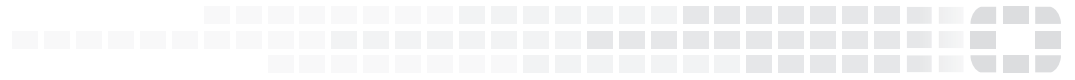


FORTINET®



FortiÜÖT ÁQ•cæ|æā } ÁBÁM] * !æå^ÁÕ˘ ãå^
VERSION 4.10.0

FORTINET DOCUMENT LIBRARY

<http://docs.fortinet.com>

FORTINET VIDEO GUIDE

<http://video.fortinet.com>

FORTINET BLOG

<https://blog.fortinet.com>

CUSTOMER SERVICE & SUPPORT

<https://support.fortinet.com>

<http://cookbook.fortinet.com/how-to-work-with-fortinet-support/>

FORTIGATE COOKBOOK

<http://cookbook.fortinet.com>

FORTINET TRAINING SERVICES

<http://www.fortinet.com/training>

FORTIGUARD CENTER

<http://www.fortiguard.com>

FORTICAST

<http://forticast.fortinet.com>

END USER LICENSE AGREEMENT

<http://www.fortinet.com/doc/legal/EULA.pdf>

FEEDBACK

Email: techdocs@fortinet.com



© 2017

FortiSIEM 4.10.0 Installation and Upgrade Guide

Revision 2

TABLE OF CONTENTS

Change Log	5
Installing FortiSIEM	6
System Performance Estimates and Recommendations for Large Scale Deployments.....	8
Browser Support and Hardware Requirements.....	11
Information Prerequisites for All FortiSIEM Installations.....	15
Hypervisor Installations.....	16
Installing in Amazon Web Services (AWS).....	17
Installing in Linux KVM.....	27
Installing in Microsoft Hyper-V.....	31
Installing in VMware ESX.....	33
ISO-Installation.....	42
Installing a Collector on Bare Metal Hardware.....	42
General Installation.....	44
Configuring Worker Settings.....	44
Registering the Supervisor.....	44
Registering the Worker.....	44
Registering the Collector to the Supervisor.....	45
Using NFS Storage with FortiSIEM.....	47
Configuring NFS Storage for VMware ESX Server.....	47
Using NFS Storage with Amazon Web Services.....	49
Moving CMDB to a separate Database Host.....	54
Freshly Installed Supervisor.....	54
FortiSIEM Windows Agent and Agent Manager Install.....	57
FortiSIEM Windows Agent Pre-installation Notes.....	58
Installing FortiSIEM Windows Agent Manager.....	64
Installing FortiSIEM Windows Agent.....	67
Upgrading FortiSIEM	70
Upgrade notes.....	71
Upgrade process.....	74
Migrating from 3.7.x versions to 4.2.1.....	77
Migrating Before Upgrading to 4.3.x.....	77
Migrating VMware ESX-based Deployments.....	78
Migrating AWS EC2 Deployments.....	93
Migrating KVM-based deployments.....	105
Migrating Collectors.....	119
Migrating the SVN Repository to a Separate Partition on a Local Disk.....	120
Special pre-upgrade instruction for 4.3.3.....	121

Special pre-upgrade instruction for 4.6.1.....	122
Enabling TLS 1.2 Patch On Old Collectors.....	123
Upgrading to 4.6.3 for TLS 1.2.....	124
Setting Up the Image Server for Collector Upgrades.....	125
Upgrading a FortiSIEM Single Node Deployment.....	126
Upgrading a FortiSIEM Cluster Deployment.....	127
Overview.....	127
Upgrading Supervisors and Workers.....	127
Upgrading Collectors.....	128
Upgrading FortiSIEM Windows Agent and Agent Manager.....	129
Upgrade from V1.0 to V1.1.....	129
Upgrade from V1.1 to V2.0.....	129
Upgrading Windows Agent License.....	130
Uninstalling Agents.....	130
Automatic OS Upgrades during Reboot.....	132

Change Log

Date	Change Description
2017-10-18	Initial version of FortiSIEM 4.10.0 Installation and Upgrade Guide.
2017-10-31	Revision 2 with updated section: 'FortiSIEM Windows Agent Pre-installation Notes'.

Installing FortiSIEM

The topics in this section are intended to guide you through the basic process of setting up and configuring your FortiSIEM deployment. This includes downloading and installing the FortiSIEM OVA image, using your hypervisor virtual machine manager to configure the hardware settings for your FortiSIEM node, setting up basic configurations on your Supervisor node, and registering your Supervisor and other nodes. Setting up IT infrastructure monitoring, including device discovery, monitoring configuration, setting up business services, is covered in under the section **Configuring Your FortiSIEM Platform**.

- [What You Need to Know before You Begin Installation](#)
- [Basic Installation Process](#)

What You Need to Know before You Begin Installation

What Kind of Deployment Will You Set Up?

Before beginning installation you should have determined the exact deployment configuration you will follow, as described in the topics under Deployment Options in the User Guide. Note that many deployment options have particular hardware requirements. For example, if you intend to use an NFS server for a cluster deployment, or if you want to use Visual Analytics, you will need to make sure that you have the necessary hardware and network components in place. We strongly recommend that you read through all the installation topics for your deployment configuration before you begin.

Who Will Install and Configure FortiSIEM?

These topics assume that you have the basic system administration skills required to install FortiSIEM, and that you are already familiar with the use of hypervisors such as VMware ESX or, if you are setting up a Cloud deployment, that you are already familiar with Cloud environments such as Amazon Web Services.

What Information Do You Need to Get Started?

You will need to have administrator-level permissions on the host where you will download and install FortiSIEM, and you will also need to have username and password associated with your FortiSIEM license. If you intend to use NFS storage for event data, you will also need to have set up an NFS server prior to installation.

Basic Installation Process

The installation process for any FortiSIEM deployment consists of a few steps:

- Import the FortiSIEM virtual appliance into a hypervisor or Amazon Web Services environment
- Edit the virtual appliance hardware settings
- Start and configure the virtual appliance from the hypervisor console
- Register the virtual appliance

Topics in this section will take you through the specific installation and configuration instructions for the most popular hypervisors and deployment configurations.

- [System Performance Estimates and Recommendations for Large Scale Deployments](#)
- [Browser Support and Hardware Requirements](#)
- [Information Prerequisites for All FortiSIEM Installations](#)
- [Hypervisor Installations](#)
- [ISO Installation](#)
- [General Installation](#)
- [Using NFS Storage with FortiSIEM](#)
- [Moving CMDB to a separate Database Host](#)
- [FortiSIEM Windows Agent and Agent Manager Install](#)

System Performance Estimates and Recommendations for Large Scale Deployments

This topic includes estimates and recommendations for storage capacity, disk performance, and network throughput for optimum performance of FortiSIEM deployments processing over 10,000 EPS.

In general, event ingestion at high EPS requires lower storage IOPS than for queries simply because queries need to scan higher volumes of data that has accumulated over time. For example, at 20,000 EPS, you have 86,400 times more data in a day than in one second, so a query such as 'Top Event types by count for the past 1 day' will need to scan $20,000 \times 86,400 = \sim 1.72$ billion events. Therefore, it is important to size your FortiSIEM cluster to handle your query and report requirements first, which will also handle event ingestion very well. These are the top 3 things to do for acceptable FortiSIEM query performance:

1. Add more worker nodes, higher than what is required for event ingestion alone
2. 10Gbps network on NFS server is a must, and if feasible on Supervisor and Worker nodes as well
3. SSD Caching on NFS server - The size of the SSD should be as close to the size required to cache hot data. In typical customer scenarios, the last 1 month data can be considered hot data because monthly reports are quite commonly run.

Schedule frequently run reports into the dashboard

If you have frequently run ranking reports that have group-by criteria (as opposed to raw message based reports), you can add such reports into a custom dashboard so that FortiSIEM schedules to run these reports in inline mode. Such reports compute their results in streaming manner as event data is processed in real-time. Such reports do not put any burden on the storage IOPS because they read very little data from the EventDB. Note that raw message reports (no group-by) are always computed directly from EventDB

An example scenario is presented at the end of this guide.

System Performance Component	Estimates and Recommendations
Event Storage Capacity	Storage capacity estimates are based on an average event size of 64 compressed bytes x EPS (events per section). Browser Support and Hardware Requirements includes a table with storage capacity requirements for up to 10,000 EPS.
Root Disk IOPS	Standard hard disk IOPS
CMDB Disk IOPS	1000 IOPS or more. Lab testing for EC2 scalability used 2000 IOPS.
SVN Disk IOPS	1000 IOPS
EventDB IOPS for Event Ingestion	1000 IOPS for 100K EPS (minimum)

System Performance Component

Estimates and Recommendations

EventDB Read IOPS for Queries

As high as feasible to improve query performance (use SSD caching on NFS server when feasible). In EC2 scalability testing, 2000 read IOPS while ingesting 100K EPS using one supervisor and two workers produced these results:

Index Query – No filter, display COUNT(Matched Events), group-by event type for 24 hours

- Total Events processed = 2,594,816,711 (2.59 billion events)
- Average events per second scanned by Query (QEPS) = 1.02 million QEPS
- Average Query Runtime = 2543 seconds (~ 42 minutes)

Raw Event Log Query - Same as Index Query with filter Raw Event Log contains 'e'

- Total Events processed = 350,914,385 (350 million events)
- Average events per second scanned by Query (QEPS) = 179,909 EPS (179k QEPS)
- Average Query Runtime = 1950 seconds (~ 33 minutes)

Network Throughput

Recommend 10Gbps network between Supervisor, Workers, and NFS server.
Using VMXNet3 Adapter for VMware

To achieve the best network throughput in VMware environments, delete the E1000 network adapter and add one that uses VMXNet3 for the `eth0/eth1` network configuration.

VMXNet3 adapter supports 10Gbps networking between VMs on the same host as well as across hosts, though you must also have a 10Gbps physical network adapter to achieve that level of throughput across hosts. You may need to upgrade the virtual hardware version ([VMWare KB 1003746](#)) in order to have the ability to use VMXNet3. More details on different types of VMWare network adapters is available in [VMWare KB 1001805](#)

Achieving 10Gbps on AWS EC2

To achieve 10Gbps in the AWS EC2 environment, you will need to:

- Deploy FortiSIEM Super, Workers, and NFS server on `8xlarge` class of instances (for example, `c3.8xlarge`). Refer to [EC2 Instance Types](#) for available types, and look for instance types with `10 Gigabit` noted next to them.
- You will need to use the HVM image for both the FortiSIEM image and NFS server image that supports [enhanced networking](#).
- Supervisor, Workers, and NFS Server must be placed under the same [AWS EC2 placement group](#) within an AWS VPC.

System Performance Component	Estimates and Recommendations
Network Interfaces	FortiSIEM recommends the use of separate network interfaces for event ingestion/GUI access and storage data to NFS
Number of Workers	6000 EPS per worker for event ingestion. More worker nodes for query performance. See example below.

Example:

An MSP customer has 12,000 EPS across all their customers. Each event takes up 64 bytes on average in compressed form in the EventDB.

Storage and Query Performance Example

1 Year total events = $12000 * 86400 * 365 = 378.432$ billion events
 1 month total events = $12000 * 86400 * 365 = 31.536$ billion events

1 Year Storage for 12,000 EPS = $12000 * 86400 * 365 * 64$ bytes = 23TB
 1 month Storage = ~ 2TB (SSD cache on NFS)

Run time for 'Top Event types by count for last 1 month' (@ 1 million QEPS using 1 super + 2 workers) = 31536 seconds = 8.75 hours

Example run time for above query using 1 super + 20 workers = 1.25 hours*

* Assuming that read IOPS are not limited due to SSD cache for 1 month data

These calculations are just extrapolations based on a test on EC2. Actual results may vary from this because of differences in hardware, event data, types of queries. Therefore, it is recommended that customers do a pilot evaluation using production data either on-premise or on AWS before arriving at an exact number of worker nodes

Browser Support and Hardware Requirements

- Supported Operating Systems and Browsers
- Hardware Requirements for Supervisor and Worker Nodes
- Hardware Requirements for Collector Nodes
- Hardware Requirements for Report Server Nodes

Supported Operating Systems and Browsers

These are the browsers and operating systems that are supported for use with the FortiSIEM web client.

OS Supported	Browser Supported
Windows	Firefox, Chrome, Internet Explorer 11.x, Microsoft Edge
Mac OS X	Firefox, Chrome, Safari
Linux	Firefox, Chrome

Hardware Requirements for Supervisor and Worker Nodes

The FortiSIEM Virtual Appliance can be installed using either storage configured within the ESX server or NFS storage. See the topic [Configuring NFS Server](#) for more information on working with NFS storage.

Event Data Storage Requirements

The storage requirement shown in the **Event Data Storage** column is only for the `eventdb` data, but the `/data` partition also includes CMDB backups and queries. You should set the `/data` partition to a larger amount of storage to accommodate for this.

Encryption for Communication Between FortiSIEM Virtual Appliances

All communication between Collectors that are installed on-premises and FortiSIEM Supervisors and Workers is secured by TLS 1.2 encryption. Communications are managed by OpenSSL/Apache HTTP Server/mod_ssl on the Supervisor/Worker side, and libcurl, using the NSS library for SSL, on the Collector side. The FortiSIEM Supervisor/Workers use RSA certificate with 2048 bits as default.

You can control the exact ciphers used for communications between virtual appliances by editing the `SSLCipherSuite` section in the file `/etc/httpd/conf.d/ssl.conf` on FortiSIEM Supervisors and Workers. You can test the ciphersuite for your Super or worker using the following nmap command:

```
nmap --script ssl-cert,ssl-enum-ciphers -p 443 <super_or_worker_fqdn>
```

Calculating Events per Second (EPS) and Exceeding the License Limit

FortiSIEM calculates the EPS for your system using a counter that records the total number of received events in a three minute time interval. Every second, a thread wakes up and checks the counter value. If the counter is less than 110% of the license limit (using the calculation $1.1 \times \text{EPS License} \times 180$), then FortiSIEM will continue to collect events. If you exceed 110% of your licensed EPS, events are dropped for the remainder of the three minute window, and an email notification is triggered. At the end of the three minute window the counter resets and resumes receiving events.

Overall EPS	Quantity	Host SW	Processor	Memory	OS/App and CMDB Storage	Event Data Storage (1 year)
1,500	1	ESXi (4.0 or later preferred)	4 Core 3 GHz, 64 bit	16 GB; 24 GB (4.5.1+)	200GB (80GB OS/App, 60GB CMDB, 60GB SVN)	3 TB

Overall EPS	Quantity	Host SW	Processor	Memory	OS/App and CMDB Storage	Event Data Storage (1 year)
4,500	1	ESXi (4.0 or later preferred)	4 Core 3 GHz, 64 bit	16 GB; 24 GB (4.5.1+)	200GB (80GB OS/App, 60GB CMDB, 60GB SVN)	8 TB
7,500	1 Super; 1 Worker	ESXi (4.0 or later preferred)	Super: 8 Core 3 GHz, 64 bit; Worker: 4 Core 3 GHz, 64 bit	Super: 24 GB; Worker: 16 GB	Super: 200GB (80GB OS/App, 60GB CMDB, 60GB SVN); Worker: 200GB (80GB OS/App)	12 TB
10,000	1 Super; 1 Worker	ESXi (4.0 or later preferred)	Super: 8 Core 3 GHz, 64 bit; Worker: 4 Core 3 GHz, 64 bit	Super: 24 GB; Worker: 16 GB	Super: 200GB (80GB OS/App, 60GB CMDB, 60GB SVN); Worker: 200GB (80GB OS/App)	17 TB
20,000	1 Super; 3 Workers	ESXi (4.0 or later preferred)	Super: 8 Core 3 GHz, 64 bit; Worker: 4 Core 3 GHz, 64 bit	Super: 24 GB; Worker: 16 GB	Super: 200GB (80GB OS/App, 60GB CMDB, 60GB SVN); Worker: 200GB (80GB OS/App)	34 TB
30,000	1 Super; 5 Workers	ESXi (4.0 or later preferred)	Super: 8 Core 3 GHz, 64 bit; Worker: 4 Core 3 GHz, 64 bit	Super: 24 GB; Worker: 16 GB	Super: 200GB (80GB OS/App, 60GB CMDB, 60GB SVN); Worker: 200GB (80GB OS/App)	50 TB
Higher than 30,000	Consult FortiSIEM					

Hardware Requirements for Collector Nodes

Component	Quantity	Host SW	Processor	Memory	OS/App Storage
Collector	1	ESX	2 Core 2 GHz, 64 bit	4 GB	40 GB
Collector	1	Native Linux Suggested Platform: Dell PowerEdge R210 Rack Server	2 Core, 64 bit	4GB	40 GB

Hardware Requirements for Report Server Nodes

Component	Quantity	Host SW	Processor	Memory	OS/App Storage	Report Data Storage (1 year)
Report Server	1	ESX	8 Core 3 GHz, 64 bit	16 GB	200GB (80GB OS/App, 60GB CMDDB, 60GB SVN)	See recommendations under Hardware Requirements for Supervisor and Worker nodes.

Information Prerequisites for All FortiSIEM Installations

You should have this information ready before you begin installing the FortiSIEM virtual appliance on ESX:

1. The static IP address and subnet mask for your FortiSIEM virtual appliance.
2. The IP address of NFS mount point and NFS share name if using NFS storage. See the topics [Configuring NFS Storage for VMware ESX Server](#) and [Setting Up NFS Storage in AWS](#) for more information.
3. The FortiSIEM host name within your local DNS server.
4. The VMWare ESX datastore location where the virtual appliance image will be stored if using ESX storage.



Proxy Server Authentication Not Supported

Proxy server authentication is not supported in this version of FortiSIEM. Turn off proxy server authentication or completely disable the proxy for your virtual appliance host.

Hypervisor Installations

Topics in this section cover the instructions for importing the FortiSIEM disk image into specific hypervisors and configuring the FortiSIEM virtual appliance. See the topics under General Installation for information on installation tasks that are common to all hypervisors.

- [Installing in Amazon Web Services \(AWS\)](#)
- [Installing in Linux KVM](#)
- [Installing in Microsoft Hyper-V](#)
- [Installing in VMware ESX](#)

Installing in Amazon Web Services (AWS)

You Must Use an Amazon Virtual Public Cloud with FortiSIEM

You must set up a Virtual Public Cloud (VPC) in Amazon Web Services for FortiSIEM deployment rather than classic-EC2. FortiSIEM does not support installation in classic-EC2. See the [Amazon VPC documentation](#) for more information on setting up and configuring a VPC. See [Creating VPC-based Elastic IPs for Supervisor and Worker Nodes in AWS](#) for information on how to prevent the public IPs of your instances from changing when they are stopped and started.

Using NFS Storage with Amazon Web Services

If the aggregate EPS for your FortiSIEM installation requires a cluster (FortiSIEM virtual appliance + worker nodes), then you **must** set up an NFS server. If your storage requirements for the EventDB are more than 1TB, it is strongly recommended that you use an NFS server where you can configure LVM+RAID0. For more information, see [Setting Up NFS Storage in AWS](#).

Note: SVN password reset issue after system reboot for FortiSIEM 3.7.6 customers in AWS Virtual Private Cloud (VPC).

FortiSIEM uses SVN to store monitored device configurations. In AWS VPC setup, we have noticed that FortiSIEM SVN password gets changed if the system reboots - this prevents FortiSIEM from storing new configuration changes and viewing old configurations. The following procedure can be used to reset the SVN password to FortiSIEM factory default so that FortiSIEM can continue working correctly.

This script needs to be run only once.

1. Logon to Super.
2. Copy the attached "ao_svnpwd_reset.sh" script to Super on EC2+VPC deployment.
3. Stop all back-end processes before running script by issuing the following command: **phtools --stop all**.
4. Run following command to change script permissions: **"chmod +x ao_svnpwd_reset.sh"**.
5. Execute "ao_svnpwd_reset.sh" as root user: **"/ao_svnpwd_reset.sh"**. The system will reboot.
6. Check SVN access to make sure that old configurations can be viewed.

Determining the Storage Type for EventDB in AWS

If the aggregate EPS for your FortiSIEM installation requires a cluster (a virtual appliance + Worker nodes), then you must set up an NFS server as described in [Using NFS Storage with Amazon Web Services](#). If your storage requirement for EventDB is more than 1TB, it is recommended that you use an NFS server where you can configure LVM+RAID0, which is also described in those topics. Although it is possible to set up a similar LVM+RAID0 on the FortiSIEM virtual appliance itself, this has not been tested.

Here's an example of how to calculate storage requirements: At 5000 EPS, you can calculate daily storage requirements to be about 22-30GB (300k events take roughly 15-20MB on average in compressed format stored in eventDB). So, in order to have 6 months of data available for querying, you need to have 4 - 6TB of storage.

If you only need one FortiSIEM node and your storage requirements are lower than 1TB, and is not expected to ever grow beyond this limit, you can avoid setting up an NFS server and use a local EBS volume for EventDB. For this option, see the topic [Configuring Local Storage in AWS for EventDB](#).

Configuring Local Storage in AWS for EventDB

- Create the Local Storage Volume
- Attach the Local Storage Volume to the Supervisor

Create the Local Storage Volume

1. Log in to AWS.
2. In the E2 dashboard, click **Volumes**.
3. Click **Create Volume**.
4. Set **Size** to 100 GB to 1 TB (depending on storage requirement).
5. Select the same **Availability Zone** region as the FortiSIEM Supervisor instance.
6. Click **Create**.

Attach the Local Storage Volume to the Supervisor

1. In the EC2 dashboard, select the local storage volume.
2. In the Actions menu, select **Attach Volume**.
3. For **Instance**, enter the Supervisor ID.
4. For **Device**, enter `/dev/xvdi`.
5. Click **Attach**.

Setting Up Supervisor, Worker and Collector Nodes in AWS

The basic process for installing FortiSIEM Supervisor, Worker, or Collector node is the same. Since Worker nodes are only used in deployments that use NFS storage, you should first configure your Supervisor node to use NFS storage, and then configure your Worker node using the Supervisor NFS mount point as the mount point for the Worker. See [Configuring NFS Storage for VMware ESX Server](#) for more information. Collector nodes are only used in multi-tenant deployments, and need to be registered with a running Supervisor node.

- [Setting Up AWS Instances](#)
- [Creating VPC-based Elastic IPs for Supervisor and Worker Nodes in AWS](#)
- [Configuring the Supervisor and Worker Nodes in AWS](#)
- [Registering the Collector to the Supervisor in AWS](#)

When you're finished with the specific hypervisor setup process, you need to complete your installation by following the steps described under [General Installation](#).

You Must Use an Amazon Virtual Public Cloud with FortiSIEM

You must set up a Virtual Public Cloud (VPC) in Amazon Web Services for FortiSIEM deployment rather than classic-EC2. FortiSIEM does not support installation in classic-EC2. See the [Amazon VPC documentation](#) for more information on setting up and configuring a VPC. See [Creating VPC-based Elastic IPs for Supervisor and Worker Nodes in AWS](#) for information on how to prevent the public IPs of your instances from changing when they are stopped and started.

Using NFS Storage with Amazon Web Services

If the aggregate EPS for your FortiSIEM installation requires a cluster (FortiSIEM virtual appliance + worker nodes), then you **must** set up an NFS server. If your storage requirements for the EventDB are more than 1TB, it is strongly recommended that you use an NFS server where you can configure LVM+RAID0. For more information, see [Setting Up NFS Storage in AWS](#).

Setting Up AWS Instances

You Must Use an Amazon Virtual Public Cloud with FortiSIEM

You must set up a Virtual Public Cloud (VPC) in Amazon Web Services for FortiSIEM deployment rather than classic-EC2. FortiSIEM does not support installation in classic-EC2. See the [Amazon VPC documentation](#) for more information on setting up and configuring a VPC. See [Creating VPC-based Elastic IPs for Supervisor and Worker Nodes in AWS](#) for information on how to prevent the public IPs of your instances from changing when they are stopped and started.

Using NFS Storage with Amazon Web Services

If the aggregate EPS for your FortiSIEM installation requires a cluster (FortiSIEM virtual appliance + worker nodes), then you **must** set up an NFS server. If your storage requirements for the EventDB are more than 1TB, it is strongly recommended that you use an NFS server where you can configure LVM+RAID0. For more information, see [Setting Up NFS Storage in AWS](#).

1. Log in to your AWS account and navigate to the EC2 dashboard.
2. Click **Launch Instance**.
3. Click **Community AMIs** and search for the AMI ID associated with your version of FortiSIEM. The latest AMI IDs are on the image server where you download the other hypervisor images.
4. Click **Select**.
5. Click **Compute Optimized**.

Using C3 Instances

You should select one of the C3 instances with a Network Performance rating of High, or 10Gb performance. The current generation of C3 instances run on the latest Intel Xeons that AWS provides. If you are running these machines in production, it is significantly cheaper to use **EC2 Reserved Instances** (1 or 3 year) as opposed to on-demand instances.

6. Click **Next: Configure Instance Details**.
7. Review these configuration options:

Network and Subnet	Select the VPC you set up for your instance.
Number of Instances	For enterprise deployments, set to 1 . For a configuration of 1 Supervisor + 2 Workers, set to 3 . You can also add instances later to meet your needs.
Public IP	Clear the option Automatically assign a public IP address to your instances if you want to use VPN.
Placement Group	A placement group is a logical grouping for your cluster instances. Placement groups have low latency, full-bisection 10Gbps bandwidth between instances. Select an existing group or create a new one.

EBS Optimized Instance

An EBS optimized instance enables dedicated throughput between Amazon EBS and Amazon EC2, providing improved performance for your EBS volumes. Note that if you select this option, additional Amazon charges may apply.

8. Click **Next: Add Storage**.
9. For **Size**, **Volume Type**, and **IOPS**, set options for your configuration.

Storage Configuration Options

In a configuration with three instances for 1 Supervisor + 2 Workers, **Volume Type** should be set to **Provisioned IOPS**, even though only the Supervisor node's CMDB data needs higher IOPS. For Workers, **Standard IOPS** is enough. You can also launch with Standard IOPS, and then add a separate EBS volume for CMDB separately with the higher Provisioned IOPS.

If you are using local storage for EventDB, click **Add New Volume** to create a new EBS volume, and set these options:

Device	/dev/xvdi
Size	50GB to 1TB, depending on storage requirement
Volume Type	Provisioned IOPS
IOPS	2000

10. Click **Next: Tag Instance**.
11. Under **Value**, enter the **Name** you want to assign to all the instances you will launch, and then click **Create Tag**. After you complete the launch process, you will have to rename each instance to correspond to its role in your configuration, such as Supervisor, Worker1, Worker2.
12. Click **Next: Configure Security Group**.
13. Select **Select an Existing Security Group**, and then select the default security group for your VPC. FortiSIEM needs access to HTTPS over port 443 for GUI and API access, and access to SSH over port 22 for remote management, which are set in the default security group. This group will allow traffic between all instances within the VPC.

Limiting IP Access

Make sure you have limited the IP addresses that can access your VPC, or that you have set up VPN access to it. VPN will block all inbound Internet traffic.

14. Click **Review and Launch**.
15. Review all your instance configuration information, and then click **Launch**.
16. Select an existing or create a new **Key Pair** to connect to these instances via SSH. If you use an existing key pair, make sure you have access to it. If you are creating a new key pair, download the private key and store it in a secure location accessible from the machine from where you usually connect to these AWS instances.
17. Click **Launch Instances**.

18. When the EC2 Dashboard reloads, check that all your instances are up and running.
19. All your instances will be tagged with the **Name** you assigned in Step 11, select an instance to rename it according to its role in your deployment.
20. For all types of instances, follow the instructions to SSH into the instances as described in [Configuring the Supervisor and Worker Nodes in AWS](#), and then run the script `phstatus.sh` to check the health of the instances.

Creating VPC-based Elastic IPs for Supervisor and Worker Nodes in AWS

You need to create VPC-based Elastic IPs and attach them to your nodes so the public IPs don't change when you stop and start instances.

1. Log in to the [Amazon VPC Console](#).
2. In the navigation pane, click **Elastic IPs**.
3. Click **Allocate New Address**.
4. In the Allocate New Address dialog box, in the **Network platform** list, select **EC2-VPC**, and then click **Yes, Allocate**.
5. Select the Elastic IP address from the list, and then click **Associate Address**.
6. In the Associate Address dialog box, select the network interface for the NAT instance. Select the address to associate the EIP with from the Private IP address list, and then click **Yes, Associate**.

Configuring the Supervisor and Worker Nodes in AWS

1. From the EC2 dashboard, select the instance, and then click **Connect**.
2. Select **Connect with a standalone SSH client**, and follow the instructions for connecting with an SSH client. For the connection command, follow the example provided in the connection dialog, but substitute the FortiSIEM root user name for `ec2-user@xxxxxx`. The `ec2-user` .name is used only for Amazon Linux NFS server.
3. SSH to the Supervisor.
4. Run `cd /opt/phoenix/deployment/jumpbox/aws`.
5. Run the script `pre-deployment.sh` to configure host name and NFS mount point.
6. Accept the License Agreements.
7. Enter the **Host Name**.

Finding the Host Name

You can find the host name on the EC2 dashboard. Select the instance, right click, and then select **Connect with a standalone SSH client**. The host name will be listed under **Public DNS**.

8. Enter the **Mount Point** for your storage configuration.

NFS Storage	<NFS Server IP>:/data For <NFS Server IP>, use the 10.0.0.X IP address of the NFS Server running within the VPC
Local Storage	/dev/xvdi

9. The system will reboot.
10. Log in to the Supervisor.
11. Register the Supervisor by following steps [here](#).
12. Run `cd /opt/phoenix/deployment/jumpbox/aws`.
13. Run the script `deployment.sh` (now includes running `post-deployment.sh` automatically). The system will reboot and is now ready.
14. To install a worker node, follow steps 1-9 and the worker is ready
15. To add a Worker to the cluster (assume Worker is already installed)
 1. Log in to the FortiSIEM GUI
 2. Go to **Admin > License Management > VA Information**
 3. Click **Add**
 4. Enter the private address of the Worker Node

Registering the Collector to the Supervisor in AWS

1. Locate a Windows machine on AWS.
2. Open a Remote desktop session from your PC to that Windows machine on AWS.
3. Within the remote desktop session, launch a browser and navigate to `https://<Collector-IP>:5480`
4. Enter the Collector setup information.

Name	Collector Name
User ID	Admin User
Password	Admin Password
Cust/Org ID	Organization Name
Cloud URL	Supervisor URL

5. Click **Save**.
The Collector will restart automatically after registration succeeds.

Installing in Linux KVM

The basic process for installing FortiSIEM Supervisor, Worker, or Collector node in Linux KVM is the same as installing these nodes under VMware ESX, and so you should follow the instructions in [Installing a Supervisor, Worker, or Collector Node in ESX](#). Since Worker nodes are only used in deployments that use NFS storage, you should first configure your Supervisor node to use NFS storage, and then configure your Worker node using the Supervisor NFS mount point as the mount point for the Worker. Collector nodes are only used in Service Provider deployments, and need to be registered with a running Supervisor node.

- [Setting up a Network Bridge for Installing FortiSIEM in KVM](#)
- [Importing the Supervisor, Collector, or Worker Image into KVM](#)
- [Configuring Supervisor Hardware Settings in KVM](#)

Setting up a Network Bridge for Installing FortiSIEM in KVM

If FortiSIEM is the first guest on KVM, then a bridge network may be required to enable network connectivity. For details see [the KVM documentation provided by IBM](#).

In these instructions, `br0` is the initial bridge network, `em1` is connected as a management network, and `em4` is connected to your local area network.

1. In the KVM host, go to the directory `/etc/sysconfig/network-scripts/`.
2. Create a bridge network config file `ifcfg-br0`.

```
DEVICE=br0
BOOTPROTO=none
NM_CONTROLLED=yes
ONBOOT=yes
TYPE=Bridge
NAME="System br0"
```

3. Edit network config file `ifcfg-em4`.

```
DEVICE=em4 BOOTPROTO=sharedNM_
CONTROLLED=noONBOOT=yesTYPE=EthernetUUID="24078f8d-67f1-41d5-
8eea-xxxxxxxxxxxx"IPV6INIT=noUSERCTL=noDEFROUTE=yesIPV4_
FAILURE_FATAL=yesNAME="System
em4"HWADDR=F0:4D:00:00:00:00BRIDGE=br0
```

4. Restart the network service.

Importing the Supervisor, Collector, or Worker Image into KVM

1. Download and uncompress the FortiSIEM OVA package from the FortiSIEM image server to the location where you want to install the image.
2. Start the KVM Virtual Machine Manager.
3. Select and right-click on a host to open the **Host Options** menu, and then select **New**.
4. In the **New VM** dialog, enter a **Name** for your FortiSIEM node.
5. Select **Import existing disk image**, and then click **Forward**.
6. **Browse** to the location of OVA package and select it.
7. Choose the **OS Type** and **Version** you want to use with this installation, and then click **Forward**.
8. Allocate **Memory** and **CPUs** to the FortiSIEM node as recommended in the topic [Browser Support and Hardware Requirements](#), and then click **Forward**.
9. Confirm the installation configuration of your node, and then click **Finish**.

Configuring Supervisor Hardware Settings in KVM

1. In KVM Virtual Machine Manager, select the FortiSIEM Supervisor, and then click **Open**.
2. Click the **Information** icon to view the Supervisor hardware settings.
3. Select the **Virtual Network Interface**.
4. For **Source Device**, select an available bridge network.
See [Setting up a Network Bridge for Installing FortiSIEM in KVM](#) for more information.
5. For **Device model**, select **Hypervisor default**, and then click **Apply**.
6. In the Supervisor **Hardware** settings, select **Virtual Disk**.
7. In the **Virtual Disk** dialog, open the **Advanced options**, and for **Disk bus**, select **IDE**.
8. Click **Add Hardware**, and then select **Storage**.
9. Select the **Select managed or other existing storage** option, and then browse to the location for your storage. You will want to set up a disk for both CMDDB (60GB) and SVN (60GB). If you are setting up FortiSIEM Enterprise, you may also want to create a storage disk for EventDB, with **Storage format** set to **Raw**.
10. In the KVM Virtual Machine Manager, connect to the FortiSIEM Supervisor and power it on.
11. Follow the instructions in [Configuring the Supervisor, Worker, or Collector from the VM Console](#) to complete the installation.

Related Links

- [Configuring the Supervisor, Worker, or Collector from the VM Console](#)

Installing in Microsoft Hyper-V

This topic describes how to install FortiSIEM on a Microsoft Hyper-V virtual server.

- [Importing a Supervisor, Collector, or Worker Image into Microsoft Hyper-V](#)

Supported Versions

FortiSIEM has been tested to run on Hyper-V on Microsoft Windows 2012.

Importing a Supervisor, Collector, or Worker Image into Microsoft Hyper-V

Using Local or NFS Storage for EventDB in Hyper-V

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

If you are going to use NFS storage for EventDB, follow the instructions in the topic [Configuring NFS Storage for VMware ESX Server](#).

Disk Formats for Data Storage

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

1. Download and uncompress the FortiSIEM.7z package (using the [7-Zip](#) tool) from FortiSIEM image server to the location where you want to install the image.
2. Start Hyper-V Manager.
3. In the **Action** menu, select **Import Virtual Machine**.
The **Import Virtual Machine Wizard** will launch.
4. Click **Next**.
5. Browse to the folder containing Hyper-V VM, and then click **Next**.
6. Select the FortiSIEM image, and then click **Next**.
7. For **Import Type**, select **Copy the virtual machine**, and then click **Next**.
8. Select the storage folders for your virtual machine files, and then click **Next**.
9. Select the storage folder for your virtual machine's hard disks, and then click **Next**.
10. Verify the installation configuration, and then click **Finish**.
11. In Hyper-V Manager, connect to the FortiSIEM virtual appliance and power it on.
12. Follow the instructions in [Configuring the Supervisor, Worker, or Collector from the VM Console](#) to complete the installation.

Related Links

- [Configuring the Supervisor, Worker, or Collector from the VM Console](#)

Installing in VMware ESX

- Setting the Network Time Protocol (NTP) for ESX
- Installing a Supervisor, Worker, or Collector Node in ESX
- Configuring the Supervisor, Worker, or Collector from the VM Console

Setting the Network Time Protocol (NTP) for ESX

It's important that your Virtual Appliance has the accurate time in order to correlate events from multiple devices within the environment.

1. Log in to your VMWare ESX server.
2. Select your ESX host server.
3. Click the **Configuration** tab.
4. Under **Software** , select **Time Configuration** .
5. Click **Properties**.
6. Select **NTP Client Enabled**.
7. Click **Options**.
8. Under **General** , select **Start automatically**.
9. Under **NTP Setting** , click **Add...**
10. Enter the IP address of the NTP servers to use.

Publicly Accessible NTP Server: If you don't have an internal NTP server, you can access a publicly available one at <http://tf.nist.gov/tf-cgi/servers.cgi>

11. Click **Restart NTP service**.
12. Click **OK** to apply the changes.

Installing a Supervisor, Worker, or Collector Node in ESX

The basic process for installing FortiSIEM Supervisor, Worker, or Collector node is the same. Since Worker nodes are only used in deployments that use NFS storage, you should first configure your Supervisor node to use NFS storage, and then configure your Worker node using the Supervisor NFS mount point as the mount point for the Worker. See [Configuring NFS Storage for VMware ESX Server](#) for more information. Collector nodes are only used in Service Provider deployments, and need to be registered with a running Supervisor node.

- [Importing the Supervisor, Collector, or Worker Image into the ESX Server](#)
- [Editing the Supervisor, Collector, or Worker Hardware Settings](#)
- [Setting Local Storage for the Supervisor](#)
- [Troubleshooting Tips for Supervisor Installations](#)

When you're finished with the specific hypervisor setup process, you need to complete your installation by following the steps described under [General Installation](#).

Importing the Supervisor, Collector, or Worker Image into the ESX Server

1. Download and uncompress the FortiSIEM OVA package from the FortiSIEM image server to the location where you want to install the image.
2. Log in to the VMware vSphere Client.
3. In the **File** menu, select **Deploy OVF Template**.
4. **Browse** to the `.ova` file (example: `FortiSIEM-VA-4.3.1.1145.ova`) and select it. On the **OVF Details** page you will see the product and file size information.
5. Click **Next**.
6. Click **Accept** to accept the "End User Licensing Agreement," and then click **Next**.
7. Enter a **Name** for the Supervisor or Worker, and then click **Next**.
8. Select a **Storage** location for the installed file, and then click **Next**.
9. Select a **Disk Format**, and then click **Next**.
Disk Format Recommendation: FortiSIEM recommends using Thick Provision Lazy Zeroed.
10. Review the **Deployment Settings**, and then click **Finish**.
Do not turn off or reboot the system. Deployment will complete in 7 to 10 minutes. Do not turn off or reboot the system during this time.
11. When the deployment completes, click **Close**.
Running on VMWare ESX 6.0: If you are importing FortiSIEM VA, Collector, or Report Server images for VMWare on an ESXi 6.0 host, you will need to also "Upgrade VM Compatibility" to ESXi 6.0. If the VM is already started, you need to shutdown the VM, and use the "Actions" menu to do this. Due to some incompatibility created by VMWare, our collector VM processes restarted and the collector could not register with the supervisor. Similar problems are also likely to occur on supervisor, worker, or report server as well, so make sure their VM compatibilities are upgraded as well. More information about VM compatibility is available in the VMWare KB below:

<https://kb.vmware.com/kb/1010675>

Editing the Supervisor, Collector, or Worker Hardware Settings

Before you start the Supervisor, Worker, or Collector for the first time you need to make some changes to its hardware settings.

1. In the VMware vSphere client, select the imported Supervisor, Worker, or Collector.
2. Right-click on the node to open the **Virtual Appliance Options** menu, and then select **Edit Settings...**
3. Select the **Hardware** tab, and check that **Memory** is set to at least **16 GB** and **CPUs** is set to **8**.

Memory Allocation for Large Deployments

For large deployments you should allocate at least 24GB of memory. See the topic [Hardware Requirements](#) for more information.

Setting Local Storage for the Supervisor

Using NFS Storage

You can install the Supervisor using either native ESX storage or NFS storage. These instructions are for creating native EXS storage. See [Configuring NFS Storage for VMware ESX Server](#) for more information. If you are using NFS storage, you will set the IP address of the NFS server during Step 15 of the **Configuring the Supervisor, Worker, or Collector from the VM Console** process.

1. On **Hardware** tab, click **Add**.
2. In the **Add Hardware** dialog, select **Hard Disk**, and then click **Next**.
3. Select **Create a new virtual disk**, and then click **Next**.
4. Check that these selections are made in the **Create a Disk** dialog:

Disk Size	300GB See the Hardware Requirements for Supervisor and Worker Nodes in the Browser Support and Hardware Requirements topic for more specific disk size recommendations based on Overall EPS .
Disk Provisioning	Thick Provision Lazy Zeroed
Location	Store to the Virtual Machine

5. In the **Advanced Options** dialog, make sure that the **Independent** option for **Mode** is not selected.
6. Check all the options for creating the virtual disk, and then click **Finish**.
7. In the **Virtual Machine Properties** dialog, click **OK**.
The **Reconfigure virtual machine** task will launch.

Troubleshooting Tips for Supervisor Installations

- Check the Supervisor System and Directory Level Permissions
- Check Backend System Health

Check the Supervisor System and Directory Level Permissions

Use SSH to connect to the Supervisor and check that the `cmdb`, `data`, `query`, `querywkr`, and `svn` permissions match those in this table:

```
[root@super ~]# ls -l /
dr-xr-xr-x.  2 root    root    4096 Oct 15 11:09 bin
dr-xr-xr-x.  5 root    root    1024 Oct 15 14:50 boot
drwxr-xr-x   4 postgres postgres 4096 Nov 10 18:59 cmdb
drwxr-xr-x   9 admin    admin   4096 Nov 11 11:32 data
drwxr-xr-x  15 root    root    3560 Nov 10 11:11 dev
-rw-r--r--   1 root    root     34 Nov 11 12:09 dump.rdb
drwxr-xr-x. 93 root    root   12288 Nov 11 12:12 etc
drwxr-xr-x.  4 root    root    4096 Nov 10 11:08 home
dr-xr-xr-x. 11 root    root    4096 Oct 15 11:13 lib
dr-xr-xr-x.  9 root    root   12288 Nov 10 19:13 lib64
drwx-----  2 root    root   16384 Oct 15 14:46 lost+found
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 media
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 mnt
drwxr-xr-x. 10 root    root    4096 Nov 10 09:37 opt
drwxr-xr-x.  2 root    root    4096 Nov 10 11:10 pbin
dr-xr-xr-x 289 root    root     0 Nov 10 11:13 proc
drwxr-xr-x.  8 admin    admin   4096 Nov 11 00:37 query
drwxr-xr-x.  8 admin    admin   4096 Nov 10 18:58 querywkr
dr-xr-x---.  7 root    root    4096 Nov 10 19:13 root
dr-xr-xr-x.  2 root    root   12288 Oct 15 11:08 sbin
drwxr-xr-x.  2 root    root    4096 Oct 15 14:47 selinux
drwxr-xr-x.  2 root    root    4096 Sep 23  2011 srv
drwxr-xr-x.  4 apache  apache  4096 Nov 10 18:58 svn
drwxr-xr-x. 13 root    root     0 Nov 10 11:13 sys
drwxrwxrwt.  9 root    root    4096 Nov 11 12:12 tmp
drwxr-xr-x. 15 root    root    4096 Oct 15 14:58 usr
drwxr-xr-x. 21 root    root    4096 Oct 15 11:01 var
```

Check that the `/data`, `/cmdb`, and `/svn` directory level permissions match those in this table:

```
[root@super ~]# ls -l /data
drwxr-xr-x 3 root    root    4096 Nov 11 02:52 archive
drwxr-xr-x 3 admin  admin  4096 Nov 11 12:01 cache
drwxr-xr-x 2 postgres postgres 4096 Nov 10 18:46 cmdb
drwxr-xr-x 2 admin  admin  4096 Nov 10 19:04 custParser
drwxr-xr-x 5 admin  admin  4096 Nov 11 00:29 eventdb
drwxr-xr-x 2 admin  admin  4096 Nov 10 19:04 jmxXml
drwxr-xr-x 2 admin  admin  4096 Nov 11 11:33 mibXml
[root@super ~]# ls -l /cmdb
drwx----- 14 postgres postgres 4096 Nov 10 11:08 data
[root@super ~]# ls -l /svn
drwxr-xr-x 6 apache apache 4096 Nov 10 18:58 repos
```

Check Backend System Health

Use SSH to connect to the supervisor and run `phstatus` to see if the system status metrics match those in this table:

```
[root@super ~]# phstatus
Every 1.0s: /opt/phoenix/bin/phstatus.py
System uptime: 12:37:58 up 17:24, 1 user, load average: 0.06, 0.01, 0.00
Tasks: 20 total, 0 running, 20 sleeping, 0 stopped, 0 zombie
Cpu(s): 8 cores, 0.6%us, 0.7%sy, 0.0%ni, 98.6%id, 0.0%wa, 0.0%hi, 0.1%si, 0.0%st
Mem: 16333720k total, 5466488k used, 10867232k free, 139660k buffers
Swap: 6291448k total, 0k used, 6291448k free, 1528488k cached
```

PROCESS	UPTIME	CPU%	VIRT_MEM	RES_MEM
phParser	12:00:34	0	1788m	280m
phQueryMaster	12:00:34	0	944m	63m
phRuleMaster	12:00:34	0	596m	85m
phRuleWorker	12:00:34	0	1256m	252m
phQueryWorker	12:00:34	0	1273m	246m
phDataManager	12:00:34	0	1505m	303m
phDiscover	12:00:34	0	383m	32m
phReportWorker	12:00:34	0	1322m	88m
phReportMaster	12:00:34	0	435m	38m
phIpIdentityWorker	12:00:34	0	907m	47m
phIpIdentityMaster	12:00:34	0	373m	26m
phAgentManager	12:00:34	0	881m	200m
phCheckpoint	12:00:34	0	98m	23m
phPerfMonitor	12:00:34	0	700m	40m
phReportLoader	12:00:34	0	630m	233m
phMonitor	31:21	0	1120m	25m
Apache	17:23:23	0	260m	11m
Node.js	17:20:54	0	656m	35m
AppSvr	17:23:16	0	8183m	1344m
DBSvr	17:23:34	0	448m	17m

Configuring the Supervisor, Worker, or Collector from the VM Console

Do Not Press Control Keys: Do not press any control keys (for example **Control-C** or **Control-Z**) while configuring the virtual appliances in the VMware console, as this might cause the installation process to stop. If this happens you must erase the virtual appliance and start the installation process again.

1. In the VMware vSphere client, select the Supervisor, Worker, or Collector virtual appliance
2. Right-click to open the **Virtual Appliance Options** menu, and then select **Power > Power On**.
3. In the **Virtual Appliance Options** menu, select **Open Console**
Network Failure Message: When the console starts up for the first time you may see a Network eth0 Failed message, but this is expected behavior.
4. In VM console, select **Set Timezone** and then press **Enter**.
5. Select your **Location**, and then press **Enter**.
6. Select your **Country**, and then press **Enter**.
7. Select your **Timezone**, and then press **Enter**.
8. Review your Timezone information, select **1**, and then press **Enter**.
9. When the **Configuration** screen reloads, select **Login**, and then press **Enter**.
10. Enter the default login credentials

Login	root
Password	ProspectHills

11. Run the `vami_config_net` script to configure the network. `/opt/vmware/share/vami/vami_config_net`
12. When prompted, enter the information for these network components to configure the Static IP address: **IP Address, Netmask, Gateway, DNS Server(s)**.
Authenticated Proxy Server Not Supported: The authenticated proxy server is not supported in this version of FortiSIEM. Turn off proxy server authentication or completely disable the proxy for the ESX host.
13. Press **Y** to accept the network configuration settings.
14. Enter the **Host name**, and then press **Enter**.
15. For the Supervisor, set either the Local or NFS storage mount point.
16. For a Worker, use the same IP address of the NFS server you set for the Supervisor.

Supervisor Local storage	<code>/dev/sdd</code>
NFS storage	<code><NFS_Server_IP_Address>:/<Directory_Path></code>

After you set the mount point, the Supervisor will automatically reboot, and in 15 to 25 minutes the Supervisor will be successfully configured.

ISO-Installation

This topic covers installation of FortiSIEM from an ISO under a native file system such as Linux, also known as installing "on bare metal."

- [Installing a Collector on Bare metal](#)

Installing a Collector on Bare Metal Hardware

You can install Collectors on bare metal hardware (without a Hypervisor layer). Be sure to read the section on **Hardware Requirements for Collectors** in [Browser Support and Hardware Requirements](#) before starting the installation process.

1. Download the Linux collector ISO image from:
<https://images-cdn.fortisiem.fortinet.com/VirtualAppliances/latestrelease.html>
2. Burn the ISO to a DVD so that you can boot from it to begin the setup.
3. Before you begin the installation, make sure the host where you want to install the Collector has an Internet connection.
4. Log into the server where you want to install the Collector as `root` and make sure your boot DVD is loaded.
5. Go to `/etc/yum.repos.d` and make sure these configuration files are in the directory:
`CentOS-Base.repo`
`CentOS-Debuginfo.repo`
`CentOS-Media.repo`
`CentOS-Vault.repo`
6. Run the `vami_config_net` script to configure the network:
`/opt/vmware/share/vami/vami_config_net`.
7. When prompted, enter the information for these network components to configure the Static IP address:
 - IP Address
 - Netmask
 - Gateway
 - DNS Server(s)
8. Press **Y** to accept the network configuration settings.
9. Enter the Host name, and press **Enter**.
The Collector reboots automatically.
10. As `root`, run the `update` command:
`yum -y update`
11. As `root`, run the `deployment` script:
`/opt/phoenix/deployment/deployment.sh`
The system will reboot itself when the installation completes.
12. Follow the instructions in [Registering the Collector to the Supervisor](#) to complete the Collector set up.

Installing in Dell PowerEdge R210 II

In the R210 II model of Dell PowerEdge, the net interface has been renamed to `p1p1` and `em1`, where in previous versions it was named `eth0`. This can cause installation issues for your Collector. FortiSIEM recommends this workaround:

1. Find the script named either `/etc/sysconfig/network-scripts/ifcfg-p1p1` or `/etc/sysconfig/network-scripts/ifcfg-em1`.
2. Rename the script to `/etc/sysconfig/network-scripts/ifcfg-eth0`.
3. In that script, edit `DEVICE=` to be `DEVICE=eth0`.

If you use the embedded NIC, the device name is **em1**, and if another NIC is inserted, the device name will be **p1p1**.

General Installation

Configuring Worker Settings

If you are using FortiSIEM clustered deployment that includes both Workers and Collectors, you must define the **Address** of your Worker nodes before you register any Collectors. When you register your Collectors, the Worker information will be retrieved and saved locally to the Collector. The Collector will then upload event and configuration change information to the Worker.

Worker Address in a Non-Clustered Environment

If you are not using FortiSIEM clustered deployment, you will not have any Worker nodes. In that case, enter the IP address of the Supervisor for the Worker Address, and your Collectors will upload their information directly to the Supervisor.

1. Log in to your Supervisor node.
2. Go to **Admin > General Settings > System**.
3. For **Worker Address**, enter a comma-separated list of IP addresses or host names for the Workers. The Collector will attempt to upload information to the listed Workers, starting with the first Worker address and proceeding until it finds an available Worker.

Using a Load Balancer with Workers

You may also enter the Host Name or IP Address of a load balancer for the Worker Address, in which case the load balancer needs to be configured to send information to the Workers.

4. Click **Save**.

Registering the Supervisor

1. In a Web browser, navigate to the Supervisor's IP address: `https://<Supervisor IP>`
2. Enter the login credentials associated with your FortiSIEM license, and then click **Register**.
3. When the **System is ready** message appears, click the **Here** link to log in to FortiSIEM.
4. Enter the default login credentials.

User ID	admin
Password	admin*1
Cust/Org ID	super

5. Go to **Admin > Cloud Health** and check that the Supervisor **Health** is **Normal**.

Registering the Worker

1. Go to **Admin > License Management > VA Information**.
2. Click **Add**, enter the new Worker's IP address, and then click **OK**.

3. When the new Worker is successfully added, click **OK**.
You will see the new Worker in the list of Virtual Appliances.
4. Go to **Admin > Cloud Health** and check that the Worker **Health** is **Normal**.

Registering the Collector to the Supervisor

The process for registering a Collector node with your Supervisor node depends on whether you are setting up the Collector as part of an enterprise or multi-tenant deployment. For a multi-tenant deployment, you must first create an organization and add Collectors to it before you register it with the Supervisor. For an enterprise deployment, you install the Collector within your IT infrastructure and then register it with the Supervisor.

- [Create an Organization and Associate Collectors with it for Multi-Tenant Deployments](#)
- [Register the Collector with the Supervisor for Enterprise Deployments](#)

Create an Organization and Associate Collectors with it for Multi-Tenant Deployments

1. Log in to the Supervisor.
2. Go to **Admin > Setup Wizard > Organizations**.
3. Click **Add**.
4. Enter **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**.
Unlimited Start and End Times: If you select Unlimited for Start Time and End Time, those fields will be grayed out for text entry.
7. Click **Save**.
The newly added organization and Collector should be listed on the **Organizations** tab.
8. In a Web browser, navigate to `https://<Collector-IP>:5480`.
9. Enter the Collector setup information.

Name	Collector Name
User ID	Organization Admin User
Password	Organization Admin Password
Cust/Org ID	Organization Name
Cloud URL	Supervisor URL

10. Click **Save**.
The Collector will restart automatically after registration succeeds.
11. In the Supervisor interface, go to **Admin > Collector Health** and check that the Collector **Health** is **Normal**.

Register the Collector with the Supervisor for Enterprise Deployments

1. Log in to the Supervisor.
2. Go to **Admin > License Management**. and check that Collectors are allowed by the license.
3. Go to **Setup Wizard > General Settings** and add at least the Supervisor's IP address.
This should contain a list of the Supervisor and Worker accessible IP addresses or FQDNs.

4. Go to **Setup Wizard > Event Collector** and add the Collector information.

Setting	Description
Name	Will be used in step 6
Guaranteed EPS	This is the number of Events per Second (EPS) that this Collector will be provisioned for
Start Time	Select Unlimited
End Time	Select Unlimited

5. Connect to the Collector at `https://:<IP Address of the Collector>:5480`.
6. Enter the **Name** from step 4.
7. **Userid** and **Password** are the same as the admin userid/password for the Supervisor.
8. The **IP address** is the IP address of the Supervisor.
9. For **Organization**, enter **Super**.
10. The Collector will reboot during the registration, and you will be able to see its status on the **Collector Health** page.

Using NFS Storage with FortiSIEM

When you install FortiSIEM, you have the option to use either local storage or NFS storage. For cluster deployments using Workers, the use of an NFS Server is required for the Supervisor and Workers to communicate with each other. These topics describe how to set up and configure NFS servers for use with FortiSIEM.

Supported Versions

FortiSIEM only supports NFS Version 3.

- [Configuring NFS Storage for VMware ESX Server](#)
- [Using NFS Storage with Amazon Web Services](#)

Configuring NFS Storage for VMware ESX Server

This topic describes the steps for installing an NFS server on CentOS Linux 6.x and higher for use with VMware ESX Server. If you are using an operating system other than CentOS Linux, follow your typical procedure for NFS server set up and configuration.

1. Login to CentOS 6.x as `root` and download and Install the NFS packages.
2. Download and Install the NFS packages.

```
yum install nfs-utils nfs-utils-lib
```

3. Run the NFS server startup scripts.

```
chkconfig nfs on
service rpcbind start
service nfs start
```

4. Check NFS service status and make sure the `nfsd` service is running.

```
service nfs status
```

5. Create a new directory in the large volume to share with the FortiSIEM Supervisor and Worker nodes, and change the access permissions to provide FortiSIEM with access to the directory.

```
mkdir /FortiSIEM
chmod -R 777 /FortiSIEM
```

6. Edit the `/etc/exports` file to share the `/FortiSIEM` directory with the FortiSIEM Supervisor and Worker nodes.

```
vi /etc/exports /FortiSIEM <Supervisor_IP_Address>(rw, sync, no_root_squash)
/FortiSIEM <Worker1_IP_Address>(rw, sync, no_root_squash) /FortiSIEM
<Worker2_IP_Address>(rw, sync, no_root_squash)
```

7. Save your changes to `/etc/exports` and restart the NFS server.

```
showmount -e localhost
Example:
Export list for localhost:
/FortiSIEM <Supervisor_IP_Address>, <Worker1_IP_Address>, <Worker2_IP_
Address>
```

8. Check shared directories.

```
service nfs restart
```

Related Links

- [Setting Up NFS Storage in AWS](#)

Using NFS Storage with Amazon Web Services

- [Setting Up NFS Storage in AWS](#)
- [Setting Up Snapshots of EBS Volumes that Host EventDB and CMDB in AWS](#)

Setting Up NFS Storage in AWS

Youtube Talk on NFS Architecture for AWS

Several architecture and partner options for setting up NFS storage that is highly available across availability zone failures are presented by an AWS Solutions Architect in this [talk](#) (40 min) and link to [slides](#).

Using EBS Volumes

These instructions cover setting up EBS volumes for NFS storage. EBS volumes have a durability guarantee that is 10 times higher than traditional disk drives. This is because data in traditional disk drives is replicated within an availability zone for [component failures \(RAID equivalent\)](#), so adding another layer of RAID does not provide higher durability guarantees. EBS has an annual failure rate (AFR) of 0.1 to 0.5%. In order to have higher durability guarantees, it is necessary to take periodic snapshots of the volumes. Snapshots are stored in AWS S3, which has [99.999999999% durability](#) (via synchronous replication of data across multiple data centers) and 99.99% availability. see the topic [Setting Up Snapshots of EBS Volumes that Host EventDB and CMDB in AWS](#) for more information.

Using EC2 Reserved Instances for Production

If you are running these machines in production, it is significantly cheaper to use [EC2 Reserved Instances](#) (1 or 3 year) as opposed to on-demand instances.

1. Log in to your AWS account and navigate to the EC2 dashboard.
2. Click **Launch Instance**.
3. Select **HVM Amazon Linux AMI (HVM) 64-bit**, and then click **Select**.
HVM v. PV
4. The reason to choose the HVM image over the default Paravirtualized (PV) image is that the HVM image automatically includes drivers to support [enhanced networking](#), which uses [SR-IOV](#) for networking and provide higher performance (packets per second), lower latency, and lower jitter.
5. Click **Compute Optimized**.

Using C3 Instances

You should select one of the C3 instances with a Network Performance rating of High, or 10Gb performance. The current generation of C3 instances run on the latest Intel Xeons that AWS provides. If you are running these machines in production, it is significantly cheaper to use [EC2 Reserved Instances](#) (1 or 3 year) as opposed to on-demand instances.

6. Click **Next: Configure Instance Details**.
7. Review these configuration options:

Network and Subnet

Select the VPC you set up for your instance.

Public IP

Clear the option **Automatically assign a public IP address to your instances** if you want to use VPN.

Placement Group	A placement group is a logical grouping for your cluster instances. Placement groups have low latency, full-bisection 10Gbps bandwidth between instances. Select an existing group or create a new one.
Shutdown Behavior	Make sure Stop is selected.
Enable Termination Protection	Make sure Protect Against Accidental Termination is selected.
EBS Optimized Instance	An EBS optimized instance enables dedicated throughput between Amazon EBS and Amazon EC2, providing improved performance for your EBS volumes. Note that if you select this option, additional Amazon charges may apply.

8. Click **Next: Add Storage**.
9. Add EBS volumes up to the capacity you need for EventDB storage.

EventDB Storage Calculation Example

At 5000 EPS, you can calculate daily storage requirements to amount to roughly 22-30GB (300k events are 15-20MB on average in compressed format stored in EventDB). In order to have 6 months of data available for querying, you need to have 4-6TB of storage. On AWS, the maximum EBS volume is sized at 1TB. In order to have larger disks, you need to create software RAID-0 volumes. You can attach, at most 8 volumes to an instance, which results in 8TB with RAID-0. There's no advantage in using a different RAID configuration other than RAID-0, because it does not increase durability guarantees. In order to ensure much better durability guarantees, plan on performing regular snapshots which store the data in S3 as described in [Setting Up Snapshots of EBS Volumes that Host EventDB and CMDB in AWS](#). Since RAID-0 stripes data across these volumes, the aggregate IOPS you get will be the sum of the IOPS on individual volumes.

10. Click **Next: Tag Instance**.
11. Under **Value**, enter the **Name** you want to assign to all the instances you will launch, and then click **Create Tag**. After you complete the launch process, you will have to rename each instance to correspond to its role in your configuration, such as Supervisor, Worker1, Worker2.
12. Click **Next: Configure Security Group**.
13. Select **Select an Existing Security Group**, and then select the default security group for your VPC. FortiSIEM needs access to HTTPS over port 443 for GUI and API access, and access to SSH over port 22 for remote management, which are set in the default security group. This group will allow traffic between all instances within the VPC.

Limiting IP Access

Make sure you have limited the IP addresses that can access your VPC, or that you have set up VPN access to it. VPN will block all inbound Internet traffic.

14. Click **Review and Launch**.
15. Review all your instance configuration information, and then click **Launch**.

16. Select an existing or create a new **Key Pair** to connect to these instances via SSH.
If you use an existing key pair, make sure you have access to it. If you are creating a new key pair, download the private key and store it in a secure location accessible from the machine from where you usually connect to these AWS instances.
17. Click **Launch Instances**.
18. When the EC2 Dashboard reloads, check that all your instances are up and running.
19. Select the NFS server instance and click **Connect**.
20. Follow the instructions to SSH into the volumes as described in [Configuring the Supervisor and Worker Nodes in AWS](#)
21. Configure the NFS mount point access to give the FortiSIEM internal IP full access.

```
# Update the OS and libraries with the latest patches
$ sudo yum update -y

$ sudo yum install -y nfs-utils nfs-utils-lib lvm2
$ sudo su -
# echo Y | mdadm --verbose --create /dev/md0 --level=0--chunk=256--raid-devices=4/dev/sdf
/dev/sdg /dev/sdh /dev/sdi
# mdadm --detail --scan > /etc/mdadm.conf
# cat /etc/mdadm.conf
# dd if=/dev/zero of=/dev/md0 bs=512count=1
# pvcreate /dev/md0
# vgcreate VolGroupData /dev/md0
# lvcreate -l 100%vg -n LogVolDataMd0 VolGroupData
# mkfs.ext4 -j /dev/VolGroupData/LogVolDataMd0
# echo "/dev/VolGroupData/LogVolDataMd0 /data      ext4      defaults      1 1">>
/etc/fstab
# mkdir /data
# mount /data
# df -kh
# vi /etc/exports
/data 10.0.0.0/24(rw,no_root_squash)
# exportfs -ar
# chkconfig --levels 2345nfs on
# chkconfig --levels 2345rpcbind on
# service rpcbind start
Starting rpcbind: [ OK ]
# service nfs start
Starting NFS services: [ OK ]
Starting NFS mountd: [ OK ]
Stopping RPC idmapd: [ OK ]
Starting RPC idmapd: [ OK ]
Starting NFS daemon: [ OK ]
```

Setting Up Snapshots of EBS Volumes that Host EventDB and CMDb in AWS

In order to have high durability guarantees for FortiSIEM data, you should periodically create EBS snapshots on an hourly, daily, or weekly basis and store them in S3. The EventDB is typically hosted as a RAID-0 volume of several EBS volumes, as described in [Setting Up NFS Storage in AWS](#). In order to reliably snapshot these EBS volumes together, you can use a script, `ec2-consistent-snapshot`, to briefly freeze the volumes and create a snapshot. You can then use a second script, `ec2-expire-snapshots`, to schedule cron jobs to delete old snapshots that are no longer needed. CMDb is hosted on a much smaller EBS volume, and you can also use the same scripts to take snapshots of it.

You can find details of how to download these scripts and set up periodic snapshots and expiration in this blog post:

<http://twigmon.blogspot.com/2013/09/installing-ec2-consistent-snapshot.html>

You can download the scripts from these from these Github projects:

- <https://github.com/alectic/ec2-consistent-snapshot>
- <https://github.com/alectic/ec2-expire-snapshots>

Moving CMDB to a separate Database Host

It is desirable to move the CMDB (postgres) database to a separate host for the following reasons:

1. *In larger deployments, reduce the database server load on the supervisor node in order to allow more resources for application server and other backend modules*
2. *Whenever high availability for CMDB data is desired, it is easier and cleaner to set up separate hosts with postgres replication that are managed separately than do this on the embedded postgres on the supervisor. This is especially true in AWS environment where AWS Postgresql Relational Database Service (RDS) is just a few clicks to set up a DB instance that replicates across availability zones and automatically does failover*

Freshly Installed Supervisor

1. *Install separate Postgresql DB servers or AWS RDS instance in Multi-AZ mode. Use Postgresql version 9.1 or greater. I'll use the RDS example in the remaining steps. For instance, let's say the hostname of RDS in us-west-2 region is phoenixdb.XXXXXX.us-west-2.rds.amazonaws.com on port 5432 with username 'phoenix', DB name 'phoenixdb' and password 'YYYYYYYYY'. You will need to allow super and worker nodes to be able to connect to port 5432 on the RDS service. You will have to change security groups to allow this*
2. *Make sure the above RDS host is reachable from FortiSIEM supervisor*
3. *Install FortiSIEM supervisor node and configure it as usual including adding a license*
4. *Stop all the running services so that CMDB will not be modified further*
5. *Dump the CMDB data in the local postgres DB into a local file*
6. *Import schema/data into the external postgres.*
7. *Change phoenix_config.txt to add DB_SERVER_* info*
8. *Change glassfish application server's domain.xml to point to the external CMDB server*
9. *Change phoenix_config.txt to remove checking for postgres process*
10. *Disable postgres from starting up*

The exact steps are given below:

Stopping services and moving CMDB data

```
#
service crond stop
# Wait for phwatchdog to stop
phxctl stop
# Wait for all processes to stop
su - postgres
pg_dump -U phoenix phoenixdb > phoenixdb-dump.sql
psql -U phoenix -h phoenixdb.XXXXXX.us-west-2.rds.amazonaws.com -p 5432 -f
phoenixdb-dump.sql
# Type the password YYYYYYYY
# Ignore some minor errors such as it will not impact the product from operating
correctly
REVOKE
psql:phoenixdbdump.sql:1017727: ERROR:  role "postgres" does not exist
```

```
psql:phoenixdbdump.sql:1017728: ERROR: role "postgres" does not exist
GRANT
```

Edit phoenix_config.txt

```
vi /opt/phoenix/config/phoenix_config.txt
# change system_services in the phMonitorSupervisor section to remove psql. The
original line is below which should be modified to the next line
#system_services=<system type-
e="phMonitorSupervisor"><service><name>httpd</name><method>phshell 0 head /etc/ht-
tpd/run/httpd.pid</method></service><service><name>glassfish</name><method>ps -ef
| grep java | grep glassfish | grep -v pid | gawk '{print
$2}'</method></service><service><name>pgsql DB</name><method>ps -ef | grep psql |
grep postgres | grep -v pid | gawk '{print $2
}'</method></service></system>#system_services=<system type-
e="phMonitorSupervisor"><service><name>httpd</name><method>phshell 0 head /etc/ht-
tpd/run/httpd.pid</method></service><service><name>glassfish</name><method>ps -ef
| grep java | grep glassfish | grep -v pid | gawk '{print
$2}'</method></service></system># Add db_server_host and db_server_pwd
# db_server_host=phoenixdb.XXXXXX.us-west-2.rds.amazonaws.com
# db_server_pwd=YYYYYYYY
```

Edit glassfish domain.xml

```
vi /opt/glassfish/domains/domain1/config/domain.xml and change db host and pwd
# Under <jdbc-connection-pool> section, change these properties
# <property name="password" value="YYYYYYYY"></property># <property name-
e="ServerName" value="phoenixdb.XXXXXX.us-west-2.rds.amazonaws.com"></property>
```

Turn off embedded postgres service

```
# Turn off postgres startup
chkconfig postgresql-9.1 off

# Remove startdb from /etc/init.d/phProvision.sh
# echo "Starting Database server ...";
# /opt/phoenix/deployment/jumpbox/startdb;
vi /etc/init.d/phProvision.sh
```

Production / Existing Supervisor

Performing these steps on an existing system may require an extended downtime of FortiSIEM services, so plan accordingly.

Make sure you have enough additional storage to dump the existing DB

1. Install and have the external postgres ready as described at the beginning of the previous section
2. Take point-in-time snapshots of supervisor to revert back if you hit any issue
3. Stop crond on super, and wait for phwatchdog to stop
4. Stop Apache on super and all workers so that collectors start buffering events
5. Shutdown the worker nodes while you move CMDB out
6. Follow the instructions from "Freshly Installed Supervisor" to complete the steps.

Related articles

- [FortiSIEM Windows Agent and Agent Manager Install](#)
- [Moving CMDB to a separate Database Host](#)

FortiSIEM Windows Agent and Agent Manager Install

FortiSIEM can discover and collect performance metrics and logs from Windows Servers in an agent less fashion via WMI. However agents are needed when there is a need to collect richer data such as file integrity monitoring and from a large number of servers.

This section describes how to setup FortiSIEM Windows Agent and Agent Manager as part of FortiSIEM infrastructure.

FortiSIEM Windows Agent Pre-installation Notes

- [Licensing](#)
- [Hardware and Software Requirements](#)
 - [Windows Agents](#)
 - [Windows Agent Manager](#)
- [Supported versions](#)
 - [Windows Agent](#)
 - [Windows Agent Manager](#)
- [Communication Ports between Agent and Agent Manager](#)

Licensing

When you purchase the Windows Agent Manager, you also purchase a set number of licenses that can be applied to the Windows devices you are monitoring. After you have set up and configured Windows Agent Manager, you can see the number of both Basic and Advanced licenses that are available and in use in your deployment by logging into your Supervisor node and going to **Admin > License Management**, where you will see an entry for **Basic Windows Licenses Allowed/Used** and **Advanced Windows Licenses Allowed/Used**. You can see how these licenses have been applied by going to **Admin > Windows Agent Health**. When you are logged into the Windows Agent Manager you can also see the number of available and assigned licenses on the **Assign Licenses to Users** page.

There are two types of licenses that you can associate with your Windows agent.

License Type	Description
None	An agent has been installed on the device, but no license is associated with it. This device will not be monitored until a license is applied to it.
Advanced	The agent is licensed to monitor all activity on the device, including logs, installed software changes, and file/folder changes
Basic	The agent is licensed to monitor only logs on the device

When applying licenses to agents, keep in mind that **Advanced** includes **Basic**, so if you have purchased a number of **Advanced** licenses, you could use all those licenses for the **Basic** purpose of monitoring logs.. For example, if you have purchased a total of 10 licenses, five of which are **Advanced** and five of which are **Basic**, you could apply all 10 licenses to your devices as **Basic**.

Feature	License Type
Windows Security Logs	Basic
Windows Application Logs	Basic

Feature	License Type
Windows System Logs	Basic
Windows DNS Logs	Basic
Windows DHCP Logs	Basic
IIS logs	Basic
DFS logs	Basic
File Integrity Monitoring	Advanced
Installed Software Change Monitoring	Advanced
Registry Change Monitoring	Advanced
Custom file monitoring	Advanced
WMI output Monitoring	Advanced
Power shell Output Monitoring	Advanced
Removable media (CD/DVD/USB) Monitoring	Advanced

Hardware and Software Requirements

Windows Agents

Component	Requirement	Notes
CPU	x86 or x64 (or compatible) at 2Ghz or higher	
Hard Disk	10 GB (minimum)	
Server OS	Windows XP-SP3 and above (Recommended)	
Desktop OS	Windows 7/8	Performance issues may occur due to limitations of desktop OS
RAM	<ul style="list-style-type: none"> 1 GB for XP 2+GB for Windows Vista & above / Windows Server 	
Installed Software	<ul style="list-style-type: none"> Windows Agent 2.1: .NET 4.5 or higher Windows Agent 2.0: .NET 4.0 PowerShell 2.0 or higher 	<ul style="list-style-type: none"> .NET Framework 4.0 can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=17718 .NET Framework 4.5 can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=30653, and is already available on Windows 8 and Windows Server 2012 You can download PowerShell from Microsoft at http://www.microsoft.com/en-us/download/details.aspx?id=4045.
Windows OS Language	All languages in which Windows Operating System is available.	

Add Port 80 and 443 as an Exception to the Inbound Firewall Rule

If you are using a firewall, make sure to add Port 80 and 443 as an exception to the inbound firewall rule.

Windows Agent Manager

The primary role of Windows Agent Manager is to configure Windows Agents with right security monitoring policies and monitor Windows Agent health.

Regarding Windows Agent log forwarding, agents can be configured in two ways:

- a. Send logs to an available Collector from a list of Collectors (preferred because of high availability).
In this scenario, each Windows Agent Manager can handle up to 10,000 agents since it is only configuring the agents.
- b. Send logs to Windows Agent Manager which then aggregates the logs from each Agent and sends to Collector or Supervisor.
In this scenario, each Windows Agent Manager can handle up to 1,000 agents at an aggregate of 7.5k events/sec.

Component	Requirement	Notes
CPU	x86 or x64 (or compatible) at 2Ghz or higher	
Hard Disk	10 GB (minimum)	
Server OS	Windows Server 2008 and above (Strongly recommended)	
Desktop OS	Windows 7/8 (performance issues might occur)	Performance issues may occur due to limitations of desktop OS
RAM	<ul style="list-style-type: none"> • For 32 bit OS, 2 GB for Windows 7 / 8 is a minimum • For 64 bit OS, 4 GB for Windows 7/8 and Windows Server 2008 / 2012 is a minimum 	
Installed Software	<ul style="list-style-type: none"> • .NET Framework 4.5 or higher • SQL Server Express or SQL Server 2012 installed using "SQL Server Authentication Mode" • Power Shell 2.0 or higher • IIS 7 or higher installed • IIS 7, 7.5: ASP .NET feature must be enabled from Application Development Role Service of IIS • IIS 8.0+: ASP .NET 4.5 feature must be enabled from Application Development Role Service of IIS 	<ul style="list-style-type: none"> • .NET Framework 4.5 can be downloaded from http://www.microsoft.com/en-us/download/details.aspx?id=30653, and is already available on Windows 8 and Windows Server 2012 • You can download PowerShell from Microsoft at http://www.microsoft.com/en-us/download/details.aspx?id=4045 . • SQL Server Express does not have any performance degradation compared to SQL Server 2012.

Component	Requirement	Notes
Windows OS Language	All languages in which Windows Operating System is available.	

Supported versions

Windows Agent

- Windows 7
- Windows 8
- Windows XP SP3 or above
- Windows Server 2003 (Use Windows Agent 2.0 since 2003 does not support TLS 1.2.)
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2016 R2

Windows Agent Manager

- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Windows Server 2016
- Windows Server 2016 R2

Communication Ports between Agent and Agent Manager

- TCP Port 443 (V1.1 on wards) and TCP Port 80 (V1.0) on Agent Manager for receiving events from Agents.
- Ports 135, 137, 139, 445 needed for NetBIOS based communication

Installing FortiSIEM Windows Agent Manager

Prerequisites

1. Make sure that the ports needed for communication between Windows Agent and Agent Manager are open and the two systems can communicate
2. For versions 1.1 and higher, Agent and Agent Manager communicate via HTTPS. For this reason, there is a special pre-requisite: Get your **Common Name / Subject Name** from IIS
 1. Logon to Windows Agent Manager
 2. Open IIS by going to Run, typing **inetmgr** and pressing enter
 3. Go to **Default Web Site** in the left pane
 4. Right click **Default Web Site** and select **Edit Bindings**.
 5. In **Site Bindings** dialog, check if you have **https** under **Type** column
 6. If **https** is available, then
 - a. Select column corresponding to **https** and click on **Edit**
 - b. In **Edit Site Binding** dialog, under **SSL certificate** section, click on **View...** button.
 - c. In **Certificate** dialog, under **General** tab, note the value of **Issued to**. This is your **Common Name / Subject Name**
3. If **https** is not available, then you need to bind the default web site with https.
 1. Import a New certificate. This can be done in one of two ways
 - a. Either create a Self Signed Certificate as follows
 - i. Open IIS by going to Run, typing **inetmgr** and pressing enter
 - ii. In the left pane, select computer name
 - iii. In the right pane, double click on **Server Certificates**
 - iv. In the **Server Certificate** section, click on **Create Self-Signed Certificate...** from the right pane
 - v. In **Create Self-Signed Certificate** dialog, specify a friendly name for the certificate and click **OK**
 - vi. You will see your new certificate in the **Server Certificates** list
 - b. Or, Import a third party certificate from a certification authority.
 - a. Buy the certificate (.pfx or .cer file)
 - b. Install the certificate file in your server
 - c. Import the certificate in IIS
 - d. Go to IIS. Select **Computer name** and in the right pane select **Server Certificates**
 - e. If certificate is PFX File
 - i. In **Server Certificates** section, click on **Import...** in right pane
 - ii. In the **Import Certificate** dialog, browse to pfx file and put it in Certificate file(.pfx) box
 - iii. Give your pfx password and click **Ok**. Your certificate gets imported to IIS
 - f. If certificate is CER File
 - i. In **Server Certificates** section, click on **Complete Certificate Request...** in right pane
 - ii. In the **Complete Certificate Request** dialog, browse to CER file and put it

- in File name section
- iii. Enter the friendly name, click **Ok**. Your certificate gets imported to IIS .
2. Bind your certificate to **Default Web Site**
 - a. Open IIS by going to Run, typing **inetmgr** and pressing enter
 - b. Right click on **Default Web Site** and select **Edit Bindings...**
 - c. In **Site Bindings...** dialog, click on **Add..**
 - d. In **Add Site Binding** dialog, select 'https' from **Type** drop down menu
 - e. The **Host name** is optional but if you want to put it, then it must be the same as the certificate's common name / Subject name
 - f. Select your certificate from **SSL certificate:** drop down list
 - g. Click **OK**.
 3. Your certificate is now bound to the **Default Web Site**.
4. **Enable TLS 1.2 for Windows Agent Manager 2.0 for operating with FortiSIEM Supervisor/Worker 4.6.3 and above.** By default SSL3 / TLS 1.0 is enabled in Windows Server 2008-R2. Hence, before proceeding with the server installation, please enable TLS 1.2 manually as follows.
 1. Start elevated Command Prompt (i.e., with administrative privilege)
 2. Run the following commands sequentially as shown.


```
REG ADD
    "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Client" /v DisabledByDefault /t REG_DWORD /d
    00000000
REG ADD
    "HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\Protocols\TLS 1.2\Server" /v DisabledByDefault /t REG_DWORD /d
    00000000
```
 3. Restart computer

Procedure

1. On the machine where you want to install the manager, launch either the `FortiSIEMServer-x86.MSI` (for 32-bit Windows) or `FortiSIEMServer-x64.MSI` (for 64-bit Windows) installer.
2. In the **Welcome** dialog , click **Next**.
3. In the **EULA** dialog, agree to the **Terms and Conditions**, and then click **Next**.
4. Specify the destination path for the installation, and then click **Next**.
By default the Windows Agent Manager will be installed at `C:\Program Files\AccelOps\Server`.
5. Specify the destination path to install the client agent installation files, and then click **Next**.
By default these files will be installed at `C:\AccelOps\Agent`. The default location will be on the drive that has the most free storage space. This path will automatically become a shared location that you will access from the agent devices to install the agent software on them.
6. In the **Database Settings** dialog,
 - a. Select the database instance where metrics and logs from the Windows devices will be stored.
 - b. Select whether you want to use Windows authentication, otherwise provide the login credentials that are needed to access the SQL Server instance where the database is located.
 - c. Enter the path where FortiSIEM Agent Manager database will be stored. By default it is `C:\AccelOps\Data`
7. Provide the path to the FortiSIEM Supervisor, Worker, or Collector that will receive information about your Windows devices. Click **Next**.

8. In the **Administrator Settings** dialog, enter username and password credentials that you will use to log in to the Windows Agent Manager.
Both your username and password should be at least six characters long.
9. (New in Release 1.1 for HTTPS communication between Agent and Agent Manager) Enter the **common name/subject name** of the SSL certificate created in pre-requisite step 2
10. Click **Install**.
11. When the installation completes, click **Finish**.
12. You can now exit the installation process, or click **Close Set Up and Run FortiSIEM** to log into your FortiSIEM virtual appliance.

Installing FortiSIEM Windows Agent

Prerequisites

1. Windows Agent and Agent Manager need to be able to communicate - agents need to access a path on the Agent Manager machine to install the agent software.
2. Starting with Version 1.1, there is a special requirement if you want user information appended to file/directory change events. Typically file/directory change events do not have information about the user who made the change. To get this information, you have to do the following steps. Without this step, File monitoring events will not have user information.
 1. In *Workgroup Environment*:
 - a. Go to **Control Panel**
 - b. Open **Administrative Tools**
 - c. Double click on **Local Security Policy**
 - d. Expand **Advanced Audit Policy** configuration in the left-pane
 - e. Under **Advanced Audit Policy**, expand **System Audit Policies – Local Group Policy Object**
 - f. Under System Audit Policies – Local Group Policy Object, select **Object Access**
 - g. Double-click on **Audit File System** in the right-pane
 - h. **Audit File System** Properties dialog opens. In this dialog, under **Policy** tab, select **Configure the following audit events**. Under this select both Success and Failure check boxes
 - i. Click **Apply** and then **OK**
 2. In *Active Directory Domain Environment*: FortiSIEM Administrator can use Group Policies to propagate the above settings to the agent computers as follows:
 - a. Go to **Control Panel**
 - b. Open **Administrative Tools**
 - c. Click on **Group Policy Management**
 - d. In **Group Policy Management** dialog, expand **Forest:<domain_name>** in the left-pane
 - e. Under **Forest:<domain_name>**, expand **Domains**
 - f. Under **Domains**, expand **<domain_name>**
 - g. Right-click on **<domain_name>** and click on '**Create a GPO in this domain, and link it here...**'
 - h. New GPO dialog appears. Enter a new name (e.g., **MyGPO**) in **Name** text box. Press **OK**.
 - i. **MyGPO** appears under the expanded **<domain_name>** in left-pane. Click on **MyGPO** and click on the **Scope** tab in the right-pane.
 - j. Under **Scope** tab, click on **Add** in **Security filtering** section
 - k. Select **User, Computer or Group** dialog opens. In this dialog click the **Object Types** button.
 - l. **Object Types** dialog appears, uncheck all options and check the **Computers** option. Click **OK**.
 - m. Back in the **Select User, Computer or Group** dialog, enter the FortiSIEM Windows Agent computer names under **Enter the object name** to select area. You can choose computer names by clicking the **Advanced** button and then in **Advanced** dialog clicking on the **Find Now** button.

- n. Once the required computer name is specified, click **OK** and you will find the selected computer name under **Security Filtering**.
- o. Repeat steps (xi) – (xiv) for all the required computers running FortiSIEM Windows Agent.
- p. Right click on **MyGPO** in the left-pane and click on **Edit**.
- q. **Group Policy Management Editor** opens. In this dialog, expand **Policies** under **Computer Configuration**.
- r. Go to **Policies > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Audit Policies > Object Access > Audit File System**.
- s. In the **Audit File System Properties** dialog, under **Policy tab** select **Configure the following audit** events. Under this, select both **Success** and **Failure** check boxes.

Installing one agent

1. Log into the machine where you want to install the agent software as an administrator.
2. Navigate to the shared location on the Windows Agent Manager machine where you installed the agent installation files in Step 5 of [Installing FortiSIEM Windows Agent Manager](#).
The default path is `C:\AccelOps\Agent`.
3. In the shared location, double-click on the appropriate .MSI file to begin installation.
FortiSIEMAgent-x64.MSI is for the 64-bit Agent, while **FortiSIEMAgent-x86.MSI** is for the 32-bit Agent
4. When the installation completes, go to **Start > Administrative Tools > Services** and make sure that the **FortiSIEM Agent Service** has a status of **Started**.

Installing multiple agents via Active Directory Group Policy

Multiple agents can be installed via GPO if all the computers are on the same domain.

1. Log on to Domain Controller
2. Create a separate Organization unit for containing all computers where FortiSIEM Windows Agent have to be installed.
 - a. Go to **Start > Administrative Tools > Active Directory Users and Computers**
 - b. Right click on the root Domain on the left side tree. Click **New > Organizational Unit**
 - c. Provide a **Name** for the newly created Organizational Unit and click **OK**.
 - d. Verify that the Organizational Unit has been created.
3. Assign computers to the new Organizational Unit.
 - a. Click **Computers** under the domain. The list of computers will be displayed on the right pane
 - b. Select a computer on the right pane. Right click and select **Move** and then select the new Organizational Unit.
 - c. Click **OK**.
4. Create a new GPO
 - a. Go to **Start > Administrative Tools > Group Policy Management**
 - b. Under Domains, select the newly created **Organization Unit**
 - c. Right click on the **Organization Unit** and select **Create and Link a GPO here...**
 - d. Enter a **Name** for the new GPO and click **OK**.
 - e. Verify that the new GPO is created under the chosen Organizational Unit
 - f. Right click on the new GPO and click **Edit**. Left tree now shows **Computer Configuration** and **User Configuration**
 - g. Under **Computer Configuration**, expand **Software Settings**.

- h. Click **New > Package**. Then go to AOWinAgt folder on the network folder. Select the Agent MSI you need - 32 bit or 64 bit. Click **OK**.
 - i. The selected MSI shows in the right pane under **Group Policy Editor** window
 - j. For **Deploy Software**, select **Assigned** and click **OK**.
5. Update the GPO on Domain Controller
 - a. Open a command prompt
 - b. Run **gpupdate /force**
6. Update GPO on Agents
 - a. Log on to the computer
 - b. Open a command prompt
 - c. Run **gpupdate**
 - d. Restart the computer
 - e. You will see FortiSIEM Windows Agent installed after restart

If you have a mix of 32 bit and 64 bit computers, need to have two separate Organizational Units - one for 32bit and one for 64bit, and then assign corresponding MSIs to each.

Upgrading FortiSIEM

- [Upgrade Notes](#)
- [Upgrade Process](#)
- [Migrating from 3.7.x versions to 4.2.1](#)
- [Migrating the SVN Repository to a Separate Partition on a Local Disk](#)
- [Special pre-upgrade instruction for 4.3.3](#)
- [Special pre-upgrade instruction for 4.6.1](#)
- [Enabling TLS 1.2 Patch On Old Collectors](#)
- [Upgrading to 4.6.3 for TLS 1.2](#)
- [Setting Up the Image Server for Collector Upgrades](#)
- [Upgrading a FortiSIEM Single Node Deployment](#)
- [Upgrading a FortiSIEM Cluster Deployment](#)
- [Upgrading FortiSIEM Windows Agent and Agent Manager](#)
- [Automatic OS Upgrades during Reboot](#)

Important Post-Upgrade Procedure

After an upgrade, please clear all browser cache before accessing FortiSIEM GUI. Otherwise, browser caching may prevent FortiSIEM GUI from working correctly.

Upgrade notes

FortiSIEM Cluster upgrade order

FortiSIEM Cluster must be upgraded in the following order:

1. Upgrade Supervisor.
2. Upgrade Workers.
3. Apply 4.10.0 license key.
4. Upgrade Collectors.

FortiSIEM Configuration file merge

FortiSIEM has several parameter settings defined in the `/opt/phoenix/config/phoenix_config.txt` file used by various modules. With each new version, new settings are added or existing settings are modified. You can also modify the `phoenix_config.txt` file in their own system.

During the upgrade process, FortiSIEM checks the existing `phoenix_config.txt` file on the system and compares it with the system provided `phoenix_config.txt` file for that version and asks users whether to keep the existing or new settings.

The following table states the correct user responses for standard upgrades for `phoenix_config.txt` changes.

The general guidelines are as follows:

- The first four fields in the table are IP addresses and the user should retain the old entries.
- For all other fields in the table, the user should choose the new entries introduced by FortiSIEM.
- If you modify any `phoenix_config.txt` file parameter to work efficiently in your environment, you need to Select 1 (Old) to keep your choice from being overwritten.

Fields in <code>phoenix_config.txt</code>	User response	User response		
		4.7.x to 4.10.0	4.8.x to 4.10.0	4.9.x to 4.10.0
APP_SERVER_HOST	Super	Select 1 (Old)	Select 1 (Old)	Select 1 (Old)
PARSER_SERVER_HOST	Super	Select 1 (Old)	Select 1 (Old)	Select 1 (Old)
parser_server_host	Super	Select 1 (Old)	Select 1 (Old)	Select 1 (Old)
MON_SERVER_HOST	Super	Select 1 (Old)	Select 1 (Old)	Select 1 (Old)
READER_LAG_RESET_PCT	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)
high_watermark	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)
low_watermark	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)

Fields in phoenix_config.txt	User response			
num_segment_mergers	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)
num_perf_event_loaders	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)
num_flow_event_loaders	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)
num_misc_event_loaders	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)
num_segment_flushers	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)
num_db_spliters	Super, Worker	Select 2 (New)	Select 2 (New)	Select 2 (New)
http_time_out	Super, Worker	Select 2 (New)	N/A	N/A
check_eventdb_size	Super, Worker	Select 2 (New)	N/A	N/A
du_check_interval	Super, Worker	Select 2 (New)	N/A	N/A
dir_access_check_timeout	Super, Worker	Select 2 (New)	N/A	N/A
show_sys_error_on_low_space	Super, Worker	Select 2 (New)	N/A	N/A
low_space_warning_threshold	Super, Worker	Select 2 (New)	N/A	N/A
archive_rename_existing_directory	Super, Worker	Select 2 (New)	N/A	N/A
low_space_warning_threshold	Super, Worker	Select 2 (New)	N/A	N/A
archive_rename_existing_directory	Super, Worker	Select 2 (New)	N/A	N/A
wmi_pull_rec_limit	Super, Worker	Select 2 (New)	N/A	N/A
wmi_pull_interval	Super, Worker	Select 2 (New)	N/A	N/A

Fields in phoenix_config.txt	User response			
rest_cache_process_list=phParser				
phDiscover				
phPerfMonitor				
phAgentManager				
phDataManager				
phQueryWorker				
phQueryMaster	Super, Worker	Select 2 (New)	N/A	N/A
phRuleWorker				
phRuleMaster				
phReportWorker				
phReportMaster				
phIpIdentityWorker				
phIpIdentityMaster				
phReportLoader				

Recovery

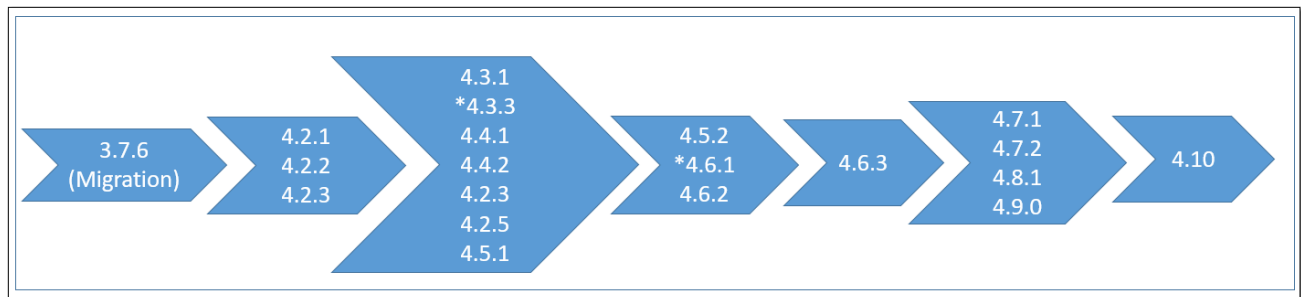
If the `phoenix_config.txt` file is damaged after upgrade due to any reason, repeat the merge process as follows:

1. Recover your `phoenix_config.txt` by copying from the backup location `/tmp/backup/phoenix_config.txt` to `/opt/phoenix/config/phoenix_config.txt`
2. Change `phoenix_config.txt` permissions by running:
 - a. `chmod 644 /opt/phoenix/config/phoenix_config.txt`
 - b. `chown admin.admin /opt/phoenix/config/phoenix_config.txt`
3. Repeat the merge process by running the command `/opt/phoenix/deployment/jumpbox/phmergeconfig` and follow the recommended upgrade response from [FortiSIEM Configuration file merge](#).
4. Reboot the system at Linux level (Super or Worker).

Upgrade process

Note the following:

- Before upgrading FortiSIEM, you **MUST** read the changes in FortiSIEM licensing documented in [Licensing Guide](#).
- You must upgrade Supervisor, Worker/s and Report server first before applying license. Apply the license after FortiSIEM cluster (Supervisor, Worker/s and Report server) upgrade.



UPGRADE REQUIREMENT

Starting 4.5, Supervisor requires 24 GB RAM. This is because Supervisor node is caching device monitoring status for faster performance.

Starting 4.6.1, Linux swap space is increased to match the physical memory size, as recommended by Linux best practices for optimal system performance. This size is automatically increased during 4.6.1 upgrade which may cause upgrade to take a little longer than normal.

FortiSIEM SNMP Configuration

If you enabled SNMP on FortiSIEM nodes (Collectors, Workers, Supervisors), it is recommended that you modify the `snmpd.local.conf` file to store special configurations. You should not modify `snmpd.conf` file since FortiSIEM upgrade will wipe away the changes in `snmpd.conf`. To prevent changes from being lost, copy the changes to `snmpd.local.conf` file and then upgrade.

Upgrading from 3.7.6 to latest

1. First upgrade to 4.2.1 following steps in [here](#). This involves OS migration
2. Upgrade from 4.2.1 to 4.3.1 following steps in [here](#). This involves SVN migration
3. Upgrade from 4.3.1 to 4.5.2. This is a regular upgrade - [single node case](#) and [multi-node case](#).
4. Upgrade from 4.5.2 to 4.6.3 following steps in [here](#). This involves TLS 1.2 upgrade.
5. Upgrade from 4.6.3 to 4.7.1 or above. This is a regular upgrade - [single node case](#) and [multi-node case](#).

Upgrading from 4.2.x to latest

1. Upgrade to 4.3.1 following steps in [here](#). This involves SVN migration.
2. Upgrade from 4.3.1 to 4.5.2. This is a regular upgrade -[single node case](#) and [multi-node case](#).
3. Upgrade from 4.5.2 to 4.6.3 following steps in [here](#). This involves TLS 1.2 upgrade.
4. Upgrade from 4.6.3 to 4.7.1 or above. This is a regular upgrade -[single node case](#) and [multi-node case](#).

Upgrading from 4.3.1 to latest

1. Upgrade from 4.3.1 to 4.5.2. This is a regular upgrade -[single node case](#) and [multi-node case](#).
2. Upgrade from 4.5.2 to 4.6.3 following steps in [here](#). This involves TLS 1.2 upgrade.
3. Upgrade from 4.6.3 to 4.7.1 or above. This is a regular upgrade -[single node case](#) and [multi-node case](#).

Upgrading from 4.3.3 to latest

1. Do the special pre-upgrade steps.
2. Upgrade to 4.5.2. This is a regular upgrade -[single node case](#) and [multi-node case](#).
3. Upgrade from 4.5.2 to 4.6.3 following steps in [here](#). This involves TLS 1.2 upgrade.
4. Upgrade from 4.6.3 to 4.7.1 or above. This is a regular upgrade -[single node case](#) and [multi-node case](#).

Upgrading from 4.4.x, 4.5.1 to latest

1. Upgrade to 4.5.2. This is a regular upgrade - [single node case](#) and [multi-node case](#).
2. Upgrade from 4.5.2 to 4.6.3 following steps in [here](#). This involves TLS 1.2 upgrade.
3. Upgrade from 4.6.3 to 4.7.1 or above. This is a regular upgrade -[single node case](#) and [multi-node case](#).

Upgrading from 4.5.2 to latest

1. Upgrade to 4.6.3 following steps in [here](#). This involves TLS 1.2 upgrade.
2. Upgrade from 4.6.3 to 4.7.1 or above. This is a regular upgrade -[single node case](#) and [multi-node case](#).

Upgrading from 4.6.1 to latest

1. Do the special pre-upgrade steps.
2. Upgrade to 4.6.3 following steps in [here](#). This involves TLS 1.2 upgrade.
3. Upgrade from 4.6.3 to 4.7.1 or above. This is a regular upgrade -[single node case](#) and [multi-node case](#).

Upgrading from 4.6.2 to latest

1. Upgrade to 4.6.3 following steps in [here](#). This involves TLS 1.2 upgrade.
2. Upgrade from 4.6.3 to 4.7.1 or above. This is a regular upgrade - [single node case](#) and [multi-node case](#).

Upgrading from 4.6.3 to latest

1. Upgrade to 4.7.1 or above. This is a regular upgrade -[single node case](#) and [multi-node case](#).

Upgrading Windows Agents

FortiSIEM Windows Agent Upgrade is covered in [Upgrading FortiSIEM Windows Agent and Agent Manager](#)

Migrating from 3.7.x versions to 4.2.1

The 4.2 version of FortiSIEM uses a new version of CentOS, and so upgrading to version 4.2 from previous versions involves a migration from those versions to 4.2.x, rather than a typical upgrade. This process involves two steps:

1. You have to migrate the 3.7.6 CMDB to a 4.2.1 CMDB on a 3.7.6 based system.
2. The migrated 4.2.1 CMDB has to be imported into a 4.2.1 system.

Topics in this section cover the migration process for supported hypervisors for both migrations in-place and using staging systems. Using a staging system requires more hardware, but minimizes downtime and CMDB migration risk compared to the in-place method. If you decide to use the in-place method, we strongly recommend that you take snapshots for recovery.

Migrating Before Upgrading to 4.3.x

If you are running a 3.7.x version of FortiSIEM, you must first migrate from that version to version 4.2.1 before you can upgrade to version 4.3.x.

- [Migrating VMware ESX-based Deployments](#)
- [Migrating AWS EC2 Deployments](#)
- [Migrating KVM-based deployments](#)
- [Migrating Collectors](#)

Migrating VMware ESX-based Deployments

The options for migrating VMware ESX deployments depend on whether you are using NFS for storage, and whether you choose to migrate in-place, or by using a staging system or rsync. Using the staging system requires more hardware, but minimizes downtime and CMDB migration risk compared to the in-place approach. The rsync method takes longer to complete because the event database has to be copied. If you use the in-place method, then we strongly recommend that you take snapshots of the CMDB for recovery.

Internet access is needed for migration to succeed. A third party library needs to access the schema website.

```
<faces-config xmlns="http://java.sun.com/xml/ns/javaee" xmlns:x-  
si="http://www.w3.org/2001/XMLSchema-instance" xm-  
lns:cdk="http://jboss.org/schema/richfaces/cdk/extensions" version="2.0" metadata-  
complete="false" xsi:schemaLocation="http://java.sun.com/xml/ns/javaee http://-  
java.sun.com/xml/ns/javaee/web-facesconfig_2_0.xsd">
```

- [Migrating an ESX Deployment with Local Storage in Place](#)
- [Migrating an ESX Local Disk-based Deployment Using an rsync Tool](#)
- [Migrating an ESX NFS-based Deployment in Place](#)
- [Migrating an ESX NFS-based Deployment via a Staging System](#)

Migrating an ESX Deployment with Local Storage in Place

This migration process is for FortiSIEM deployment with a single virtual appliance and the CMDB data stored on a local VMware disk, and where you intend to run a 4.2.x version on the same physical machine as the 3.7.x version, but as a new virtual machine. This process requires these steps:

- [Prerequisites](#)
- [Upgrading the 3.7.x CMDB to 4.2.1 CMDB](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor](#)
- [Registering Workers to the Supervisor](#)

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Use More Storage for Your 4.2.1 Virtual Appliance

Install the 4.2.1 virtual appliance on the same host as the 3.7.x version with a local disk that is larger than the original 3.7.x version. You will need the extra disk space for copying operations during the migration.

Upgrading the 3.7.x CMDB to 4.2.1 CMDB

1. Log in over SSH to your running 3.7.x virtual appliance as root.
2. Change the directory to `/root`.
3. Move or copy the migration script `ao-db-migration-4.2.1.tar` to `/root`.
4. Untar the migration script.
5. Run `ls -al` to check that `root` is the owner of the files `ao-db-migration.sh` and `ao-db-migration-archiver.sh`.
6. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command. `phtools --stop all`.
7. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command. `phtools --stop all`
8. Run the archive script to create an archive version of the CMDB, and specify the directory where it should be created. `./ao-db-migration-archiver.sh /tmp/376_archive/`
9. Check the that archive files `phoenixdb_migration_*` and `opt-migration-*.tar` were successfully created in the destination directory.
10. Copy the `opt-migration-*.tar` file to `/root`.
This contains various data files outside of CMDB that will be needed to restore the upgraded CMDB.
11. Run the migration script on the 3.7.x CMDB archive you created in step 7.
The first argument is the location of the archived 3.7.x CMDB, and the second argument is the location where the migrated CMDB file will be kept.

```
/root/ao-db-migration.sh /tmp/376_archive/cmdb-migration-xyz /tmp/376_
migration
```

12. Make sure the migrated files were successfully created.
13. Copy the migrated CMDB `phoenixdb_migration_xyz` file to the `/root` directory of your 4.2.1 virtual appliance
This file will be used during the CMDB restoration process.

Removing the Local Disk from the 3.7.x Virtual Appliance

1. Log in to your vSphere client.
2. Select your 3.7.x virtual appliance and power it off.
3. Open the **Hardware** properties for your virtual appliance.
4. Select `Hard disk 3`, and then click **Remove**.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as `root`.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-migration-xyz.tar
```
4. When the migration script completes the virtual appliance will reboot.

Adding the Local Disk to the 4.2.1 Virtual Appliance

1. Log into your vSphere client.
2. Select your 4.2.1 virtual appliance and power it off.
3. Go the **Hardware** settings for your virtual appliance and select `Hard disk 3`.
4. Click **Remove**.
5. Click **Add**.
6. For **Device Type**, select **Hard Disk**, and then click **Next**.
7. Select **Use an existing virtual disk**, and then click **Next**.
8. Browse to the location of the migrated virtual disk that was created by the migration script, and then click **OK**.
9. Power on the virtual appliance.

Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor

1. In the vSphere client, power off the 3.7.x Supervisor.
The IP Address for the 3.7.x Supervisor will be transferred to the 4.2.1 Supervisor.
2. Log in to the 3.7.x Supervisor as `root` over SSH.
3. Run the `vami_config_net` script. Your virtual appliance will reboot when the IP address change is complete.

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


Registering Workers to the Supervisor

1. Log in to the Supervisor as admin.
2. Go to **Admin > License Management**.
3. Under **VA Information**, click **Add**, and add the Worker.
4. Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as root over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating an ESX Local Disk-based Deployment Using an rsync Tool

This process requires these steps:

- [Overview](#)
- [Prerequisites](#)
- [Copy the 3.7.x CMDB to a 4.2.1 Virtual Appliance Using rsync](#)
- [Upgrading the 3.7.x CMDB to 4.2.1 CMDB](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor](#)
- [Registering Workers to the Supervisor](#)

Overview

This migration process is for FortiSIEM deployment with a single virtual appliance and the CMDB data stored on a local VMware disk, and where you intend to run the 4.2.1 version on a different physical machine as the 3.7.x version.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Copy the 3.7.x CMDB to a 4.2.1 Virtual Appliance Using rsync

Installing rsynch

Before you can copy CMDB, you need to have rsync installed on the 3.7.x virtual appliance where you will be making the copy.

1. Log in to the 3.7.x Supervisor as root over SSH.
2. Copy `CentOS-Base.repo` to `/etc/yum.repos.d`.

```
cp /etc/yum.repos.d.orig/CentOS-Base.repo /etc/yum.repos.d
```

3. Install `rsync` yum repo.

```
yum install rsync
```

Procedure

1. Log in to the 4.2.1 virtual appliance as root.
2. Check the disk size in the remote system to make sure that there is enough space for the database to be copied over.
3. Copy the directory `/data` from the 3.7.x virtual appliance to the 4.2.1 virtual appliance using the rsync tool.

rsync Command Syntax

Make sure that the trailing `/` is used in the final two arguments in the rsync command

```
rsync --progress -av root@<3.7.x_VA_ip_address>:/data/ /data/
```

4. After copying is complete, make sure that the size of the event database is identical to the 3.7.x system.

Upgrading the 3.7.x CMDB to 4.2.1 CMDB

1. Log in over SSH to your running 3.7.x virtual appliance as root.
2. Change the directory to `/root`.
3. Move or copy the migration script `ao-db-migration-4.2.1.tar` to `/root`.
4. Untar the migration script.
5. Run `ls -al` to check that `root` is the owner of the files `ao-db-migration.sh` and `ao-db-migration-archiver.sh`.
6. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command.

```
phtools --stop all
```

7. Run the archive script to create an archive version of the CMDB, and specify the directory where it should be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```

8. Check that the archive files `phoenixdb_migration_*` and `opt-migration-*.tar` were successfully created in the destination directory.
9. Copy the `opt-migration-*.tar` file to `/root`.
This contains various data files outside of CMDB that will be needed to restore the upgraded CMDB.
10. Run the migration script on the 3.7.x CMDB archive you created in step 7.
The first argument is the location of the archived 3.7.x CMDB, and the second argument is the location where the migrated CMDB file will be kept.

```
/root/ao-db-migration.sh /tmp/376_archive/cmdb-migration-xyz /tmp/376_migration
```

11. Make sure the migrated files were successfully created.
12. Copy the migrated CMDB `phoenixdb_migration_xyz` file to the `/root` directory of your 4.2.1 virtual appliance.
This file will be used during the CMDB restoration process.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor

1. In the vSphere client, power off the 3.7.x Supervisor.
The IP Address for the 3.7.x Supervisor will be transferred to the 4.2.1 Supervisor.

2. Log in to the 3.7.x Supervisor as `root` over SSH.
3. Run the `vami_config_net` script.
Your virtual appliance will reboot when the IP address change is complete.

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

Registering Workers to the Supervisor

1. Log in to the Supervisor as `admin`.
2. Go to **Admin > License Management**.
3. Under **VA Information**, click **Add**, and add the Worker.
4. Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as `root` over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating an ESX NFS-based Deployment in Place

The steps for this process are:

- [Overview](#)
- [Prerequisites](#)
- [Upgrading the 3.7.x CMDB to 4.2.1 CMDB](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Mounting the NFS Storage on Supervisors and Workers](#)
- [Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor](#)
- [Registering Workers to the Supervisor](#)

Overview

In this migration method, the production FortiSIEM systems are upgraded in-place, meaning that the production 3.7.x virtual appliance is stopped and used for migrating the CMDB to the 4.2.1 virtual appliance. The advantage of this approach is that no extra hardware is needed, while the disadvantage is extended downtime during the CMDB archive and upgrade process. During this downtime events are not lost but are buffered at the collector. However, incidents are not triggered while events are buffered. Prior to the CMDB upgrade process, you might want to take a snapshot of CMDB to use as a backup if needed.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Upgrading the 3.7.x CMDB to 4.2.1 CMDB

1. Log in over SSH to your running 3.7.x virtual appliance as root.
2. Change the directory to `/root`.
3. Move or copy the migration script `ao-db-migration-4.2.1.tar` to `/root`.
4. Untar the migration script.
5. Run `ls -al` to check that `root` is the owner of the files `ao-db-migration.sh` and `ao-db-migration-archiver.sh`.
6. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command.

```
phtools --stop all
```
7. Run the archive script to create an archive version of the CMDB, and specify the directory where it should be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```
8. Check the that archive files `phoenixdb_migration_*` and `opt-migration-*.tar` were successfully created in the destination directory.

9. Copy the `opt-migration-*.tar` file to `/root`.
This contains various data files outside of CMDB that will be needed to restore the upgraded CMDB.
10. Run the migration script on the 3.7.x CMDB archive you created in step 7.
The first argument is the location of the archived 3.7.x CMDB, and the second argument is the location where the migrated CMDB file will be kept.

```
/root/ao-db-migration.sh /tmp/376_archive/cmdb-migration-xyz /tmp/376_
migration
```

11. Make sure the migrated files were successfully created.
12. Copy the migrated CMDB `phoenixdb_migration_xyz` file to the `/root` directory of your 4.2.1 virtual appliance
This file will be used during the CMDB restoration process.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-
migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Mounting the NFS Storage on Supervisors and Workers

Follow this process for each Supervisor and Worker in your deployment.

1. Log in to your virtual appliance as root over SSH.
2. Run the `mount` command to check the mount location.
3. Stop all FortiSIEM processes.

```
service crond stop
phtools --stop all
killall -9 phMonitor
su - admin
/opt/glassfish/bin/asadmin stop-domain
exit
service postgresql-9.1 stop
service httpd stop
```

4. Unmount 4.2.1 NFS storage location.

```
umount /data
```

5. Mount back to the 3.7.x NFS storage location.

```
Usage: mount -t nfs -o nfsvers=3 <NFS_Server_IP>:<Mount_Path> /data
ex: mount -t nfs -o nfsvers=3 192.168.67.168:/data/mig/SP61_376 /data
```

- Verify mount location on the Supervisor or Workers.

```
[root@SP421_from_376 ~]# mount
/dev/sda3 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda1 on /boot type ext3 (rw)
/dev/sdb1 on /cldb type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
192.168.65.91:/A0/mig/SP376_205 on /data type nfs (rw,nfsvers=3,addr=192.168.65.91)
[root@SP421_from_376 ~]#
[root@SP421_from_376 ~]# df -h
Filesystem      Size  Used Avail Use% Mounted on
/dev/sda3       73G   4.9G   65G   8% /
tmpfs           7.8G   0     7.8G   0% /dev/shm
/dev/sda1       124M   26M   93M   22% /boot
/dev/sdb1       60G   727M   56G   2% /cldb
192.168.65.91:/A0/mig/SP376_205
                    50G   37G   11G   78% /data
[root@SP421_from_376 ~]# █
```

- Change to the 3.7.x mount path location in the `/etc/fstab` file on the Supervisor or Workers.

```
# /etc/fstab
# Created by anaconda on Fri Apr  4 22:34:44 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=8c2439d2-5c46-45ac-a669-8ea4c4a20913 / ext3 defaults 1 1
UUID=4a2c534d-4027-4d36-ad62-c696c75d22c6 /boot ext3 defaults 1 2
UUID=4a0debf8-feeb-4937-9909-7919e430d899 swap swap defaults 0 0
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
/dev/sdb1 /cldb ext3 defaults 0 1
192.168.65.91:/A0/mig/SP376_205 /data nfs defaults,nfsvers=3,noatime,nolock 0 0
~
```

- Reboot the Supervisor or Worker.

Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor

In the vSphere client, power off the 3.7.x Supervisor.

The IP Address for the 3.7.x Supervisor will be transferred to the 4.2.1 Supervisor.

- Log in to the 3.7.x Supervisor as `root` over SSH.
- Run the `vami_config_net` script.
Your virtual appliance will reboot when the IP address change is complete.

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

Registering Workers to the Supervisor

- Log in to the Supervisor as `admin`.
- Go to **Admin > License Management**.
- Under **VA Information**, click **Add**, and add the Worker.
- Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as root over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating an ESX NFS-based Deployment via a Staging System

The steps in this process are:

- [Overview](#)
- [Prerequisites](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Mounting the NFS Storage on Supervisors and Workers](#)
- [Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor](#)
- [Registering Workers to the Supervisor](#)

Overview

In this migration method, the production 3.7.x FortiSIEM systems are left untouched. A separate mirror image 3.7.x system is first created, and then upgraded to 4.2.1. The NFS storage is mounted to the upgraded 4.2.1 system, and the collectors are redirected to the upgraded 4.2.1 system. The upgraded 4.2.1 system now becomes the production system, while the old 3.7.6 system can be decommissioned. The collectors can then be upgraded one by one. The advantages of this method is minimal downtime in which incidents aren't triggered, and no upgrade risk. If for some reason the upgrade fails, it can be aborted without any risk to your production CMDB data. The disadvantages of this method are the requirement for hardware to set up the mirror 3.7.x mirror system, and longer time to complete the upgrade because of the time needed to set up the mirror system.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Create the 3.7.x CMDB Archive

1. Log in to your running 3.7.x production AccelOp virtual appliance as root.
2. Change the directory to `/root`.
3. Copy the migration script `ao-db-migration-4.2.1.tar` to the `/root` directory.
4. Untar the migration script.
5. Make sure that the owner of `ao-db-migration.sh` and `ao-db-migration-archiver.sh` files is root.
6. Run the archive script, specifying the directory where you want the archive file to be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```
7. Check that the archived files were successfully created in the destination directory. You should see two files, `cmdb-migration-*.tar`, which will be used to migrate the 3.7.x CMDB, and `opt-migration-*.tar`, which contains files stored outside of CMDM that will be needed to restore the upgraded CMDB to your new 4.2.1 virtual appliance.
8. Copy the `cmdb-migration-*.tar` file to the 3.7.x staging Supervisor, using the same directory name you used in Step 6.
9. Copy the `opt-migration-*.tar` file to the `/root` directory of the 4.2.1 Supervisor.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-  
migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Mounting the NFS Storage on Supervisors and Workers

Follow this process for each Supervisor and Worker in your deployment.

1. Log in to your virtual appliance as root over SSH.
2. Run the `mount` command to check the mount location.
3. Stop all FortiSIEM processes.

```
service crond stop  
phtools --stop all  
killall -9 phMonitor  
su - admin  
/opt/glassfish/bin/asadmin stop-domain  
exit  
service postgresql-9.1 stop  
service httpd stop
```

4. Unmount 4.2.1 NFS storage location.

```
umount /data
```

5. Mount back to the 3.7.x NFS storage location.

```
Usage: mount -t nfs -o nfsvers=3 <NFS_Server_IP>:<Mount_Path> /data  
ex: mount -t nfs -o nfsvers=3 192.168.67.168:/data/mig/SP61_376 /data
```

- Verify mount location on the Supervisor or Workers.

```
[root@SP421_from_376 ~]# mount
/dev/sda3 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda1 on /boot type ext3 (rw)
/dev/sdb1 on /cldb type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
192.168.65.91:/A0/mig/SP376_205 on /data type nfs (rw,nfsvers=3,addr=192.168.65.91)
[root@SP421_from_376 ~]#
[root@SP421_from_376 ~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/sda3                73G   4.9G   65G   8% /
tmpfs                    7.8G   0       7.8G   0% /dev/shm
/dev/sda1                124M   26M    93M   22% /boot
/dev/sdb1                60G   727M   56G   2% /cldb
192.168.65.91:/A0/mig/SP376_205
                        50G   37G   11G   78% /data
[root@SP421_from_376 ~]#
```

- Change to the 3.7.x mount path location in the `/etc/fstab` file on the Supervisor or Workers.

```
# /etc/fstab
# Created by anaconda on Fri Apr  4 22:34:44 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=8c2439d2-5c46-45ac-a669-8ea4c4a20913 /          ext3 defaults 1 1
UUID=4a2c534d-4027-4d36-ad62-c696c75d22c6 /boot      ext3 defaults 1 2
UUID=4a0debf8-feeb-4937-9909-7919e430d899 swap       swap defaults 0 0
tmpfs      /dev/shm          tmpfs defaults 0 0
devpts     /dev/pts          devpts gid=5,mode=620 0 0
sysfs      /sys              sysfs defaults 0 0
proc       /proc             proc defaults 0 0
/dev/sdb1 /cldb ext3 defaults 0 1
192.168.65.91:/A0/mig/SP376_205 /data      nfs defaults,nfsvers=3,noatime,nolock 0 0
~
```

- Reboot the Supervisor or Worker.

Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor

- In the vSphere client, power off the 3.7.x Supervisor.
The IP Address for the 3.7.x Supervisor will be transferred to the 4.2.1 Supervisor.
- Log in to the 3.7.x Supervisor as `root` over SSH.
- Run the `vami_config_net` script.
Your virtual appliance will reboot when the IP address change is complete.

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

Registering Workers to the Supervisor

- Log in to the Supervisor as `admin`.
- Go to **Admin > License Management**.
- Under **VA Information**, click **Add**, and add the Worker.
- Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as root over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating AWS EC2 Deployments

This section covers migrating FortiSIEM AWS EC2 based Virtual Appliances from 3.7.x to 4.2.1. Since FortiSIEM 4.2.1 has new CentOS version, the procedure is unlike a regular upgrade (say from 3.7.5 to 3.7.6) - certain special procedures have to be followed.

Very broadly, 3.7.6 CMDB have to be first migrated to a 4.2.1 CMDB on a 3.7.6 based system and then the migrated 4.2.1 CMDB has to be imported to a 4.2.1 system.

There are 4 choices based on

- NFS or a single Virtual appliance based deployment
- In-place or Staging based method is chosen for data migration

The various methods are explained later, but stated simply, staging approach take more hardware but minimizes downtime and CMDB migration risk compared to the in-place approach.

If in-place method is to be deployed, then a snapshot method is highly recommended for recovery purposes.

Note: Internet access is needed for migration to succeed. A third party library needs to access the schema website.

```
<faces-config xmlns="http://java.sun.com/xml/ns/javaee"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:cdk="http://jboss.org/schema/richfaces/cdk/extensions"
  version="2.0" metadata-complete="false"
  xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
  http://java.sun.com/xml/ns/javaee/web-facesconfig_2_0.xsd">
```

- [Migrating an AWS EC2 Local Disk-based Deployment](#)
- [Migrating an AWS EC2 NFS-based Deployment in Place](#)
- [Migrating an AWS EC2 NFS-based Deployment via a Staging System](#)

Migrating an AWS EC2 Local Disk-based Deployment

- [Overview](#)
- [Prerequisites](#)
- [Upgrading the 3.7.x CMDB to 4.2.1 CMDB](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Change Local Volumes for Your AWS Instances](#)
- [Change the IP Addresses Associated with Your Virtual Appliances](#)
- [Registering Workers to the Supervisor](#)
- [Setting the 4.2.1 SVN Password to the 3.7.x Password](#)

Overview

This migration process is for FortiSIEM deployment with a single virtual appliance and the CMDB data stored on a local AWS volume, and where you intend to run a 4.2.x version on the same physical machine as the 3.7.x version, but as a new virtual machine.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the User name and Password associated with your FortiSIEM license to access the scripts.

Upgrading the 3.7.x CMDB to 4.2.1 CMDB

1. Log in over SSH to your running 3.7.x virtual appliance as root.
2. Change the directory to `/root`.
3. Move or copy the migration script `ao-db-migration-4.2.1.tar` to `/root`.
4. Untar the migration script.
5. Run `ls -al` to check that `root` is the owner of the files `ao-db-migration.sh` and `ao-db-migration-archiver.sh`.
6. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command.

```
phtools --stop all
```
7. Run the archive script to create an archive version of the CMDB, and specify the directory where it should be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```
8. Check that the archive files `phoenixdb_migration_*` and `opt-migration-*.tar` were successfully created in the destination directory.
9. Copy the `opt-migration-*.tar` file to `/root`.
This contains various data files outside of CMDB that will be needed to restore the upgraded CMDB.
10. Run the migration script on the 3.7.x CMDB archive you created in step 7.
The first argument is the location of the archived 3.7.x CMDB, and the second argument is the location where the

migrated CMDB file will be kept.

```
/root/ao-db-migration.sh /tmp/376_archive/cmdb-migration-xyz /tmp/376_migration
```

11. Make sure the migrated files were successfully created.
12. Copy the migrated CMDB `phoenixdb_migration_xyz` file to the `/root` directory of your 4.2.1 virtual appliance
This file will be used during the CMDB restoration process.

Log in to the AWS EC2 dashboard and stop your 3.7.x virtual appliance.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Change Local Volumes for Your AWS Instances

1. Log in to AWS EC2 dashboard and power off your 4.2.1 virtual appliance.
2. In the Volumes table, find your production 3.7.x volume and tag it so you can identify it later, while also making a note of its **ID**.
For instance, `3.7.x_data_volume`.
3. **Detach** the volume.
4. In the **Volumes** tab, find your 4.2.1 volume, and **Detach** it.
5. Attach your 3.7.x volume to your 4.2.1 virtual appliance.

4.2.1 Volume Device Name

Make sure the Device name for your 4.2.1 volume is `dev/xvdf`.

6. Power on your 4.2.1 virtual appliance.
7. Stop all back-end processes and change the SVN URL and Server IP address in database by running these commands.

```
phtools --stop all
```

```
psql -U phoenix -d phoenixdb -c "update ph_sys_conf set value='https://<4.2.1-Private-IP-address>/repos/cmdb' where property='svn_url'"
psql -U phoenix -d phoenixdb -c "update ph_sys_server set ip_addr='<4.2.1-Private-IP-address>' where id='1'"
```

Change the IP Addresses Associated with Your Virtual Appliances

1. Log in to the AWS EC2 dashboard.
2. Click **Elastic IPS**, and then select the public IP associated with your 4.2.1 virtual appliance.

3. Click **Disassociate Address**, and then **Yes, Disassociate**.
4. In **Elastic IPs**, select the IP address associated with your 3.7.x virtual appliance.
5. Click **Disassociate Address**, and then **Yes, Disassociate**.
6. In **Elastic IPs**, select the production public IP of your 3.7.x virtual appliance, and click **Associate Address** to associate it with your 4.2.1 virtual appliance.
The virtual appliance will reboot automatically after the IP address is changed.

Registering Workers to the Supervisor

1. Log in to the Supervisor as admin.
2. Go to **Admin > License Management**.
3. Under **VA Information**, click **Add**, and add the Worker.
4. Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as root over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating an AWS EC2 NFS-based Deployment in Place

The steps for this process are:

- [Overview](#)
- [Prerequisites](#)
- [Upgrading the 3.7.x CMDB to 4.2.1 CMDB](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Mounting the NFS Storage on Supervisors and Workers](#)
- [Change the SVN URL and Server IP Address](#)
- [Change the IP Addresses Associated with Your Virtual Appliances](#)
- [Registering Workers to the Supervisor](#)
- [Setting the 4.2.1 SVN Password to the 3.7.x Password](#)

Overview

In this migration method, the production FortiSIEM systems are upgraded in-place, meaning that the production 3.7.x virtual appliance is stopped and used for migrating the CMDB to the 4.2.1 virtual appliance. The advantage of this approach is that no extra hardware is needed, while the disadvantage is extended downtime during the CMDB archive and upgrade process. During this downtime events are not lost but are buffered at the collector. However, incidents are not triggered while events are buffered. Prior to the CMDB upgrade process, you might want to take a snapshot of CMDB to use as a backup if needed.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Upgrading the 3.7.x CMDB to 4.2.1 CMDB

1. Log in over SSH to your running 3.7.x virtual appliance as root.
2. Change the directory to `/root`.
3. Move or copy the migration script `ao-db-migration-4.2.1.tar` to `/root`.
4. Untar the migration script.
5. Run `ls -al` to check that `root` is the owner of the files `ao-db-migration.sh` and `ao-db-migration-archiver.sh`.
6. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command.

```
phtools --stop all
```

7. Run the archive script to create an archive version of the CMDB, and specify the directory where it should be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```

8. Check that the archive files `phoenixdb_migration_*` and `opt-migration-*.tar` were successfully created in the destination directory.
9. Copy the `opt-migration-*.tar` file to `/root`.
This contains various data files outside of CMDB that will be needed to restore the upgraded CMDB.
10. Run the migration script on the 3.7.x CMDB archive you created in step 7.
The first argument is the location of the archived 3.7.x CMDB, and the second argument is the location where the migrated CMDB file will be kept.

```
/root/ao-db-migration.sh /tmp/376_archive/cmdb-migration-xyz /tmp/376_
migration
```

11. Make sure the migrated files were successfully created.
12. Copy the migrated CMDB `phoenixdb_migration_xyz` file to the `/root` directory of your 4.2.1 virtual appliance
This file will be used during the CMDB restoration process.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-
migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Mounting the NFS Storage on Supervisors and Workers

Follow this process for each Supervisor and Worker in your deployment.

1. Log in to your virtual appliance as root over SSH.
2. Run the `mount` command to check the mount location.
3. Stop all FortiSIEM processes.

```
service crond stop
phtools --stop all
killall -9 phMonitor
su - admin
/opt/glassfish/bin/asadmin stop-domain
exit
service postgresql-9.1 stop
service httpd stop
```

4. Unmount 4.2.1 NFS storage location.

```
umount /data
```

5. Mount back to the 3.7.x NFS storage location.

```
Usage: mount -t nfs -o nfsvers=3 <NFS_Server_IP>:<Mount_Path> /data
ex: mount -t nfs -o nfsvers=3 192.168.67.168:/data/mig/SP61_376 /data
```

6. Verify mount location on the Supervisor or Workers.

```
[root@SP421_from_376 ~]# mount
/dev/sda3 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda1 on /boot type ext3 (rw)
/dev/sdb1 on /cldb type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
192.168.65.91:/A0/mig/SP376_205 on /data type nfs (rw,nfsvers=3,addr=192.168.65.91)
[root@SP421_from_376 ~]#
[root@SP421_from_376 ~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/sda3                73G   4.9G   65G   8% /
tmpfs                    7.8G   0    7.8G   0% /dev/shm
/dev/sda1                124M   26M   93M  22% /boot
/dev/sdb1                60G   727M   56G   2% /cldb
192.168.65.91:/A0/mig/SP376_205
                        50G   37G   11G   78% /data
[root@SP421_from_376 ~]#
```

7. Change to the 3.7.x mount path location in the `/etc/fstab` file on the Supervisor or Workers.

```
# /etc/fstab
# Created by anaconda on Fri Apr  4 22:34:44 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=8c2439d2-5c46-45ac-a669-8ea4c4a20913 /                ext3    defaults    1 1
UUID=4a2c534d-4027-4d36-ad62-c696c75d22c6 /boot            ext3    defaults    1 2
UUID=4a0deb18-fee8-4937-9909-7919e430d899 swap             swap    defaults    0 0
tmpfs                    /dev/shm        tmpfs    defaults    0 0
devpts                   /dev/pts        devpts   gid=5,mode=620 0 0
sysfs                    /sys            sysfs    defaults    0 0
proc                     /proc           proc     defaults    0 0
/dev/sdb1 /cldb ext3 defaults 0 1
192.168.65.91:/A0/mig/SP376_205 /data           nfs     defaults,nfsvers=3,noatime,nolock 0 0
~
```

8. Reboot the Supervisor or Worker.

Change the SVN URL and Server IP Address

Run these commands.

```
phntools --stop all psql -U phoenix -d phoenixdb -c "update ph_sys_conf set
value='https://<4.2.1-Private-IP-address>/repos/cldb' where property='svn_url'" psql -U
phoenix -d phoenixdb -c "update ph_sys_server set ip_addr='<4.2.1-Private-IP-address>'
where id='1'"
```

Change the IP Addresses Associated with Your Virtual Appliances

1. Log in to the AWS EC2 dashboard.
2. Click **Elastic IPs**, and then select the public IP associated with your 4.2.1 virtual appliance.
3. Click **Disassociate Address**, and then **Yes, Disassociate**.

4. In **Elastic IPs**, select the IP address associated with your 3.7.x virtual appliance.
5. Click **Disassociate Address**, and then **Yes, Disassociate**.
6. In **Elastic IPs**, select the production public IP of your 3.7.x virtual appliance, and click **Associate Address** to associate it with your 4.2.1 virtual appliance.
The virtual appliance will reboot automatically after the IP address is changed.

Registering Workers to the Supervisor

1. Log in to the Supervisor as admin.
2. Go to **Admin > License Management**.
3. Under **VA Information**, click **Add**, and add the Worker.
4. Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as root over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating an AWS EC2 NFS-based Deployment via a Staging System

- [Overview](#)
- [Prerequisites](#)
- [Create the 3.7.x CMDB Archive](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Mounting the NFS Storage on Supervisors and Workers](#)
- [Change the IP Addresses Associated with Your Virtual Appliances](#)
- [Registering Workers to the Supervisor](#)
- [Setting the 4.2.1 SVN Password to the 3.7.x Password](#)

Overview

In this migration method, the production 3.7.x FortiSIEM systems are left untouched. A separate mirror image 3.7.x system is first created, and then upgraded to 4.2.1. The NFS storage is mounted to the upgraded 4.2.1 system, and the collectors are redirected to the upgraded 4.2.1 system. The upgraded 4.2.1 system now becomes the production system, while the old 3.7.6 system can be decommissioned. The collectors can then be upgraded one by one. The advantages of this method is minimal downtime in which incidents aren't triggered, and no upgrade risk. If for some reason the upgrade fails, it can be aborted without any risk to your production CMDB data. The disadvantages of this method are the requirement for hardware to set up the mirror 3.7.x mirror system, and longer time to complete the upgrade because of the time needed to set up the mirror system.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Create the 3.7.x CMDB Archive

1. Log in to your running 3.7.x production AccelOp virtual appliance as root.
2. Change the directory to `/root`.
3. Copy the migration script `ao-db-migration-4.2.1.tar` to the `/root` directory.
4. Untar the migration script.
5. Make sure that the owner of `ao-db-migration.sh` and `ao-db-migration-archiver.sh` files is root.
6. Run the archive script, specifying the directory where you want the archive file to be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```

7. Check that the archived files were successfully created in the destination directory. You should see two files, `cmdb-migration-*.tar`, which will be used to migrate the 3.7.x CMDB, and `opt-migration-*.tar`, which contains files stored outside of CMDM that will be needed to restore the upgraded CMDB to your new 4.2.1 virtual appliance.
8. Copy the `cmdb-migration-*.tar` file to the 3.7.x staging Supervisor, using the same directory name you used in Step 6.
9. Copy the `opt-migration-*.tar` file to the `/root` directory of the 4.2.1 Supervisor.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-  
migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Mounting the NFS Storage on Supervisors and Workers

Follow this process for each Supervisor and Worker in your deployment.

1. Log in to your virtual appliance as root over SSH.
2. Run the `mount` command to check the mount location.
3. Stop all FortiSIEM processes.

```
service crond stop  
phtools --stop all  
killall -9 phMonitor  
su - admin  
/opt/glassfish/bin/asadmin stop-domain  
exit  
service postgresql-9.1 stop  
service httpd stop
```

4. Unmount 4.2.1 NFS storage location.

```
umount /data
```

5. Mount back to the 3.7.x NFS storage location.

```
Usage: mount -t nfs -o nfsvers=3 <NFS_Server_IP>:<Mount_Path> /data  
ex: mount -t nfs -o nfsvers=3 192.168.67.168:/data/mig/SP61_376 /data
```

- Verify mount location on the Supervisor or Workers.

```
[root@SP421_from_376 ~]# mount
/dev/sda3 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda1 on /boot type ext3 (rw)
/dev/sdb1 on /cndb type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
192.168.65.91:/A0/mig/SP376_205 on /data type nfs (rw,nfsvers=3,addr=192.168.65.91)
[root@SP421_from_376 ~]#
[root@SP421_from_376 ~]# df -h
Filesystem              Size  Used Avail Use% Mounted on
/dev/sda3                73G   4.9G   65G   8% /
tmpfs                   7.8G   0    7.8G   0% /dev/shm
/dev/sda1               124M   26M   93M  22% /boot
/dev/sdb1                60G   727M   56G   2% /cndb
192.168.65.91:/A0/mig/SP376_205
                    50G   37G   11G  78% /data
[root@SP421_from_376 ~]# █
```

- Change to the 3.7.x mount path location in the `/etc/fstab` file on the Supervisor or Workers.

```
# /etc/fstab
# Created by anaconda on Fri Apr  4 22:34:44 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=8c2439d2-5c46-45ac-a669-8ea4c4a20913 / ext3 defaults 1 1
UUID=4a2c534d-4027-4d36-ad62-c696c75d22c6 /boot ext3 defaults 1 2
UUID=4a0debfb-feeb-4937-9909-7919e430d899 swap swap defaults 0 0
tmpfs /dev/shm tmpfs defaults 0 0
devpts /dev/pts devpts gid=5,mode=620 0 0
sysfs /sys sysfs defaults 0 0
proc /proc proc defaults 0 0
/dev/sdb1 /cndb ext3 defaults 0 1
192.168.65.91:/A0/mig/SP376_205 /data nfs defaults,nfsvers=3,noatime,nolock 0 0
~
```

- Reboot the Supervisor or Worker.

Change the IP Addresses Associated with Your Virtual Appliances

- Log in to the AWS EC2 dashboard.
- Click **Elastic IPs**, and then select the public IP associated with your 4.2.1 virtual appliance.
- Click **Disassociate Address**, and then **Yes, Disassociate**.
- In **Elastic IPs**, select the IP address associated with your 3.7.x virtual appliance.
- Click **Disassociate Address**, and then **Yes, Disassociate**.
- In **Elastic IPs**, select the production public IP of your 3.7.x virtual appliance, and click **Associate Address** to associate it with your 4.2.1 virtual appliance.
The virtual appliance will reboot automatically after the IP address is changed.

Registering Workers to the Supervisor

- Log in to the Supervisor as admin.
- Go to **Admin > License Management**.

3. Under **VA Information**, click **Add**, and add the Worker.
4. Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as root over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating KVM-based deployments

This section covers migrating FortiSIEM KVM based Virtual Appliances from 3.7.x to 4.2.1. Since FortiSIEM 4.2.1 has new CentOS version, the procedure is unlike a regular upgrade (say from 3.7.5 to 3.7.6) - certain special procedures have to be followed.

Very broadly, 3.7.6 CMDB have to be first migrated to a 4.2.1 CMDB on a 3.7.6 based system and then the migrated 4.2.1 CMDB has to be imported to a 4.2.1 system.

There are 4 choices based on

- NFS or a single Virtual appliance based deployment
- In-place or Staging or rsync based method is chosen for data migration

The various methods are explained later, but stated simply

- Staging approach take more hardware but minimizes downtime and CMDB migration risk compared to the in-place approach
- rsync method takes longer to finish as event database has to be copied

If in-place method is to be deployed, then a snapshot method is highly recommended for recovery purposes.

Note: Internet access is needed for migration to succeed. A third party library needs to access the schema website.

```
<faces-config xmlns="http://java.sun.com/xml/ns/javaee"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
xmlns:cdk="http://jboss.org/schema/richfaces/cdk/extensions"
version="2.0" metadata-complete="false"
xsi:schemaLocation="http://java.sun.com/xml/ns/javaee
http://java.sun.com/xml/ns/javaee/web-facesconfig_2_0.xsd">
```

Migrating a KVM Local Disc-based Deployment In Place

This process requires these steps:

- [Overview](#)
- [Prerequisites](#)
- [Upgrading the 3.7.x CMDB to 4.2.1 CMDB](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor](#)
- [Registering Workers to the Supervisor](#)

Overview

This migration process is for FortiSIEM deployment with a single virtual appliance and the CMDB data stored on a local VMware disk, and where you intend to run a 4.2.x version on the same physical machine as the 3.7.x version, but as a new virtual machine.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Use More Storage for Your 4.2.1 Virtual Appliance

Install the 4.2.1 virtual appliance on the same host as the 3.7.x version with a local disk that is larger than the original 3.7.x version. You will need the extra disk space for copying operations during the migration.

Upgrading the 3.7.x CMDB to 4.2.1 CMDB

1. Log in over SSH to your running 3.7.x virtual appliance as root.
2. Change the directory to `/root`.
3. Move or copy the migration script `ao-db-migration-4.2.1.tar` to `/root`.
4. Untar the migration script.
5. Run `ls -al` to check that `root` is the owner of the files `ao-db-migration.sh` and `ao-db-migration-archiver.sh`.
6. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command.

```
phtools --stop all
```
7. Run the archive script to create an archive version of the CMDB, and specify the directory where it should be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```
8. Check the that archive files `phoenixdb_migration_*` and `opt-migration-*.tar` were successfully created in the destination directory.

9. Copy the `opt-migration-*.tar` file to `/root`.
This contains various data files outside of CMDB that will be needed to restore the upgraded CMDB.
10. Run the migration script on the 3.7.x CMDB archive you created in step 7.
The first argument is the location of the archived 3.7.x CMDB, and the second argument is the location where the migrated CMDB file will be kept.

```
/root/ao-db-migration.sh /tmp/376_archive/cmdb-migration-xyz /tmp/376_
migration
```

11. Make sure the migrated files were successfully created.
12. Copy the migrated CMDB `phoenixdb_migration_xyz` file to the `/root` directory of your 4.2.1 virtual appliance
This file will be used during the CMDB restoration process.

Removing the Local Disk from the 3.7.x Virtual Appliance

1. Log in to your vSphere client.
2. Select your 3.7.x virtual appliance and power it off.
3. Open the **Hardware** properties for your virtual appliance.
4. Select **IDE Disk 2**, and then click **Remove**.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-
migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Adding the Local Disk to the 4.2.1 Virtual Appliance

1. Log in to Virtual Machine Manager.
2. Select your 4.2.1 virtual appliance and power it off.
3. Go the **Hardware** settings for your virtual appliance and select **IDE Disk 3**.
4. Click **Remove**.
5. Click **Add Hardware**.
6. Select **Storage**.
7. Select the option to use **managed or existing storage**, and then browse to the location of the detached 3.7.x disk.
8. Click **Finish**.
9. Select **Use an existing virtual disk**, and then click **Next**.
10. Browse to the location of the migrated virtual disk that was created by the migration script, and then click **OK**.
11. Power on the virtual appliance.

Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor

1. In the vSphere client, power off the 3.7.x Supervisor.
The IP Address for the 3.7.x Supervisor will be transferred to the 4.2.1 Supervisor.
2. Log in to the 3.7.x Supervisor as `root` over SSH.
3. Run the `vami_config_net` script.
Your virtual appliance will reboot when the IP address change is complete.

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

Registering Workers to the Supervisor

1. Log in to the Supervisor as `admin`.
2. Go to **Admin > License Management**.
3. Under **VA Information**, click **Add**, and add the Worker.
4. Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as `root` over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating a KVM Local Disk-based Deployment using an RSYNC Tool

This process requires these steps:

- [Overview](#)
- [Prerequisites](#)
- [Copy the 3.7.x CMDB to a 4.2.1 Virtual Appliance Using rsync](#)
- [Upgrading the 3.7.x CMDB to 4.2.1 CMDB](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor](#)
- [Registering Workers to the Supervisor](#)

Overview

This migration process is for FortiSIEM deployment with a single virtual appliance and the CMDB data stored on a local VMware disk, and where you intend to run the 4.2.1 version on a different physical machine as the 3.7.x version. This process requires these steps:

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Copy the 3.7.x CMDB to a 4.2.1 Virtual Appliance Using rsync

Installing rsynch

Before you can copy CMDB, you need to have rsync installed on the 3.7.x virtual appliance where you will be making the copy.

1. Log in to the 3.7.x Supervisor as root over SSH.
2. Copy `CentOS-Base.repo` to `/etc/yum.repos.d`.

```
cp /etc/yum.repos.d.orig/CentOS-Base.repo /etc/yum.repos.d
```

3. Install `rsync` yum repo.

```
yum install rsync
```

Procedure

1. Log in to the 4.2.1 virtual appliance as root.
2. Check the disk size in the remote system to make sure that there is enough space for the database to be copied over.
3. Copy the directory `/data` from the 3.7.x virtual appliance to the 4.2.1 virtual appliance using the rsync tool. rsync Command Syntax Make sure that the trailing `/` is used in the final two arguments in the rsync command

```
rsync --progress -av root@<3.7.x_VA_ip_address>:/data/ /data/
```

4. After copying is complete, make sure that the size of the event database is identical to the 3.7.x system.

Upgrading the 3.7.x CMDB to 4.2.1 CMDB

1. Log in over SSH to your running 3.7.x virtual appliance as root.
2. Change the directory to `/root`.
3. Move or copy the migration script `ao-db-migration-4.2.1.tar` to `/root`.
4. Untar the migration script.
5. Run `ls -al` to check that `root` is the owner of the files `ao-db-migration.sh` and `ao-db-migration-archiver.sh`.
6. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command.

```
phtools --stop all
```

7. Run the archive script to create an archive version of the CMDB, and specify the directory where it should be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```

8. Check that the archive files `phoenixdb_migration_*` and `opt-migration-*.tar` were successfully created in the destination directory.
9. Copy the `opt-migration-*.tar` file to `/root`.
This contains various data files outside of CMDB that will be needed to restore the upgraded CMDB.
10. Run the migration script on the 3.7.x CMDB archive you created in step 7.
The first argument is the location of the archived 3.7.x CMDB, and the second argument is the location where the migrated CMDB file will be kept.

```
/root/ao-db-migration.sh /tmp/376_archive/cmdb-migration-xyz /tmp/376_migration
```

11. Make sure the migrated files were successfully created.
12. Copy the migrated CMDB `phoenixdb_migration_xyz` file to the `/root` directory of your 4.2.1 virtual appliance.
This file will be used during the CMDB restoration process.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Assigning the 3.7.x Supervisor's IP Address to the 4.2.1 Supervisor

1. In the vSphere client, power off the 3.7.x Supervisor.
The IP Address for the 3.7.x Supervisor will be transferred to the 4.2.1 Supervisor.

2. Log in to the 3.7.x Supervisor as `root` over SSH.
3. Run the `vami_config_net` script.
Your virtual appliance will reboot when the IP address change is complete.

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

Registering Workers to the Supervisor

1. Log in to the Supervisor as `admin`.
2. Go to **Admin > License Management**.
3. Under **VA Information**, click **Add**, and add the Worker.
4. Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

1. Log in to the 4.2.1 Supervisor as `root` over SSH.
2. Change the directory to `/opt/phoenix/deployment/jumpbox`.
3. Run the SVN password reset script `./phsetsvnpwd.sh`
4. Enter the following full admin credential to reset SVN password
Organization: Super
User: admin
Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating a KVM NFS-based Deployment In Place

The steps for this process are:

- [Overview](#)
- [Prerequisites](#)
- [Upgrading the 3.7.x CMDB to 4.2.1 CMDB](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Mounting the NFS Storage on Supervisors and Workers](#)
- [Registering Workers to the Supervisor](#)

Overview

In this migration method, the production FortiSIEM systems are upgraded in-place, meaning that the production 3.7.x virtual appliance is stopped and used for migrating the CMDB to the 4.2.1 virtual appliance. The advantage of this approach is that no extra hardware is needed, while the disadvantage is extended downtime during the CMDB archive and upgrade process. During this downtime events are not lost but are buffered at the collector. However, incidents are not triggered while events are buffered. Prior to the CMDB upgrade process, you might want to take a snapshot of CMDB to use as a backup if needed.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Upgrading the 3.7.x CMDB to 4.2.1 CMDB

1. Log in over SSH to your running 3.7.x virtual appliance as root.
2. Change the directory to `/root`.
3. Move or copy the migration script `ao-db-migration-4.2.1.tar` to `/root`.
4. Untar the migration script.
5. Run `ls -al` to check that `root` is the owner of the files `ao-db-migration.sh` and `ao-db-migration-archiver.sh`.
6. For each FortiSIEM Supervisor, Worker, or Collector node, stop all backend processes by running the `phtools` command.

```
phtools --stop all
```
7. Run the archive script to create an archive version of the CMDB, and specify the directory where it should be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```
8. Check that the archive files `phoenixdb_migration_*` and `opt-migration-*.tar` were successfully created in the destination directory.
9. Copy the `opt-migration-*.tar` file to `/root`.
This contains various data files outside of CMDB that will be needed to restore the upgraded CMDB.

- Run the migration script on the 3.7.x CMDB archive you created in step 7.
The first argument is the location of the archived 3.7.x CMDB, and the second argument is the location where the migrated CMDB file will be kept.

```
/root/ao-db-migration.sh /tmp/376_archive/cmdb-migration-xyz /tmp/376_migration
```

- Make sure the migrated files were successfully created.
- Copy the migrated CMDB `phoenixdb_migration_xyz` file to the `/root` directory of your 4.2.1 virtual appliance
This file will be used during the CMDB restoration process.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

- Log in to your 4.2.1 virtual appliance as root.
- Change the directory to `/opt/phoenix/deployment/`.
- Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-migration-xyz.tar
```

- When the migration script completes the virtual appliance will reboot.

Mounting the NFS Storage on Supervisors and Workers

Follow this process for each Supervisor and Worker in your deployment.

- Log in to your virtual appliance as root over SSH.
- Run the `mount` command to check the mount location.
- Stop all FortiSIEM processes.

```
service crond stop
phtools --stop all
killall -9 phMonitor
su - admin
/opt/glassfish/bin/asadmin stop-domain
exit
service postgresql-9.1 stop
service httpd stop
```

- Unmount 4.2.1 NFS storage location.

```
umount /data
```

- Mount back to the 3.7.x NFS storage location.

```
Usage: mount -t nfs -o nfsvers=3 <NFS_Server_IP>:<Mount_Path> /data
ex: mount -t nfs -o nfsvers=3 192.168.67.168:/data/mig/SP61_376 /data
```

- Verify mount location on the Supervisor or Workers.

```
[root@SP421_from_376 ~]# mount
/dev/sda3 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda1 on /boot type ext3 (rw)
/dev/sdb1 on /cldb type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
192.168.65.91:/A0/mig/SP376_205 on /data type nfs (rw,nfsvers=3,addr=192.168.65.91)
[root@SP421_from_376 ~]#
[root@SP421_from_376 ~]# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/sda3                  73G       4.9G   65G   8% /
tmpfs                      7.8G       0       7.8G   0% /dev/shm
/dev/sda1                  124M       26M    93M  22% /boot
/dev/sdb1                   60G       727M    56G   2% /cldb
192.168.65.91:/A0/mig/SP376_205
                          50G       37G    11G  78% /data
[root@SP421_from_376 ~]# █
```

- Change to the 3.7.x mount path location in the `/etc/fstab` file on the Supervisor or Workers.
- Reboot the Supervisor or Worker.

Registering Workers to the Supervisor

- Log in to the Supervisor as admin.
- Go to **Admin > License Management**.
- Under **VA Information**, click **Add**, and add the Worker.
- Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

- Log in to the 4.2.1 Supervisor as root over SSH.
- Change the directory to `/opt/phoenix/deployment/jumpbox`.
- Run the SVN password reset script `./phsetsvnpwd.sh`
- Enter the following full admin credential to reset SVN password


```
Organization: Super
User: admin
Password:****
```

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully.

Migrating a KVM NFS-based Deployment via a Staging System

The steps in this process are:

- [Overview](#)
- [Prerequisites](#)
- [Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance](#)
- [Mounting the NFS Storage on Supervisors and Workers](#)
- [Registering Workers to the Supervisor](#)
- [Setting the 4.2.1 SVN Password to the 3.7.x Password](#)

Overview

In this migration method, the production 3.7.x FortiSIEM systems are left untouched. A separate mirror image 3.7.x system is first created, and then upgraded to 4.2.1. The NFS storage is mounted to the upgraded 4.2.1 system, and the collectors are redirected to the upgraded 4.2.1 system. The upgraded 4.2.1 system now becomes the production system, while the old 3.7.6 system can be decommissioned. The collectors can then be upgraded one by one. The advantages of this method is minimal downtime in which incidents aren't triggered, and no upgrade risk. If for some reason the upgrade fails, it can be aborted without any risk to your production CMDB data. The disadvantages of this method are the requirement for hardware to set up the mirror 3.7.x mirror system, and longer time to complete the upgrade because of the time needed to set up the mirror system.

Prerequisites

- Contact FortiSIEM Support to reset your license
- Take a snapshot of your 3.7.x installation for recovery purposes if needed
- Make sure the 3.7.x virtual appliance has Internet access
- Download the [4.2.1 migration scripts \(ao-db-migration-4.2.1.tar\)](#). You will need the Username and Password associated with your FortiSIEM license to access the scripts.

Create the 3.7.x CMDB Archive

1. Log in to your running 3.7.x production AccelOp virtual appliance as root.
2. Change the directory to `/root`.
3. Copy the migration script `ao-db-migration-4.2.1.tar` to the `/root` directory.
4. Untar the migration script.
5. Make sure that the owner of `ao-db-migration.sh` and `ao-db-migration-archiver.sh` files is root.
6. Run the archive script, specifying the directory where you want the archive file to be created.

```
./ao-db-migration-archiver.sh /tmp/376_archive/
```
7. Check that the archived files were successfully created in the destination directory. You should see two files, `cmdb-migration-*.tar`, which will be used to migrate the 3.7.x CMDB, and `opt-migration-*.tar`, which contains files stored outside of CMDM that will be needed to restore the upgraded CMDB to your new 4.2.1 virtual appliance.
8. Copy the `cmdb-migration-*.tar` file to the 3.7.x staging Supervisor, using the same directory name you used in Step 6.
9. Copy the `opt-migration-*.tar` file to the `/root` directory of the 4.2.1 Supervisor.

Restoring the Upgraded CMDB in a 4.2.1 Virtual Appliance

1. Log in to your 4.2.1 virtual appliance as root.
2. Change the directory to `/opt/phoenix/deployment/`.
3. Run the `post-ao-db-migration.sh` script with the 3.7.x migration files `phoenixdb_migration_xyz` and `opt-migration-*.tar`.

```
./post-ao-db-migration.sh /root/phoenixdb_migration_xyz /root/opt-  
migration-xyz.tar
```

4. When the migration script completes the virtual appliance will reboot.

Mounting the NFS Storage on Supervisors and Workers

Follow this process for each Supervisor and Worker in your deployment.

1. Log in to your virtual appliance as root over SSH.
2. Run the `mount` command to check the mount location.
3. Stop all FortiSIEM processes.

```
service crond stop  
phtools --stop all  
killall -9 phMonitor  
su - admin  
/opt/glassfish/bin/asadmin stop-domain  
exit  
service postgresql-9.1 stop  
service httpd stop
```

4. Unmount 4.2.1 NFS storage location.

```
umount /data
```

5. Mount back to the 3.7.x NFS storage location.

```
Usage: mount -t nfs -o nfsvers=3 <NFS_Server_IP>:<Mount_Path> /data  
ex: mount -t nfs -o nfsvers=3 192.168.67.168:/data/mig/SP61_376 /data
```

- Verify mount location on the Supervisor or Workers.

```
[root@SP421_from_376 ~]# mount
/dev/sda3 on / type ext3 (rw)
proc on /proc type proc (rw)
sysfs on /sys type sysfs (rw)
devpts on /dev/pts type devpts (rw,gid=5,mode=620)
tmpfs on /dev/shm type tmpfs (rw)
/dev/sda1 on /boot type ext3 (rw)
/dev/sdb1 on /cndb type ext3 (rw)
none on /proc/sys/fs/binfmt_misc type binfmt_misc (rw)
sunrpc on /var/lib/nfs/rpc_pipefs type rpc_pipefs (rw)
192.168.65.91:/A0/mig/SP376_205 on /data type nfs (rw,nfsvers=3,addr=192.168.65.91)
[root@SP421_from_376 ~]#
[root@SP421_from_376 ~]# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/sda3                  73G       4.9G   65G   8% /
tmpfs                      7.8G       0       7.8G   0% /dev/shm
/dev/sda1                  124M       26M    93M  22% /boot
/dev/sdb1                   60G       727M    56G   2% /cndb
192.168.65.91:/A0/mig/SP376_205
                          50G       37G    11G  78% /data
[root@SP421_from_376 ~]# █
```

- Change to the 3.7.x mount path location in the `/etc/fstab` file on the Supervisor or Workers.

```
# /etc/fstab
# Created by anaconda on Fri Apr  4 22:34:44 2014
#
# Accessible filesystems, by reference, are maintained under '/dev/disk'
# See man pages fstab(5), findfs(8), mount(8) and/or blkid(8) for more info
#
UUID=8c2439d2-5c46-45ac-a669-8ea4c4a20913 /          ext3 defaults 1 1
UUID=4a2c534d-4027-4d36-ad62-c696c75d22c6 /boot      ext3 defaults 1 2
UUID=4a0debf8-feeb-4937-9909-7919e430d899 swap       swap defaults 0 0
tmpfs      /dev/shm          tmpfs defaults 0 0
devpts     /dev/pts          devpts gid=5,mode=620 0 0
sysfs     /sys              sysfs defaults 0 0
proc      /proc             proc  defaults 0 0
/dev/sdb1 /cndb ext3 defaults 0 1
192.168.65.91:/A0/mig/SP376_205 /data      nfs defaults,nfsvers=3,noatime,nolock 0 0
~
```

- Reboot the Supervisor or Worker.

Registering Workers to the Supervisor

- Log in to the Supervisor as admin.
- Go to **Admin > License Management**.
- Under **VA Information**, click **Add**, and add the Worker.
- Under **Admin > Collector Health** and **Cloud Health**, check that the health of the virtual appliances is normal.

Setting the 4.2.1 SVN Password to the 3.7.x Password

- Log in to the 4.2.1 Supervisor as root over SSH.
- Change the directory to `/opt/phoenix/deployment/jumpbox`.
- Run the SVN password reset script `./phsetsvnpwd.sh`
- Enter the following full admin credential to reset SVN password
 - Organization: Super
 - User: admin
 - Password:****

Migration is now complete - Make sure all devices, user created rules, reports, dashboards are migrated successfully

Migrating Collectors

1. After migrating all your Supervisors and Workers to 4.2.1, install the 4.2.1 Collectors.
2. SSH to the 3.7.x Collector as root.
3. Change the directory to `/opt/phoenix/cache/parser/events`.
4. Copy the files from this directory to the same directory on the 4.2.1 system.
5. Change the directory to `/opt/phoenix/cache/parser/upload/svn`.
6. Copy the files from this directory to the same directory on the 4.2.1 system.
7. Power off the 3.7.x Collector.
8. SSH to the 4.2.1 Collector and change its IP address to the same as the 3.7.x Collector by running the `vami_config_net` script.

```
    /opt/vmware/share/vami/vami_config_net
```
9. In a browser, navigate to `https://<4.2.1_Collector_IP_address>:5480` and fill in the administration information to complete the Collector setup/

Migrating the SVN Repository to a Separate Partition on a Local Disk

If you are using NFS storage, your SVN repository will be migrated to a local disk to improve performance and reliability. If you are using local storage only, the SVN repository will be moved out of the `/data` partition and into an `/svn` partition.

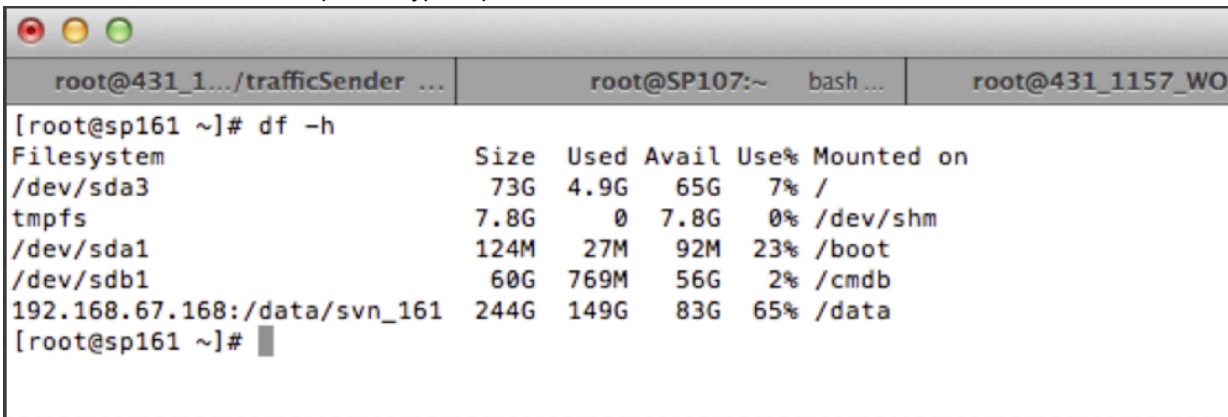
60 GB Local Disk Storage Required

You must have 60 GB of local storage on Supervisor node available for the SVN repository migration. Please create a new virtual disk size with a size of 60 GB before starting the SVN migration.

1. SSH as `root` into the Supervisor node where you want to run the SVN migration.

```
ssh root@<Super IP>
```

2. Run `df -h` to see if an `/svn` partition does NOT exist. The migration script is going to create that partition. This screenshot shows an expected typical partition structure.



```

root@431_1.../trafficSender ... | root@SP107:~ bash ... | root@431_1157_WO
[root@sp161 ~]# df -h
Filesystem                Size      Used Avail Use% Mounted on
/dev/sda3                  73G       4.9G   65G   7% /
tmpfs                      7.8G       0    7.8G   0% /dev/shm
/dev/sda1                  124M       27M    92M  23% /boot
/dev/sdb1                   60G       769M    56G   2% /cldb
192.168.67.168:/data/svn_161 244G     149G    83G  65% /data
[root@sp161 ~]#

```

3. Download `ao-svn-migration.sh` script from image server. (<https://images.FortiSIEM.net/upgrade/va/4.3.1>)
4. Copy or move the `ao-svn-migration.sh` script to `/root`.
5. Run `ls -al` to check that `root` is the owner of `ao-svn-migration.sh`.
6. Run `chmod` to change the permissions on `ao-svn-migration.sh` to `755`: `chmod 755 ao-svn-migration`
7. Reboot the machine.
8. Log into the Supervisor as `root`.
9. Run `ao-svn-migration.sh`.


```
. /ao-svn-migration
```
10. When the script executes, you will be asked to confirm that you have 60GB of local storage available for the migration. When the script completes, you will see the message `Upgrade Completed. SVN disk migration done.`
11. Run `df -h` to confirm that the `/svn` partition was completed.

Special pre-upgrade instruction for 4.3.3

1. SSH as root into the Supervisor node
2. Download "phupdateinstall-4.3.3.sh" script
3. Copy or move the phupdateinstall-4.3.3.sh script to /root
4. Run chmod to change the permissions on phupdateinstall-4.3.3.sh to 755: `chmod 755 phupdateinstall-4.3.3.sh`
5. Run phupdateinstall-4.3.3.sh: `./phupdateinstall-4.3.3.sh`
6. Repeat step 1 to 5 on Worker/s and Report Server node

Special pre-upgrade instruction for 4.6.1

Instructions for Supervisor node

Run the following command as root:

```
rpm -e vmware-jre
```

Instructions for Collector nodes

Run the following command as root on each collector prior to upgrading the collector from the GUI, or the upgrade will fail:

```
mkdir -p /opt/phoenixphscripts/bin  
ln -sf /opt/phoenix/phscripts/bin/phcollectorimageinstaller.py  
/opt/phoenixphscripts/bin/phcollectorimageinstaller.py
```

Enabling TLS 1.2 Patch On Old Collectors

Older FortiSIEM collectors 4.5.2 or earlier running JDK 1.7 do not have TLS 1.2 enabled. To enable them to communicate to FortiSIEM 4.6.3, follow these steps

1. SSH to Collector and edit `/opt/phoenix/bin/runJavaAgent.sh`
2. Enable TLS v1.2 option.

```
exec ${JAVA_HOME}/bin/java $initialJobXML -  
Djava.library.path=/opt/phoenix/lib64 -  
Dhttps.protocols=SSLv3,TLSv1,TLSv1.1,TLSv1.2 -classpath ${MY_CLASS_PATH} -  
Xmx2048M com.ph.phoenix.agent.AgentMain "$@"
```

3. Save changes, restart Java and phAgentManager:

```
killall -9 java  
killall -9 phAgentManager
```

Upgrading to 4.6.3 for TLS 1.2

Enforcing TLS 1.2 requires that the following steps be **followed in strict order** for upgrade to succeed.

Additional steps for TLS 1.2 compatibility are marked in bold.

1. Remove/etc/yum.repos.d/accelops* and **Run "yum update" on Collectors, Worker(s)**, Supervisor and to get all TLS 1.2 related libraries up to date. Follow this yum update order **Collectors → Worker(s) → Supervisor**.
2. If your environment has a collector and it is running FortiSIEM 4.5.2 or earlier (with JDK 1.7), then first patch the Collector for TLS 1.2 compatibility (see [here](#)). This step is not required for Collectors running FortiSIEM 4.6.1 or later.
3. Pre-upgrade step for upgrading Supervisor: Stop FortiSIEM (previously FortiSIEM) processes all Workers by running "phtools --stop ALL". Collectors can be up and running. This is to avoid build up of report files.
4. Upgrade Supervisor following usual steps.
5. If your environment has Worker nodes, Upgrade Workers following usual steps.
6. If your environment has FortiSIEM Windows Agents, then upgrade Windows Agent Manager from 1.1 to 2.0. Note **there are special pre-upgrade steps to enable TLS 1.2** (see [here](#)).
7. If your environment has Collectors, upgrade Collectors following usual steps.

Setting Up the Image Server for Collector Upgrades

If you want to upgrade a multi-tenant deployment that includes Collectors, you must set up and then specify an image server that will be used as a repository for the Collector upgrade files. You can use a standard HTTP server for this purpose, but there is a preferred directory structure for the server. These instructions describe how to set up that structure, and then add a reference to the image server in your Supervisor node.

Setting Up the Image Server Directories

1. Log into the image server with Admin rights.
2. Create the directory `images/collector/upgrade`.
3. Go to <https://images-cdn.fortisiem.fortinet.com/VirtualAppliances/latestrelease.html>. Scroll down to the 'Upgrade packages' section and download the latest collector image upgrade file to `images/collector/upgrade`.

4. Untar the file. You should see a set of files that looks like this:

```
[image]# tar xvf /root/CO-4.3.3.1189.tar CO-4.3.3.1189/ CO-4.3.3.1189/RPM-GPG-KEY CO-4.3.3.1189/FortiSIEM-collector-4.3.3.1189.rpm CO-4.3.3.1189/repdata/ CO-4.3.3.1189/repdata/other.xml.gz CO-4.3.3.1189/repdata/filelists.xml.gz CO-4.3.3.1189/repdata/primary.xml.gz CO-4.3.3.1189/repdata/repomd.xml
```

5. Use the `ln` command to create a symbolic link to the latest directory.

```
/bin/ln -sf /images/collector/upgrade/CO-x.x.x.xxxx  
/images/collector/upgrade/latest
```

6. Make sure a directory tree structure like this is created in the `images` directory before proceeding:

```
/images/collector/upgrade/CO-x.x.x.xxxx  
/FortiSIEM-collector-x.x.x.xxxx.rpm/RPM-GPG-KEY/repdata  
/filelists.xml.gz  
/other.xml.gz/primary.xml.gz  
/repomd.xml
```

7. Create a link from the image directories to the webserver html pages.

```
/bin/ln -sf /images/collector/upgrade/latest  
/var/www/html/vms/collector/upgrade/latest
```

8. Test the image server locations by entering one of the following addresses into a browser:

- <http://images.myserver.net/vms/collector/upgrade/latest/>
- <https://images.myserver.net/vms/collector/upgrade/latest/>

Setting the Image Server in the Supervisor

1. Log in to your Supervisor node.
2. Go to **Admin > General Settings > System**.
3. Under **Image Server**, enter the URL or IP address for your image server.
4. Enter the authentication credentials for your image server.
5. Click **Save**.

Upgrading a FortiSIEM Single Node Deployment

These instructions cover the upgrade process for FortiSIEM Enterprise deployment with a single Supervisor.

1. Using SSH, log in to the FortiSIEM virtual appliance as the root user.
2. Change to the `pbin` directory:
`cd /pbin`
3. Run the command to download the image:
`./phdownloadimage <userID> <password> <downloadUrl>`

Note: You can enter any values in the User id and password fields. These values are not linked to any account.

Example command to download the upgrade image:

```
./phdownloadimage <userID> <password> <https://images-cdn.fortisiem.fortinet.com/VirtualAppliances/4.10.0/upgrade/4.9.0-4.10.0/va/4.10.0.1102>
```

4. Select **Yes** to confirm the download.
The console will show the progress of the download.
Do Not Stop the Download Process: It takes 40 - 60 minutes to download the upgrade image depending on network traffic. Do not stop the download process manually.
5. After the download completes, run this command to upgrade your virtual appliance: `./phupgradeimage`
Do Not Stop the Upgrade Process:
The system upgrade takes 10 - 30 minutes depending on the size of your databases and system resources. Do not stop the upgrade process manually. Your console will display the progress of the upgrade process.
6. When the upgrade process is complete, your FortiSIEM virtual appliance will reboot.
7. Log in to your virtual appliance, and in the **Admin > Cloud Health** page, check that you are running the upgraded version of FortiSIEM.

Upgrading a FortiSIEM Cluster Deployment

- [Overview](#)
- [Upgrading Supervisors and Workers](#)
- [Upgrading Collectors](#)

Overview

Follow these steps while upgrading a VA cluster

1. Shutdown all Workers. Collectors can be up and running.
2. Upgrade Super first (while all workers are shutdown)
3. After Super is up and running, upgrade worker one by one.
4. Upgrade collectors

Step #1 prevents the accumulation of Report files while Super is not available during upgrade (#2). If these steps are not followed, Supervisor may not be able to come up after upgrade because of excessive unprocessed report file accumulation.

Note: Both Super and Worker MUST be on the same FortiSIEM version, else various software modules may not work properly. However, Collectors can be in older versions - they will work except that they may not have the latest discovery and performance monitoring features in the Super/Worker versions. So FortiSIEM recommends that you also upgrade Collectors within a short period of time. If you have Collectors in your deployment, make sure you have [configured an image server](#) to use as a repository for the Collector

Upgrading Supervisors and Workers

For both Supervisor and Worker nodes, follow the upgrade process described here, but be sure to upgrade the Supervisor node first.

1. Using SSH, log in to the FortiSIEM virtual appliance as the root user.
2. Change to the `pbin` directory. Run the command to download the upgrade image.
`./phdownloadimage <userID> <password> <downloadUrl>`

Note: You can enter any values in the User id and Password fields. These are not linked to any account.

Example command to download the upgrade image:

```
./phdownloadimage <userID> <password> <https://images-cdn.fortisiem.fortinet.com/VirtualAppliances/4.10.0/upgrade/4.9.0-4.10.0/va/4.10.0.1102>
```

3. Select `Yes` to confirm the download.
4. The console will show the progress of the download. Do Not Stop the Download Process. It takes 40 - 60 minutes to download the upgrade image depending on network traffic. Do not stop the download process manually.
5. After the download completes, run this command to upgrade your virtual appliance.

```
./phupgradeimage
```

Do Not Stop the Upgrade Process: The system upgrade takes 10 - 30 minutes depending on the size of your databases and system resources. Do not stop the upgrade process manually.

Your console will display the progress of the upgrade process. When the upgrade process is complete, your FortiSIEM virtual appliance will reboot.

6. Log in to your virtual appliance, and in the **Admin > Cloud Health** page, check that you are running the upgraded version of FortiSIEM.

Upgrading Collectors

The process for upgrading Collectors is similar to the process for Supervisors and Workers, but you must initiate the Collector process from the Supervisor.

1. Log in to the Supervisor node as an administrator.
2. Go to **Admin > General Settings**
3. Under **Image Server Settings**, enter the download path to the upgrade image, and the **Username** and **Password** associated with your license.
4. Go to **Admin > Collector Health**.
5. Click **Download Image**, and then click **Yes** to confirm the download.
As the download progresses you can click **Refresh** to check its status.
6. When **Finished** appears in the **Download Status** column of the **Collector Health** page, click **Install Image**.
The upgrade process will begin, and when it completes, your virtual appliance will reboot. The amount of time it takes for the upgrade to complete depends on the network speed between your Supervisor node and the Collectors.
7. When the upgrade is complete, make sure that your Collector is running the upgraded version of FortiSIEM.

Upgrading FortiSIEM Windows Agent and Agent Manager

- Upgrade from V1.0 to V1.1
- Upgrade from V1.1 to V2.0
- Upgrading Windows Agent License
- Uninstalling Agents

Upgrade from V1.0 to V1.1

Version 1.0 and 1.1 Backward Incompatibility

Note 1.0 Agents and Agent Managers communicate only over HTTP while 1.1 Agents and Agent Managers communicate only over HTTPS. Subsequently, 1.1 Agents and Agent managers are not backward compatible with 1.0 Agents and Agent Managers. You have to completely upgrade the entire system of Agents and Agent Managers.

1. Uninstall V1.0 Agents
2. Close V1.0 Agent Manager Application.
3. Uninstall V1.0 Agent Manager
4. Bind Default Website with HTTPS as described in Pre-requisite in [Installing FortiSIEM Windows Agent Manager](#).
5. Install V1.1 Agent Manager following [Installing FortiSIEM Windows Agent Manager](#).
 - a. In Database Settings dialog, enter the V1.0 database path as the "FortiSIEM Windows Agent Manager" SQL Server database path (Procedures Step 6 in [Installing FortiSIEM Windows Agent Manager](#)).
 - b. Enter the same Administrator username and password (as the previous installation) in the Agent Manager Administrator account creation dialog
6. Install V1.1 Agents
7. Assign licenses again. Use the Export and Import feature.

Upgrade from V1.1 to V2.0

Windows Agent Manager

1. **Enable TLS 1.2 on Agent Manager** - FortiSIEM Supervisor/Worker 4.6.3 and above enforces the use of TLS 1.2 for tighter security. However, by default only SSL3 / TLS 1.0 is enabled in Windows Server 2008-R2. Therefore, enable TLS 1.2 for Windows Agent Manager 2.0 for operating with FortiSIEM Supervisor/Worker 4.6.3 and above.
 - a. Start elevated Command Prompt (i.e., with administrative privilege) to Windows Agent Manager 1.1.
 - b. Run the following commands sequentially as shown.

```
REG ADD
"HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.1\Client" /v DisabledByDefault /t REG_DWORD /d
00000000 REG ADD
"HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.1\Server" /v DisabledByDefault /t REG_DWORD /d
00000000 REG ADD
```

```
"HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.2\Client" /v DisabledByDefault /t REG_DWORD /d
00000000 REG ADD
"HKLM\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL
\Protocols\TLS 1.2\Server" /v DisabledByDefault /t REG_DWORD /d
00000000
```

- c. Restart computer
2. Uninstall Agent Manager 1.1
3. Install SQL Server 2012-SP1 Feature Pack on Agent manager available at <https://www.microsoft.com/en-in/download/details.aspx?id=35580>.
 - a. Select the language of your choice and mark the following two MSIs (choose x86 or x64 depending on your platform) for download:
 - i. SQLSysClrTypes.msi
 - ii. SharedManagementObjects.msi
 - b. Click on the Download button to download those two MSIs. Then double-click on those MSIs to install those one by one.
4. Install Agent Manager 2.0
 - a. In Database Settings dialog, set the old database path as FortiSIEMCAC database path.
 - b. Enter the same Administrator username and password (as in the previous installation) in the new Agent Manager Administrator account creation dialog.
5. Run Database migration utility to convert from 1.1 to 2.0
 - a. Open a Command Prompt window
 - b. Go to the installation directory (say, C:\Program Files\AccelOps\Server)
 - c. Run AOUpdateManager.exe with script.zip as the command line parameter. You will find script.zip alongside the MSI.

Windows Agent

1. Uninstall V1.0 Agents
2. Install Agents

Upgrading Windows Agent License

Follow these steps if you have bought additional Windows Agent licenses or extended the term of the license.

1. Login to FortiSIEM Supervisor using admin account
2. Go to **Admin > License Management** and make sure that the license is updated
3. Go to **Admin > Setup Wizard > Windows Agent**
4. Edit each **Windows Agent Manager** entry and modify the agent count and license expiry date if needed

The new license will be automatically pushed to each Windows Agent Manager. You can now logon to each Windows Agent Manager and allocate the additional licenses if needed.

Uninstalling Agents

Single Agent

- Simply uninstall like a regular Windows service

Multiple Agents using Group Policy

1. Go to the **Group Policy** you created during Agent installation. Right click and select **Edit**.
2. In the **Group Policy Management Editor**, go to **MyGPO > Computer Configuration > Policies > Software Settings > Software Installation**
3. Right click on **FortiSIEM Windows Agent <version>**
4. Click **All Tasks > Remove**
5. In **Remove Software** dialog, choose the option **Immediately uninstall the software from users and computers**. Then click **OK**.
6. The **FortiSIEM Windows Agent <version>** entry will disappear from the right pane. Close the **Group Policy Management Editor**.
7. Force the group policy update
 - a. On Domain Controller > cmd, run gpupdate /force
 - b. On Agent server > cmd, run gpupdate
8. Restart each Agent Computer to complete the uninstall.

Automatic OS Upgrades during Reboot

In order to patch CentOS and system packages for **security updates** as well as bugfixes and make the system on-par with a fresh installed FortiSIEM node, the following script is made available. Internet connectivity to CentOS mirrors should be working in order for the following script to be successful, otherwise the script will print an error and exit. This script is available on all nodes starting from 4.6.3: Supervisor, Workers, Collectors, and Report Server

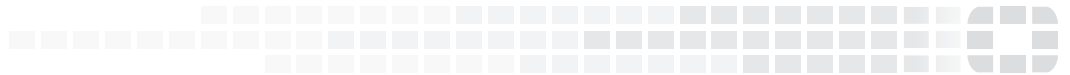
```
/opt/phoenix/phscripts/bin/phUpdateSystem.sh
```

The above script is also invoked during **system boot up** and is invoked in the following script:

```
/etc/init.d/phProvision.sh
```

This ensures that the node is up to date right after an upgrade and system reboot. If you are running a node that was first installed in an older release and upgraded to 4.6.3, then there are many OS/system packages that will be downloaded and installed the first time. Therefore, upgrade time is longer than usual. On subsequent upgrades and reboots, the updates will be small.

Nodes that are deployed in bandwidth constrained environments can disable this by commenting out the line `phUpdateSystem.sh` in `phProvision.sh` above. However, it is **strongly recommended** to keep this in-place to ensure that your node has security fixes from CentOS and minimize the risk of an exploit. Alternatively, in bandwidth constrained environments, you can deploy a freshly installed collector to ensure that security fixes are up to date.



Copyright© 2017 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.