FortiSIEM - NFS Storage Guide

Version 6.1.1

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/training-certification

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://www.fortiguard.com

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

FEEDBACK
Email: techdoc@fortinet.com

11/01/2021
FortiSIEM 6.1.1 NFS Storage Guide

TABLE OF CONTENTS

Change Log

Date	Change Description
03/30/2018	Initial version of FortiSIEM - NFS Storage Guide
11/20/2019	Revision 1: FortiSIEM - NFS Storage Guide.
03/30/2020	Release 2: FortiSIEM - NFS Storage Guide.
11/11/2020	Release 3: Updates for CentOS 7.x and 8.x.

Installing NFS Server for FortiSIEM Event Storage

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. This document describes how to set up and configure NFS servers for use with FortiSIEM.

- NFS Server on Windows is not supported.
- 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.
- If NFS is chosen as the storage option, FortiSIEM mounts the NFS partition using NFSv3 protocol by default. However, most Linux based NFS servers and commercial servers also support the NFSv4.1 protocol which allows parallel I/O from threads/processes on the same node. NFSv3 serializes I/O across threads/processes on one machine. Based on the FortiSIEM performance testing results using NFSv4.1 protocol - if the customer NFS server supports NFS v4.1, it is recommended to change the mount option manually across Super and Workers and reboot the cluster. In the `/etc/fstab` file, change the value `nfsvers=3` to `nfsvers=4.1`. Make sure you test this on a separate mount point before making the change on FortiSIEM cluster.
- For sizing the NFS event storage please refer to the Sizing Guide.
- There are differences between CentOS 7.x and CentOS 8.x. For more information on setting up the server and client for CentOS 8.x, see https://www.tecmint.com/install-nfs-server-on-centos-8/.

Installation in CentOS Linux 7.x or 8.x

Step 1: Install the NFS Server

Follow these steps to install NFS Server in CentOS Linux:

1. Login to the CentOS server as `root`.
2. Download and install the NFS packages using this command:
   - For CentOS Linux 7.x, use the command line:
     ```
     # yum install nfs-utils nfs-utils-lib
     ```
   - For Centos 8.x, use the command line:
     ```
     # dnf install nfs-utils
     ```
3. Start and enable the NFS service by running these scripts:
   - For CentOS 7.x use these commands:
     ```
     # systemctl start nfs-server
     ```

```
# systemctl enable nfs-server
```

- For CentOS 8.x, use these commands:

```
# systemctl start nfs-server.service
# systemctl enable nfs-server.service
```

4. Check NFS service status:

```
# systemctl status nfs-server
```

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

```
# mkdir /FortiSIEM
# chmod -R 777 /FortiSIEM // without this permission, installation won't work
```

6. Edit and the save the `/etc/exports` file by adding the following lines. This enables the FortiSIEM Supervisor and Worker nodes access to the `/FortiSIEM` directory.

```
/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. Export the directories in `/etc/exports` by running this command:

```
# exportfs -arv
```

8. If `firewalld` is installed, then enable the FortiSIEM Supervisor and Worker to communicate by adding these firewall rules:

```
firewall-cmd --permanent --add-service=nfs
firewall-cmd --permanent --add-service=rpc-bind
firewall-cmd --permanent --add-service=mountd
firewall-cmd --reload
```

9. Restart the NFS server using the command:

```
# systemctl status nfs-server
```

Step 2: Check the Exported Directories

Follow these steps to check the exported directories from the FortiSIEM Supervisor and Worker Nodes:

1. Login to the Supervisor and run this command:

```
# showmount -e <NFS Server>
```

2. Make sure the exported list is correct as follows:

```
/FortiSIEM <Supervisor_IP>,<Worker1_IP>,<Worker2_IP>
```

3. Repeat the previous steps for each Worker node.

Step 3. Optional—Enable NFS 4.1 on FortiSIEM Nodes

Follow these steps to enable NFS 4.1 on FortiSIEM Super and Worker Nodes:

1. Make sure your NFS Server supports NFS 4.1.
2. Login to each node.
3. Edit the `/etc/fstab` file to change the value `nfsvers=3` to `nfsvers=4.1`.
4. Save the file.
5. Reboot the node.

Installation in an AWS Environment

Follow these steps to install NFS Server in an AWS Environment

- Step 1: Launch NFS Server
- Step 2: Start and Configure the NFS Server

Step 1: Launch NFS Server

Follow these steps to launch the NFS Server from the AWS Marketplace

1. Login to your AWS account.
2. Go to **Services** > **Compute** > **EC2**.
3. Click **EC2 Dashboard > Launch Instance**.
4. Select the **CentOS 8** Instance.
5. Click **Compute Optimized C5 Instance**.
6. Configure the Instance details following the steps:
   a. Choose '1' in the number of instances.
   b. Choose 'Network' as the VPC selected for Supervisor and Worker nodes.
   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. You can select 'Auto-Assign' which is the default option.
   h. Click **Add Storage**.
   You can the default for root partition. Since you need 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 EventDB NFS” to search the instance.
   j. Click **Configure Security Group**.
   k. Create a new **Security Group** and keep the defaults which are needed for FortiSIEM to operate.
   l. Click **Review and Launch** and click **Launch**.
   m. Select **Create a new key pair** and provide a **key pair name** of your choice.
   n. Click **Download Key Pair** and save the `.pem` file.
   o. Click **Launch Instance** and wait for the instance to start.
7. Configure Elastic IP following these steps:
   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 6i.
   f. Click **Associate**.

Step 2: Start and Configure the NFS Server

Follow these steps to start and configure the NFS server.

1. SSH into the NFS server using the keys in Step 6m above, using user 'centos'.
   For details about connecting to the instance, see here.
2. Follow the instructions in Steps 1, 2 and 3 in Installation in CentOS Linux 7.x or 8.x.