools, APIs, alternative graphical user interface tools.

Before you start your FortiAnalyzer appliance for the first time, you might need to adjust virtual disk sizes and networking settings. The first time you start FortiAnalyzer, you will have access only through the console window of your VM server environment. After you configure one network interface with an IP address and administrative access, you can access the FortiAnalyzer GUI (see Enabling GUI access on page 16).

If the FortiAnalyzerdoes not have a valid Logical Volume Management (LVM) configuration, the LVM service will not start automatically upon boot-up when the disk already contains data. To manually enable the service, use the `execute lvm start` CLI command.

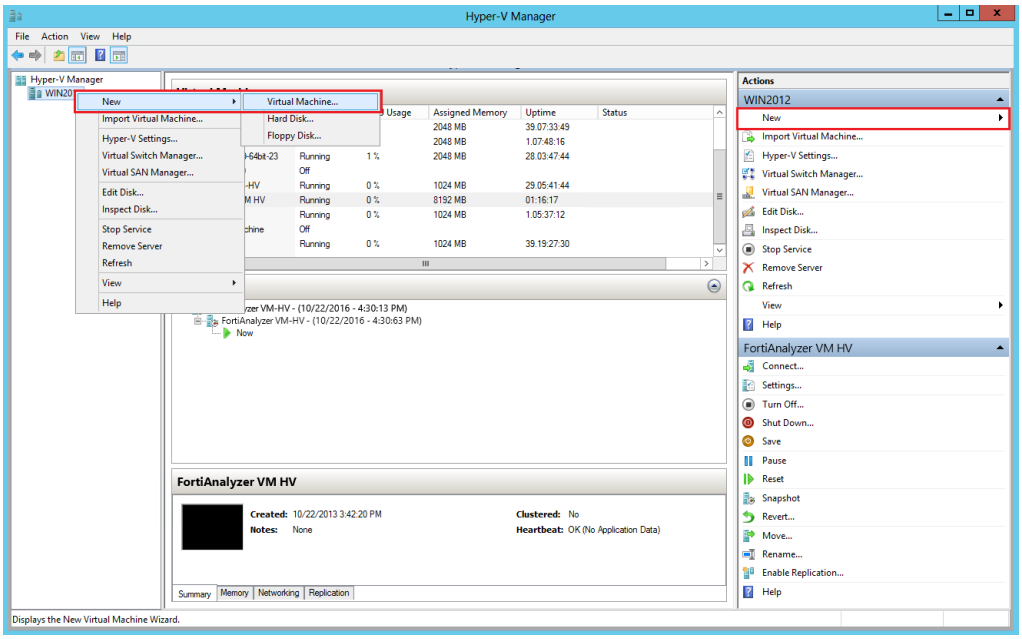
Deploying FortiAnalyzer on Microsoft Hyper-V

After you download the `FAZ_VM64_HV-vX-buildxxxx-FORTINET.out.hyperv.zip` file and extract the package contents to a folder on your Microsoft server, you can deploy the VHD package to your Microsoft Hyper-V environment.

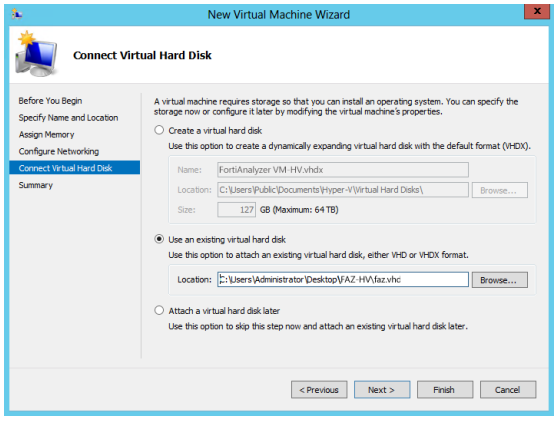
Creating the virtual machine

To create the virtual machine:

1. Launch the Hyper-V Manager in your Microsoft server. The *Hyper-V Manager* homepage opens.
2. Select the server in the right tree menu. The server details page opens.
3. Right-click the server and select *New* > *Virtual Machine*, or in the *Actions* menu, select *New* > *Virtual Machine*. The *New Virtual Machine Wizard* opens.



4. Configure the VM:
   a. Click *Next* to create a VM with a custom configuration. The *Specify Name and Location* page opens.
   b. Enter a name for this VM. The name displays in the Hyper-V Manager.
   c. Click *Next* to continue to the *Specify Generation* page.
   d. Select *Generation 1*. Generation 2 is currently not supported.
   e. Click *Next* to continue to the *Assign Memory* page.
   f. Specify the amount of memory to allocate to this VM. See Minimum system requirements on page 7 to determine your required memory.
   g. Click *Next* to continue to the *Configure Networking* page.
   h. You must configure network adapters in the *Settings* page. Each new VM includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected. FortiAnalyzer requires four network adapters.
   i. Select *Next* to continue to the *Connect Virtual Hard Disk* page.

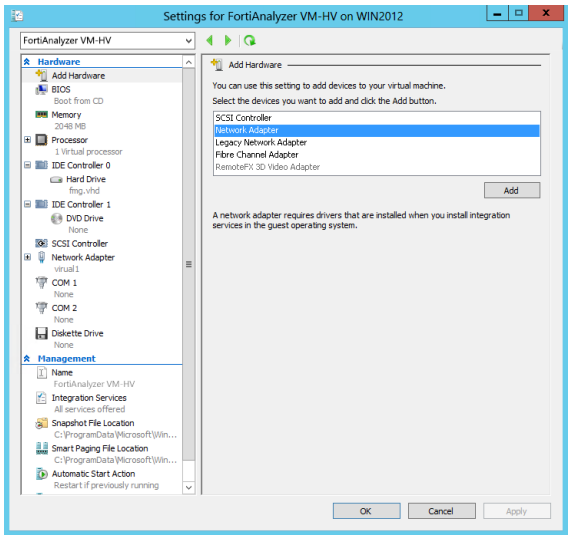


   j. Select to use an existing virtual hard disk and browse for the `faz.vhd` file that you downloaded from the Fortinet Customer Service & Support portal.
5. Select *Next* to continue to the *Summary* page.
6. To create the VM and close the wizard, select *Finish*.

Configuring hardware settings

Before powering on your FortiAnalyzer-VM, you must configure the virtual processors, memory, network adapters, and hard disk to match your FortiAnalyzer license. See Licensing on page 5 for FortiAnalyzer license information.

To open the *Settings* page, in the Hyper-V Manager, right-click the VM name and select *Settings*, or select the VM then click *Settings* from the *Actions* menu.

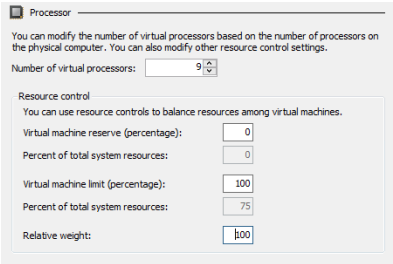


To configure virtual memory:

1. In the *Settings* page, select *Memory* from the *Hardware* menu. The *Memory* page displays.
2. Configure the VM memory. See Minimum system requirements on page 7 to determine your required memory.
3. Click *Apply* to save your settings.

To configure virtual processors:

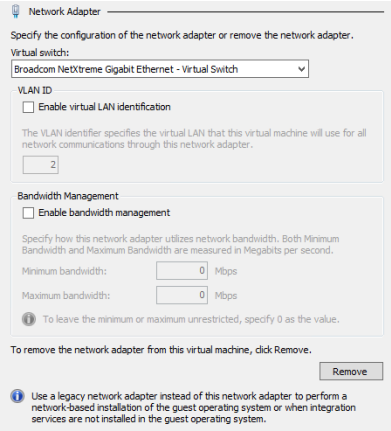
1. In the *Settings* page, select *Processor* from the *Hardware* menu. The *Processor* page displays.



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

To configure network adapters:

1. In the *Settings* page, select *Add Hardware* from the *Hardware* menu.
2. From the device list, select *Network Adapter*, then click *Add*. The *Network Adapter* page opens.



3. Manually configure four network adapters in the settings page. For each network adapter, select a virtual switch from the dropdown list.
4. Click *Apply* to save your settings.

To configure the virtual hard disk:

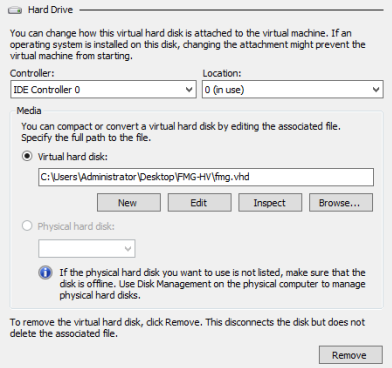
The FortiAnalyzer-VM requires at least two virtual hard disks. Before powering on the FortiAnalyzer-VM, you must add at least one more virtual hard disk. The default hard drive, `faz.vhd`, contains the OS. The FortiAnalyzer-VM uses the second hard drive for logs.

If you know your environment will expand in the future, adding hard disks larger than the 500 GB base license requirement is recommended. This allows your environment to expand as required while not taking up more space in the Storage Area Network (SAN) than is needed. See Licensing on page 5 for more information.

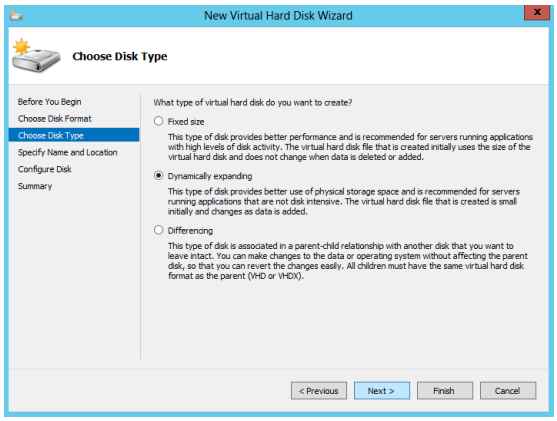
The FortiAnalyzer-VM allows you to add twelve virtual log disks to a deployed instance. When adding additional hard disks, use the following CLI command to extend the LVM logical volume:

```
execute lvm start
execute lvm extend <arg ..>
```

1. In the *Settings* page, select *IDE Controller 0* from the *Hardware* menu.
2. Select the type of drive that you want to attach to the controller, then click *Add*. The *Hard Drive* page opens.

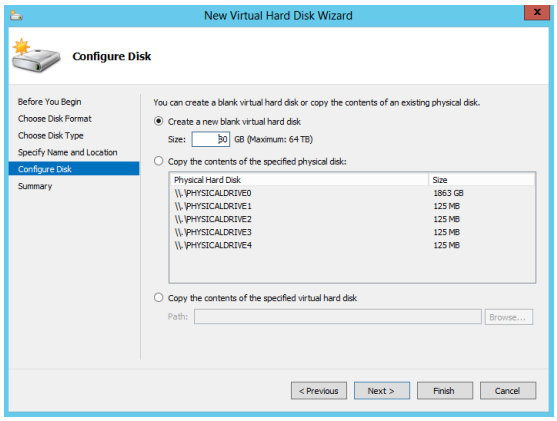


3. Click *New* to create a new virtual hard disk. The *New Virtual Hard Disk Wizard* opens to help you create a new virtual hard disk.
4. Configure the new virtual hard disk:
   a. Click *Next* to continue to the *Choose Disk Format* page.
   b. Select to use VHDX format virtual hard disks. This format supports virtual disks up to 64 TB and is resilient to consistency issues that may occur from power failures. Operating systems earlier than Windows Server 2012 do not support this format.
   c. Click *Next* to continue to the *Choose Disk Type* page.



   d. Select the type of virtual disk you want to use, one of the following:
      - *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 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).
   e. Click *Next* to continue to the *Specify Name and Location* page.
   f. Specify the name and location of the virtual hard disk file. Use the *Browse* button to select a specific file folder on your server.

g. Click *Next* to continue to the *Configure Disk* page.



h. Select *Create a new blank virtual hard disk*, then enter the size of the disk in GB. The maximum size depends on your server environment.

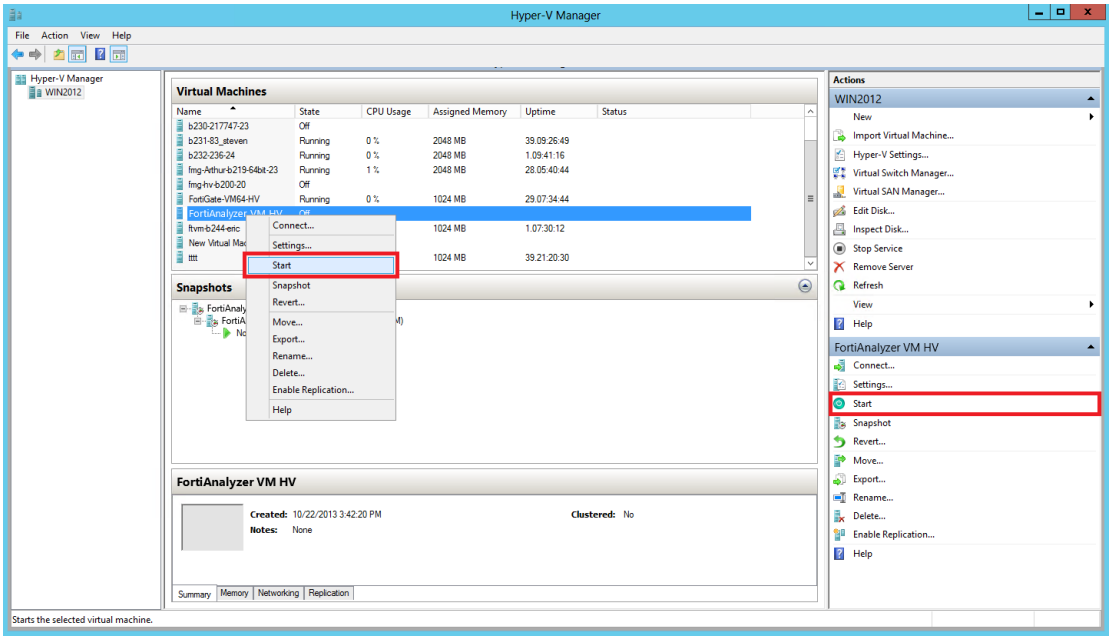
5. Click *Next* to continue to the *Summary* page. The summary page provides details about the virtual hard disk.
6. Click *Finish* to create the virtual hard disk, then click *Apply* to save the settings, and then click *OK* to exit the settings page.

Starting the virtual machine

You can now proceed to power on your FortiAnalyzer.

To start the FortiAnalyzer-VM:

1. In the list of VMs, right-click the FortiAnalyzer-VM name and select *Start*.
2. Select the FortiAnalyzer-VM from the list of VMs, then click *Start* from the *Actions* menu.



After the VM starts, proceed with the initial configuration. See Configuring initial settings on page 16.

Configuring initial settings

Before you can connect to the FortiAnalyzer-VM, you must configure basic network settings via the CLI console. Once configured, you can connect to the FortiAnalyzer GUI.

Enabling GUI access

To enable GUI access to the FortiAnalyzer, you must configure the IP address and network mask of the appropriate port on the FortiAnalyzer. The following instructions use port 1.

You can determine the appropriate by matching the network adapter's MAC address and the `HWaddr` that the CLI command `diagnose fmnetwork interface list` provides.

To configure the port1 IP address and netmask:

1. In your hypervisor manager, start the FortiAnalyzer and access the console window. You might need to press *Enter* to see the login prompt.
2. At the FortiAnalyzer login prompt, enter the username *admin*, then press *Enter*. By default, there is no password.
3. Using CLI commands, configure the port1 IP address and netmask.

```
config system interface
   edit port1
      set ip <IP address> <netmask>
end
```

The port management interface should match the first network adapter and virtual switch that you have configured in the hypervisor VM settings.

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

```
config system route
   edit 1
      set device port1
      set gateway <gateway_ipv4_address>
end
```

The Customer Service & Support portal does not currently support IPv6 for FortiAnalyzer license validation. You must specify an IPv4 address in the support portal and the port management interface.

Connecting to the GUI and enabling a trial license

Once you have configured a port's IP address and network mask, you can connect to the GUI by using a web browser.

To connect to the GUI and enable a trial license:

1. Launch a web browser, and enter the IP address you configured for the port management interface.
2. At the login page, click the *Login with FortiCloud* button to start the process of activating your free trial license.

See also FortiAnalyzer 6.4 Trial License Guide.

Upgrading to an add-on license

You must activate a trial license before you can upgrade FortiAnalyzer-VM to a purchased add-on license.

See also FortiAnalyzer 6.4 Trial License Guide.

Configuring your FortiAnalyzer

Once the FortiAnalyzer license has been validated, you can configure your device.

If the amount of memory or number of CPUs is too small for the VM, or if the allocated hard drive space is less than the licensed VM storage volume, warning messages show in the GUI in the *System Resources* widget on the dashboard and in the *Notification* list.