FortiSIEM - Azure Installation Guide

Version 5.2.6

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

11/20/2019
FortiSIEM 5.2.6 Azure Installation Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
11/20/2019	Initial release of Azure Installation Guide for 5.2.6.

Installing FortiSIEM Azure Super/Worker

This document provides instructions to install FortiSIEM Azure Super/Worker. Currently, FortiSIEM images are not available in Azure market place. It is recommended to use your own account to download and launch FortiSIEM Virtual Machine (VM).

1. Download FortiSIEM Azure Super image (vhd) file from the Fortinet Support website https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Log in to Azure portal.
3. Upload the vhd file in the Azure Portal:
   a. Click **Storage Accounts** and select the storage account where the Security Access Manager vhd file will be uploaded to. If you do not have a storage account, click **Add** to create one.
   Note: The selected location will determine where the image can be created and subsequently deployed.
   b. Under **Blob Service**, select **Containers**.
   c. Select a container to upload the Security Access Manager vhd file.
   If you do not have a storage container, click **Add Container** to create one.
   d. Click **Upload** and select the Azure-compliant Security Access Manager vhd file to upload.
   Ensure that the **Blob type** is set to "Page Blob".This process might take a long time depending on your network connection and the location of your Azure storage account.
4. Create an image in the Azure Portal:
   a. Select Images and click **Add** to create a new image.
      i. Enter a **Name** for the image. Remember that this image is a template that will be later deployed to a virtual machine with a different name.
      ii. Ensure that the location is the same as the location of your storage account.
      iii. In the **OS disk** section:
      • Select **Linux** and the **OS type**.
      • Click **Browse** on the **Storage Blob** field. A new panel will list your storage accounts.
      • Using this panel, navigate through the storage account and container to locate the Security Access Manager vhd that was uploaded.
      iv. Click **Create** to start the image creation process. This process typically takes few minutes to complete.
   b. When the process is completed, return to the **Images** panel and verify that the new image was created.
   This image can now be used to deploy new Security Access Manager virtual machines in Azure.
5. Go to **All services > Images** and select the Virtual Image created in Step 4 above.
6. Click **Create VM** to create a VM and launch with reference to the Azure documentation here:
   https://docs.microsoft.com/en-us/azure/virtual-machines/linux/quick-create-portal
   Note: You must use the image from Step 5 above instead of selecting one from Azure Marketplace. Follow the minimum hardware requirements for the Collector with reference to the FortiSIEM Sizing Guide.
   Click **Add disks** and add three disks.
   - 50GB for opt
   - 60GB for svn
   - 60GB for cmdb
7. Go to **All Services > Virtual machines**, then click the recently created VM.

8. On the VM, go to **Settings > Networking** and click **Network Interface > Settings > IP configurations**, then click "ipconfig1" to change **Private IP address settings** to "Static" and save the changes.
9. Connect to the VM.
10. Run command `execute factoryreset`.
11. After `factoryreset` executes successfully, reboot the system.
12. After system is up and running, connect to the VM and run the command `/opt/vmware/share/vami/vami_config_net`.
13. Respond to the questions asked by the system.

Installing FortiSIEM Azure Collector

This document provides instructions to install FortiSIEM Azure Collector. Currently, FortiSIEM images are not available in Azure market place. It is recommended to use your own account to download and launch FortiSIEM Virtual Machine (VM).

1. Download FortiSIEM Azure Collector image (vhd) file from the Fortinet Support website https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Log in to Azure portal.
3. Upload the vhd file in the Azure Portal:
    1. Click **Storage Accounts** and select the storage account where the Security Access Manager vhd file will be uploaded to. If you do not have a storage account, click **Add** to create one.
    Note: The selected location will determine where the image can be created and subsequently deployed.
    2. Under **Blob Service**, select **Containers**.
    3. Select a container to upload the Security Access Manager vhd file. If you do not have a storage container, click **Add Container** to create one.
    4. Click **Upload** and select the Azure-compliant Security Access Manager vhd file to upload. Ensure that the **Blob type** is set to 'Page Blob'.
    This process might take a long time depending on your network connection and the location of your Azure storage account.
4. Create an image in the Azure Portal:
    1. Select **Images** and click **Add** to create a new image.
        a. Enter a **Name** for the image. Remember that this image is a template that will be later deployed to a virtual machine with a different name.
        b. Ensure that the location is the same as the location of your storage account.
        c. In the **OS disk** section:
            - Select **Linux** and the **OS type**.
            - Click **Browse** on the **Storage Blob** field. A new panel will list your storage accounts.
            - Using this panel, navigate through the storage account and container to locate the Security Access Manager vhd that was uploaded.
        d. Click **Create** to start the image creation process. This process typically takes few minutes to complete.
    2. When the process is completed, return to the **Images** panel and verify that the new image was created.
    This image can now be used to deploy new Security Access Manager virtual machines in Azure.
5. Go to **All services** > **Images** and select the Virtual Image created in Step 4 above.
6. Click **Create VM** to create a VM and launch with reference to the Azure documentation here: https://docs.microsoft.com/en-us/azure/virtual-machines/linux/quick-create-portal.
Note: You must use the image from Step 5 above instead of selecting one from Azure Marketplace.
Follow the minimum hardware requirements for the Collector with reference to the FortiSIEM Sizing Guide.
7. Go to **All Services** > **Virtual machines** > click on the recently created VM.
8. On the VM, go to **Settings** > **Networking** and click on **Network Interface** > **Settings** > **IP configurations** > click

on ‘ipconfig1’ to change **Private IP address settings** to ‘Static’ and save the changes.

9. On the VM, go to **Serial Console** > log in to the console and run `/opt/vmware/share/vami/vami_config_net` script.

(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. 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 **Name** 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 **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. 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
7. Go to **ADMIN** > **Health** > **Collector Health** and check the status.