FortiSIEM - OpenStack 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

02/05/2020
FortiSIEM 5.2.6 OpenStack Installation Guide

TABLE OF CONTENTS

Change Log **4**
Installing FortiSIEM in OpenStack **5**
Installing a Supervisor, Worker, or All-In-One Node 5
Step 1: Download the KVM Image 5
Step 2: Create a Volume 5
Step 3: Create an Instance 5
Step 4: Attach the Volume to the Instance 6
Installing a Collector 6
Step 1: Download the KVM Image 6
Step 2: Create a Volume 6
Step 3: Create an Instance 6

Change Log

Date	Change Description
04/08/2019	Initial version of FortiSIEM OpenStack Installation Guide.
08/19/2019	Revision 1: Updated the location of the image download site.
11/20/2019	Release of FortiSIEM OpenStack Installation Guide for 5.2.6.
02/05/2020	Revision 2: Removed references to Volume Source. Removed references to vpn and cmdb from Collector installation. Changed "OpenStack image" to "KVM image".

Installing FortiSIEM in OpenStack

This document provides instructions for installing FortiSIEM on OpenStack.

Installing a Supervisor, Worker, or All-In-One Node

Follow these steps for installing a FortiSIEM Supervisor, Worker, or All-In-One node on OpenStack

Step 1: Download the KVM Image

1. Download the KVM Image from the Fortinet Support website https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Unzip the Images.
3. Verify that there are three disks: `system`, `svn`, and `cmdb`.

Step 2: Create a Volume

1. Log in to the OpenStack dashboard.
2. Select the appropriate project from the drop-down menu at the top left.
3. On the **Project** tab, open the **Volumes** tab and click the **Volumes** category.
4. Click **Create Volume**.
   In the dialog box that opens, enter or select the following values.
   - **Volume Name**: Specify a name for the volume.
   - **Description**: Optionally, provide a brief description for the volume.
   - **Type**: Leave this field blank.
   - **Size (GB)**: Specify the size of the volume in gigabytes (GiB).
   - **Availability Zone**: Select the Availability Zone from the list. By default, this value is set to the availability zone given by the cloud provider (for example, `us-west` or `apac-south`). For some cases, it could be `nova`.
5. Click **Create Volume**.
6. Repeat Steps 1 through 5 for the `svn` and `cmdb` disks.

Step 3: Create an Instance

Create an instance from the volume created with the `system` disk (see substeps 1 to 5 in Step 2: Create a Volume), but **do not** boot the instance.

Step 4: Attach the Volume to the Instance

1. Attach the CMDB volume you created in substeps 1 to 5 in Step 2: Create a Volume, then attach it to the instance created in Step 3: Create an Instance.
2. Attach the SVN volume you created in substeps 1 to 5 in Step 2: Create a Volume, then attach it to the instance created in Step 3: Create an Instance.
3. Boot the instance.

Installing a Collector

Follow these steps to install a FortiSIEM collector on OpenStack.

Step 1: Download the KVM Image

1. Download the KVM Image from the Fortinet Support website https://support.fortinet.com. See "Downloading FortiSIEM Products" for more information on downloading products from the support website.
2. Unzip the Images.
3. Verify the presence of the `system` disk.

Step 2: Create a Volume

1. Log in to the OpenStack dashboard.
2. Select the appropriate project from the drop-down menu at the top left.
3. On the **Project** tab, open the **Volumes** tab and click the **Volumes** category.
4. Click **Create Volume**.

   In the dialog box that opens, enter or select the following values.
   - **Volume Name**: Specify a name for the volume.
   - **Description**: Optionally, provide a brief description for the volume.
   - **Type**: Leave this field blank.
   - **Size (GB)**: Specify the size of the volume in gigabytes (GiB).
   - **Availability Zone**: Select the Availability Zone from the list. By default, this value is set to the availability zone given by the cloud provider (for example, `us-west` or `apac-south`). For some cases, it could be `nova`.
5. Click **Create Volume**.

Step 3: Create an Instance

Create an instance from the volume created with the `system` disk (see substeps 1 to 5 in Step 2: Create a Volume), but **do not** boot the instance.

Copyright© (Undefined variable: FortinetVariables.Copyright Year) 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.