Perform the prerequisite tasks for installation

Element Software

amitha, Megan Bock
April 27, 2021

Table of Contents

Perform the prerequisite tasks for installation

Ensure that you perform the necessary checks and verify that your environment meets the configuration, IP addressing, and networking requirements before you install SolidFire eSDS.

Install the required hardware

- Install the supported server. See NetApp Interoperability Matrix (login required) for more information.
- Ensure that your hardware configuration is balanced and all channels are populated. For more information about maximizing bandwidth, see the KB article (login required).

Configure the host (node)

- Install RHEL based on the supported versions listed in the NetApp Interoperability Matrix (login required).
- Configure a Network Time Protocol (NTP) server to use with all the hosts in your network.
- When selecting the installation destination, select the radio button to manually configure file system partitioning. On the **Manual Partitioning** page, use the **+** and **-** buttons to remove any existing partitions, and create new partitions and size them following the recommendations listed here. Using the default LVM partitioning scheme enables you to easily resize later, if needed.

By default, RHEL chooses `xfs` as the default file system for the partitions that you manually create. You should 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 remaining space

The minimum required partition layout is as follows:

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

The `/dev/sdb` disk is not used by any process.

- Disable RAID for /boot.
- On the Software Selection screen, where you select specific packages to install, select **Server** or **Infrastructure Server** based on your RHEL version.
- After the first boot, do the following:
  - Install Red Hat Subscription Manager, and enable the following repositories:

```
rhel-7-server-ansible-2.9-rpms
rhel-7-server-optional-rpms
rhel-7-server-extras-rpms
```

  - Enable SSH on your nodes.
  - If you want to disable IPv6, follow the steps detailed in this KB article (login required).

Install the required software

- Install Ansible, Git, and Python 3.0.

Verify that your configuration matches NetApp's requirements for installing SolidFire eSDS

- Use the SolidFire eSDS configuration listed in the NetApp Interoperability Matrix Tool (IMT) as a reference.

If you contact NetApp Support for assistance with issues relating to SolidFire eSDS, Support will first verify that your platform complies with the reference configuration for SolidFire eSDS listed in the IMT. If Support determines that your underlying platform does not comply with the reference configuration, Support will guide you in aligning the non-compliant firmware, software, and/or hardware components with the correct versions in the IMT.

- Run a compliance check for SolidFire eSDS.

i. Run the `ansible-galaxy install` command to install the `nar_solidfire_sds_compliance` role.

```
ansible-galaxy install git+https://github.com/NetApp-
Automation/nar_solidfire_sds_compliance.git
```

You can also manually install the role by copying it from the NetApp GitHub repository and placing the role in the `~/.ansible/roles` directory. NetApp provides a README file, which includes information about how to run a role.

Ensure that you always download the latest versions of the roles.

ii. Move the roles that you downloaded up one directory from where they were installed.

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

iii. 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)
```

iv. Create the playbook to use for the compliance check.

v. Run the compliance check playbook as shown in the following example:

```
$ ansible-playbook -i yourinventory.yml yourplaybook.yml
```

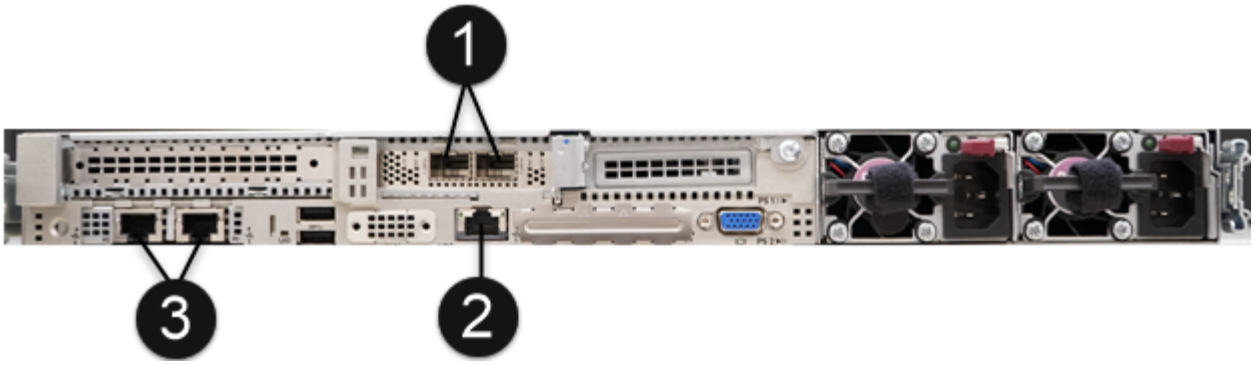
Even after you start using the SolidFire eSDS system, you should run the compliance check regularly to ensure that your system is in compliance. In some cases, NetApp Support will ask you to run the compliance check to help diagnose and troubleshoot issues.

Understand network and IP address requirements

- Familiarize yourself with how to configure and manage networks and network interfaces in RHEL. See the RedHat documentation.
- Configure your network following the IP requirements detailed here:

Component	Storage network IP address	Management network IP address	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

- Configure the storage network on 25GbE Ethernet switches and the management network on 10GbE switches. See the following cabling illustration:



Item	Description
1	Ports for storage network
2	Port for IPMI
3	Ports for management network

The illustration given here is intended to be an example. Your actual hardware might be different based on the server you have.

- Change the switch port MTU to 9216 bytes.

Allow specific ports through your datacenter's firewall

- If `firewalld` is enabled on the storage node running RHEL, ensure that you have the following ports open, so that you can manage the system remotely, allow clients outside of your datacenter to connect to resources, and ensure that internal services can function properly:

Source	Destination	Port	Description
Storage node MIP	Management node	80 TCP/UDP	Cluster upgrades
SNMP server	Storage node MIP	161 UDP	SNMP polling
System administrator PC	Management node	442 TCP	HTTPS UI access to management node
System administrator PC	Storage node MIP	442 TCP	HTTPS UI access to storage node
iSCSI clients	Storage cluster MVIP	443 TCP	(Optional) UI and API access
Management node	monitoring.solidfire.com	443 TCP	Storage cluster reporting to Active IQ

Source	Destination	Port	Description
Storage node MIP	Remote storage cluster MVIP	443 TCP	Remote replication cluster pairing communication
Storage node MIP	Remote storage node MIP	443 TCP	Remote replication cluster pairing communication
SolidFire eSDSsfapp	Per-node UI and API access to create a cluster	2010 UDP	Cluster beacon (to discover nodes to add to a cluster)
iSCSI clients	Storage cluster SVIP	3260 TCP	Client iSCSI communications
iSCSI clients	Storage cluster SIP	3260 TCP	Client iSCSI communications
SOAP server	SolidFire eSDSsfapp	7627 TCP	SOAP web services
System administrator PC	N/A	8080 TCP	System administrator communications
vCenter Server	Management node	8443 TCP	vCenter Plug-in QoSSIOC service

Ports 2181, 2182, and 2183 are needed for are needed for the Element distributed database, and will be dynamically opened from the Element container when you install SolidFire eSDS.

- Use the following commands to open the ports mentioned above:

```
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
```

Configure your host network

- Configure your host network using the best practices provided.

You should complete the steps to configure your host network to ensure a successful installation of SolidFire eSDS.

Complete additional requirements

- Install One Collect, which will be used by NetApp Support for host log collection. You can install One Collect from here. You need a NetApp account to access the download. You can also find the One Collect Installation Guide and Release Notes at the same location.

You must download and install One Collect in order to receive an optimal support experience.

- Install the management node for log collection and to enable NetApp Support access for troubleshooting. For information about management node and installation steps, see here.

Find more information

- NetApp SolidFire Resources Page
- Documentation for earlier versions of NetApp SolidFire and Element products