



FortiSIEM - NFS Storage Guide

Version 5.3.1



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/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



05/29/2020

FortiSIEM 5.3.1 NFS Storage Guide

TABLE OF CONTENTS

Change Log	. 4
Installing NFS Server for FortiSIEM Event Storage	
Installation in CentOS Linux 6.x	Ę
Installation in AWS Environment	. 7
Step 1: Launch FortiSIEM Supervisor from AWS Marketplace	. 7
Step 2: Start and Configure NFS Server	. 8

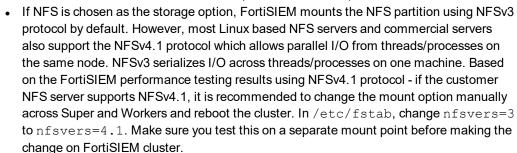
Change Log

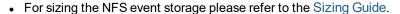
Date	Change Description
03/30/2018	Initial version of FortiSIEM - NFS Storage Guide
11/20/2019	Release of FortiSIEM - NFS Storage Guide for 5.2.6.
03/30/2020	Release of FortiSIEM - NFS Storage Guide for 5.3.0.

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.







Installation in CentOS Linux 6.x

Follow the steps below to install NFS Server in CentOS Linux 6.x:

- 1. Login to CentOS 6.x as 'root'.
- **2.** Download and install the NFS packages using the command: yum install nfs-utils nfs-utils-lib
- 3. Run the NFS server start-up scripts:

```
chkconfig nfs on
service rpcbind start
service nfs start
```

4. Check NFS service status and make sure the nfsd service using the command:

```
service nfs status
```

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
```

6. Edit the /etc/exports file to share the /FortiSIEM directory with the FortiSIEM Supervisor and Worker nodes by running:

```
vi /etc/exports /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. Save your changes to /etc/exports and restart the NFS server using the command:

```
service nfs restart
```

8. Check shared directories using the command:

showmount -e localhost Example: Export list for localhost

/FortiSIEM <Supervisor_IP_Address>, <Worker1_IP_Address>, <Worker2_IP_Address>

Installation in AWS Environment

Follow the steps below to install NFS Server in an AWS Environment:

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.
- 4. Select HVM Amazon Linux 2 LTS AMI (HVM) 64-bit 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.
- I. 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 the steps:
 - a. Go to EC2 Dashboard > Elastic IPs.
 - b. Click Allocate New Address.
 - $\textbf{c.} \quad \text{Select VPC} \text{ and click } \textbf{Allocate}.$
 - 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 NFS Server



Do not press any control keys (for example - Ctrll-C or Ctrll-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 keys in Step 6m above using user 'ec2-user'. For details about connecting to the instance, see here.
- 2. Configure the NFS mount point access to give the FortiSIEM internal IP full access.

 An example of creating a 1TB EventDB volume and exporting it as NFS is shown below:

```
[ec2-user@ip-10-0-5-152 ~]$ sudo su -
Last login: Tue Mar 27 23:57:47 UTC 2018 on pts/0
[root@ip-10-0-5-152 ~] # yum update -y
[root@ip-10-0-5-152 ~]# reboot
[root@ip-10-0-5-152 ~]# pvcreate /dev/nvmeln1
Physical volume "/dev/nvmeln1" successfully created.
[root@ip-10-0-5-152 ~] # pvdisplay
"/dev/sdb" is a new physical volume of "1.00 TiB"
--- NEW Physical volume ---
                      /dev/sdb
PV Name
VG Name
PV Size
                      1.00 TiB
Allocatable
                      NO
PE Size
                      0
Total PE
                      Λ
Free PE
                      0
Allocated PE
PV UUID
                      7x0c00-vuaA-3djP-CerD-TxPd-9Uge-1fm0hk
[root@ip-10-0-5-152 ~] # vgcreate VGEventDB /dev/sdb
Volume group "VGEventDB" successfully created
[root@ip-10-0-5-152 ~]# lvcreate -1 100%vg -n LVEventDB VGEventDB
Logical volume "LVEventDB" created.
[root@ip-10-0-5-152 ~] # mkfs.ext4 -j /dev/VGEventDB/LVEventDB
mke2fs 1.42.9 (28-Dec-2013)
Filesystem label=
```

```
OS type: Linux
Block size=4096 (log=2)
Fragment size=4096 (log=2)
Stride=0 blocks, Stripe width=0 blocks
67108864 inodes, 268434432 blocks
13421721 blocks (5.00%) reserved for the super user
First data block=0
Maximum filesystem blocks=2415919104
8192 block groups
32768 blocks per group, 32768 fragments per group
8192 inodes per group
Superblock backups stored on blocks:
32768, 98304, 163840, 229376, 294912, 819200, 884736, 1605632, 2654208,
4096000, 7962624, 11239424, 20480000, 23887872, 71663616, 78675968,
102400000, 214990848
Allocating group tables: done
Writing inode tables: done
Creating journal (32768 blocks): done
Writing superblocks and filesystem accounting information: done
[\verb|root@ip-10-0-5-152| \sim] \# echo "/dev/VGEventDB/LVEventDB / data ext4 defaults 1 1" >> 
/etc/fstab
[root@ip-10-0-5-152 ~] # mkdir /data
[root@ip-10-0-5-152 ~] # mount /data
[root@ip-10-0-5-152 ~]# echo "/data
                                      10.0.0.0/16(rw,no_root_squash)" > /etc/exports
[root@ip-10-0-5-152 \sim] # exportfs -ar
[root@ip-10-0-5-152 ~] # chkconfig --levels 2345 nfs on
Note: Forwarding request to 'systemctl enable nfs.service'.
Created symlink from /etc/systemd/system/multi-user.target.wants/nfs-server.service to
/usr/lib/systemd/system/nfs-server.service.
[root@ip-10-0-5-152 ~] # chkconfig --levels 2345 rpcbind on
Note: Forwarding request to 'systemctl enable rpcbind.service'.
[root@ip-10-0-5-152 ~]# service rpcbind start
Redirecting to /bin/systemctl start rpcbind.service
[root@ip-10-0-5-152 ~] # service nfs start
Redirecting to /bin/systemctl start nfs.service
```





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.