



FortiSIEM - Azure Installation and Migration Guide

Version 6.1.1

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 6.1.1 Azure Installation and Migration Guide

TABLE OF CONTENTS

Change Log	4
Fresh Installation	5
Pre-Installation Checklist	5
All-in-one Installation	6
Create a FortiSIEM Image in Azure Using the Published VHD	6
Create a VM Using a FortiSIEM 6.1.1 Azure Image	8
Configure FortiSIEM via GUI	17
Upload the FortiSIEM License	20
Choose an Event Database	21
Cluster Installation	22
Install Supervisor	22
Install Workers	23
Register Workers	23
Install Collectors	24
Register Collectors	24
Migrating from FortiSIEM 5.3.x or 5.4.0	28
Pre-Migration Checklist	28
Migrate All-in-one Installation	29
Download the Backup Script	29
Run the Backup Script and Shutdown System	29
Create 6.1.1 New Root Disk	30
Swap 6.1.1 OS Disk on Your 5.3.x or 5.4.0 Instance	33
Boot up the 5.3.x or 5.4.0 Instance and Migrate to 6.1.1	37
Migrate Cluster Installation	42
Delete Workers	42
Migrate Supervisor	42
Install New Worker(s)	42
Register Workers	42
Set Up Collector-to-Worker Communication	43
Working with Pre-6.1.0 Collectors	43
Install 6.1.1 Collectors	43
Register 6.1.1 Collectors	43

Change Log

Date	Change Description
10/06/2020	Initial release of Azure Installation and Migration Guide.
11/03/2020	Revision 1: Release of Azure Installation and Migration Guide for 6.1.1.
12/07/2020	Revision 2: Small addition to Register Collectors.
02/05/2021	Revision 3: Migration update.
08/03/2021	Revision 4: Boot up the 5.3.x or 5.4.0 Instance and Migrate to 6.1.1 section updated for 6.1.1 Azure Installation and Migration Guide.
09/01/2021	Revision 5: Create 6.1.1 New Root Disk section updated for 6.1.1 Azure Installation and Migration Guide.
11/19/2021	Revision 6: Updated Register Collectors section for 6.1.1 Guide.
08/18/2022	Revision 7: Updated All-in-one Installation section.
10/20/2022	Revision 8: Updated Register Collectors instructions for 6.x guides.

Fresh Installation

This section describes how to install FortiSIEM for the current release.

- [Pre-Installation Checklist](#)
- [All-in-one Installation](#)
- [Cluster Installation](#)

Pre-Installation Checklist

Before you begin, check the following:

- 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 and choose the Azure instance type accordingly:

Node	vCPU	RAM	Local Disks
Supervisor (All in one)	Minimum – 12 Recommended - 32	Minimum <ul style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• 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 style="list-style-type: none">• without UEBA – 24GB• with UEBA - 32GB Recommended <ul style="list-style-type: none">• without UEBA – 32GB• with UEBA - 64GB	OS – 25GB OPT – 100GB CMDB – 60GB SVN – 60GB
Workers	Minimum – 8 Recommended - 16	Minimum – 16GB Recommended – 24GB	OS – 25GB OPT – 100GB

Node	vCPU	RAM	Local Disks
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.sh` runs.

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

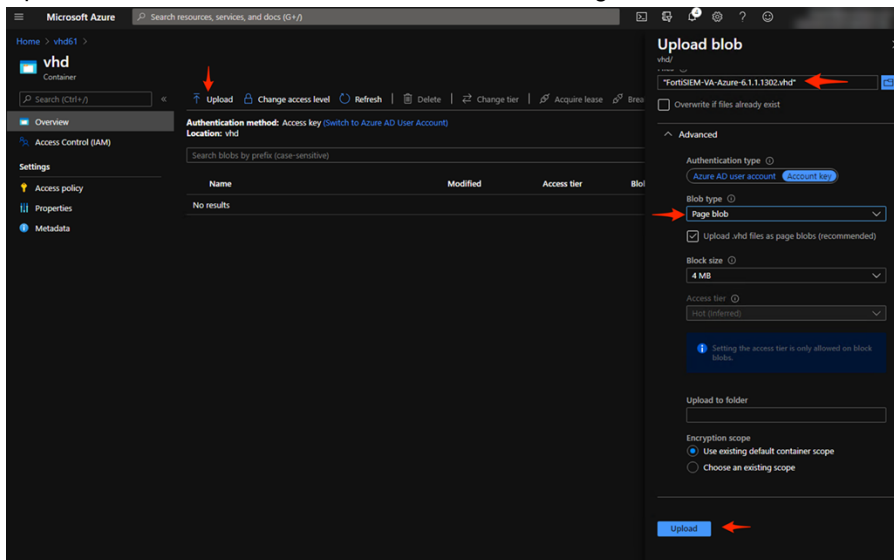
This is the simplest installation with a single Virtual Appliance. If storage is external, then you must configure external storage before proceeding with installation.

- [Create a FortiSIEM Image in Azure Using the Published VHD](#)
- [Create a VM Using FortiSIEM 6.1.1 Azure Image](#)
- [Configure FortiSIEM via GUI](#)
- [Upload the FortiSIEM License](#)
- [Choose an Event Database](#)

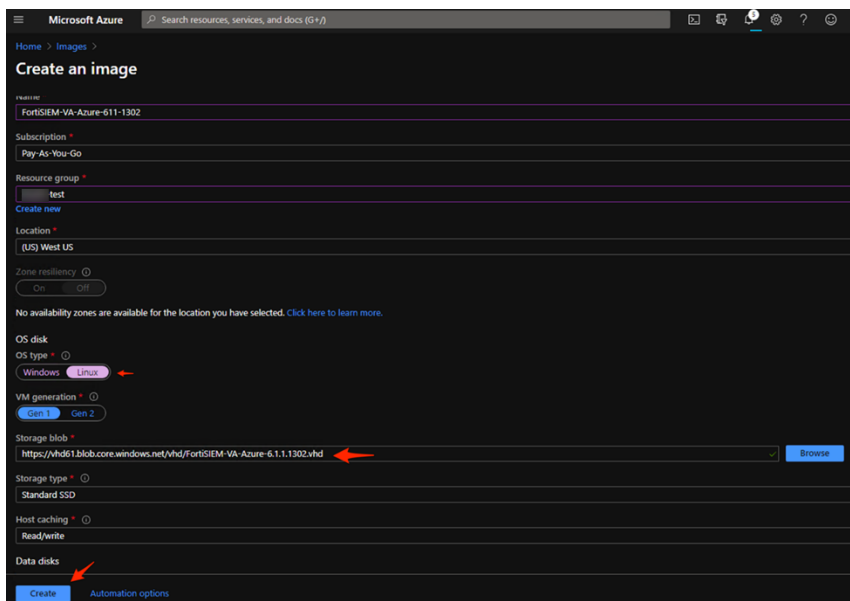
Create a FortiSIEM Image in Azure Using the Published VHD

1. Go to the Fortinet Support website <https://support.fortinet.com> to download the Azure package `FSM_Full_All_AZURE_6.1.1_Build0118.zip`.
See [Downloading FortiSIEM Products](#) for more information on downloading products from the support website.
2. Download the package for Super/Worker and Collector (for example, `FSM_Full_All_AZURE_6.1.1_Build0118.zip`) to the location where you want to install the image.
3. Unzip the `.zip` file to get the `FortiSIEM-VA-Azure-6.1.1.0118.vhd` file.

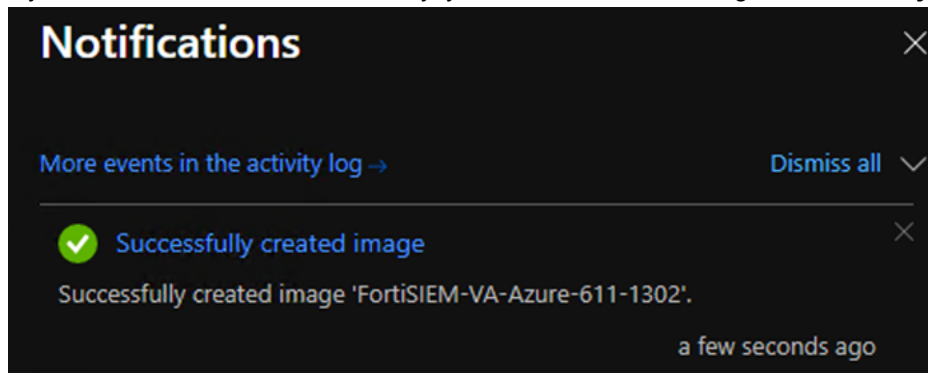
4. Upload the `.vhd` file to a container in an Azure Storage account in the location where you want to create an Image.



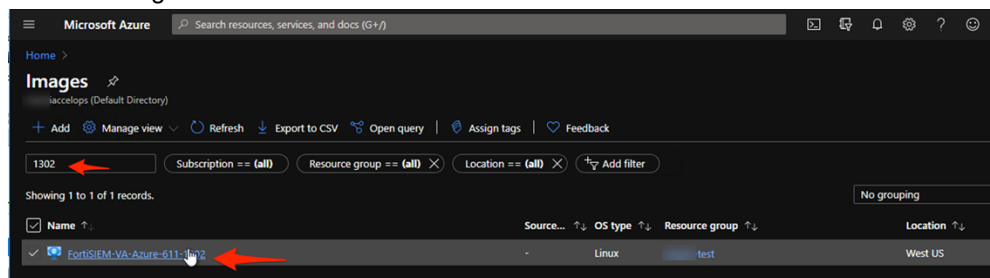
5. Wait for it to complete uploading fully (the file is approximately 25GB).
6. Navigate to the uploaded VHD and copy the URL of the object.
7. Navigate to the **Azure Images** page and click **Add**.
8. Provide the following information:
 - a. Enter the image **Name**, select the appropriate **Resource group**, and **Location**.
 - b. Choose **Linux** as the **OS type** and **Gen 1** as the **VM generation**.
 - c. Paste the URL of the object from [step 6](#) under **Storage blob**.
 - d. Choose **Standard SSD** as **Storage type**.
 - e. Click **Create**.



9. If you entered the information correctly, you should see the message: **Successfully created Image**.

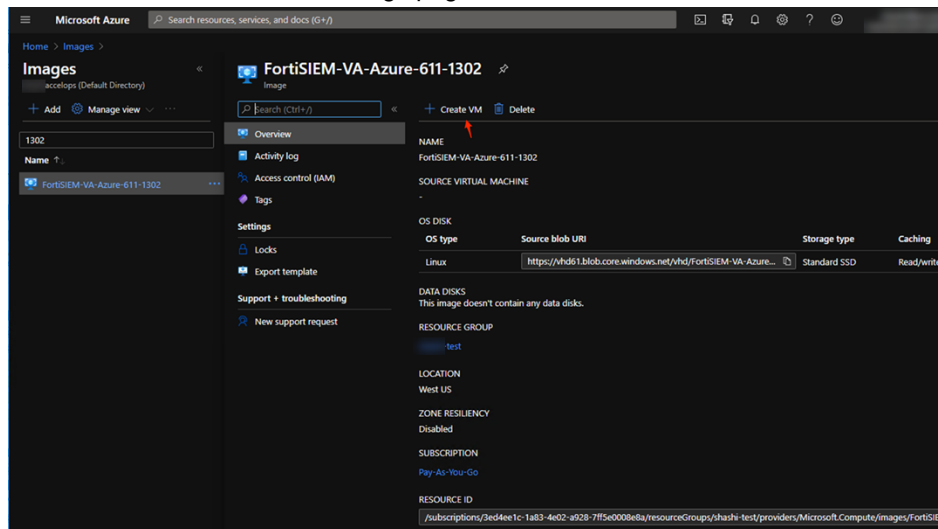


10. Navigate to **Home > Images** and search for your image name.
 11. Click the Image.



Create a VM Using a FortiSIEM 6.1.1 Azure Image

1. On the FortiSIEM 6.1.1 Azure Image page, Click **Create VM**.



2. On the **Create a virtual machine** page, choose a **Resource group**, specify a **Virtual machine name**, select an appropriate **VM Size** based on node type and hardware requirements, and generate a new **Key pair** (or use an existing one). The **Username** is specified as `azureuser`.

Microsoft Azure Search resources, services, and docs (G+)

Home > Images > FortiSIEM-VA-Azure-611-1302 >

Create a virtual machine

Basics Disks Networking Management Advanced Tags Review + create

Create a virtual machine that runs Linux or Windows. Select an image from Azure marketplace or use your own customized image. Complete the Basics tab then Review + create to provision a virtual machine with default parameters or review each tab for full customization. [Learn more](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription

Resource group * [Create new](#)

Instance details

Virtual machine name *

Region

Availability options

Image * [Browse all public and private images](#)

Azure Spot instance ☐ Yes ☒ No

Size * [Select size](#)

Administrator account

Authentication type ☒ SSH public key ☐ Password

Azure now automatically generates an SSH key pair for you and allows you to store it for future use. It is a fast, simple, and secure way to connect to your virtual machine.

Username *

SSH public key source

Key pair name *

[Review + create](#) [< Previous](#) [Next : Disks >](#)

3. Also select Inbound ports to port 22 and 443 (for production, use the **Advanced** tab for fine grained controls). Click **Next: Disks**

Inbound port rules

Select which virtual machine network ports are accessible from the public internet. You can specify more limited or granular network access on the Networking tab.

Public inbound ports * ☐ None ☒ Allow selected ports

Select inbound ports *

This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

[Review + create](#) [< Previous](#) [Next : Disks >](#)

Use these partition values:

Volume Name	Size	Disk Name
Data Disk LUN 0	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 <code>configFSM.sh</code> runs.
Data Disk LUN 1	60GB	/cmdb
Data Disk LUN 2	60GB	/svn
Data Disk LUN 3	60GB+	/data (see the following note)

Note on Data Disk LUN 3:

- Add a 4th Data 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.
- Choose Standard SSD volume type for all volumes. For the CMDb partition, you can choose to modify your volume type to Premium SSD or Ultra SSD based on your system workload if you see the consistently high IOPS requirement in your deployment.

Microsoft Azure Search resources, services, and docs (G+)

Home > Images > FortiSIEM-VA-Azure-611-1302 >

Create a virtual machine

Basics **Disks** Networking Management Advanced Tags Review + create

Azure VMs have one operating system disk and a temporary disk for short-term storage. You can attach additional data disks. The size of the VM determines the type of storage you can use and the number of data disks allowed. [Learn more](#)

Disk options

OS disk type *

Encryption type *

Enable Ultra Disk compatibility ☐ Yes ☒ No

Data disks

You can add and configure additional data disks for your virtual machine or attach existing disks. This VM also comes with a temporary disk.

LUN	Name	Size (GiB)	Disk type	Host caching
0	opt_super-611-1302_...	100	Standard SSD	Read-only
1	svn_super-611-1302_D...	60	Standard SSD	Read-only
2	cmdb_super-611-1302...	60	Premium SSD	None
3	eventdb_super-611-13...	1024	Standard SSD	Read-only

[Create and attach a new disk](#) [Attach an existing disk](#)

Advanced

[Review + create](#) [< Previous](#) [Next: Networking >](#)

- In the **Networking** tab, accept the defaults except for **NIC network security groups**. For production, choose **Advanced** and configure the required inbound ports and IP addresses (refer to [Azure documentation](#)). Click **Next: Management**.

Microsoft Azure

Search resources, services, and docs (G+/)

Home > Images > FortiSIEM-VA-Azure-611-1302 >

Create a virtual machine

Basics Disks **Networking** Management Advanced Tags Review + create

Define network connectivity for your virtual machine by configuring network interface card (NIC) settings. You can control ports, inbound and outbound connectivity with security group rules, or place behind an existing load balancing solution. [Learn more](#)

Network interface

When creating a virtual machine, a network interface will be created for you.

Virtual network *	<div>test-vnet</div> <div>Create new</div>
Subnet *	<div>default (10.1.0.0/24)</div> <div>Manage subnet configuration</div>
Public IP	<div>(new) super-611-1302-ip</div> <div>Create new</div>
NIC network security group	<div><input type="radio"/> None <input checked="" type="radio"/> Basic <input type="radio"/> Advanced</div>
Public inbound ports *	<div><input type="radio"/> None <input checked="" type="radio"/> Allow selected ports</div>
Select inbound ports *	<div>HTTPS (443), SSH (22)</div>

⚠ This will allow all IP addresses to access your virtual machine. This is only recommended for testing. Use the Advanced controls in the Networking tab to create rules to limit inbound traffic to known IP addresses.

Accelerated networking ☐ On ☒ Off

The selected image does not support accelerated networking.

Load balancing

You can place this virtual machine in the backend pool of an existing Azure load balancing solution. [Learn more](#)

Review + create

< Previous

Next : Management >

5. In the **Management** tab, accept the defaults (or change them as per [Azure documentation](#)). Click **Next: Advanced**.

The screenshot shows the 'Create a virtual machine' page in the Microsoft Azure portal, specifically the 'Management' tab. The page is for a VM named 'FortiSIEM-VA-Azure-611-1302'. The 'Management' tab is selected, and the 'Review + create' button is highlighted. The page displays configuration options for monitoring and management, including Azure Security Center, Monitoring, Identity, and Auto-shutdown. The 'Next: Advanced' button is highlighted with a red arrow.

Microsoft Azure Search resources, services, and docs (G+)

Home > Images > FortiSIEM-VA-Azure-611-1302 >

Create a virtual machine

Basics Disks Networking **Management** Advanced Tags Review + create

Configure monitoring and management options for your VM.

Azure Security Center

Azure Security Center provides unified security management and advanced threat protection across hybrid cloud workloads. [Learn more](#)

✓ Your subscription is protected by Azure Security Center standard plan.

Monitoring

Boot diagnostics ⓘ ☒ Enable with managed storage account (recommended) ☐ Enable with custom storage account ☐ Disable

OS guest diagnostics ⓘ ☐ On ☒ Off

Identity

System assigned managed identity ⓘ ☐ On ☒ Off

Auto-shutdown

Enable auto-shutdown ⓘ ☐ On ☒ Off

Review + create < Previous Next : Advanced >

6. In **Tags** tab, add a **Name** tag and other tags as needed. Click **Next: Review + create**.

The screenshot shows the 'Create a virtual machine' wizard in the Microsoft Azure portal, specifically the 'Tags' tab. The breadcrumb navigation at the top indicates the path: Home > Images > FortiSIEM-VA-Azure-611-1302 >. The wizard has several tabs: Basics, Disks, Networking, Management, Advanced, Tags (which is selected and underlined), and Review + create. Below the tabs, there is explanatory text about tags and a note that tags will be automatically updated if resource settings are changed on other tabs. The main area contains a table for adding tags with columns for Name, Value, and Resource. The first row has 'name' in the Name column, 'super-611-1302' in the Value column, and '12 selected' in the Resource column. A second empty row is provided below. Red arrows point to the 'Name' and 'Value' headers, and another red arrow points to the 'Next: Review + create >' button at the bottom right. The bottom left has a 'Review + create' button.

Name ⓘ	Value ⓘ	Resource
name	super-611-1302	12 selected
		12 selected

7. In the **Review + create** tab, verify that all the information is correct. Click **Create**.

Microsoft Azure Search resources, services, and docs (G+)

Home > Images > FortiSIEM-VA-Azure-611-1302 >

Create a virtual machine

✓ Validation passed

Management

Boot diagnostics	On
OS guest diagnostics	Off
Azure Security Center	Standard
System assigned managed identity	Off
Auto-shutdown	Off

Advanced

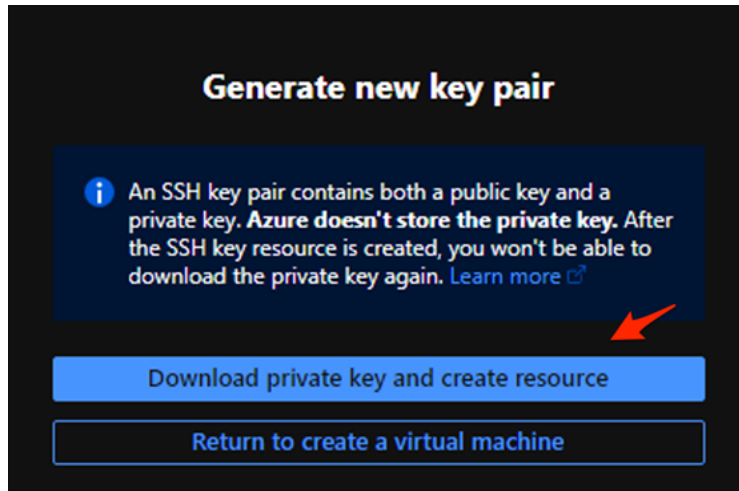
Extensions	None
Cloud init	No
Proximity placement group	None

Tags

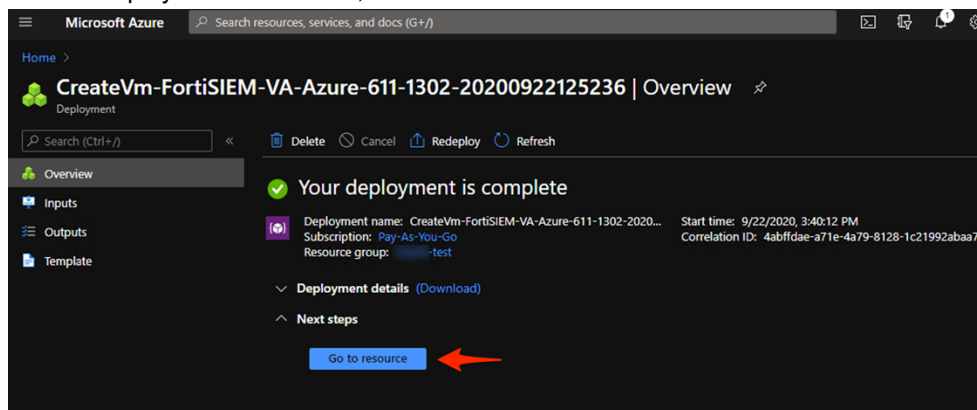
name	super-611-1302 (Auto-shutdown schedule)
name	super-611-1302 (Availability set)
name	super-611-1302 (Disk)
name	super-611-1302 (Network interface)
name	super-611-1302 (Network security group)
name	super-611-1302 (Public IP address)
name	super-611-1302 (Recovery Services vault)
name	super-611-1302 (SSH key)
name	super-611-1302 (Storage account)
name	super-611-1302 (Virtual machine)
name	super-611-1302 (Virtual machine extension)
name	super-611-1302 (Virtual network)

Create < Previous Next > Download a template for automation

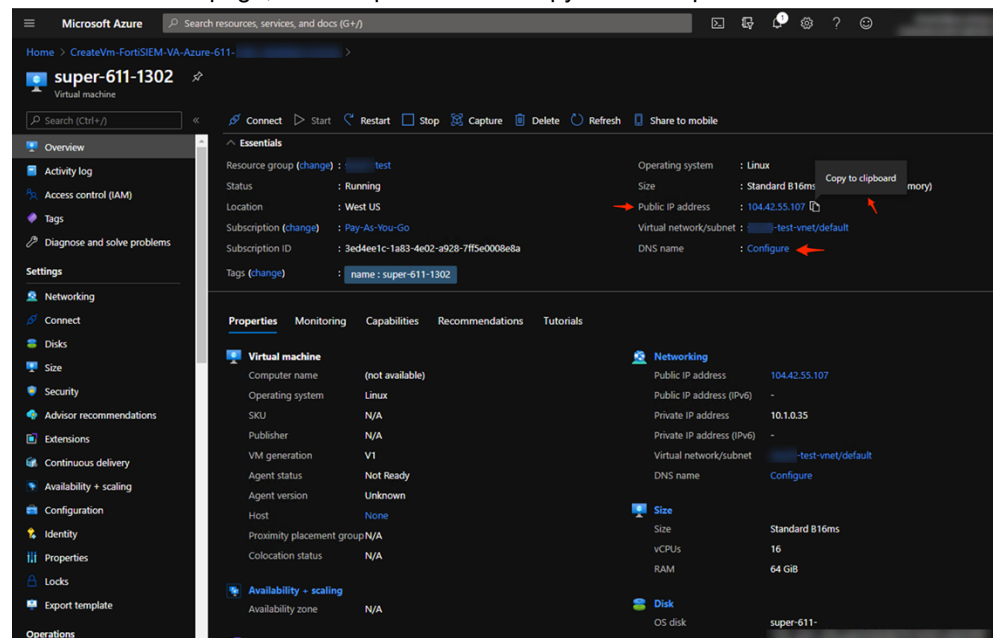
8. If you chose to create a new SSH key, then you will be asked to download the private key and create the resource. Click **Download private key and create resource**.



9. Wait for deployment to succeed, then click **Go to resource**.



10. On the **Resource** page, note the public IP and copy it to the clipboard.



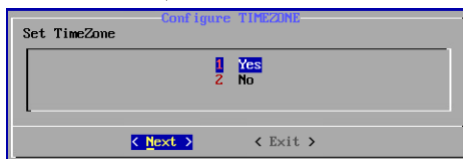
11. (Optional) Configure the DNS name as according to Azure documentation.
12. SSH to the FortiSIEM VM with user `azureuser` (as specified in page 8, step 2) and the downloaded SSH key. Run `sudo su -` to become user `root`. Alternatively, the `root` user name, is also enabled with the default password `ProspectHills`. You will have to change this password upon first log in or disable it if you prefer to only log in with SSH key.

```
[ $ ssh -i ~/.ssh/fsm-westus-ssh-key.pem azureuser@104.42.55.107
Last login: Tue Sep 22 17:55:11 2020 from 69.181.213.37
[azureuser@super-611-1302 ~]$ sudo su -
Last login: Tue Sep 22 17:55:15 CDT 2020 on pts/0
[root@super-611-1302 ~]# configFSM.sh
```

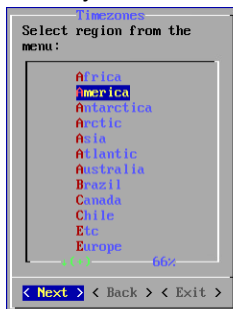
Configure FortiSIEM via GUI

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

1. At the `root` command prompt, go to `/usr/local/bin` and enter `configFSM.sh`, for example:
`# configFSM.sh`
2. In VM console, select **1 Set Timezone** and then press **Next**.



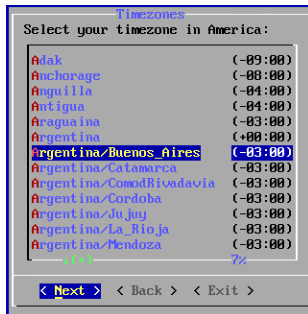
3. Select your **Location**, and press **Next**.



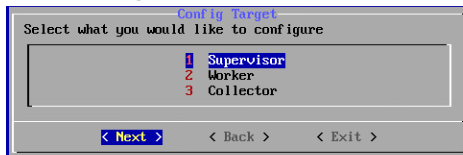
4. Select your **Continent**, and press **Next**.



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

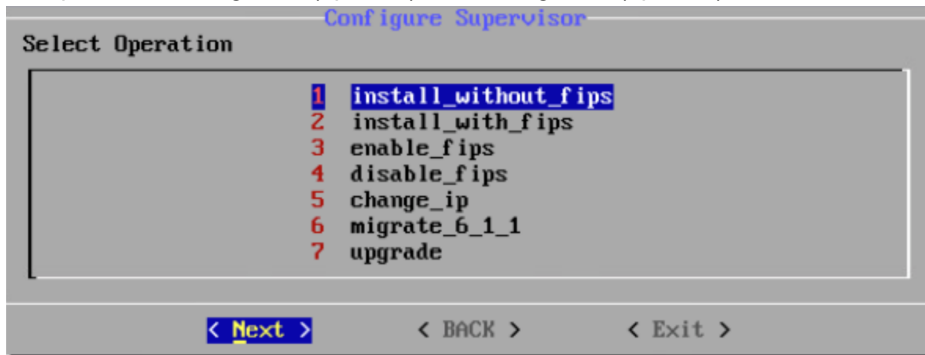


6. Select **1 Supervisor**. Press **Next**.



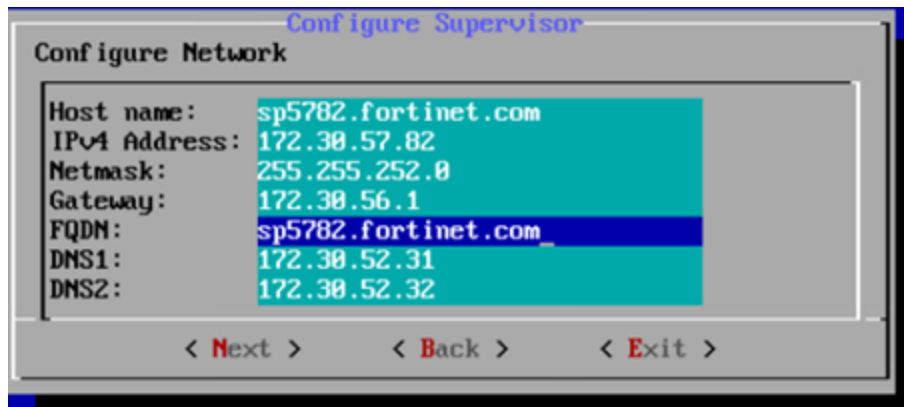
Regardless of whether you select **Supervisor**, **Worker**, or **Collector**, you will see the same series of screens.

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



8. Configure the network by entering the following fields. Press **Next**.

Option	Description
Host Name	The Supervisor's host name
IPv4 Address	The Supervisor's IPv4 address
Netmask	The Supervisor's subnet
Gateway	Network gateway address
FQDN	Fully-qualified domain name
DNS1, DNS2	Addresses of the DNS servers



9. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and responds to ping. The host can either be an internal host or a public domain host like google.com. In order for the migration to complete, the system still needs https connectivity to FortiSIEM OS update servers – `os-pkgs-cdn.fortisiem.fortinet.com` and `os-pkgs-c8.fortisiem.fortinet.com`. Then, click **Next**.



10. 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

Option	Description
-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 4 (for ipv4) or 6 (for v6) Note: the 6 value is not currently supported.
--dns1, --dns2	Addresses of the DNS server 1 and DNS server 2.
-o	Installation option (install_without_fips , install_with_fips , enable_fips , disable_fips , change_ip , or migrate_6_1_1)
-z	Time zone. Possible values are US/Pacific , Asia/Shanghai , Europe/London , or Africa/Tunis
--testpinghost	The URL used to test connectivity

11. 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.
2. The License Upload dialog box will open.

- Click **Browse** and upload the license file.
Make sure that the **Hardware ID** shown in the License Upload page matches the license.
- 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.
- 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](#).



FortiSIEM

Event Database storage:

☐ Local Disk

☐ NFS

☐ Elasticsearch

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: 21:12:02 up 1:11, 1 user, load average: 0.16, 0.20, 0.36
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 16.0% user, 6.2% sys, 2.1% id, 0.0% ni, 91.4% do, 0.0% wa, 0.2% hi, 0.1% si, 0.0% st
Mem: 65782100k total, 18366836k used, 55336864k free, 4352k buffers
Swap: 2621436k total, 0k used, 2621436k free, 2465828k cached

PROCESS          UPTIME          CPU%          VIRT_MEM        RES_MEM
phParser          41:23           0             2176m           550m
phQueryMaster     41:41           0             1820m           77m
phRuleMaster      41:41           0             1972m           594m
phRuleKeeper      41:41           0             1363m           295m
phQueryWorker     41:41           0             1383m           279m
phDataManager     41:41           0             1419m           285m
phDiscover        41:41           0             513m            53m
phReportWorker    41:41           0             1433m           95m
phReportMaster    41:41           0             683m            67m
phIdentityWorker  41:41           0             1827m           50m
phIdentityMaster  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           270m
phBeaconEventPackager 41:41           0             1125m           65m
phDataPurger      41:41           0             588m           50m
phEventForwarder  41:41           0             240m            46m
phMonitor         37:24           0             2880m           53m
Apache            01:10:40        0             310m            16m
Node.js-charting  01:10:19        0             216m            71m
Node.js-pm2       01:10:13        0             26m             26m
AppSvc            01:10:07        0             15172m          3826m
DBSvc             01:10:30        0             317m            30m
phAnomaly         01:00:07        0             907m            64m
phFortiInsightAI  01:10:40        0             23432m          430m
Redis             01:10:10        0             55m             25m
```

Cluster Installation

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

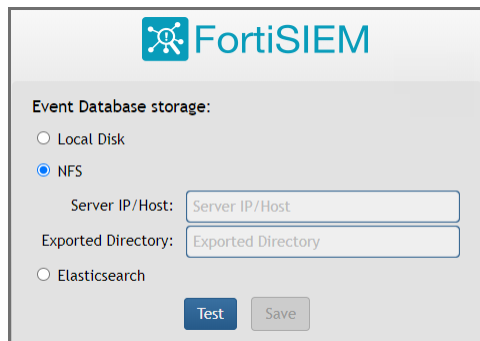
- [Install Supervisor](#)
- [Install Workers](#)
- [Register Workers](#)
- [Install Collectors](#)
- [Register Collectors](#)

Install Supervisor

Follow the steps in [All-in-one Install](#) with two differences:

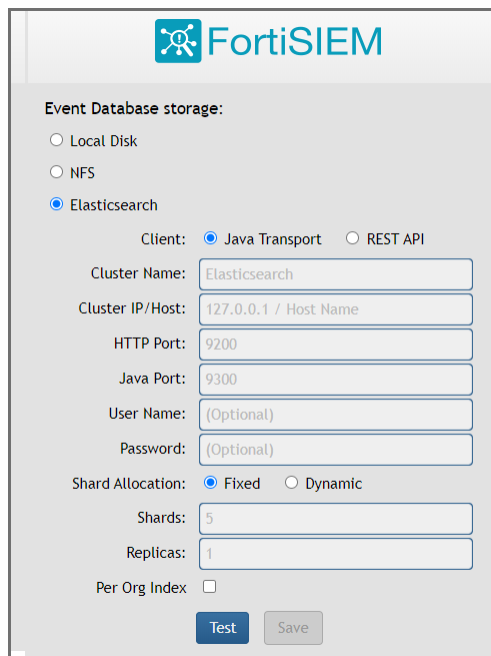
- Setting up hardware - you do not need to add an EBS Volume 5 for Event database.
- Setting up an Event database - Configure the cluster for either NFS or Elasticsearch.

NFS



The screenshot shows the FortiSIEM configuration interface for NFS storage. The 'Event Database storage:' section has three radio buttons: 'Local Disk', 'NFS' (selected), and 'Elasticsearch'. Below the 'NFS' option, there are two text input fields: 'Server IP/Host:' and 'Exported Directory:'. At the bottom of the form are two buttons: 'Test' and 'Save'.

Elasticsearch



The screenshot shows the FortiSIEM configuration interface for Elasticsearch storage. The 'Event Database storage:' section has three radio buttons: 'Local Disk', 'NFS', and 'Elasticsearch' (selected). Below the 'Elasticsearch' option, there is a 'Client:' section with two radio buttons: 'Java Transport' (selected) and 'REST API'. Below this are several text input fields: 'Cluster Name:' (containing 'Elasticsearch'), 'Cluster IP/Host:' (containing '127.0.0.1 / Host Name'), 'HTTP Port:' (containing '9200'), 'Java Port:' (containing '9300'), 'User Name:' (containing '(Optional)'), and 'Password:' (containing '(Optional)'). Below these is a 'Shard Allocation:' section with two radio buttons: 'Fixed' (selected) and 'Dynamic'. Below this are two text input fields: 'Shards:' (containing '5') and 'Replicas:' (containing '1'). At the bottom is a 'Per Org Index' checkbox (unchecked). At the bottom of the form are two buttons: 'Test' and 'Save'.

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 you need to only choose OS and OPT disks. The recommended CPU and memory settings for Worker node, and required hard disk settings are:

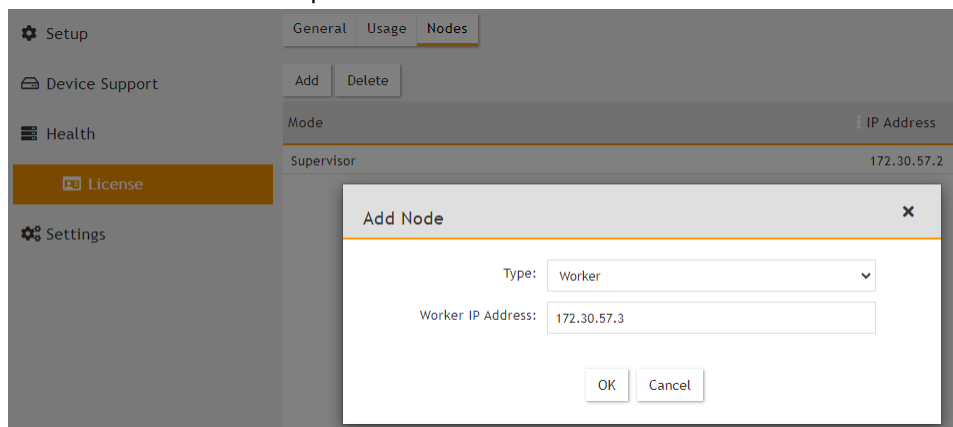
- CPU = 8
- Memory = 24 GB
- Two hard disks:
 - OS – 25GB
 - OPT – 100GB

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.sh` runs.

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. Click **Add**.



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

system.

The screenshot displays the FortiSIEM Cloud Health interface. The left sidebar contains navigation options: Setup, Device Support, Health (selected), License, and Settings. The main content area is divided into two sections. The top section, titled 'Cloud Health', shows a table with columns: Name, IP Address, Module Role, Health, Version, Load Average, CPU, and Swap Used. It lists two nodes: 'sp572.fortinet.com' (Supervisor) and 'wk573.fortinet.com' (Worker), both with a 'Normal' health status. The bottom section, titled 'Process level metrics for wk573.fortinet.com (172.30.57.3)', shows a table with columns: Process Name, Status, Up Time, CPU, Physical Memory, Virtual Memory, SharedStore ID, and SharedStore Position. It lists several processes including 'Node.js-charting', 'httpd', 'Redis', 'Node.js-pm2', 'rsyslogd', and 'phpDataManager', all with a status of 'Up'. The footer of the interface includes copyright information for Fortinet, Inc. (2020) and the FortiSIEM logo.

Name	IP Address	Module Role	Health	Version	Load Average	CPU	Swap Used
sp572.fortinet.com	172.30.57.2	Supervisor	Normal	6.1.0.1238	0.95,0.47,0.43	4%	0 KB
wk573.fortinet.com	172.30.57.3	Worker	Normal	6.1.0.1238	0.1,0.2,0.16	2%	0 KB

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		
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		
phpDataManager	Up	14m 6s	0%	103 MB	1229 MB	1	126108

Install Collectors

Once Supervisor and Workers are installed, follow the same steps in [All-in-one Install](#) to install a Collector except when adding disks, you need to only add a data disk for OPT. The recommended CPU and memory settings for Collector node, and required hard disk settings 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.sh` runs.

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:

```
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.

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	1.1.1.1	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 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**.

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

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.

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

```
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.

- Set `user` and `password` using the admin user name and password for the Organization that the Collector is going to be registered to.
- Set `Super IP` or `Host` as the Supervisor's IP address.
- Set `Organization` as the name of an organization created on the Supervisor.
- Set `CollectorName` from [Step 6](#).

```
root@co574 ~# phProvisionCollector
Usage: phProvisionCollector --add <Organization-user-name> <Organization-user-password> <Supervisor-IP> <Organization-name> <Collector-name>
root@co574 ~# phProvisionCollector --add admin admin=11 172.30.57.2 ORG CO-ORG
Continuing to provision the Collector
This collector is registered successfully. Normal Exit and restart of phMonitor after collector license registration.
root@co574 ~# _
```

The Collector will reboot during the Registration.

- Go to **ADMIN > Health > Collector Health** and check the status.

The screenshot shows the FortiSIEM interface with the 'Collector Health' tab selected. The main table displays the status of the 'Super' collector for the 'CO-ORG' organization. Below this, a 'Show Processes' panel is open, showing a detailed view of the collector's internal processes.

Organization	Name	IP Address	Status	Health	Up Time	CPU	Memory	Allocated EPS	Incoming EPS	Version	Col
Super	CO-ORG	1 172.30.57.2	up	Normal	3m 4s	65%	5%	200	0	6.1.0...	100

Process Name	Status	Up Time	CPU	Physical Memory	Virtual Memory	SharedStore ID	SharedStore Position
phMonitorAgent	Up	29s	0%	575 MB	1116 MB		
phParser	Up	17s	0%	106 MB	1190 MB	99	0
phPerfMonitor	Up	17s	0%	79 MB	766 MB		
phEventForwarder	Up	17s	0%	48 MB	547 MB		
phDiscover	Up	17s	0%	53 MB	513 MB		

Migrating from FortiSIEM 5.3.x or 5.4.0

Migration limitations: If migrating from 5.3.3 or 5.4.0 to 6.1.1, please be aware that the following features will not be available after migration.

- Pre-compute feature
- Elastic Cloud support

If any of these features are critical to your organization, then please wait for a later version where these features are available after migration.

This section describes how to migrate from FortiSIEM 5.3.x or 5.4.0 to FortiSIEM 6.1.1. FortiSIEM performs migration in-place. The migration process backs up some important information from the original 5.3.x or 5.4.0 root disk, and then changes the root disk to boot up from a new 6.1.1 root disk. There is no need to copy disks. The instance identity remains the same.

- [Pre-Migration checklist](#)
- [Migrate All-in-one Installation](#)
- [Migrate Cluster](#)

Pre-Migration Checklist

To perform the migration, the following prerequisites must be met:

- 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.
- Delete the Worker from the Super GUI.
- Stop/Shutdown the Worker.
- Note the `/svn` partition by running the `df -h` command. the partition is used to mount `/svn/53x-settings`. You will need this information for a later step.
- Create a `/svn/53x-settings` directory and symlink it to `/images`. The `/svn` partition should have at enough space to hold `/opt/phoenix` from your current system. Typically, 10 GB is enough. See the following example:

```
[root@fsm-super-532 ~]# cat /opt/phoenix/bin/VERSION
Version: 5.3.2.1672
DSVersion: 5.3.2.1672
CommitHash:ea7d59d2f
Built on: 1594088061
Local time: Mon Jul  6 19:14:21 PDT 2020
[root@fsm-super-532 ~]# mkdir /svn/53x-settings
[root@fsm-super-532 ~]# ln -sf /svn/53x-settings /images
[root@fsm-super-532 ~]#
```

Migrate All-in-one Installation

- [Download the Backup Script](#)
- [Run the Backup Script and Shutdown](#)
- [Create 6.1.1 New Root Disk](#)
- [Swap 6.1.1 OS Disk on Your 5.3.x or 5.4.x Instance](#)
- [Boot Up the 5.3.x or 5.4.0 Instance and Migrate to 6.1.1](#)

Download the Backup Script

Download FortiSIEM Azure backup script to start migration. Follow these steps:

1. # Download the file `FSM_Backup_5.3_Files_6.1.1_Build0118` file from the [support site](#) and copy it to the 5.3.x or 5.4.0 Azure instance that you are planning to migrate to 6.1.1 (for example, `/svn/53x-settings`).
2. Unzip the .zip file, for example:
`unzip FSM_Backup_5.3_Files_6.1.1_Build0118.zip`

Run the Backup Script and Shutdown System

Follow these steps to run the backup script and shut down the system:

1. Go to the directory where you downloaded the backup script, for example:
`cd /svn/53x-settings/FSM_Backup_5.3_Files_6.1.1_Build0118`
2. Run the backup script with the `sh backup` command to backup 5.3.x or 5.4.x settings that will be migrated later into the new 6.1.1 OS. For example:
`sh backup`
3. Run the `shutdown` command to shut down the FortiSIEM instance, for example:
`shutdown -h now`

```
[root@fsm-super-532 FSM_Backup_5.3_Files_6.1.1_build1307]# sh backup
backing up DataBases
Stopping httpd: [ OK ]
Stopping postgresql-9.4 service: [ OK ]
Log Directory /opt/phoenix/log Exists, Cleaning
Log Directory /opt/glassfish3/glassfish/domains/domain1/logs Exists, Cleaning
Compressing /opt/glassfish3 to fsm_53_glassfish.xz
/images/fsm_53_glassfish.xz (1/1)
100 % 593.1 MiB / 959.4 MiB = 0.618 40 MiB/s 0:24
Compressing /opt/phoenix to fsm_53_phoenix.xz
/images/fsm_53_phoenix.xz (1/1)
100 % 1,230.1 MiB / 3,363.9 MiB = 0.366 63 MiB/s 0:53
backing Up Network Parameters
SSLCertificateFile setting is a self-signed certificate file localhost.crt, ignoring the file for migration...
localhost.key
SSLCertificateKeyFile setting is a self-signed certificate key file localhost.key, skipping backup of SSL certificate key file...
No certificate chain file defined in SSLCertificateChainFile setting. Skipping backup of SSL certificate chain file...
[root@fsm-super-532 FSM_Backup_5.3_Files_6.1.1_build1307]# shutdown -h now

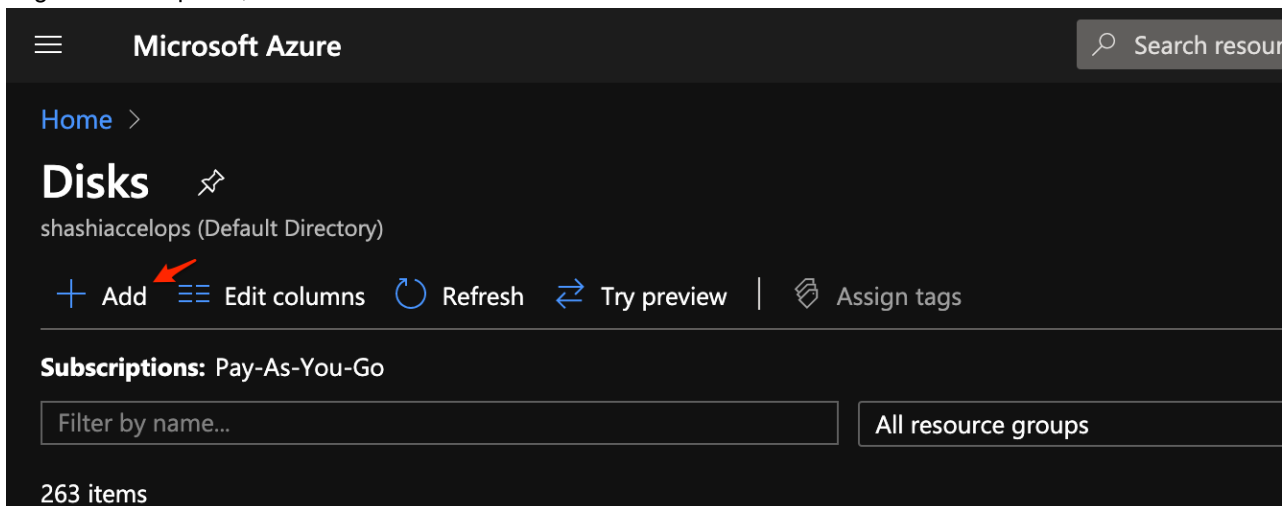
Broadcast message from azureuser@fsm-super-532
(/dev/pts/2) at 0:09 ...

The system is going down for halt NOW!
[root@fsm-super-532 FSM_Backup_5.3_Files_6.1.1_build1307]# Connection to 168.62.218.75 closed by remote host.
Connection to 168.62.218.75 closed.
```

Create 6.1.1 New Root Disk

Follow these steps to create a new 6.1.1 root disk from the Azure portal.

1. Log in to Azure portal, select **Home > Disks** service and then click **Add**.



2. Fill in the disk details and choose **Storage blob** as the Source type and find 6.1.1 OS VHD (refer to earlier section on how to upload this VHD).
Note: The root disk must be 25GB, and the size must not be changed.

3. Click **Review + Create** after filling in the rest of the details if necessary.

Microsoft Azure Search resources, services, and docs (G)

Home > Disks >

Create a managed disk

Basics Encryption Advanced Networking Tags Review + create

Select the disk type and size needed for your workload. Azure disks are designed for 99.999% availability. Azure managed disks encrypt your data at rest, by default, using Storage Service Encryption. [Learn more about disks.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Pay-As-You-Go

Resource group * ⓘ -test [Create new](#)

Disk details

Disk name * ⓘ 6-1-1-1309-root-disk ✓

Region * ⓘ (US) West US

Availability zone None

Source type ⓘ Storage blob

Source subscription Pay-As-You-Go

Source blob * ⓘ <https://vhd61.blob.core.windows.net/vhd/FortiSIEM-VA-Azure-6.1.1.1309.vhd> ✓ [Browse](#)

OS type ⓘ Windows Linux None (data disk)

VM generation ⓘ Gen 1 Gen 2

Size * ⓘ 25 GiB
Standard SSD
[Change size](#)

[Review + create](#) < Previous Next : Encryption >

4. Verify that of the details are correct, then click **Create**.

Microsoft Azure

Search resources, services, a

Home > Disks >

Create a managed disk

✓ Validation passed

Basics Encryption Advanced Networking Tags Review + create

Basics

Subscription	Pay-As-You-Go
Resource group	-test
Region	West US
Disk name	6-1-1-1309-root-disk
Availability zone	None
Source type	Storage blob
Source blob	https://vhd61.blob.core.windows.net/vhd/FortiSIEM-VA-Azure-6.1.1.1309.vhd
OS type	Linux

Size

Size	25 GiB
Storage type	Standard SSD

Encryption

Encryption type	Platform-managed key
-----------------	----------------------

Advanced

Enable shared disk	No
--------------------	----

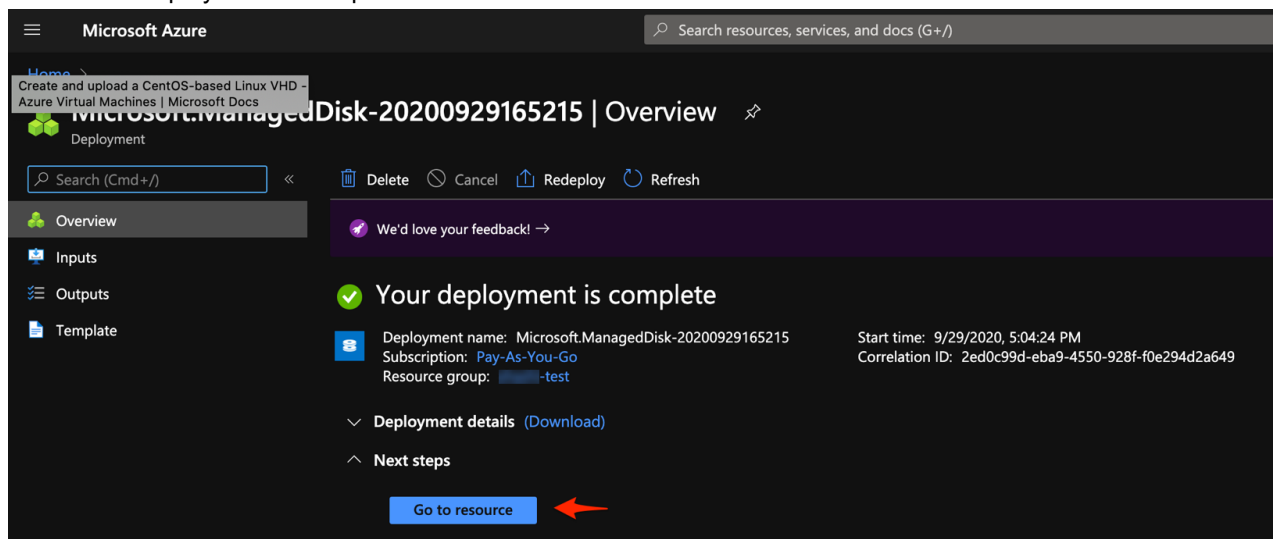
Networking

Connectivity method	AllowAll
---------------------	----------

Tags

Create < Previous Next > Download a template for automation

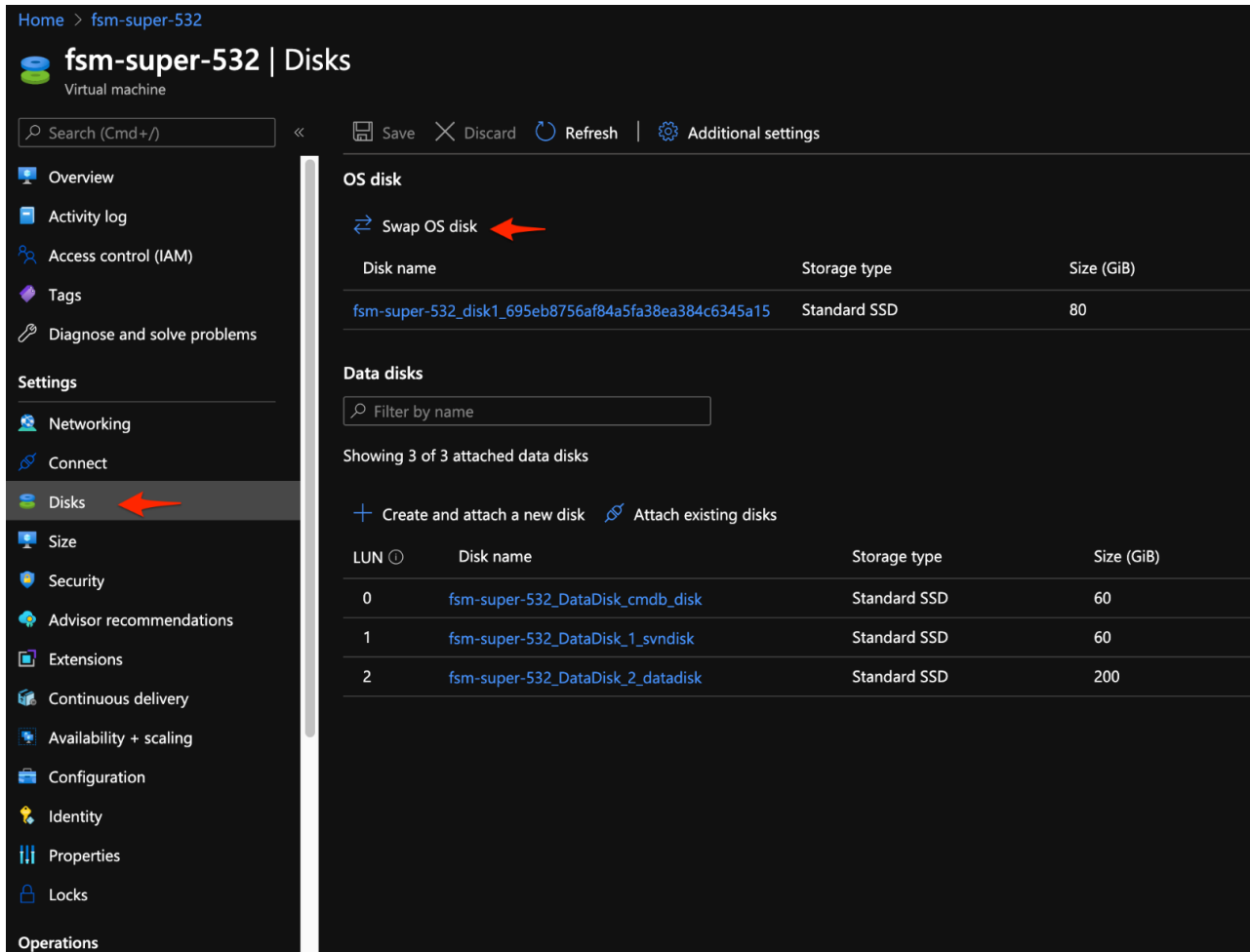
- Wait for the deployment to complete. Click **Go to resource** and note the name of the resource.



Swap 6.1.1 OS Disk on Your 5.3.x or 5.4.0 Instance

Follow these steps to swap OS disk from the 5.3.x or 5.4.0 disk to 6.1.1 disk on the 5.3.x or 5.4.0 instance that you are migrating.

1. Navigate to the 5.3.x or 5.4.0 VM and navigate to **Disks**, which is located in the side bar. Click **Swap OS disk**.



Home > fsm-super-532

fsm-super-532 | Disks

Virtual machine

Search (Cmd+/) << Save Discard Refresh Additional settings

- Overview
- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems
- Settings
 - Networking
 - Connect
 - Disks**
 - Size
 - Security
 - Advisor recommendations
 - Extensions
 - Continuous delivery
 - Availability + scaling
 - Configuration
 - Identity
 - Properties
 - Locks
- Operations

OS disk

Swap OS disk

Disk name	Storage type	Size (GiB)
fsm-super-532_disk1_695eb8756af84a5fa38ea384c6345a15	Standard SSD	80

Data disks

Filter by name

Showing 3 of 3 attached data disks

+ Create and attach a new disk Attach existing disks

LUN	Disk name	Storage type	Size (GiB)
0	fsm-super-532_DataDisk_cmdb_disk	Standard SSD	60
1	fsm-super-532_DataDisk_1_svndisk	Standard SSD	60
2	fsm-super-532_DataDisk_2_datadisk	Standard SSD	200

2. Choose the 6.1.1 root disk you just created, fill in the confirmation box and click **OK**.

Microsoft Azure

Home > fsm-super-532 >

Swap OS Disk

Swap the OS disk for a backup disk or another disk for VM troubleshooting, [Learn more](#).

Choose disk *

6-1-1-1309-root-disk

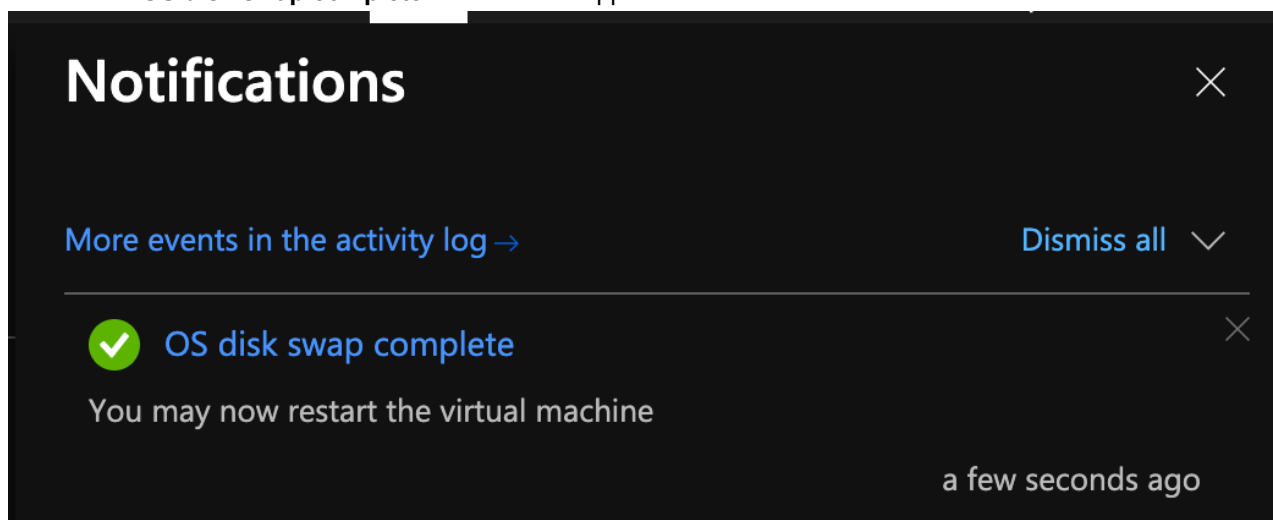
⚠ This VM will be stopped (deallocated) and the OS disk will be replaced. Any existing data on the OS disk will be lost.

Confirm you want to swap the OS disk for this VM by entering the name of the vm 'fsm-super-532'

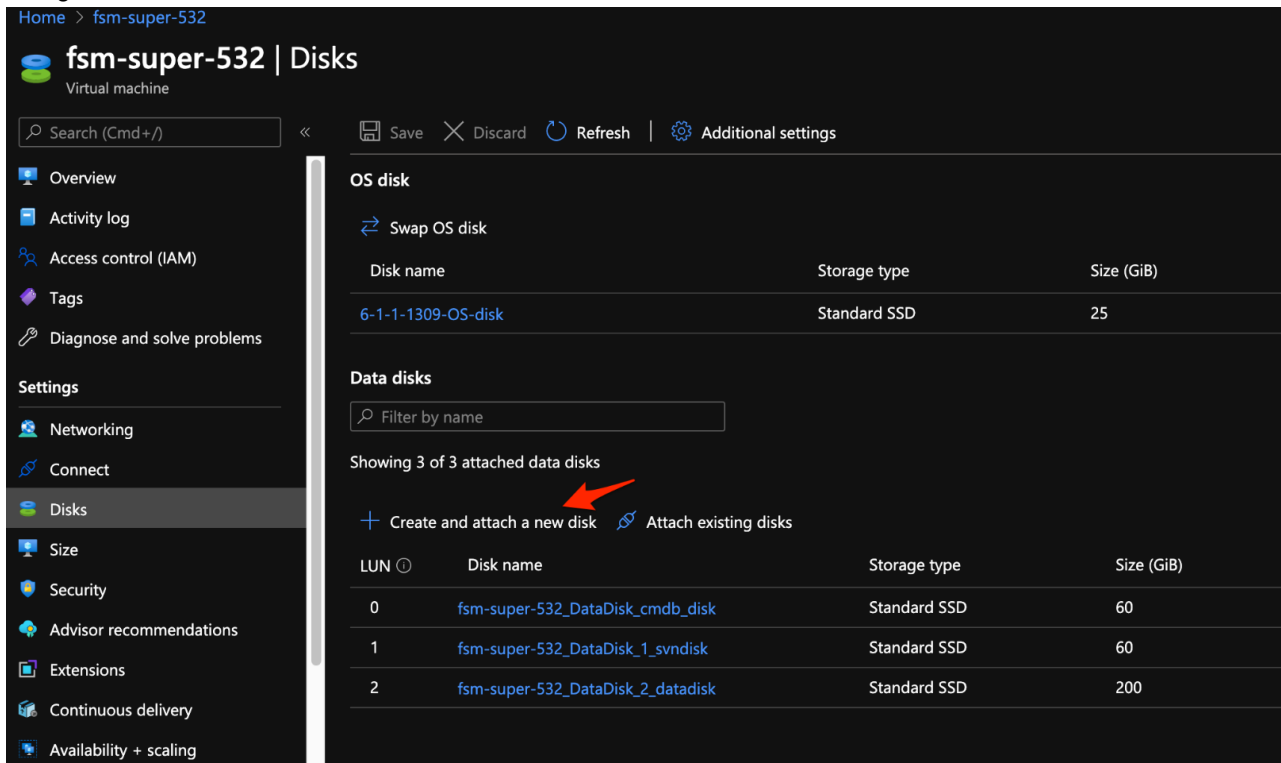
fsm-super-532

OK

3. Wait for the **OS disk swap complete** notification to appear.



4. Navigate to the VM Overview, then click **Disks** in the sidebar. Click **Create and attach a new disk**.



The screenshot shows the Azure portal interface for a virtual machine named 'fsm-super-532'. The 'Disks' section is active in the sidebar. The main content area shows the 'OS disk' and 'Data disks' sections. The 'OS disk' section shows a single disk named '6-1-1-1309-OS-disk' with a storage type of 'Standard SSD' and a size of '25 GiB'. The 'Data disks' section shows three attached data disks. A red arrow points to the 'Create and attach a new disk' button.

LUN	Disk name	Storage type	Size (GiB)
0	fsm-super-532_DataDisk_cmdb_disk	Standard SSD	60
1	fsm-super-532_DataDisk_1_svndisk	Standard SSD	60
2	fsm-super-532_DataDisk_2_datadisk	Standard SSD	200

5. Add a 100 GiB opt disk and click **OK**

Microsoft Azure

Home > fsm-super-532 >

Create a new disk

Create a new disk to store applications and data on your VM. Disk pricing varies based on factors including disk size, storage type, and number of transactions. [Learn more](#)

Name * →

Source type * ⓘ

Size * ⓘ → **100 GiB**
Standard SSD
[Change size](#)

Encryption type *

OK ←

6. On the **Disks** page, select **Read-only** under **Host caching**, and click **Save**.

Save Discard Refresh Additional settings

OS disk

Swap OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...)	Encryption ⓘ	Host caching ⓘ
6-1-1-1309-OS-disk	Standard SSD	25	500	60	SSE with PMK	Read/write

Data disks

Filter by name

Showing 4 of 4 attached data disks

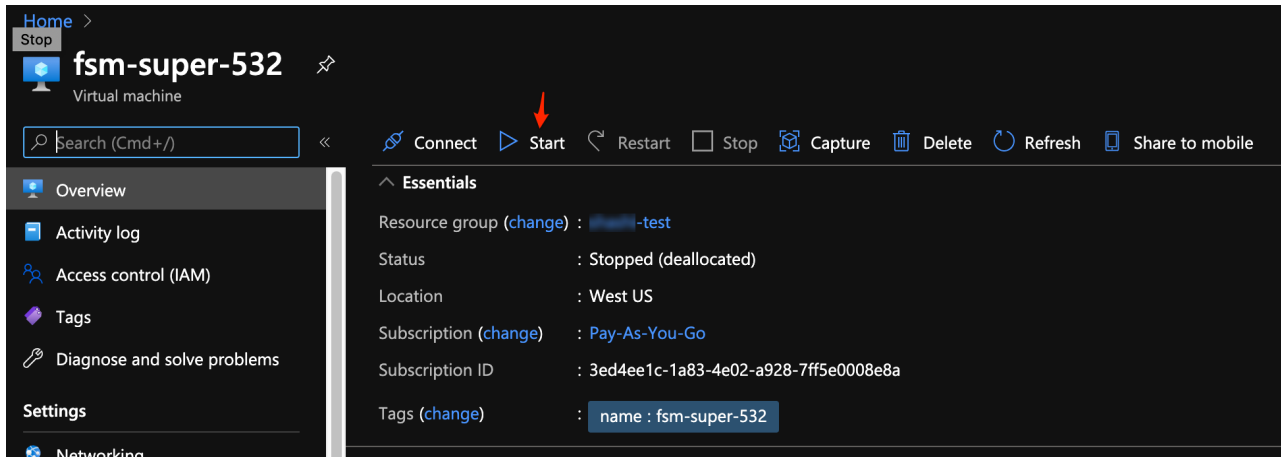
+ Create and attach a new disk Attach existing disks

LUN ⓘ	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...)	Encryption ⓘ	Host caching ⓘ
0	fsm-super-532_DataDisk_cmdb_disk	Standard SSD	60	500	60	SSE with PMK	Read-only
1	fsm-super-532_DataDisk_1_syndisk	Standard SSD	60	500	60	SSE with PMK	Read-only
2	fsm-super-532_DataDisk_2_datadisk	Standard SSD	200	500	60	SSE with PMK	Read-only
4	opt-disk	Standard SSD	100	500	60	SSE with PMK	Read-only

Boot up the 5.3.x or 5.4.0 Instance and Migrate to 6.1.1

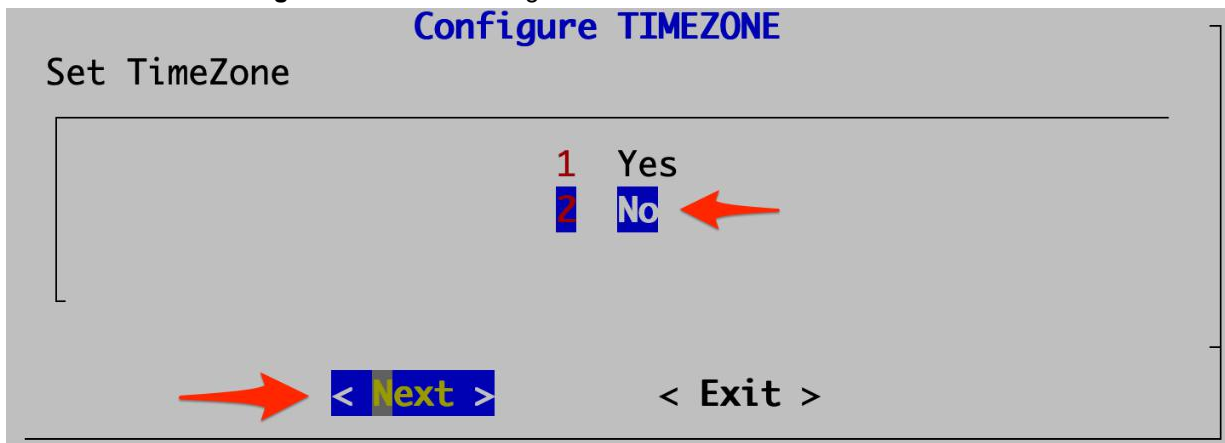
Follow these steps to complete the migration process:

1. Navigate to the VM **Overview**, click **Refresh**, and **Start** the virtual machine.

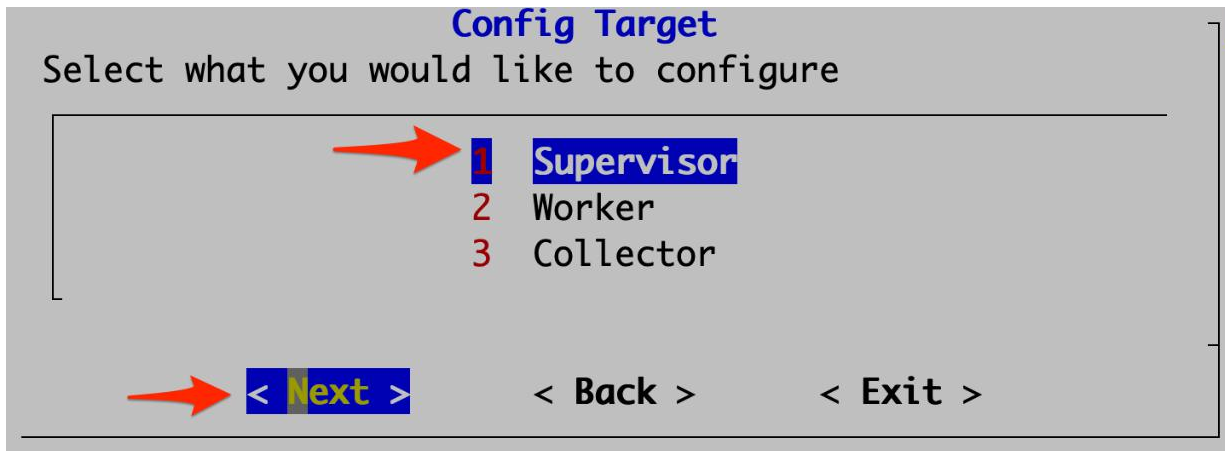


2. At the end of booting, log in with the default login credentials: User: `root` and Password: `ProspectHills`. You must use `root` to login to the system after booting up the 6.1.1 OS disk. The 5.3.x or 5.4.0 configure user name can not be used to login to the system.
3. You will be required to change the password. Remember this password for future use.
4. Use the `/svn` partition noted earlier and mount it to `/mnt`. This contains the backup of the 5.3.x or 5.4.0 system settings that will be used during migration. Copy the 5.3.x or 5.4.0 settings that were previously backed up and unmount `/mnt`. For example:

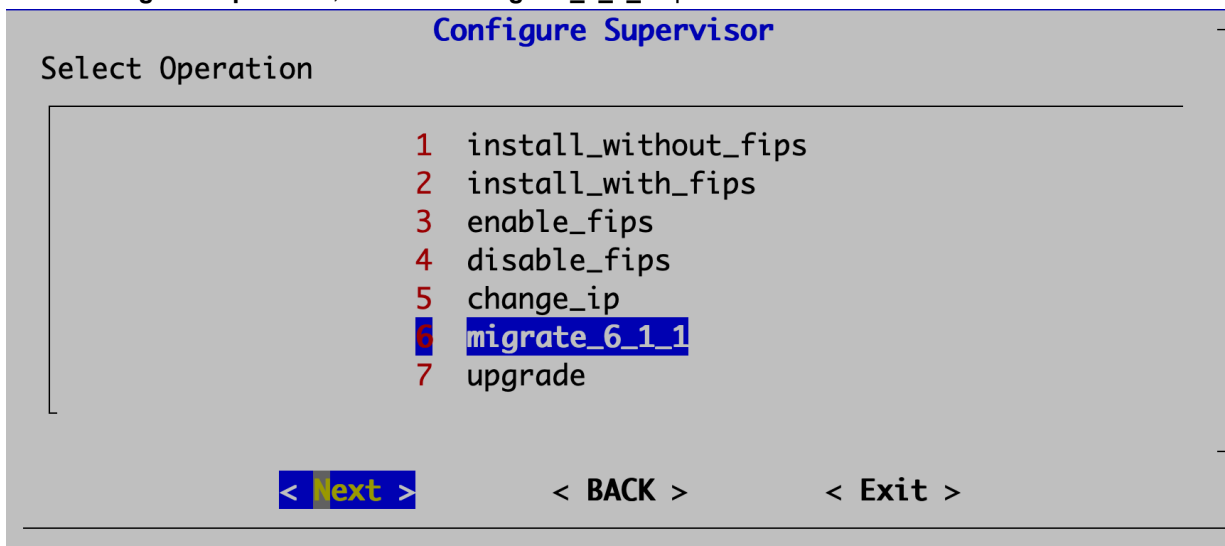
```
# mount /dev/sdb1 /mnt
# mkdir /restore-53x-settings
# cd /restore-53x-settings
# rsync -av /mnt/53x-settings/ .
# ln -sf /restore-53x-settings /images
# umount /mnt
```
5. Run the command `configFSM.sh` script to open the configuration GUI:
 - a. Select **2 No** in the **Configure TIMEZONE** dialog and then click **Next**.



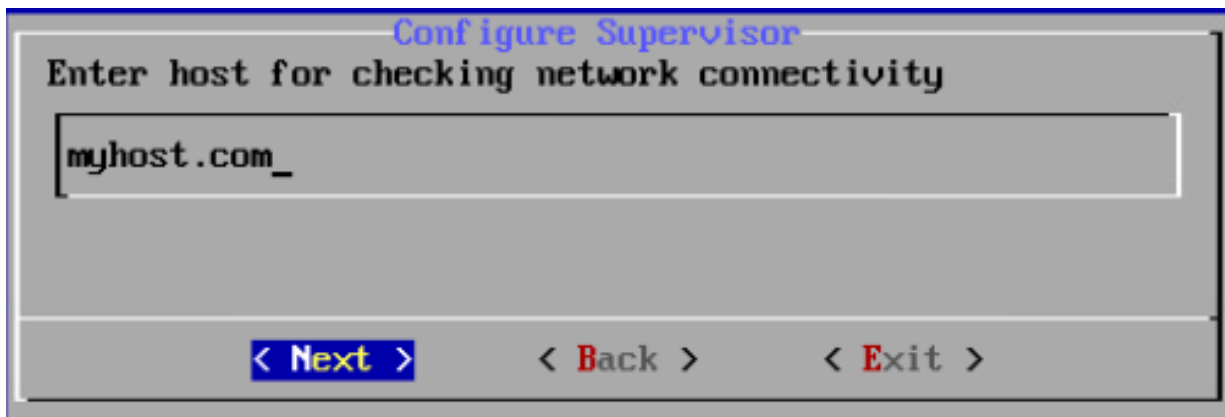
- b. In **Config Target**, select your node type: Supervisor, Worker, or Collector. This step is usually performed on Supervisor (**1 Supervisor**). Click **Next**.



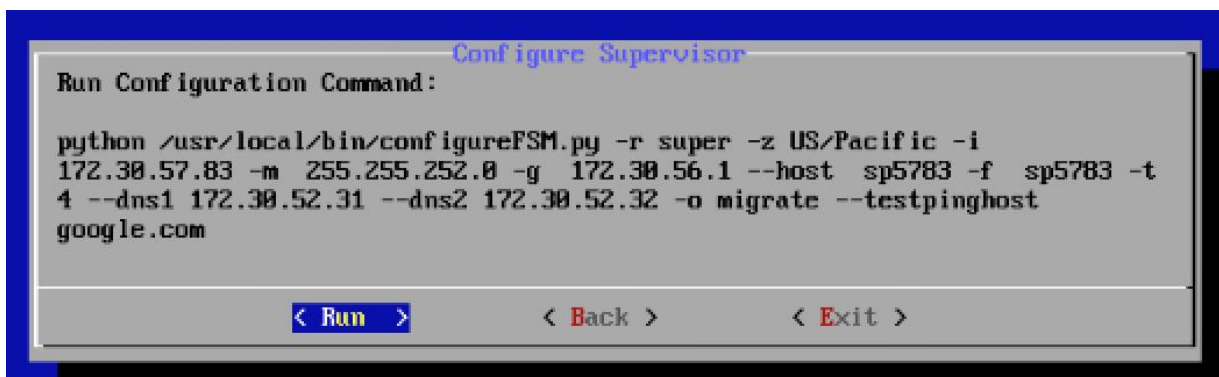
- c. In the **Configure Supervisor**, select the **6 migrate_6_1_1** operation and then click **Next**.



- d. Test network connectivity by entering a host name that can be resolved by your DNS Server (entered in the previous step) and responds to ping. The host can either be an internal host or a public domain host like google.com. In order for the migration to complete, the system still needs https connectivity to FortiSIEM OS update servers - os-pkgs-cdn.fortisiem.fortinet.com and os-pkgs-c8.fortisiem.fortinet.com. Click **Next**.



- e. Run on the confirmation page once you make sure all the values are correct. The options are described in the table [here](#).



- f. Wait for the operations to complete and the system to reboot.
- g. Wait for about 2 minutes before logging into the system. Wait another 5-10 minutes for all of the processes to start up. Then, execute the `phstatus` command to see the status of FortiSIEM processes.


```

root@168.62.218.75's password:
Last failed login: Wed Sep 30 23:08:54 PDT 2020 from 222.186.30.76 on ssh:notty
There were 6 failed login attempts since the last successful login.
Last login: Wed Sep 30 23:08:10 2020 from 69.181.213.37
[root@fsm-super-532 ~]# phstatus.py
System uptime: 23:09:35 up 5 min, 1 user, load average: 0.23, 0.81, 0.47
Tasks: 27 total, 0 running, 26 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 0.4%us, 0.6%sy, 0.0%ni, 98.9%id, 0.0%wa, 0.1%hi, 0.0%si, 0.0%st
Mem: 32769032k total, 9756828k used, 23012204k free, 10972k buffers
Swap: 26058744k total, 0k used, 26058744k free, 2471156k cached

```

PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM
phParser	03:19	0	2186m	591m
phQueryMaster	03:36	0	955m	74m
phRuleMaster	03:36	0	1106m	530m
phRuleWorker	03:36	0	1366m	292m
phQueryWorker	03:36	0	1377m	286m
phDataManager	03:36	0	1233m	91m
phDiscover	03:36	0	508m	52m
phReportWorker	03:36	0	1428m	287m
phReportMaster	03:36	0	558m	58m
phIpIdentityWorker	03:36	0	1030m	57m
phIpIdentityMaster	03:36	0	492m	41m
phAgentManager	03:36	0	1420m	52m
phCheckpoint	03:36	0	315m	33m
phPerfMonitor	03:36	0	810m	70m
phReportLoader	03:36	0	772m	288m
phBeaconEventPackager	03:36	0	1129m	65m
phDataPurger	03:36	0	583m	60m
phEventForwarder	03:36	0	549m	46m
phMonitor	03:40	0	1306m	614m
Apache	05:30	0	311m	15m
Node.js-charting	05:23	0	914m	84m
Node.js-pm2	05:20	0	0	7932
AppSvr	05:17	0	10992m	2679m
DBSvr	05:29	0	326m	31m
phAnomaly	03:38	0	983m	64m
phFortiInsightAI	05:30	0	13788m	324m
Redis	05:23	0	57m	23m

```

[root@fsm-super-532 ~]#

```

- h. Remove the restored settings directories because you no longer need them, for example:

```

# rm -rf /restore-53x-settings
# rm -rf /svn/53x-settings
# rm -f /images

```

Migrate Cluster Installation

This section provides instructions on how to migrate Supervisor, Workers, and Collectors separately in a cluster environment,

- [Delete Workers](#)
- [Migrate Supervisor](#)
- [Install New Worker\(s\)](#)
- [Register Workers](#)
- [Set Up Collector-to-Worker Communication](#)
- [Working with Pre-6.1.0 Collectors](#)
- [Install 6.1.1 Collectors](#)
- [Register 6.1.1 Collectors](#)

Delete Workers

1. Login to the Supervisor.
2. Go to **Admin > License > Nodes** and delete the Workers one-by-one.
3. Go to the **Admin > Cloud Health** page and make sure that the Workers are not present.
Note that the Collectors will buffer events while the Workers are down.
4. Shutdown the Workers.
SSH to the Workers one-by-one and shutdown the Workers.

Migrate Supervisor

Follow the steps in [Migrate All-in-one Installation](#) to migrate the supervisor node. **Note:** FortiSIEM 6.1 does not support Worker or Collector migration.

Install New Worker(s)

Follow the steps in [Cluster Installation > Install Workers](#) to install new Workers. You can either keep the same IP address or change the address.

Register Workers

Follow the steps in [Cluster Installation > Register Workers](#) to register the newly created 6.1.1 Workers to the 6.1.1 Supervisor. The 6.1.1 FortiSIEM Cluster is now ready.

Set Up Collector-to-Worker Communication

1. Go to **Admin > Systems > Settings**.
2. Add the Workers to the Event Worker or Query Worker as appropriate.
3. Click **Save**.

Working with Pre-6.1.0 Collectors

Pre-6.1.0 Collectors and agents will work with 6.1.1 Supervisor and Workers. You can install 6.1.1 collectors at your convenience.

Install 6.1.1 Collectors

FortiSIEM does not support Collector migration to 6.1.1. You can install new 6.1.1 Collectors and register them to 6.1.1 Supervisor in a specific way so that existing jobs assigned to Collectors and Windows agent associations are not lost. Follow these steps:

1. Copy the http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector.
2. Disconnect the pre-6.1.1 Collector.
3. Install the 6.1.1 Collector with the old IP address by the following the steps in [Cluster Installation > Install Collectors](#).
4. Copy the saved http hashed password file (`/etc/httpd/accounts/passwds`) from the old Collector to the 6.1.1 Collector. This step is needed for Agents to work seamlessly with 6.1.1 Collectors. The reason for this step is that when the Agent registers, a password for Agent-to-Collector communication is created and the hashed version is stored in the Collector. During 6.1.1 migration, this password is lost.

Register 6.1.1 Collectors

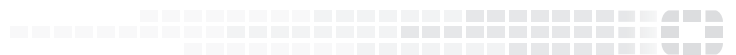
Follow the steps in [Cluster Installation > Register Collectors](#), with the following difference: in the `phProvisionCollector` command, use the `--update` option instead of `--add`. Other than this, use the exactly the same parameters that were used to register the pre-6.1.1 Collector. Specifically, use this form of the

`phProvisionCollector` command to register a 6.1.1 Collector and keep the old associations:

```
# /opt/phoenix/bin/phProvisionCollector --update <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.

Re-install new Windows Agents with the old `InstallSettings.xml` file. Both the migrated and the new agents will work. The new Linux Agent and migrated Linux Agent will also work.



Copyright© 2023 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.