FortiSIEM - AWS Installation Guide

Version 5.2.5

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

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

FEEDBACK
Email: techdoc@fortinet.com

11/11/2019
FortiSIEM 5.2.5 AWS Installation Guide

TABLE OF CONTENTS

Change Log **4**
Installing FortiSIEM on AWS **5**
Pre-installation check-list 5
Step A: Determine your FortiSIEM hardware needs and deployment type 5
Step B: Deploy Remote Storage 5
Step C: Setup Amazon Virtual Public Cloud (VPC) 5
Installing FortiSIEM Virtual Appliance on AWS 6
Step 1: Launch FortiSIEM Supervisor from AWS Marketplace 6
Step 2: Start and Configure FortiSIEM 7
Step 3: Upload the FortiSIEM License on Supervisor 7
Step 4: Choose FortiSIEM Event Database Storage 8
Step 5: (Optional) Install Workers and Add to Supervisor Node 8
Step 6: (Optional) Install Collectors 8
Step 7: (Optional) Register Collectors to Supervisor Node 8
Installing FortiSIEM Report Server on AWS 10
Step 1: Launch FortiSIEM Supervisor from AWS Marketplace 10
Step 2: Start and Configure FortiSIEM 11
Step 3: Register FortiSIEM Report Server to Supervisor 11
Step 4: Sync Reports from FortiSIEM Supervisor to the Report Server 12

Change Log

Date	Change Description
05/09/2019	Initial version of FortiSIEM - AWS Installation Guide
03/22/2019	Revision 2 updated instructions for Service Provider deployments.
11/11/2019	Revision 3: small change to installation instructions for FortiSIEM and FortiSIEM REport Server.

Installing FortiSIEM on AWS

This document provides instructions to install FortiSIEM Virtual Appliance and FortiSIEM Report Server on Amazon Web Services (AWS).

- Pre-installation check-list
- Installing FortiSIEM Virtual Appliance on AWS
- Installing FortiSIEM Report Server on AWS

Pre-installation check-list

Step A: Determine your FortiSIEM hardware needs and deployment type

Before you begin, check the following:

1. Number of Workers needed, if any.
2. Number of Collectors needed, if any.
3. Hardware specification of Supervisor, Worker and Collectors (CPU, RAM, Local Storage)

If Elasticsearch is chosen as the Event Database, the Supervisor needs an additional 8 GB RAM - in this case, the minimum requirement of the Supervisor is 32 GB RAM.

4. Event Database Storage – Local or Remote (For Remote - NFS or Elasticsearch)
   Note: Remote option is required if you are deploying Workers. If you are going to add Workers in the future, then it is recommended to choose a Remote database option to avoid data migration.
5. Deployment type – Enterprise or Service Provider

Step B: Deploy Remote Storage

If required, install and configure NFS or Elasticsearch before beginning the installation below:

- *For NFS deployment, see here.*
- *For Elasticsearch deployment, see here.*

Step C: Setup Amazon Virtual Public Cloud (VPC)

You must set up a Virtual Public Cloud (VPC) in Amazon Web Services for FortiSIEM deployment.

1. Keep private IPs across reboot.
2. Specify private IPs of your choice within that subnet range.

Installing FortiSIEM Virtual Appliance on AWS

Installation scripts, such as, `/opt/phoenix/deployment/jumpbox/aws/pre-deployment.sh` are not available in FortiSIEM 5.0.0 and later releases because they are no longer needed. Use `vami_config_net` script instead, similar to other platforms.

Follow the steps below to install the FortiSIEM Virtual Appliance on AWS:

Step 1: Launch FortiSIEM Supervisor from AWS Marketplace

1. Logon to your AWS account.
2. Go to **Services** > **Compute** > **EC2**.
3. Click **EC2 Dashboard** > **Launch Instance** and **Select AWS Marketplace**.
4. Search for 'FortiSIEM'.
5. Select **Fortinet FortiSIEM-VM** and click **Continue**.
6. Choose an instance type based on Step A.
7. Configure the Instance details:
   a. Choose the **number of instances** as the sum of number of Supervisor and Worker nodes.
   b. Choose **Network** as the VPC selected in Step C.
   c. Choose **Subnet** as the subnet where you want to launch FortiSIEM VMs.
   d. Set **Auto-assign public IP** as 'Disabled'.
   e. Set **Shutdown behavior** as Stop.
   f. Check **Enable termination protection**.
   g. In Network Interfaces, choose the Primary IP as the Private IP of your choice within that subnet.
   h. Click **Add Storage**.
   You can keep the defaults for root partition, CMDB and SVN. If you want the local storage for event data, add a new EBS volume based on your storage requirements (minimum 50GB).
   i. Click **Add Tags**. You can add a tag similar to “FortiSIEM Supervisor” to search the instance.
   j. Click **Configure Security Group** and create a new **Security Group**.
   Retain the defaults which are needed for FortiSIEM to operate.
   k. Click **Review and Launch** and click **Launch**.
   l. Select **Create a new key pair** and provide a **key pair name** of your choice.
   m. Click **Download Key Pair** and save the `.pem` file.
   n. Click **Launch Instance** and wait for the instance to start.
8. Configure **Elastic IP**:
   a. Go to **EC2 Dashboard** > **Elastic IPs**.
   b. Click **Allocate New Address**.
   c. Select **VPC** and click **Allocate**.
   The IP address will be allocated.
   d. Click the **Elastic IP** that was allocated.
   e. Click **Actions** > **Associate address** and select the instance by searching the tag you created in Step 7i.
   f. Click **Associate**.

Step 2: Start and Configure FortiSIEM

Do not press any control keys (for example - Ctrl-C or Ctrl-Z) while configuring the virtual appliances, as this may cause the installation process to stop. If this happens, you must erase the virtual appliance and start the installation process again.

1. SSH into Supervisor console using the keys in Step 7m.
   For details about connecting to the instance, see here.
2. Become the root user. Run the command `sudo su -`.
3. Run the script `/opt/vmware/share/vami/vami_set_timezone` to set the time zone.
4. Run the script `/opt/vmware/share/vami/vami_config_net` to configure the network.
   You must keep all the default values except host name.
5. Based on your network type, enter one of the options below:
   - **1** for **IPv6 Network Only**
     - When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, and IPv6 DNS Server(s).
   - **2** for **IPv4 Network Only**
     - When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Netmask, IPv4 Gateway, and IPv4 DNS Server(s).
   - **3** for **Both Networks**
     i. When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, IPv6 DNS Server(s).
     ii. Follow Step 5 below to turn off the proxy server and continue with step c.
     iii. When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Prefix, IPv4 Gateway, IPv4 DNS Server(s).
6. Enter **n**. **Note**: The authenticated proxy server is not supported in this version of FortiSIEM. You must turn off the proxy server authentication or completely disable the proxy for the AWS host.
7. Enter **y** to accept the network configuration settings.
8. For Supervisor and Worker: You will be prompted to choose Supervisor [s] or Worker [w].
   Choose accordingly:
   a. For Supervisor, the system will initialize the PostGreSQL database which will take around 20 minutes and then reboot the system. A few minutes after reboot, the system GUI will be ready to upload license and configure the Event Database Storage option.
   b. For a Worker node, the system will reboot quickly and a few minutes after reboot, it will be ready to be added as a Worker from the Supervisor GUI.
9. For Collector, the system will reboot and after a few minutes it will be ready.

Step 3: Upload the FortiSIEM License on Supervisor

You will now be asked to input a license.

1. Click **Browse** and upload the license file.
   Make sure that the 'Hardware ID' shown in the **License Upload** page matches the license.
2. For **User ID** and **Password**, choose any 'Full Admin' credentials.
   For the first time, install by choosing user as 'admin' and password as 'admin*1'

3. Choose **License type** as 'Enterprise' or 'Service Provider'.
   This option is available only on first install. Once the database is configured, this option will not be available.

Step 4: Choose FortiSIEM Event Database Storage

For fresh installation, you will be taken to the Event Database Storage page. Based on Step-B, you will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options.

For more details, see here.

Step 5: (Optional) Install Workers and Add to Supervisor Node

1. Follow Steps 1 and 2 to configure a Worker.
2. Add the Worker node to the Supervisor by visiting **ADMIN** > **License** > **Nodes** > **Add**.
3. See **ADMIN** > **Health** > **Cloud Health** to ensure that the Workers are up, healthy and properly added to the system.

Step 6: (Optional) Install Collectors

Collectors can be installed as Virtual Appliances or Hardware appliances (FSM-500F). For AWS based Virtual Appliances, set up the Collector by following Steps 1 and 2 above, except search for FortiSIEM-Collector – VM in AWS marketplace.

Step 7: (Optional) Register Collectors to Supervisor Node

For Enterprise deployments, follow these steps.

1. Login to Supervisor with 'Admin' privileges.
2. Go to **ADMIN** > **Setup** > **Collectors** and add a Collector by entering:
   a. **Name** – Collector Name
   b. **Guaranteed EPS** – this is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time** and **End Time** – set 'Unlimited'.
3. To address security vulnerabilities with lighttpd port 5480, Collectors cannot be registered to Supervisor via GUI. Instead, Collectors must be registered by running this script:
   `phProvisionCollector --add <user> <password> <super IP or host> <organization> <collectorName>`
   where `user` and `password` are the admin User Name and password for the Supervisor, `super IP or host` is 'Supervisor IP', `organization` is 'Super' , and collectorName is the **Name** from Step 2a.
4. Go to **ADMIN** > **Health** > **Collector Health** and see the status.

For Service Provider deployments, follow these steps.

1. Login to Supervisor with 'Admin' privileges.
2. Go to **ADMIN** > **Setup** > **Organizations** and add an Organization.

3. Enter the **Organization Name**, **Admin User**, **Admin Password**, and **Admin Email**.
4. Under **Collectors**, click **New**.
5. Enter the **Collector Name**, **Guaranteed EPS**, **Start Time**, and **End Time**. The last two values could be set as 'Unlimited'. Guaranteed EPS is the EPS that Collector will always be able to send. It could send more if there is excess EPS available.
6. To address security vulnerabilities with lighttpd port 5480, Collectors cannot be registered to Supervisor by using the GUI. Instead, Collectors must be registered by running this script:
   `phProvisionCollector --add <user> <password> <super IP or host> <organization> <collectorName>`
7. Go to **ADMIN** > **Health** > **Collector Health** and check the status.

Installing FortiSIEM Report Server on AWS

Installation scripts, such as, `/opt/phoenix/deployment/jumpbox/aws/pre-deployment.sh` are not available in FortiSIEM 5.0.0 and later releases because they are no longer needed. Use `vami_config_net` script instead, similar to other platforms.

Follow the steps below to install the FortiSIEM Report Server on AWS:

Step 1: Launch FortiSIEM Supervisor from AWS Marketplace

1. Logon to your AWS account.
2. Go to **Services** > **Compute** > **EC2**.
3. Click **EC2 Dashboard** > **Launch Instance** and **Select AWS Marketplace**.
4. Search for 'FortiSIEM'.
5. Select **Fortinet FortiSIEM-Report Server** and click **Continue**.
6. Choose an instance type based on Step A.
7. Configure the Instance details:
   a. Choose the **number of instances** as the sum of number of Supervisor and Worker nodes.
   b. Choose **Network** as the VPC selected in Step C.
   c. Choose **Subnet** as the subnet where you want to launch FortiSIEM Report Server.
   d. Set **Auto-assign public IP** as 'Disabled'.
   e. Set **Shutdown behavior** as Stop.
   f. Check **Enable termination protection**.
   g. In Network Interfaces, choose the Primary IP as the Private IP of your choice within that subnet
   h. Click **Add Storage**.
   You can keep the defaults for root partition, CMDB and SVN. If you want the **Local** storage for event data, add a new EBS volume based on your storage requirements (minimum 50 GB)
   i. Click **Add Tags**. You can add a tag similar to “FortiSIEM Supervisor” to search the instance.
   j. Click **Configure Security Group** and create a new **Security Group**.
   Retain the defaults which are needed for FortiSIEM to operate.
   k. Click **Review and Launch** and click **Launch**.
   l. Select **Create a new key pair** and provide a **key pair name** of your choice.
   m. Click **Download Key Pair** and save the `.pem` file.
   n. Click **Launch Instance** and wait for the instance to start.
8. Configure **Elastic IP**:
   a. Go to **EC2 Dashboard** > **Elastic IPs**.
   b. Click **Allocate New Address**.
   c. Select **VPC** and click **Allocate**.
   The IP address will be allocated
   d. Click the **Elastic IP** that was allocated.
   e. Click **Actions** > **Associate address** and select the instance by searching the tag you created in Step 7i.
   f. Click **Associate**.

Step 2: Start and Configure FortiSIEM

Do not press any control keys (for example - Ctrl-C or Ctrl-Z) while configuring the virtual appliances, as this may cause the installation process to stop. If this happens, you must erase the virtual appliance and start the installation process again.

1. SSH into Supervisor console using the keys in Step 7m.
   For details about connecting to the instance, see here.
2. Become the root user. Run the command `sudo su -`.
3. For Local storage, add the data disk. Use the command `fdisk -l` to get the disk name.
4. Run the script `/opt/vmware/share/vami/vami_set_timezone` to set the time zone.
5. Run the script `/opt/vmware/share/vami/vami_config_net` to configure the network.
6. Based on your network type, enter one of the options below:
   - **1** for **IPv6 Network Only**
     - When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, and IPv6 DNS Server(s).
   - **2** for **IPv4 Network Only**
     - When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Netmask, IPv4 Gateway, and IPv4 DNS Server(s).
   - **3** for **Both Networks**
     i. When prompted, enter the information for these IPv6 network components to configure the Static IPv6 address: IPv6 Address, IPv6 Prefix, IPv6 Gateway, IPv6 DNS Server(s).
     ii. Follow Step 6 below to turn off the proxy server and continue with step c.
     iii. When prompted, enter the information for these IPv4 network components to configure the Static IPv4 address: IPv4 Address, IPv4 Prefix, IPv4 Gateway, IPv4 DNS Server(s).
7. Enter **n**. **Note**: The authenticated proxy server is not supported in this version of FortiSIEM. You must turn off the proxy server authentication or completely disable the proxy for the AWS host.
8. Enter **y** to accept the network configuration settings.
9. Enter the **Host name**, and then press **Enter**.
10. Enter the mount point for your data. Set one of the following:
    - 'Local' (/dev/<disk_name>)
    - 'NFS' storage mount point
      Note: Do not use the same mount point as EventDB on Supervisor. This should be a different mount point/storage path.

    After you set the mount point, the Report Server will automatically reboot, and in 10 to 15 minutes the Report Server will be successfully configured.

Step 3: Register FortiSIEM Report Server to Supervisor

1. Log in to your Supervisor node.
2. Open the 'License Management' page on:
   - Flash GUI: Go to **Admin** > **License Management**. Under 'Report Server Information', click **Add**.
   - HTML5 GUI: Go to **ADMIN** > **License** > **Nodes** tab. Click **Add** and select '**Report Server**' from the **Type** drop-down.

3. Enter the **Report Server IP Address**, **Database Username** and **Database Password** of the Report Server you want to use to administer.
   Use the same credentials to set up the Visual Analytics Server for reading data from the Report Server.
4. Click **Run in Background** if you want Report Server registration to run in the background for larger installations. When CMDB size is below 1 GB, registration takes approximately three minutes to complete.
5. When the registration is complete, click **OK** in the confirmation dialog.
6. Make sure the Report Server is up and running by navigating to:
   - Flash GUI: **Admin** > **Cloud Health**
   - HTML5 GUI: **ADMIN** > **Health** > **Cloud Health**

Step 4: Sync Reports from FortiSIEM Supervisor to the Report Server

1. Log in to your Supervisor node.
2. Select **Synced Reports** from:
   - Flash GUI: **RESOURCE > Reports** > **Synced Reports**
   - HTML5 GUI: **RESOURCES** > **Reports** > **Synced Reports**
3. Select a Report.
   Currently, only reports that contain a 'Group By' condition can be synced. Both system and user-created reports can be synched as long as it contains a 'Group By' condition.
4. Select **Sync**.
   When the sync process initiates, the Supervisor node dynamically creates a table within the Report Server reportdb database. When the sync is established, it will run every five minutes, and the last five minutes of data in the synced report will be pushed to the corresponding table. This lets you run Visual Analytics on event data stored in the Report Server reportdb database.