

SolidFire Enterprise SDS

Quick Start Guide

NetApp SolidFire Enterprise SDS (eSDS) provides the benefits of SolidFire scale out technology and NetApp Element software data services on the hardware of your choice that meets the reference configuration for SolidFire eSDS. This Quick Start Guide is a condensed set of instructions for installing SolidFire eSDS. For details, see the [Installation Guide](#).

Prepare for installation | Stage 1

For a more detailed list of prerequisites, see the [Installation Guide](#).

Hardware and software requirements

Verify that your configuration matches the reference configuration listed in the NetApp [Interoperability Matrix Tool \(IMT\)](#). You can also run the reference configuration compliance check using the steps listed [here](#).

Note: Use RHEL with the Infrastructure Server group and select the first SATA drive as the installation target.

Host partitioning requirements

By default, RHEL chooses xfs as the default file system for the partitions that you create. You must change it to ext4, except for the /boot and swap partitions. Your /boot partition should use ext2.

Partition	Size
/boot	1GB
/opt	50GB
/var	50GB
swap	4GB
/home	5GB
/ and /usr	Split the remaining space

The minimum required partition layout is as follows:

Partition	Size
/opt	40GB
/var	40GB
/	10GB (RedHat recommendation)

Networking requirements

You should configure separate network segments for the different types of traffic.

- Storage network:
 - Includes all storage/iSCSI traffic.
 - Can be routed if you want to mount from hosts located on a different layer 3 network or if you plan to replicate data between clusters.
 - Should be configured with network interfaces on the same layer 2 broadcast domain.
- Management network:
 - Includes all management traffic.
 - Can be routed if you want to access the cluster API or UI from a different layer 3 network.
 - Should be configured with network interfaces on the same layer 2 broadcast domain.

IP address requirements

Component	Storage network IP	Management network IP	Total # of IP addresses
Storage node	1	1	2 per node
Management node	(Optional) 1	1	1 per cluster on the storage network + 1 per cluster on the management network + 1 FQDN per cluster for the management node
Storage cluster	1 storage IP (SVIP)	1 management IP (MVIP)	2 per storage cluster

Port requirements

Port type	Default port
Cluster upgrades	80 TCP/UDP
SNMP polling	161 UDP
UI and API access to storage node	442 TCP/UDP
Storage cluster reporting to Active IQ, remote replication cluster pairing communication	443 TCP/UDP
Cluster beacon (to discover nodes to add to a cluster)	2010 UDP
Client iSCSI communications	3260 TCP

SOAP web services	7627 TCP
vCenter Plug-in QoSSIOC service	8443 TCP

Additional requirements

- Install the management node to enable log collection and NetApp Support access for troubleshooting.
- Install One Collect, which will be used by NetApp Support for log collection.
- Run the Ansible role for pre-configuration compliance check provided by NetApp.

Configure your network

Review the detailed guidelines and examples provided in the [Installation Guide](#).

1. Run the following commands to open the required ports:

```
systemctl start firewalld
firewall-cmd --permanent --add-service=snmp
firewall-cmd --permanent --add-port=80/tcp
firewall-cmd --permanent --add-port=80/udp
firewall-cmd --permanent --add-port=442-443/tcp
firewall-cmd --permanent --add-port=442-443/udp
firewall-cmd --permanent --add-port=2010/udp
firewall-cmd --permanent --add-source-port=2010/udp
firewall-cmd --permanent --add-port=3260/tcp
firewall-cmd --permanent --add-port=7627/tcp
firewall-cmd --permanent --add-port=8080/tcp
firewall-cmd --permanent --add-port=8443/tcp
firewall-cmd --reload
```

2. Install `NetworkManager-dispatcher-routing-rules` and ensure that the appropriate repositories are configured.
3. Configure your network switch using the best practices provided [here](#).
4. Set up network teaming for management traffic using active/passive or LACP mode.
5. Set up network teaming for storage traffic using LACP mode.
6. For optimal performance, configure your server-side storage interfaces with the same MTU as the NetApp SolidFire storage nodes (9000 bytes).
7. Configure network switches to support an MTU of at least 9016 bytes to account for jumbo frame overhead and for proper forwarding through the network.
8. Create the IP rules for the storage and management interfaces and restart the network service.

Install SolidFire eSDS | Stage 2

For more details about the installation procedure, see the [Installation Guide](#).

Note: Ensure that you download the latest versions of the roles. NetApp provides a README file, which includes information about how to run a role.

Downloading and installing SolidFire eSDS

1. Install Ansible by following the instructions listed [here](#).
2. Run the `ansible-galaxy` command to install all the roles relevant to SolidFire eSDS provided by NetApp.

```
$ ansible-galaxy install git+https://github.com/netapp/ansible.git
- extracting ansible to ~/.ansible/roles/ansible
- ansible was installed successfully
```

3. Move the relevant SolidFire eSDS roles up one directory from where they were installed.

```
$ mv ~/.ansible/roles/ansible/nar_solidfire_sds_* ~/.ansible/roles/
```

4. Run the `ansible-galaxy role list` command to ensure that Ansible is configured to utilize the new roles.

```
$ ansible-galaxy role list

# ~/.ansible/roles

- nar_solidfire_sds_install, (unknown version)
- nar_solidfire_sds_upgrade, (unknown version)
- ansible, (unknown version)
- nar_solidfire_sds_compliance, (unknown version)
```

5. Create the inventory file in your Ansible working directory.

Tip: In the inventory file, you should include all the hosts (nodes) on which you want to install SolidFire eSDS. You should also define variables, such as username and password for your storage nodes, and names of the management interface and storage interface.

6. Download the Red Hat Package Manager (RPM) file to the file directory on a local web server accessible from the server running Ansible and the storage nodes.

7. Create the Ansible playbook.

8. Install SolidFire eSDS by running the playbook you created in the previous step:

```
$ ansible-playbook -i inventory.yaml sample_playbook.yaml
```

Replace `sample_playbook.yaml` with the name of your playbook and `inventory.yaml` with the name of your inventory file.

9. To verify that the SolidFire service was started correctly, run the `systemctl status solidfire` command, and check for `Active:active (exited)...` in the output.

Perform post-installation tasks | Stage 3

1. Configure the cluster name using the [SetClusterConfig API method or the per-node UI](#).
2. Create the cluster using the [CreateCluster API method](#).
3. Add drives to the cluster using the [AddDrives API method](#).
4. Create volumes using the [CreateVolume API method](#).

Monitor SolidFire eSDS clusters | Stage 4

- [View the nodes in your cluster](#).
- [Monitor volumes on your storage cluster](#).
- [Monitor performance, capacity, and cluster health with Active IQ](#).
- [Collect logs for troubleshooting](#).

Maintain SolidFire eSDS systems | Stage 5

- [Enable maintenance mode](#).
- [Replace drives](#).

Where to find additional information

- SolidFire and Element 12.2 Documentation Center: <http://docs.netapp.com/sfe-122/index.jsp>
- SolidFire Enterprise SDS installation information: [SolidFire eSDS Installation Guide](#)
- SolidFire Enterprise SDS running Microsoft SQL Server and Virtualized Infrastructure: <https://www.netapp.com/pdf.html?item=/media/20030-tr-4866.pdf>
- SolidFire Enterprise SDS upgrade and maintenance information: [SolidFire eSDS User Guide](#)
- SolidFire networking best practices: <https://www.netapp.com/us/media/tr-4763.pdf>
- Management node content: https://docs.netapp.com/us-en/hci/docs/task_mnode_work_overview.html