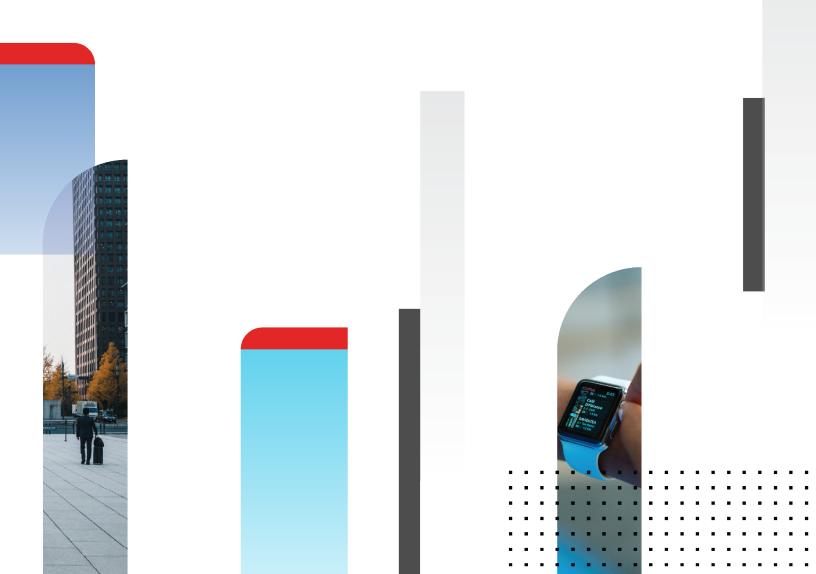
### F**E**RTINET.

# **ESX Installation Guide**

# FortiSIEM 6.4.0



### 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

### FORTINET TRAINING 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



10/04/2023 FortiSIEM 6.4.0 ESX Installation Guide

## **TABLE OF CONTENTS**

Change Log	
Fresh Installation	6
Pre-Installation Checklist	6
All-in-one Installation	7
Set Network Time Protocol for ESX	7
Import FortiSIEM into ESX	
Edit FortiSIEM Hardware Settings	
Start FortiSIEM from the VMware Console	
Configure FortiSIEM via GUI	
Upload the FortiSIEM License	
Choose an Event Database	
Cluster Installation	
Install Supervisor	
Install Workers	
Register Workers	
Install Collectors	
Register Collectors	
Installing on ESX 6.5	
Importing a 6.5 ESX Image	
Resolving Disk Save Error	
Adding a 5th Disk for /data	
Install Log	

# Change Log

Date	Change Description
09/05/2018	Initial version of FortiSIEM - ESX Installation Guide.
03/29/2019	Revision 1: updated the instructions for registering the Collector on the Supervisor node.
05/22/2019	Revision 2: added a note regarding VMotion support.
11/20/2019	Release of FortiSIEM - ESX Installation Guide for 5.2.6.
03/30/2020	Release of FortiSIEM - ESX Installation Guide for 5.3.0.
08/15/2020	Revision 3: Updated deployment and installation for FortiSIEM 6.1.0 on VMware ESX.
11/03/2020	Revision 4: Updated deployment and installation for FortiSIEM 6.1.1 on VMware ESX.
02/04/2021	Revision 5: Updated Migration content.
02/16/2021	Revision 6: Added Installing on ESX 6.5 content to 6.1.1.
02/23/2021	Revision 7: Minor update to Pre-Migration Checklist.
03/18/2021	Revision 8: Minor update to Pre-Migration Checklist for 6.1.1.
03/29/2021	Revision 9: Minor update to Pre-Migration Checklist for 6.1.1.
04/21/2021	Revision 10: Added Installing on ESX 6.5 content to 6.2.0. Minor update to Pre-Installation Checklist to 6.1.1 and 6.2.0.
04/22/2021	Revision 11: Added Installing on ESX 6.5 content to 6.1.0. Minor update to Pre-Installation Checklist to 6.1.0.
4/28/2021	Revision 12: Updated Pre-Installation Checklist for 6.1.0, 6.1.1 and 6.2.0.
05/07/2021	Release of FortiSIEM - ESX Installation Guide for 6.2.1.
06/07/2021	Revision 13: Elasticsearch screenshot updated for 6.2.x guides.
07/06/2021	Release of FortiSIEM - ESX Installation Guide for 6.3.0.
08/26/2021	Release of FortiSIEM - ESX Installation Guide for 6.3.1.
09/13/2021	Updated Importing a 6.5 ESX Image section for 6.3.x guides.
10/15/2021	Release of FortiSIEM - ESX Installation Guide for 6.3.2.
11/17/2021	Updated Register Collectors instructions for 6.x guides.
12/22/2021	Release of FortiSIEM - ESX Installation Guide for 6.3.3.

### Change Log

Date	Change Description
01/18/2022	Release of FortiSIEM - ESX Installation Guide for 6.4.0.
05/23/2022	Release of FortiSIEM - ESX Installation Guide for 6.4.1.
08/18/2022	Updated All-in-one Installation section.
10/06/2022	Added Collector with Reduced Disk in OT Environments under Install Collectors for 6.4.0-6.6.2 guides.
10/20/2022	Updated Register Collectors instructions for 6.x guides.
12/14/2022	Release of FortiSIEM - ESX Installation Guide for 6.4.2.
08/23/2023	Changed "Collector with Reduced Disk in OT Environments" to "Collector with Different OPT Disk Sizes" under Install Collectors.
09/01/2023	Release of FortiSIEM - ESX Installation Guide for 6.4.3.

# **Fresh Installation**

- Pre-Installation Checklist
- All-in-one Installation
- Cluster Installation
- Installing on ESX 6.5

### **Pre-Installation Checklist**

Before you begin, check the following:

- Release 6.4.0 requires at least ESX 6.5, and ESX 6.7 Update 2 is recommended. To install on ESX 6.5, See Installing on ESX 6.5.
- Ensure that your system can connect to the network. You will be asked to provide a DNS Server and a host that can be resolved by the DNS Server and responds to ping. The host can either be an internal host or a public domain host like google.com.
- Deployment type Enterprise or Service Provider. The Service Provider deployment provides multi-tenancy.
- Whether FIPS should be enabled
- Install type:
  - All-in-one with Supervisor only, or
  - Cluster with Supervisor and Workers
- Storage type
  - Online Local or NFS or Elasticsearch
  - Archive NFS or HDFS
- Before beginning FortiSIEM deployment, you must configure external storage
- Determine hardware requirements:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum • without UEBA – 24GB • with UEBA - 32GB Recommended • without UEBA – 32GB • with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB Local Event database – based on need
Supervisor (Cluster)	Minimum – 12 Recommended - 32	Minimum <ul> <li>without UEBA – 24GB</li> <li>with UEBA - 32GB</li> </ul> Recommended <ul> <li>without UEBA – 32GB</li> <li>with UEBA - 64GB</li> </ul>	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB

Node	vCPU	RAM	Local Disks
Workers	Minimum – 8 Recommended - 16	Minimum – 16GB Recommended – 24GB	OS – 25GB OPT – 100GB
Collector	Minimum – 4 Recommended – 8 ( based on load)	Minimum – 4GB Recommended – 8GB	OS – 25GB OPT – 100GB

Note: compared to FortiSIEM 5.x, you need one more disk (OPT) which provides a cache for FortiSIEM.

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.shruns.

Before proceeding to FortiSIEM deployment, you must configure the external storage.

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

### **All-in-one Installation**

This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

- Set Network Time Protocol for ESX
- Import FortiSIEM into ESX
- Edit FortiSIEM Hardware Settings
- Start FortiSIEM from the VMware Console
- Configure FortiSIEM via GUI
- Upload the FortiSIEM License
- Choose an Event Database

### **Set Network Time Protocol for ESX**

FortiSIEM needs accurate time. To do this you must enable NTP on the ESX host which FortiSIEM Virtual Appliance is going to be installed.

- 1. Log in to your VCenter and select your ESX host.
- 2. Click the Configure tab.

- 3. Under System, select Time Configuration. □ ussvnplesx51.fortinet-us.com ACTIONS -Summary Monitor Configure Permissions VMs Datastores Networks Updates vivi atantuo/anutuo. Time Configuration EDIT Agent VM Settings Default VM Compati... Date & Time 06/17/2020, 4:33:48 PM Swap File Location NTP Client Enabled System Licensing NTP Service Status Running Host Profile NTP Servers 172.30.254.1, 172.30.254.65 Time Configuration Authentication Se Certificate Power Management
- 4. Click Edit.
- 5. Enter the time zone properties.

Specify how the date and time on this h	st should be set.	
O Manually configure the date and tim	on this host	
06/17/2020 16:37:22		
(time is in ISO 8601 format)		
Use Network Time Protocol (Enable	ITP client)	
NTP Servers		
172.30.254.1,172.30.254.65		
Separate servers with commas, e.g. 1	31.21.2, fe00::2800	
NTP Service Status:	Running	
NTP Service Startup Policy:	Start and stop with host	

- Enter the IP address of the NTP servers to use. If you do not have an internal NTP server, you can access a publicly available one at http://tf.nist.gov/tfcgi/servers.cgi.
- 7. Choose an NTP Service Startup Policy.
- 8. Click **OK** to apply the changes.

### Import FortiSIEM into ESX

- 1. Go to the Fortinet Support website https://support.fortinet.com to download the ESX package FSM\_FULL\_ALL\_ ESX\_6.4.0\_Build1412.zip. See Downloading FortiSIEM Products for more information on downloading products from the support website.
- 2. Uncompress the packages for Super/Worker and Collector (using 7-Zip tool) to the location where you want to install the image. Identify the .ova file.
- **3.** Right-click on your own host and choose **Deploy OVF Template**. The Deploy OVA Template dialog box appears.
- 4. In 1 Select an OVF template select Local file and navigate to the .ova file. Click Next. If you are installing from a URL, select URL and paste the OVA URL into the field beneath URL.
- 5. In 2 Select a Name and Folder, make any needed edits to the Virtual machine name field. Click Next.

6. In 3 Select a compute resource, select any needed resource from the list. Click Next.

### Deploy OVF Template

~	1 Select an OVF template	Select a compute resource
~	2 Select a name and folder	Select the destination compute resource for this operation
	3 Select a compute resource	
	4 Review details	✓ 📠 US-NPL
	5 Select storage	> 🗍 NPL
	6 Ready to complete	> 📋 NPL-MGMT

- 7. Review the information in 4 Review details and click Next.
- 8. 5 License agreements. Click Next.

### Deploy OVF Template

	Fortinet Product License Agreement / EULA and Warranty Terms				
2 Select a name and folder					
3 Select a compute resource	Trademarks and Copyright Statement				
4 Review details	FortinetÆ, FortiGateÆ, and FortiGuardÆ are registered trademarks of Fortinet,				
5 License agreements	Inc., and other Fortinet names may also be trademarks, registered or otherwise,				
6 Select storage	of Fortinet. All other product or company names may be trademarks of their				
7 Select networks	respective owners. Copyright $©$ 2018 Fortinet, Inc., All Rights reserved. Contents				
8 Ready to complete	and terms are subject to change by Fortinet without prior notice. No part of this				
	publication may be reproduced in any form or by any means or used to make any				
	derivative such as translation, transformation, or adaptation without permission				
	from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.				
	Product License Agreement				
	The parties to this agreement are you, the end customer, and either (i) where you				
	have purchased your Product within the Americas, Fortinet, Inc., or (ii) where you	_			

- 9. In 6 Select Storage select the following, then click Next:
  - a. A disk format from the Select virtual disk format drop-down list. Select Thin Provision.
  - b. A VM Storage Policy from the drop-down list.
  - c. Select **Disable Storage DRS for this virtual machine**, if necessary, and choose the storage DRS from the table.

### Deploy OVF Template

1 Select an OVF template	Select storage					
2 Select a name and folder	Select the storage for the configuration and disk files					
• 3 Select a compute reِlmurce • 4 Review details	Select virtual disk format:		Thin Provision	~		
5 License agreements	VM Storage Policy:		<u>/</u>			
6 Select storage	Disable Storage DRS for the storage DRS for	nis virtual machir	ne			
7 Select networks 8 Ready to complete	Name	Capacity	Provisioned	Free	Typ	
	PL_DSCluster	100.04 TB	58.07 TB	41.97 TB		
	_templates	931.25 GB	133.79 GB	918.01 GB	VN	
	archive	2.73 TB	1.14 TB	1.59 TB	VN	
	ISO	931.25 GB	67.6 GB	863.65 GB	VN •	
	Compatibility					
	✓ Compatibility checks survey	cceeded.				
			CANCEL	ВАСК	NEX	

#### 10. In 7 Select networks, select the source and destination networks from the drop down lists. Click Next.

1 Select an OVF template	Select networks				
2 Select a name and folder	Select a destination network for ea	ach source	network.		
3 Select a compute resource					
4 Review details	Source Network	T	Destination Network	T	
5 License agreements	NAT		VLAN- Sanbox	 $\sim$	-
6 Select storage				1 item	s
7 Select networks					
8 Ready to complete	IP Allocation Settings				
	IP allocation:	Sta	atic - Manual		
	IP protocol:	IP۱	v4		

- 11. In 8 Ready to complete, review the information and click Finish.
- **12.** In the VSphere client, go to your installed OVA.

- 13. Right-click your installed OVA (example: FortiSIEM-611.1412.ova) and select Edit Settings > VM Options > General Options . Setup Guest OS and Guest OS Version (Linux and 64-bit).
- 14. Open the Virtual Hardware tab. Set CPU to 16 and Memory to 64GB.
- 15. Click Add New Device and create a device.

Add additional disks to the virtual machine definition. These will be used for the additional partitions in the virtual appliance. An All In One deployment requires the following additional partitions.

Disk	Size	Disk Name
Hard Disk 2	100GB	/opt For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.shruns.
Hard Disk 3	60GB	/cmdb
Hard Disk 4	60GB	/svn
Hard Disk 5	60GB+	/data (see the following note)

### Note on Hard Disk 5:

- Add a 5th disk if using local storage in an All In One deployment. Otherwise, a separate NFS share or Elasticsearch cluster must be used for event storage.
- 60GB is the minimum event DB disk size for small deployments, provision significantly more event storage for higher EPS deployments. See the FortiSIEM Sizing Guide for additional information.
- NFS or Elasticsearch event DB storage is mandatory for multi-node cluster deployments.

After you click **OK**, a Datastore Recommendations dialog box opens. Click **Apply**.

### Datastore Recommendations

 $\times$ 

vCenter Server recommends the following datastores for the virtual machines. Recommedations for virtual machines within the same datastore cluster are linked together and must either be accepted or rejected as a group. Click Apply if these recommendations are acceptable.

Recommendation	Space Utilization %	Space Utilization %	I/O Latency Before	
Recommendation 1 (Reason: Satisfy storage initial placement				4
requests)         Place       FortiSIEM-VA-6.1.0.1238"'s disk "New Hard Disk 0"         Place       FortiSIEM-VA-6.1.0.1238"'s disk "New Hard Disk 1"         Place       FortiSIEM-VA-6.1.0.1238"'s disk "New Hard Disk 1"	57.2 57.2 57.2	62.6 62.6 62.6	3.9 3.9 3.9	
Place         FortiSIEM-VA-6.1.0.1238"'s disk "New Hard Disk 2"           Place         FortiSIEM-VA-6.1.0.1238"'s disk "New Hard Disk 3"	57.2	62.6	3.9	

16. Do not turn off or reboot the system during deployment, which may take 7 to 10 minutes to complete. When the deployment completes, click **Close**.

### Edit FortiSIEM Hardware Settings

- 1. In the VMware vSphere client, select the imported Supervisor.
- 2. Go to Edit Settings > Virtual hardware.
- 3. Set hardware settings as in Pre-Installation Checklist. The recommended settings for the Supervisor node are:
  - CPU = 16
  - Memory = 64 GB
  - Four hard disks:
    - OS 25GB
    - OPT 100GB
    - CMDB-60GB
    - SVN-60GB

Example settings for the Supervisor node:

- If event database is local, then choose another disk for storing event data based on your needs.
- Network Interface card

### Start FortiSIEM from the VMware Console

- 1. In the VMware vSphere client, select the Supervisor, Worker, or Collector virtual appliance.
- 2. Right-click to open the options menu and select **Power > Power On**.
- 3. Open the Summary tab for the , select Launch Web Console. Network Failure Message: When the console starts up for the first time you may see a Network eth0 Failed message, but this is expected behavior.
- 4. Select Web Console in the Launch Console dialog box.

Launch Console	×
• Web Console	
<ul> <li>VMware Remote Console (VMRC)</li> <li>Remember my choice</li> </ul>	
	CANCEL

- 5. When the command prompt window opens, log in with the default login credentials user: root and Password: ProspectHills.
- 6. You will be required to change the password. Remember this password for future use.

At this point, you can continue configuring FortiSIEM by using the GUI.

### **Configure FortiSIEM via GUI**

Follow these steps to configure FortiSIEM by using a simple GUI.

- 1. Log in as user root with the password you set in Step 6 above.
- 2. At the command prompt, go to /usr/local/bin and enter configFSM.sh, for example:
   # configFSM.sh

3. In VM console, select 1 Set Timezone and then press Next.



4. Select your Region, and press Next.

	Africa
	America
	Antarctica
	Arctic
	Asia
	Atlantic
	Australia
	Brazil
	Canada
	Chile
	Etc
	Europe
L	(+) 66%

5. Select your Country, and press Next.



6. Select the Country and City for your timezone, and press Next.



7. Select 1 Supervisor. Press Next.





Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

8. If you want to enable FIPS, then choose 2. Otherwise, choose 1. You have the option of enabling FIPS (option 3) or disabling FIPS (option 4) later.

**Note**: After Installation, a 5th option to change your network configuration (**5 change\_network\_config**) is available. This allows you to change your network settings and/or host name.

Content Select Operation	onfigure Supervisor		]
2 3 4	<pre>install_without_fip install_with_fips enable_fips disable_fips</pre>	)S	
< Next >	< BACK >	< Exit >	-

9. Determine whether your network supports IPv4-only, IPv6-only, or both IPv4 and IPv6 (Dual Stack). Choose 1 for IPv4-only, choose 2 for IPv6-only, or choose 3 for both IPv4 and IPv6.

Select Operation	Configure Supervisor
	1 1Pv4 2 IPv6
	3 Both IPv4 and IPv6
-	-
< Next >	< BACK > < Exit >

- 10. If you choose 1 (IPv4) or choose 3 (Both IPv4 and IPv6), and press Next, then you will move to step 11. If you choose 2 (IPv6), and press Next, then skip to step 12.
- **11.** Configure the IPv4 network by entering the following fields, then press **Next**.

Option	Description
IPv4 Address	The Supervisor's IPv4 address
NetMask	The Supervisor's IPv4 subnet
Gateway	IPv4 Network gateway address
DNS1, DNS2	Addresses of the IPv4 DNS server 1 and DNS server2

IPv4 Address		
Netmask:	255.255.252.0	
Gateway:	172.30.56.1	
DNS1:	172.30.1.105	
DNS2:	172.30.1.106	

12. If you chose 1 in step 9, then you will need to skip to step 13. If you chose 2 or 3 in step 9, then you will configure the IPv6 network by entering the following fields, then press **Next**.

Option	Description
IPv6 Address	The Supervisor's IPv6 address
prefix (Netmask)	The Supervisor's IPv6 prefix
Gateway ipv6	IPv6 Network gateway address
DNS1 IPv6, DNS2 IPv6	Addresses of the IPv6 DNS server 1 and DNS server2

Configure IPU6 Net IPv6 Address: prefix (Netmask): Gateway ipv6: DNS1 IPv6: DNS2 IPv6:	gure IPv6 for Supervisor work 2001:815a:1:1::ac1e:2050 64 2001:815a:1:1::ac1e:3820 2001:815a:1:1::ac1e:1007	
<pre>     L</pre>	<pre>     Back &gt; &lt; Exit &gt; </pre>	

**Note**: If you chose option **3** in step 9 for both IPv4 and IPv6, then even if you configure 2 DNS servers for IPv4 and IPv6, the system will only use the first DNS server from IPv4 and the first DNS server from the IPv6 configuration. **Note**: In many dual stack networks, IPv4 DNS server(s) can resolve names to both IPv4 and IPv6. In such environments, if you do not have an IPv6 DNS server, then you can use public IPv6 DNS servers or use IPv4-mapped IPv6 address.

13. Configure Hostname for Supervisor. Press Next.

Co Configure host	<b>nfigure Hostname</b> name	For Supervisor
Host name:	Supervisor-Host	name
< Ne	xt > < Back	> < <b>Exit</b> >

Note: FQDN is no longer needed.

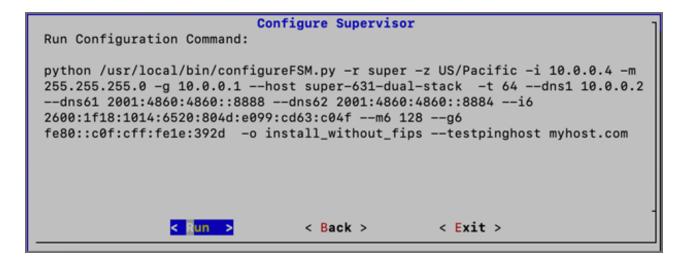
14. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and can respond to a ping. The host can either be an internal host or a public domain host like google.com. Press **Next**.

**Note**: By default, "google.com" is shown for the connectivity test, but if configuring IPv6, you must enter an accessible internally approved IPv6 DNS server, for example: "ipv6-dns.fortinet.com"

**Note**: When configuring both IPv4 and IPv6, only testing connectivity for the IPv6 DNS is required because the IPV6 takes higher precedence. So update the host field with an approved IPv6 DNS server.

Enter host for checkin	gure Supervis g network con		
ipv6-dns.fortinet.com	I		
-			
< Next >	< Back >	< Exit >	

**15.** The final configuration confirmation is displayed. Verify that the parameters are correct. If they are not, then press **Back** to return to previous dialog boxes to correct any errors. If everything is OK, then press **Run**.



The options are described in the following table.

Option	Description
-r	The FortiSIEM component being configured
-Z	The time zone being configured
-i	IPv4-formatted address
-m	Address of the subnet mask
-g	Address of the gateway server used
host	Host name
-f	FQDN address: fully-qualified domain name
-t	The IP type. The values can be either <b>4</b> (for <b>ipv4</b> ) or <b>6</b> (for <b>v6</b> ) or <b>64</b> (for both <b>IPv4</b> and <b>IPv6</b> ).
dns1,dns2	Addresses of DNS server 1 and DNS server 2.
i6	IPv6-formatted address
m6	IPv6 prefix
g6	IPv6 gateway
-0	Installation option ( <b>install_without_fips</b> , <b>install_with_fips</b> , <b>enable_fips</b> , or <b>disable_fips</b> , <b>change_network_config*</b> ) *Option only available after installation.
-Z	Time zone. Possible values are <b>US/Pacific</b> , <b>Asia/Shanghai, Europe/London</b> , or <b>Africa/Tunis</b>
testpinghost	The URL used to test connectivity

16. It will take some time for this process to finish. When it is done, proceed to Upload the FortiSIEM License. If the VM fails, you can inspect the ansible.log file located at /usr/local/fresh-install/logs to try and identify the problem.

### Upload the FortiSIEM License



Before proceeding, make sure that you have obtained valid FortiSIEM license from Forticare. For more information, see the Licensing Guide.

You will now be asked to input a license.

- 1. Open a Web browser and log in to the FortiSIEM UI. Use link https://<supervisor-ip> to login. Please note that if you are logging into FortiSIEM with an IPv6 address, you should input https://[IPv6 address] on the browser tab.
- 2. The License Upload dialog box will open.

<b>FortiSIEM</b>	
Hardware ID:	17082942-2e97-01cd-7f81-d0eb9fd682f2
Select license file:	Browse
User ID:	
Password:	
License Type:	ullet Enterprise $igodot$ Service Provider
	Upload

- Click Browse and upload the license file.
   Make sure that the Hardware ID shown in the License Upload page matches the license.
- 4. For User ID and Password, choose any Full Admin credentials. For the first time installation, enter admin as the user and admin\*1 as the password. You will then be asked to create a new password for GUI access.
- Choose License type as Enterprise or Service Provider. This option is available only for a first time installation. Once the database is configured, this option will not be available.
- 6. Proceed to Choose an Event Database.

### **Choose an Event Database**

For a fresh installation, you will be taken to the Event Database Storage page. You will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options. For more details, see Configuring Storage.



After the License has been uploaded, and the Event Database Storage setup is configured, FortiSIEM installation is complete. If the installation is successful, the VM will reboot automatically. Otherwise, the VM will stop at the failed task.

You can inspect the ansible.log file located at /usr/local/fresh-install/logs if you encounter any issues during FortiSIEM installation.

After installation completes, ensure that the phMonitor is up and running, for example:

# phstatus

The response should be similar to the following.

Every 1.0s: /opt/phoenix/bin/phstatus.py								
System uptime: 21:12:6 Tasks: 27 total, 0 runn Cpu(s): 16 cores, 6.220 Mem: 65702100k total, 1 Swap: 2621436k total, 6	ning, 26 sleep us, 2.1%sy, 0. U0366036k used	ing, 0 stoppe 0%ni, 91.4%id , 55336064k fi	d, 0 zombie , 0.0χωα, 0.2χhi, ree, 4352k buffer:	0.1%si, 0.0%st				
PROCESS	UPTIME	CPU>:	VIRT_MEM	RES_MEM				
phParser	41:23	0	2176m	558m				
phQueryMaster	41:41	0	1020m	77m				
phRuleMaster	41:41	Ø	1079m	504m				
phRuleWorker	41:41	Ø	1363m	285m				
phQueryWorker	41:41	0	1383m	279m				
phDataManager	41:41	0	1419m	285m				
phDiscover	41:41	0	513m	53m				
phReportWorker	41:41	Ø	1433m	95m				
phReportMaster	41:41	0	603m	67m				
phlpldentityWorker	41:41	0	1027m	58m				
phIpIdentityMaster	41:41	0	491m	39m				
phAgentManager	41:41	0	1425m	54m				
phCheckpoint	42:31	0	325m	34m				
phPerfMonitor	41:41	0	782m	70m				
phReportLoader	41:41	0	769m	278m				
phBeaconEventPackager	41:41	0	1125m	65m				
phDataPurger	41:41	0	588m	58m				
phEventForwarder	41:41	0	548m	46m				
phMonitor	37:24	0	2888m	53m				
Apache	01:10:40	0	310m	16m				
Node.js-charting	01:10:19	0	916m	71m				
Node.js-pm2	01:10:13			26m				
AppSor	01:10:07		15172m	3026m				
DBSvr	01:10:38	0	317m	30m				
phAnoma ly	01:08:07		987m	64m				
phFortiInsightAI	01:10:40		23432m	438m				
Redis	01:10:18		55m	25m				

### **Cluster Installation**

For larger installations, you can choose Worker nodes, Collector nodes, and external storage (NFS or Elasticsearch).

- Install Supervisor
- Install Workers
- Register Workers
- Install Collectors
- Register Collectors

### **Install Supervisor**

Follow the steps in All-in-one Install with two differences:

- Setting up hardware you do not need an event database.
- Setting up an external Event database configure the cluster for either NFS or Elasticsearch.

### NFS

X	FortiSIEM
Event Database stora	age:
○ Local Disk	
NFS	
Server IP/Host:	Server IP/Host
Exported Directory:	Exported Directory
○ Elasticsearch	
	Test Save

### Elasticsearch

	🕵 FortiSIEM
Event Database storage: Local Disk NFS Elasticsearch	
ES Service Type:	• Native • Amazon • Elastic Cloud
URL:	https://
REST Port:	443 🙂
User Name:	(Optional)
Password:	(Optional)
Confirm Password:	
Shard Allocation:	Fixed Opnamic
Shards:	5
Replicas:	1
Per Org Index	
	Test

You must choose external storage listed in Choose an Event Database.

### **Install Workers**

Once the Supervisor is installed, follow the same steps in All-in-one Install to install a Worker except only choose OS and OPT disks. The recommended settings for Worker node are:

- CPU = 8
- Memory = 24 GB
- Two hard disks:
  - OS 25GB
  - OPT 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.shruns.

### **Register Workers**

Once the Worker is up and running, add the Worker to the Supervisor node.

- 1. Go to ADMIN > License > Nodes.
- 2. Select Worker from the drop-down list and enter the Worker's IP address and host name. Click Add.

	Add Node		×	
	Туре:	Worker 🗸		I
	Worker IP Address:	172.30.58.9		lole
	Host Name:	wk589		
l		Save Cancel		

3. See ADMIN > Health > Cloud Health to ensure that the Workers are up, healthy, and properly added to the

system.									
Setup	Cloud Health Colle	ector Health							
🖨 Device Support	Search	Columns 🗸						Lines: 2 Last update at 8:4	9:17 PM 🟾
🗮 Health	Name	IP Address	Module Role	Health Ve	rsion	Load Average	CPU	Swap Used	
_	sp572.fortinet.com	172.30.57.2	Supervisor	Normal 6.	1.0.1238	0.95,0.47,0.4	3 4%	0 KB	
License	wk573.fortinet.com	172.30.57.3	Worker	Normal 6.	1.0.1238	0.1,0.2,0.16	2%	0 KB	
💠 Settings									
	Search	Columns -		Proces	s level metrics for wk	73.fortinet.com (17	72.30.57.3)		Lines: 17
	Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position	
	Node.js-charting	Up	1h 3m	0%	70 MB	916 MB			A
	httpd	Up	14m 6s	0%	16 MB	310 MB			_
	Redis	Up	14m 6s	0%	22 MB	51 MB			
	Node.js-pm2	Up	1h 3m	0%	44 MB	899 MB			
	rsyslogd	Up	1h 3m	0%	7 MB	189 MB			
	phDataManager	UD	14m 6s	0%	103 MB	1229 MB	1	126108	•
Copyright © 2020 Fortinet, Inc. All rights	reserved.		Organization:	Super User: adm	in Scope: Global				FortiSIEM

### **Install Collectors**

Once Supervisor and Workers are installed, follow the same steps in All-in-one Install to install a Collector except in Edit FortiSIEM Hardware Settings, only choose OS and OPT disks.

- Collector in Regular IT Environments
- Collector with Different OPT Disk Sizes

### **Collector in Regular IT Environments**

The recommended settings for Collector node are:

- CPU = 4
- Memory = 8GB
- Two hard disks:
- OS 25GB
  - OPT 100GB

For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.shruns.

### **Collector with Different OPT Disk Sizes**

FortiSIEM installations require the disk for OPT+SWAP to have exactly 100 GB. This is valid for all three node options (Supervisor, Worker and Collectors).

Depending on your situation, you may want to increase or decrease the size of the log collector. For example, an Operational Technology (OT) may find it difficult to dedicate 125 GB to a log collector, and want to decrease the size of the log collector. In another circumstance, a company may want to increase the event cache for their collectors, which usually means increasing the OPT disk size. For more information, see Increasing Collector Event Buffer Size in the Online Help.

The steps here explain how to bypass the requirement for Collector install. Be aware that reducing the size of the disk also reduces the size of the available cache when there is a connection interruption between Collector and Workers/Supervisor, and may result in loss of logs. Increasing the size of the disk provides a larger available cache.

- 1. Follow the installation guide but instead of adding a 100 GB disk for OPT, add a disk of whatever size you require.
- 2. In this example, we will assume the OPT disk is 35 GB, so in total, the Collector VM will have 70 GB (25 for OS + 35 for OPT).

Edit Settings   JYU-COL-RE	EDUCE_OPT-OT-VA-
	ADD NEW DEVIC
> CPU	<u> </u>
> Memory	24 × <u>GB ×</u>
> Hard disk 1	25
✓ Hard disk 2	35 <u>GB ~</u>
Maximum Size	1.19 TB
VM storage policy	
Туре	Thin Provision
Sharing	No sharing Y
Disk File	[PVVol_B008] JYU-COL-REDUCE_OPT-OT-VA-
Shares	<u>Normal v</u> 1000 v
Limit - IOPs	Unlimited V
Disk Mode	Dependent ~
Virtual Device Node	SCSI controller 0 V SCSI(0:1) Hard disk 2 V
> SCSI controller 0	VMware Paravirtual
> Network adapter 1	Connect
> Video card	Specify custom settings 🖌
VMCI device	
> Other	Additional Hardware
	CANCEL

3. After you boot the VM and change the password, you will be editing the following files.

- /usr/local/syslib/config/disksConfig.json
- /usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml

Note: You must make changes to these files before running the configureFSM.sh installer.

4. The disksConfig.json file contains a map of installation types and node types. It defines the required sizes of disks so that the installer can validate them. Since we are changing the KVM Collector opt disk requirement to 35 GB in this example, we must reflect that size in this file. Using a text editor, modify the "opt" line in the disksConfig.json file, shown in blue to your requirement.

```
"FSIEMVMWARE": {
 "SUPER": {
   "number": "3",
    "opt": "100",
    "svn": "60",
    "cmdb": "60"
  },
 "FSMMANAGER": {
    "number": "2",
    "opt": "100",
    "cmdb": "60"
 },
 "WORKER": {
    "number": "1",
    "opt": "100"
  },
 "COLLECTOR": {
    "number": "1",
    "opt": "35"
 }
},
```

- 5. Save the disksConfig.json file.
- 6. Load the /usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml file via a text editor. You can choose to adjust only the (step a) OPT disk or (step b) adjust the swap disk and OPT disk. To change only the OPT disk, proceed with step a, then skip to step 7. To adjust the swap disk and reduce the OPT disk, skip step a and proceed with step b.

#### a. ADJUST OPT DISK ONLY

Navigate to line 54 in the /usr/local/install/roles/fsm-disk-mgmt/tasks/disks.yml file and change the line. Original line (The original line assumes the drive is 100 GB)

```
parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
100G && sleep 5
```

Change this line to reflect the size of your OPT disk (in this example 35 GB), marked in blue.

```
parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
35G && sleep 5
```

Skip step b and c, and proceed to step 7.

#### b. ADJUST SWAP DISK and REDUCE OPT DISK

Reduce the Swap Disk by changing the following original line (The original line assumes swap disk to be 25GB).

parted -a optimal --script "{{ item.disk }}" mklabel gpt mkpart primary linux-swap 1G
25G && sleep 5

Change to (in this example 10G), marked in blue:

```
parted -a optimal --script "{{ item.disk }}" mklabel gpt mkpart primary linux-swap 1G
10G && sleep 5
```

c. Reduce /OPT disk: by changing the following line (The original line assumes the drive is 100 GB).

```
parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 26G
100G && sleep 5
```

Change to reflect the size of your OPT disk (in this example 35 GB), marked in blue.

```
parted -a optimal --script "{{ item.disk }}" mkpart primary "{{ item.fstype }}" 11G
35G && sleep 5
```

- 7. Save the disks.yml file.
- 8. Run configFSM.sh to install the collector. When it reboots, you can provision it using the phProvisionCollector command. Your partition output should appear similar to the following.

```
Partition Output of deployment:
                 0 35G 0 disk
sdb
           8:16
-sdb1
            8:17
                 0 8.4G 0 part [SWAP]
L_sdb2
           8:18 0 22.4G 0 part /opt
# df -h
Filesystem
                 Size Used Avail Use% Mounted on
devtmpfs
                  12G
                          0 12G 0%/dev
                          0 12G 0% /dev/shm
tmpfs
                  12G
tmpfs
                  12G
                       17M 12G 1%/run
tmpfs
                  12G
                        0
                             12G
                                  0% /sys/fs/cqroup
/dev/mapper/rl-root 22G 8.1G 14G 38% /
/dev/sdb2
                  23G 4.3G
                            19G 19% /opt
/dev/sda1
               1014M 661M 354M 66% /boot
tmpfs
                 2.4G 0 2.4G 0% /run/user/500
tmpfs
                 2.4G
                        0 2.4G 0% /run/user/0
```

### **Register Collectors**

Collectors can be deployed in Enterprise or Service Provider environments.

- Enterprise Deployments
- Service Provider Deployments

### **Enterprise Deployments**

For Enterprise deployments, follow these steps.

- 1. Log in to Supervisor with 'Admin' privileges.
- 2. Go to ADMIN > Settings > System > Event Worker.
  - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.

Note: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP

addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.

- b. Click OK.
- 3. 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 to Unlimited.
- 4. SSH to the Collector and run following script to register Collectors:

```
# /opt/phoenix/bin/phProvisionCollector --add <user> '<password>' <Super IP or
Host> <Organization> <CollectorName>
```

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

- a. Set user and password using the admin user name and password for the Supervisor.
- **b.** Set Super IP or Host as the Supervisor's IP address.
- c. Set Organization. For Enterprise deployments, the default name is Super.
- d. Set CollectorName from Step 2a.

The Collector will reboot during the Registration.

5. Go to ADMIN > Health > Collector Health for the status.

🌣 Setup	Cloud Health	Collector Health												
🖨 Device Support	Show Processes	Tunnels 🏚	Action 👻	Search		Columns	•				Lines: 1	Last update at 8	8:54:17 PM	Ç
📑 Health	Organization	Name	E IP	Address	Status	He	alth Up	Tíme C	PU	Memory	Allocated EPS	Incoming EPS	Version	Col
I License	Super	CO-ORG	17	2.30.57.4	up	No	rmal 3m	4s 6	55%	5%	200	0	6.1.0	100
😂 Settings														
	4													Þ
	Close Panel	Search		Columns 👻							Lir	nes: 9 Last upda	te at 8:54:2	24 PM
	Process Name	13	Status	Jp Time	C	PU P	hysical Memory	Virtual Memory	Sha ID	aredStore	SharedStore P	osition		
	phMonitorAgent		Up	29s	0	1% 5	75 MB	1116 MB						*
	phParser		Up	17s	0	1% 1	06 MB	1190 MB	99		0			
	phPerfMonitor		Up	17s	0	1% 7	9 MB	766 MB						
	phEventForwarder		Up	17s	0	1% 4	18 MB	547 MB						
	phDiscover		Up	17s	0	NS 5	i3 MB	513 MB						
														*

### **Service Provider Deployments**

For Service Provider deployments, follow these steps.

- 1. Log in to Supervisor with 'Admin' privileges.
- 2. Go to ADMIN > Settings > System > Event Worker.
  - a. Enter the IP of the Worker node. If a Supervisor node is only used, then enter the IP of the Supervisor node. Multiple IP addresses can be entered on separate lines. In this case, the Collectors will load balance the upload of events to the listed Event Workers.

**Note**: Rather than using IP addresses, a DNS name is recommended. The reasoning is, should the IP addressing change, it becomes a matter of updating the DNS rather than modifying the Event Worker IP addresses in FortiSIEM.

#### **b.** Click **OK**.

Setup	← All Settings > System > Event Worker
🖨 Device Support	Worker Address: 172.30.57.3 + -
📕 Health	
I License	Save
😂 Settings	

3. Go to ADMIN > Setup > Organizations and click New to add an Organization.

Organization Definiti	on (ORG)		*
Organization:	ORG	Include IP/IP Range:	
Full Name:		Exclude IP/IP Range:	
Admin User:	admin	Agent User:	
Admin Password:	•••••	Agent Password:	
Confirm Admin Password:	•••••	Confirm Agent Password:	
Admin Email:	Required	Max Devices:	
Phone:		Address:	
Account Number:		Account Type:	
Support Tier:		Account Status:	
Support Team:		Account Manager:	
Collectors:	New Edit Delete		
	Collector Name Collector EPS	UpLoad Rate Limit	Valid Start Date Valid End Date
	Save	Cancel	

- 4. Enter the Organization Name, Admin User, Admin Password, and Admin Email.
- 5. Under Collectors, click New.
- 6. Enter the Collector Name, Guaranteed EPS, Start Time, and End Time. The last two values could be set as Unlimited. Guaranteed EPS is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.

Organization Definition (ORG) - Add Collector									
Name:	Required								
Guaranteed EPS:	Required								
Upload Rate Limit (Kbps):	Unlimited								
Start Time:	Unlimited								
End Time:	Unlimited								
	Save Cancel								

7. SSH to the Collector and run following script to register Collectors:

# /opt/phoenix/bin/phProvisionCollector --add <user> '<password>' <Super IP or
Host> <Organization> <CollectorName>

The password should be enclosed in single quotes to ensure that any non-alphanumeric characters are escaped.

- a. Set user and password using the admin user name and password for the Organization that the Collector is going to be registered to.
- **b.** Set Super IP or Host as the Supervisor's IP address.
- c. Set Organization as the name of an organization created on the Supervisor.
- d. Set CollectorName from Step 6.



The Collector will reboot during the Registration.

8. Go to ADMIN > Health > Collector Health and check the status.

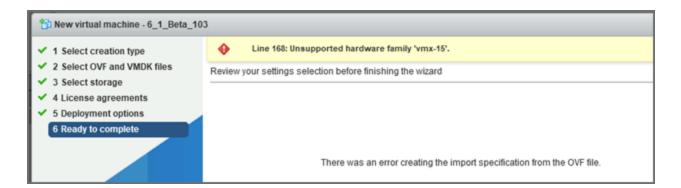
🌣 Setup	Cloud Health	Collector Healt	th										
🖨 Device Support	Show Processes	Tunnels	🌣 Action 👻	Search		Columns 👻				Lines: 1	Last update at 8	8:54:17 PM	C.
📰 Health	Organization	Name	IP A	ddress	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	i c
🗉 License	Super	CO-ORG	172.	30.57.4	up	Normal	3m 4s	65%	5%	200	0	6.1.0	
🛠 Settings													
	<												
	<ul> <li>Close Panel</li> </ul>	Search	Co	lumns <del>-</del>				-	-	Liı	nes: 9 Last updat	te at 8:54:	:24
	Close Panel	Search	Co Status   Up		CPU	Physical Mer	mory : Virtual Memor	y Sha ID	redStore	Lii SharedStore P		te at 8:54::	:24
		Search		Time	CPU 0%	i Physical Mer 575 MB	mory : Virtual Memor 1116 MB	y Sha ID	redStore			te at 8:54:	24
	Process Name	Search	Status Up	o Time				y Sha ID 99	redStore			te at 8:54:1	:24
	Process Name phMonitorAgent	Search	Status Up Up 29	o Time Is Is	0%	575 MB	1116 MB	V ID	redStore	SharedStore P		te at 8:54:1	:24
	Process Name phMonitorAgent phParser		Status Up Up 25 Up 17	o Time Is Is Is	0% 0%	575 MB 106 MB	1116 MB 1190 MB	V ID	redStore	SharedStore P		te at 8:54:	:24
	Process Name phMonitorAgent phParser phPerfMonitor		Status Up Up 29 Up 17 Up 17	o Time is is is is is	0% 0% 0%	575 MB 106 MB 79 MB	1116 MB 1190 MB 766 MB	V ID	redStore	SharedStore P		te at 8:54:	2

### **Installing on ESX 6.5**

- Importing a 6.5 ESX Image
- Resolving Disk Save Error
- Adding a 5th Disk for /data

### Importing a 6.5 ESX Image

When installing with ESX 6.5, or an earlier version, you will get an error message when you attempt to import the image.



To resolve this import issue, you will need to take the following steps:

- 1. Install 7-Zip.
- 2. Extract the OVA file into a directory.
- 3. In the directory where you extracted the OVA file, edit the file FortiSIEM-VA-6.4.0.1412.ovf, and replace all references to vmx-15 with your compatible ESX hardware version shown in the following table.

**Note**: For example, for ESX 6.5, replace vmx-15 with vmx-13.

<virtualhardwaresection></virtualhardwaresection>
<info>Virtual hardware requirements for a virtual machine</info>
<system></system>
<vssd:elementname>Virtual Hardware Family</vssd:elementname>
<vssd:instanceid>0</vssd:instanceid>
<vssd:virtualsystemidentifier>FSM-VA-C8</vssd:virtualsystemidentifier>
<vssd:virtualsystemtype>vmx-15</vssd:virtualsystemtype>
<item></item>
<rasd:caption>4 virtual CPU</rasd:caption>
<rasd:description>Number of virtual CPUs</rasd:description>
<pre>crasd.FlementName&gt;16 virtual CPU/rasd.FlementName&gt;</pre>

Note: For example, for ESX 6.5, replace vmx-15 with vmx-13.

Compatibility	Description
EXSi 6.5 and later	This virtual machine (hardware version 13) is compatible with ESXi 6.5.
EXSi 6.0 and later	This virtual machine (hardware version 11) is compatible with ESXi 6.0 and ESXi 6.5.
EXSi 5.5 and later	This virtual machine (hardware version 10) is compatible with ESXi 5.5, ESXi 6.0, and ESXi 6.5.
EXSi 5.1 and later	This virtual machine (hardware version 9) is compatible with ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.
EXSi 5.0 and later	This virtual machine (hardware version 8) is compatible with ESXI 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.

Compatibility	Description
ESX/EXSi 4.0 and later	This virtual machine (hardware version 7) is compatible with ESX/ESXi 4.0, ESX/ESXi 4.1, ESXI 5.0, ESXi 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5.
EXS/ESXi 3.5 and later	This virtual machine (hardware version 4) is compatible with ESX/ESXi 3.5, ESX/ESXi 4.0, ESX/ESXi 4.1, ESXI 5.1, ESXi 5.5, ESXi 6.0, and ESXi 6.5. It is also compatible with VMware Server 1.0 and later. ESXi 5.0 does not allow creation of virtual machines with ESX/ESXi 3.5 and later compatibility, but you can run such virtual machines if they were created on a host with different compatibility.
ESX Server 2.x and later	This virtual machine (hardware version 3) is compatible with ESX Server 2.x, ESX/ESXi 3.5, ESX/ESXi 4.0, ESX/ESXi 4.1, and ESXI 5.0. You cannot create, edit, turn on, clone, or migrate virtual machines with ESX Server 2.x compatibility. You can only register or upgrade them.

**Note**: For more information, see here.

- 4. Right click on your host and choose **Deploy OVF Template**. The Deploy OVA Template dialog box appears.
- 5. In 1 Select an OVF template, select Local File.
- 6. Navigate to the folder with the OVF file.
- 7. Select all the contents that are included with the OVF.
- 8. Click Next.

### **Resolving Disk Save Error**

You may encounter an error message asking you to select a valid controller for the disk if you attempt to add an additional 4th disk (/opt, /cmd, /svn, and /data). This is likely due to an old IDE controller issue in VMware, where you are normally limited to 2 IDE controllers, 0, 1, and 2 disks per controller (Master/Slave).

D Edit settings - FSM6_1_Beta (ESXi 6.5 virtual machine)				
Please select a valid controller for the disk				
Add hard disk M Add network adapter SAdd other device				
> 🖬 CPU	8 🔻 🚺			
Memory	16384 MB *			
Hard disk 1	25 GB 🔻			
▶ □ New Hard disk	100 GB 🔻			
▶ □ New Hard disk	60 GB 🔻			
▶ 🔤 New Hard disk	60 GB <b>v</b>			
▶ 🔤 New Hard disk	75 GB 🔻			
INE Network Adapter 1	VM Network	🔻 🗹 Connect		
Video Card	Cossify austors actions	•		

If you are attempting to add 5 disks in total, such as this following example, you will need to take the following steps:

#### Fresh Installation

Disk	Usage
1st	25GB default for image
2nd	100GB for /opt For OPT - 100GB, the 100GB disk for /opt will consist of a single disk that will split into 2 partitions, /OPT and swap. The partitions will be created and managed by FortiSIEM when configFSM.sh runs.
3rd	60GB for / cmdb
4th	60GB for /svn
5th	75GB for /data (optional, or use with NFS or ES storage)

- 1. Go to Edit settings, and add each disk individually, clicking save after adding each disk.
- When you reach the 4th disk, you will receive the "Please select a valid controller for the disk" message. This is because the software has failed to identify the virtual device node controller/Master or Slave for some unknown reason.
- 2. Expand the disk setting for each disk and review which IDE Controller Master/Slave slots are in use. For example, in one installation, there may be an attempt for the 4th disk to be added to IDE Controller 0 when the Master/Slave slots are already in use. In this situation, you would need to put the 4th disk on IDE Controller 1 in the Slave position, as shown here. In your situation, make the appropriate configuration setting change.

🔁 Edit settings - FSM6_1_Beta (ESXi 6.5 virtual machine)				
Please select a valid controller for the disk				
✓	60 GB V			
Maximum Size	2.02 TB			
Location	[datastore1] FSM6_1_Beta/ Browse			
Disk Provisioning	<ul> <li>Thin provisioned</li> <li>Thick provisioned, lazily zeroed</li> <li>Thick provisioned, eagerly zeroed</li> </ul>			
Shares	Normal			
Limit - IOPs	Unlimited			
Virtual Device Node	IDE controller 1   Slave			
Disk mode	Dependent •			

3. Click save to ensure your work has been saved.

### Adding a 5th Disk for /data

When you need to add a 5th disk, such as for /data, and there is no available slot, you will need to add a SATA controller to the VM by taking the following steps:

- 1. Go to Edit settings.
- 2. Select Add Other Device, and select SCSI Controller (or SATA).

You will now be able to add a 5th disk for /data, and it should default to using the additional controller. You should be able to save and power on your VM. At this point, follow the normal instructions for installation.

Note: When adding the local disk in the GUI, the path should be /dev/sda or /dev/sdd. You can use one of the following commands to locate:

# fdisk-1
or
# lsblk

# **Install Log**

The install ansible log file is located here: /usr/local/fresh-install/logs/ansible.log.

Errors can be found at the end of the file.



www.fortinet.com

Copyright© 2023 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, FortiCare® and FortiGuard®, and certain other marks are registered trademarks of Fortinet, Inc., 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. 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.