FortiSIEM - Alibaba Cloud Installation Guide

Version 5.4.0

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

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

FORTINET BLOG
https://blog.fortinet.com

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

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/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

Installing Alibaba Cloud Supervisor-Worker

This chapter describes how to install the FortiSIEM Alibaba Cloud Supervisor-Worker.

Step 1: Download the Alibaba Package

Download the Alibaba Cloud Super/Worker package from the Fortinet Support website: https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website. The name of the Super-Worker download is `FSM_Full_Super-Worker_AlibabaCloud_5.4.0_build<build_number>.zip`.

Step 2: Upload to Alibaba Cloud

1. Create a bucket:
   a. Log in to the OSS Console with your Alibaba cloud credentials: https://oss.console.aliyun.com/
   b. Create a bucket with a name of your choice.
2. Download the command line client installation package based on your operating system from this URL.
   `https://www.alibabacloud.com/help/doc-detail/120075.htm?spm=a2c63.p38356.879954.7.49a865d0gY29c1#concept-303829`
3. Run the corresponding binary file for your operating system.
4. Install the command line client `ossutil`.
   Note: The commands illustrated in this section assume you are using the command line client for the 64-bit macOS platform.
   a. Download the `ossutil` installation package.
      `curl -o ossutilmac64 http://gosspublic.alicdn.com/ossutil/1.6.7/ossutilmac64`
   b. Modify the file execution permissions:
      `chmod 755 ossutilmac64`
   c. Generate the configuration file. For more information about the parameters, see the configuration parameters described in the preceding Linux section.

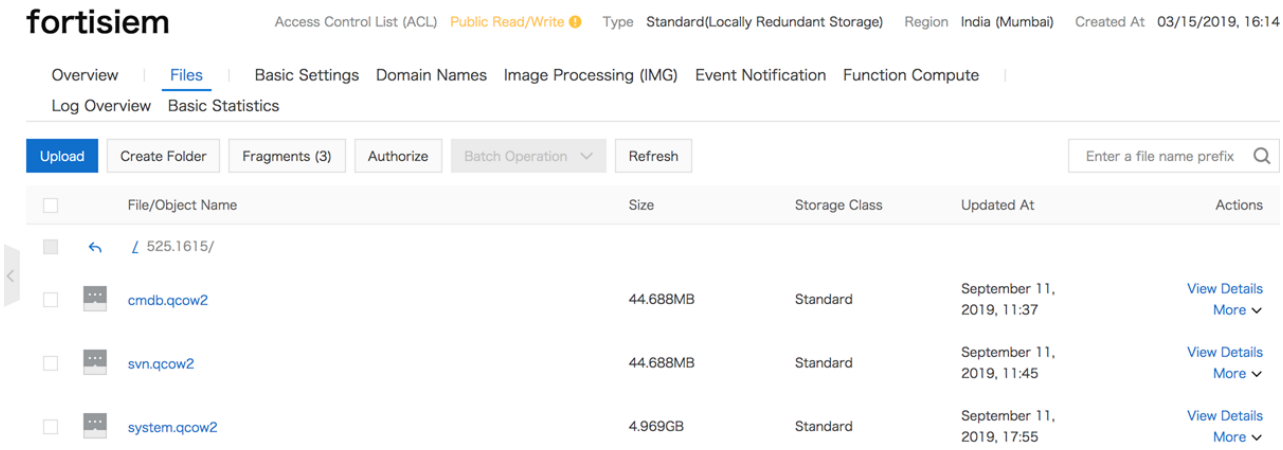
```
./ossutilmac64 config
```

This command generates a configuration file to store configuration information. Enter the path of the configuration file. The default path is `/home/user/.ossutilconfig`. If you press **Enter** without specifying a path, the file is generated in the default path. If you want to generate the file in another path, set the `--config-file` option to the path.

If the path of the configuration file is not specified, the default path `/home/user/.ossutilconfig` is used. The following parameters are ignored if you press **Enter** without configuring them. For more information about the parameters, run the `help config` command.

Enter the endpoint: `http://xxxx.aliyuncs.com`
Enter the **AccessKey ID**: your AccessKey ID
Enter the **AccessKey Secret**: your AccessKey Secret
Enter the **STS token**: *(required only when you use a temporary STS token to access the OSS bucket. Otherwise, you can leave this parameter unspecified)*

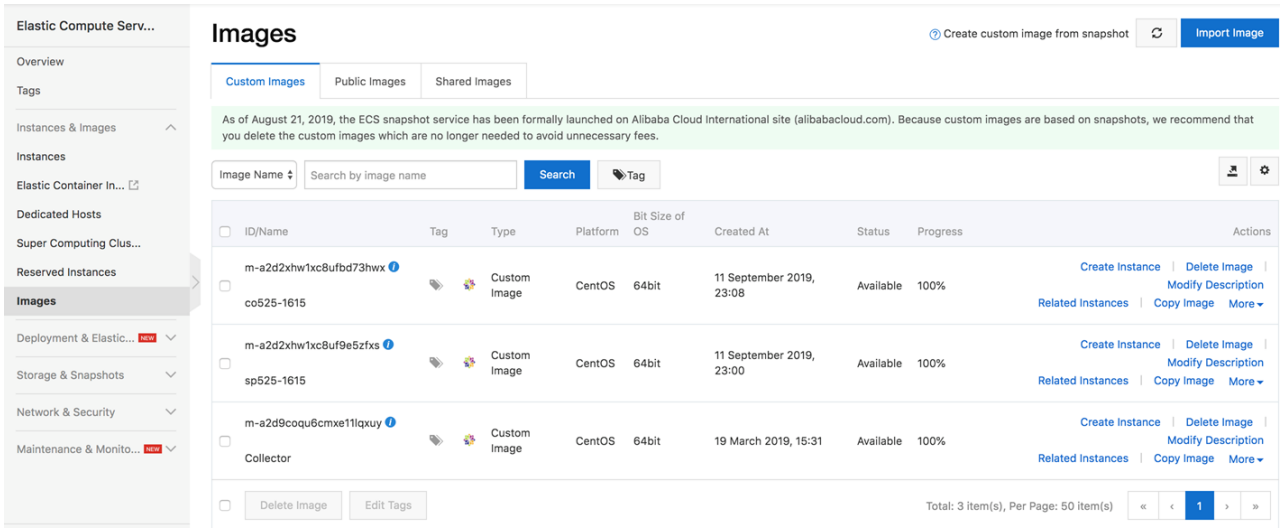
5. Upload the package to the Alibaba bucket:
   Upload a single file:
   ```
   $./ossutilmac64 cp file oss://bucketName/FileName
   ```
   Upload a folder:
   ```
   $./ossutilmac64 cp -r dir oss://bucketName/FolderName
   ```
   The package in the bucket will look like this:



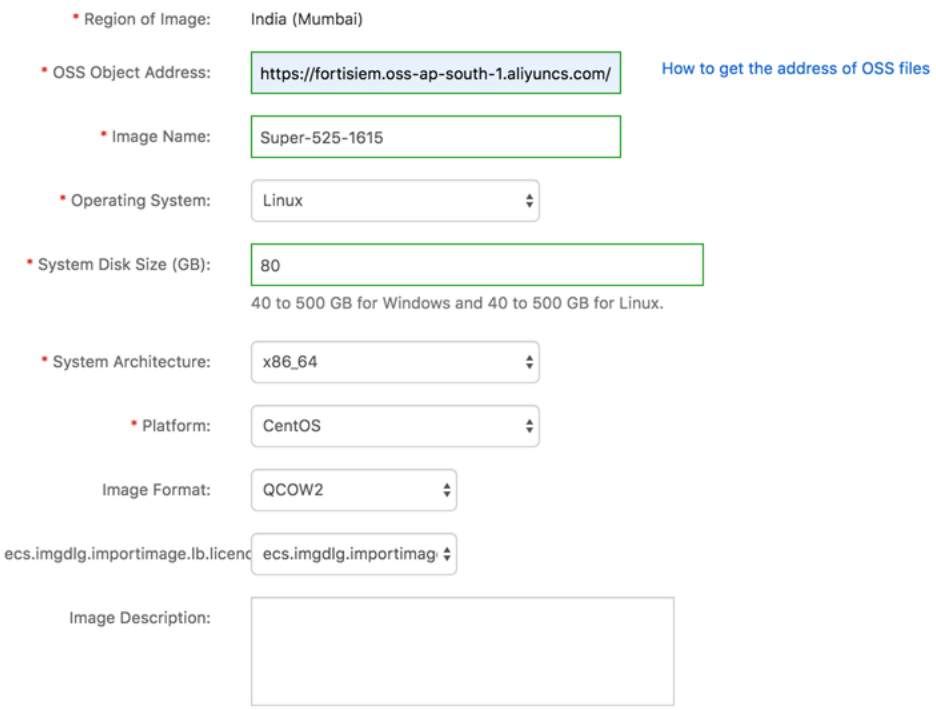
6. Get the OSS link:
   a. Log in to the Alibaba Cloud Web UI (Web interface).
   b. Select the uploaded file: **File> Preview**.
   c. Copy the file's URL.

Step 3: Create the Image from the Uploaded File

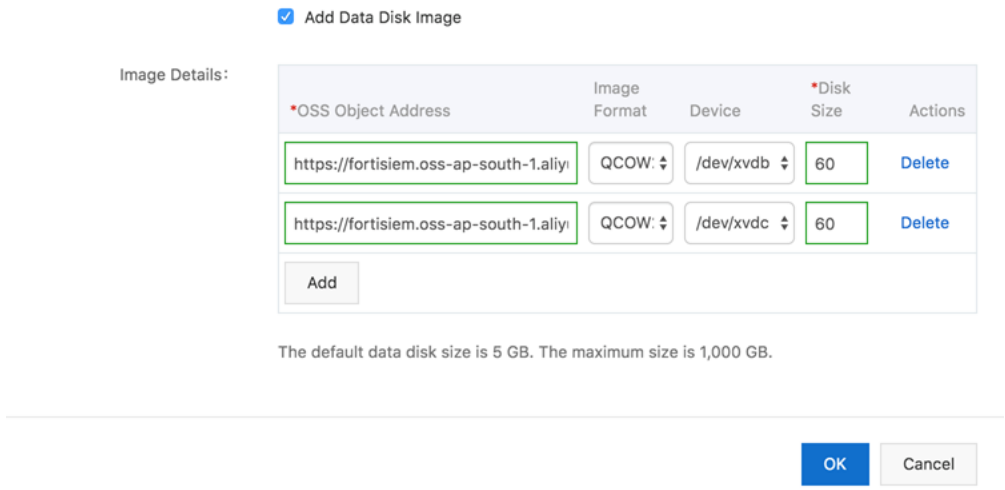
1. Log in to the Alibaba Cloud Web UI.
2. Navigate to the ECS (Elastic Computing Service).
3. Click the **Images** tab.
4. Select **Custom Images** under **SnapShot and Images** in the left-hand pane.
5. Click **Import Image** on the top right of the **Images** screen.



6. Enter the OSS object Address of `system.qcow2` that you copied in Step 2: "Upload to Alibaba Cloud", Sub-step 5: "Get the OSS link".



7. Select **Add Data Disk Image**, import the `cmdb.qcow2`, and then import the `svn.qcow2`.



8. Click **OK**.
9. Wait until the image is created.

Step 4: Create an Instance from the Created Image

1. Select the image you created from the table on the **Images** tab in the Web UI.
2. Click **Create Instance** in the lower-right side of the **Images** tab. Enter all of the required details, such as VPC, Security Groups, Elastic IP keypair, and so on, similar to Amazon AWS.

Step 5: 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 you created in Step 2: Upload to Alibaba Cloud.
   For details about connecting to the instance, see here.
2. Run the script `/opt/vmware/share/vami/vami_set_timezone` to set the time zone.
3. Run the script `/opt/vmware/share/vami/vami_config_net` to configure the network.
   You must keep all the default values except host name.
4. 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**
  a. 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).
  b. Follow Step 5 below to turn off the proxy server and continue with step c.
  c. 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).

5. 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.
6. Enter **y** to accept the network configuration settings.
7. 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.
8. For Collector, the system will reboot and after a few minutes it will be ready.

Step 6: 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 7: Choose FortiSIEM Event Database Storage

For fresh installation, you will be taken to the Event Database Storage page. Based on Step-6, you will be asked to choose between **Local Disk**, **NFS** or **Elasticsearch** options.

For more details, see here.

Step 8: (Optional) Install Workers and Add to Supervisor Node

1. Follow Steps 4 and 5 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.

Installing Alibaba Cloud Collector

This chapter describes how to install the FortiSIEM Alibaba Cloud Collector.

Step 1: Download the Alibaba Package

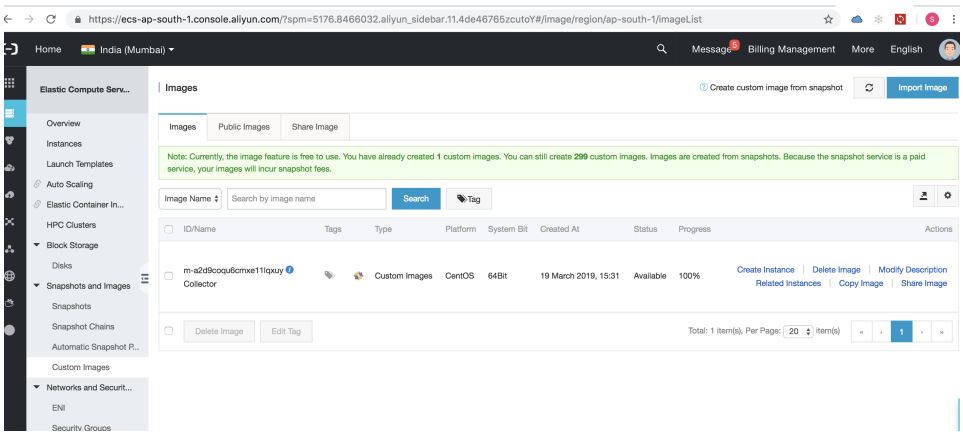
Download the Alibaba Cloud Collector package from the Fortinet Support website https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website. The name of the collector download is `FSM_Full_Collector_AlibabaCloud_5.4.0_build<build_number>.zip`.

Step 2: Upload to Alibaba Cloud

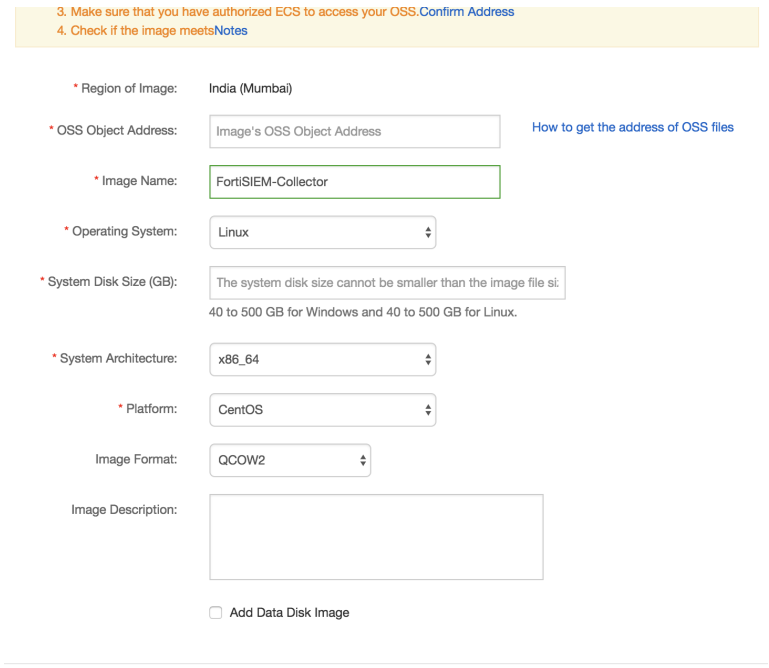
1. Use the following command to upload the collector image you created in the previous step:
   `$./ossutilmac64 cp file oss://<bucketName>/<FileName>`
2. Get the OSS link:
   Log in to the Alibaba Cloud Web UI (Web interface). From the UI, select the uploaded file: **File> Preview**, and copy the file's URL.

Step 3: Create the Image from the Uploaded File

1. Log in to the Alibaba Cloud Web UI.
2. Navigate to the ECS (Elastic Computing Service).
3. Click the **Images** tab.
4. Select **Custom Images** under **SnapShot and Images** in the left-hand pane:



5. Click **Import Image** on the top right of the **Images** screen.



6. Enter the **OSS object Address** that you copied in Step 2: "Upload to Alibaba Cloud", Sub-step 2: "Get the OSS link".
7. Click **OK**.
8. Wait until the image is created.

Step 4: Create an Instance from the Created Image

1. Select the image you created from the table on the **Images** tab in the Web UI.
2. Click **Create Instance** in the lower-right side of the **Images** tab.

Enter all of the required details, such as VPC, Security Groups, Elastic IP keypair, and so on, similar to Amazon AWS.

Step 5: 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 the Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time** and **End Time** – set to 'Unlimited'.
3. SSH to the Collector and run following script to register Collectors:
   ```
   phProvisionCollector --add <user> <password> <Super IP or Host> <Organization> <CollectorName>
   ```
   a. Set **User** and **Password** use the admin User Name and password for the Supervisor
   b. Set **IP Address** as 'Supervisor IP'.
   c. Set **Organization** as 'Super'.
   d. Set **CollectorName** from Step 2a.
   The Collector will reboot during the Registration
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 following details:
   a. **Collector Name** – Collector Name.
   b. **Guaranteed EPS** – this is the EPS that the Collector will always be able to send. It could send more if there is excess EPS available.
   c. **Start Time**, and **End Time** - could be set as 'Unlimited'.
6. SSH to the Collector and run following script to register Collectors:
   ```
   phProvisionCollector --add <user> <password> <Super IP or Host> <Organization> <CollectorName>
   ```
   a. Set **User** and **Password** use the admin User Name and password for the Supervisor
   b. Set **IP Address** as 'Supervisor IP'.
   c. Set **Organization** as 'Super'.
   d. Set **CollectorName**.
   The Collector will reboot during the Registration
7. Go to **ADMIN > Health > Collector Health** and check the status.