Install and upgrade software

StorageGRID

NetApp
October 03, 2025

This PDF was generated from https://docs.netapp.com/us-en/storagegrid-115/rhel/installation-overview.html on October 03, 2025. Always check docs.netapp.com for the latest.

Table of Contents

Install and upgrade software . . . 1
- Install Red Hat Enterprise Linux or CentOS . . . 1
  - Installation overview . . . 1
  - Planning and preparation . . . 2
  - Deploying virtual grid nodes . . . 24
  - Configuring the grid and completing installation . . . 48
  - Automating the installation . . . 63
  - Overview of the installation REST API . . . 65
  - Where to go next . . . 66
  - Troubleshooting installation issues . . . 67
  - Example /etc/sysconfig/network-scripts . . . 68
- Install Ubuntu or Debian . . . 70
  - Installation overview . . . 70
  - Planning and preparation . . . 72
  - Deploying virtual grid nodes . . . 94
  - Configuring the grid and completing installation . . . 118
  - Automating the installation . . . 132
  - Overview of the installation REST API . . . 135
  - Where to go next . . . 135
  - Troubleshooting installation issues . . . 136
  - Example /etc/network/interfaces . . . 137
- Install VMware . . . 139
  - Installation overview . . . 139
  - Planning and preparation . . . 140
  - Deploying virtual machine grid nodes in VMware vSphere Web Client . . . 149
  - Configuring the grid and completing installation . . . 157
  - Automating the installation . . . 172
  - Overview of the installation REST API . . . 185
  - Where to go next . . . 186
  - Troubleshooting installation issues . . . 187
- Upgrade software . . . 188
  - About StorageGRID 11.5 . . . 188
  - Upgrade planning and preparation . . . 201
  - Performing the upgrade . . . 212
  - Troubleshooting upgrade issues . . . 224

Install and upgrade software

Install Red Hat Enterprise Linux or CentOS

Learn how to install StorageGRID software in Red Hat Enterprise Linux or CentOS deployments.

- Installation overview
- Planning and preparation
- Deploying virtual grid nodes
- Configuring the grid and completing installation
- Automating the installation
- Overview of the installation REST API
- Where to go next
- Troubleshooting installation issues
- Example /etc/sysconfig/network-scripts

Installation overview

Installing a StorageGRID system in a Red Hat Enterprise Linux (RHEL) or CentOS Linux environment includes three primary steps.

1. **Preparation**: During planning and preparation, you perform the following tasks:
   - Learn about the hardware and storage requirements for StorageGRID.
   - Learn about the specifics of StorageGRID networking so you can configure your network appropriately. For more information, see the StorageGRID networking guidelines.
   - Identify and prepare the physical or virtual servers you plan to use to host your StorageGRID grid nodes.
   - On the servers you have prepared:
     - Install Linux
     - Configure the host network
     - Configure host storage
     - Install Docker
     - Install the StorageGRID host services
2. **Deployment**: Deploy grid nodes using the appropriate user interface. When you deploy grid nodes, they are created as part of the StorageGRID system and connected to one or more networks.
   a. Use the Linux command line and node configuration files to deploy software-based grid nodes on the hosts you prepared in step 1.
   b. Use the StorageGRID Appliance Installer to deploy StorageGRID appliance nodes.

> Hardware-specific installation and integration instructions are not included in the StorageGRID installation procedure. To learn how to install StorageGRID appliances, see the installation and maintenance instructions for your appliance.

3. **Configuration**: When all nodes have been deployed, use the StorageGRIDGrid Manager to configure the grid and complete the installation.

These instructions recommend a standard approach for deploying and configuring a StorageGRID system. See also the information about the following alternative approaches:

- Use a standard orchestration framework such as Ansible, Puppet, or Chef to install RHEL or CentOS, configure networking and storage, install Docker and the StorageGRID host service, and deploy virtual grid nodes.
- Automate the deployment and configuration of the StorageGRID system using a Python configuration script (provided in the installation archive).
- Automate the deployment and configuration of appliance grid nodes with a Python configuration script (available from the installation archive or from the StorageGRID Appliance Installer).
- If you are an advanced developer of StorageGRID deployments, use the installation REST APIs to automate the installation of StorageGRID grid nodes.

Related information

Planning and preparation

Deploying virtual grid nodes

Configuring the grid and completing installation

Automating the installation

Overview of the installation REST API

Network guidelines

Planning and preparation

Before deploying grid nodes and configuring the StorageGRID grid, you must be familiar with the steps and requirements for completing the procedure.

The StorageGRID deployment and configuration procedures assume that you are familiar with the architecture and operation of the StorageGRID system.

You can deploy a single site or multiple sites at one time; however, all sites must meet the minimum requirement of having at least three Storage Nodes.

Before starting a StorageGRID installation, you must:

- Understand StorageGRID's compute requirements, including the minimum CPU and RAM requirements for each node.
- Understand how StorageGRID supports multiple networks for traffic separation, security, and administrative convenience, and have a plan for which networks you intend to attach to each StorageGRID node.

  See the StorageGRID networking guidelines.

- Understand the storage and performance requirements of each type of grid node.
- Identify a set of servers (physical, virtual, or both) that, in aggregate, provide sufficient resources to support the number and type of StorageGRID nodes you plan to deploy.
- Understand the requirements for node migration, if you want to perform scheduled maintenance on physical hosts without any service interruption.
- Gather all networking information in advance. Unless you are using DHCP, gather the IP addresses to assign to each grid node, and the IP addresses of the domain name system (DNS) and network time protocol (NTP) servers that will be used.
- Install, connect, and configure all required hardware, including any StorageGRID appliances, to specifications.

> Hardware-specific installation and integration instructions are not included in the StorageGRID installation procedure. To learn how to install StorageGRID appliances, see the installation and maintenance instructions for your appliance.

- Decide which of the available deployment and configuration tools you want to use.

Related information

Network guidelines

SG100 & SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

Required materials

Before you install StorageGRID, you must gather and prepare required materials.

Item	Notes
NetApp StorageGRID license	You must have a valid, digitally signed NetApp license. **Note**: A non-production license, which can be used for testing and proof of concept grids, is included in the StorageGRID installation archive.
StorageGRID installation archive	You must download the StorageGRID installation archive and extract the files.
Service laptop	The StorageGRID system is installed through a service laptop. The service laptop must have: • Network port • SSH client (for example, PuTTY) • Supported web browser

Item	Notes
StorageGRID documentation	• Release Notes • Instructions for administering StorageGRID

Related information

Downloading and extracting the StorageGRID installation files

Web browser requirements

Administer StorageGRID

Release notes

Downloading and extracting the StorageGRID installation files

You must download the StorageGRID installation archive and extract the required files.

Steps

1. Go to the NetApp Downloads page for StorageGRID.

   NetApp Downloads: StorageGRID

2. Select the button for downloading the latest release, or select another version from the drop-down menu and select **Go**.
3. Sign in with the username and password for your NetApp account.
4. If a Caution/MustRead statement appears, read it and select the check box.

   You must apply any required hotfixes after you install the StorageGRID release. For more information, see the hotfix procedure in the recovery and maintenance instructions.

5. Read the End User License Agreement, select the check box, and then select **Accept & Continue**.
6. In the **Install StorageGRID** column, select the appropriate software.

   Download the `.tgz` or `.zip` archive file for your platform.

   The compressed files contain the RPM files and scripts for Red Hat Enterprise Linux or CentOS.

   > Use the `.zip` file if you are running Windows on the service laptop.

7. Save and extract the archive file.
8. Choose the files you need from the following list.

   The files you need depend on your planned grid topology and how you will deploy your StorageGRID system.

   > The paths listed in the table are relative to the top-level directory installed by the extracted installation archive.

Path and file name	Description
`./rpms/README`	A text file that describes all of the files contained in the StorageGRID download file.
`./rpms/NLF000000.txt`	A free license that does not provide any support entitlement for the product.
`./rpms/StorageGRID-Webscale-Images-`*`version`*`-SHA.rpm`	RPM package for installing the StorageGRID node images on your RHEL or CentOS hosts.
`./rpms/StorageGRID-Webscale-Service-`*`version`*`-SHA.rpm`	RPM package for installing the StorageGRID host service on your RHEL or CentOS hosts.
Deployment scripting tool	**Description**
`./rpms/configure-storagegrid.py`	A Python script used to automate the configuration of a StorageGRID system.
`./rpms/configure-sga.py`	A Python script used to automate the configuration of StorageGRID appliances.
`./rpms/configure-storagegrid.sample.json`	A sample configuration file for use with the `configure-storagegrid.py` script.
`./rpms/storagegrid-ssoauth.py`	An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled.
`./rpms/configure-storagegrid.blank.json`	A blank configuration file for use with the `configure-storagegrid.py` script.
`./rpms/extras/ansible`	Example Ansible role and playbook for configuring RHEL or CentOS hosts for StorageGRID container deployment. You can customize the role or playbook as necessary.

Related information

Maintain & recover

CPU and RAM requirements

Before installing StorageGRID software, verify and configure the hardware so that it is ready to support the StorageGRID system.

For information about supported servers, see the Interoperability Matrix.

Each StorageGRID node requires the following minimum resources:

- CPU cores: 8 per node

- RAM: At least 24 GB per node, and 2 to 16 GB less than the total system RAM, depending on the total RAM available and the amount of non-StorageGRID software running on the system

Ensure that the number of StorageGRID nodes you plan to run on each physical or virtual host does not exceed the number of CPU cores or the physical RAM available. If the hosts are not dedicated to running StorageGRID (not recommended), be sure to consider the resource requirements of the other applications.

> Monitor your CPU and memory usage regularly to ensure that these resources continue to accommodate your workload. For example, doubling the RAM and CPU allocation for virtual Storage Nodes would provide similar resources to those provided for StorageGRID appliance nodes. Additionally, if the amount of metadata per node exceeds 500 GB, consider increasing the RAM per node to 48 GB or more. For information about managing object metadata storage, increasing the Metadata Reserved Space setting, and monitoring CPU and memory usage, see the instructions for administering, monitoring, and upgrading StorageGRID.

If hyperthreading is enabled on the underlying physical hosts, you can provide 8 virtual cores (4 physical cores) per node. If hyperthreading is not enabled on the underlying physical hosts, you must provide 8 physical cores per node.

If you are using virtual machines as hosts and have control over the size and number of VMs, you should use a single VM for each StorageGRID node and size the VM accordingly.

For production deployments, you should not run multiple Storage Nodes on the same physical storage hardware or virtual host. Each Storage Node in a single StorageGRID deployment should be in its own isolated failure domain. You can maximize the durability and availability of object data if you ensure that a single hardware failure can only impact a single Storage Node.

See also the information about storage requirements.

Related information

NetApp Interoperability Matrix Tool

Storage and performance requirements

Administer StorageGRID

Monitor & troubleshoot

Upgrade software

Storage and performance requirements

You must understand the storage requirements for StorageGRID nodes, so you can provide enough space to support the initial configuration and future storage expansion.

StorageGRID nodes require three logical categories of storage:

- **Container pool** — Performance-tier (10K SAS or SSD) storage for the node containers, which will be assigned to the Docker storage driver when you install and configure Docker on the hosts that will support your StorageGRID nodes.
- **System data** — Performance-tier (10K SAS or SSD) storage for per-node persistent storage of system data and transaction logs, which the StorageGRID host services will consume and map into individual nodes.

- **Object data** — Performance-tier (10K SAS or SSD) storage and capacity-tier (NL-SAS/SATA) bulk storage for the persistent storage of object data and object metadata.

You must use RAID-backed block devices for all storage categories. Non-redundant disks, SSDs, or JBODs are not supported. You can use shared or local RAID storage for any of the storage categories; however, if you want to use StorageGRID's node migration capability, you must store both system data and object data on shared storage.

Performance requirements

The performance of the volumes used for the container pool, system data, and object metadata significantly impacts the overall performance of the system. You should use performance-tier (10K SAS or SSD) storage for these volumes to ensure adequate disk performance in terms of latency, input/output operations per second (IOPS), and throughput. You can use capacity-tier (NL-SAS/SATA) storage for the persistent storage of object data.

The volumes used for the container pool, system data, and object data must have write-back caching enabled. The cache must be on a protected or persistent media.

Requirements for hosts that use NetApp AFF storage

If the StorageGRID node uses storage assigned from a NetApp AFF system, confirm that the volume does not have a FabricPool tiering policy enabled. Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.

> Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

Number of hosts required

Each StorageGRID site requires a minimum of three Storage Nodes.

> In a production deployment, do not run more than one Storage Node on a single physical or virtual host. Using a dedicated host for each Storage Node provides an isolated failure domain.

Other types of nodes, such as Admin Nodes or Gateway Nodes, can be deployed on the same hosts, or they can be deployed on their own dedicated hosts as required.

Number of storage volumes for each host

The following table shows the number of storage volumes (LUNs) required for each host and the minimum size required for each LUN, based on which nodes will be deployed on that host.

The maximum tested LUN size is 39 TB.

> These numbers are for each host, not for the entire grid.

LUN purpose	Storage category	Number of LUNs	Minimum size/LUN
Docker storage pool	Container pool	1	Total number of nodes × 100 GB

LUN purpose	Storage category	Number of LUNs	Minimum size/LUN
`/var/local` volume	System data	1 for each node on this host	90 GB
Storage Node	Object data	3 for each Storage Node on this host **Note:** A software-based Storage Node can have 1 to 16 storage volumes; at least 3 storage volumes are recommended.	4,000 GB See Storage requirements for Storage Nodes for more information.
Admin Node audit logs	System data	1 for each Admin Node on this host	200 GB
Admin Node tables	System data	1 for each Admin Node on this host	200 GB

Depending on the audit level configured, the size of user inputs such as S3 object key name, and how much audit log data you need to preserve, you might need to increase the size of the audit log LUN on each Admin Node. As a general rule, a grid generates approximately 1 KB of audit data per S3 operation, which would mean that a 200 GB LUN would support 70 million operations per day or 800 operations per second for two to three days.

Minimum storage space for a host

The following table shows the minimum storage space required for each type of node. You can use this table to determine the minimum amount of storage you must provide to the host in each storage category, based on which nodes will be deployed on that host.

Disk snapshots cannot be used to restore grid nodes. Instead, refer to the recovery and maintenance procedures for each type of node.

Type of node	Container pool	System data	Object data
Storage Node	100 GB	90 GB	4,000 GB
Admin Node	100 GB	490 GB (3 LUNs)	*not applicable*
Gateway Node	100 GB	90 GB	*not applicable*
Archive Node	100 GB	90 GB	*not applicable*

Example: Calculating the storage requirements for a host

Suppose you plan to deploy three nodes on the same host: one Storage Node, one Admin Node, and one Gateway Node. You should provide a minimum of nine storage volumes to the host. You will need a minimum

of 300 GB of performance-tier storage for the node containers, 670 GB of performance-tier storage for system data and transaction logs, and 12 TB of capacity-tier storage for object data.

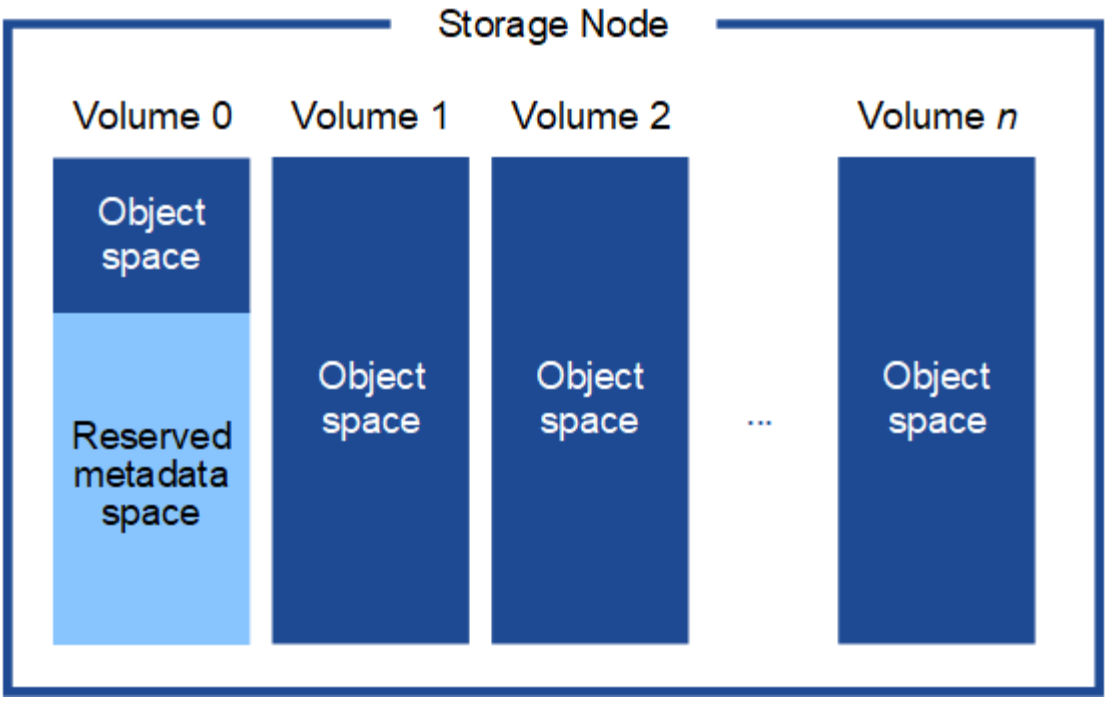
Type of node	LUN purpose	Number of LUNs	LUN size
Storage Node	Docker storage pool	1	300 GB (100 GB/node)
Storage Node	`/var/local` volume	1	90 GB
Storage Node	Object data	3	4,000 GB
Admin Node	`/var/local` volume	1	90 GB
Admin Node	Admin Node audit logs	1	200 GB
Admin Node	Admin Node tables	1	200 GB
Gateway Node	`/var/local` volume	1	90 GB
Total		**9**	**Container pool:** 300 GB **System data:** 670 GB **Object data:** 12,000 GB

Storage requirements for Storage Nodes

A software-based Storage Node can have 1 to 16 storage volumes—3 or more storage volumes are recommended. Each storage volume should be 4 TB or larger.

> An appliance Storage Node can have up to 48 storage volumes.

As shown in the figure, StorageGRID reserves space for object metadata on storage volume 0 of each Storage Node. Any remaining space on storage volume 0 and any other storage volumes in the Storage Node are used exclusively for object data.



To provide redundancy and to protect object metadata from loss, StorageGRID stores three copies of the metadata for all objects in the system at each site. The three copies of object metadata are evenly distributed across all Storage Nodes at each site.

When you assign space to volume 0 of a new Storage Node, you must ensure there is adequate space for that node's portion of all object metadata.

- At a minimum, you must assign at least 4 TB to volume 0.

> If you use only one storage volume for a Storage Node and you assign 4 TB or less to the volume, the Storage Node might enter the Storage Read-Only state on startup and store object metadata only.

- If you are installing a new StorageGRID 11.5 system and each Storage Node has 128 GB or more of RAM, you should assign 8 TB or more to volume 0. Using a larger value for volume 0 can increase the space allowed for metadata on each Storage Node.
- When configuring different Storage Nodes for a site, use the same setting for volume 0 if possible. If a site contains Storage Nodes of different sizes, the Storage Node with the smallest volume 0 will determine the metadata capacity of that site.

For details, go to the instructions for administering StorageGRID and search for "managing object metadata storage."

Administer StorageGRID

Related information

Node container migration requirements

Maintain & recover

Node container migration requirements

The node migration feature allows you to manually move a node from one host to another. Typically, both hosts are in the same physical data center.

Node migration allows you to perform physical host maintenance without disrupting grid operations. You simply move all StorageGRID nodes, one at a time, to another host before taking the physical host offline. Migrating nodes requires only a short downtime for each node and should not affect operation or availability of grid services.

If you want to use the StorageGRID node migration feature, your deployment must meet additional requirements:

- Consistent network interface names across hosts in a single physical data center
- Shared storage for StorageGRID metadata and object repository volumes that is accessible by all hosts in a single physical data center. For example, you might use NetApp E-Series storage arrays.

If you are using virtual hosts and the underlying hypervisor layer supports VM migration, you might want to use this capability instead of StorageGRID's node migration feature. In this case, you can ignore these additional requirements.

Before performing migration or hypervisor maintenance, shut down the nodes gracefully. See the recovery and maintenance instructions for shutting down a grid node.

VMware Live Migration not supported

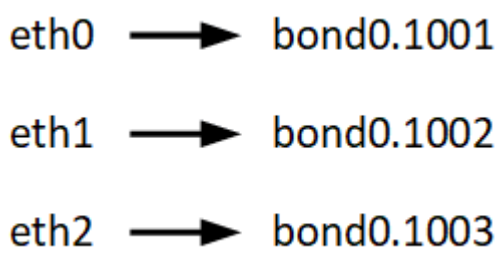
OpenStack Live Migration and VMware live vMotion cause the virtual machine clock time to jump and are not supported for grid nodes of any type. Though rare, incorrect clock times can result in loss of data or configuration updates.

Cold migration is supported. In cold migration, you shut down the StorageGRID nodes before migrating them between hosts. See the procedure for shutting down a grid node in the recovery and maintenance instructions.

Consistent network interface names

In order to move a node from one host to another, the StorageGRID host service needs to have some confidence that the external network connectivity the node has at its current location can be duplicated at the new location. It gets this confidence through the use of consistent network interface names in the hosts.

Suppose, for example, that StorageGRID NodeA running on Host1 has been configured with the following interface mappings:



The lefthand side of the arrows corresponds to the traditional interfaces as viewed from within a StorageGRID container (that is, the Grid, Admin, and Client Network interfaces, respectively). The righthand side of the arrows corresponds to the actual host interfaces providing these networks, which are three VLAN interfaces

subordinate to the same physical interface bond.

Now, suppose you want to migrate NodeA to Host2. If Host2 also has interfaces named bond0.1001, bond0.1002, and bond0.1003, the system will allow the move, assuming that the like-named interfaces will provide the same connectivity on Host2 as they do on Host1. If Host2 does not have interfaces with the same names, the move will not be allowed.

There are many ways to achieve consistent network interface naming across multiple hosts; see “Configuring the host network” for some examples.

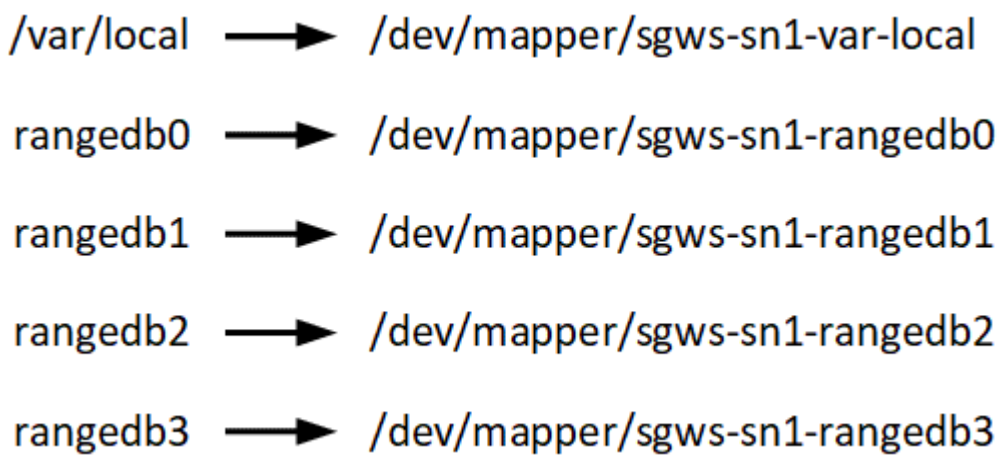
Shared storage

In order to achieve rapid, low-overhead node migrations, the StorageGRID node migration feature does not physically move node data. Instead, node migration is performed as a pair of export and import operations, as follows:

1. During the “node export” operation, a small amount of persistent state data is extracted from the node container running on HostA and cached on that node’s system data volume. Then, the node container on HostA is deinstantiated.
2. During the “node import” operation, the node container on HostB that uses the same network interface and block storage mappings that were in effect on HostA is instantiated. Then, the cached persistent state data is inserted into the new instance.

Given this mode of operation, all of the node’s system data and object storage volumes must be accessible from both HostA and HostB for the migration to be allowed, and to work. In addition, they must have been mapped into the node using names that are guaranteed to refer to the same LUNs on HostA and HostB.

The following example shows one solution for block device mapping for a StorageGRID Storage Node, where DM multipathing is in use on the hosts, and the alias field has been used in `/etc/multipath.conf` to provide consistent, friendly block device names available on all hosts.



Related information

Configuring the host network

Maintain & recover

Web browser requirements

You must use a supported web browser.

Web browser	Minimum supported version
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

You should set the browser window to a recommended width.

Browser width	Pixels
Minimum	1024
Optimum	1280

Deployment tools

You might benefit from automating all or part of the StorageGRID installation.

Automating the deployment might be useful in any of the following cases:

- You already use a standard orchestration framework, such as Ansible, Puppet, or Chef, to deploy and configure physical or virtual hosts.
- You intend to deploy multiple StorageGRID instances.
- You are deploying a large, complex StorageGRID instance.

The StorageGRID host service is installed by a package and driven by configuration files that can be created interactively during a manual installation, or prepared ahead of time (or programmatically) to enable automated installation using standard orchestration frameworks. StorageGRID provides optional Python scripts for automating the configuration of StorageGRID appliances, and the whole StorageGRID system (the “grid”). You can use these scripts directly, or you can inspect them to learn how to use the StorageGRID Installation REST API in grid deployment and configuration tools you develop yourself.

If you are interested in automating all or part of your StorageGRID deployment, review “Automating the installation” before beginning the installation process.

Related information

Overview of the installation REST API

Automating the installation

Preparing the hosts

You must complete the following steps to prepare your physical or virtual hosts for StorageGRID. Note that you can automate many or all of these steps using standard server configuration frameworks such as Ansible, Puppet, or Chef.

Related information

Automating the installation and configuration of the StorageGRID host service

Installing Linux

You must install Red Hat Enterprise Linux or CentOS Linux on all grid hosts. Use the NetApp Interoperability Matrix Tool to get a list of supported versions.

Steps

1. Install Linux on all physical or virtual grid hosts according to the distributor's instructions or your standard procedure.

   > If you are using the standard Linux installer, NetApp recommends selecting the "compute node" software configuration, if available, or "minimal install" base environment. Do not install any graphical desktop environments.

2. Ensure that all hosts have access to package repositories, including the Extras channel.

   You might need these additional packages later in this installation procedure.

3. If swap is enabled:

   a. Run the following command: `$ sudo swapoff --all`

   b. Remove all swap entries from `/etc/fstab` to persist the settings.

   > Failing to disable swap entirely can severely lower performance.

Related information

NetApp Interoperability Matrix Tool

Configuring the host network

After completing the Linux installation on your hosts, you might need to perform some additional configuration to prepare a set of network interfaces on each host that are suitable for mapping into the StorageGRID nodes you will deploy later.

What you'll need

- You have reviewed the StorageGRID networking guidelines.

  Network guidelines

- You have reviewed the information about node container migration requirements.

  Node container migration requirements

- If you are using virtual hosts, you have read the considerations and recommendations for MAC address cloning before configuring the host network.

  Considerations and recommendations for MAC address cloning

> If you are using VMs as hosts, you should select VMXNET 3 as the virtual network adapter. The VMware E1000 network adapter has caused connectivity issues with StorageGRID containers deployed on certain distributions of Linux.

About this task

Grid nodes must be able to access the Grid Network and, optionally, the Admin and Client Networks. You provide this access by creating mappings that associate the host's physical interface to the virtual interfaces for each grid node. When creating host interfaces, use friendly names to facilitate deployment across all hosts, and to enable migration.

The same interface can be shared between the host and one or more nodes. For example, you might use the same interface for host access and node Admin Network access, to facilitate host and node maintenance. Although the same interface can be shared between the host and individual nodes, all must have different IP addresses. IP addresses cannot be shared between nodes or between the host and any node.

You can use the same host network interface to provide the Grid Network interface for all StorageGRID nodes on the host; you can use a different host network interface for each node; or you can do something in between. However, you would not typically provide the same host network interface as both the Grid and Admin Network interfaces for a single node, or as the Grid Network interface for one node and the Client Network interface for another.

You can complete this task in many ways. For example, if your hosts are virtual machines and you are deploying one or two StorageGRID nodes for each host, you can simply create the correct number of network interfaces in the hypervisor, and use a 1-to-1 mapping. If you are deploying multiple nodes on bare metal hosts for production use, you can leverage the Linux networking stack's support for VLAN and LACP for fault tolerance and bandwidth sharing. The following sections provide detailed approaches for both of these examples. You do not need to use either of these examples; you can use any approach that meets your needs.

> Do not use bond or bridge devices directly as the container network interface. Doing so could prevent node start-up caused by a kernel issue with the use of MACVLAN with bond and bridge devices in the container namespace. Instead, use a non-bond device, such as a VLAN or virtual Ethernet (veth) pair. Specify this device as the network interface in the node configuration file.

Related information

Network guidelines

Node container migration requirements

Creating node configuration files

Considerations and recommendations for MAC address cloning

MAC address cloning causes the Docker container to use the MAC address of the host, and the host to use the MAC address of either an address you specify or a randomly generated one. You should use MAC address cloning to avoid the use of promiscuous mode network configurations.

Enabling MAC cloning

In certain environments, security can be enhanced through MAC address cloning because it enables you to use a dedicated virtual NIC for the Admin Network, Grid Network, and Client Network. Having the Docker container use the MAC address of the dedicated NIC on the host allows you to avoid using promiscuous mode

network configurations.

> MAC address cloning is intended to be used with virtual server installations and might not function properly with all physical appliance configurations.

> If a node fails to start due to a MAC cloning targeted interface being busy, you might need to set the link to "down" before starting node. Additionally, it is possible that the virtual environment might prevent MAC cloning on a network interface while the link is up. If a node fails to set the MAC address and start due to an interface being busy, setting the link to "down" before starting the node might fix the issue.

MAC address cloning is disabled by default and must be set by node configuration keys. You should enable it when you install StorageGRID.

There is one key for each network:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Setting the key to "true" causes the Docker container to use the MAC address of the host's NIC. Additionally, the host will then use the MAC address of the specified container network. By default, the container address is a randomly generated address, but if you have set one using the `_NETWORK_MAC` node configuration key, that address is used instead. The host and container will always have different MAC addresses.

> Enabling MAC cloning on a virtual host without also enabling promiscuous mode on the hypervisor might cause Linux host networking using the host's interface to stop working.

MAC cloning use cases

There are two use cases to consider with MAC cloning:

- MAC cloning not enabled: When the `_CLONE_MAC` key in the node configuration file is not set, or set to "false," the host will use the host NIC MAC and the container will have a StorageGRID-generated MAC unless a MAC is specified in the `_NETWORK_MAC` key. If an address is set in the `_NETWORK_MAC` key, the container will have the address specified in the `_NETWORK_MAC` key. This configuration of keys requires the use of promiscuous mode.
- MAC cloning enabled: When the `_CLONE_MAC` key in the node configuration file is set to "true," the container uses the host NIC MAC, and the host uses a StorageGRID-generated MAC unless a MAC is specified in the `_NETWORK_MAC` key. If an address is set in the `_NETWORK_MAC` key, the host uses the specified address instead of a generated one. In this configuration of keys, you should not use promiscuous mode.

> If you do not want to use MAC address cloning and would rather allow all interfaces to receive and transmit data for MAC addresses other than the ones assigned by the hypervisor, ensure that the security properties at the virtual switch and port group levels are set to **Accept** for Promiscuous Mode, MAC Address Changes, and Forged Transmits. The values set on the virtual switch can be overridden by the values at the port group level, so ensure that settings are the same in both places.

To enable MAC cloning, see the instructions for creating node configuration files.

MAC cloning example

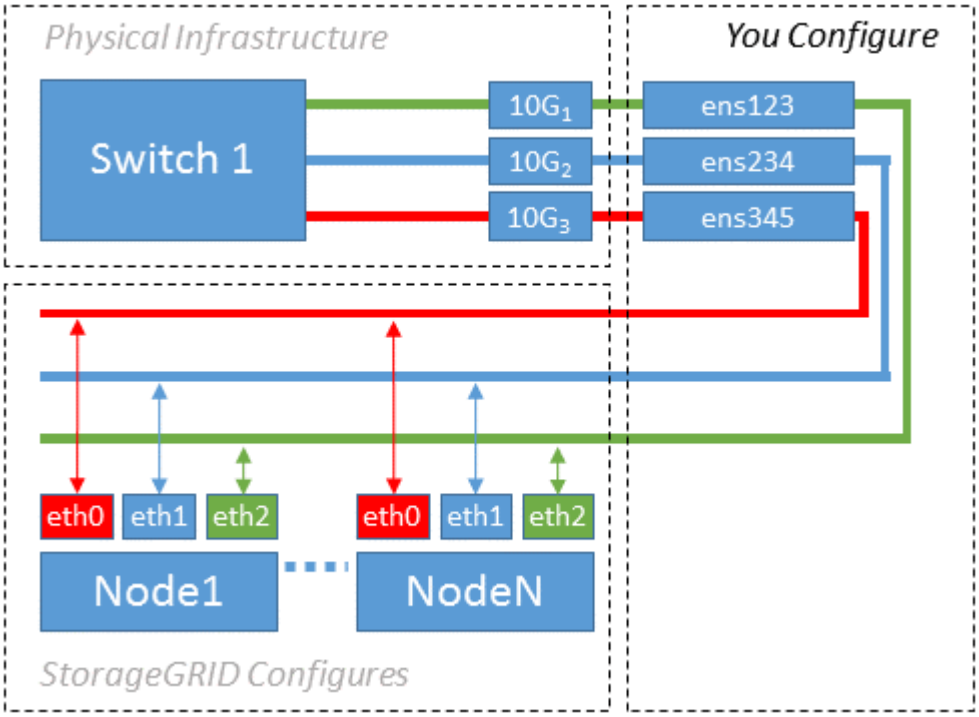
Example of MAC cloning enabled with a host having MAC address of 11:22:33:44:55:66 for the interface ens256 and the following keys in the node configuration file:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Result: the host MAC for ens256 is b2:9c:02:c2:27:10 and the Admin Network MAC is 11:22:33:44:55:66

Example 1: 1-to-1 mapping to physical or virtual NICs

Example 1 describes a simple physical interface mapping that requires little or no host-side configuration.



The Linux operating system creates the `ensXYZ` interfaces automatically during installation or boot, or when the interfaces are hot-added. No configuration is required other than ensuring that the interfaces are set to come up automatically after boot. You do have to determine which `ensXYZ` corresponds to which StorageGRID network (Grid, Admin, or Client) so you can provide the correct mappings later in the configuration process.

Note that the figure show multiple StorageGRID nodes; however, you would normally use this configuration for single-node VMs.

If Switch 1 is a physical switch, you should configure the ports connected to interfaces 10G1 through 10G3 for access mode, and place them on the appropriate VLANs.

Example 2: LACP bond carrying VLANs

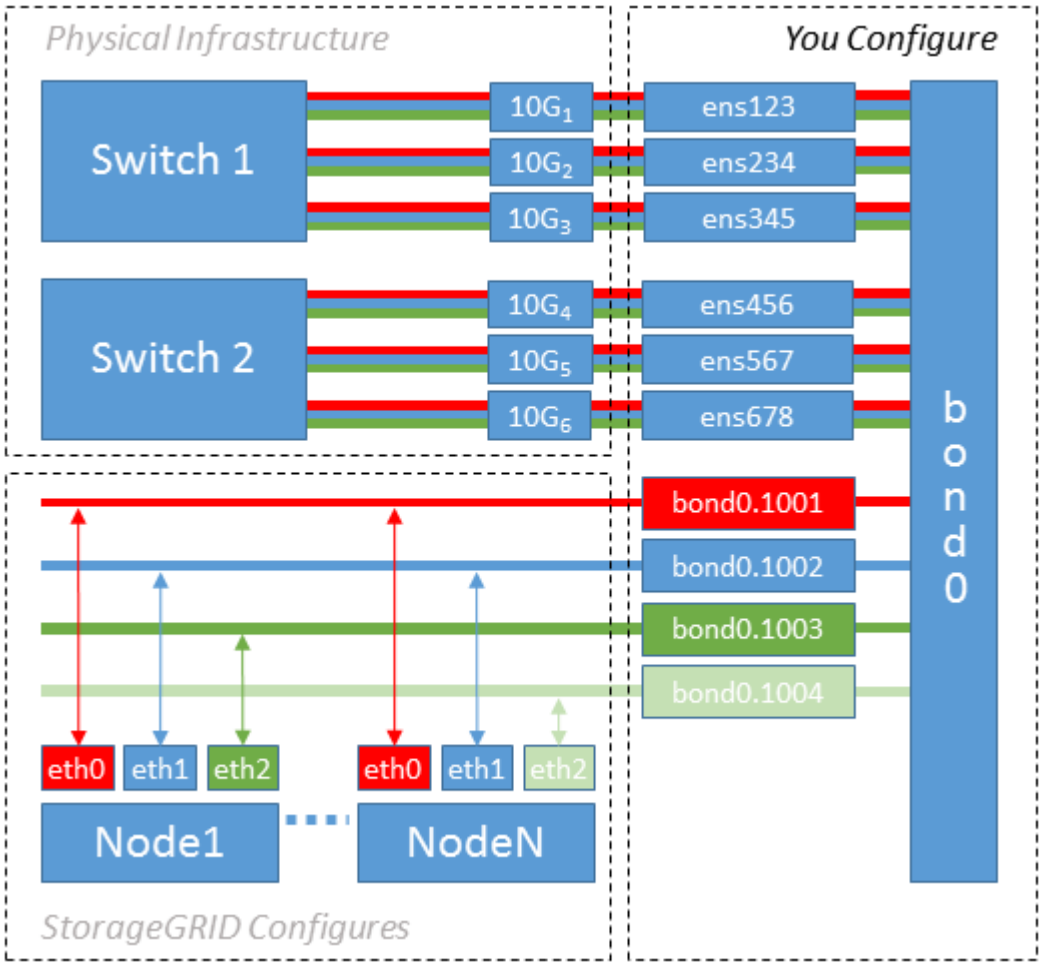
Example 2 assumes you are familiar with bonding network interfaces and with creating

VLAN interfaces on the Linux distribution you are using.

Example 2 describes a generic, flexible, VLAN-based scheme that facilitates the sharing of all available network bandwidth across all nodes on a single host. This example is particularly applicable to bare metal hosts.

To understand this example, suppose you have three separate subnets for the Grid, Admin, and Client Networks at each data center. The subnets are on separate VLANs (1001, 1002, and 1003) and are presented to the host on a LACP-bonded trunk port (bond0). You would configure three VLAN interfaces on the bond: bond0.1001, bond0.1002, and bond0.1003.

If you require separate VLANs and subnets for node networks on the same host, you can add VLAN interfaces on the bond and map them into the host (shown as bond0.1004 in the illustration).



Steps

1. Aggregate all physical network interfaces that will be used for StorageGRID network connectivity into a single LACP bond.

   Use the same name for the bond on every host, for example, bond0.

2. Create VLAN interfaces that use this bond as their associated “physical device,” using the standard VLAN interface naming convention `physdev-name.VLAN ID`.

   Note that steps 1 and 2 require appropriate configuration on the edge switches terminating the other ends of the network links. The edge switch ports must also be aggregated into a LACP port channel, configured

as a trunk, and allowed to pass all required VLANs.

Sample interface configuration files for this per-host networking configuration scheme are provided.

Related information

Example /etc/sysconfig/network-scripts

Configuring host storage

You must allocate block storage volumes to each host.

What you'll need

You have reviewed the following topics, which provide information you need to accomplish this task:

- Storage and performance requirements
- Node container migration requirements

About this task

When allocating block storage volumes (LUNs) to hosts, use the tables in "Storage requirements" to determine the following:

- Number of volumes required for each host (based on the number and types of nodes that will be deployed on that host)
- Storage category for each volume (that is, System Data or Object Data)
- Size of each volume

You will use this information as well as the persistent name assigned by Linux to each physical volume when you deploy StorageGRID nodes on the host.

> You do not need to partition, format, or mount any of these volumes; you just need to ensure they are visible to the hosts.

Avoid using "raw" special device files (`/dev/sdb`, for example) as you compose your list of volume names. These files can change across reboots of the host, which will impact proper operation of the system. If you are using iSCSI LUNs and device mapper multipathing, consider using multipath aliases in the `/dev/mapper` directory, especially if your SAN topology includes redundant network paths to the shared storage. Alternatively, you can use the system-created softlinks under `/dev/disk/by-path/` for your persistent device names.

For example:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Results will differ for each installation.

Assign friendly names to each of these block storage volumes to simplify the initial StorageGRID installation and future maintenance procedures. If you are using the device mapper multipath driver for redundant access to shared storage volumes, you can use the `alias` field in your `/etc/multipath.conf` file.

For example:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

This will cause the aliases to appear as block devices in the `/dev/mapper` directory on the host, allowing you to specify a friendly, easily-validated name whenever a configuration or maintenance operation requires specifying a block storage volume.

> If you are setting up shared storage to support StorageGRID node migration and using device mapper multipathing, you can create and install a common `/etc/multipath.conf` on all co-located hosts. Just make sure to use a different Docker storage volume on each host. Using aliases and including the target hostname in the alias for each Docker storage volume LUN will make this easy to remember and is recommended.

Related information

Installing Docker

Configuring the Docker storage volume

Before installing Docker, you might need to format the Docker storage volume and mount it on `/var/lib/docker`.

About this task

You can skip these steps if you plan to use local storage for the Docker storage volume and have sufficient space available on the host partition containing `/var/lib`.

Steps

1. Create a file system on the Docker storage volume:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Mount the Docker storage volume:

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Add an entry for docker-storage-volume-device to /etc/fstab.

   This step ensures that the storage volume will remount automatically after host reboots.

Installing Docker

The StorageGRID system runs on Red Hat Enterprise Linux or CentOS as a collection of Docker containers. Before you can install StorageGRID, you must install Docker.

Steps

1. Install Docker by following the instructions for your Linux distribution.

   > If Docker is not included with your Linux distribution, you can download it from the Docker website.

2. Ensure Docker has been enabled and started by running the following two commands:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirm you have installed the expected version of Docker by entering the following:

```
sudo docker version
```

The Client and Server versions must be 1.10.3 or later.

```
Client:
  Version: 1.10.3
  API version: 1.22
  Package version: docker-common-1.10.3-46.el7.14.x86_64
  Go version: go1.6.2
  Git commit: 5206701-unsupported
  Built: Mon Aug 29 14:00:01 2016
  OS/Arch: linux/amd64

Server:
  Version: 1.10.3
  API version: 1.22
  Package version: docker-common-1.10.3-46.el7.14.x86_64
  Go version: go1.6.2
  Git commit: 5206701-unsupported
  Built: Mon Aug 29 14:00:01 2016
  OS/Arch: linux/amd64
```

Related information

Configuring host storage

Installing StorageGRID host services

You use the StorageGRID RPM package to install the StorageGRID host services.

About this task

These instructions describe how to install the host services from the RPM packages. As an alternative, you can use the Yum repository metadata included in the installation archive to install the RPM packages remotely. See the Yum repository instructions for your Linux operating system.

Steps

1. Copy the StorageGRID RPM packages to each of your hosts, or make them available on shared storage.

   For example, place them in the `/tmp` directory, so you can use the example command in the next step.

2. Log in to each host as root or using an account with sudo permission, and run the following commands in the order specified:

   ```
   sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Images-
   version-SHA.rpm
   ```

   ```
   sudo yum --nogpgcheck localinstall /tmp/StorageGRID-Webscale-Service-
   version-SHA.rpm
   ```

You must install the Images package first, and the Service package second.

If you placed the packages in a directory other than `/tmp`, modify the command to reflect the path you used.

Deploying virtual grid nodes

To deploy virtual grid nodes on Red Hat Enterprise Linux or CentOS hosts, you create node configuration files for all nodes, validate the files, and start the StorageGRID host service, which starts the nodes. If you need to deploy any StorageGRID appliance Storage Nodes, see the installation and maintenance instructions for the appliance after you have deployed all virtual nodes.

- Creating node configuration files
- Validating the StorageGRID configuration
- Starting the StorageGRID host service

Related information

SG100 & SG1000 services appliances

SG5600 storage appliances

SG5700 storage appliances

SG6000 storage appliances

Creating node configuration files

Node configuration files are small text files that provide the information the StorageGRID host service needs to start a node and connect it to the appropriate network and block storage resources. Node configuration files are used for virtual nodes and are not used for appliance nodes.

Where do I put the node configuration files?

You must place the configuration file for each StorageGRID node in the `/etc/storagegrid/nodes` directory on the host where the node will run. For example, if you plan to run one Admin Node, one Gateway Node, and one Storage Node on HostA, you must place three node configuration files in `/etc/storagegrid/nodes` on HostA. You can create the configuration files directly on each host using a text editor, such as vim or nano, or you can create them elsewhere and move them to each host.

What do I name the node configuration files?

The names of the configuration files are significant. The format is `node-name.conf`, where `node-name` is a name you assign to the node. This name appears in the StorageGRID Installer and is used for node maintenance operations, such as node migration.

Node names must follow these rules:

- Must be unique
- Must start with a letter
- Can contain the characters A through Z and a through z
- Can contain the numbers 0 through 9
- Can contain one or more hyphens (-)
- Must be no more than 32 characters, not including the `.conf` extension

Any files in `/etc/storagegrid/nodes` that do not follow these naming conventions will not be parsed by the host service.

If you have a multi-site topology planned for your grid, a typical node naming scheme might be:

```
site-nodetype-nodenumber.conf
```

For example, you might use `dc1-adm1.conf` for the first Admin Node in Data Center 1, and `dc2-sn3.conf` for the third Storage Node in Data Center 2. However, you can use any scheme you like, as long as all node names follow the naming rules.

What is in a node configuration file?

The configuration files contain key/value pairs, with one key and one value per line. For each key/value pair, you must follow these rules:

- The key and the value must be separated by an equal sign (=) and optional whitespace.
- The keys can contain no spaces.
- The values can contain embedded spaces.
- Any leading or trailing whitespace is ignored.

Some keys are required for every node, while others are optional or only required for certain node types.

The table defines the acceptable values for all supported keys. In the middle column:

R: required
BP: best practice
O: optional

Key	R, BP, or O?	Value
ADMIN_IP	BP	Grid Network IPv4 address of the primary Admin Node for the grid to which this node belongs. Use the same value you specified for GRID_NETWORK_IP for the grid node with NODE_TYPE = VM_Admin_Node and ADMIN_ROLE = Primary. If you omit this parameter, the node attempts to discover a primary Admin Node using mDNS. See “How grid nodes discover the primary Admin Node.” **Note**: This value is ignored, and might be prohibited, on the primary Admin Node.
ADMIN_NETWORK_CONFIG	O	DHCP, STATIC, or DISABLED
ADMIN_NETWORK_ESL	O	Comma-separated list of subnets in CIDR notation to which this node should communicate via the Admin Network gateway. Example: 172.16.0.0/21,172.17.0.0/21
ADMIN_NETWORK_GATEWAY	O (**R**)	IPv4 address of the local Admin Network gateway for this node. Must be on the subnet defined by ADMIN_NETWORK_IP and ADMIN_NETWORK_MASK. This value is ignored for DHCP-configured networks. **Note**: This parameter is required if ADMIN_NETWORK_ESL is specified. Examples: • 1.1.1.1 • 10.224.4.81

Key	R, BP, or O?	Value
ADMIN_NETWORK_IP	O	IPv4 address of this node on the Admin Network. This key is only required when ADMIN_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 1.1.1.1 • 10.224.4.81
ADMIN_NETWORK_MAC	O	The MAC address for the Admin Network interface in the container. This field is optional. If omitted, a MAC address will be generated automatically. Must be 6 pairs of hexadecimal digits separated by colons. Example: b2:9c:02:c2:27:10
ADMIN_NETWORK_MASK	O	IPv4 netmask for this node, on the Admin Network. This key is only required when ADMIN_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 255.255.255.0 • 255.255.248.0

Key	R, BP, or O?	Value
ADMIN_NETWORK_MTU	O	The maximum transmission unit (MTU) for this node on the Admin Network. Do not specify if ADMIN_NETWORK_CONFIG = DHCP. If specified, the value must be between 1280 and 9216. If omitted, 1500 is used. If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value. **IMPORTANT**: The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur. Examples: • 1500 • 8192

Key	R, BP, or O?	Value
ADMIN_NETWORK_TARGET	BP	Name of the host device that you will use for Admin Network access by the StorageGRID node. Only network interface names are supported. Typically, you use a different interface name than what was specified for GRID_NETWORK_TARGET or CLIENT_NETWORK_TARGET. **Note**: Do not use bond or bridge devices as the network target. Either configure a VLAN (or other virtual interface) on top of the bond device, or use a bridge and virtual Ethernet (veth) pair. **Best practice:** Specify a value even if this node will not initially have an Admin Network IP address. Then you can add an Admin Network IP address later, without having to reconfigure the node on the host. Examples: • bond0.1002 • ens256
ADMIN_NETWORK_TARGET_TYPE	O	Interface (This is the only supported value.)

Key	R, BP, or O?	Value
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	True or False Set the key to "true" to cause the StorageGRID container use the MAC address of the host host target interface on the Admin Network. **Best practice:** In networks where promiscuous mode would be required, use the ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC key instead. For more details on MAC cloning, see the considerations and recommendations for MAC address cloning. Considerations and recommendations for MAC address cloning
ADMIN_ROLE	**R**	Primary or Non-Primary This key is only required when NODE_TYPE = VM_Admin_Node; do not specify it for other node types.
BLOCK_DEVICE_AUDIT_LOGS	**R**	Path and name of the block device special file this node will use for persistent storage of audit logs. This key is only required for nodes with NODE_TYPE = VM_Admin_Node; do not specify it for other node types. Examples: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-adm1-audit-logs`

Key	R, BP, or O?	Value
BLOCK_DEVICE_RANGEDB_00 BLOCK_DEVICE_RANGEDB_01 BLOCK_DEVICE_RANGEDB_02 BLOCK_DEVICE_RANGEDB_03 BLOCK_DEVICE_RANGEDB_04 BLOCK_DEVICE_RANGEDB_05 BLOCK_DEVICE_RANGEDB_06 BLOCK_DEVICE_RANGEDB_07 BLOCK_DEVICE_RANGEDB_08 BLOCK_DEVICE_RANGEDB_09 BLOCK_DEVICE_RANGEDB_10 BLOCK_DEVICE_RANGEDB_11 BLOCK_DEVICE_RANGEDB_12 BLOCK_DEVICE_RANGEDB_13 BLOCK_DEVICE_RANGEDB_14 BLOCK_DEVICE_RANGEDB_15	**R**	Path and name of the block device special file this node will use for persistent object storage. This key is only required for nodes with NODE_TYPE = VM_Storage_Node; do not specify it for other node types. Only BLOCK_DEVICE_RANGEDB_00 is required; the rest are optional. The block device specified for BLOCK_DEVICE_RANGEDB_00 must be at least 4 TB; the others can be smaller. **Note**: Do not leave gaps. If you specify BLOCK_DEVICE_RANGEDB_05, you must also specify BLOCK_DEVICE_RANGEDB_04. Examples: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-sn1-rangedb-0`

Key	R, BP, or O?	Value
BLOCK_DEVICE_TABLES	**R**	Path and name of the block device special file this node will use for persistent storage of database tables. This key is only required for nodes with NODE_TYPE = VM_Admin_Node; do not specify it for other node types. Examples: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-adm1-tables`
BLOCK_DEVICE_VAR_LOCAL	**R**	Path and name of the block device special file this node will use for its /var/local persistent storage. Examples: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-sn1-var-local`
CLIENT_NETWORK_CONFIG	O	DHCP, STATIC, or DISABLED

Key	R, BP, or O?	Value
CLIENT_NETWORK_GATEWAY	O	IPv4 address of the local Client Network gateway for this node, which must be on the subnet defined by CLIENT_NETWORK_IP and CLIENT_NETWORK_MASK. This value is ignored for DHCP-configured networks. Examples: • 1.1.1.1 • 10.224.4.81
CLIENT_NETWORK_IP	O	IPv4 address of this node on the Client Network. This key is only required when CLIENT_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 1.1.1.1 • 10.224.4.81
CLIENT_NETWORK_MAC	O	The MAC address for the Client Network interface in the container. This field is optional. If omitted, a MAC address will be generated automatically. Must be 6 pairs of hexadecimal digits separated by colons. Example: b2:9c:02:c2:27:20
CLIENT_NETWORK_MASK	O	IPv4 netmask for this node on the Client Network. This key is only required when CLIENT_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 255.255.255.0 • 255.255.248.0

Key	R, BP, or O?	Value
CLIENT_NETWORK_MTU	O	The maximum transmission unit (MTU) for this node on the Client Network. Do not specify if CLIENT_NETWORK_CONFIG = DHCP. If specified, the value must be between 1280 and 9216. If omitted, 1500 is used. If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value. **IMPORTANT**: The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur. Examples: • 1500 • 8192

Key	R, BP, or O?	Value
CLIENT_NETWORK_TARGET	BP	Name of the host device that you will use for Client Network access by the StorageGRID node. Only network interface names are supported. Typically, you use a different interface name than what was specified for GRID_NETWORK_TARGET or ADMIN_NETWORK_TARGET. **Note**: Do not use bond or bridge devices as the network target. Either configure a VLAN (or other virtual interface) on top of the bond device, or use a bridge and virtual Ethernet (veth) pair. **Best practice:** Specify a value even if this node will not initially have a Client Network IP address. Then you can add a Client Network IP address later, without having to reconfigure the node on the host. Examples: • bond0.1003 • ens423
CLIENT_NETWORK_TARGET_TYPE	O	Interface (This is only supported value.)

Key	R, BP, or O?	Value
CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	True or False Set the key to "true" to cause the StorageGRID container to use the MAC address of the host target interface on the Client Network. **Best practice:** In networks where promiscuous mode would be required, use the CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC key instead. For more details on MAC cloning, see the considerations and recommendations for MAC address cloning. Considerations and recommendations for MAC address cloning
GRID_NETWORK_CONFIG	BP	STATIC or DHCP (Defaults to STATIC if not specified.)
GRID_NETWORK_GATEWAY	**R**	IPv4 address of the local Grid Network gateway for this node, which must be on the subnet defined by GRID_NETWORK_IP and GRID_NETWORK_MASK. This value is ignored for DHCP-configured networks. If the Grid Network is a single subnet with no gateway, use either the standard gateway address for the subnet (X.Y.Z.1) or this node's GRID_NETWORK_IP value; either value will simplify potential future Grid Network expansions.

Key	R, BP, or O?	Value
GRID_NETWORK_IP	**R**	IPv4 address of this node on the Grid Network. This key is only required when GRID_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 1.1.1.1 • 10.224.4.81
GRID_NETWORK_MAC	O	The MAC address for the Grid Network interface in the container. This field is optional. If omitted, a MAC address will be generated automatically. Must be 6 pairs of hexadecimal digits separated by colons. Example: b2:9c:02:c2:27:30
GRID_NETWORK_MASK	O	IPv4 netmask for this node on the Grid Network. This key is only required when GRID_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 255.255.255.0 • 255.255.248.0

Key	R, BP, or O?	Value
GRID_NETWORK_MTU	O	The maximum transmission unit (MTU) for this node on the Grid Network. Do not specify if GRID_NETWORK_CONFIG = DHCP. If specified, the value must be between 1280 and 9216. If omitted, 1500 is used. If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value. **IMPORTANT**: The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur. **IMPORTANT**: For the best network performance, all nodes should be configured with similar MTU values on their Grid Network interfaces. The **Grid Network MTU mismatch** alert is triggered if there is a significant difference in MTU settings for the Grid Network on individual nodes. The MTU values do not have to be the same for all network types. Examples: • 1500 • 8192

Key	R, BP, or O?	Value
GRID_NETWORK_TARGET	**R**	Name of the host device that you will use for Grid Network access by the StorageGRID node. Only network interface names are supported. Typically, you use a different interface name than what was specified for ADMIN_NETWORK_TARGET or CLIENT_NETWORK_TARGET. **Note**: Do not use bond or bridge devices as the network target. Either configure a VLAN (or other virtual interface) on top of the bond device, or use a bridge and virtual Ethernet (veth) pair. Examples: • bond0.1001 • ens192
GRID_NETWORK_TARGET_TYPE	O	Interface (This is the only supported value.)
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	True or False Set the value of the key to "true" to cause the StorageGRID container to use the MAC address of the host target interface on the Grid Network. **Best practice:** In networks where promiscuous mode would be required, use the GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC key instead. For more details on MAC cloning, see the considerations and recommendations for MAC address cloning. Considerations and recommendations for MAC address cloning

Key	R, BP, or O?	Value
MAXIMUM_RAM	O	The maximum amount of RAM that this node is allowed to consume. If this key is omitted, the node has no memory restrictions. When setting this field for a production-level node, specify a value that is at least 24 GB and 16 to 32 GB less than the total system RAM. **Note**: The RAM value affects a node's actual metadata reserved space. See the instructions for administering StorageGRID for a description of what Metadata Reserved Space is. The format for this field is `<number><unit>`, where `<unit>` can be `b`, `k`, `m`, or `g`. Examples: 24g 38654705664b **Note**: If you want to use this option, you must enable kernel support for memory cgroups.
NODE_TYPE	**R**	Type of node: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway

Key	R, BP, or O?	Value
PORT_REMAP	O	Remaps any port used by a node for internal grid node communications or external communications. Remapping ports is necessary if enterprise networking policies restrict one or more ports used by StorageGRID, as described in “Internal grid node communications” or “External communications.” **IMPORTANT**: Do not remap the ports you are planning to use to configure load balancer endpoints. **Note**: If only PORT_REMAP is set, the mapping that you specify is used for both inbound and outbound communications. If PORT_REMAP_INBOUND is also specified, PORT_REMAP applies only to outbound communications. The format used is: `<network type>/<protocol>/<default port used by grid node>/<new port>`, where `<network type>` is grid, admin, or client, and protocol is tcp or udp. For example: `PORT_REMAP = client/tcp/18082/443`

Key	R, BP, or O?	Value
PORT_REMAP_INBOUND	O	Remaps inbound communications to the specified port. If you specify PORT_REMAP_INBOUND but do not specify a value for PORT_REMAP, outbound communications for the port are unchanged. **IMPORTANT**: Do not remap the ports you are planning to use to configure load balancer endpoints. The format used is: `<network type>/<protocol:>/<remapped port >/<default port used by grid node>`, where `<network type>` is grid, admin, or client, and protocol is tcp or udp. For example: `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Related information

How grid nodes discover the primary Admin Node

Network guidelines

Administer StorageGRID

How grid nodes discover the primary Admin Node

Grid nodes communicate with the primary Admin Node for configuration and management. Each grid node must know the IP address of the primary Admin Node on the Grid Network.

To ensure that a grid node can access the primary Admin Node, you can do either of the following when deploying the node:

- You can use the ADMIN_IP parameter to enter the primary Admin Node's IP address manually.
- You can omit the ADMIN_IP parameter to have the grid node discover the value automatically. Automatic discovery is especially useful when the Grid Network uses DHCP to assign the IP address to the primary Admin Node.

Automatic discovery of the primary Admin Node is accomplished using a multicast Domain Name System (mDNS). When the primary Admin Node first starts up, it publishes its IP address using mDNS. Other nodes on the same subnet can then query for the IP address and acquire it automatically. However, because multicast IP

traffic is not normally routable across subnets, nodes on other subnets cannot acquire the primary Admin Node's IP address directly.

> If you use automatic discovery:
>
> - You must include the ADMIN_IP setting for at least one grid node on any subnets that the primary Admin Node is not directly attached to. This grid node will then publish the primary Admin Node's IP address for other nodes on the subnet to discover with mDNS.
> - Ensure that your network infrastructure supports passing multi-cast IP traffic within a subnet.

Example node configuration files

You can use the example node configuration files to help set up the node configuration files for your StorageGRID system. The examples show node configuration files for all types of grid nodes.

For most nodes, you can add Admin and Client Network addressing information (IP, mask, gateway, and so on) when you configure the grid using the Grid Manager or the Installation API. The exception is the primary Admin Node. If you want to browse to the Admin Network IP of the primary Admin Node to complete grid configuration (because the Grid Network is not routed, for example), you must configure the Admin Network connection for the primary Admin Node in its node configuration file. This is shown in the example.

> In the examples, the Client Network target has been configured as a best practice, even though the Client Network is disabled by default.

Example for primary Admin Node

Example file name: `/etc/storagegrid/nodes/dc1-adm1.conf`

Example file contents:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Example for Storage Node

Example file name: `/etc/storagegrid/nodes/dc1-sn1.conf`

Example file contents:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Example for Archive Node

Example file name: `/etc/storagegrid/nodes/dc1-arc1.conf`

Example file contents:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Example for Gateway Node

Example file name: `/etc/storagegrid/nodes/dc1-gw1.conf`

Example file contents:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Example for a non-primary Admin Node

Example file name: `/etc/storagegrid/nodes/dc1-adm2.conf`

Example file contents:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validating the StorageGRID configuration

After creating configuration files in `/etc/storagegrid/nodes` for each of your StorageGRID nodes, you must validate the contents of those files.

To validate the contents of the configuration files, run the following command on each host:

```
sudo storagegrid node validate all
```

If the files are correct, the output shows **PASSED** for each configuration file, as shown in the example.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

> For an automated installation, you can suppress this output by using the `-q` or `--quiet` options in the `storagegrid` command (for example, `storagegrid --quiet…`). If you suppress the output, the command will have a non-zero exit value if any configuration warnings or errors were detected.

If the configuration files are incorrect, the issues are shown as **WARNING** and **ERROR**, as shown in the example. If any configuration errors are found, you must correct them before you continue with the installation.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Starting the StorageGRID host service

To start your StorageGRID nodes, and ensure they restart after a host reboot, you must enable and start the StorageGRID host service.

Steps

1. Run the following commands on each host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Run the following command to ensure the deployment is proceeding:

```
sudo storagegrid node status node-name
```

For any node that returns a status of “Not-Running” or “Stopped”, run the following command:

```
sudo storagegrid node start node-name
```

3. If you have previously enabled and started the StorageGRID host service (or if you are unsure if the service has been enabled and started), also run the following command:

```
sudo systemctl reload-or-restart storagegrid
```

Configuring the grid and completing installation

You complete installation by configuring the StorageGRID system from the Grid Manager on the primary Admin Node.

- Navigating to the Grid Manager
- Specifying the StorageGRID license information
- Adding sites
- Specifying Grid Network subnets
- Approving pending grid nodes
- Specifying Network Time Protocol server information
- Specifying Domain Name System server information
- Specifying the StorageGRID system passwords
- Reviewing your configuration and completing installation
- Post-installation guidelines

Navigating to the Grid Manager

You use the Grid Manager to define all of the information required to configure your StorageGRID system.

What you’ll need

The primary Admin Node must be deployed and have completed the initial startup sequence.

Steps

1. Open your web browser and navigate to one of the following addresses:

   `https://primary_admin_node_ip`

   `client_network_ip`

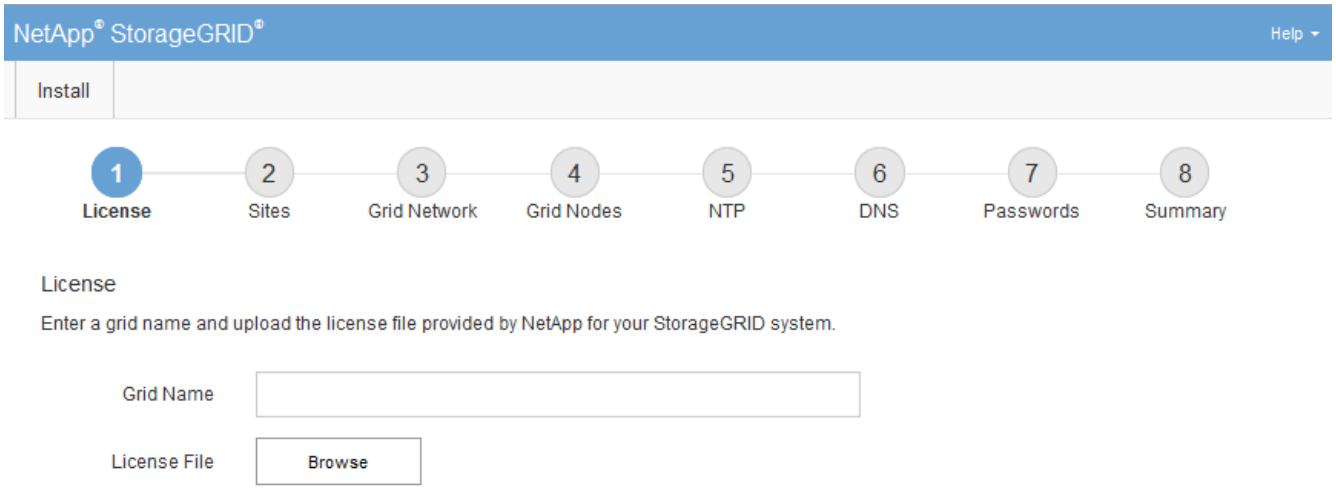
Alternatively, you can access the Grid Manager on port 8443:

```
https://primary_admin_node_ip:8443
```

> You can use the IP address for the primary Admin Node IP on the Grid Network or on the Admin Network, as appropriate for your network configuration.

2. Click **Install a StorageGRID system**.

   The page used to configure a StorageGRID system appears.



Specifying the StorageGRID license information

You must specify the name for your StorageGRID system and upload the license file provided by NetApp.

Steps

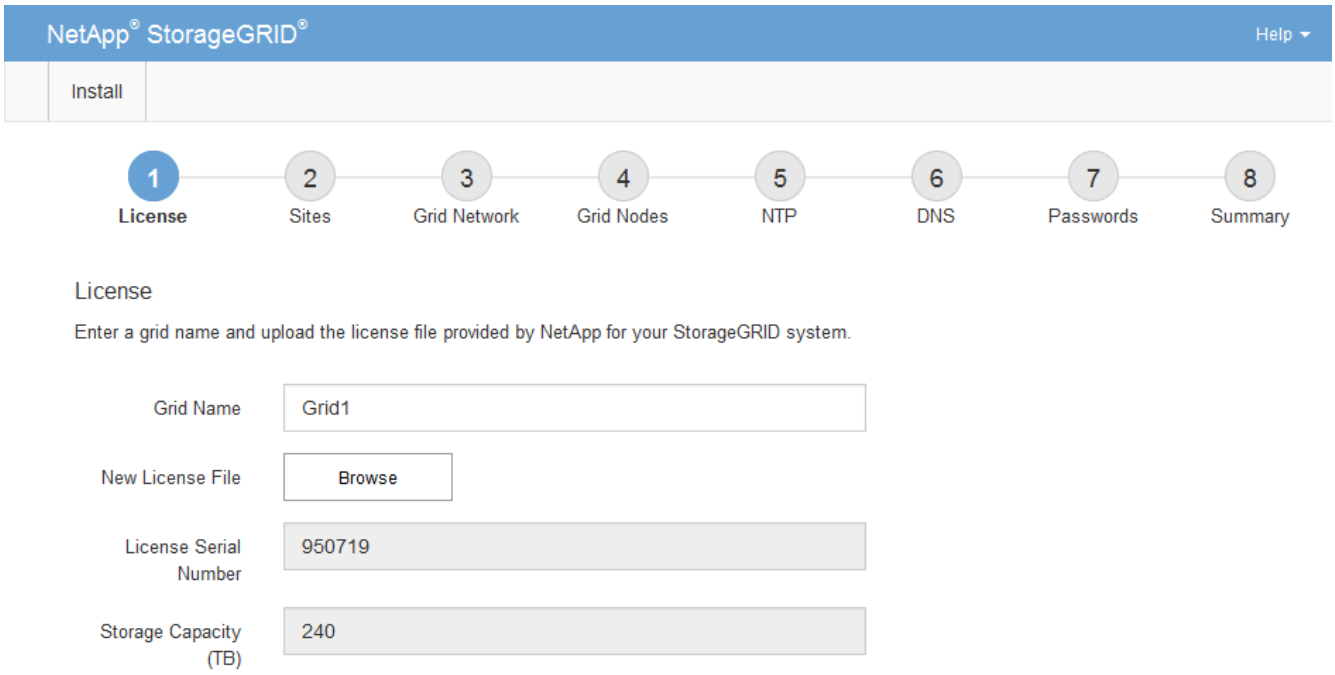
1. On the License page, enter a meaningful name for your StorageGRID system in **Grid Name**.

   After installation, the name is displayed at the top of the Nodes menu.

2. Click **Browse**, locate the NetApp License File (`NLFunique_id.txt`), and click **Open**.

   The license file is validated, and the serial number and licensed storage capacity are displayed.

> The StorageGRID installation archive includes a free license that does not provide any support entitlement for the product. You can update to a license that offers support after installation.



3. Click **Next**.

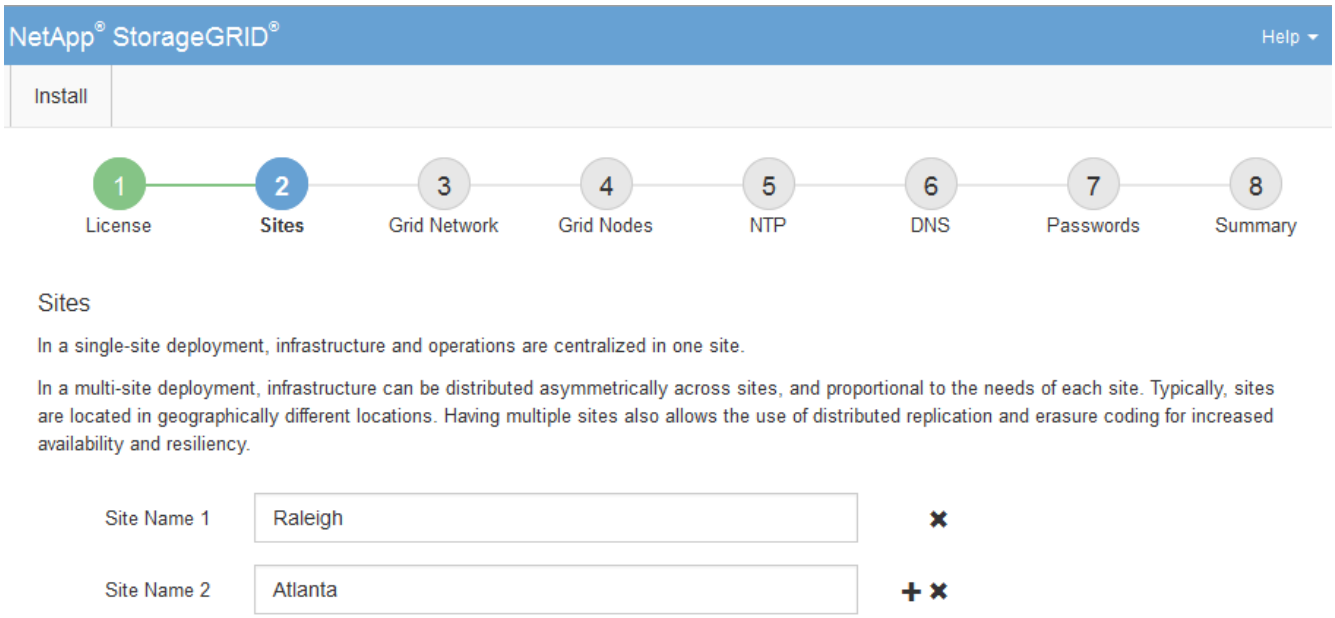
Adding sites

You must create at least one site when you are installing StorageGRID. You can create additional sites to increase the reliability and storage capacity of your StorageGRID system.

Steps

1. On the Sites page, enter the **Site Name**.
2. To add additional sites, click the plus sign next to the last site entry and enter the name in the new **Site Name** text box.

   Add as many additional sites as required for your grid topology. You can add up to 16 sites.



3. Click **Next**.

Specifying Grid Network subnets

You must specify the subnets that are used on the Grid Network.

About this task

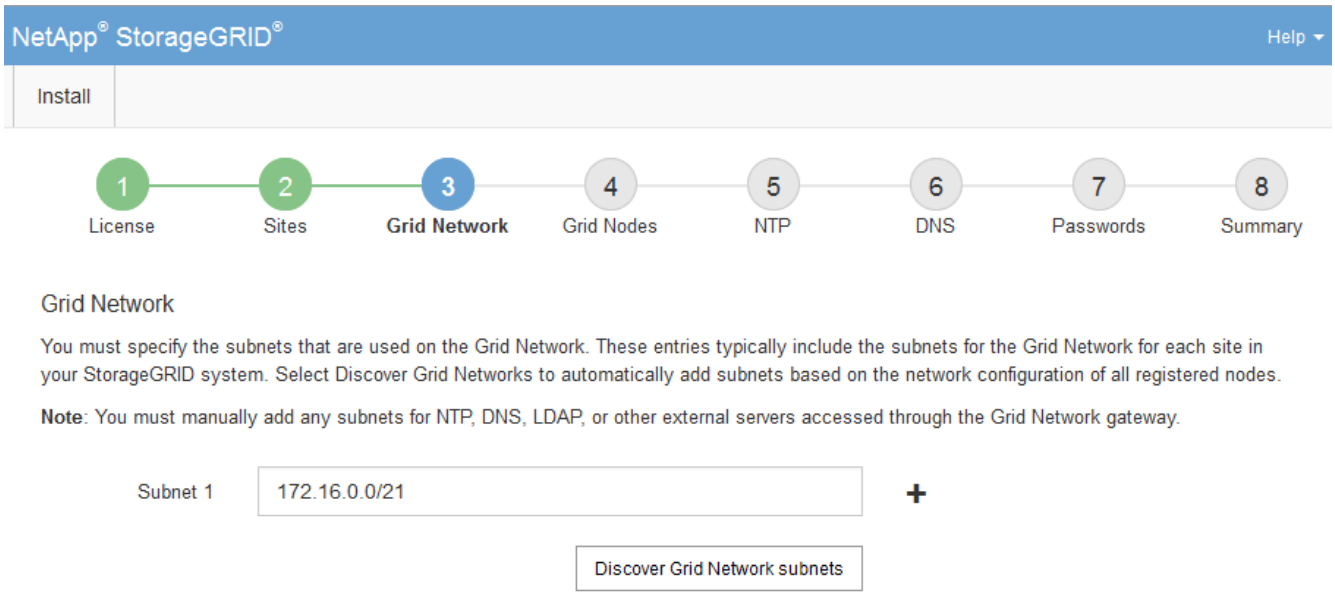
The subnet entries include the subnets for the Grid Network for each site in your StorageGRID system, along with any subnets that need to be reachable via the Grid Network.

If you have multiple grid subnets, the Grid Network gateway is required. All grid subnets specified must be reachable through this gateway.

Steps

1. Specify the CIDR network address for at least one Grid Network in the **Subnet 1** text box.
2. Click the plus sign next to the last entry to add an additional network entry.

   If you have already deployed at least one node, click **Discover Grid Networks Subnets** to automatically populate the Grid Network Subnet List with the subnets reported by grid nodes that have registered with the Grid Manager.



3. Click **Next**.

Approving pending grid nodes

You must approve each grid node before it can join the StorageGRID system.

What you'll need

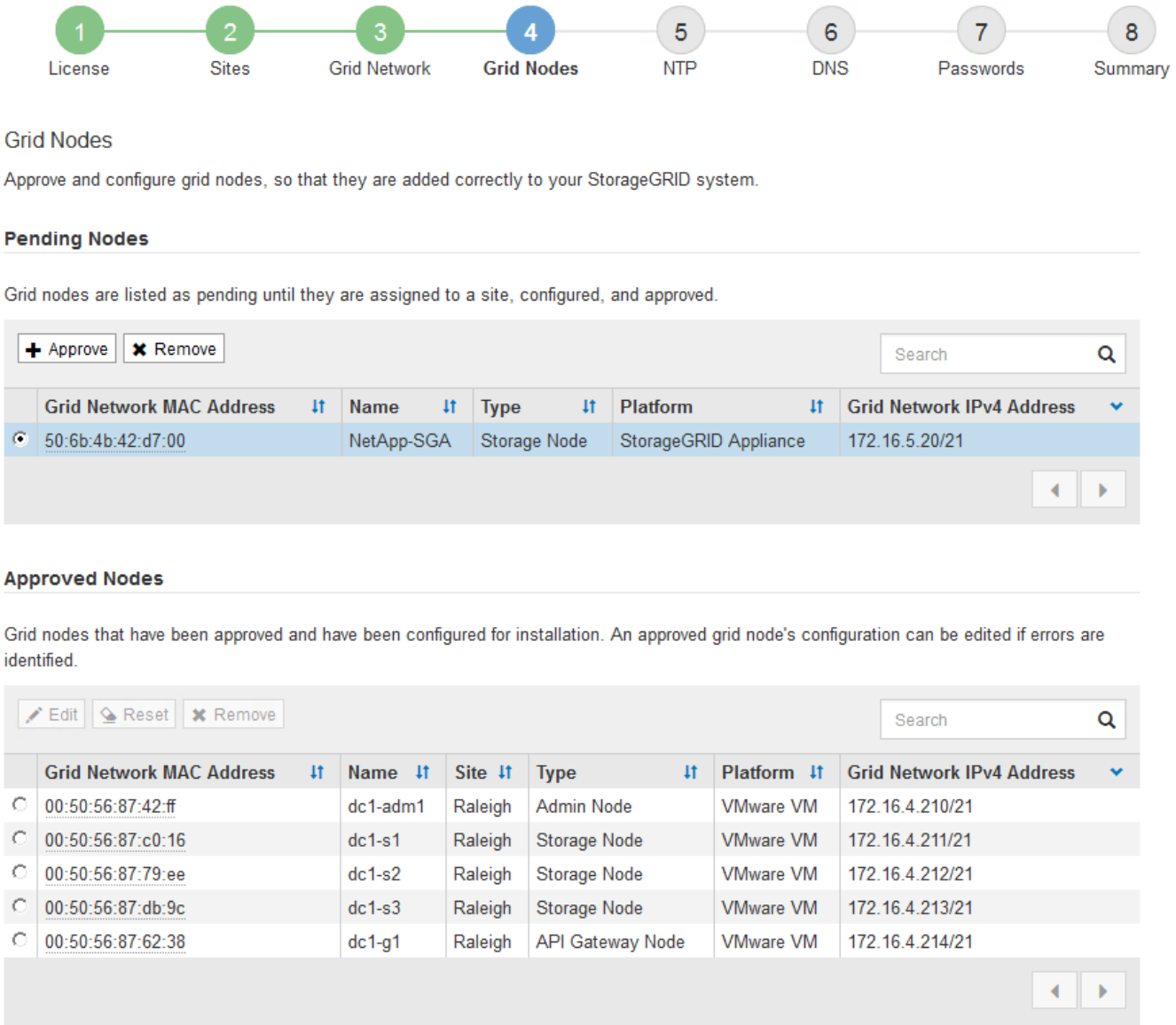
All virtual and StorageGRID appliance grid nodes must have been deployed.

Steps

1. Review the Pending Nodes list, and confirm that it shows all of the grid nodes you deployed.

   If a grid node is missing, confirm that it was deployed successfully.

2. Select the radio button next to a pending node you want to approve.



3. Click **Approve**.
4. In General Settings, modify settings for the following properties, as necessary:

Storage Node Configuration

General Settings

Site	Raleigh
Name	NetApp-SGA
NTP Role	Automatic
ADC Service	Automatic

Grid Network

Configuration	STATIC
IPv4 Address (CIDR)	172.16.5.20/21
Gateway	172.16.5.20

Admin Network

Configuration	STATIC
IPv4 Address (CIDR)	10.224.5.20/21
Gateway	10.224.0.1
Subnets (CIDR)	10.0.0.0/8
	172.19.0.0/16
	172.21.0.0/16

Client Network

Configuration	STATIC
IPv4 Address (CIDR)	47.47.5.20/21
Gateway	47.47.0.1

- **Site**: The name of the site with which this grid node will be associated.
- **Name**: The name that will be assigned to the node, and the name that will be displayed in the Grid Manager. The name defaults to the name you specified when you configured the node. During this step of the installation process, you can change the name as required.

> After you complete the installation, you cannot change the name of the node.

> For a VMware node, you can change the name here, but this action will not change the name of the virtual machine in vSphere.

- **NTP Role**: The Network Time Protocol (NTP) role of the grid node. The options are **Automatic**, **Primary**, and **Client**. Selecting **Automatic** assigns the Primary role to Admin Nodes, Storage Nodes with ADC services, Gateway Nodes, and any grid nodes that have non-static IP addresses. All other grid nodes are assigned the Client role.

  > Make sure that at least two nodes at each site can access at least four external NTP sources. If only one node at a site can reach the NTP sources, timing issues will occur if that node goes down. In addition, designating two nodes per site as primary NTP sources ensures accurate timing if a site is isolated from the rest of the grid.

- **ADC service** (Storage Nodes only): Select **Automatic** to let the system determine whether the node requires the Administrative Domain Controller (ADC) service. The ADC service keeps track of the location and availability of grid services. At least three Storage Nodes at each site must include the ADC service. You cannot add the ADC service to a node after it is deployed.

5. In Grid Network, modify settings for the following properties as necessary:

   - **IPv4 Address (CIDR)**: The CIDR network address for the Grid Network interface (eth0 inside the container). For example: 192.168.1.234/21
   - **Gateway**: The Grid Network gateway. For example: 192.168.0.1

     The gateway is required if there are multiple grid subnets.

   > If you selected DHCP for the Grid Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

6. If you want to configure the Admin Network for the grid node, add or update the settings in the Admin Network section as necessary.

   Enter the destination subnets of the routes out of this interface in the **Subnets (CIDR)** text box. If there are multiple Admin subnets, the Admin gateway is required.

   > If you selected DHCP for the Admin Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

   Appliances: For a StorageGRID appliance, if the Admin Network was not configured during the initial installation using the StorageGRID Appliance Installer, it cannot be configured in this Grid Manager dialog box. Instead, you must follow these steps:

   a. Reboot the appliance: In the Appliance Installer, select **Advanced** > **Reboot**.

      Rebooting can take several minutes.

   b. Select **Configure Networking** > **Link Configuration** and enable the appropriate networks.
   c. Select **Configure Networking** > **IP Configuration** and configure the enabled networks.
   d. Return to the Home page and click **Start Installation**.
   e. In the Grid Manager: If the node is listed in the Approved Nodes table, reset the node.
   f. Remove the node from the Pending Nodes table.
   g. Wait for the node to reappear in the Pending Nodes list.

h. Confirm that you can configure the appropriate networks. They should already be populated with the information you provided on the IP Configuration page.

   For additional information, see the installation and maintenance instructions for your appliance model.

7. If you want to configure the Client Network for the grid node, add or update the settings in the Client Network section as necessary. If the Client Network is configured, the gateway is required, and it becomes the default gateway for the node after installation.

   > If you selected DHCP for the Client Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

   Appliances: For a StorageGRID appliance, if the Client Network was not configured during the initial installation using the StorageGRID Appliance Installer, it cannot be configured in this Grid Manager dialog box. Instead, you must follow these steps:

   a. Reboot the appliance: In the Appliance Installer, select **Advanced** > **Reboot**.

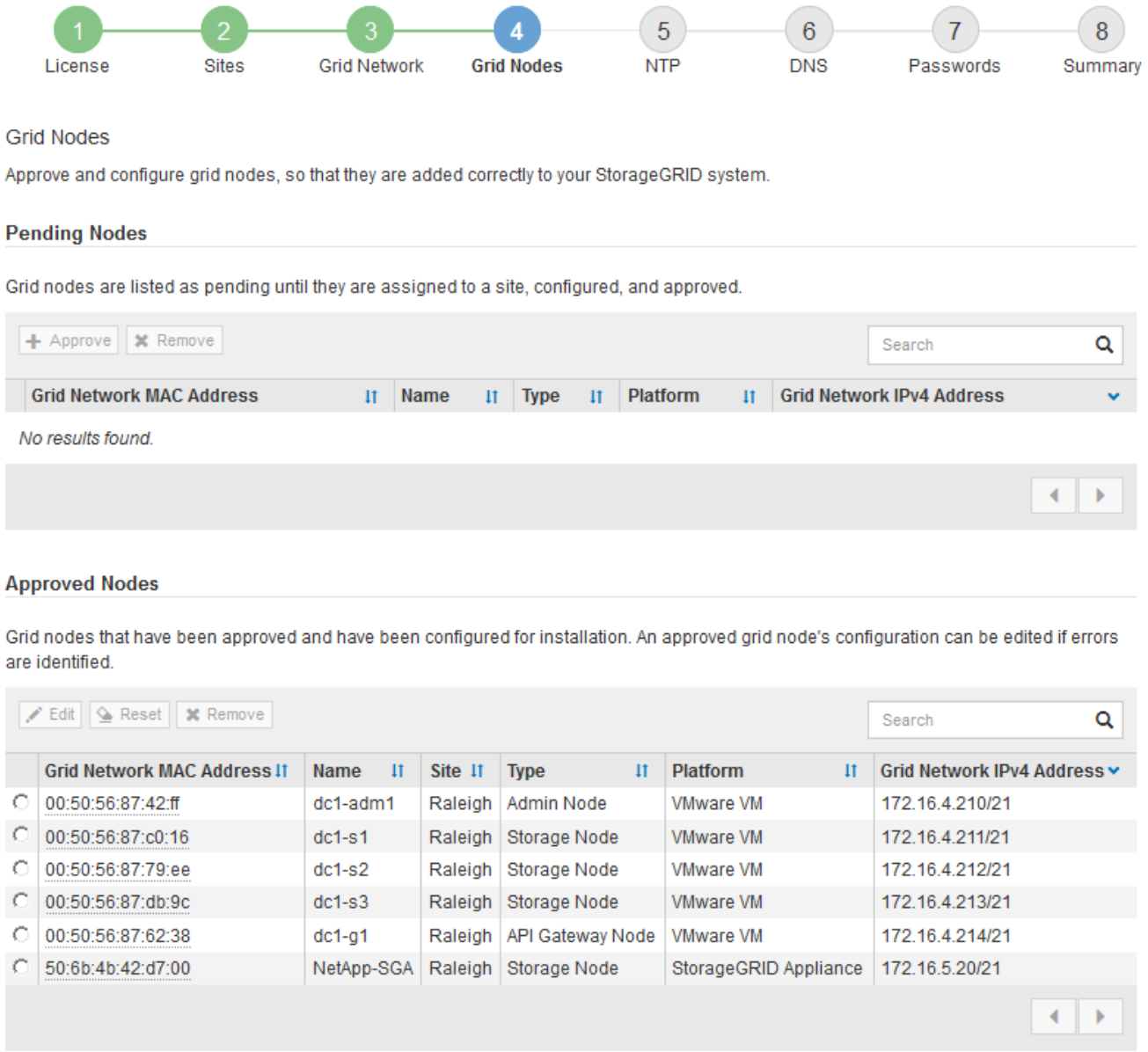
      Rebooting can take several minutes.

   b. Select **Configure Networking** > **Link Configuration** and enable the appropriate networks.
   c. Select **Configure Networking** > **IP Configuration** and configure the enabled networks.
   d. Return to the Home page and click **Start Installation**.
   e. In the Grid Manager: If the node is listed in the Approved Nodes table, reset the node.
   f. Remove the node from the Pending Nodes table.
   g. Wait for the node to reappear in the Pending Nodes list.
   h. Confirm that you can configure the appropriate networks. They should already be populated with the information you provided on the IP Configuration page.

      For additional information, see the installation and maintenance instructions for your appliance.

8. Click **Save**.

   The grid node entry moves to the Approved Nodes list.



9. Repeat these steps for each pending grid node you want to approve.

   You must approve all nodes that you want in the grid. However, you can return to this page at any time before you click **Install** on the Summary page. You can modify the properties of an approved grid node by selecting its radio button and clicking **Edit**.

10. When you are done approving grid nodes, click **Next**.

Specifying Network Time Protocol server information

You must specify the Network Time Protocol (NTP) configuration information for the StorageGRID system, so that operations performed on separate servers can be kept synchronized.

About this task

You must specify IPv4 addresses for the NTP servers.

You must specify external NTP servers. The specified NTP servers must use the NTP protocol.

You must specify four NTP server references of Stratum 3 or better to prevent issues with time drift.

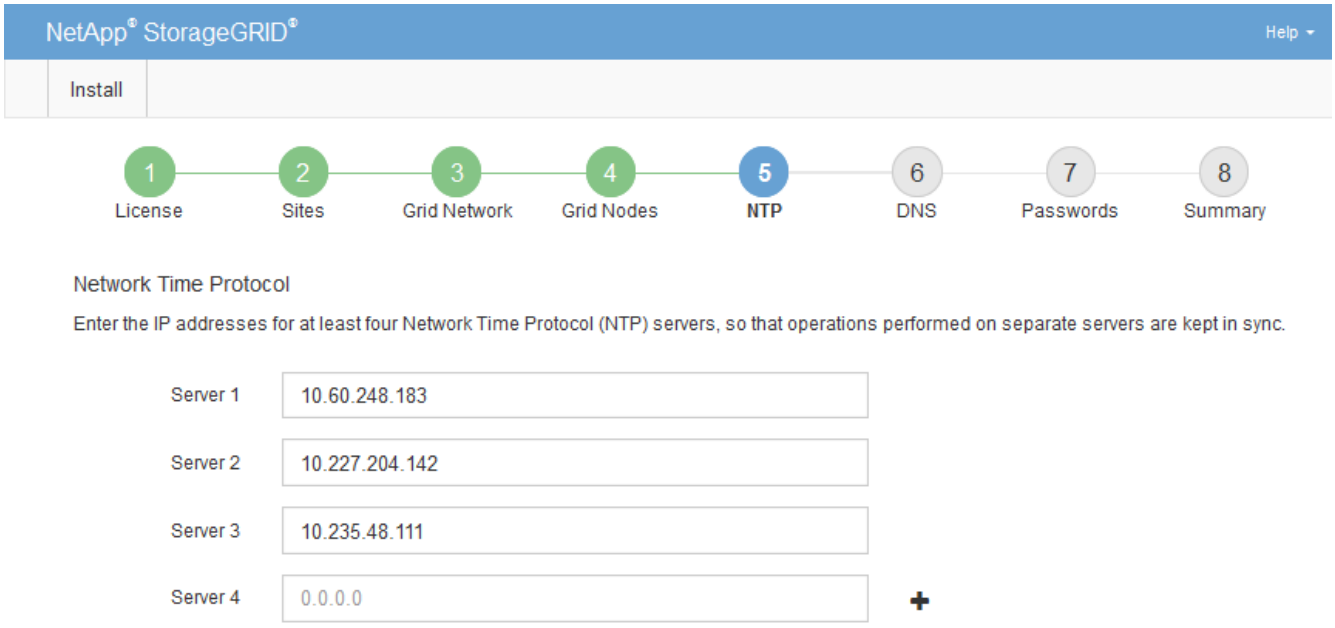
> When specifying the external NTP source for a production-level StorageGRID installation, do not use the Windows Time (W32Time) service on a version of Windows earlier than Windows Server 2016. The time service on earlier versions of Windows is not sufficiently accurate and is not supported by Microsoft for use in high-accuracy environments, such as StorageGRID. See Support boundary to configure the Windows Time service for high-accuracy environments.

The external NTP servers are used by the nodes to which you previously assigned Primary NTP roles.

> Make sure that at least two nodes at each site can access at least four external NTP sources. If only one node at a site can reach the NTP sources, timing issues will occur if that node goes down. In addition, designating two nodes per site as primary NTP sources ensures accurate timing if a site is isolated from the rest of the grid.

Steps

1. Specify the IPv4 addresses for at least four NTP servers in the **Server 1** to **Server 4** text boxes.
2. If necessary, select the plus sign next to the last entry to add additional server entries.



3. Select **Next**.

Specifying Domain Name System server information

You must specify Domain Name System (DNS) information for your StorageGRID system, so that you can access external servers using hostnames instead of IP addresses.

About this task

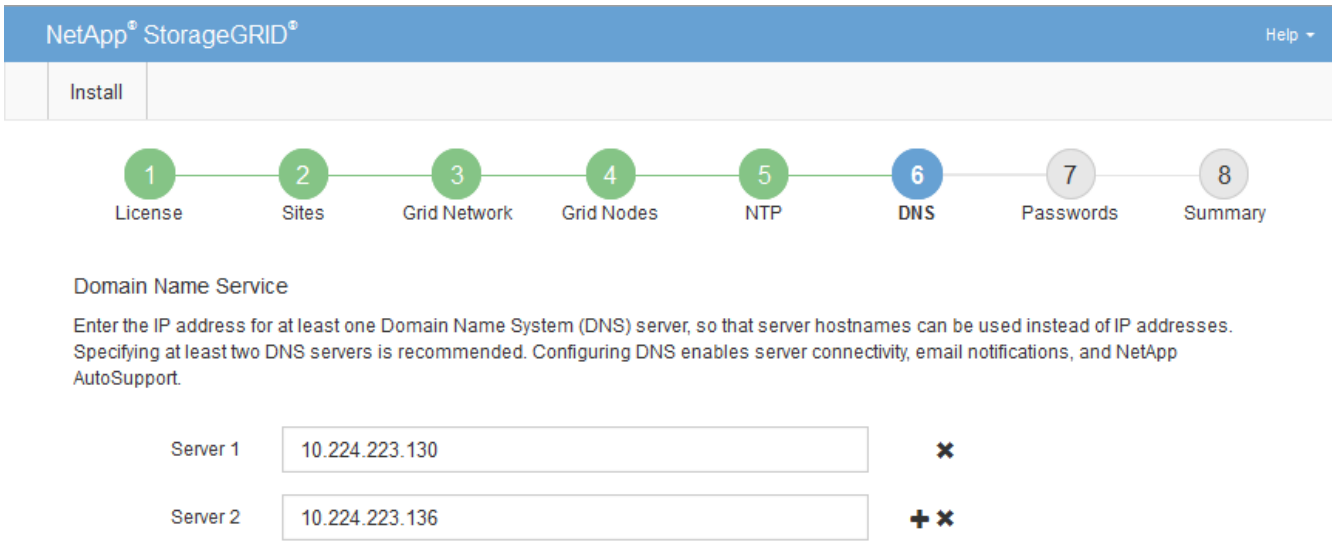
Specifying DNS server information allows you to use Fully Qualified Domain Name (FQDN) hostnames rather than IP addresses for email notifications and AutoSupport. Specifying at least two DNS servers is recommended.

> Provide two to six IPv4 addresses for DNS servers. You should select DNS servers that each site can access locally in the event of network islanding. This is to ensure an islanded site continues to have access to the DNS service. After configuring the grid-wide DNS server list, you can further customize the DNS server list for each node. For details, see the information about modifying the DNS configuration in the recovery and maintenance instructions.

If the DNS server information is omitted or incorrectly configured, a DNST alarm is triggered on each grid node's SSM service. The alarm clears when DNS is configured correctly and the new server information has reached all grid nodes.

Steps

1. Specify the IPv4 address for at least one DNS server in the **Server 1** text box.
2. If necessary, select the plus sign next to the last entry to add additional server entries.



   The best practice is to specify at least two DNS servers. You can specify up to six DNS servers.

3. Select **Next**.

Specifying the StorageGRID system passwords

As part of installing your StorageGRID system, you need to enter the passwords to use to secure your system and perform maintenance tasks.

About this task

Use the Install passwords page to specify the provisioning passphrase and the grid management root user password.

- The provisioning passphrase is used as an encryption key and is not stored by the StorageGRID system.
- You must have the provisioning passphrase for installation, expansion, and maintenance procedures, including downloading the recovery package. Therefore, it is important that you store the provisioning passphrase in a secure location.
- You can change the provisioning passphrase from the Grid Manager if you have the current one.
- The grid management root user password may be changed using the Grid Manager.
- Randomly generated command line console and SSH passwords are stored in the Passwords.txt file in the

recovery package.

Steps

1. In **Provisioning Passphrase**, enter the provisioning passphase that will be required to make changes to the grid topology of your StorageGRID system.

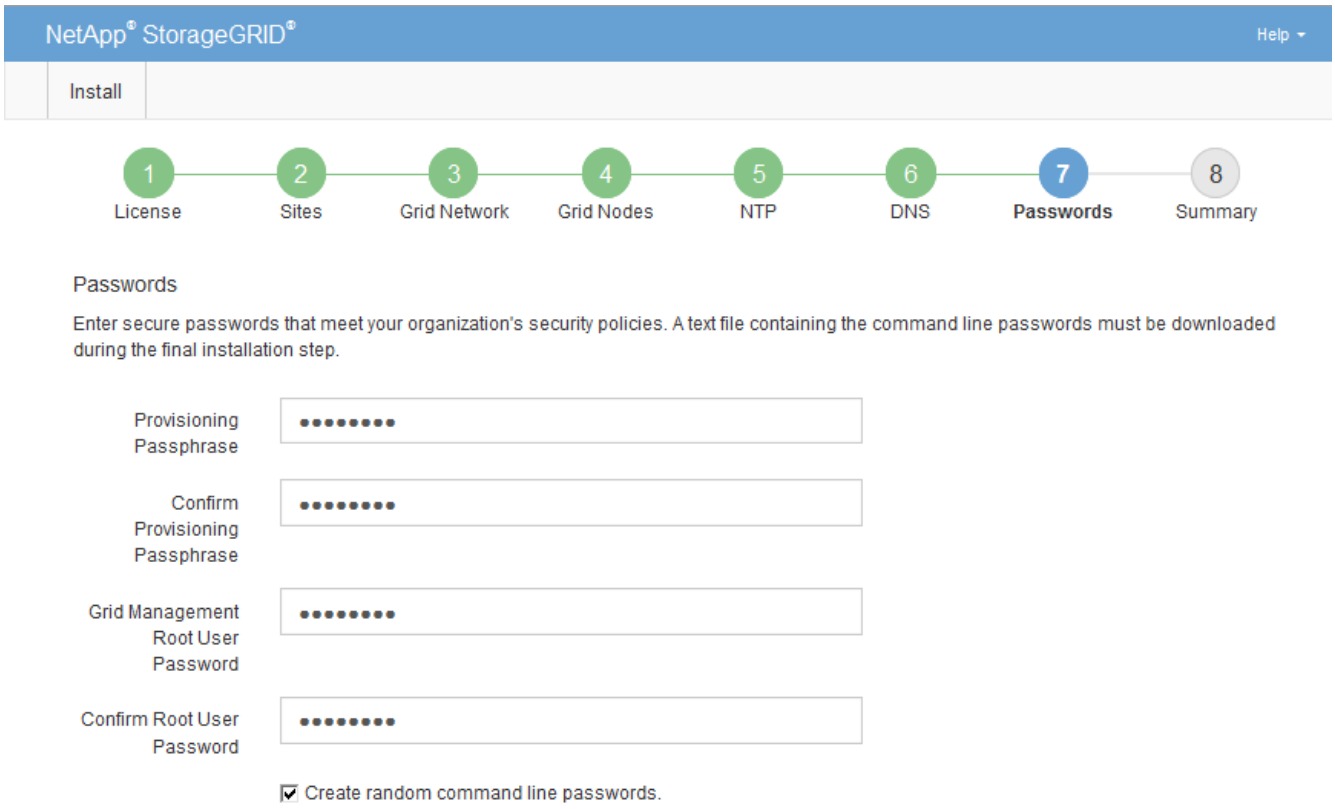
   Store the provisioning passphrase in a secure place.

   > If after the installation completes and you want to change the provisioning passphrase later, you can use the Grid Manager. Select **Configuration** > **Access Control** > **Grid Passwords**.

2. In **Confirm Provisioning Passphrase**, reenter the provisioning passphrase to confirm it.
3. In **Grid Management Root User Password**, enter the password to use to access the Grid Manager as the “root” user.

   Store the password in a secure place.

4. In **Confirm Root User Password**, reenter the Grid Manager password to confirm it.



5. If you are installing a grid for proof of concept or demo purposes, optionally deselect the **Create random command line passwords** check box.

   For production deployments, random passwords should always be used for security reasons. Deselect **Create random command line passwords** only for demo grids if you want to use default passwords to access grid nodes from the command line using the “root” or “admin” account.

> You are prompted to download the Recovery Package file (`sgws-recovery-package-id-revision.zip`) after you click **Install** on the Summary page. You must download this file to complete the installation. The passwords required to access the system are stored in the `Passwords.txt` file, contained in the Recovery Package file.

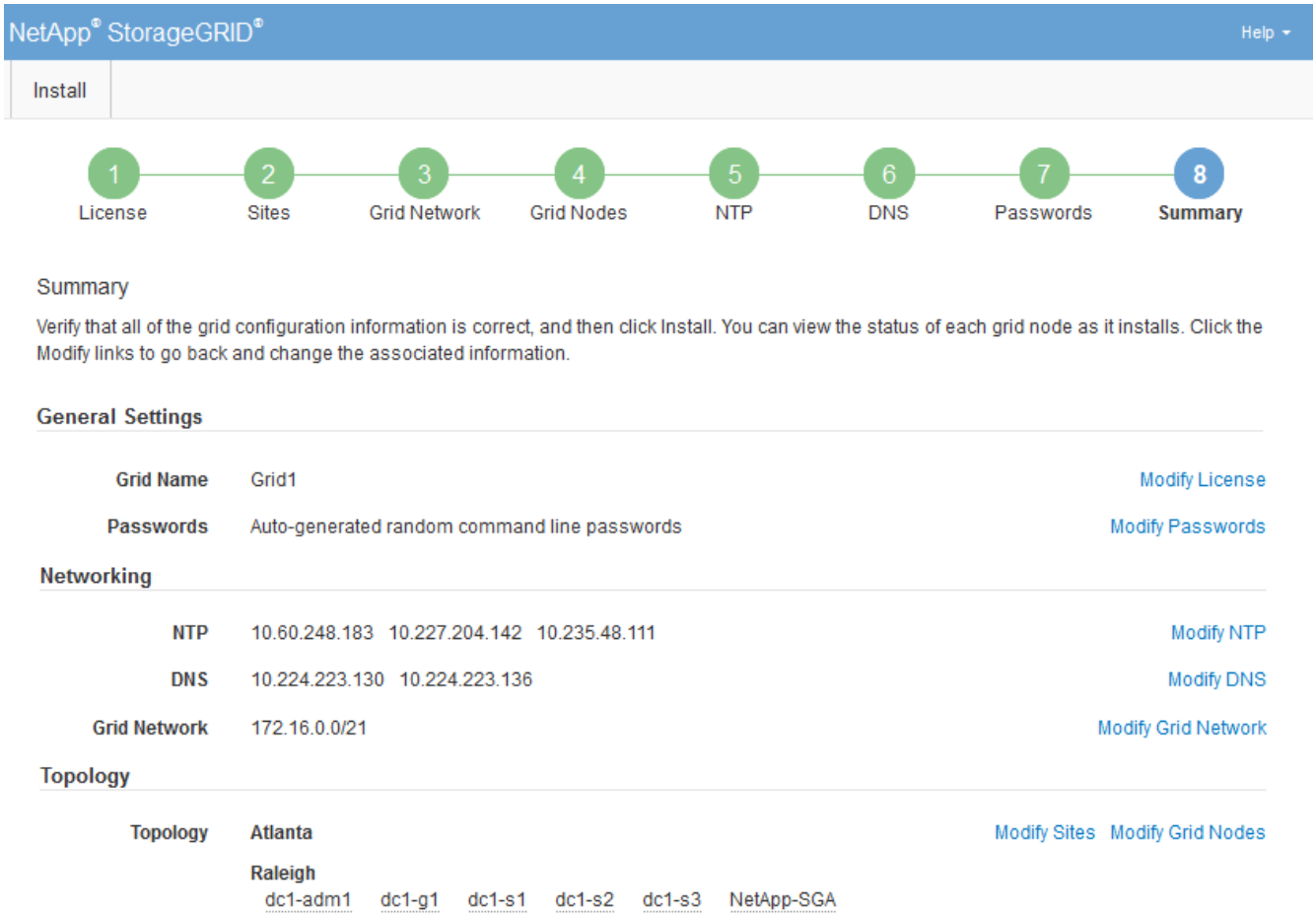
6. Click **Next**.

Reviewing your configuration and completing installation

You must carefully review the configuration information you have entered to ensure that the installation completes successfully.

Steps

1. View the **Summary** page.



2. Verify that all of the grid configuration information is correct. Use the Modify links on the Summary page to go back and correct any errors.
3. Click **Install**.

> If a node is configured to use the Client Network, the default gateway for that node switches from the Grid Network to the Client Network when you click **Install**. If you lose connectivity, you must ensure that you are accessing the primary Admin Node through an accessible subnet. See Networking guidelines for details.

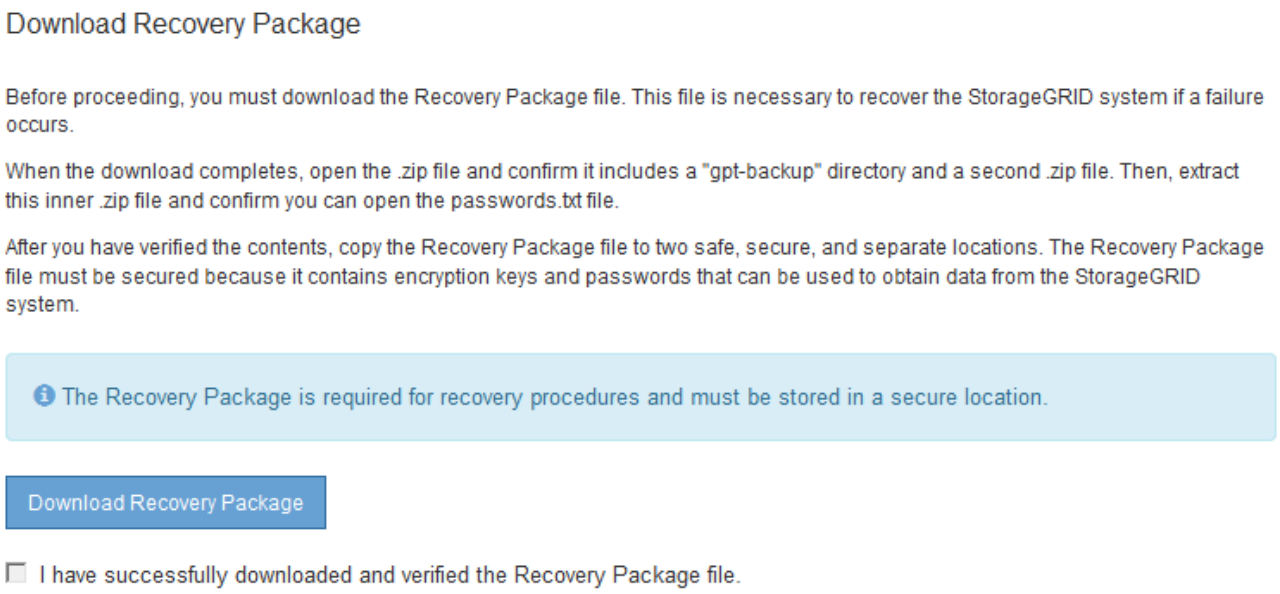
4. Click **Download Recovery Package**.

   When the installation progresses to the point where the grid topology is defined, you are prompted to download the Recovery Package file (`.zip`), and confirm that you can successfully access the contents of this file. You must download the Recovery Package file so that you can recover the StorageGRID system if one or more grid nodes fail. The installation continues in the background, but you cannot complete the installation and access the StorageGRID system until you download and verify this file.

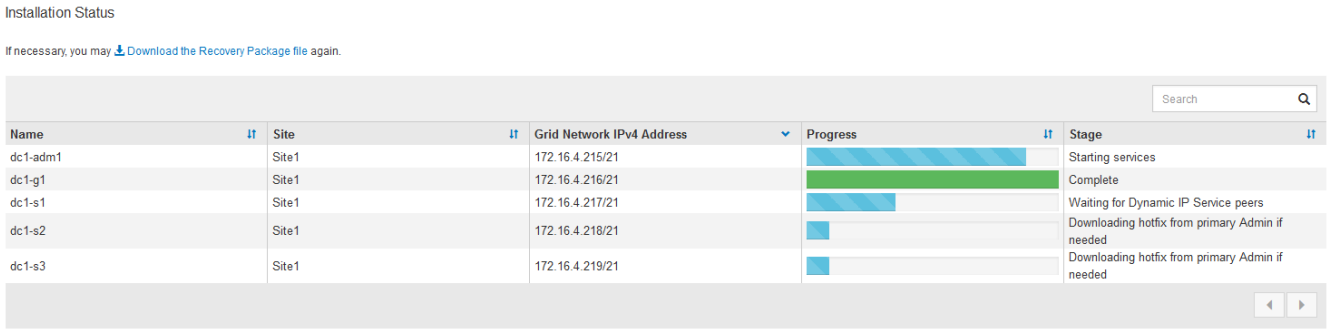
5. Verify that you can extract the contents of the `.zip` file, and then save it in two safe, secure, and separate locations.

   > The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

6. Select the **I have successfully downloaded and verified the Recovery Package file** check box, and click **Next**.



   If the installation is still in progress, the status page appears. This page indicates the progress of the installation for each grid node.



   When the Complete stage is reached for all grid nodes, the sign-in page for the Grid Manager appears.

7. Sign in to the Grid Manager using the "root" user and the password you specified during the installation.

Post-installation guidelines

After completing grid node deployment and configuration, follow these guidelines for DHCP addressing and network configuration changes.

- If DHCP was used to assign IP addresses, configure a DHCP reservation for each IP address on the networks being used.

  You can only set up DHCP during the deployment phase. You cannot set up DHCP during configuration.

  > Nodes reboot when their IP addresses change, which can cause outages if a DHCP address change affects multiple nodes at the same time.

- You must use the Change IP procedures if you want to change IP addresses, subnet masks, and default gateways for a grid node. See the information about configuring IP addresses in the recovery and maintenance instructions.
- If you make networking configuration changes, including routing and gateway changes, client connectivity to the primary Admin Node and other grid nodes might be lost. Depending on the networking changes applied, you might need to re-establish these connections.

Automating the installation

You can automate the installation of the StorageGRID host service, and the configuration of grid nodes.

About this task

Automating the deployment might be useful in any of the following cases:

- You already use a standard orchestration framework, such as Ansible, Puppet, or Chef, to deploy and configure physical or virtual hosts.
- You intend to deploy multiple StorageGRID instances.
- You are deploying a large, complex StorageGRID instance.

The StorageGRID host service is installed by a package and driven by configuration files that can be created interactively during a manual installation, or prepared ahead of time (or programmatically) to enable automated installation using standard orchestration frameworks. StorageGRID provides optional Python scripts for automating the configuration of StorageGRID appliances, and the whole StorageGRID system (the “grid”). You can use these scripts directly, or you can inspect them to learn how to use the StorageGRID Installation REST API in grid deployment and configuration tools you develop yourself.

If you are interested in automating all or part of your StorageGRID deployment, review “Automating the installation” before beginning the installation process.

Automating the installation and configuration of the StorageGRID host service

You can automate the installation of the StorageGRID host service using standard orchestration frameworks such as Ansible, Puppet, Chef, Fabric, or SaltStack.

The StorageGRID host service is packaged in an RPM and is driven by configuration files that can be prepared ahead of time (or programmatically) to enable automated installation. If you already use a standard orchestration framework to install and configure RHEL or CentOS, adding StorageGRID to your playbooks or

recipes should be straightforward.

An example Ansible role and playbook are supplied with the installation archive in the `/extras` folder. The Ansible playbook shows how the `storagegrid` role prepares the host and installs StorageGRID onto the target servers. You can customize the role or playbook as necessary.

> The example playbook does not include the steps required to create network devices before starting the StorageGRID host service. Add these steps before finalizing and using the playbook.

You can automate all of the steps for preparing the hosts and deploying virtual grid nodes.

Automating the configuration of StorageGRID

After deploying the grid nodes, you can automate the configuration of the StorageGRID system.

What you'll need

- You know the location of the following files from the installation archive.

Filename	Description
`configure-storagegrid.py`	Python script used to automate the configuration
`configure-storagegrid.sample.json`	Sample configuration file for use with the script
`configure-storagegrid.blank.json`	Blank configuration file for use with the script

- You have created a `configure-storagegrid.json` configuration file. To create this file, you can modify the sample configuration file (`configure-storagegrid.sample.json`) or the blank configuration file (`configure-storagegrid.blank.json`).

About this task

You can use the `configure-storagegrid.py` Python script and the `configure-storagegrid.json` configuration file to automate the configuration of your StorageGRID system.

> You can also configure the system using the Grid Manager or the Installation API.

Steps

1. Log in to the Linux machine you are using to run the Python script.
2. Change to the directory where you extracted the installation archive.

   For example:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   where `platform` is `debs`, `rpms`, or `vsphere`.

3. Run the Python script and use the configuration file you created.

   For example:

```
./configure-storagegrid.py ./configure-storagegrid.json --start-install
```

Result

A Recovery Package `.zip` file is generated during the configuration process, and it is downloaded to the directory where you are running the installation and configuration process. You must back up the Recovery Package file so that you can recover the StorageGRID system if one or more grid nodes fails. For example, copy it to a secure, backed up network location and to a secure cloud storage location.

> The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

If you specified that random passwords should be generated, you need to extract the `Passwords.txt` file and look for the passwords required to access your StorageGRID system.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Your StorageGRID system is installed and configured when a confirmation message is displayed.

```
StorageGRID has been configured and installed.
```

Related information

Configuring the grid and completing installation

Overview of the installation REST API

Overview of the installation REST API

StorageGRID provides the StorageGRID Installation API for performing installation tasks.

The API uses the Swagger open source API platform to provide the API documentation. Swagger allows both developers and non-developers to interact with the API in a user interface that illustrates how the API responds to parameters and options. This documentation assumes that you are familiar with standard web technologies and the JSON (JavaScript Object Notation) data format.

> Any API operations you perform using the API Docs webpage are live operations. Be careful not to create, update, or delete configuration data or other data by mistake.

Each REST API command includes the API's URL, an HTTP action, any required or optional URL parameters, and an expected API response.

StorageGRID Installation API

The StorageGRID Installation API is only available when you are initially configuring your StorageGRID system, and in the event that you need to perform a primary Admin Node recovery. The Installation API can be accessed over HTTPS from the Grid Manager.

To access the API documentation, go to the installation web page on the primary Admin Node and select **Help** > **API Documentation** from the menu bar.

The StorageGRID Installation API includes the following sections:

- **config** — Operations related to the product release and versions of the API. You can list the product release version and the major versions of the API supported by that release.
- **grid** — Grid-level configuration operations. You can get and update grid settings, including grid details, Grid Network subnets, grid passwords, and NTP and DNS server IP addresses.
- **nodes** — Node-level configuration operations. You can retrieve a list of grid nodes, delete a grid node, configure a grid node, view a grid node, and reset a grid node's configuration.
- **provision** — Provisioning operations. You can start the provisioning operation and view the status of the provisioning operation.
- **recovery** — Primary Admin Node recovery operations. You can reset information, upload the Recover Package, start the recovery, and view the status of the recovery operation.
- **recovery-package** — Operations to download the Recovery Package.
- **sites** — Site-level configuration operations. You can create, view, delete, and modify a site.

Where to go next

After completing an installation, you must perform a series of integration and configuration steps. Some steps are required; others are optional.

Required tasks

- Create a tenant account for each client protocol (Swift or S3) that will be used to store objects on your StorageGRID system.
- Control system access by configuring groups and user accounts. Optionally, you can configure a federated identity source (such as Active Directory or OpenLDAP), so you can import administration groups and users. Or, you can create local groups and users.
- Integrate and test the S3 or Swift API client applications you will use to upload objects to your StorageGRID system.
- When you are ready, configure the information lifecycle management (ILM) rules and ILM policy you want to use to protect object data.

> When you install StorageGRID, the default ILM policy, Baseline 2 Copies Policy, is active. This policy includes the stock ILM rule (Make 2 Copies), and it applies if no other policy has been activated.

- If your installation includes appliance Storage Nodes, use SANtricity software to complete the following

tasks:

  - Connect to each StorageGRID appliance.
  - Verify receipt of AutoSupport data.

- If your StorageGRID system includes any Archive Nodes, configure the Archive Node's connection to the target external archival storage system.

> If any Archive Nodes will use Tivoli Storage Manager as the external archival storage system, you must also configure Tivoli Storage Manager.

- Review and follow the StorageGRID system hardening guidelines to eliminate security risks.
- Configure email notifications for system alerts.

Optional tasks

- If you want to receive notifications from the (legacy) alarm system, configure mailing lists and email notifications for alarms.
- Update grid node IP addresses if they have changed since you planned your deployment and generated the Recovery Package. See information about changing IP addresses in the recovery and maintenance instructions.
- Configure storage encryption, if required.
- Configure storage compression to reduce the size of stored objects, if required.
- Configure audit client access. You can configure access to the system for auditing purposes through an NFS or a CIFS file share. See the instructions for administering StorageGRID.

> Audit export through CIFS/Samba has been deprecated and will be removed in a future StorageGRID release.

Troubleshooting installation issues

If any problems occur while installing your StorageGRID system, you can access the installation log files. Technical support might also need to use the installation log files to resolve issues.

The following installation log files are available from the container that is running each node:

- `/var/local/log/install.log` (found on all grid nodes)
- `/var/local/log/gdu-server.log` (found on the primary Admin Node)

The following installation log files are available from the host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/node-name.log`

To learn how to access the log files, see the instructions for monitoring and troubleshooting StorageGRID. For help troubleshooting appliance installation issues, see the installation and maintenance instructions for your appliances. If you need additional help, contact technical support.

Related information

Monitor & troubleshoot

SG100 & SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

NetApp Support

Example /etc/sysconfig/network-scripts

You can use the example files to aggregate four Linux physical interfaces into a single LACP bond and then establish three VLAN interfaces subtending the bond for use as StorageGRID Grid, Admin, and Client network interfaces.

Physical interfaces

Note that the switches at the other ends of the links must also treat the four ports as a single LACP trunk or port channel, and must pass at least the three referenced VLANs with tags.

/etc/sysconfig/network-scripts/ifcfg-ens160

```
TYPE=Ethernet
NAME=ens160
UUID=011b17dd-642a-4bb9-acae-d71f7e6c8720
DEVICE=ens160
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens192

```
TYPE=Ethernet
NAME=ens192
UUID=e28eb15f-76de-4e5f-9a01-c9200b58d19c
DEVICE=ens192
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens224

```
TYPE=Ethernet
NAME=ens224
UUID=b0e3d3ef-7472-4cde-902c-ef4f3248044b
DEVICE=ens224
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

/etc/sysconfig/network-scripts/ifcfg-ens256

```
TYPE=Ethernet
NAME=ens256
UUID=7cf7aabc-3e4b-43d0-809a-1e2378faa4cd
DEVICE=ens256
ONBOOT=yes
MASTER=bond0
SLAVE=yes
```

Bond interface

/etc/sysconfig/network-scripts/ifcfg-bond0

```
DEVICE=bond0
TYPE=Bond
BONDING_MASTER=yes
NAME=bond0
ONBOOT=yes
BONDING_OPTS=mode=802.3ad
```

VLAN interfaces

/etc/sysconfig/network-scripts/ifcfg-bond0.1001

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1001
PHYSDEV=bond0
VLAN_ID=1001
REORDER_HDR=0
BOOTPROTO=none
UUID=296435de-8282-413b-8d33-c4dd40fca24a
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1002

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1002
PHYSDEV=bond0
VLAN_ID=1002
REORDER_HDR=0
BOOTPROTO=none
UUID=dbaaec72-0690-491c-973a-57b7dd00c581
ONBOOT=yes
```

/etc/sysconfig/network-scripts/ifcfg-bond0.1003

```
VLAN=yes
TYPE=Vlan
DEVICE=bond0.1003
PHYSDEV=bond0
VLAN_ID=1003
REORDER_HDR=0
BOOTPROTO=none
UUID=d1af4b30-32f5-40b4-8bb9-71a2fbf809a1
ONBOOT=yes
```

Install Ubuntu or Debian

Learn how to install StorageGRID software in Ubuntu or Debian deployments.

- Installation overview
- Planning and preparation
- Deploying virtual grid nodes
- Configuring the grid and completing installation
- Automating the installation
- Overview of the installation REST API
- Where to go next
- Troubleshooting installation issues
- Example /etc/network/interfaces

Installation overview

Installing a StorageGRID system in an Ubuntu or Debian environment includes three primary steps.

1. **Preparation**: During planning and preparation, you perform the following tasks:
    - Learn about the hardware and storage requirements for StorageGRID.
    - Learn about the specifics of StorageGRID networking so you can configure your network appropriately. For more information, see the StorageGRID networking guidelines.
    - Identify and prepare the physical or virtual servers you plan to use to host your StorageGRID grid nodes.
    - On the servers you have prepared:
        - Install Ubuntu or Debian
        - Configure the host network
        - Configure host storage
        - Install Docker
        - Install the StorageGRID host services
2. **Deployment**: Deploy grid nodes using the appropriate user interface. When you deploy grid nodes, they are created as part of the StorageGRID system and connected to one or more networks.
    a. Use the Ubuntu or Debian command line and node configuration files to deploy virtual grid nodes on the hosts you prepared in step 1.
    b. Use the StorageGRID Appliance Installer to deploy StorageGRID appliance nodes.

    > Hardware-specific installation and integration instructions are not included in the StorageGRID installation procedure. To learn how to install StorageGRID appliances, see the installation and maintenance instructions for your appliance.

3. **Configuration**: When all nodes have been deployed, use the Grid Manager to configure the grid and complete the installation.

These instructions recommend a standard approach for deploying and configuring a StorageGRID system in an Ubuntu or Debian environment. See also the information about the following alternative approaches:

- Use a standard orchestration framework such as Ansible, Puppet, or Chef to install Ubuntu or Debian, configure networking and storage, install Docker and the StorageGRID host service, and deploy virtual grid nodes.
- Automate the deployment and configuration of the StorageGRID system using a Python configuration script (provided in the installation archive).
- Automate the deployment and configuration of appliance grid nodes with a Python configuration script (available from the installation archive or from the StorageGRID Appliance Installer).
- If you are an advanced developer of StorageGRID deployments, use the installation REST APIs to automate the installation of StorageGRID grid nodes.

Related information

Planning and preparation

Deploying virtual grid nodes

Configuring the grid and completing installation

Automating the installation and configuration of the StorageGRID host service

Overview of the installation REST API

Network guidelines

Planning and preparation

Before deploying grid nodes and configuring the StorageGRID grid, you must be familiar with the steps and requirements for completing the procedure.

The StorageGRID deployment and configuration procedures assume that you are familiar with the architecture and operation of the StorageGRID system.

You can deploy a single site or multiple sites at one time; however, all sites must meet the minimum requirement of having at least three Storage Nodes.

Before starting a StorageGRID installation, you must:

- Understand StorageGRID's compute requirements, including the minimum CPU and RAM requirements for each node.
- Understand how StorageGRID supports multiple networks for traffic separation, security, and administrative convenience, and have a plan for which networks you intend to attach to each StorageGRID node.

  See the StorageGRID networking guidelines.

- Understand the storage and performance requirements of each type of grid node.
- Identify a set of servers (physical, virtual, or both) that, in aggregate, provide sufficient resources to support the number and type of StorageGRID nodes you plan to deploy.
- Understand the requirements for node migration, if you want to perform scheduled maintenance on physical hosts without any service interruption.
- Gather all networking information in advance. Unless you are using DHCP, gather the IP addresses to assign to each grid node, and the IP addresses of the domain name system (DNS) and network time protocol (NTP) servers that will be used.
- Install, connect, and configure all required hardware, including any StorageGRID appliances, to specifications.

  > Hardware-specific installation and integration instructions are not included in the StorageGRID installation procedure. To learn how to install StorageGRID appliances, see the installation and maintenance instructions for your appliance.

- Decide which of the available deployment and configuration tools you want to use.

Related information

Network guidelines

SG100 & SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

Node container migration requirements

Required materials

Before you install StorageGRID, you must gather and prepare required materials.

Item	Notes
NetApp StorageGRID license	You must have a valid, digitally signed NetApp license. **Note**: A non-production license, which can be used for testing and proof of concept grids, is included in the StorageGRID installation archive.
StorageGRID installation archive	You must download the StorageGRID installation archive and extract the files.
Service laptop	The StorageGRID system is installed through a service laptop. The service laptop must have: • Network port • SSH client (for example, PuTTY) • Supported web browser
StorageGRID documentation	• Release notes • Instructions for administering StorageGRID

Related information

Downloading and extracting the StorageGRID installation files

Web browser requirements

Administer StorageGRID

Release notes

Downloading and extracting the StorageGRID installation files

You must download the StorageGRID installation archive and extract the required files.

Steps

1. Go to the NetApp Downloads page for StorageGRID.

   NetApp Downloads: StorageGRID

2. Select the button for downloading the latest release, or select another version from the drop-down menu and select **Go**.

3. Sign in with the username and password for your NetApp account.
4. If a Caution/MustRead statement appears, read it and select the check box.

   You must apply any required hotfixes after you install the StorageGRID release. For more information, see the hotfix procedure in the recovery and maintenance instructions.

5. Read the End User License Agreement, select the check box, and then select **Accept & Continue**.

   The downloads page for the version you selected appears. The page contains three columns:

6. In the **Install StorageGRID** column, select the appropriate software.

   Select the `.tgz` or `.zip` archive file for your platform.

   - `StorageGRID-Webscale-version-DEB-uniqueID.zip`
   - `StorageGRID-Webscale-version-DEB-uniqueID.tgz`

     The compressed files contain the DEB files and scripts for Ubuntu or Debian.

     Use the `.zip` file if you are running Windows on the service laptop.

7. Save and extract the archive file.
8. Choose the files you need from the following list.

   The set of files you need depends on your planned grid topology and how you will deploy your StorageGRID grid.

   The paths listed in the table are relative to the top-level directory installed by the extracted installation archive.

Path and file name	Description
`./debs/README`	A text file that describes all of the files contained in the StorageGRID download file.
`./debs/NLF000000.txt`	A non-production NetApp License File that you can use for testing and proof of concept deployments.
`./debs/storagegrid-webscale-images-version-SHA.deb`	DEB package for installing the StorageGRID node images on Ubuntu or Debian hosts.
`./debs/storagegrid-webscale-images-version-SHA.deb.md5`	MD5 checksum for the file `/debs/storagegrid-webscale-images-version-SHA.deb`.
`./debs/storagegrid-webscale-service-version-SHA.deb`	DEB package for installing the StorageGRID host service on Ubuntu or Debian hosts.
Deployment scripting tool	**Description**

Path and file name	Description
`./debs/configure-storagegrid.py`	A Python script used to automate the configuration of a StorageGRID system.
`./debs/configure-sga.py`	A Python script used to automate the configuration of StorageGRID appliances.
`./debs/storagegrid-ssoauth.py`	An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled.
`./debs/configure-storagegrid.sample.json`	A sample configuration file for use with the `configure-storagegrid.py` script.
`./debs/configure-storagegrid.blank.json`	A blank configuration file for use with the `configure-storagegrid.py` script.
`./debs/extras/ansible`	Example Ansible role and playbook for configuring Ubuntu or Debian hosts for StorageGRID container deployment. You can customize the role or playbook as necessary.

Related information

Maintain & recover

CPU and RAM requirements

Before installing StorageGRID software, verify and configure the hardware so that it is ready to support the StorageGRID system.

For information about supported servers, see the Interoperability Matrix.

Each StorageGRID node requires the following minimum resources:

- CPU cores: 8 per node
- RAM: At least 24 GB per node, and 2 to 16 GB less than the total system RAM, depending on the total RAM available and the amount of non-StorageGRID software running on the system

Ensure that the number of StorageGRID nodes you plan to run on each physical or virtual host does not exceed the number of CPU cores or the physical RAM available. If the hosts are not dedicated to running StorageGRID (not recommended), be sure to consider the resource requirements of the other applications.

> Monitor your CPU and memory usage regularly to ensure that these resources continue to accommodate your workload. For example, doubling the RAM and CPU allocation for virtual Storage Nodes would provide similar resources to those provided for StorageGRID appliance nodes. Additionally, if the amount of metadata per node exceeds 500 GB, consider increasing the RAM per node to 48 GB or more. For information about managing object metadata storage, increasing the Metadata Reserved Space setting, and monitoring CPU and memory usage, see the instructions for administering, monitoring, and upgrading StorageGRID.

If hyperthreading is enabled on the underlying physical hosts, you can provide 8 virtual cores (4 physical cores)

per node. If hyperthreading is not enabled on the underlying physical hosts, you must provide 8 physical cores per node.

If you are using virtual machines as hosts and have control over the size and number of VMs, you should use a single VM for each StorageGRID node and size the VM accordingly.

For production deployments, you should not run multiple Storage Nodes on the same physical storage hardware or virtual host. Each Storage Node in a single StorageGRID deployment should be in its own isolated failure domain. You can maximize the durability and availability of object data if you ensure that a single hardware failure can only impact a single Storage Node.

See also the information about storage requirements.

Related information

NetApp Interoperability Matrix Tool

Storage and performance requirements

Administer StorageGRID

Monitor & troubleshoot

Upgrade software

Storage and performance requirements

You must understand the storage requirements for StorageGRID nodes, so you can provide enough space to support the initial configuration and future storage expansion.

StorageGRID nodes require three logical categories of storage:

- **Container pool** — Performance-tier (10K SAS or SSD) storage for the node containers, which will be assigned to the Docker storage driver when you install and configure Docker on the hosts that will support your StorageGRID nodes.
- **System data** — Performance-tier (10K SAS or SSD) storage for per-node persistent storage of system data and transaction logs, which the StorageGRID host services will consume and map into individual nodes.
- **Object data** — Performance-tier (10K SAS or SSD) storage and capacity-tier (NL-SAS/SATA) bulk storage for the persistent storage of object data and object metadata.

You must use RAID-backed block devices for all storage categories. Non-redundant disks, SSDs, or JBODs are not supported. You can use shared or local RAID storage for any of the storage categories; however, if you want to use StorageGRID's node migration capability, you must store both system data and object data on shared storage.

Performance requirements

The performance of the volumes used for the container pool, system data, and object metadata significantly impacts the overall performance of the system. You should use performance-tier (10K SAS or SSD) storage for these volumes to ensure adequate disk performance in terms of latency, input/output operations per second (IOPS), and throughput. You can use capacity-tier (NL-SAS/SATA) storage for the persistent storage of object data.

The volumes used for the container pool, system data, and object data must have write-back caching enabled.

The cache must be on a protected or persistent media.

Requirements for hosts that use NetApp AFF storage

If the StorageGRID node uses storage assigned from a NetApp AFF system, confirm that the volume does not have a FabricPool tiering policy enabled. Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.

> Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

Number of hosts required

Each StorageGRID site requires a minimum of three Storage Nodes.

> In a production deployment, do not run more than one Storage Node on a single physical or virtual host. Using a dedicated host for each Storage Node provides an isolated failure domain.

Other types of nodes, such as Admin Nodes or Gateway Nodes, can be deployed on the same hosts, or they can be deployed on their own dedicated hosts as required.

Number of storage volumes for each host

The following table shows the number of storage volumes (LUNs) required for each host and the minimum size required for each LUN, based on which nodes will be deployed on that host.

The maximum tested LUN size is 39 TB.

> These numbers are for each host, not for the entire grid.

LUN purpose	Storage category	Number of LUNs	Minimum size/LUN
Docker storage pool	Container pool	1	Total number of nodes × 100 GB
`/var/local` volume	System data	1 for each node on this host	90 GB
Storage Node	Object data	3 for each Storage Node on this host **Note:** A software-based Storage Node can have 1 to 16 storage volumes; at least 3 storage volumes are recommended.	4,000 GB See storage requirements for Storage Nodes for more information.
Admin Node audit logs	System data	1 for each Admin Node on this host	200 GB

LUN purpose	Storage category	Number of LUNs	Minimum size/LUN
Admin Node tables	System data	1 for each Admin Node on this host	200 GB

> Depending on the audit level configured, the size of user inputs such as S3 object key name, and how much audit log data you need to preserve, you might need to increase the size of the audit log LUN on each Admin Node. As a general rule, a grid generates approximately 1 KB of audit data per S3 operation, which would mean that a 200 GB LUN would support 70 million operations per day or 800 operations per second for two to three days.

Minimum storage space for a host

The following table shows the minimum storage space required for each type of node. You can use this table to determine the minimum amount of storage you must provide to the host in each storage category, based on which nodes will be deployed on that host.

> Disk snapshots cannot be used to restore grid nodes. Instead, refer to the recovery and maintenance procedures for each type of node.

Type of node	Container pool	System data	Object data
Storage Node	100 GB	90 GB	4,000 GB
Admin Node	100 GB	490 GB (3 LUNs)	*not applicable*
Gateway Node	100 GB	90 GB	*not applicable*
Archive Node	100 GB	90 GB	*not applicable*

Example: Calculating the storage requirements for a host

Suppose you plan to deploy three nodes on the same host: one Storage Node, one Admin Node, and one Gateway Node. You should provide a minimum of nine storage volumes to the host. You will need a minimum of 300 GB of performance-tier storage for the node containers, 670 GB of performance-tier storage for system data and transaction logs, and 12 TB of capacity-tier storage for object data.

Type of node	LUN purpose	Number of LUNs	LUN size
Storage Node	Docker storage pool	1	300 GB (100 GB/node)
Storage Node	`/var/local` volume	1	90 GB
Storage Node	Object data	3	4,000 GB
Admin Node	`/var/local` volume	1	90 GB
Admin Node	Admin Node audit logs	1	200 GB

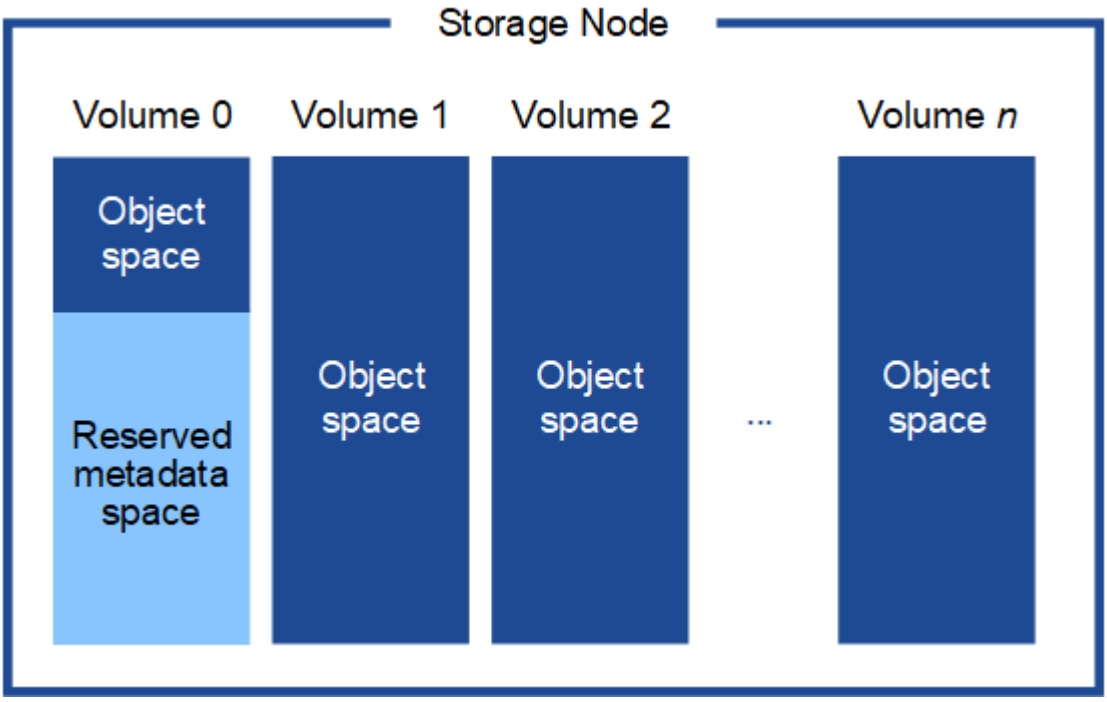
Type of node	LUN purpose	Number of LUNs	LUN size
Admin Node	Admin Node tables	1	200 GB
Gateway Node	`/var/local` volume	1	90 GB
Total		**9**	**Container pool:** 300 GB **System data:** 670 GB **Object data:** 12,000 GB

Storage requirements for Storage Nodes

A software-based Storage Node can have 1 to 16 storage volumes—3 or more storage volumes are recommended. Each storage volume should be 4 TB or larger.

> An appliance Storage Node can have up to 48 storage volumes.

As shown in the figure, StorageGRID reserves space for object metadata on storage volume 0 of each Storage Node. Any remaining space on storage volume 0 and any other storage volumes in the Storage Node are used exclusively for object data.



To provide redundancy and to protect object metadata from loss, StorageGRID stores three copies of the metadata for all objects in the system at each site. The three copies of object metadata are evenly distributed across all Storage Nodes at each site.

When you assign space to volume 0 of a new Storage Node, you must ensure there is adequate space for that node's portion of all object metadata.

- At a minimum, you must assign at least 4 TB to volume 0.

> If you use only one storage volume for a Storage Node and you assign 4 TB or less to the volume, the Storage Node might enter the Storage Read-Only state on startup and store object metadata only.

- If you are installing a new StorageGRID 11.5 system and each Storage Node has 128 GB or more of RAM, you should assign 8 TB or more to volume 0. Using a larger value for volume 0 can increase the space allowed for metadata on each Storage Node.
- When configuring different Storage Nodes for a site, use the same setting for volume 0 if possible. If a site contains Storage Nodes of different sizes, the Storage Node with the smallest volume 0 will determine the metadata capacity of that site.

For details, go to the instructions for administering StorageGRID and search for “managing object metadata storage.”

Administer StorageGRID

Related information

Node container migration requirements

Maintain & recover

Node container migration requirements

The node migration feature allows you to manually move a node from one host to another. Typically, both hosts are in the same physical data center.

Node migration allows you to perform physical host maintenance without disrupting grid operations. You simply move all StorageGRID nodes, one at a time, to another host before taking the physical host offline. Migrating nodes requires only a short downtime for each node and should not affect operation or availability of grid services.

If you want to use the StorageGRID node migration feature, your deployment must meet additional requirements:

- Consistent network interface names across hosts in a single physical data center
- Shared storage for StorageGRID metadata and object repository volumes that is accessible by all hosts in a single physical data center. For example, you might use NetApp E-Series storage arrays.

If you are using virtual hosts and the underlying hypervisor layer supports VM migration, you might want to use this capability instead of StorageGRID’s node migration feature. In this case, you can ignore these additional requirements.

Before performing migration or hypervisor maintenance, shut down the nodes gracefully. See the recovery and maintenance instructions for shutting down a grid node.

VMware Live Migration not supported

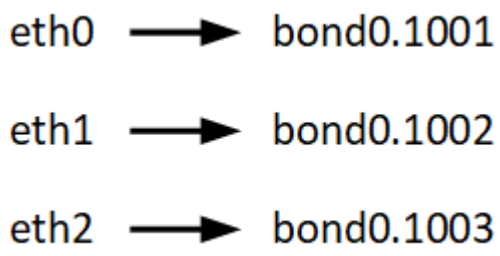
OpenStack Live Migration and VMware live vMotion cause the virtual machine clock time to jump and are not supported for grid nodes of any type. Though rare, incorrect clock times can result in loss of data or configuration updates.

Cold migration is supported. In cold migration, you shut down the StorageGRID nodes before migrating them between hosts. See the procedure for shutting down a grid node in the recovery and maintenance instructions.

Consistent network interface names

In order to move a node from one host to another, the StorageGRID host service needs to have some confidence that the external network connectivity the node has at its current location can be duplicated at the new location. It gets this confidence through the use of consistent network interface names in the hosts.

Suppose, for example, that StorageGRID NodeA running on Host1 has been configured with the following interface mappings:



The lefthand side of the arrows corresponds to the traditional interfaces as viewed from within a StorageGRID container (that is, the Grid, Admin, and Client Network interfaces, respectively). The righthand side of the arrows corresponds to the actual host interfaces providing these networks, which are three VLAN interfaces subordinate to the same physical interface bond.

Now, suppose you want to migrate NodeA to Host2. If Host2 also has interfaces named bond0.1001, bond0.1002, and bond0.1003, the system will allow the move, assuming that the like-named interfaces will provide the same connectivity on Host2 as they do on Host1. If Host2 does not have interfaces with the same names, the move will not be allowed.

There are many ways to achieve consistent network interface naming across multiple hosts; see “Configuring the host network” for some examples.

Shared storage

In order to achieve rapid, low-overhead node migrations, the StorageGRID node migration feature does not physically move node data. Instead, node migration is performed as a pair of export and import operations, as follows:

Steps

1. During the “node export” operation, a small amount of persistent state data is extracted from the node container running on HostA and cached on that node’s system data volume. Then, the node container on HostA is deinstantiated.
2. During the “node import” operation, the node container on HostB that uses the same network interface and block storage mappings that were in effect on HostA is instantiated. Then, the cached persistent state data is inserted into the new instance.

Given this mode of operation, all of the node’s system data and object storage volumes must be accessible from both HostA and HostB for the migration to be allowed, and to work. In addition, they must have been mapped into the node using names that are guaranteed to refer to the same LUNs on HostA and HostB.

The following example shows one solution for block device mapping for a StorageGRID Storage Node, where DM multipathing is in use on the hosts, and the alias field has been used in `/etc/multipath.conf` to provide consistent, friendly block device names available on all hosts.

/var/local → /dev/mapper/sgws-sn1-var-local

rangedb0 → /dev/mapper/sgws-sn1-rangedb0

rangedb1 → /dev/mapper/sgws-sn1-rangedb1

rangedb2 → /dev/mapper/sgws-sn1-rangedb2

rangedb3 → /dev/mapper/sgws-sn1-rangedb3

Related information

Configuring the host network

Maintain & recover

Web browser requirements

You must use a supported web browser.

Web browser	Minimum supported version
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

You should set the browser window to a recommended width.

Browser width	Pixels
Minimum	1024
Optimum	1280

Deployment tools

You might benefit from automating all or part of the StorageGRID installation.

Automating the deployment might be useful in any of the following cases:

- You already use a standard orchestration framework, such as Ansible, Puppet, or Chef, to deploy and configure physical or virtual hosts.
- You intend to deploy multiple StorageGRID instances.
- You are deploying a large, complex StorageGRID instance.

The StorageGRID host service is installed by a package and driven by configuration files that can be created interactively during a manual installation, or prepared ahead of time (or programmatically) to enable automated installation using standard orchestration frameworks. StorageGRID provides optional Python scripts for automating the configuration of StorageGRID appliances, and the whole StorageGRID system (the “grid”). You can use these scripts directly, or you can inspect them to learn how to use the StorageGRID Installation REST API in grid deployment and configuration tools you develop yourself.

If you are interested in automating all or part of your StorageGRID deployment, review “Automating the installation” before beginning the installation process.

Related information

Automating the installation

Preparing the hosts

You must complete the following steps to prepare your physical or virtual hosts for StorageGRID. Note that you can automate many or all of these steps using standard server configuration frameworks such as Ansible, Puppet, or Chef.

Related information

Automating the installation and configuration of the StorageGRID host service

Installing Linux

You must install Ubuntu or Debian on all grid hosts. Use the NetApp Interoperability Matrix Tool to get a list of supported versions.

Steps

1. Install Ubuntu or Debian on all physical or virtual grid hosts according to the distributor’s instructions or your standard procedure.

   > Do not install any graphical desktop environments. When installing Ubuntu, you must select **standard system utilities**. Selecting **OpenSSH server** is recommended to enable ssh access to your Ubuntu hosts. All other options can remain unselected.

2. Ensure that all hosts have access to Ubuntu or Debian package repositories.
3. If swap is enabled:

   a. Run the following command: `$ sudo swapoff --all`

   b. Remove all swap entries from `/etc/fstab` to persist the settings.

   > Failing to disable swap entirely can severely lower performance.

Related information

NetApp Interoperability Matrix Tool

Understanding AppArmor profile installation

If you are operating in a self-deployed Ubuntu environment and using the AppArmor mandatory access control system, the AppArmor profiles associated with packages you

install on the base system might be blocked by the corresponding packages installed with StorageGRID.

By default, AppArmor profiles are installed for packages that you install on the base operating system. When you run these packages from the StorageGRID system container, the AppArmor profiles are blocked. The DHCP, MySQL, NTP, and tcdump base packages conflict with AppArmor, and other base packages might also conflict.

You have two choices for handling AppArmor profiles:

- Disable individual profiles for the packages installed on the base system that overlap with the packages in the StorageGRID system container. When you disable individual profiles, an entry appears in the StorageGRID log files indicating that AppArmor is enabled.

  Use the following commands:

  ```
  sudo ln -s /etc/apparmor.d/<profile.name> /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/<profile.name>
  ```

  Example:

  ```
  sudo ln -s /etc/apparmor.d/bin.ping /etc/apparmor.d/disable/
  sudo apparmor_parser -R /etc/apparmor.d/bin.ping
  ```

- Disable AppArmor altogether. For Ubuntu 9.10 or later, follow the instructions in the Ubuntu online community: Disable AppArmor.

  Once you disable AppArmor, no entries indicating that AppArmor is enabled will appear in the StorageGRID log files.

Configuring the host network

After completing the Linux installation on your hosts, you might need to perform some additional configuration to prepare a set of network interfaces on each host that are suitable for mapping into the StorageGRID nodes you will deploy later.

What you'll need

- You have reviewed the StorageGRID networking guidelines.

  Network guidelines

- You have reviewed the information about node container migration requirements.

  Node container migration requirements

- If you are using virtual hosts, you have read the considerations and recommendations for MAC address cloning before configuring the host network.

  Considerations and recommendations for MAC address cloning

> If you are using VMs as hosts, you should select VMXNET 3 as the virtual network adapter. The VMware E1000 network adapter has caused connectivity issues with StorageGRID containers deployed on certain distributions of Linux.

About this task

Grid nodes must be able to access the Grid Network and, optionally, the Admin and Client Networks. You provide this access by creating mappings that associate the host's physical interface to the virtual interfaces for each grid node. When creating host interfaces, use friendly names to facilitate deployment across all hosts, and to enable migration.

The same interface can be shared between the host and one or more nodes. For example, you might use the same interface for host access and node Admin Network access, to facilitate host and node maintenance. Although the same interface can be shared between the host and individual nodes, all must have different IP addresses. IP addresses cannot be shared between nodes or between the host and any node.

You can use the same host network interface to provide the Grid Network interface for all StorageGRID nodes on the host; you can use a different host network interface for each node; or you can do something in between. However, you would not typically provide the same host network interface as both the Grid and Admin Network interfaces for a single node, or as the Grid Network interface for one node and the Client Network interface for another.

You can complete this task in many ways. For example, if your hosts are virtual machines and you are deploying one or two StorageGRID nodes for each host, you can simply create the correct number of network interfaces in the hypervisor, and use a 1-to-1 mapping. If you are deploying multiple nodes on bare metal hosts for production use, you can leverage the Linux networking stack's support for VLAN and LACP for fault tolerance and bandwidth sharing. The following sections provide detailed approaches for both of these examples. You do not need to use either of these examples; you can use any approach that meets your needs.

> Do not use bond or bridge devices directly as the container network interface. Doing so could prevent node start-up caused by a kernel issue with the use of MACVLAN with bond and bridge devices in the container namespace. Instead, use a non-bond device, such as a VLAN or virtual Ethernet (veth) pair. Specify this device as the network interface in the node configuration file.

Considerations and recommendations for MAC address cloning

MAC address cloning causes the Docker container to use the MAC address of the host, and the host to use the MAC address of either an address you specify or a randomly generated one. You should use MAC address cloning to avoid the use of promiscuous mode network configurations.

Enabling MAC cloning

In certain environments, security can be enhanced through MAC address cloning because it enables you to use a dedicated virtual NIC for the Admin Network, Grid Network, and Client Network. Having the Docker container use the MAC address of the dedicated NIC on the host allows you to avoid using promiscuous mode network configurations.

> MAC address cloning is intended to be used with virtual server installations and might not function properly with all physical appliance configurations.

> If a node fails to start due to a MAC cloning targeted interface being busy, you might need to set the link to "down" before starting node. Additionally, it is possible that the virtual environment might prevent MAC cloning on a network interface while the link is up. If a node fails to set the MAC address and start due to an interface being busy, setting the link to "down" before starting the node might fix the issue.

MAC address cloning is disabled by default and must be set by node configuration keys. You should enable it when you install StorageGRID.

There is one key for each network:

- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`
- `CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC`

Setting the key to "true" causes the Docker container to use the MAC address of the host's NIC. Additionally, the host will then use the MAC address of the specified container network. By default, the container address is a randomly generated address, but if you have set one using the `_NETWORK_MAC` node configuration key, that address is used instead. The host and container will always have different MAC addresses.

> Enabling MAC cloning on a virtual host without also enabling promiscuous mode on the hypervisor might cause Linux host networking using the host's interface to stop working.

MAC cloning use cases

There are two use cases to consider with MAC cloning:

- MAC cloning not enabled: When the `_CLONE_MAC` key in the node configuration file is not set, or set to "false," the host will use the host NIC MAC and the container will have a StorageGRID-generated MAC unless a MAC is specified in the `_NETWORK_MAC` key. If an address is set in the `_NETWORK_MAC` key, the container will have the address specified in the `_NETWORK_MAC` key. This configuration of keys requires the use of promiscuous mode.
- MAC cloning enabled: When the `_CLONE_MAC` key in the node configuration file is set to "true," the container uses the host NIC MAC, and the host uses a StorageGRID-generated MAC unless a MAC is specified in the `_NETWORK_MAC` key. If an address is set in the `_NETWORK_MAC` key, the host uses the specified address instead of a generated one. In this configuration of keys, you should not use promiscuous mode.

> If you do not want to use MAC address cloning and would rather allow all interfaces to receive and transmit data for MAC addresses other than the ones assigned by the hypervisor, ensure that the security properties at the virtual switch and port group levels are set to **Accept** for Promiscuous Mode, MAC Address Changes, and Forged Transmits. The values set on the virtual switch can be overridden by the values at the port group level, so ensure that settings are the same in both places.

To enable MAC cloning, see the instructions for creating node configuration files.

Creating node configuration files

MAC cloning example

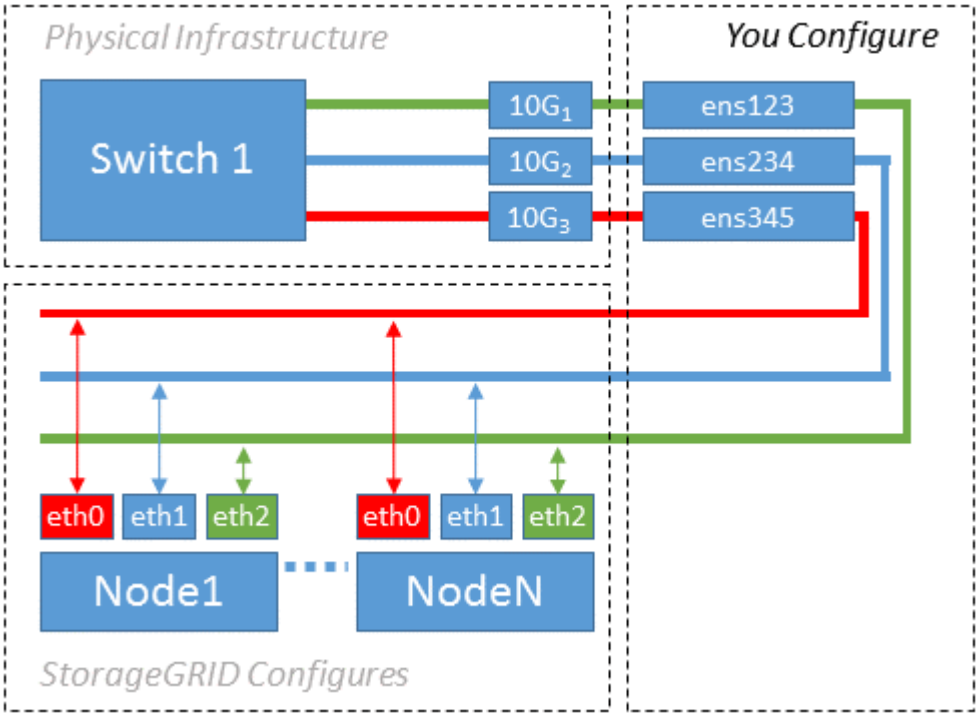
Example of MAC cloning enabled with a host having MAC address of 11:22:33:44:55:66 for the interface ens256 and the following keys in the node configuration file:

- `ADMIN_NETWORK_TARGET = ens256`
- `ADMIN_NETWORK_MAC = b2:9c:02:c2:27:10`
- `ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC = true`

Result: the host MAC for ens256 is b2:9c:02:c2:27:10 and the Admin Network MAC is 11:22:33:44:55:66

Example 1: 1-to-1 mapping to physical or virtual NICs

Example 1 describes a simple physical interface mapping that requires little or no host-side configuration.



The Linux operating system creates the ensXYZ interfaces automatically during installation or boot, or when the interfaces are hot-added. No configuration is required other than ensuring that the interfaces are set to come up automatically after boot. You do have to determine which ensXYZ corresponds to which StorageGRID network (Grid, Admin, or Client) so you can provide the correct mappings later in the configuration process.

Note that the figure show multiple StorageGRID nodes; however, you would normally use this configuration for single-node VMs.

If Switch 1 is a physical switch, you should configure the ports connected to interfaces $10G_1$ through $10G_3$ for access mode, and place them on the appropriate VLANs.

Example 2: LACP bond carrying VLANs

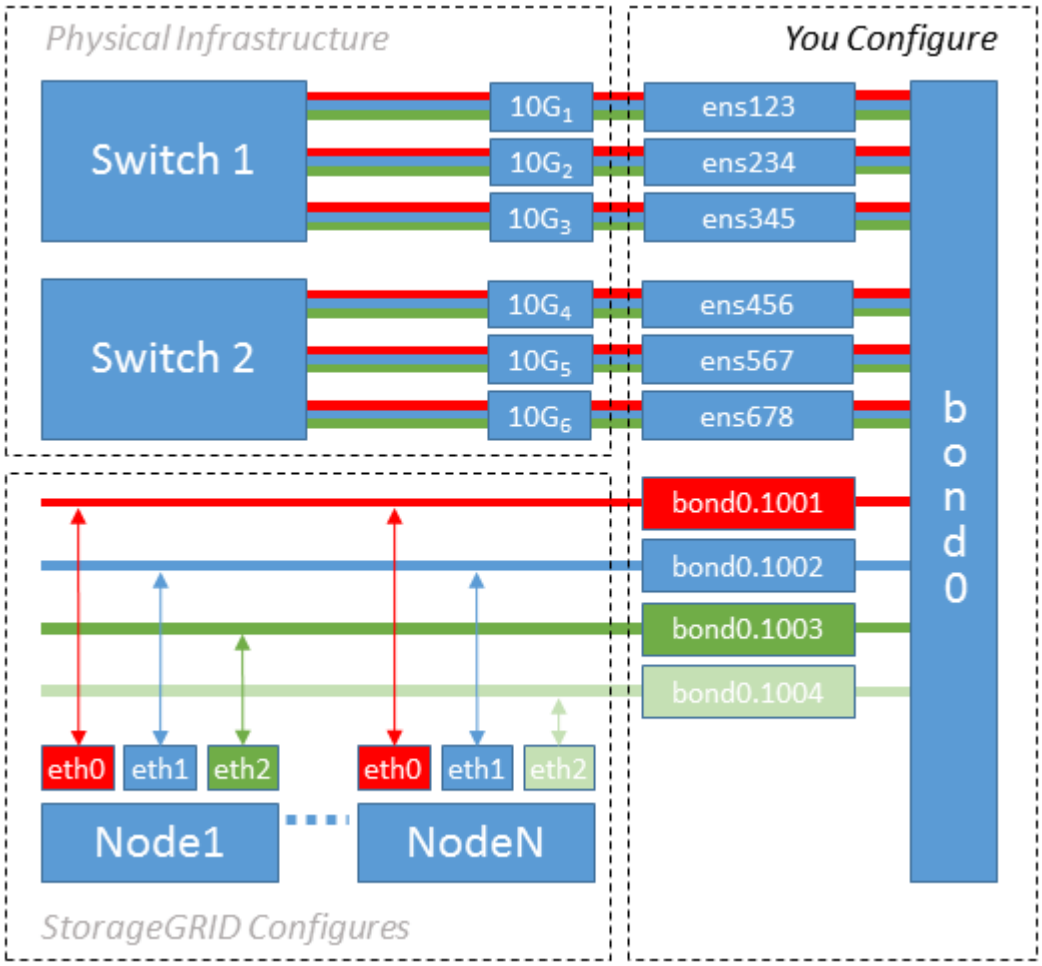
Example 2 assumes you are familiar with bonding network interfaces and with creating VLAN interfaces on the Linux distribution you are using.

About this task

Example 2 describes a generic, flexible, VLAN-based scheme that facilitates the sharing of all available network bandwidth across all nodes on a single host. This example is particularly applicable to bare metal hosts.

To understand this example, suppose you have three separate subnets for the Grid, Admin, and Client Networks at each data center. The subnets are on separate VLANs (1001, 1002, and 1003) and are presented to the host on a LACP-bonded trunk port (bond0). You would configure three VLAN interfaces on the bond: bond0.1001, bond0.1002, and bond0.1003.

If you require separate VLANs and subnets for node networks on the same host, you can add VLAN interfaces on the bond and map them into the host (shown as bond0.1004 in the illustration).



Steps

1. Aggregate all physical network interfaces that will be used for StorageGRID network connectivity into a single LACP bond.

   Use the same name for the bond on every host, for example, bond0.

2. Create VLAN interfaces that use this bond as their associated “physical device,” using the standard VLAN interface naming convention `physdev-name.VLAN ID`.

   Note that steps 1 and 2 require appropriate configuration on the edge switches terminating the other ends of the network links. The edge switch ports must also be aggregated into a LACP port channel, configured as a trunk, and allowed to pass all required VLANs.

Sample interface configuration files for this per-host networking configuration scheme are provided.

Related information

Example /etc/network/interfaces

Configuring host storage

You must allocate block storage volumes to each host.

What you'll need

You have reviewed the following topics, which provide information you need to accomplish this task:

Storage and performance requirements

Node container migration requirements

About this task

When allocating block storage volumes (LUNs) to hosts, use the tables in "Storage requirements" to determine the following:

- Number of volumes required for each host (based on the number and types of nodes that will be deployed on that host)
- Storage category for each volume (that is, System Data or Object Data)
- Size of each volume

You will use this information as well as the persistent name assigned by Linux to each physical volume when you deploy StorageGRID nodes on the host.

> You do not need to partition, format, or mount any of these volumes; you just need to ensure they are visible to the hosts.

Avoid using "raw" special device files (`/dev/sdb`, for example) as you compose your list of volume names. These files can change across reboots of the host, which will impact proper operation of the system. If you are using iSCSI LUNs and device mapper multipathing, consider using multipath aliases in the `/dev/mapper` directory, especially if your SAN topology includes redundant network paths to the shared storage. Alternatively, you can use the system-created softlinks under `/dev/disk/by-path/` for your persistent device names.

For example:

```
ls -l
$ ls -l /dev/disk/by-path/
total 0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:00:07.1-ata-2 -> ../../sr0
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0 ->
../../sda
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part1
-> ../../sda1
lrwxrwxrwx 1 root root 10 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:0:0-part2
-> ../../sda2
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:1:0 ->
../../sdb
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:2:0 ->
../../sdc
lrwxrwxrwx 1 root root  9 Sep 19 18:53 pci-0000:03:00.0-scsi-0:0:3:0 ->
../../sdd
```

Results will differ for each installation.

Assign friendly names to each of these block storage volumes to simplify the initial StorageGRID installation and future maintenance procedures. If you are using the device mapper multipath driver for redundant access to shared storage volumes, you can use the `alias` field in your `/etc/multipath.conf` file.

For example:

```
multipaths {
     multipath {
          wwid 3600a09800059d6df00005df2573c2c30
          alias docker-storage-volume-hostA
     }
     multipath {
          wwid 3600a09800059d6df00005df3573c2c30
          alias sgws-adm1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df4573c2c30
          alias sgws-adm1-audit-logs
     }
     multipath {
          wwid 3600a09800059d6df00005df5573c2c30
          alias sgws-adm1-tables
     }
     multipath {
          wwid 3600a09800059d6df00005df6573c2c30
          alias sgws-gw1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-var-local
     }
     multipath {
          wwid 3600a09800059d6df00005df7573c2c30
          alias sgws-sn1-rangedb-0
     }
     …
```

This will cause the aliases to appear as block devices in the `/dev/mapper` directory on the host, allowing you to specify a friendly, easily-validated name whenever a configuration or maintenance operation requires specifying a block storage volume.

> If you are setting up shared storage to support StorageGRID node migration and using device mapper multipathing, you can create and install a common `/etc/multipath.conf` on all co-located hosts. Just make sure to use a different Docker storage volume on each host. Using aliases and including the target hostname in the alias for each Docker storage volume LUN will make this easy to remember and is recommended.

Related information

Storage and performance requirements

Node container migration requirements

Configuring the Docker storage volume

Before installing Docker, you might need to format the Docker storage volume and mount it on `/var/lib/docker`.

About this task

You can skip these steps if you plan to use local storage for the Docker storage volume and have sufficient space available on the host partition containing `/var/lib`.

Steps

1. Create a file system on the Docker storage volume:

```
sudo mkfs.ext4 docker-storage-volume-device
```

2. Mount the Docker storage volume:

```
sudo mkdir -p /var/lib/docker
sudo mount docker-storage-volume-device /var/lib/docker
```

3. Add an entry for docker-storage-volume-device to /etc/fstab.

   This step ensures that the storage volume will remount automatically after host reboots.

Installing Docker

The StorageGRID system runs on Linux as a collection of Docker containers. Before you can install StorageGRID, you must install Docker.

Steps

1. Install Docker by following the instructions for your Linux distribution.

   > If Docker is not included with your Linux distribution, you can download it from the Docker website.

2. Ensure Docker has been enabled and started by running the following two commands:

```
sudo systemctl enable docker
```

```
sudo systemctl start docker
```

3. Confirm you have installed the expected version of Docker by entering the following:

```
sudo docker version
```

The Client and Server versions must be 1.10.3 or later.

```
Client:
  Version:      1.10.3
  API version:  1.22
  Go version:   go1.6.1
  Git commit:   20f81dd
  Built:        Wed, 20 Apr 2016 14:19:16 -0700
  OS/Arch:      linux/amd64

Server:
  Version:      1.10.3
  API version:  1.22
  Go version:   go1.6.1
  Git commit:   20f81dd
  Built:        Wed, 20 Apr 2016 14:19:16 -0700
  OS/Arch:      linux/amd64
```

Related information

Configuring host storage

Installing StorageGRID host services

You use the StorageGRID DEB package to install the StorageGRID host services.

About this task

These instructions describe how to install the host services from the DEB packages. As an alternative, you can use the APT repository metadata included in the installation archive to install the DEB packages remotely. See the APT repository instructions for your Linux operating system.

Steps

1. Copy the StorageGRID DEB packages to each of your hosts, or make them available on shared storage.

   For example, place them in the `/tmp` directory, so you can use the example command in the next step.

2. Log in to each host as root or using an account with sudo permission, and run the following commands.

   You must install the `images` package first, and the `service` package second. If you placed the packages in a directory other than `/tmp`, modify the command to reflect the path you used.

   ```
   sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb
   ```

   ```
   sudo dpkg --install /tmp/storagegrid-webscale-service-version-SHA.deb
   ```

> Python 2.7 must already be installed before the StorageGRID packages can be installed. The `sudo dpkg --install /tmp/storagegrid-webscale-images-version-SHA.deb` command will fail until you have done so.

Deploying virtual grid nodes

When you deploy grid nodes in an Ubuntu or Debian environment, you create node configuration files for all nodes, validate the files, and start the StorageGRID host service, which starts the nodes. If you need to deploy any StorageGRID appliance Storage Nodes, see the installation and maintenance instructions for the appliance after you have deployed all virtual nodes.

- Creating node configuration files
- Validating the StorageGRID configuration
- Starting the StorageGRID host service

Related information

SG100 & SG1000 services appliances

SG5600 storage appliances

SG5700 storage appliances

SG6000 storage appliances

Creating node configuration files

Node configuration files are small text files that provide the information the StorageGRID host service needs to start a node and connect it to the appropriate network and block storage resources. Node configuration files are used for virtual nodes and are not used for appliance nodes.

Where do I put the node configuration files?

You must place the configuration file for each StorageGRID node in the `/etc/storagegrid/nodes` directory on the host where the node will run. For example, if you plan to run one Admin Node, one Gateway Node, and one Storage Node on HostA, you must place three node configuration files in `/etc/storagegrid/nodes` on HostA. You can create the configuration files directly on each host using a text editor, such as vim or nano, or you can create them elsewhere and move them to each host.

What do I name the node configuration files?

The names of the configuration files are significant. The format is `<node-name>.conf`, where `<node-name>` is a name you assign to the node. This name appears in the StorageGRID Installer and is used for node maintenance operations, such as node migration.

Node names must follow these rules:

- Must be unique

- Must start with a letter
- Can contain the characters A through Z and a through z
- Can contain the numbers 0 through 9
- Can contain one or more hyphens (-)
- Must be no more than 32 characters, not including the `.conf` extension

Any files in `/etc/storagegrid/nodes` that do not follow these naming conventions will not be parsed by the host service.

If you have a multi-site topology planned for your grid, a typical node naming scheme might be:

```
<site>-<node type>-<node number>.conf
```

For example, you might use `dc1-adm1.conf` for the first Admin Node in Data Center 1, and `dc2-sn3.conf` for the third Storage Node in Data Center 2. However, you can use any scheme you like, as long as all node names follow the naming rules.

What is in a node configuration file?

The configuration files contain key/value pairs, with one key and one value per line. For each key/value pair, you must follow these rules:

- The key and the value must be separated by an equal sign (=) and optional whitespace.
- The keys can contain no spaces.
- The values can contain embedded spaces.
- Any leading or trailing whitespace is ignored.

Some keys are required for every node, while others are optional or only required for certain node types.

The table defines the acceptable values for all supported keys. In the middle column:

R: required
BP: best practice
O: optional

Key	R, BP, or O?	Value
ADMIN_IP	BP	Grid Network IPv4 address of the primary Admin Node for the grid to which this node belongs. Use the same value you specified for GRID_NETWORK_IP for the grid node with NODE_TYPE = VM_Admin_Node and ADMIN_ROLE = Primary. If you omit this parameter, the node attempts to discover a primary Admin Node using mDNS. See “How grid nodes discover the primary Admin Node.” **Note**: This value is ignored, and might be prohibited, on the primary Admin Node.
ADMIN_NETWORK_CONFIG	O	DHCP, STATIC, or DISABLED
ADMIN_NETWORK_ESL	O	Comma-separated list of subnets in CIDR notation to which this node should communicate via the Admin Network gateway. Example: 172.16.0.0/21,172.17.0.0/21
ADMIN_NETWORK_GATEWAY	O (**R**)	IPv4 address of the local Admin Network gateway for this node. Must be on the subnet defined by ADMIN_NETWORK_IP and ADMIN_NETWORK_MASK. This value is ignored for DHCP-configured networks. **Note**: This parameter is required if ADMIN_NETWORK_ESL is specified. Examples: • 1.1.1.1 • 10.224.4.81

Key	R, BP, or O?	Value
ADMIN_NETWORK_IP	O	IPv4 address of this node on the Admin Network. This key is only required when ADMIN_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 1.1.1.1 • 10.224.4.81
ADMIN_NETWORK_MAC	O	The MAC address for the Admin Network interface in the container. This field is optional. If omitted, a MAC address will be generated automatically. Must be 6 pairs of hexadecimal digits separated by colons. Example: b2:9c:02:c2:27:10
ADMIN_NETWORK_MASK	O	IPv4 netmask for this node, on the Admin Network. This key is only required when ADMIN_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 255.255.255.0 • 255.255.248.0

Key	R, BP, or O?	Value
ADMIN_NETWORK_MTU	O	The maximum transmission unit (MTU) for this node on the Admin Network. Do not specify if ADMIN_NETWORK_CONFIG = DHCP. If specified, the value must be between 1280 and 9216. If omitted, 1500 is used. If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value. **IMPORTANT**: The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur. Examples: • 1500 • 8192

Key	R, BP, or O?	Value
ADMIN_NETWORK_TARGET	BP	Name of the host device that you will use for Admin Network access by the StorageGRID node. Only network interface names are supported. Typically, you use a different interface name than what was specified for GRID_NETWORK_TARGET or CLIENT_NETWORK_TARGET. **Note**: Do not use bond or bridge devices as the network target. Either configure a VLAN (or other virtual interface) on top of the bond device, or use a bridge and virtual Ethernet (veth) pair. **Best practice:** Specify a value even if this node will not initially have an Admin Network IP address. Then you can add an Admin Network IP address later, without having to reconfigure the node on the host. Examples: • bond0.1002 • ens256
ADMIN_NETWORK_TARGET_TYPE	O	Interface (This is the only supported value.)

Key	R, BP, or O?	Value
ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	True or False Set the key to "true" to cause the StorageGRID container use the MAC address of the host host target interface on the Admin Network. **Best practice:** In networks where promiscuous mode would be required, use the ADMIN_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC key instead. For more details on MAC cloning, see the considerations and recommendations for MAC address cloning. Considerations and recommendations for MAC address cloning
ADMIN_ROLE	**R**	Primary or Non-Primary This key is only required when NODE_TYPE = VM_Admin_Node; do not specify it for other node types.
BLOCK_DEVICE_AUDIT_LOGS	**R**	Path and name of the block device special file this node will use for persistent storage of audit logs. This key is only required for nodes with NODE_TYPE = VM_Admin_Node; do not specify it for other node types. Examples: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-adm1-audit-logs`

Key	R, BP, or O?	Value
BLOCK_DEVICE_RANGEDB_00 BLOCK_DEVICE_RANGEDB_01 BLOCK_DEVICE_RANGEDB_02 BLOCK_DEVICE_RANGEDB_03 BLOCK_DEVICE_RANGEDB_04 BLOCK_DEVICE_RANGEDB_05 BLOCK_DEVICE_RANGEDB_06 BLOCK_DEVICE_RANGEDB_07 BLOCK_DEVICE_RANGEDB_08 BLOCK_DEVICE_RANGEDB_09 BLOCK_DEVICE_RANGEDB_10 BLOCK_DEVICE_RANGEDB_11 BLOCK_DEVICE_RANGEDB_12 BLOCK_DEVICE_RANGEDB_13 BLOCK_DEVICE_RANGEDB_14 BLOCK_DEVICE_RANGEDB_15	**R**	Path and name of the block device special file this node will use for persistent object storage. This key is only required for nodes with NODE_TYPE = VM_Storage_Node; do not specify it for other node types. Only BLOCK_DEVICE_RANGEDB_00 is required; the rest are optional. The block device specified for BLOCK_DEVICE_RANGEDB_00 must be at least 4 TB; the others can be smaller. **Note**: Do not leave gaps. If you specify BLOCK_DEVICE_RANGEDB_05, you must also specify BLOCK_DEVICE_RANGEDB_04. Examples: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-sn1-rangedb-0`

Key	R, BP, or O?	Value
BLOCK_DEVICE_TABLES	**R**	Path and name of the block device special file this node will use for persistent storage of database tables. This key is only required for nodes with NODE_TYPE = VM_Admin_Node; do not specify it for other node types. Examples: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-adm1-tables`
BLOCK_DEVICE_VAR_LOCAL	**R**	Path and name of the block device special file this node will use for its /var/local persistent storage. Examples: • `/dev/disk/by-path/pci-0000:03:00.0-scsi-0:0:0:0` • `/dev/disk/by-id/wwn-0x600a09800059d6df000060d757b475fd` • `/dev/mapper/sgws-sn1-var-local`
CLIENT_NETWORK_CONFIG	O	DHCP, STATIC, or DISABLED

Key	R, BP, or O?	Value
CLIENT_NETWORK_GATEWAY	O	IPv4 address of the local Client Network gateway for this node, which must be on the subnet defined by CLIENT_NETWORK_IP and CLIENT_NETWORK_MASK. This value is ignored for DHCP-configured networks. Examples: • 1.1.1.1 • 10.224.4.81
CLIENT_NETWORK_IP	O	IPv4 address of this node on the Client Network. This key is only required when CLIENT_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 1.1.1.1 • 10.224.4.81
CLIENT_NETWORK_MAC	O	The MAC address for the Client Network interface in the container. This field is optional. If omitted, a MAC address will be generated automatically. Must be 6 pairs of hexadecimal digits separated by colons. Example: b2:9c:02:c2:27:20
CLIENT_NETWORK_MASK	O	IPv4 netmask for this node on the Client Network. This key is only required when CLIENT_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 255.255.255.0 • 255.255.248.0

Key	R, BP, or O?	Value
CLIENT_NETWORK_MTU	O	The maximum transmission unit (MTU) for this node on the Client Network. Do not specify if CLIENT_NETWORK_CONFIG = DHCP. If specified, the value must be between 1280 and 9216. If omitted, 1500 is used. If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value. **IMPORTANT**: The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur. Examples: • 1500 • 8192

Key	R, BP, or O?	Value
CLIENT_NETWORK_TARGET	BP	Name of the host device that you will use for Client Network access by the StorageGRID node. Only network interface names are supported. Typically, you use a different interface name than what was specified for GRID_NETWORK_TARGET or ADMIN_NETWORK_TARGET. **Note**: Do not use bond or bridge devices as the network target. Either configure a VLAN (or other virtual interface) on top of the bond device, or use a bridge and virtual Ethernet (veth) pair. **Best practice:** Specify a value even if this node will not initially have a Client Network IP address. Then you can add a Client Network IP address later, without having to reconfigure the node on the host. Examples: • bond0.1003 • ens423
CLIENT_NETWORK_TARGET_TYPE	O	Interface (This is only supported value.)

Key	R, BP, or O?	Value
CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	BP	True or False Set the key to "true" to cause the StorageGRID container to use the MAC address of the host target interface on the Client Network. **Best practice:** In networks where promiscuous mode would be required, use the CLIENT_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC key instead. For more details on MAC cloning, see the considerations and recommendations for MAC address cloning. Considerations and recommendations for MAC address cloning
GRID_NETWORK_CONFIG	BP	STATIC or DHCP (Defaults to STATIC if not specified.)
GRID_NETWORK_GATEWAY	**R**	IPv4 address of the local Grid Network gateway for this node, which must be on the subnet defined by GRID_NETWORK_IP and GRID_NETWORK_MASK. This value is ignored for DHCP-configured networks. If the Grid Network is a single subnet with no gateway, use either the standard gateway address for the subnet (X.Y.Z.1) or this node's GRID_NETWORK_IP value; either value will simplify potential future Grid Network expansions.

Key	R, BP, or O?	Value
GRID_NETWORK_IP	**R**	IPv4 address of this node on the Grid Network. This key is only required when GRID_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 1.1.1.1 • 10.224.4.81
GRID_NETWORK_MAC	O	The MAC address for the Grid Network interface in the container. This field is optional. If omitted, a MAC address will be generated automatically. Must be 6 pairs of hexadecimal digits separated by colons. Example: b2:9c:02:c2:27:30
GRID_NETWORK_MASK	O	IPv4 netmask for this node on the Grid Network. This key is only required when GRID_NETWORK_CONFIG = STATIC; do not specify it for other values. Examples: • 255.255.255.0 • 255.255.248.0

Key	R, BP, or O?	Value
GRID_NETWORK_MTU	O	The maximum transmission unit (MTU) for this node on the Grid Network. Do not specify if GRID_NETWORK_CONFIG = DHCP. If specified, the value must be between 1280 and 9216. If omitted, 1500 is used. If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value. **IMPORTANT**: The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur. **IMPORTANT**: For the best network performance, all nodes should be configured with similar MTU values on their Grid Network interfaces. The **Grid Network MTU mismatch** alert is triggered if there is a significant difference in MTU settings for the Grid Network on individual nodes. The MTU values do not have to be the same for all network types. Examples: • 1500 • 8192

Key	R, BP, or O?	Value
GRID_NETWORK_TARGET	**R**	Name of the host device that you will use for Grid Network access by the StorageGRID node. Only network interface names are supported. Typically, you use a different interface name than what was specified for ADMIN_NETWORK_TARGET or CLIENT_NETWORK_TARGET. **Note**: Do not use bond or bridge devices as the network target. Either configure a VLAN (or other virtual interface) on top of the bond device, or use a bridge and virtual Ethernet (veth) pair. Examples: • bond0.1001 • ens192
GRID_NETWORK_TARGET_TYPE	O	Interface (This is the only supported value.)
GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC	**BP**	True or False Set the value of the key to "true" to cause the StorageGRID container to use the MAC address of the host target interface on the Grid Network. **Best practice:** In networks where promiscuous mode would be required, use the GRID_NETWORK_TARGET_TYPE_INTERFACE_CLONE_MAC key instead. For more details on MAC cloning, see the considerations and recommendations for MAC address cloning. Considerations and recommendations for MAC address cloning

Key	R, BP, or O?	Value
MAXIMUM_RAM	O	The maximum amount of RAM that this node is allowed to consume. If this key is omitted, the node has no memory restrictions. When setting this field for a production-level node, specify a value that is at least 24 GB and 16 to 32 GB less than the total system RAM. **Note**: The RAM value affects a node's actual metadata reserved space. See the instructions for administering StorageGRID for a description of what Metadata Reserved Space is. The format for this field is `<number><unit>`, where `<unit>` can be `b`, `k`, `m`, or `g`. Examples: 24g 38654705664b **Note**: If you want to use this option, you must enable kernel support for memory cgroups.
NODE_TYPE	**R**	Type of node: • VM_Admin_Node • VM_Storage_Node • VM_Archive_Node • VM_API_Gateway

Key	R, BP, or O?	Value
PORT_REMAP	O	Remaps any port used by a node for internal grid node communications or external communications. Remapping ports is necessary if enterprise networking policies restrict one or more ports used by StorageGRID, as described in “Internal grid node communications” or “External communications.” **IMPORTANT**: Do not remap the ports you are planning to use to configure load balancer endpoints. **Note**: If only PORT_REMAP is set, the mapping that you specify is used for both inbound and outbound communications. If PORT_REMAP_INBOUND is also specified, PORT_REMAP applies only to outbound communications. The format used is: `<network type>/<protocol>/<default port used by grid node>/<new port>`, where network type is grid, admin, or client, and protocol is tcp or udp. For example: `PORT_REMAP = client/tcp/18082/443`

Key	R, BP, or O?	Value
PORT_REMAP_INBOUND	O	Remaps inbound communications to the specified port. If you specify PORT_REMAP_INBOUND but do not specify a value for PORT_REMAP, outbound communications for the port are unchanged. **IMPORTANT**: Do not remap the ports you are planning to use to configure load balancer endpoints. The format used is: `<network type>/<protocol:>/<remapped port >/<default port used by grid node>`, where network type is grid, admin, or client, and protocol is tcp or udp. For example: `PORT_REMAP_INBOUND = grid/tcp/3022/22`

Related information

How grid nodes discover the primary Admin Node

Network guidelines

Administer StorageGRID

How grid nodes discover the primary Admin Node

Grid nodes communicate with the primary Admin Node for configuration and management. Each grid node must know the IP address of the primary Admin Node on the Grid Network.

To ensure that a grid node can access the primary Admin Node, you can do either of the following when deploying the node:

- You can use the ADMIN_IP parameter to enter the primary Admin Node's IP address manually.
- You can omit the ADMIN_IP parameter to have the grid node discover the value automatically. Automatic discovery is especially useful when the Grid Network uses DHCP to assign the IP address to the primary Admin Node.

Automatic discovery of the primary Admin Node is accomplished using a multicast Domain Name System (mDNS). When the primary Admin Node first starts up, it publishes its IP address using mDNS. Other nodes on the same subnet can then query for the IP address and acquire it automatically. However, because multicast IP traffic is not normally routable across subnets, nodes on other subnets cannot acquire the primary Admin

Node's IP address directly.

> If you use automatic discovery:
>
> - You must include the ADMIN_IP setting for at least one grid node on any subnets that the primary Admin Node is not directly attached to. This grid node will then publish the primary Admin Node's IP address for other nodes on the subnet to discover with mDNS.
> - Ensure that your network infrastructure supports passing multi-cast IP traffic within a subnet.

Example node configuration files

You can use the example node configuration files to help set up the node configuration files for your StorageGRID system. The examples show node configuration files for all types of grid nodes.

For most nodes, you can add Admin and Client Network addressing information (IP, mask, gateway, and so on) when you configure the grid using the Grid Manager or the Installation API. The exception is the primary Admin Node. If you want to browse to the Admin Network IP of the primary Admin Node to complete grid configuration (because the Grid Network is not routed, for example), you must configure the Admin Network connection for the primary Admin Node in its node configuration file. This is shown in the example.

> In the examples, the Client Network target has been configured as a best practice, even though the Client Network is disabled by default.

Example for primary Admin Node

Example file name: `/etc/storagegrid/nodes/dc1-adm1.conf`

Example file contents:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Primary
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm1-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm1-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm1-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.2
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1

ADMIN_NETWORK_CONFIG = STATIC
ADMIN_NETWORK_IP = 192.168.100.2
ADMIN_NETWORK_MASK = 255.255.248.0
ADMIN_NETWORK_GATEWAY = 192.168.100.1
ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0.0/21,172.17.0.0/21
```

Example for Storage Node

Example file name: `/etc/storagegrid/nodes/dc1-sn1.conf`

Example file contents:

```
NODE_TYPE = VM_Storage_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-sn1-var-local
BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/dc1-sn1-rangedb-0
BLOCK_DEVICE_RANGEDB_01 = /dev/mapper/dc1-sn1-rangedb-1
BLOCK_DEVICE_RANGEDB_02 = /dev/mapper/dc1-sn1-rangedb-2
BLOCK_DEVICE_RANGEDB_03 = /dev/mapper/dc1-sn1-rangedb-3
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.3
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Example for Archive Node

Example file name: `/etc/storagegrid/nodes/dc1-arc1.conf`

Example file contents:

```
NODE_TYPE = VM_Archive_Node
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-arc1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.4
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Example for Gateway Node

Example file name: `/etc/storagegrid/nodes/dc1-gw1.conf`

Example file contents:

```
NODE_TYPE = VM_API_Gateway
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-gw1-var-local
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003
GRID_NETWORK_IP = 10.1.0.5
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Example for a non-primary Admin Node

Example file name: `/etc/storagegrid/nodes/dc1-adm2.conf`

Example file contents:

```
NODE_TYPE = VM_Admin_Node
ADMIN_ROLE = Non-Primary
ADMIN_IP = 10.1.0.2
BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/dc1-adm2-var-local
BLOCK_DEVICE_AUDIT_LOGS = /dev/mapper/dc1-adm2-audit-logs
BLOCK_DEVICE_TABLES = /dev/mapper/dc1-adm2-tables
GRID_NETWORK_TARGET = bond0.1001
ADMIN_NETWORK_TARGET = bond0.1002
CLIENT_NETWORK_TARGET = bond0.1003

GRID_NETWORK_IP = 10.1.0.6
GRID_NETWORK_MASK = 255.255.255.0
GRID_NETWORK_GATEWAY = 10.1.0.1
```

Validating the StorageGRID configuration

After creating configuration files in `/etc/storagegrid/nodes` for each of your StorageGRID nodes, you must validate the contents of those files.

To validate the contents of the configuration files, run the following command on each host:

```
sudo storagegrid node validate all
```

If the files are correct, the output shows **PASSED** for each configuration file, as shown in the example.

```
Checking for misnamed node configuration files… PASSED
Checking configuration file for node dc1-adm1… PASSED
Checking configuration file for node dc1-gw1… PASSED
Checking configuration file for node dc1-sn1… PASSED
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes… PASSED
```

> For an automated installation, you can suppress this output by using the `-q` or `--quiet` options in the `storagegrid` command (for example, `storagegrid --quiet…`). If you suppress the output, the command will have a non-zero exit value if any configuration warnings or errors were detected.

If the configuration files are incorrect, the issues are shown as **WARNING** and **ERROR**, as shown in the example. If any configuration errors are found, you must correct them before you continue with the installation.

```
Checking for misnamed node configuration files…
  WARNING: ignoring /etc/storagegrid/nodes/dc1-adm1
  WARNING: ignoring /etc/storagegrid/nodes/dc1-sn2.conf.keep
  WARNING: ignoring /etc/storagegrid/nodes/my-file.txt
Checking configuration file for node dc1-adm1…
  ERROR: NODE_TYPE = VM_Foo_Node
         VM_Foo_Node is not a valid node type.  See *.conf.sample
  ERROR: ADMIN_ROLE = Foo
         Foo is not a valid admin role.  See *.conf.sample
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-gw1-var-local
         /dev/mapper/sgws-gw1-var-local is not a valid block device
Checking configuration file for node dc1-gw1…
  ERROR: GRID_NETWORK_TARGET = bond0.1001
         bond0.1001 is not a valid interface.  See `ip link show`
  ERROR: GRID_NETWORK_IP = 10.1.3
         10.1.3 is not a valid IPv4 address
  ERROR: GRID_NETWORK_MASK = 255.248.255.0
         255.248.255.0 is not a valid IPv4 subnet mask
Checking configuration file for node dc1-sn1…
  ERROR: GRID_NETWORK_GATEWAY = 10.2.0.1
         10.2.0.1 is not on the local subnet
  ERROR: ADMIN_NETWORK_ESL = 192.168.100.0/21,172.16.0foo
         Could not parse subnet list
Checking configuration file for node dc1-sn2… PASSED
Checking configuration file for node dc1-sn3… PASSED
Checking for duplication of unique values between nodes…
  ERROR: GRID_NETWORK_IP = 10.1.0.4
         dc1-sn2 and dc1-sn3 have the same GRID_NETWORK_IP
  ERROR: BLOCK_DEVICE_VAR_LOCAL = /dev/mapper/sgws-sn2-var-local
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_VAR_LOCAL
  ERROR: BLOCK_DEVICE_RANGEDB_00 = /dev/mapper/sgws-sn2-rangedb-0
         dc1-sn2 and dc1-sn3 have the same BLOCK_DEVICE_RANGEDB_00
```

Starting the StorageGRID host service

To start your StorageGRID nodes, and ensure they restart after a host reboot, you must enable and start the StorageGRID host service.

Steps

1. Run the following commands on each host:

```
sudo systemctl enable storagegrid
sudo systemctl start storagegrid
```

2. Run the following command to ensure the deployment is proceeding:

```
sudo storagegrid node status node-name
```

For any node that returns a status of “Not Running” or “Stopped”, run the following command:

```
sudo storagegrid node start node-name
```

3. If you have previously enabled and started the StorageGRID host service (or if you are unsure if the service has been enabled and started), also run the following command:

```
sudo systemctl reload-or-restart storagegrid
```

Configuring the grid and completing installation

You complete installation by configuring the StorageGRID system from the Grid Manager on the primary Admin Node.

- Navigating to the Grid Manager
- Specifying the StorageGRID license information
- Adding sites
- Specifying Grid Network subnets
- Approving pending grid nodes
- Specifying Network Time Protocol server information
- Specifying Domain Name System server information
- Specifying the StorageGRID system passwords
- Reviewing your configuration and completing installation
- Post-installation guidelines

Navigating to the Grid Manager

You use the Grid Manager to define all of the information required to configure your StorageGRID system.

What you’ll need

The primary Admin Node must be deployed and have completed the initial startup sequence.

Steps

1. Open your web browser and navigate to one of the following addresses:

```
https://primary_admin_node_ip

client_network_ip
```

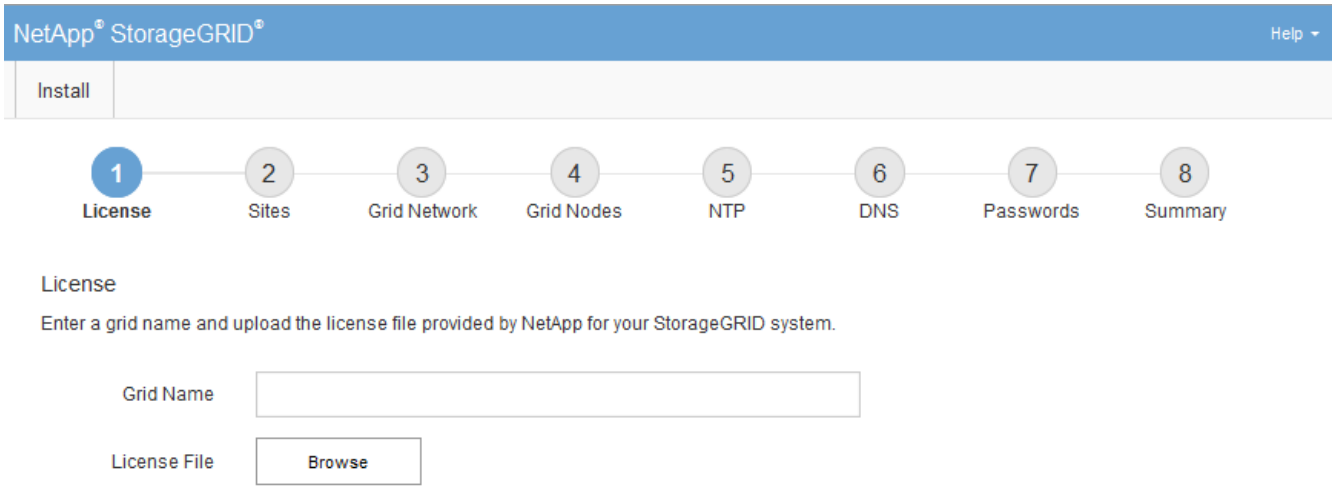
Alternatively, you can access the Grid Manager on port 8443:

```
https://primary_admin_node_ip:8443
```

> You can use the IP address for the primary Admin Node IP on the Grid Network or on the Admin Network, as appropriate for your network configuration.

1. Click **Install a StorageGRID system**.

   The page used to configure a StorageGRID grid appears.



Specifying the StorageGRID license information

You must specify the name for your StorageGRID system and upload the license file provided by NetApp.

Steps

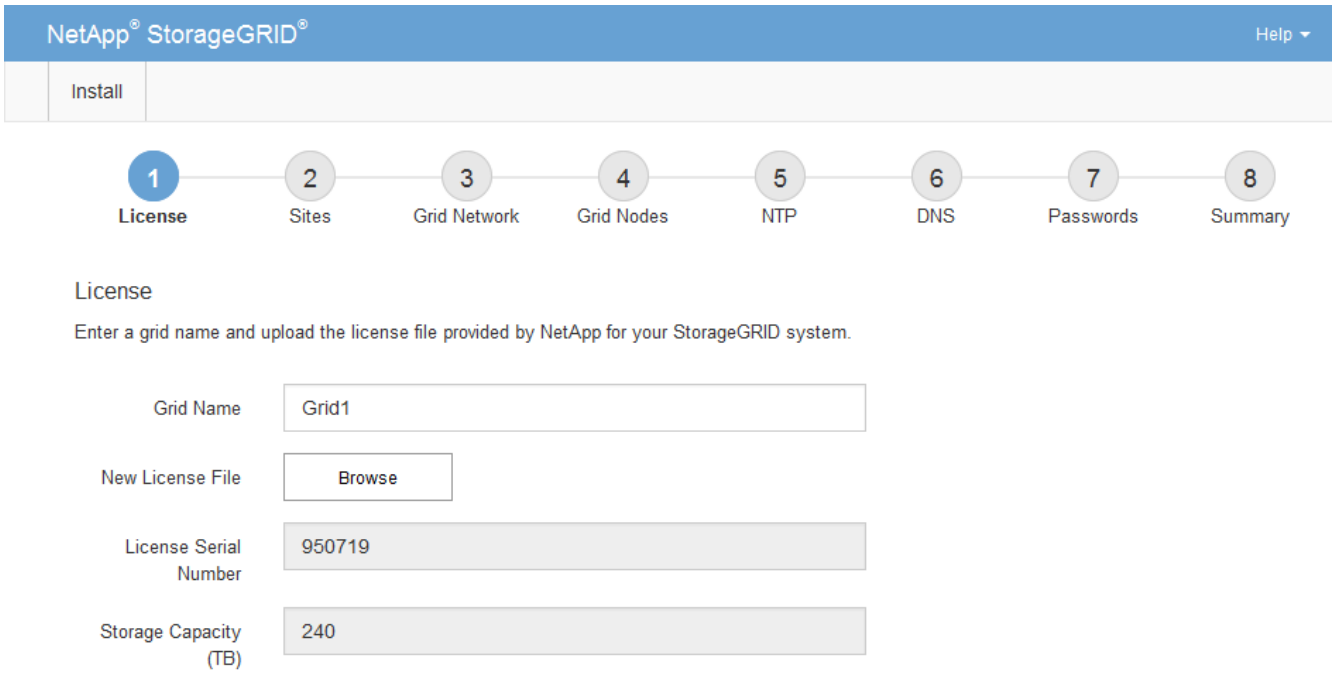
1. On the License page, enter a meaningful name for your StorageGRID system in **Grid Name**.

   After installation, the name is displayed at the top of the Nodes menu.

2. Click **Browse**, locate the NetApp License File (`NLFunique_id.txt`), and click **Open**.

   The license file is validated, and the serial number and licensed storage capacity are displayed.

   > The StorageGRID installation archive includes a free license that does not provide any support entitlement for the product. You can update to a license that offers support after installation.



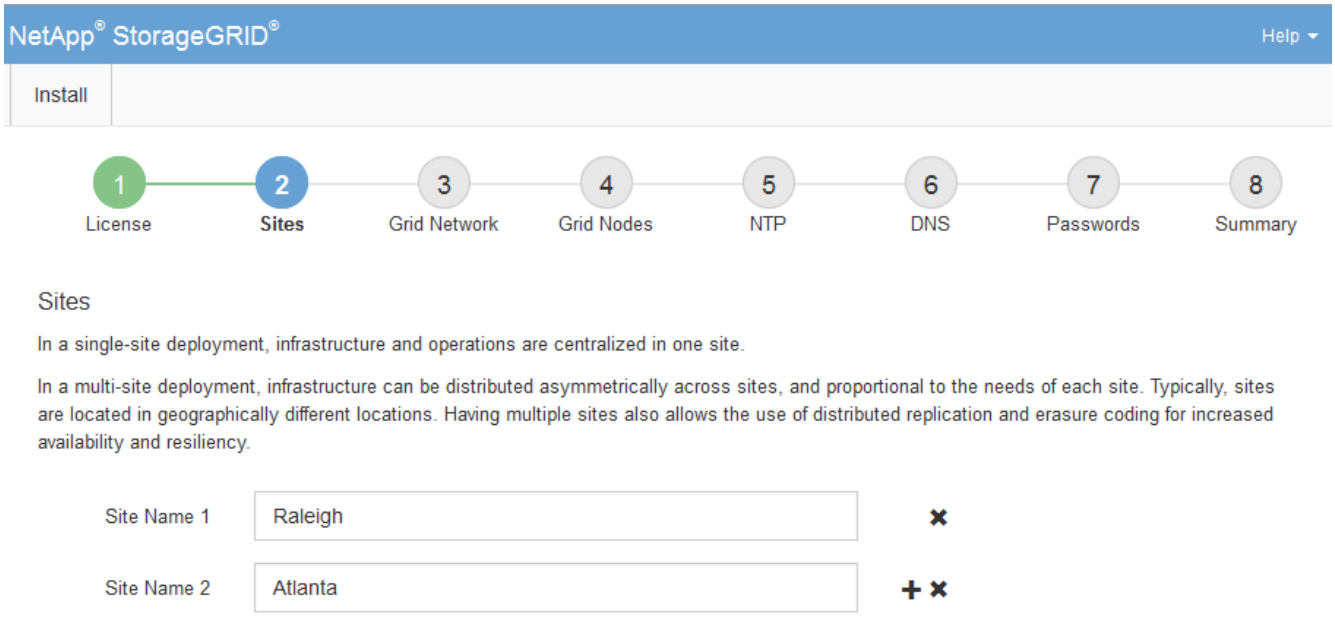
3. Click **Next**.

Adding sites

You must create at least one site when you are installing StorageGRID. You can create additional sites to increase the reliability and storage capacity of your StorageGRID system.

1. On the Sites page, enter the **Site Name**.
2. To add additional sites, click the plus sign next to the last site entry and enter the name in the new **Site Name** text box.

   Add as many additional sites as required for your grid topology. You can add up to 16 sites.



3. Click **Next**.

Specifying Grid Network subnets

You must specify the subnets that are used on the Grid Network.

About this task

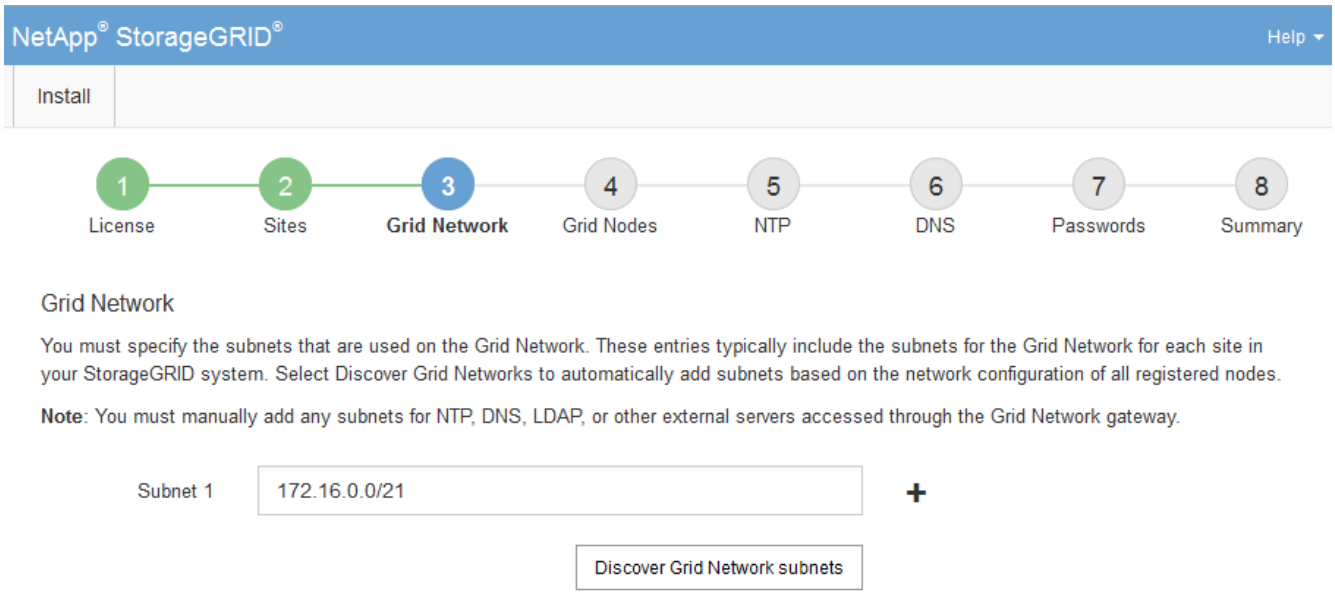
The subnet entries include the subnets for the Grid Network for each site in your StorageGRID system, along with any subnets that need to be reachable via the Grid Network.

If you have multiple grid subnets, the Grid Network gateway is required. All grid subnets specified must be reachable through this gateway.

Steps

1. Specify the CIDR network address for at least one Grid Network in the **Subnet 1** text box.
2. Click the plus sign next to the last entry to add an additional network entry.

   If you have already deployed at least one node, click **Discover Grid Networks Subnets** to automatically populate the Grid Network Subnet List with the subnets reported by grid nodes that have registered with the Grid Manager.



3. Click **Next**.

Approving pending grid nodes

You must approve each grid node before it can join the StorageGRID system.

What you'll need

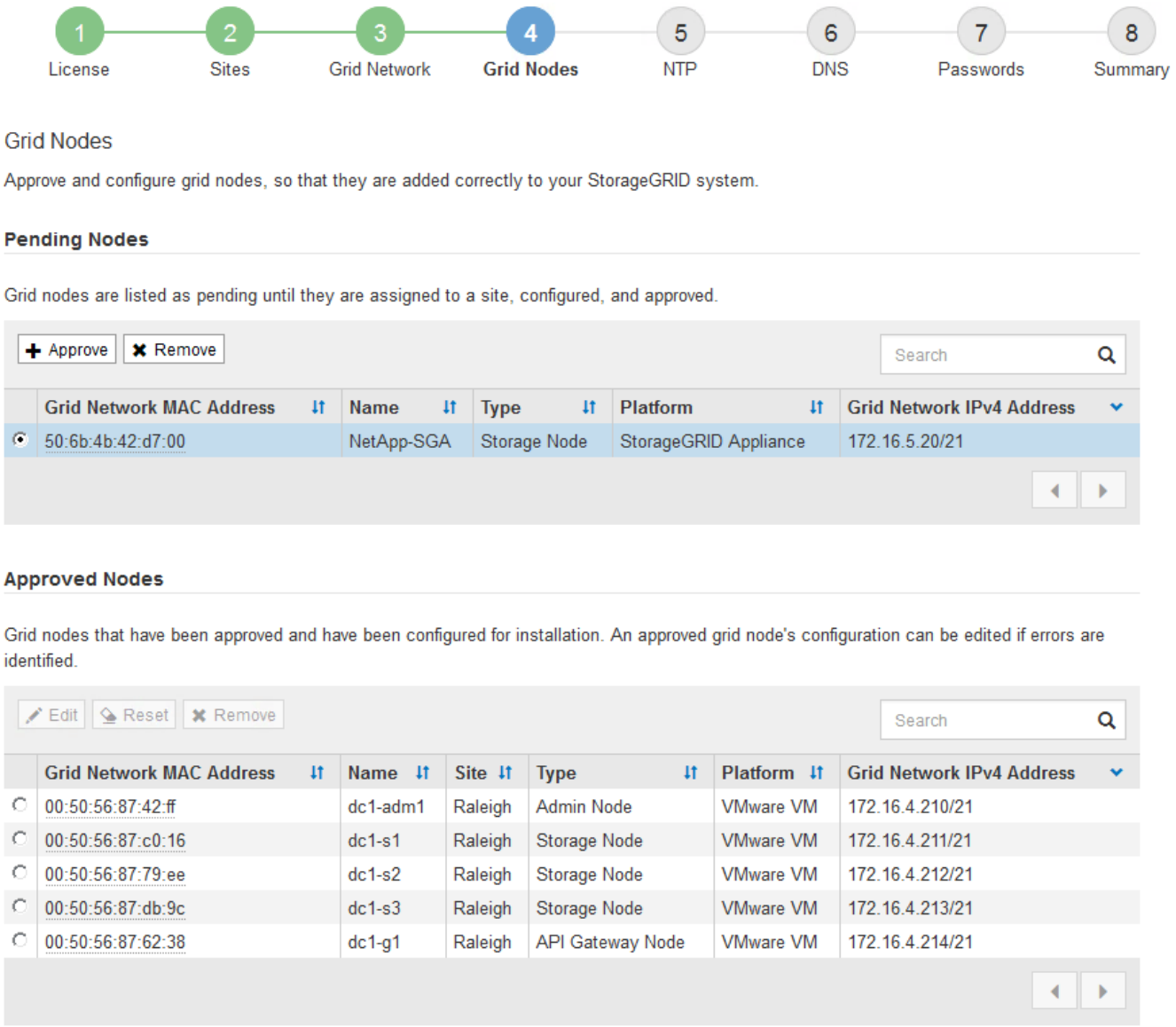
All virtual and StorageGRID appliance grid nodes must have been deployed.

Steps

1. Review the Pending Nodes list, and confirm that it shows all of the grid nodes you deployed.

   If a grid node is missing, confirm that it was deployed successfully.

2. Select the radio button next to a pending node you want to approve.



3. Click **Approve**.
4. In General Settings, modify settings for the following properties, as necessary:

Storage Node Configuration

General Settings

Site	Raleigh
Name	NetApp-SGA
NTP Role	Automatic
ADC Service	Automatic

Grid Network

Configuration	STATIC
IPv4 Address (CIDR)	172.16.5.20/21
Gateway	172.16.5.20

Admin Network

Configuration	STATIC
IPv4 Address (CIDR)	10.224.5.20/21
Gateway	10.224.0.1
Subnets (CIDR)	10.0.0.0/8
	172.19.0.0/16
	172.21.0.0/16

Client Network

Configuration	STATIC
IPv4 Address (CIDR)	47.47.5.20/21
Gateway	47.47.0.1

- **Site**: The name of the site with which this grid node will be associated.
- **Name**: The name that will be assigned to the node, and the name that will be displayed in the Grid Manager. The name defaults to the name you specified when you configured the node. During this step of the installation process, you can change the name as required.

> After you complete the installation, you cannot change the name of the node.

> For a VMware node, you can change the name here, but this action will not change the name of the virtual machine in vSphere.

- **NTP Role**: The Network Time Protocol (NTP) role of the grid node. The options are **Automatic**, **Primary**, and **Client**. Selecting **Automatic** assigns the Primary role to Admin Nodes, Storage Nodes with ADC services, Gateway Nodes, and any grid nodes that have non-static IP addresses. All other grid nodes are assigned the Client role.

  > Make sure that at least two nodes at each site can access at least four external NTP sources. If only one node at a site can reach the NTP sources, timing issues will occur if that node goes down. In addition, designating two nodes per site as primary NTP sources ensures accurate timing if a site is isolated from the rest of the grid.

- **ADC service** (Storage Nodes only): Select **Automatic** to let the system determine whether the node requires the Administrative Domain Controller (ADC) service. The ADC service keeps track of the location and availability of grid services. At least three Storage Nodes at each site must include the ADC service. You cannot add the ADC service to a node after it is deployed.

5. In Grid Network, modify settings for the following properties as necessary:

   - **IPv4 Address (CIDR)**: The CIDR network address for the Grid Network interface (eth0 inside the container). For example: 192.168.1.234/21
   - **Gateway**: The Grid Network gateway. For example: 192.168.0.1

     The gateway is required if there are multiple grid subnets.

   > If you selected DHCP for the Grid Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

6. If you want to configure the Admin Network for the grid node, add or update the settings in the Admin Network section as necessary.

   Enter the destination subnets of the routes out of this interface in the **Subnets (CIDR)** text box. If there are multiple Admin subnets, the Admin gateway is required.

   > If you selected DHCP for the Admin Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

   Appliances: For a StorageGRID appliance, if the Admin Network was not configured during the initial installation using the StorageGRID Appliance Installer, it cannot be configured in this Grid Manager dialog box. Instead, you must follow these steps:

   a. Reboot the appliance: In the Appliance Installer, select **Advanced** > **Reboot**.

      Rebooting can take several minutes.

   b. Select **Configure Networking** > **Link Configuration** and enable the appropriate networks.
   c. Select **Configure Networking** > **IP Configuration** and configure the enabled networks.
   d. Return to the Home page and click **Start Installation**.
   e. In the Grid Manager: If the node is listed in the Approved Nodes table, reset the node.
   f. Remove the node from the Pending Nodes table.
   g. Wait for the node to reappear in the Pending Nodes list.

h. Confirm that you can configure the appropriate networks. They should already be populated with the information you provided on the IP Configuration page.

   For additional information, see the installation and maintenance instructions for your appliance model.

7. If you want to configure the Client Network for the grid node, add or update the settings in the Client Network section as necessary. If the Client Network is configured, the gateway is required, and it becomes the default gateway for the node after installation.

   > If you selected DHCP for the Client Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

   Appliances: For a StorageGRID appliance, if the Client Network was not configured during the initial installation using the StorageGRID Appliance Installer, it cannot be configured in this Grid Manager dialog box. Instead, you must follow these steps:

   a. Reboot the appliance: In the Appliance Installer, select **Advanced** > **Reboot**.

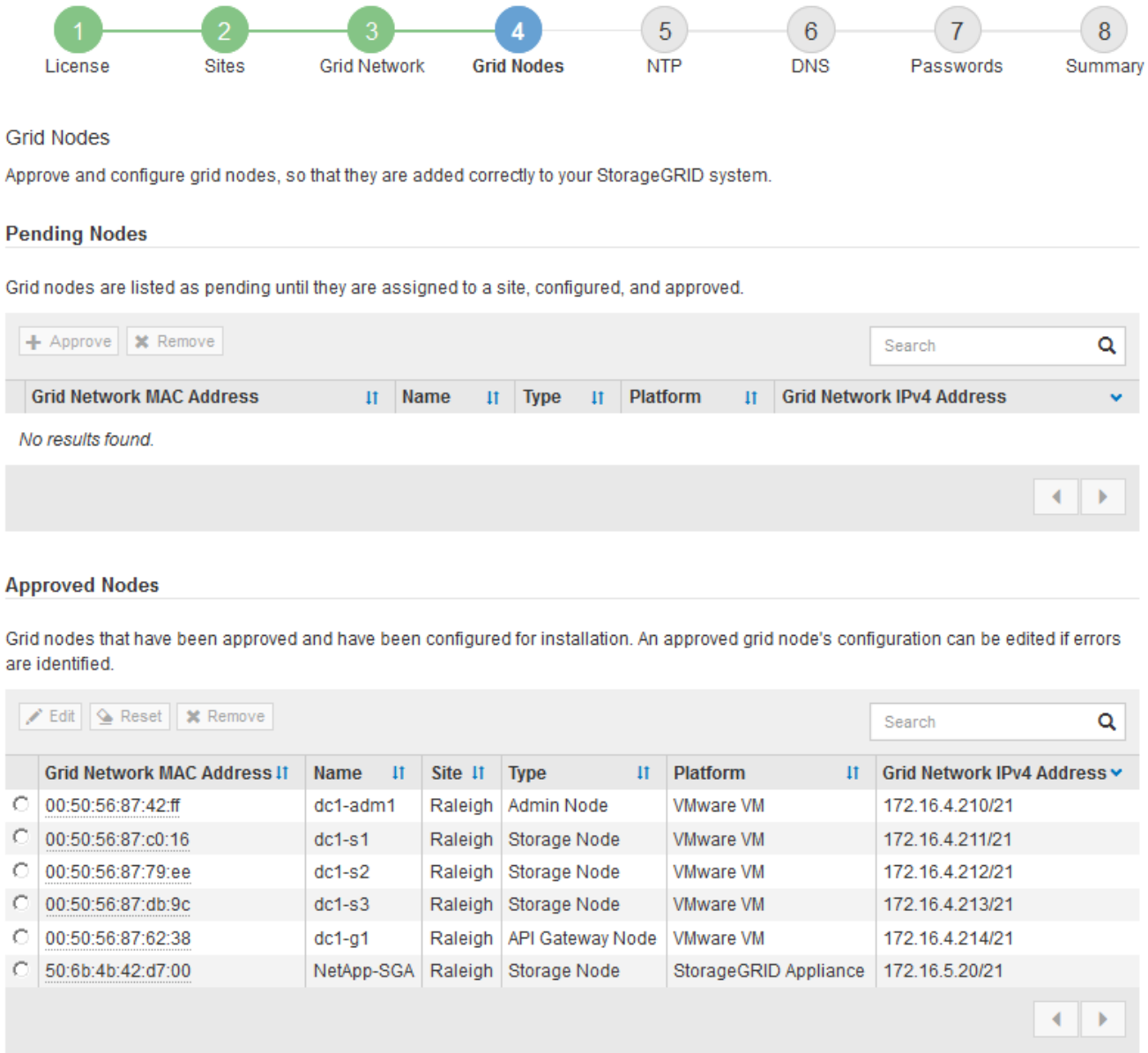
      Rebooting can take several minutes.

   b. Select **Configure Networking** > **Link Configuration** and enable the appropriate networks.
   c. Select **Configure Networking** > **IP Configuration** and configure the enabled networks.
   d. Return to the Home page and click **Start Installation**.
   e. In the Grid Manager: If the node is listed in the Approved Nodes table, reset the node.
   f. Remove the node from the Pending Nodes table.
   g. Wait for the node to reappear in the Pending Nodes list.
   h. Confirm that you can configure the appropriate networks. They should already be populated with the information you provided on the IP Configuration page.

      For additional information, see the installation and maintenance instructions for your appliance.

8. Click **Save**.

   The grid node entry moves to the Approved Nodes list.



9. Repeat these steps for each pending grid node you want to approve.

   You must approve all nodes that you want in the grid. However, you can return to this page at any time before you click **Install** on the Summary page. You can modify the properties of an approved grid node by selecting its radio button and clicking **Edit**.

10. When you are done approving grid nodes, click **Next**.

Specifying Network Time Protocol server information

You must specify the Network Time Protocol (NTP) configuration information for the StorageGRID system, so that operations performed on separate servers can be kept synchronized.

About this task

You must specify IPv4 addresses for the NTP servers.

You must specify external NTP servers. The specified NTP servers must use the NTP protocol.

You must specify four NTP server references of Stratum 3 or better to prevent issues with time drift.

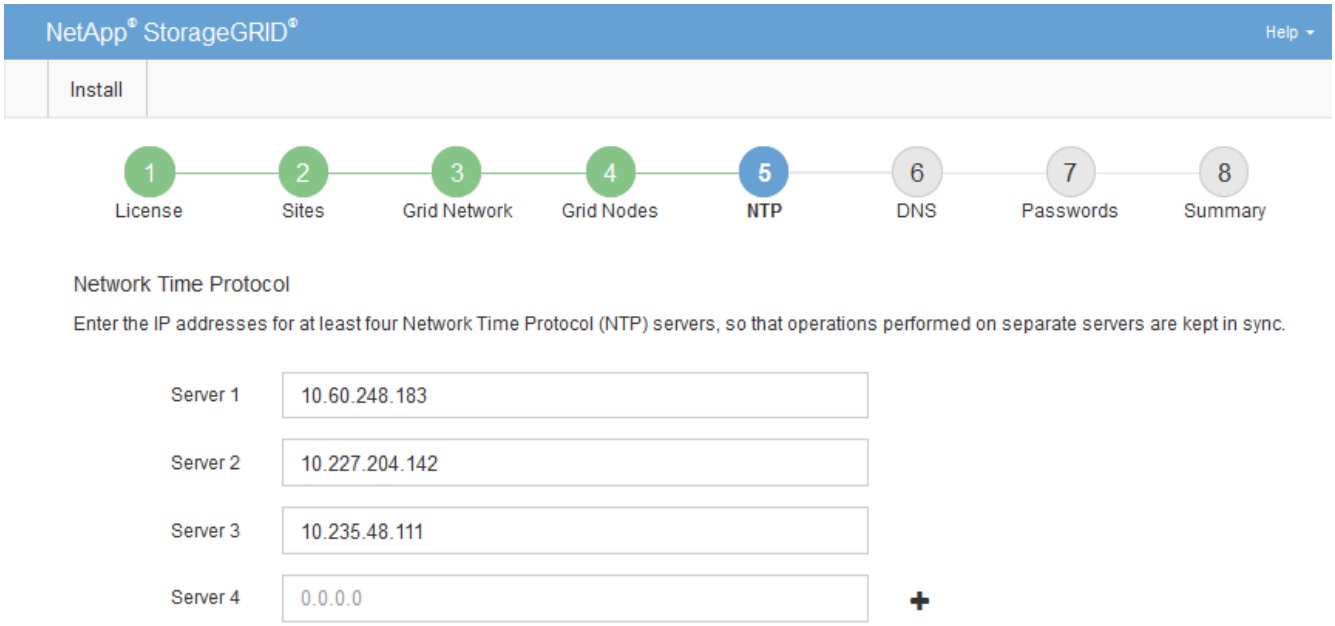
> When specifying the external NTP source for a production-level StorageGRID installation, do not use the Windows Time (W32Time) service on a version of Windows earlier than Windows Server 2016. The time service on earlier versions of Windows is not sufficiently accurate and is not supported by Microsoft for use in high-accuracy environments, such as StorageGRID.
>
> Support boundary to configure the Windows Time service for high-accuracy environments

The external NTP servers are used by the nodes to which you previously assigned Primary NTP roles.

> Make sure that at least two nodes at each site can access at least four external NTP sources. If only one node at a site can reach the NTP sources, timing issues will occur if that node goes down. In addition, designating two nodes per site as primary NTP sources ensures accurate timing if a site is isolated from the rest of the grid.

Steps

1. Specify the IPv4 addresses for at least four NTP servers in the **Server 1** to **Server 4** text boxes.
2. If necessary, select the plus sign next to the last entry to add additional server entries.



3. Select **Next**.

Related information

Network guidelines

Specifying Domain Name System server information

You must specify Domain Name System (DNS) information for your StorageGRID system, so that you can access external servers using hostnames instead of IP addresses.

About this task

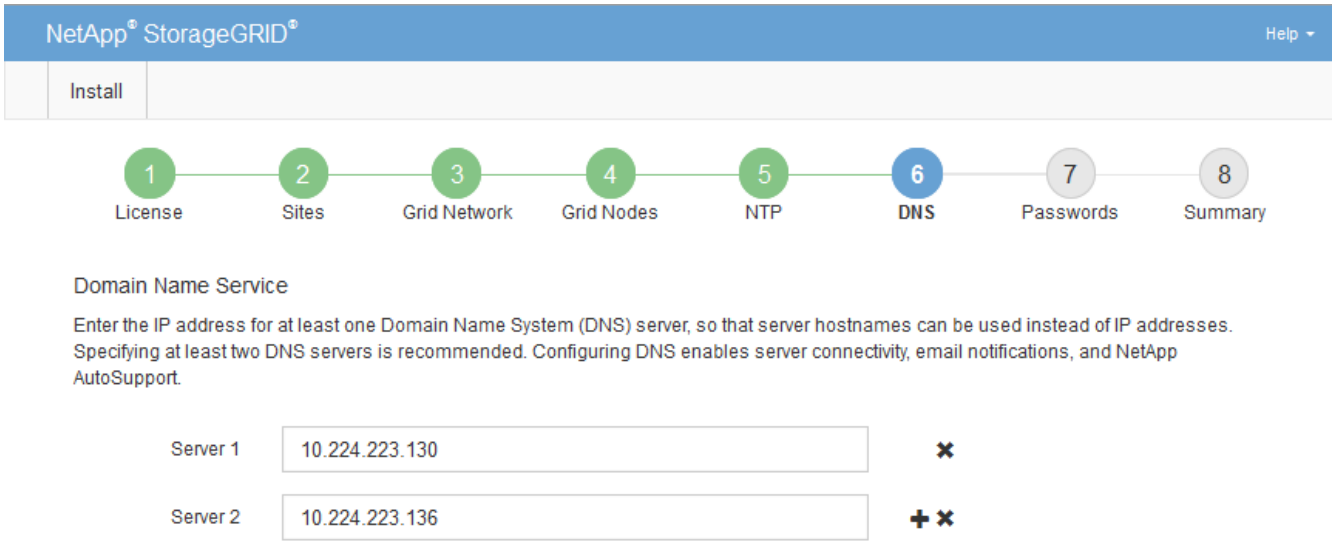
Specifying DNS server information allows you to use Fully Qualified Domain Name (FQDN) hostnames rather than IP addresses for email notifications and AutoSupport. Specifying at least two DNS servers is recommended.

> Provide two to six IPv4 addresses for DNS servers. You should select DNS servers that each site can access locally in the event of network islanding. This is to ensure an islanded site continues to have access to the DNS service. After configuring the grid-wide DNS server list, you can further customize the DNS server list for each node. For details, see the information about modifying the DNS configuration in the recovery and maintenance instructions.

If the DNS server information is omitted or incorrectly configured, a DNST alarm is triggered on each grid node's SSM service. The alarm clears when DNS is configured correctly and the new server information has reached all grid nodes.

Steps

1. Specify the IPv4 address for at least one DNS server in the **Server 1** text box.
2. If necessary, select the plus sign next to the last entry to add additional server entries.



   The best practice is to specify at least two DNS servers. You can specify up to six DNS servers.

3. Select **Next**.

Specifying the StorageGRID system passwords

As part of installing your StorageGRID system, you need to enter the passwords to use to secure your system and perform maintenance tasks.

About this task

Use the Install passwords page to specify the provisioning passphrase and the grid management root user password.

- The provisioning passphrase is used as an encryption key and is not stored by the StorageGRID system.
- You must have the provisioning passphrase for installation, expansion, and maintenance procedures, including downloading the recovery package. Therefore, it is important that you store the provisioning

passphrase in a secure location.

- You can change the provisioning passphrase from the Grid Manager if you have the current one.
- The grid management root user password may be changed using the Grid Manager.
- Randomly generated command line console and SSH passwords are stored in the Passwords.txt file in the recovery package.

Steps

1. In **Provisioning Passphrase**, enter the provisioning passphase that will be required to make changes to the grid topology of your StorageGRID system.

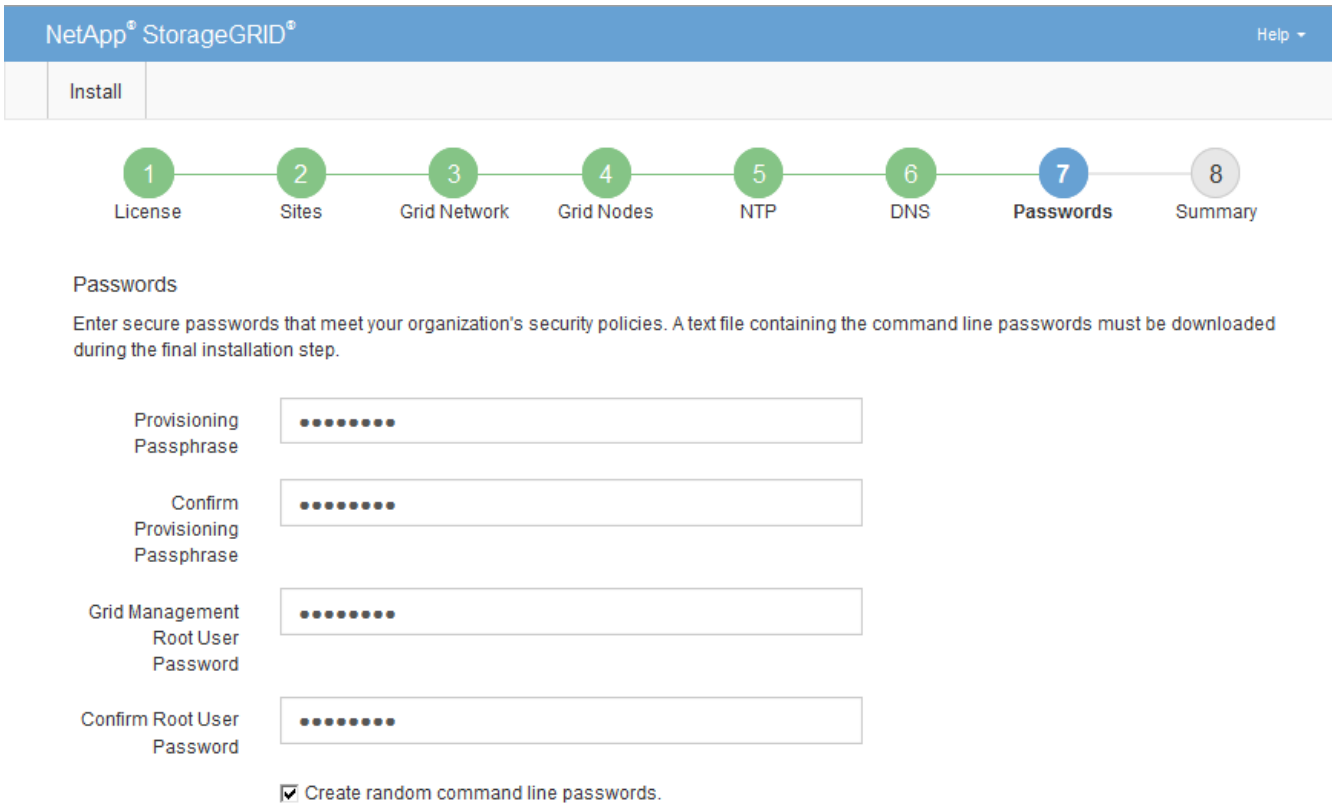
   Store the provisioning passphrase in a secure place.

   > If after the installation completes and you want to change the provisioning passphrase later, you can use the Grid Manager. Select **Configuration** > **Access Control** > **Grid Passwords**.

2. In **Confirm Provisioning Passphrase**, reenter the provisioning passphrase to confirm it.
3. In **Grid Management Root User Password**, enter the password to use to access the Grid Manager as the "root" user.

   Store the password in a secure place.

4. In **Confirm Root User Password**, reenter the Grid Manager password to confirm it.



5. If you are installing a grid for proof of concept or demo purposes, optionally deselect the **Create random command line passwords** check box.

   For production deployments, random passwords should always be used for security reasons. Deselect

Create random command line passwords only for demo grids if you want to use default passwords to access grid nodes from the command line using the “root” or “admin” account.

> You are prompted to download the Recovery Package file (`sgws-recovery-package-id-revision.zip`) after you click **Install** on the Summary page. You must download this file to complete the installation. The passwords required to access the system are stored in the Passwords.txt file, contained in the Recovery Package file.

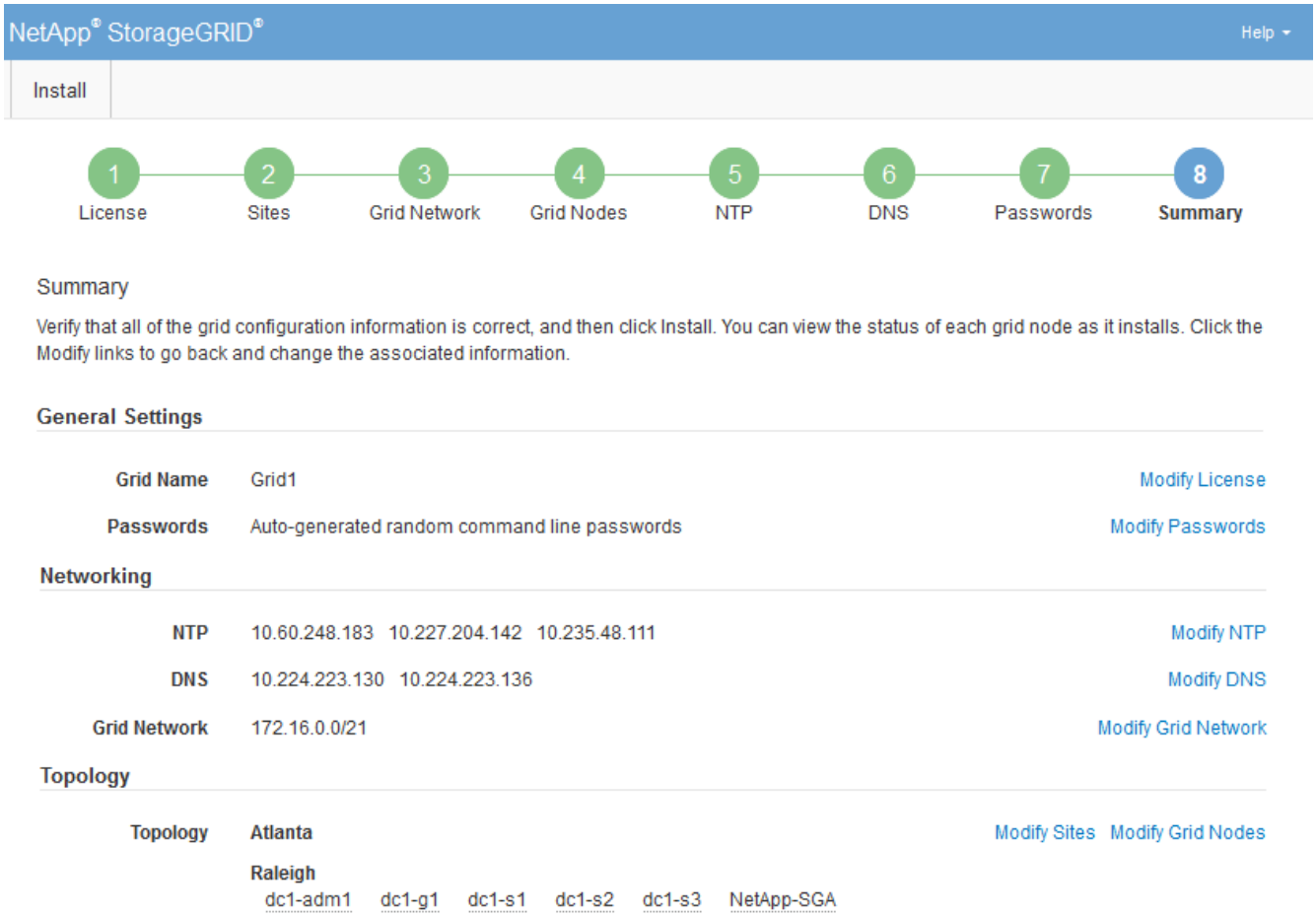
6. Click **Next**.

Reviewing your configuration and completing installation

You must carefully review the configuration information you have entered to ensure that the installation completes successfully.

Steps

1. View the **Summary** page.



2. Verify that all of the grid configuration information is correct. Use the Modify links on the Summary page to go back and correct any errors.
3. Click **Install**.

> If a node is configured to use the Client Network, the default gateway for that node switches from the Grid Network to the Client Network when you click **Install**. If you lose connectivity, you must ensure that you are accessing the primary Admin Node through an accessible subnet. See Networking guidelines for details.

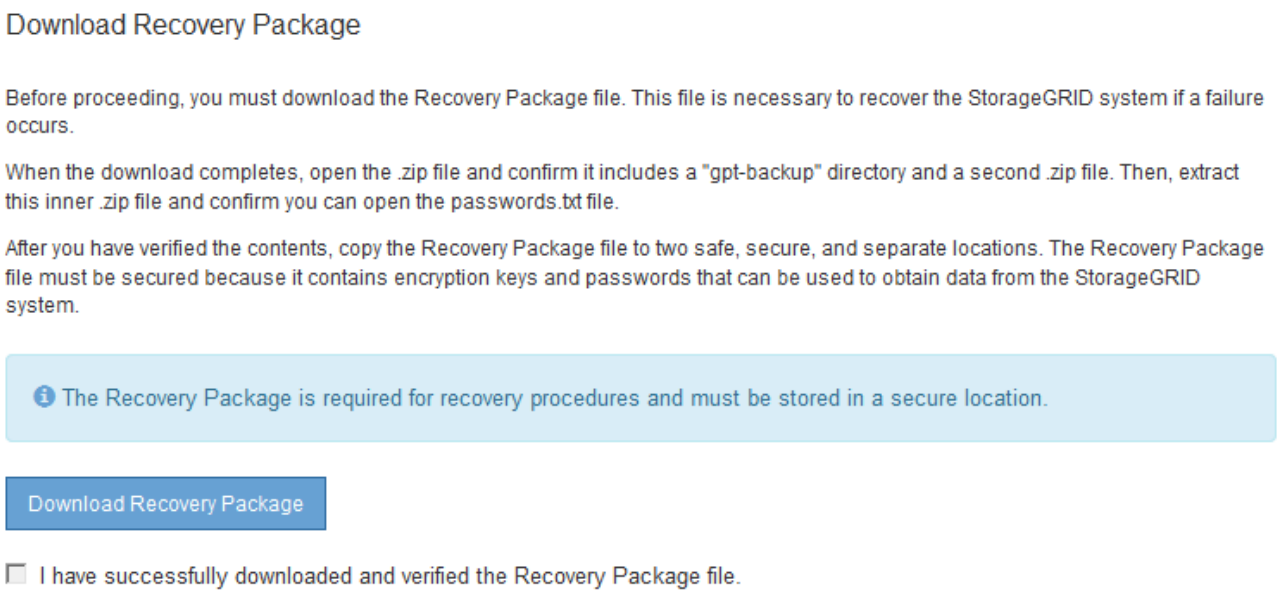
4. Click **Download Recovery Package**.

   When the installation progresses to the point where the grid topology is defined, you are prompted to download the Recovery Package file (`.zip`), and confirm that you can successfully access the contents of this file. You must download the Recovery Package file so that you can recover the StorageGRID system if one or more grid nodes fail. The installation continues in the background, but you cannot complete the installation and access the StorageGRID system until you download and verify this file.

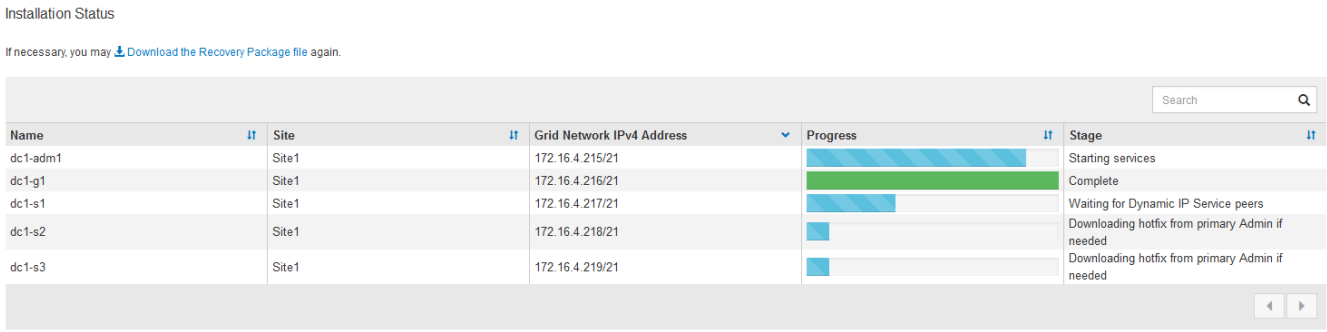
5. Verify that you can extract the contents of the `.zip` file, and then save it in two safe, secure, and separate locations.

   > The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

6. Select the **I have successfully downloaded and verified the Recovery Package file** check box, and click **Next**.



If the installation is still in progress, the status page appears. This page indicates the progress of the installation for each grid node.



When the Complete stage is reached for all grid nodes, the sign-in page for the Grid Manager appears.

7. Sign in to the Grid Manager using the "root" user and the password you specified during the installation.

Post-installation guidelines

After completing grid node deployment and configuration, follow these guidelines for DHCP addressing and network configuration changes.

- If DHCP was used to assign IP addresses, configure a DHCP reservation for each IP address on the networks being used.

  You can only set up DHCP during the deployment phase. You cannot set up DHCP during configuration.

  > Nodes reboot when their IP addresses change, which can cause outages if a DHCP address change affects multiple nodes at the same time.

- You must use the Change IP procedures if you want to change IP addresses, subnet masks, and default gateways for a grid node. See the information about configuring IP addresses in the recovery and maintenance instructions.
- If you make networking configuration changes, including routing and gateway changes, client connectivity to the primary Admin Node and other grid nodes might be lost. Depending on the networking changes applied, you might need to re-establish these connections.

Automating the installation

You can automate the installation of the StorageGRID host service, and the configuration of grid nodes.

About this task

Automating the deployment might be useful in any of the following cases:

- You already use a standard orchestration framework, such as Ansible, Puppet, or Chef, to deploy and configure physical or virtual hosts.
- You intend to deploy multiple StorageGRID instances.
- You are deploying a large, complex StorageGRID instance.

The StorageGRID host service is installed by a package and driven by configuration files that can be created interactively during a manual installation, or prepared ahead of time (or programmatically) to enable automated installation using standard orchestration frameworks. StorageGRID provides optional Python scripts for automating the configuration of StorageGRID appliances, and the whole StorageGRID system (the “grid”). You can use these scripts directly, or you can inspect them to learn how to use the StorageGRID Installation REST API in grid deployment and configuration tools you develop yourself.

Automating the installation and configuration of the StorageGRID host service

You can automate the installation of the StorageGRID host service using standard orchestration frameworks such as Ansible, Puppet, Chef, Fabric, or SaltStack.

The StorageGRID host service is packaged in a DEB and is driven by configuration files that can be prepared ahead of time (or programmatically) to enable automated installation. If you already use a standard

orchestration framework to install and configure Ubuntu or Debian, adding StorageGRID to your playbooks or recipes should be straightforward.

You can automate these tasks:

1. Installing Linux
2. Configuring Linux
3. Configuring host network interfaces to meet StorageGRID requirements
4. Configuring host storage to meet StorageGRID requirements
5. Installing Docker
6. Installing the StorageGRID host service
7. Creating StorageGRID node configuration files in `/etc/storagegrid/nodes`
8. Validating StorageGRID node configuration files
9. Starting the StorageGRID host service

Example Ansible role and playbook

Example Ansible role and playbook are supplied with the installation archive in the /extras folder. The Ansible playbook shows how the `storagegrid` role prepares the hosts and installs StorageGRID onto the target servers. You can customize the role or playbook as necessary.

Automating the configuration of StorageGRID

After deploying the grid nodes, you can automate the configuration of the StorageGRID system.

What you'll need

- You know the location of the following files from the installation archive.

Filename	Description
`configure-storagegrid.py`	Python script used to automate the configuration
`configure-storagegrid.sample.json`	Sample configuration file for use with the script
`configure-storagegrid.blank.json`	Blank configuration file for use with the script

- You have created a `configure-storagegrid.json` configuration file. To create this file, you can modify the sample configuration file (`configure-storagegrid.sample.json`) or the blank configuration file (`configure-storagegrid.blank.json`).

About this task

You can use the `configure-storagegrid.py` Python script and the `configure-storagegrid.json` configuration file to automate the configuration of your StorageGRID system.

> You can also configure the system using the Grid Manager or the Installation API.

Steps

1. Log in to the Linux machine you are using to run the Python script.
2. Change to the directory where you extracted the installation archive.

   For example:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   where `platform` is `debs`, `rpms`, or `vsphere`.

3. Run the Python script and use the configuration file you created.

   For example:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Result

A Recovery Package `.zip` file is generated during the configuration process, and it is downloaded to the directory where you are running the installation and configuration process. You must back up the Recovery Package file so that you can recover the StorageGRID system if one or more grid nodes fails. For example, copy it to a secure, backed up network location and to a secure cloud storage location.

> The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

If you specified that random passwords should be generated, you need to extract the `Passwords.txt` file and look for the passwords required to access your StorageGRID system.

```
######################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
######################################################################
```

Your StorageGRID system is installed and configured when a confirmation message is displayed.

```
StorageGRID has been configured and installed.
```

Related information

Configuring the grid and completing installation

Overview of the installation REST API

Overview of the installation REST API

StorageGRID provides the StorageGRID Installation API for performing installation tasks.

The API uses the Swagger open source API platform to provide the API documentation. Swagger allows both developers and non-developers to interact with the API in a user interface that illustrates how the API responds to parameters and options. This documentation assumes that you are familiar with standard web technologies and the JSON (JavaScript Object Notation) data format.

> Any API operations you perform using the API Docs webpage are live operations. Be careful not to create, update, or delete configuration data or other data by mistake.

Each REST API command includes the API's URL, an HTTP action, any required or optional URL parameters, and an expected API response.

StorageGRID Installation API

The StorageGRID Installation API is only available when you are initially configuring your StorageGRID system, and in the event that you need to perform a primary Admin Node recovery. The Installation API can be accessed over HTTPS from the Grid Manager.

To access the API documentation, go to the installation web page on the primary Admin Node and select **Help** > **API Documentation** from the menu bar.

The StorageGRID Installation API includes the following sections:

- **config** — Operations related to the product release and versions of the API. You can list the product release version and the major versions of the API supported by that release.
- **grid** — Grid-level configuration operations. You can get and update grid settings, including grid details, Grid Network subnets, grid passwords, and NTP and DNS server IP addresses.
- **nodes** — Node-level configuration operations. You can retrieve a list of grid nodes, delete a grid node, configure a grid node, view a grid node, and reset a grid node's configuration.
- **provision** — Provisioning operations. You can start the provisioning operation and view the status of the provisioning operation.
- **recovery** — Primary Admin Node recovery operations. You can reset information, upload the Recover Package, start the recovery, and view the status of the recovery operation.
- **recovery-package** — Operations to download the Recovery Package.
- **sites** — Site-level configuration operations. You can create, view, delete, and modify a site.

Related information

Automating the installation

Where to go next

After completing an installation, you must perform a series of integration and configuration steps. Some steps are required; others are optional.

Required tasks

- Create a tenant account for each client protocol (Swift or S3) that will be used to store objects on your

StorageGRID system.

- Control system access by configuring groups and user accounts. Optionally, you can configure a federated identity source (such as Active Directory or OpenLDAP), so you can import administration groups and users. Or, you can create local groups and users.
- Integrate and test the S3 or Swift API client applications you will use to upload objects to your StorageGRID system.
- When you are ready, configure the information lifecycle management (ILM) rules and ILM policy you want to use to protect object data.

> When you install StorageGRID, the default ILM policy, Baseline 2 Copies Policy, is active. This policy includes the stock ILM rule (Make 2 Copies), and it applies if no other policy has been activated.

- If your installation includes appliance Storage Nodes, use SANtricity software to complete the following tasks:
  - Connect to each StorageGRID appliance.
  - Verify receipt of AutoSupport data.
- If your StorageGRID system includes any Archive Nodes, configure the Archive Node's connection to the target external archival storage system.

> If any Archive Nodes will use Tivoli Storage Manager as the external archival storage system, you must also configure Tivoli Storage Manager.

- Review and follow the StorageGRID system hardening guidelines to eliminate security risks.
- Configure email notifications for system alerts.

Optional tasks

- If you want to receive notifications from the (legacy) alarm system, configure mailing lists and email notifications for alarms.
- Update grid node IP addresses if they have changed since you planned your deployment and generated the Recovery Package. See information about changing IP addresses in the recovery and maintenance instructions.
- Configure storage encryption, if required.
- Configure storage compression to reduce the size of stored objects, if required.
- Configure audit client access. You can configure access to the system for auditing purposes through an NFS or a CIFS file share. See the instructions for administering StorageGRID.

> Audit export through CIFS/Samba has been deprecated and will be removed in a future StorageGRID release.

Troubleshooting installation issues

If any problems occur while installing your StorageGRID system, you can access the installation log files. Technical support might also need to use the installation log files to resolve issues.

The following installation log files are available from the container that is running each node:

- `/var/local/log/install.log` (found on all grid nodes)
- `/var/local/log/gdu-server.log` (found on the primary Admin Node)

The following installation log files are available from the host:

- `/var/log/storagegrid/daemon.log`
- `/var/log/storagegrid/nodes/<node-name>.log`

To learn how to access the log files, see the instructions for monitoring and troubleshooting StorageGRID. For help troubleshooting appliance installation issues, see the installation and maintenance instructions for your appliances. If you need additional help, contact technical support.

Related information

Monitor & troubleshoot

SG100 & SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

NetApp Support

Example /etc/network/interfaces

The `/etc/network/interfaces` file includes three sections, which define the physical interfaces, bond interface, and VLAN interfaces. You can combine the three example sections into a single file, which will aggregate four Linux physical interfaces into a single LACP bond and then establish three VLAN interfaces subtending the bond for use as StorageGRID Grid, Admin, and Client Network interfaces.

Physical interfaces

Note that the switches at the other ends of the links must also treat the four ports as a single LACP trunk or port channel, and must pass at least the three referenced VLANs with tags.

```
# loopback interface
auto lo
iface lo inet loopback

# ens160 interface
auto ens160
iface ens160 inet manual
    bond-master bond0
    bond-primary en160

# ens192 interface
auto ens192
iface ens192 inet manual
    bond-master bond0

# ens224 interface
auto ens224
iface ens224 inet manual
    bond-master bond0

# ens256 interface
auto ens256
iface ens256 inet manual
    bond-master bond0
```

Bond interface

```
# bond0 interface
auto bond0
iface bond0 inet manual
    bond-mode 4
    bond-miimon 100
    bond-slaves ens160 ens192 end224 ens256
```

VLAN interfaces

```
# 1001 vlan
auto bond0.1001
iface bond0.1001 inet manual
vlan-raw-device bond0

# 1002 vlan
auto bond0.1002
iface bond0.1002 inet manual
vlan-raw-device bond0

# 1003 vlan
auto bond0.1003
iface bond0.1003 inet manual
vlan-raw-device bond0
```

Install VMware

Learn how to install StorageGRID in VMware deployments.

- Installation overview
- Planning and preparation
- Deploying virtual machine grid nodes in VMware vSphere Web Client
- Configuring the grid and completing installation
- Automating the installation
- Overview of the installation REST API
- Where to go next
- Troubleshooting installation issues

Installation overview

Installing a StorageGRID system in a VMware environment includes three primary steps.

1. **Preparation**: During planning and preparation, you perform the following tasks:
   - Learn about the hardware, software, virtual machine, storage, and performance requirements for StorageGRID.
   - Learn about the specifics of StorageGRID networking so you can configure your network appropriately. For more information, see the StorageGRID networking guidelines.
   - Identify and prepare the physical servers you plan to use to host your StorageGRID grid nodes.
   - On the servers you have prepared:
     - Install VMware vSphere Hypervisor
     - Configure the ESX hosts
     - Install and configure VMware vSphere and vCenter

2. **Deployment**: Deploy grid nodes using the VMware vSphere Web Client. When you deploy grid nodes, they are created as part of the StorageGRID system and connected to one or more networks.
   a. Use the VMware vSphere Web Client, a .vmdk file, and a set of .ovf file templates to deploy the software-based nodes as virtual machines (VMs) on the servers you prepared in step 1.
   b. Use the StorageGRID Appliance Installer to deploy StorageGRID appliance nodes.

> Hardware-specific installation and integration instructions are not included in the StorageGRID installation procedure. To learn how to install StorageGRID appliances, see the installation and maintenance instructions for your appliance.

3. **Configuration**: When all nodes have been deployed, use the StorageGRIDGrid Manager to configure the grid and complete the installation.

These instructions recommend a standard approach for deploying and configuring a StorageGRID system in a VMware environment. See also the information about the following alternative approaches:

- Use the deploy-vsphere-ovftool.sh Bash script (available from the installation archive) to deploy grid nodes in VMware vSphere.
- Automate the deployment and configuration of the StorageGRID system using a Python configuration script (provided in the installation archive).
- Automate the deployment and configuration of appliance grid nodes with a Python configuration script (available from the installation archive or from the StorageGRID Appliance Installer).
- If you are an advanced developer of StorageGRID deployments, use the installation REST APIs to automate the installation of StorageGRID grid nodes.

Related information

Planning and preparation

Deploying virtual machine grid nodes in VMware vSphere Web Client

Configuring the grid and completing installation

Automating the installation

Overview of the installation REST API

Network guidelines

Planning and preparation

Before deploying grid nodes and configuring the StorageGRID grid, you must be familiar with the steps and requirements for completing the procedure.

The StorageGRID deployment and configuration procedures assume that you are familiar with the architecture and operational functionality of the StorageGRID system.

You can deploy a single site or multiple sites at one time; however, all sites must meet the minimum requirement of having at least three Storage Nodes.

Before starting the node deployment and grid configuration procedure, you must:

- Plan the StorageGRID deployment.
- Install, connect, and configure all required hardware, including any StorageGRID appliances, to specifications.

> Hardware-specific installation and integration instructions are not included in the StorageGRID installation procedure. To learn how to install StorageGRID appliances, see the installation and maintenance instructions for your appliance.

- Understand the available network options and how each network option should be implemented on grid nodes. See the StorageGRID networking guidelines.
- Gather all networking information in advance. Unless you are using DHCP, gather the IP addresses to assign to each grid node, and the IP addresses of the domain name system (DNS) and network time protocol (NTP) servers that will be used.
- Decide which of the available deployment and configuration tools you want to use.

Related information

Network guidelines

SG100 & SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

Required materials

Before you install StorageGRID, you must gather and prepare required materials.

Item	Notes
NetApp StorageGRID license	You must have a valid, digitally signed NetApp license. **Note**: The StorageGRID installation archive includes a free license that does not provide any support entitlement for the product.
StorageGRID installation archive for VMware	You must download the StorageGRID installation archive and extract the files.
VMware software and documentation	During installation, you deploy virtual grid nodes on virtual machines in VMware vSphere Web Client.For supported versions, see the Interoperability Matrix.

Item	Notes
Service laptop	The StorageGRID system is installed through a service laptopThe service laptop must have: • Network port • SSH client (for example, PuTTY) • Supported web browser
StorageGRID documentation	• Release Notes • Instructions for administering StorageGRID

Related information

NetApp Interoperability Matrix Tool

Downloading and extracting the StorageGRID installation files

Web browser requirements

Administer StorageGRID

Release notes

Downloading and extracting the StorageGRID installation files

You must download the StorageGRID installation archives and extract the files.

Steps

1. Go to the NetApp Downloads page for StorageGRID.

   NetApp Downloads: StorageGRID

2. Select the button for downloading the latest release, or select another version from the drop-down menu and select **Go**.
3. Sign in with the username and password for your NetApp account.
4. If a Caution/MustRead statement appears, read it and select the check box.

   You must apply any required hotfixes after you install the StorageGRID release. For more information, see the hotfix procedure in the recovery and maintenance instructions.

5. Read the End User License Agreement, select the check box, and then select **Accept & Continue**.
6. In the **Install StorageGRID** column, select the appropriate software.

   Download the `.tgz` or `.zip` archive file for your platform.

   - `StorageGRID-Webscale-version-VMware-uniqueID.zip`
   - `StorageGRID-Webscale-version-VMware-uniqueID.tgz`

   Use the `.zip` file if you are running Windows on the service laptop.

7. Save and extract the archive file.
8. Choose the files you need from the following list.

   The files you need depend on your planned grid topology and how you will deploy your StorageGRID system.

> The paths listed in the table are relative to the top-level directory installed by the extracted installation archive.

Path and file name	Description
`./vsphere/README`	A text file that describes all of the files contained in the StorageGRID download file.
`./vsphere/NLF000000.txt`	A free license that does not provide any support entitlement for the product.
`./vsphere/NetApp-SG-version-SHA.vmdk`	The virtual machine disk file that is used as a template for creating grid node virtual machines.
`./vsphere/vsphere-primary-admin.ovf` `./vsphere/vsphere-primary-admin.mf`	The Open Virtualization Format template file (`.ovf`) and manifest file (`.mf`) for deploying the primary Admin Node.
`./vsphere/vsphere-non-primary-admin.ovf` `./vsphere/vsphere-non-primary-admin.mf`	The template file (`.ovf`) and manifest file (`.mf`) for deploying non-primary Admin Nodes.
`./vsphere/vsphere-archive.ovf` `./vsphere/vsphere-archive.mf`	The template file (`.ovf`) and manifest file (`.mf`) for deploying Archive Nodes.
`./vsphere/vsphere-gateway.ovf` `./vsphere/vsphere-gateway.mf`	The template file (`.ovf`) and manifest file (`.mf`) for deploying Gateway Nodes.
`./vsphere/vsphere-storage.ovf` `./vsphere/vsphere-storage.mf`	The template file (`.ovf`) and manifest file (`.mf`) for deploying virtual machine-based Storage Nodes.
Deployment scripting tool	**Description**
`./vsphere/deploy-vsphere-ovftool.sh`	A Bash shell script used to automate the deployment of virtual grid nodes.
`./vsphere/deploy-vsphere-ovftool-sample.ini`	A sample configuration file for use with the `deploy-vsphere-ovftool.sh` script.
`./vsphere/configure-storagegrid.py`	A Python script used to automate the configuration of a StorageGRID system.

Path and file name	Description
`./vsphere/configure-sga.py`	A Python script used to automate the configuration of StorageGRID appliances.
`./vsphere/storagegrid-ssoauth.py`	An example Python script that you can use to sign in to the Grid Management API when single sign-on is enabled.
`./vsphere/configure-storagegrid.sample.json`	A sample configuration file for use with the `configure-storagegrid.py` script.
`./vsphere/configure-storagegrid.blank.json`	A blank configuration file for use with the `configure-storagegrid.py` script.

Related information

Maintain & recover

Software requirements

You can use a virtual machine to host any type of StorageGRID grid node. One virtual machine is required for each grid node installed on the VMware server.

VMware vSphere Hypervisor

You must install VMware vSphere Hypervisor on a prepared physical server. The hardware must be configured correctly (including firmware versions and BIOS settings) before you install VMware software.

- Configure networking in the hypervisor as required to support networking for the StorageGRID system you are installing.

  Networking guidelines

- Ensure that the datastore is large enough for the virtual machines and virtual disks that are required to host the grid nodes.
- If you create more than one datastore, name each datastore so that you can easily identify which datastore to use for each grid node when you create virtual machines.

ESX host configuration requirements

> You must properly configure the network time protocol (NTP) on each ESX host. If the host time is incorrect, negative effects, including data loss, could occur.

VMware configuration requirements

You must install and configure VMware vSphere and vCenter before deploying StorageGRID grid nodes.

For supported versions of VMware vSphere Hypervisor and VMware vCenter Server software, see the Interoperability Matrix.

For the steps required to install these VMware products, see the VMware documentation.

Related information

NetApp Interoperability Matrix Tool

CPU and RAM requirements

Before installing StorageGRID software, verify and configure the hardware so that it is ready to support the StorageGRID system.

For information about supported servers, see the Interoperability Matrix.

Each StorageGRID node requires the following minimum resources:

- CPU cores: 8 per node
- RAM: At least 24 GB per node, and 2 to 16 GB less than the total system RAM, depending on the total RAM available and the amount of non-StorageGRID software running on the system

Ensure that the number of StorageGRID nodes you plan to run on each physical or virtual host does not exceed the number of CPU cores or the physical RAM available. If the hosts are not dedicated to running StorageGRID (not recommended), be sure to consider the resource requirements of the other applications.

> Monitor your CPU and memory usage regularly to ensure that these resources continue to accommodate your workload. For example, doubling the RAM and CPU allocation for virtual Storage Nodes would provide similar resources to those provided for StorageGRID appliance nodes. Additionally, if the amount of metadata per node exceeds 500 GB, consider increasing the RAM per node to 48 GB or more. For information about managing object metadata storage, increasing the Metadata Reserved Space setting, and monitoring CPU and memory usage, see the instructions for administering, monitoring, and upgrading StorageGRID.

If hyperthreading is enabled on the underlying physical hosts, you can provide 8 virtual cores (4 physical cores) per node. If hyperthreading is not enabled on the underlying physical hosts, you must provide 8 physical cores per node.

If you are using virtual machines as hosts and have control over the size and number of VMs, you should use a single VM for each StorageGRID node and size the VM accordingly.

For production deployments, you should not run multiple Storage Nodes on the same physical storage hardware or virtual host. Each Storage Node in a single StorageGRID deployment should be in its own isolated failure domain. You can maximize the durability and availability of object data if you ensure that a single hardware failure can only impact a single Storage Node.

See also the information about storage requirements.

Related information

NetApp Interoperability Matrix Tool

Storage and performance requirements

Administer StorageGRID

Monitor & troubleshoot

Upgrade software

Storage and performance requirements

You must understand the storage and performance requirements for StorageGRID nodes hosted by virtual machines, so you can provide enough space to support the initial configuration and future storage expansion.

Performance requirements

The performance of the OS volume and of the first storage volume significantly impacts the overall performance of the system. Ensure that these provide adequate disk performance in terms of latency, input/output operations per second (IOPS), and throughput.

All StorageGRID nodes require that the OS drive and all storage volumes have write-back caching enabled. The cache must be on a protected or persistent media.

Requirements for virtual machines that use NetApp AFF storage

If you are deploying a StorageGRID node as a virtual machine with storage assigned from a NetApp AFF system, you have confirmed that the volume does not have a FabricPool tiering policy enabled. For example, if a StorageGRID node is running as an virtual machine on a VMWare host, ensure the volume backing the datastore for the node does not have a FabricPool tiering policy enabled. Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.

> Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

Number of virtual machines required

Each StorageGRID site requires a minimum of three Storage Nodes.

> In a production deployment, do not run more than one Storage Node on a single virtual machine server. Using a dedicated virtual machine host for each Storage Node provides an isolated failure domain.

Other types of nodes, such as Admin Nodes or Gateway Nodes, can be deployed on the same virtual machine host, or they can be deployed on their own dedicated virtual machine hosts as required. However, if you have multiple nodes of the same type (two Gateway Nodes, for example), do not install all instances on the same virtual machine host.

Storage requirements by node type

In a production environment, the virtual machines for StorageGRID grid nodes must meet different requirements, depending on the types of nodes.

> Disk snapshots cannot be used to restore grid nodes. Instead, refer to the recovery and maintenance procedures for each type of node.

Node Type	Storage
Admin Node	100 GB LUN for OS 200 GB LUN for Admin Node tables 200 GB LUN for Admin Node audit log
Storage Node	100 GB LUN for OS 3 LUNs for each Storage Node on this host **Note**: A Storage Node can have 1 to 16 storage LUNs; at least 3 storage LUNs are recommended. Minimum size per LUN: 4 TB Maximum tested LUN size: 39 TB.
Gateway Node	100 GB LUN for OS
Archive Node	100 GB LUN for OS

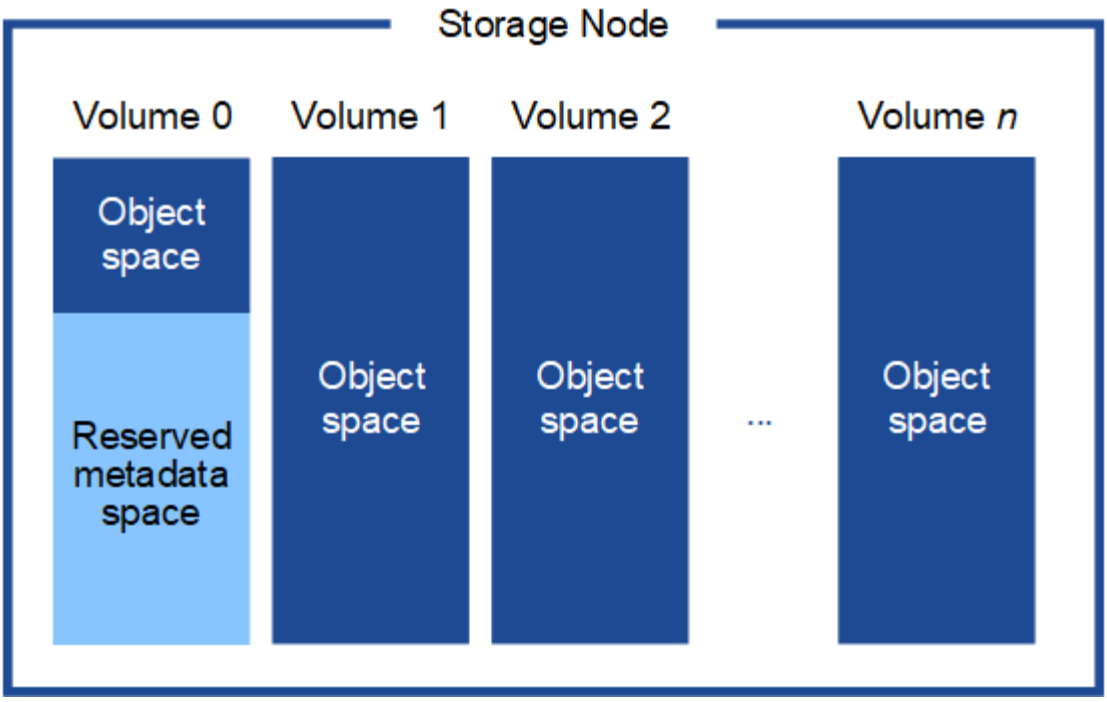
> Depending on the audit level configured, the size of user inputs such as S3 object key name, and how much audit log data you need to preserve, you might need to increase the size of the audit log LUN on each Admin Node. As a general rule, a grid generates approximately 1 KB of audit data per S3 operation, which would mean that a 200 GB LUN would support 70 million operations per day or 800 operations per second for two to three days.

Storage requirements for Storage Nodes

A software-based Storage Node can have 1 to 16 storage volumes—3 or more storage volumes are recommended. Each storage volume should be 4 TB or larger.

> An appliance Storage Node can have up to 48 storage volumes.

As shown in the figure, StorageGRID reserves space for object metadata on storage volume 0 of each Storage Node. Any remaining space on storage volume 0 and any other storage volumes in the Storage Node are used exclusively for object data.



To provide redundancy and to protect object metadata from loss, StorageGRID stores three copies of the metadata for all objects in the system at each site. The three copies of object metadata are evenly distributed across all Storage Nodes at each site.

When you assign space to volume 0 of a new Storage Node, you must ensure there is adequate space for that node's portion of all object metadata.

- At a minimum, you must assign at least 4 TB to volume 0.

> If you use only one storage volume for a Storage Node and you assign 4 TB or less to the volume, the Storage Node might enter the Storage Read-Only state on startup and store object metadata only.

- If you are installing a new StorageGRID 11.5 system and each Storage Node has 128 GB or more of RAM, you should assign 8 TB or more to volume 0. Using a larger value for volume 0 can increase the space allowed for metadata on each Storage Node.
- When configuring different Storage Nodes for a site, use the same setting for volume 0 if possible. If a site contains Storage Nodes of different sizes, the Storage Node with the smallest volume 0 will determine the metadata capacity of that site.

For details, go to the instructions for administering StorageGRID and search for "managing object metadata storage."

Administer StorageGRID

Related information

Maintain & recover

Web browser requirements

You must use a supported web browser.

Web browser	Minimum supported version
Google Chrome	87
Microsoft Edge	87
Mozilla Firefox	84

You should set the browser window to a recommended width.

Browser width	Pixels
Minimum	1024
Optimum	1280

Deploying virtual machine grid nodes in VMware vSphere Web Client

You use VMware vSphere Web Client to deploy each grid node as a virtual machine. During deployment, each grid node is created and connected to one or more networks. If you need to deploy any StorageGRID appliance Storage Nodes, see the installation and maintenance instructions for the appliance after you have deployed all virtual machine grid nodes.

- Collecting information about your deployment environment
- How grid nodes discover the primary Admin Node
- Deploying a StorageGRID node as a virtual machine

Related information

SG100 & SG1000 services appliances

SG5600 storage appliances

SG5700 storage appliances

SG6000 storage appliances

Collecting information about your deployment environment

Before deploying grid nodes, you must collect information about your network configuration and VMware environment.

VMware information

You must access the deployment environment and collect information about the VMware environment; the networks that were created for the Grid, Admin, and Client Networks; and the storage volume types you plan to use for Storage Nodes.

You must collect information about your VMware environment, including the following:

- The username and password for a VMware vSphere account that has appropriate permissions to complete the deployment.
- Host, datastore, and network configuration information for each StorageGRID grid node virtual machine.

> VMware live vMotion causes the virtual machine clock time to jump and is not supported for grid nodes of any type. Though rare, incorrect clock times can result in loss of data or configuration updates.

Grid Network information

You must collect information about the VMware network created for the StorageGRID Grid Network (required), including:

- The network name.
- If you are not using DHCP, the required networking details for each grid node (IP address, gateway, and network mask).
- If you are not using DHCP, the IP address of the primary Admin Node on the Grid Network. See “How grid nodes discover the primary Admin Node” for more information.

Admin Network information

For nodes that will be connected to the optional StorageGRID Admin Network, you must collect information about the VMware network created for this network, including:

- The network name.
- The method used to assign IP addresses, either static or DHCP.
- If you are using static IP addresses, the required networking details for each grid node (IP address, gateway, network mask).
- The external subnet list (ESL) for the Admin Network.

Client Network information

For nodes that will be connected to the optional StorageGRID Client Network, you must collect information about the VMware network created for this network, including:

- The network name.
- The method used to assign IP addresses, either static or DHCP.
- If you are using static IP addresses, the required networking details for each grid node (IP address, gateway, network mask).

Storage volumes for virtual Storage Nodes

You must collect the following information for virtual machine-based Storage Nodes:

- The number and size of storage volumes (storage LUNs) you plan to add. See “Storage and performance requirements.”

Grid configuration information

You must collect information to configure your grid:

- Grid license
- Network Time Protocol (NTP) server IP addresses
- Domain Name System (DNS) server IP addresses

Related information

How grid nodes discover the primary Admin Node

Storage and performance requirements

How grid nodes discover the primary Admin Node

Grid nodes communicate with the primary Admin Node for configuration and management. Each grid node must know the IP address of the primary Admin Node on the Grid Network.

To ensure that a grid node can access the primary Admin Node, you can do either of the following when deploying the node:

- You can use the ADMIN_IP parameter to enter the primary Admin Node's IP address manually.
- You can omit the ADMIN_IP parameter to have the grid node discover the value automatically. Automatic discovery is especially useful when the Grid Network uses DHCP to assign the IP address to the primary Admin Node.

Automatic discovery of the primary Admin Node is accomplished using a multicast Domain Name System (mDNS). When the primary Admin Node first starts up, it publishes its IP address using mDNS. Other nodes on the same subnet can then query for the IP address and acquire it automatically. However, because multicast IP traffic is not normally routable across subnets, nodes on other subnets cannot acquire the primary Admin Node's IP address directly.

> If you use automatic discovery:
>
> - You must include the ADMIN_IP setting for at least one grid node on any subnets that the primary Admin Node is not directly attached to. This grid node will then publish the primary Admin Node's IP address for other nodes on the subnet to discover with mDNS.
> - Ensure that your network infrastructure supports passing multi-cast IP traffic within a subnet.

Deploying a StorageGRID node as a virtual machine

You use VMware vSphere Web Client to deploy each grid node as a virtual machine. During deployment, each grid node is created and connected to one or more StorageGRID networks. Optionally, you can remap node ports or increase CPU or memory settings for the node before powering it on.

What you'll need

- You have reviewed the planning and preparation topics, and you understand the requirements for software, CPU and RAM, and storage and performance.

  Planning and preparation

- You are familiar with VMware vSphere Hypervisor and have experience deploying virtual machines in this

environment.

> The `open-vm-tools` package, an open-source implementation similar to VMware Tools, is included with the StorageGRID virtual machine. You do not need to install VMware Tools manually.

- You have downloaded and extracted the correct version of the StorageGRID installation archive for VMware.

> If you are deploying the new node as part of an expansion or recovery operation, you must use the version of StorageGRID that is currently running on the grid.

- You have the StorageGRID Virtual Machine Disk (`.vmdk`) file:

```
NetApp-<em>SG-version</em>-SHA.vmdk
```

- You have the `.ovf` and `.mf` files for each type of grid node you are deploying:

Filename	Description

`vsphere-primary-admin.ovf`
 	
`vsphere-primary-admin.mf`
	The template file and manifest file for the primary Admin Node.

`vsphere-non-primary-admin.ovf`
 	
`vsphere-non-primary-admin.mf`
	The template file and manifest file for a non-primary Admin Node.

`vsphere-archive.ovf`
 	
`vsphere-archive.mf`
	The template file and manifest file for an Archive Node.

`vsphere-gateway.ovf`
 	
`vsphere-gateway.mf`
	The template file and manifest file for a Gateway Node.

`vsphere-storage.ovf`
 	
`vsphere-storage.mf`
	The template file and manifest file for a Storage Node.

- The `.vdmk`, `.ovf`, and `.mf` files are all in the same directory.
- You have a plan to minimize failure domains. For example, you should not deploy all Gateway Nodes on a single virtual machine server.

> In a production deployment, do not run more than one Storage Node on a single virtual machine server. Using a dedicated virtual machine host for each Storage Node provides an isolated failure domain.

- If you are deploying a node as part of an expansion or recovery operation, you have the instructions for expanding a StorageGRID system or the recovery and maintenance instructions.
  - Expand your grid

    - Maintain & recover

- If you are deploying a StorageGRID node as a virtual machine with storage assigned from a NetApp AFF system, you have confirmed that the volume does not have a FabricPool tiering policy enabled. For example, if a StorageGRID node is running as an virtual machine on a VMWare host, ensure the volume backing the datastore for the node does not have a FabricPool tiering policy enabled. Disabling FabricPool tiering for volumes used with StorageGRID nodes simplifies troubleshooting and storage operations.

> Never use FabricPool to tier any data related to StorageGRID back to StorageGRID itself. Tiering StorageGRID data back to StorageGRID increases troubleshooting and operational complexity.

About this task

Follow these instructions to initially deploy VMware nodes, add a new VMware node in an expansion, or replace a VMware node as part of a recovery operation. Except as noted in the steps, the node deployment procedure is the same for all node types, including Admin Nodes, Storage Nodes, Gateway Nodes, and Archive Nodes.

If you are installing a new StorageGRID system:

- You must deploy the primary Admin Node before you deploy any other grid node.
- You must ensure that each virtual machine can connect to the primary Admin Node over the Grid Network.
- You must deploy all grid nodes before configuring the grid.

If you are performing an expansion or recovery operation:

- You must ensure that the new virtual machine can connect to the primary Admin Node over the Grid Network.

If you need to remap any of the node's ports, do not power on the new node until the port remap configuration is complete.

Steps

1. Using VCenter, deploy an OVF template.

   If you specify a URL, point to a folder containing the following files. Otherwise, select each of these files from a local directory.

   ```
   NetApp-<em>SG-version</em>-SHA.vmdk
   vsphere-<em>node</em>.ovf
   vsphere-<em>node</em>.mf
   ```

   For example, if this is the first node you are deploying, use these files to deploy the primary Admin Node for your StorageGRID system:

   ```
   NetApp-<em>SG-version</em>-SHA.vmdk
   sphere-primary-admin.ovf
   sphere-primary-admin.mf
   ```

2. Provide a name for the virtual machine.

   The standard practice is to use the same name for both the virtual machine and the grid node.

3. Place the virtual machine in the appropriate vApp or resource pool.
4. If you are deploying the primary Admin Node, read and accept the End User License Agreement.

   > Depending on your version of vCenter, the order of the steps will vary for accepting the End User License Agreement, specifying the name of the virtual machine, and selecting a datastore

5. Select storage for the virtual machine.

   > If you are deploying a node as part of recovery operation, perform the instructions in the storage recovery step to add new virtual disks, reattach virtual hard disks from the failed grid node, or both.

   When deploying a Storage Node, use 3 or more storage volumes, with each storage volume being 4 TB or larger. You must assign at least 4 TB to volume 0.

   > The Storage Node .ovf file defines several VMDKs for storage. Unless these VMDKs meet your storage requirements, you should remove them and assign appropriate VMDKs or RDMs for storage before powering up the node. VMDKs are more commonly used in VMware environments and are easier to manage, while RDMs may provide better performance for workloads that use larger object sizes (for example, greater than 100 MB).

6. Select networks.

   Determine which StorageGRID networks the node will use by selecting a destination network for each source network.

   - The Grid Network is required. You must select a destination network in the vSphere environment.
   - If you use the Admin Network, select a different destination network in the vSphere environment. If you do not use the Admin Network, select the same destination you selected for the Grid Network.
   - If you use the Client Network, select a different destination network in the vSphere environment. If you do not use the Client Network, select the same destination you selected for the Grid Network.

7. Under **Customize Template**, configure the required StorageGRID node properties.
   a. Enter the **Node name**.

      > If you are recovering a grid node, you must enter the name of the node you are recovering.

   b. In the **Grid Network (eth0)** section, select STATIC or DHCP for the **Grid network IP configuration**.
      - If you select STATIC, enter the **Grid network IP**, **Grid network mask**, **Grid network gateway**, and **Grid network MTU**.
      - If you select DHCP, the **Grid network IP**, **Grid network mask**, and **Grid network gateway** are automatically assigned.

   c. In the **Primary Admin IP** field, enter the IP address of the primary Admin Node for the Grid Network.

> This step does not apply if the node you are deploying is the primary Admin Node.

If you omit the primary Admin Node IP address, the IP address will be automatically discovered if the primary Admin Node, or at least one other grid node with ADMIN_IP configured, is present on the same subnet. However, it is recommended to set the primary Admin Node IP address here.

d. In the **Admin Network (eth1)** section, select STATIC, DHCP, or DISABLED for the **Admin network IP configuration**.
   - If you do not want to use the Admin Network, select DISABLED and enter **0.0.0.0** for the Admin Network IP. You can leave the other fields blank.
   - If you select STATIC, enter the **Admin network IP**, **Admin network mask**, **Admin network gateway**, and **Admin network MTU**.
   - If you select STATIC, enter the **Admin network external subnet list**. You must also configure a gateway.
   - If you select DHCP, the **Admin network IP**, **Admin network mask**, and **Admin network gateway** are automatically assigned.

e. In the **Client Network (eth2)** section, select STATIC, DHCP, or DISABLED for the **Client network IP configuration**.
   - If you do not want to use the Client Network, select DISABLED and enter **0.0.0.0** for the Client network IP. You can leave the other fields blank.
   - If you select STATIC, enter the **Client network IP**, **Client network mask**, **Client network gateway**, and **Client network MTU**.
   - If you select DHCP, the **Client network IP**, **Client network mask**, and **Client network gateway** are automatically assigned.

8. Review the virtual machine configuration and make any changes necessary.
9. When you are ready to complete, select **Finish** to start the upload of the virtual machine.
10. If you deployed this node as part of recovery operation and this is not a full-node recovery, perform these steps after deployment is complete:
    a. Right-click the virtual machine, and select **Edit Settings**.
    b. Select each default virtual hard disk that has been designated for storage, and select **Remove**.
    c. Depending on your data recovery circumstances, add new virtual disks according to your storage requirements, reattach any virtual hard disks preserved from the previously removed failed grid node, or both.

       Note the following important guidelines:

       - If you are adding new disks you should use the same type of storage device that was in use before node recovery.
       - The Storage Node .ovf file defines several VMDKs for storage. Unless these VMDKs meet your storage requirements, you should remove them and assign appropriate VMDKs or RDMs for storage before powering up the node. VMDKs are more commonly used in VMware environments and are easier to manage, while RDMs may provide better performance for workloads that use larger object sizes (for example, greater than 100 MB).
11. If you need to remap the ports used by this node, follow these steps.

    You might need to remap a port if your enterprise networking policies restrict access to one or more ports that are used by StorageGRID. See the networking guidelines for the ports used by StorageGRID.

> Do not remap the ports used in load balancer endpoints.

a. Select the new VM.

b. From the Configure tab, select **Settings** > **vApp Options**.

> The location of **vApp Options** depends on the version of vCenter.

c. In the **Properties** table, locate PORT_REMAP_INBOUND and PORT_REMAP.

d. To symmetrically map both inbound and outbound communications for a port, select **PORT_REMAP**.

> If only PORT_REMAP is set, the mapping that you specify applies to both inbound and outbound communications. If PORT_REMAP_INBOUND is also specified, PORT_REMAP applies only to outbound communications.

i. Scroll back to the top of the table, and select **Edit**.

ii. On the Type tab, select **User configurable**, and select **Save**.

iii. Select **Set Value**.

iv. Enter the port mapping:

```
<network type>/<protocol>/<default port used by grid node>/<new
port>
```

`<network type>` is grid, admin, or client, and `<protocol>` is tcp or udp.

For example, to remap ssh traffic from port 22 to port 3022, enter:

```
client/tcp/22/3022
```

v. Select **OK**.

e. To specify the port used for inbound communications to the node, select **PORT_REMAP_INBOUND**.

> If you specify PORT_REMAP_INBOUND and do not specify a value for PORT_REMAP, outbound communications for the port are unchanged.

i. Scroll back to the top of the table, and select **Edit**.

ii. On the Type tab, select **User configurable**, and select **Save**.

iii. Select **Set Value**.

iv. Enter the port mapping:

```
<network type>/<protocol>/<remapped inbound port>/<default inbound
port used by grid node>
```

`<network type>` is grid, admin, or client, and `<protocol>` is tcp or udp.

For example, to remap inbound SSH traffic that is sent to port 3022 so that it is received at port 22 by the grid node, enter the following:

```
client/tcp/3022/22
```

v. Select **OK**

12. If you want to increase the CPU or memory for the node from the default settings:
    a. Right-click the virtual machine, and select **Edit Settings**.
    b. Change the number of CPUs or the amount of memory as required.

       Set the **Memory Reservation** to the same size as the **Memory** allocated to the virtual machine.

    c. Select **OK**.
13. Power on the virtual machine.

After you finish

If you deployed this node as part of an expansion or recovery procedure, return to those instructions to complete the procedure.

Configuring the grid and completing installation

You complete installation by configuring the StorageGRID system from the Grid Manager on the primary Admin Node.

- Navigating to the Grid Manager
- Specifying the StorageGRID license information
- Adding sites
- Specifying Grid Network subnets
- Approving pending grid nodes
- Specifying Network Time Protocol server information
- Specifying Domain Name System server information
- Specifying the StorageGRID system passwords
- Reviewing your configuration and completing installation
- Post-installation guidelines

Navigating to the Grid Manager

You use the Grid Manager to define all of the information required to configure your

StorageGRID system.

What you'll need

The primary Admin Node must be deployed and have completed the initial startup sequence.

Steps

1. Open your web browser and navigate to one of the following addresses:

   `https://primary_admin_node_ip`

   `client_network_ip`

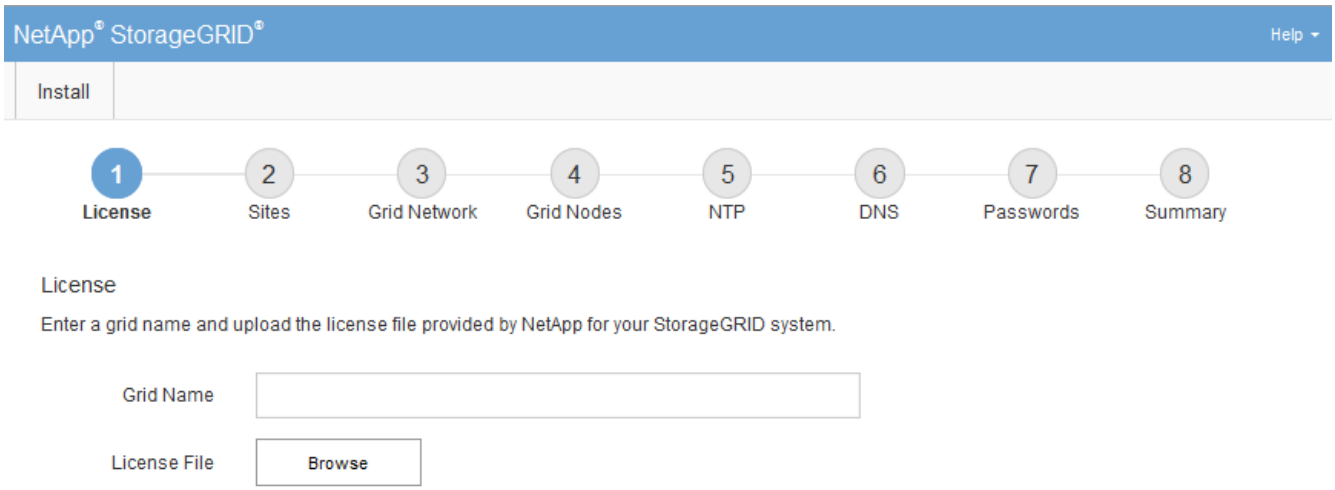
   Alternatively, you can access the Grid Manager on port 8443:

   `https://primary_admin_node_ip:8443`

   > You can use the IP address for the primary Admin Node IP on the Grid Network or on the Admin Network, as appropriate for your network configuration.

2. Click **Install a StorageGRID system**.

   The page used to configure a StorageGRID grid appears.



Specifying the StorageGRID license information

You must specify the name for your StorageGRID system and upload the license file provided by NetApp.

Steps

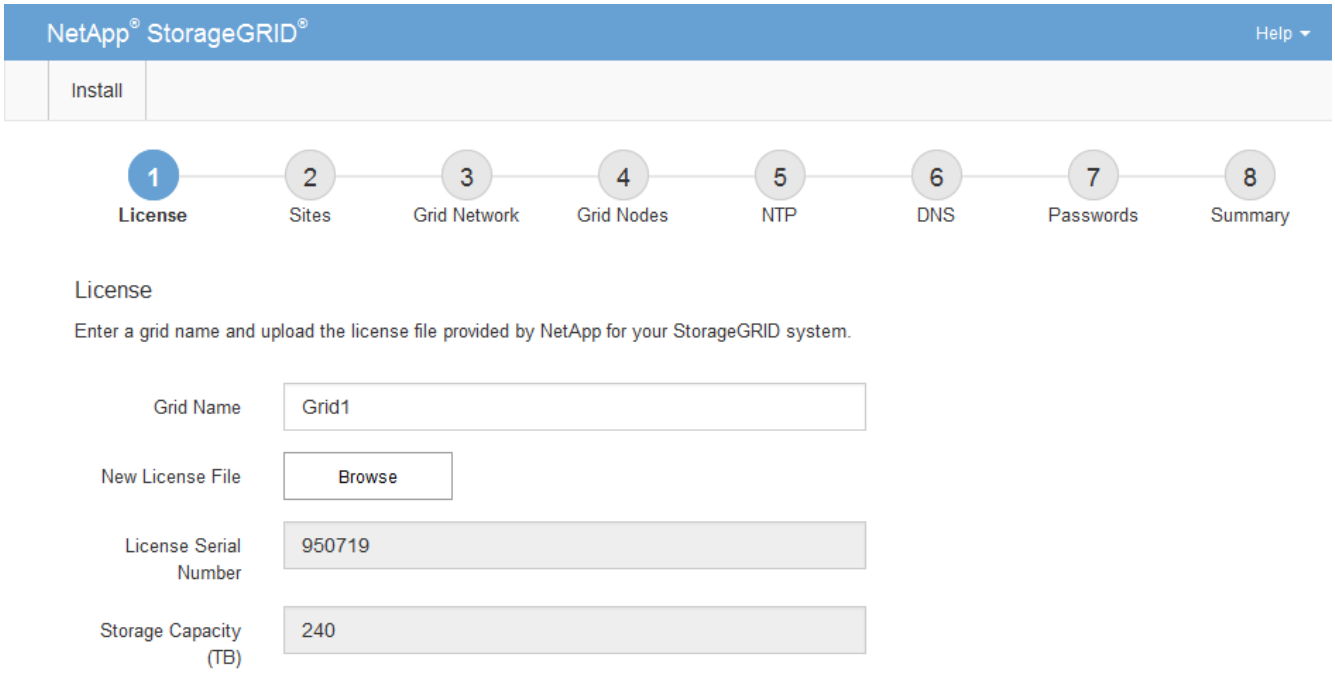
1. On the License page, enter a meaningful name for your StorageGRID system in **Grid Name**.

   After installation, the name is displayed at the top of the Nodes menu.

2. Click **Browse**, locate the NetApp License File (`NLFunique_id.txt`) and click **Open**.

   The license file is validated, and the serial number and licensed storage capacity are displayed.

The StorageGRID installation archive includes a free license that does not provide any support entitlement for the product. You can update to a license that offers support after installation.



3. Click **Next**.

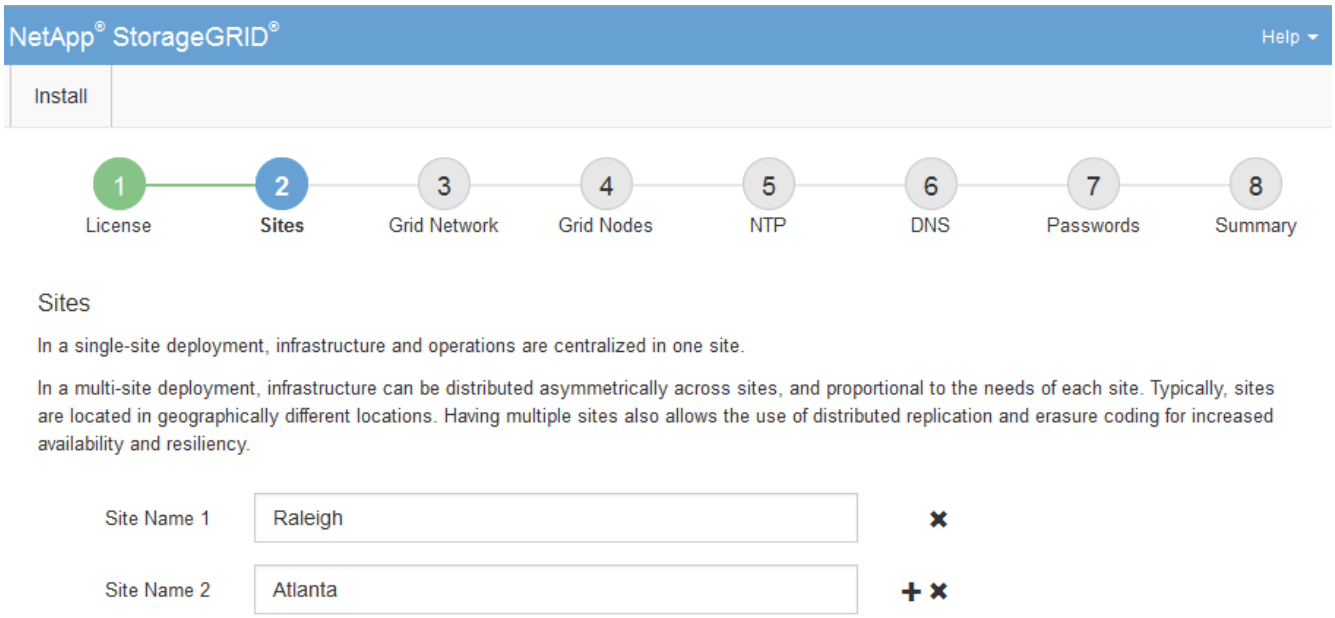
Adding sites

You must create at least one site when you are installing StorageGRID. You can create additional sites to increase the reliability and storage capacity of your StorageGRID system.

Steps

1. On the Sites page, enter the **Site Name**.
2. To add additional sites, click the plus sign next to the last site entry and enter the name in the new **Site Name** text box.

   Add as many additional sites as required for your grid topology. You can add up to 16 sites.



3. Click **Next**.

Specifying Grid Network subnets

You must specify the subnets that are used on the Grid Network.

About this task

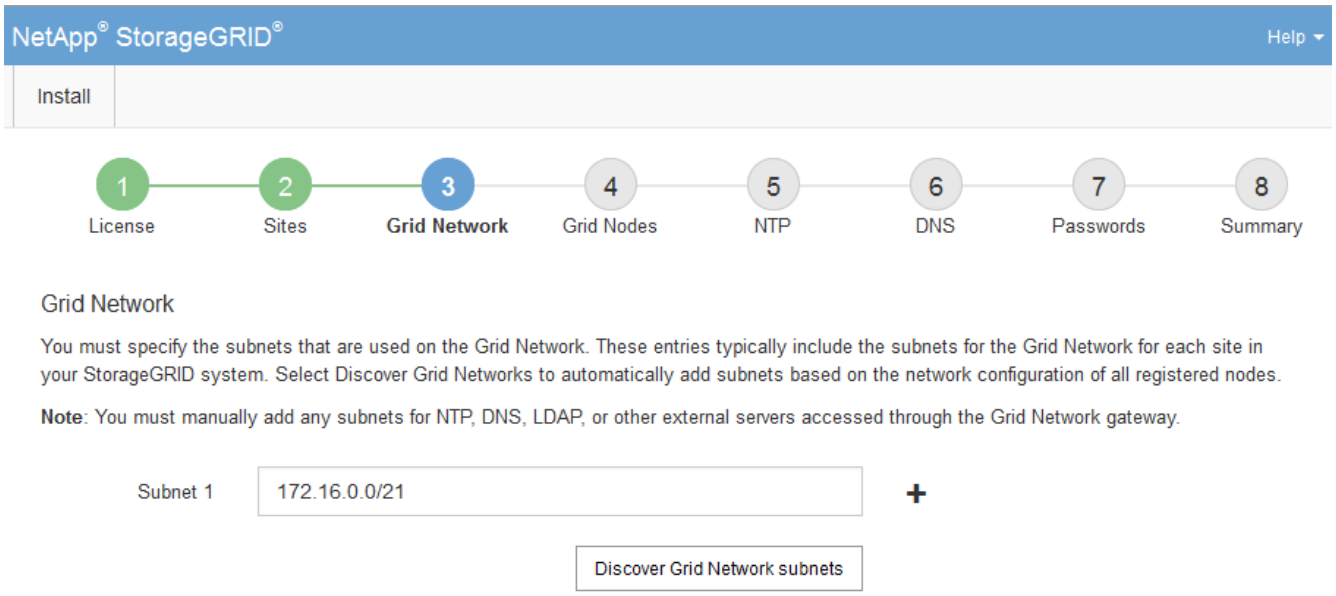
The subnet entries include the subnets for the Grid Network for each site in your StorageGRID system, along with any subnets that need to be reachable via the Grid Network.

If you have multiple grid subnets, the Grid Network gateway is required. All grid subnets specified must be reachable through this gateway.

Steps

1. Specify the CIDR network address for at least one Grid Network in the **Subnet 1** text box.
2. Click the plus sign next to the last entry to add an additional network entry.

   If you have already deployed at least one node, click **Discover Grid Networks Subnets** to automatically populate the Grid Network Subnet List with the subnets reported by grid nodes that have registered with the Grid Manager.



3. Click **Next**.

Approving pending grid nodes

You must approve each grid node before it can join the StorageGRID system.

What you'll need

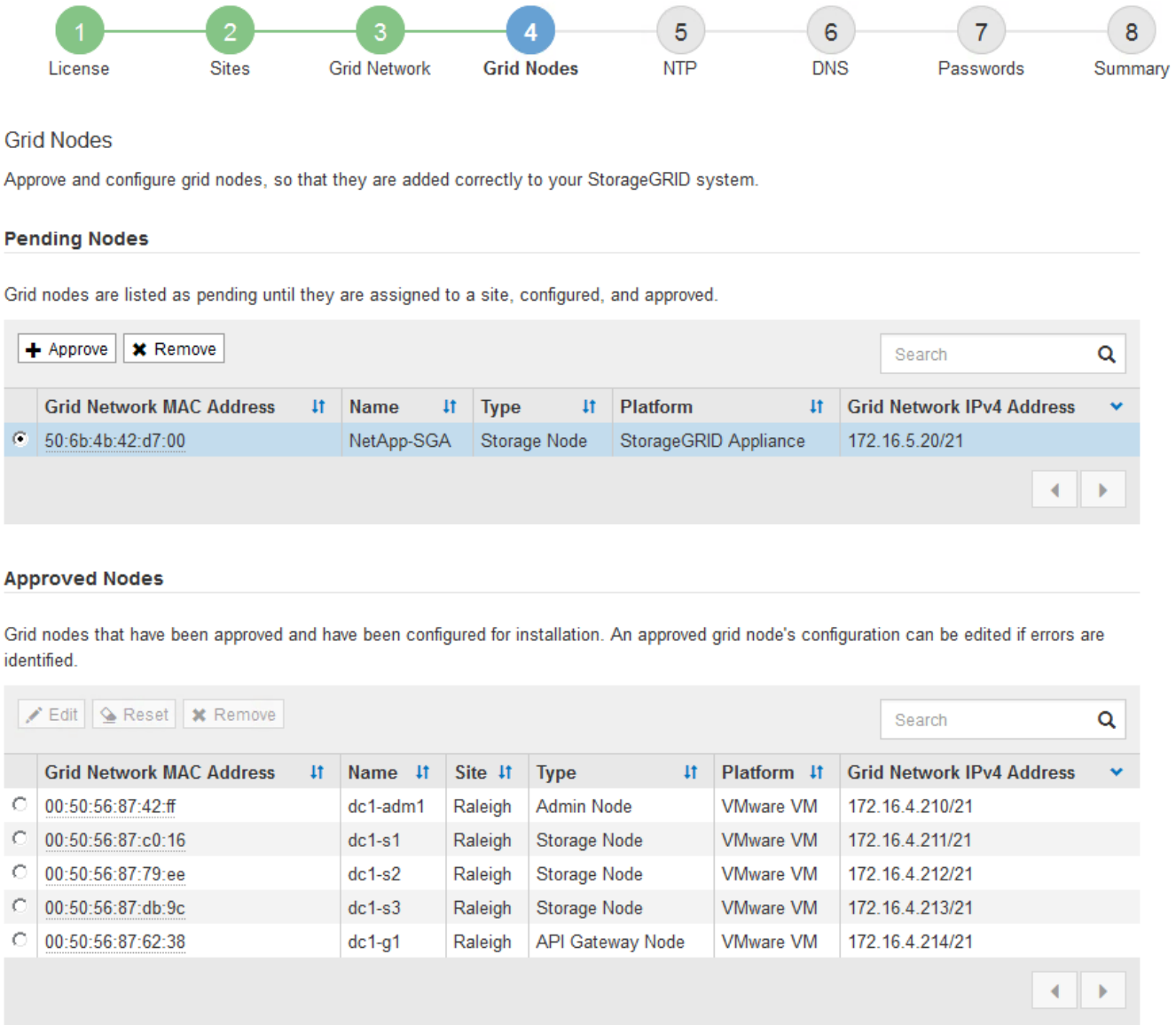
All virtual and StorageGRID appliance grid nodes must have been deployed.

Steps

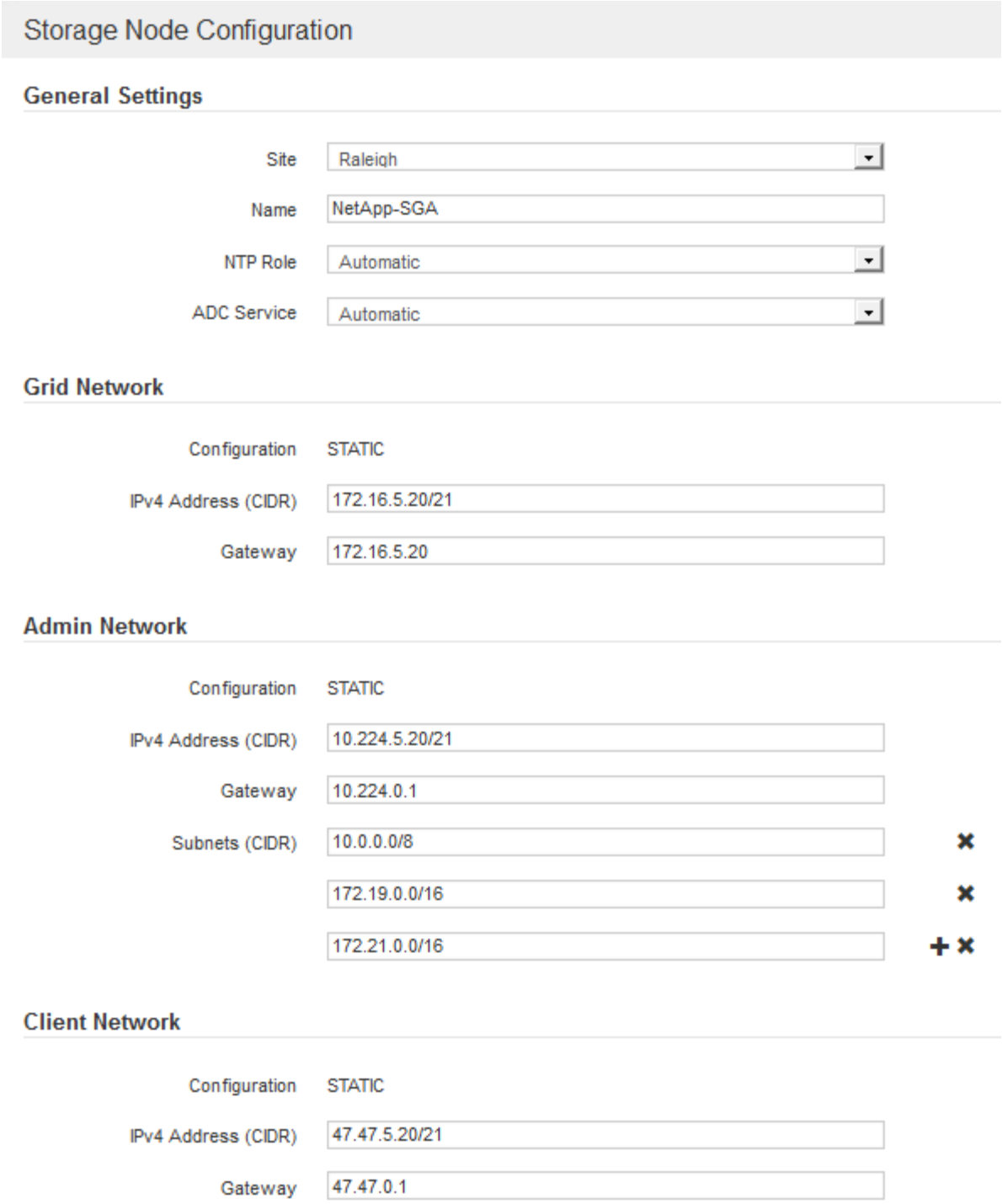
1. Review the Pending Nodes list, and confirm that it shows all of the grid nodes you deployed.

   > If a grid node is missing, confirm that it was deployed successfully.

2. Select the radio button next to a pending node you want to approve.



3. Click **Approve**.
4. In General Settings, modify settings for the following properties, as necessary:



- **Site**: The name of the site with which this grid node will be associated.
- **Name**: The name that will be assigned to the node, and the name that will be displayed in the Grid Manager. The name defaults to the name you specified when you configured the node. During this step of the installation process, you can change the name as required.

> After you complete the installation, you cannot change the name of the node.

> For a VMware node, you can change the name here, but this action will not change the name of the virtual machine in vSphere.

- **NTP Role**: The Network Time Protocol (NTP) role of the grid node. The options are **Automatic**, **Primary**, and **Client**. Selecting **Automatic** assigns the Primary role to Admin Nodes, Storage Nodes with ADC services, Gateway Nodes, and any grid nodes that have non-static IP addresses. All other grid nodes are assigned the Client role.

  > Make sure that at least two nodes at each site can access at least four external NTP sources. If only one node at a site can reach the NTP sources, timing issues will occur if that node goes down. In addition, designating two nodes per site as primary NTP sources ensures accurate timing if a site is isolated from the rest of the grid.

- **ADC service** (Storage Nodes only): Select **Automatic** to let the system determine whether the node requires the Administrative Domain Controller (ADC) service. The ADC service keeps track of the location and availability of grid services. At least three Storage Nodes at each site must include the ADC service. You cannot add the ADC service to a node after it is deployed.

5. In Grid Network, modify settings for the following properties as necessary:
   - **IPv4 Address (CIDR)**: The CIDR network address for the Grid Network interface (eth0 inside the container). For example: 192.168.1.234/21
   - **Gateway**: The Grid Network gateway. For example: 192.168.0.1

     > The gateway is required if there are multiple grid subnets.

     > If you selected DHCP for the Grid Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

6. If you want to configure the Admin Network for the grid node, add or update the settings in the Admin Network section as necessary.

   Enter the destination subnets of the routes out of this interface in the **Subnets (CIDR)** text box. If there are multiple Admin subnets, the Admin gateway is required.

   > If you selected DHCP for the Admin Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

   Appliances: For a StorageGRID appliance, if the Admin Network was not configured during the initial installation using the StorageGRID Appliance Installer, it cannot be configured in this Grid Manager dialog box. Instead, you must follow these steps:

   a. Reboot the appliance: In the Appliance Installer, select **Advanced** > **Reboot**.

      Rebooting can take several minutes.

   b. Select **Configure Networking** > **Link Configuration** and enable the appropriate networks.
   c. Select **Configure Networking** > **IP Configuration** and configure the enabled networks.
   d. Return to the Home page and click **Start Installation**.
   e. In the Grid Manager: If the node is listed in the Approved Nodes table, reset the node.
   f. Remove the node from the Pending Nodes table.
   g. Wait for the node to reappear in the Pending Nodes list.

h. Confirm that you can configure the appropriate networks. They should already be populated with the information you provided on the IP Configuration page.

   For additional information, see the installation and maintenance instructions for your appliance model.

7. If you want to configure the Client Network for the grid node, add or update the settings in the Client Network section as necessary. If the Client Network is configured, the gateway is required, and it becomes the default gateway for the node after installation.

   > If you selected DHCP for the Client Network configuration and you change the value here, the new value will be configured as a static address on the node. You must make sure the resulting IP address is not within a DHCP address pool.

   Appliances: For a StorageGRID appliance, if the Client Network was not configured during the initial installation using the StorageGRID Appliance Installer, it cannot be configured in this Grid Manager dialog box. Instead, you must follow these steps:

   a. Reboot the appliance: In the Appliance Installer, select **Advanced** > **Reboot**.

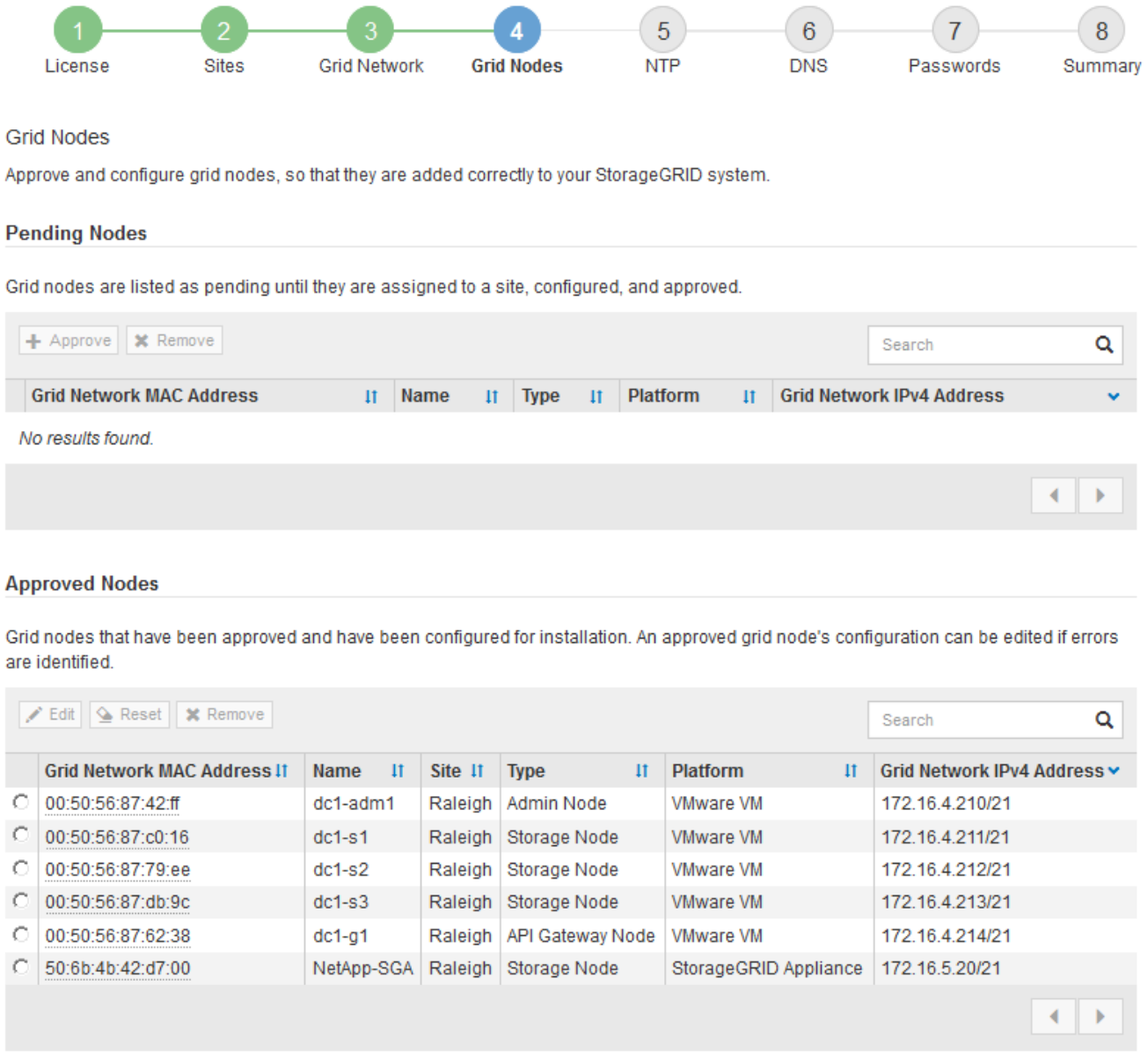
      Rebooting can take several minutes.

   b. Select **Configure Networking** > **Link Configuration** and enable the appropriate networks.
   c. Select **Configure Networking** > **IP Configuration** and configure the enabled networks.
   d. Return to the Home page and click **Start Installation**.
   e. In the Grid Manager: If the node is listed in the Approved Nodes table, reset the node.
   f. Remove the node from the Pending Nodes table.
   g. Wait for the node to reappear in the Pending Nodes list.
   h. Confirm that you can configure the appropriate networks. They should already be populated with the information you provided on the IP Configuration page.

      For additional information, see the installation and maintenance instructions for your appliance.

8. Click **Save**.

   The grid node entry moves to the Approved Nodes list.



9. Repeat these steps for each pending grid node you want to approve.

   You must approve all nodes that you want in the grid. However, you can return to this page at any time before you click **Install** on the Summary page. You can modify the properties of an approved grid node by selecting its radio button and clicking **Edit**.

10. When you are done approving grid nodes, click **Next**.

Specifying Network Time Protocol server information

You must specify the Network Time Protocol (NTP) configuration information for the StorageGRID system, so that operations performed on separate servers can be kept synchronized.

About this task

You must specify IPv4 addresses for the NTP servers.

You must specify external NTP servers. The specified NTP servers must use the NTP protocol.

You must specify four NTP server references of Stratum 3 or better to prevent issues with time drift.

> When specifying the external NTP source for a production-level StorageGRID installation, do not use the Windows Time (W32Time) service on a version of Windows earlier than Windows Server 2016. The time service on earlier versions of Windows is not sufficiently accurate and is not supported by Microsoft for use in high-accuracy environments, such as StorageGRID.

Support boundary to configure the Windows Time service for high-accuracy environments

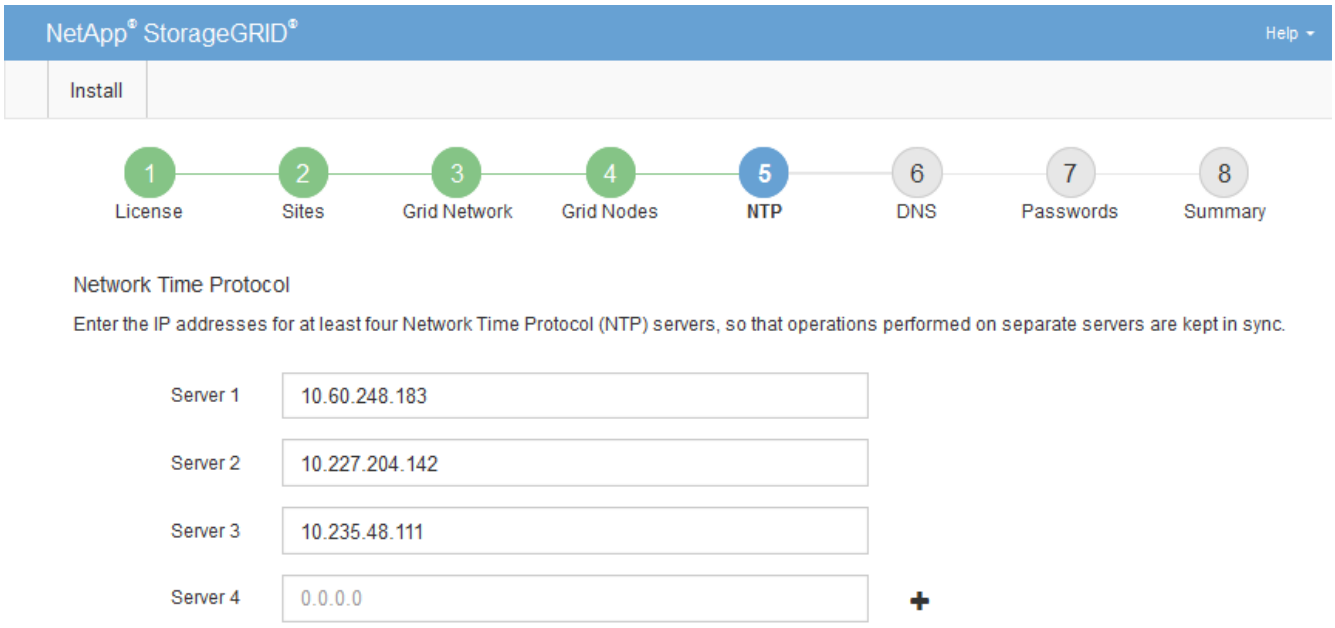
The external NTP servers are used by the nodes to which you previously assigned Primary NTP roles.

> Make sure that at least two nodes at each site can access at least four external NTP sources. If only one node at a site can reach the NTP sources, timing issues will occur if that node goes down. In addition, designating two nodes per site as primary NTP sources ensures accurate timing if a site is isolated from the rest of the grid.

Perform additional checks for VMware, such as ensuring that the hypervisor uses the same NTP source as the virtual machine, and using VMTools to disable the time sync between the hypervisor and StorageGRID virtual machines.

Steps

1. Specify the IPv4 addresses for at least four NTP servers in the **Server 1** to **Server 4** text boxes.
2. If necessary, select the plus sign next to the last entry to add additional server entries.



3. Select **Next**.

Specifying Domain Name System server information

You must specify Domain Name System (DNS) information for your StorageGRID system, so that you can access external servers using hostnames instead of IP addresses.

About this task

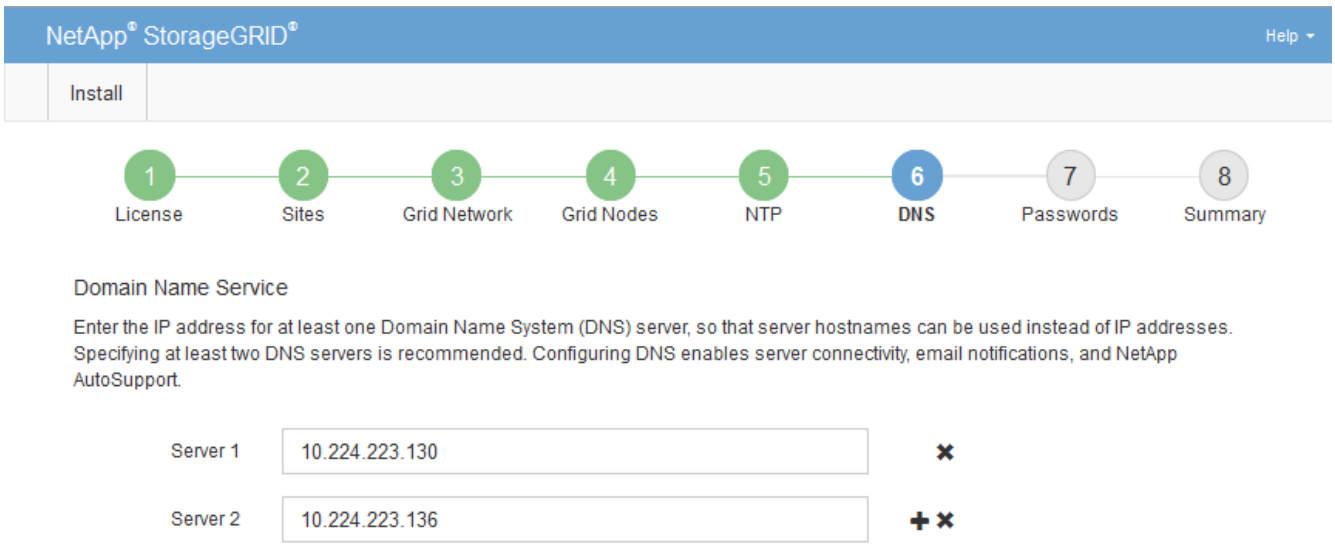
Specifying DNS server information allows you to use Fully Qualified Domain Name (FQDN) hostnames rather than IP addresses for email notifications and AutoSupport. Specifying at least two DNS servers is recommended.

> Provide two to six IPv4 addresses for DNS servers. You should select DNS servers that each site can access locally in the event of network islanding. This is to ensure an islanded site continues to have access to the DNS service. After configuring the grid-wide DNS server list, you can further customize the DNS server list for each node. For details, see the information about modifying the DNS configuration in the recovery and maintenance instructions.

If the DNS server information is omitted or incorrectly configured, a DNST alarm is triggered on each grid node's SSM service. The alarm clears when DNS is configured correctly and the new server information has reached all grid nodes.

Steps

1. Specify the IPv4 address for at least one DNS server in the **Server 1** text box.
2. If necessary, select the plus sign next to the last entry to add additional server entries.



   The best practice is to specify at least two DNS servers. You can specify up to six DNS servers.

3. Select **Next**.

Related information

Maintain & recover

Specifying the StorageGRID system passwords

As part of installing your StorageGRID system, you need to enter the passwords to use to secure your system and perform maintenance tasks.

About this task

Use the Install passwords page to specify the provisioning passphrase and the grid management root user password.

- The provisioning passphrase is used as an encryption key and is not stored by the StorageGRID system.
- You must have the provisioning passphrase for installation, expansion, and maintenance procedures, including downloading the recovery package. Therefore, it is important that you store the provisioning passphrase in a secure location.
- You can change the provisioning passphrase from the Grid Manager if you have the current one.
- The grid management root user password may be changed using the Grid Manager.
- Randomly generated command line console and SSH passwords are stored in the `Passwords.txt` file in the recovery package.

Steps

1. In **Provisioning Passphrase**, enter the provisioning passphase that will be required to make changes to the grid topology of your StorageGRID system.

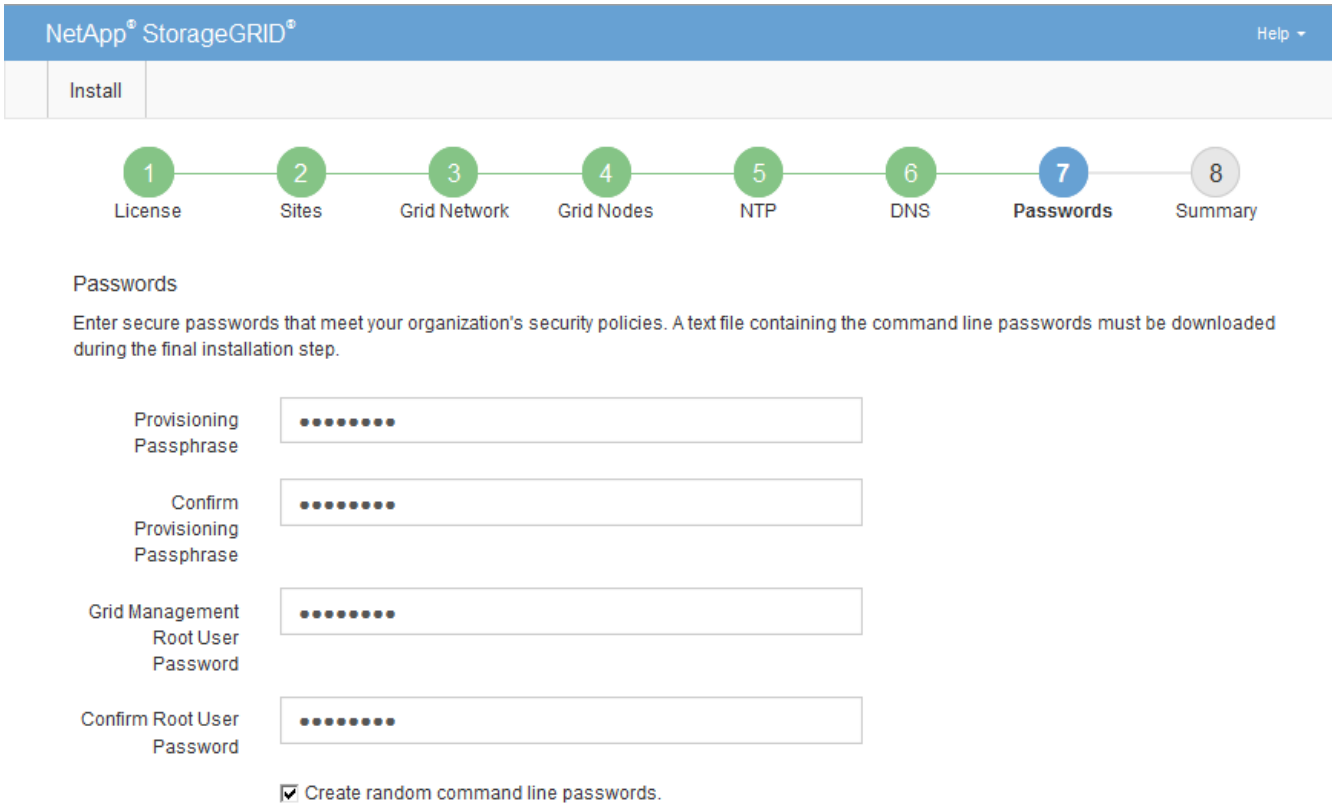
   Store the provisioning passphrase in a secure place.

   > If after the installation completes and you want to change the provisioning passphrase later, you can use the Grid Manager. Select **Configuration** > **Access Control** > **Grid Passwords**.

2. In **Confirm Provisioning Passphrase**, reenter the provisioning passphrase to confirm it.
3. In **Grid Management Root User Password**, enter the password to use to access the Grid Manager as the “root” user.

   Store the password in a secure place.

4. In **Confirm Root User Password**, reenter the Grid Manager password to confirm it.



5. If you are installing a grid for proof of concept or demo purposes, optionally deselect the **Create random command line passwords** check box.

   For production deployments, random passwords should always be used for security reasons. Deselect **Create random command line passwords** only for demo grids if you want to use default passwords to access grid nodes from the command line using the “root” or “admin” account.

   > You are prompted to download the Recovery Package file (`sgws-recovery-package-id-revision.zip`) after you click **Install** on the Summary page. You must download this file to complete the installation. The passwords required to access the system are stored in the `Passwords.txt` file, contained in the Recovery Package file.

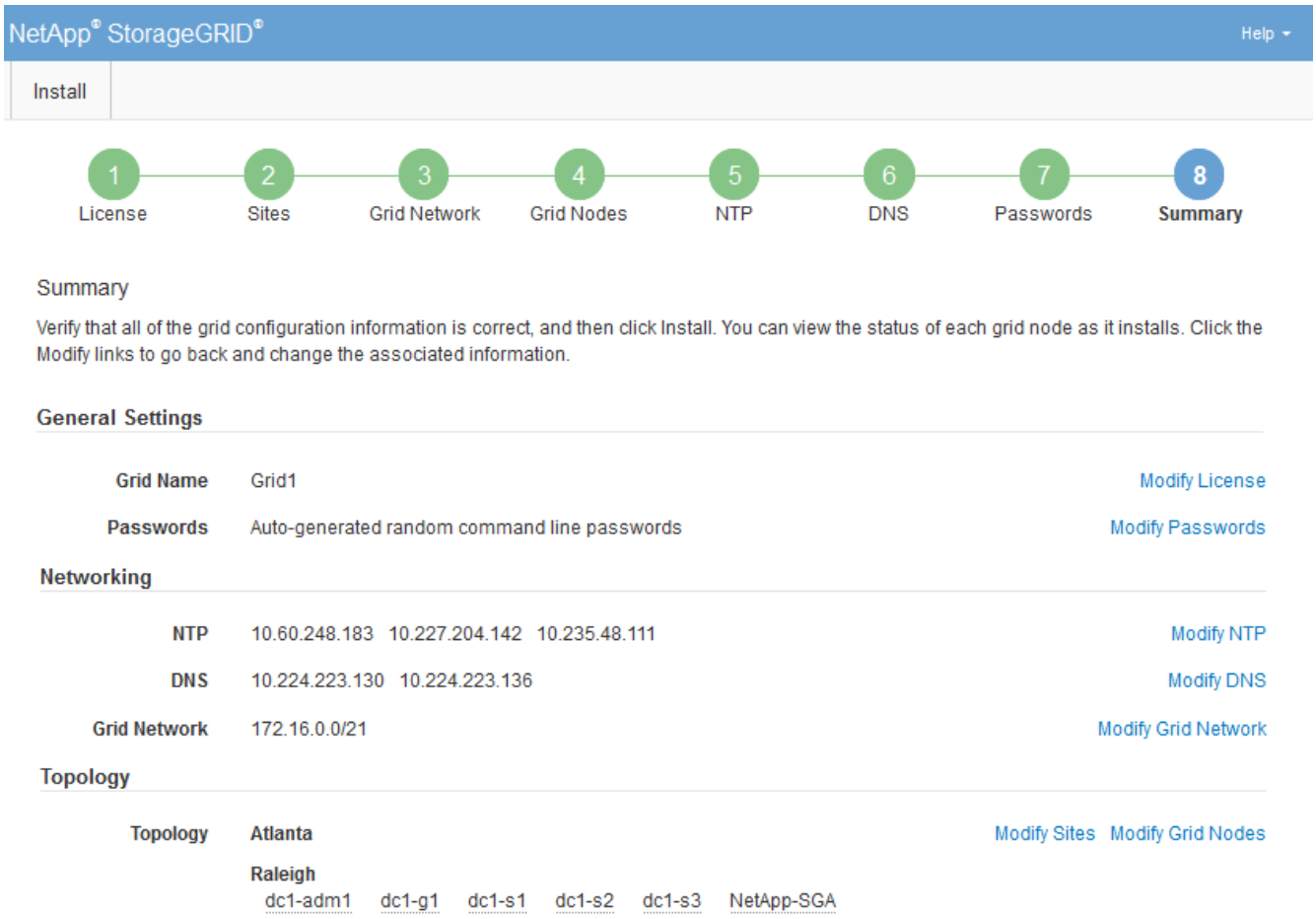
6. Click **Next**.

Reviewing your configuration and completing installation

You must carefully review the configuration information you have entered to ensure that the installation completes successfully.

Steps

1. View the **Summary** page.



2. Verify that all of the grid configuration information is correct. Use the Modify links on the Summary page to go back and correct any errors.

3. Click **Install**.

> If a node is configured to use the Client Network, the default gateway for that node switches from the Grid Network to the Client Network when you click **Install**. If you lose connectivity, you must ensure that you are accessing the primary Admin Node through an accessible subnet. See Networking guidelines for details.

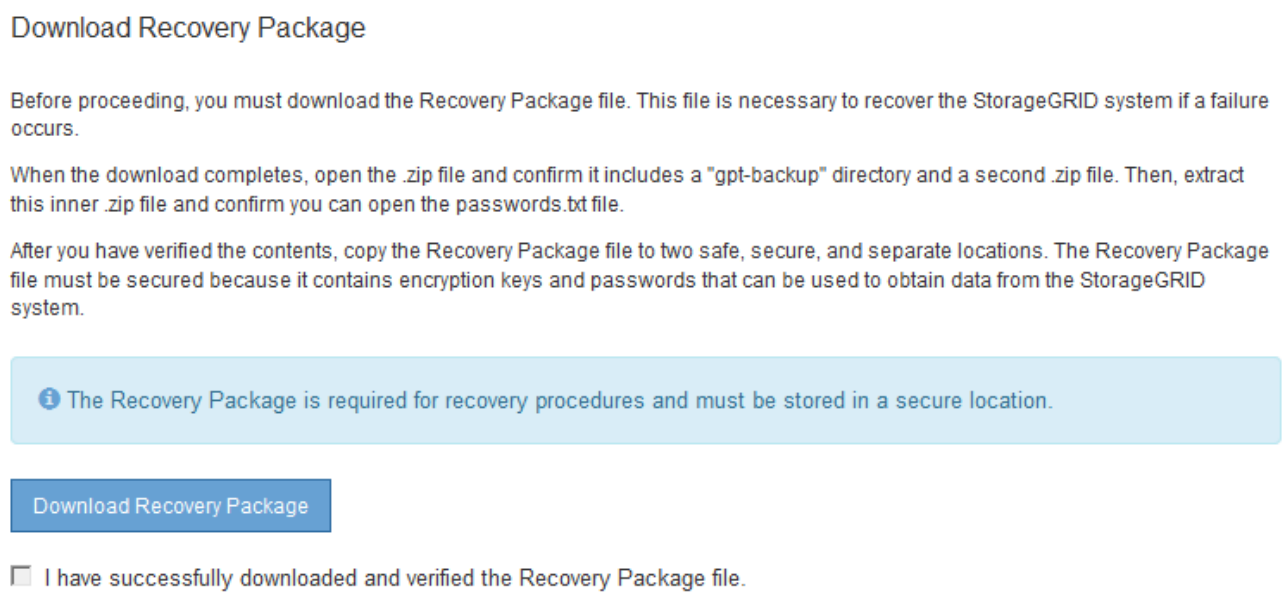
4. Click **Download Recovery Package**.

   When the installation progresses to the point where the grid topology is defined, you are prompted to download the Recovery Package file (`.zip`), and confirm that you can successfully access the contents of this file. You must download the Recovery Package file so that you can recover the StorageGRID system if one or more grid nodes fail. The installation continues in the background, but you cannot complete the installation and access the StorageGRID system until you download and verify this file.

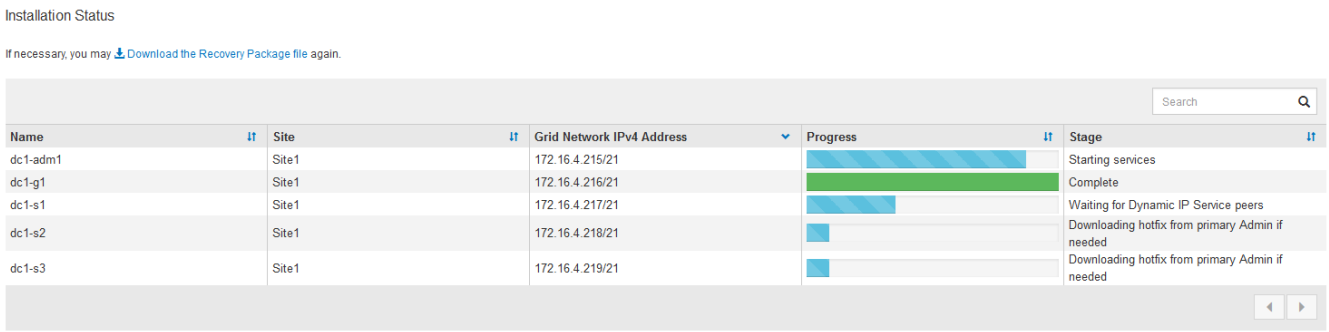
5. Verify that you can extract the contents of the `.zip` file, and then save it in two safe, secure, and separate locations.

> The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

6. Select the **I have successfully downloaded and verified the Recovery Package file** check box, and click **Next**.



   If the installation is still in progress, the status page appears. This page indicates the progress of the installation for each grid node.



When the Complete stage is reached for all grid nodes, the sign-in page for the Grid Manager appears.

7. Sign in to the Grid Manager using the “root” user and the password you specified during the installation.

Post-installation guidelines

After completing grid node deployment and configuration, follow these guidelines for DHCP addressing and network configuration changes.

- If DHCP was used to assign IP addresses, configure a DHCP reservation for each IP address on the networks being used.

  You can only set up DHCP during the deployment phase. You cannot set up DHCP during configuration.

  > Nodes reboot when their IP addresses change, which can cause outages if a DHCP address change affects multiple nodes at the same time.

- You must use the Change IP procedures if you want to change IP addresses, subnet masks, and default gateways for a grid node. See the information about configuring IP addresses in the recovery and maintenance instructions.
- If you make networking configuration changes, including routing and gateway changes, client connectivity to the primary Admin Node and other grid nodes might be lost. Depending on the networking changes applied, you might need to re-establish these connections.

Automating the installation

You can automate the deployment of VMware virtual grid nodes, the configuration of grid nodes, and the configuration of StorageGRID appliances.

- Automating grid node deployment in VMware vSphere
- Automating the configuration of StorageGRID

Automating grid node deployment in VMware vSphere

You can automate the deployment of StorageGRID grid nodes in VMware vSphere.

What you’ll need

- You have access to a Linux/Unix system with Bash 3.2 or later.
- You have VMware OVF Tool 4.1 installed and correctly configured.
- You know the username and password required to access VMware vSphere using the OVF Tool.

- You know the virtual infrastructure (VI) URL for the location in vSphere where you want to deploy the StorageGRID virtual machines. This URL will typically be a vApp, or Resource Pool. For example: `vi://vcenter.example.com/vi/sgws`

> You can use the VMware `ovftool` utility to determine this value (see the `ovftool` documentation for details).

> If you are deploying to a vApp, the virtual machines will not start automatically the first time, and you must power them on manually.

- You have collected all the required information for the configuration file. See Collecting information about your deployment environment for information.
- You have access to the following files from the VMware installation archive for StorageGRID:

Filename	Description
`NetApp-SG-version-SHA.vmdk`	The virtual machine disk file that is used as a template for creating grid node virtual machines. **Note:** This file must be in the same folder as the `.ovf` and `.mf` files.

`vsphere-primary-admin.ovf`
 	
`vsphere-primary-admin.mf`
	The Open Virtualization Format template file (`.ovf`) and manifest file (`.mf`) for deploying the primary Admin Node.

`vsphere-non-primary-admin.ovf`
 	
`vsphere-non-primary-admin.mf`
	The template file (`.ovf`) and manifest file (`.mf`) for deploying non-primary Admin Nodes.

`vsphere-archive.ovf`
 	
`vsphere-archive.mf`
	The template file (`.ovf`) and manifest file (`.mf`) for deploying Archive Nodes.

`vsphere-gateway.ovf`
 	
`vsphere-gateway.mf`
	The template file (`.ovf`) and manifest file (`.mf`) for deploying Gateway Nodes.

`vsphere-storage.ovf`
 	
`vsphere-storage.mf`
	The template file (`.ovf`) and manifest file (`.mf`) for deploying virtual machine-based Storage Nodes.

`deploy-vsphere-ovftool.sh`	The Bash shell script used to automate the deployment of virtual grid nodes.
`deploy-vsphere-ovftool-sample.ini`	The sample configuration file for use with the `deploy-vsphere-ovftool.sh` script.

Defining the configuration file for your deployment

You specify the information needed to deploy virtual grid nodes for StorageGRID in a configuration file, which is used by the `deploy-vsphere-ovftool.sh` Bash script. You

can modify a sample configuration file, so that you do not have to create the file from scratch.

Steps

1. Make a copy of the sample configuration file (`deploy-vsphere-ovftool.sample.ini`). Save the new file as `deploy-vsphere-ovftool.ini` in the same directory as `deploy-vsphere-ovftool.sh`.
2. Open `deploy-vsphere-ovftool.ini`.
3. Enter all of the information required to deploy VMware virtual grid nodes.

   See Configuration file settings for information.

4. When you have entered and verified all of the necessary information, save and close the file.

Configuration file settings

The `deploy-vsphere-ovftool.ini` configuration file contains the settings that are required to deploy virtual grid nodes.

The configuration file first lists global parameters, and then lists node-specific parameters in sections defined by node name. When the file is used:

- *Global parameters* are applied to all grid nodes.
- *Node-specific parameters* override global parameters.

Global parameters

Global parameters are applied to all grid nodes, unless they are overridden by settings in individual sections. Place the parameters that apply to multiple nodes in the global parameter section, and then override these settings as necessary in the sections for individual nodes.

- **OVFTOOL_ARGUMENTS**: You can specify OVFTOOL_ARGUMENTS as global settings, or you can apply arguments individually to specific nodes. For example:

  ```
  OVFTOOL_ARGUMENTS = --powerOn --noSSLVerify --diskMode=thin
  --datastore='<em>datastore_name</em>'
  ```

  You can use the `--powerOffTarget` and `--overwrite` options to shut down and replace existing virtual machines.

  > You should deploy nodes to different datastores and specify OVFTOOL_ARGUMENTS for each node, instead of globally.

- **SOURCE**: The path to the StorageGRID virtual machine template (`.vmdk`) file and the `.ovf` and `.mf` files for individual grid nodes. This defaults to the current directory.

  ```
  SOURCE = /downloads/StorageGRID-Webscale-<em>version</em>/vsphere
  ```

- **TARGET**: The VMware vSphere virtual infrastructure (vi) URL for the location where StorageGRID will be deployed. For example:

```
TARGET = vi://vcenter.example.com/vm/sgws
```

- **GRID_NETWORK_CONFIG**: The method used to acquire IP addresses, either STATIC or DHCP. The default is STATIC. If all or most of the nodes use the same method for acquiring IP addresses, you can specify that method here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
GRID_NETWORK_CONFIG = DHCP
```

- **GRID_NETWORK_TARGET**: The name of an existing VMware network to use for the Grid Network. If all or most of the nodes use the same network name, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
GRID_NETWORK_TARGET = SG-Admin-Network
```

- **GRID_NETWORK_MASK**: The network mask for the Grid Network. If all or most of the nodes use the same network mask, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
GRID_NETWORK_MASK = 255.255.255.0
```

- **GRID_NETWORK_GATEWAY**: The network gateway for the Grid Network. If all or most of the nodes use the same network gateway, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
GRID_NETWORK_GATEWAY = 10.1.0.1
```

- **GRID_NETWORK_MTU**: Optional. The maximum transmission unit (MTU) on the Grid Network. If specified, the value must be between 1280 and 9216. For example:

```
GRID_NETWORK_MTU = 8192
```

  If omitted, 1400 is used.

  If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value.

  > The MTU value of the network must match the value configured on the switch port the node is connected to. Otherwise, network performance issues or packet loss might occur.

> For the best network performance, all nodes should be configured with similar MTU values on their Grid Network interfaces. The **Grid Network MTU mismatch** alert is triggered if there is a significant difference in MTU settings for the Grid Network on individual nodes. The MTU values do not have to be the same for all network types.

- **ADMIN_NETWORK_CONFIG**: The method used to acquire IP addresses, either DISABLED, STATIC, or DHCP. The default is DISABLED. If all or most of the nodes use the same method for acquiring IP addresses, you can specify that method here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
ADMIN_NETWORK_CONFIG = STATIC
```

- **ADMIN_NETWORK_TARGET**: The name of an existing VMware network to use for the Admin Network. This setting is required unless the Admin Network is disabled. If all or most of the nodes use the same network name, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
ADMIN_NETWORK_TARGET = SG-Admin-Network
```

- **ADMIN_NETWORK_MASK**: The network mask for the Admin Network. This setting is required if you are using static IP addressing. If all or most of the nodes use the same network mask, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
ADMIN_NETWORK_MASK = 255.255.255.0
```

- **ADMIN_NETWORK_GATEWAY**: The network gateway for the Admin Network. This setting is required if you are using static IP addressing and you specify external subnets in the ADMIN_NETWORK_ESL setting. (That is, it is not required if ADMIN_NETWORK_ESL is empty.) If all or most of the nodes use the same network gateway, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
ADMIN_NETWORK_GATEWAY = 10.3.0.1
```

- **ADMIN_NETWORK_ESL**: The external subnet list (routes) for the Admin Network, specified as a comma-separated list of CIDR route destinations. If all or most of the nodes use the same external subnet list, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
ADMIN_NETWORK_ESL = 172.16.0.0/21,172.17.0.0/21
```

- **ADMIN_NETWORK_MTU**: Optional. The maximum transmission unit (MTU) on the Admin Network. Do not specify if ADMIN_NETWORK_CONFIG = DHCP. If specified, the value must be between 1280 and 9216. If omitted, 1400 is used. If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value. If all or most of the nodes use the same MTU for the

Admin Network, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
ADMIN_NETWORK_MTU = 8192
```

- **CLIENT_NETWORK_CONFIG**: The method used to acquire IP addresses, either DISABLED, STATIC, or DHCP. The default is DISABLED. If all or most of the nodes use the same method for acquiring IP addresses, you can specify that method here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
CLIENT_NETWORK_CONFIG = STATIC
```

- **CLIENT_NETWORK_TARGET**: The name of an existing VMware network to use for the Client Network. This setting is required unless the Client Network is disabled. If all or most of the nodes use the same network name, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
CLIENT_NETWORK_TARGET = SG-Client-Network
```

- **CLIENT_NETWORK_MASK**: The network mask for the Client Network. This setting is required if you are using static IP addressing. If all or most of the nodes use the same network mask, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
CLIENT_NETWORK_MASK = 255.255.255.0
```

- **CLIENT_NETWORK_GATEWAY**: The network gateway for the Client Network. This setting is required if you are using static IP addressing. If all or most of the nodes use the same network gateway, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
CLIENT_NETWORK_GATEWAY = 10.4.0.1
```

- **CLIENT_NETWORK_MTU**: Optional. The maximum transmission unit (MTU) on the Client Network. Do not specify if CLIENT_NETWORK_CONFIG = DHCP. If specified, the value must be between 1280 and 9216. If omitted, 1400 is used. If you want to use jumbo frames, set the MTU to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value. If all or most of the nodes use the same MTU for the Client Network, you can specify it here. You can then override the global setting by specifying different settings for one or more individual nodes. For example:

```
CLIENT_NETWORK_MTU = 8192
```

- **PORT_REMAP**: Remaps any port used by a node for internal grid node communications or external communications. Remapping ports is necessary if enterprise networking policies restrict one or more ports

used by StorageGRID. For the list of ports used by StorageGRID, see internal grid node communications and external communications in Networking guidelines.

> Do not remap the ports you are planning to use to configure load balancer endpoints.

> If only PORT_REMAP is set, the mapping that you specify is used for both inbound and outbound communications. If PORT_REMAP_INBOUND is also specified, PORT_REMAP applies only to outbound communications.

The format used is: *network type/protocol/_default port used by grid node/new port*, where network type is grid, admin, or client, and protocol is tcp or udp.

For example:

```
PORT_REMAP = client/tcp/18082/443
```

If used alone, this example setting symmetrically maps both inbound and outbound communications for the grid node from port 18082 to port 443. If used in conjunction with PORT_REMAP_INBOUND, this example setting maps outbound communications from port 18082 to port 443.

- **PORT_REMAP_INBOUND**: Remaps inbound communications for the specified port. If you specify PORT_REMAP_INBOUND but do not specify a value for PORT_REMAP, outbound communications for the port are unchanged.

> Do not remap the ports you are planning to use to configure load balancer endpoints.

The format used is: *network type/protocol/_default port used by grid node/new port*, where network type is grid, admin, or client, and protocol is tcp or udp.

For example:

```
PORT_REMAP_INBOUND = client/tcp/443/18082
```

This example takes traffic that is sent to port 443 to pass an internal firewall and directs it to port 18082, where the grid node is listening for S3 requests.

Node-specific parameters

Each node is in its own section of the configuration file. Each node requires the following settings:

- The section head defines the node name that will be displayed in the Grid Manager. You can override that value by specifying the optional NODE_NAME parameter for the node.
- **NODE_TYPE**: VM_Admin_Node, VM_Storage_Node, VM_Archive_Node, or VM_API_Gateway_Node
- **GRID_NETWORK_IP**: The IP address for the node on the Grid Network.
- **ADMIN_NETWORK_IP**: The IP address for the node on the Admin Network. Required only if the node is attached to the Admin Network and ADMIN_NETWORK_CONFIG is set to STATIC.
- **CLIENT_NETWORK_IP**: The IP address for the node on the Client Network. Required only if the node is

attached to the Client Network and CLIENT_NETWORK_CONFIG for this node is set to STATIC.

- **ADMIN_IP**: The IP address for the primary Admin node on the Grid Network. Use the value that you specify as the GRID_NETWORK_IP for the primary Admin Node. If you omit this parameter, the node attempts to discover the primary Admin Node IP using mDNS. For more information, see How grid nodes discover the primary Admin Node.

  The ADMIN_IP parameter is ignored for the primary Admin Node.

- Any parameters that were not set globally. For example, if a node is attached to the Admin Network and you did not specify ADMIN_NETWORK parameters globally, you must specify them for the node.

Primary Admin Node

The following additional settings are required for the primary Admin Node:

- **NODE_TYPE**: VM_Admin_Node
- **ADMIN_ROLE**: Primary

This example entry is for a primary Admin Node that is on all three networks:

```
[DC1-ADM1]
  ADMIN_ROLE = Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_IP = 10.1.0.2
  ADMIN_NETWORK_IP = 10.3.0.2
  CLIENT_NETWORK_IP = 10.4.0.2
```

The following additional setting is optional for the primary Admin Node:

- **DISK**: By default, Admin Nodes are assigned two additional 200 GB hard disks for audit and database use. You can increase these settings using the DISK parameter. For example:

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

  For Admin nodes, INSTANCES must always equal 2.

Storage Node

The following additional setting is required for Storage Nodes:

- **NODE_TYPE**: VM_Storage_Node

  This example entry is for a Storage Node that is on the Grid and Admin Networks, but not on the Client Network. This node uses the ADMIN_IP setting to specify the primary Admin Node's IP address on the Grid Network.

```
[DC1-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.0.3
  ADMIN_NETWORK_IP = 10.3.0.3

  ADMIN_IP = 10.1.0.2
```

This second example entry is for a Storage Node on a Client Network where the customer's enterprise networking policy states that an S3 client application is only permitted to access the Storage Node using either port 80 or 443. The example configuration file uses PORT_REMAP to enable the Storage Node to send and receive S3 messages on port 443.

```
[DC2-S1]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3
  CLIENT_NETWORK_IP = 10.4.1.3
  PORT_REMAP = client/tcp/18082/443

  ADMIN_IP = 10.1.0.2
```

The last example creates a symmetric remapping for ssh traffic from port 22 to port 3022, but explicitly sets the values for both inbound and outbound traffic.

```
[DC1-S3]
  NODE_TYPE = VM_Storage_Node

  GRID_NETWORK_IP = 10.1.1.3

  PORT_REMAP = grid/tcp/22/3022
  PORT_REMAP_INBOUND = grid/tcp/3022/22

  ADMIN_IP = 10.1.0.2
```

The following additional setting is optional for Storage Nodes:

- **DISK**: By default, Storage Nodes are assigned three 4 TB disks for RangeDB use. You can increase these settings with the DISK parameter. For example:

```
DISK = INSTANCES=16, CAPACITY=4096
```

Archive Node

The following additional setting is required for Archive Nodes:

- **NODE_TYPE**: VM_Archive_Node

This example entry is for an Archive Node that is on the Grid and Admin Networks, but not on the Client Network.

```
[DC1-ARC1]
  NODE_TYPE = VM_Archive_Node

  GRID_NETWORK_IP = 10.1.0.4
  ADMIN_NETWORK_IP = 10.3.0.4

  ADMIN_IP = 10.1.0.2
```

Gateway Node

The following additional setting is required for Gateway Nodes:

- **NODE_TYPE**: VM_API_Gateway

This example entry is for an example Gateway Node on all three networks. In this example, no Client Network parameters were specified in the global section of the configuration file, so they must be specified for the node:

```
[DC1-G1]
  NODE_TYPE = VM_API_Gateway

  GRID_NETWORK_IP = 10.1.0.5
  ADMIN_NETWORK_IP = 10.3.0.5

  CLIENT_NETWORK_CONFIG = STATIC
  CLIENT_NETWORK_TARGET = SG-Client-Network
  CLIENT_NETWORK_MASK = 255.255.255.0
  CLIENT_NETWORK_GATEWAY = 10.4.0.1
  CLIENT_NETWORK_IP = 10.4.0.5

  ADMIN_IP = 10.1.0.2
```

Non-primary Admin Node

The following additional settings are required for non-primary Admin Nodes:

- **NODE_TYPE**: VM_Admin_Node
- **ADMIN_ROLE**: Non-Primary

This example entry is for a non-primary Admin Node that is not on the Client Network:

```
[DC2-ADM1]
  ADMIN_ROLE = Non-Primary
  NODE_TYPE = VM_Admin_Node

  GRID_NETWORK_TARGET = SG-Grid-Network
  GRID_NETWORK_IP = 10.1.0.6
  ADMIN_NETWORK_IP = 10.3.0.6

  ADMIN_IP = 10.1.0.2
```

The following additional setting is optional for non-primary Admin Nodes:

- **DISK**: By default, Admin Nodes are assigned two additional 200 GB hard disks for audit and database use. You can increase these settings using the DISK parameter. For example:

  ```
  DISK = INSTANCES=2, CAPACITY=300
  ```

> For Admin nodes, INSTANCES must always equal 2.

Related information

How grid nodes discover the primary Admin Node

Networking guidelines

Running the Bash script

You can use the `deploy-vsphere-ovftool.sh` Bash script and the deploy-vsphere-ovftool.ini configuration file you modified to automate the deployment of StorageGRID grid nodes in VMware vSphere.

What you'll need

- You have created a deploy-vsphere-ovftool.ini configuration file for your environment.

You can use the help available with the Bash script by entering the help commands (`-h/--help`). For example:

```
./deploy-vsphere-ovftool.sh -h
```

or

```
./deploy-vsphere-ovftool.sh --help
```

Steps

1. Log in to the Linux machine you are using to run the Bash script.
2. Change to the directory where you extracted the installation archive.

   For example:

   ```
   cd StorageGRID-Webscale-version/vsphere
   ```

3. To deploy all grid nodes, run the Bash script with the appropriate options for your environment.

   For example:

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd ./deploy-
   vsphere-ovftool.ini
   ```

4. If a grid node failed to deploy because of an error, resolve the error and rerun the Bash script for only that node.

   For example:

   ```
   ./deploy-vsphere-ovftool.sh --username=user --password=pwd --single
   -node="DC1-S3" ./deploy-vsphere-ovftool.ini
   ```

The deployment is complete when the status for each node is “Passed.”

```
Deployment Summary
+-----------------------------+----------+----------------------+
| node                        | attempts | status               |
+-----------------------------+----------+----------------------+
| DC1-ADM1                    |        1 | Passed               |
| DC1-G1                      |        1 | Passed               |
| DC1-S1                      |        1 | Passed               |
| DC1-S2                      |        1 | Passed               |
| DC1-S3                      |        1 | Passed               |
+-----------------------------+----------+----------------------+
```

Automating the configuration of StorageGRID

After deploying the grid nodes, you can automate the configuration of the StorageGRID system.

What you’ll need

- You know the location of the following files from the installation archive.

Filename	Description
`configure-storagegrid.py`	Python script used to automate the configuration
`configure-storagegrid.sample.json`	Sample configuration file for use with the script
`configure-storagegrid.blank.json`	Blank configuration file for use with the script

- You have created a `configure-storagegrid.json` configuration file. To create this file, you can modify the sample configuration file (`configure-storagegrid.sample.json`) or the blank configuration file (`configure-storagegrid.blank.json`).

You can use the `configure-storagegrid.py` Python script and the `configure-storagegrid.json` configuration file to automate the configuration of your StorageGRID system.

> You can also configure the system using the Grid Manager or the Installation API.

Steps

1. Log in to the Linux machine you are using to run the Python script.
2. Change to the directory where you extracted the installation archive.

   For example:

   ```
   cd StorageGRID-Webscale-version/platform
   ```

   where `platform` is debs, rpms, or vsphere.

3. Run the Python script and use the configuration file you created.

   For example:

   ```
   ./configure-storagegrid.py ./configure-storagegrid.json --start-install
   ```

Result

A Recovery Package .zip file is generated during the configuration process, and it is downloaded to the directory where you are running the installation and configuration process. You must back up the Recovery Package file so that you can recover the StorageGRID system if one or more grid nodes fails. For example, copy it to a secure, backed up network location and to a secure cloud storage location.

> The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

If you specified that random passwords should be generated, you need to extract the Passwords.txt file and look for the passwords required to access your StorageGRID system.

```
#####################################################################
##### The StorageGRID "recovery package" has been downloaded as: #####
#####           ./sgws-recovery-package-994078-rev1.zip          #####
#####   Safeguard this file as it will be needed in case of a    #####
#####                 StorageGRID node recovery.                 #####
#####################################################################
```

Your StorageGRID system is installed and configured when a confirmation message is displayed.

```
StorageGRID has been configured and installed.
```

Related information

Navigating to the Grid Manager

Overview of the installation REST API

Overview of the installation REST API

StorageGRID provides the StorageGRID Installation API for performing installation tasks.

The API uses the Swagger open source API platform to provide the API documentation. Swagger allows both developers and non-developers to interact with the API in a user interface that illustrates how the API responds to parameters and options. This documentation assumes that you are familiar with standard web technologies and the JSON (JavaScript Object Notation) data format.

> Any API operations you perform using the API Docs webpage are live operations. Be careful not to create, update, or delete configuration data or other data by mistake.

Each REST API command includes the API's URL, an HTTP action, any required or optional URL parameters, and an expected API response.

StorageGRID Installation API

The StorageGRID Installation API is only available when you are initially configuring your StorageGRID system, and in the event that you need to perform a primary Admin Node recovery. The Installation API can be accessed over HTTPS from the Grid Manager.

To access the API documentation, go to the installation web page on the primary Admin Node and select **Help** > **API Documentation** from the menu bar.

The StorageGRID Installation API includes the following sections:

- **config** — Operations related to the product release and versions of the API. You can list the product release version and the major versions of the API supported by that release.
- **grid** — Grid-level configuration operations. You can get and update grid settings, including grid details, Grid Network subnets, grid passwords, and NTP and DNS server IP addresses.
- **nodes** — Node-level configuration operations. You can retrieve a list of grid nodes, delete a grid node, configure a grid node, view a grid node, and reset a grid node's configuration.

- **provision** — Provisioning operations. You can start the provisioning operation and view the status of the provisioning operation.
- **recovery** — Primary Admin Node recovery operations. You can reset information, upload the Recover Package, start the recovery, and view the status of the recovery operation.
- **recovery-package** — Operations to download the Recovery Package.
- **sites** — Site-level configuration operations. You can create, view, delete, and modify a site.

Where to go next

After completing an installation, you must perform a series of integration and configuration steps. Some steps are required; others are optional.

Required tasks

- Configure VMware vSphere Hypervisor for automatic restart.

  You must configure the hypervisor to restart the virtual machines when the server restarts. Without an automatic restart, the virtual machines and grid nodes remain shut down after the server restarts. For details, see the VMware vSphere Hypervisor documentation.

- Create a tenant account for each client protocol (Swift or S3) that will be used to store objects on your StorageGRID system.
- Control system access by configuring groups and user accounts. Optionally, you can configure a federated identity source (such as Active Directory or OpenLDAP), so you can import administration groups and users. Or, you can create local groups and users.
- Integrate and test the S3 or Swift API client applications you will use to upload objects to your StorageGRID system.
- When you are ready, configure the information lifecycle management (ILM) rules and ILM policy you want to use to protect object data.

  When you install StorageGRID, the default ILM policy, Baseline 2 Copies Policy, is active. This policy includes the stock ILM rule (Make 2 Copies), and it applies if no other policy has been activated.

- If your installation includes appliance Storage Nodes, use SANtricity software to complete the following tasks:
  - Connect to each StorageGRID appliance.
  - Verify receipt of AutoSupport data.
- If your StorageGRID system includes any Archive Nodes, configure the Archive Node's connection to the target external archival storage system.

  If any Archive Nodes will use Tivoli Storage Manager as the external archival storage system, you must also configure Tivoli Storage Manager.

- Review and follow the StorageGRID system hardening guidelines to eliminate security risks.
- Configure email notifications for system alerts.

Optional tasks

- If you want to receive notifications from the (legacy) alarm system, configure mailing lists and email notifications for alarms.
- Update grid node IP addresses if they have changed since you planned your deployment and generated the Recovery Package. See information about changing IP addresses in the recovery and maintenance instructions.
- Configure storage encryption, if required.
- Configure storage compression to reduce the size of stored objects, if required.
- Configure audit client access. You can configure access to the system for auditing purposes through an NFS or a CIFS file share. See the instructions for administering StorageGRID.

> Audit export through CIFS/Samba has been deprecated and will be removed in a future StorageGRID release.

Troubleshooting installation issues

If any problems occur while installing your StorageGRID system, you can access the installation log files.

The following are the main installation log files, which technical support might need to resolve issues.

- `/var/local/log/install.log` (found on all grid nodes)
- `/var/local/log/gdu-server.log` (found on the primary Admin Node)

To learn how to access the log files, see the instructions for monitoring and troubleshooting StorageGRID. For help troubleshooting appliance installation issues, see the installation and maintenance instructions for your appliances. If you need additional help, contact technical support.

Related information

Monitor & troubleshoot

SG100 & SG1000 services appliances

SG6000 storage appliances

SG5700 storage appliances

SG5600 storage appliances

NetApp Support

Virtual machine resource reservation requires adjustment

OVF files include a resource reservation designed to ensure that each grid node has sufficient RAM and CPU to operate efficiently. If you create virtual machines by deploying these OVF files on VMware and the predefined number of resources are not available, the virtual machines will not start.

About this task

If you are certain that the VM host has sufficient resources for each grid node, manually adjust the resources allocated for each virtual machine, and then try starting the virtual machines.

Steps

1. In the VMware vSphere Hypervisor client tree, select the virtual machine that is not started.
2. Right-click the virtual machine, and select **Edit Settings**.
3. From the Virtual Machines Properties window, select the **Resources** tab.
4. Adjust the resources allocated to the virtual machine:
   a. Select **CPU**, and then use the Reservation slider to adjust the MHz reserved for this virtual machine.
   b. Select **Memory**, and then use the Reservation slider to adjust the MB reserved for this virtual machine.
5. Click **OK**.
6. Repeat as required for other virtual machines hosted on the same VM host.

Upgrade software

Learn how to upgrade a StorageGRID system to a new release.

- About StorageGRID 11.5
- Upgrade planning and preparation
- Performing the upgrade
- Troubleshooting upgrade issues

About StorageGRID 11.5

Before starting an upgrade, review this section to learn about the new features and enhancements in StorageGRID 11.5, determine whether any features have been deprecated or removed, and find out about changes to StorageGRID APIs.

- What's new in StorageGRID 11.5
- Removed or deprecated features
- Changes to the Grid Management API
- Changes to the Tenant Management API

What's new in StorageGRID 11.5

StorageGRID 11.5 introduces S3 Object Lock, support for KMIP encryption of data, usability improvements to ILM, a redesigned Tenant Manager user interface, support for decommissioning a StorageGRID site, and an appliance node clone procedure.

S3 Object Lock for compliant data

The S3 Object Lock feature in StorageGRID 11.5 is an object-protection solution that is equivalent to S3 Object Lock in Amazon Simple Storage Service (Amazon S3). You can enable the global S3 Object Lock setting for a StorageGRID system to allow S3 tenant accounts to create buckets with S3 Object Lock enabled. The tenant can then use an S3 client application to optionally specify retention and legal hold settings for the objects in those buckets.

S3 Object Lock lets tenant users comply with regulations that require certain objects to be retained for a fixed amount of time or indefinitely.

Learn more

- Manage objects with ILM
- Use S3
- Use a tenant account

KMS encryption key management

You can now configure one or more external key management servers (KMS) in the Grid Manager to provide encryption keys to StorageGRID services and storage appliances. Each KMS or KMS cluster uses the Key Management Interoperability Protocol (KMIP) to provide an encryption key to the appliance nodes at the associated StorageGRID site. After the appliance volumes are encrypted, you cannot access any data on the appliance unless the node can communicate with the KMS.

> If you want to use encryption key management, you must use the StorageGRID Appliance Installer to enable the **Node Encryption** setting for the appliance before you add the appliance to the grid.

Learn more

- Administer StorageGRID

Usability enhancements for information lifecycle management (ILM)

- You can now view the total capacity of a storage pool, including the amount of used and free space. You can also see which nodes are included in a storage pool and which ILM rules and Erasure Coding profiles use the storage pool.
- You can now design ILM rules that apply to more than one tenant account.
- When you create an ILM rule for erasure coding, you are now reminded to set the Object Size (MB) advanced filter to greater than 0.2 to ensure that very small objects are not erasure coded.
- The ILM policy interface now ensures that the default ILM rule will be always be used for any objects not matched by another rule. Starting in StorageGRID 11.5, the default rule cannot use any basic or advanced filters and is automatically placed as the last rule in the policy.

  > If your current ILM policy does not conform to the new requirements, you can continue to use it after you upgrade to StorageGRID 11.5. However, if you attempt to clone a non-conforming policy after you upgrade, you are prompted to select a default rule that does not include filters and you are required to place the default rule at the end of the policy.

- The stock All Storage Nodes storage pool is no longer selected by default when you create a new ILM rule or a new Erasure Coding profile. In addition, you can now remove the All Storage Nodes storage pool as long as it not used in any rule.

  > Using the All Storage Nodes storage pool is not recommended because this storage pool contains all sites. Multiple copies of an object might be placed on the same site if you use this storage pool with a StorageGRID system that includes more than one site.

- You can now remove the stock Make 2 Copies rule (which uses the All Storage Nodes storage pool) as long as it is not used in an active or proposed policy.

- Objects stored in a Cloud Storage Pool can now be deleted immediately (synchronous deletion).

Learn more

- Manage objects with ILM

Enhancements to the Grid Manager

- The redesigned Tenant Accounts page makes it easier to view tenant account usage. The tenant summary table now includes columns for Space Used, Quota Utilization, Quota, and Object Count. A new **View Details** button accesses an overview of each tenant as well as details about the account's S3 buckets or Swift containers. In addition, you can now export two `.csv` files for tenant usage: one containing usage values for all tenants and one containing details about a tenant's buckets or containers.

  Related to this change, three new Prometheus metrics were added to track tenant account usage:

  - `storagegrid_tenant_usage_data_bytes`
  - `storagegrid_tenant_usage_object_count`
  - `storagegrid_tenant_usage_quota_bytes`
- The new **Access Mode** field on the Admin Groups page (**Configuration** > **Access Control**) allows you to specify whether the management permissions for the group are read-write (default) or read-only. Users who belong to a group with read-write access mode can change settings and perform operations in the Grid Manager and the Grid Management API. Users who belong to a group with read-only access mode can only view the settings and features that are selected for the group.

  > When you upgrade to StorageGRID 11.5, the read-write access mode option is selected for all existing admin groups.

- The AutoSupport user interface was redesigned. You can now configure event-triggered, user-triggered, and weekly AutoSupport messages from a single page in the Grid Manager. You can also configure an additional destination for AutoSupport messages.

  > If AutoSupport has not been enabled, a reminder message now appears on the Grid ManagerDashboard.

- When viewing the **Storage Used - Object Data** chart on the Nodes page, you can now see estimates for the amount of replicated object data and the amount of erasure-coded data on the grid, site, or Storage Node (**Nodes** > ***grid/site/Storage Node*** > **Storage**).
- Grid Manager menu options were reorganized to make options easier to find. For example, a new **Network Settings** submenu was added to the **Configuration** menu and options in the **Maintenance** and **Support** menus are now listed in alphabetic order.

Learn more

- Administer StorageGRID

Enhancements to the Tenant Manager

- The appearance and organization of the Tenant Manager user interface has been completely redesigned to improve the user experience.
- The new Tenant Manager dashboard provides a high-level summary of each account: it provides bucket details and shows the number of buckets or containers, groups, users, and platform services endpoints (if configured).

Learn more

- Use a tenant account

Client certificates for Prometheus metrics export

You can now upload or generate client certificates (**Configuration** > **Access Control** > **Client Certificates**), which can be used to provide secure, authenticated access to the StorageGRID Prometheus database. For example, you can use client certificates if you need to monitor StorageGRID externally using Grafana.

Learn more

- Administer StorageGRID

Load balancer enhancements

- When handling routing requests at a site, the Load Balancer service now performs load aware routing: it considers the CPU availability of the Storage Nodes at the same site. In some cases, information about CPU availability is limited to the site where the Load Balancer service is located.

  > CPU awareness will be not enabled until at least two-thirds of the Storage Nodes at a site have been upgraded to StorageGRID 11.5 and are reporting CPU statistics.

- For added security, you can now specify a binding mode for each load balancer endpoint. Endpoint pinning lets you restrict the accessibility of each endpoint to specific high availability groups or node interfaces.

Learn more

- Administer StorageGRID

Object metadata changes

- **New Actual reserved space metric**: To help you understand and monitor object metadata space usage on each Storage Node, a new Prometheus metric is shown on the Storage Used - Object Metadata graph for a Storage Node (**Nodes** > ***Storage Node*** > **Storage**).

  ```
  storagegrid_storage_utilization_metadata_reserved
  ```

  The **Actual reserved space** metric indicates how much space StorageGRID has reserved for object metadata on a specific Storage Node.

- **Metadata space increased for installations with larger Storage Nodes**: The system-wide Metadata Reserved Space setting has been increased for StorageGRID systems containing Storage Nodes with 128 GB or more of RAM, as follows:
  - **8 TB for new installations**: If you are installing a new StorageGRID 11.5 system and each Storage Node in the grid has 128 GB or more of RAM, the system-wide Metadata Reserved Space setting is now set to 8 TB instead of 3 TB.
  - **4 TB for upgrades**: If you are upgrading to StorageGRID 11.5 and each Storage Node at any one site has 128 GB or more of RAM, the system-wide Metadata Reserved Space setting is now set to 4 TB instead of 3 TB.

    The new values for the Metadata Reserved Space setting increase the allowed metadata space for these larger Storage Nodes, up to 2.64 TB, and ensure that adequate metadata space is reserved for future hardware and software versions.

> If your Storage Nodes have enough RAM and sufficient space on volume 0, you can manually increase the Metadata Reserved Space setting up to 8 TB after you upgrade. Reserving additional metadata space after the StorageGRID 11.5 upgrade will simplify future hardware and software upgrades.
>
> Increasing the Metadata Reserved Space setting

> If your StorageGRID system stores (or is expected to store) more than 2.64 TB of metadata on any Storage Node, the allowed metadata space can be increased in some cases. If your Storage Nodes each have available free space on storage volume 0 and more than 128 GB of RAM, contact your NetApp account representative. NetApp will review your requirements and increase the allowed metadata space for each Storage Node, if possible.

- **Automatic cleanup of deleted metadata**: When 20% or more of the metadata stored on a Storage Node is ready to be removed (because the corresponding objects were deleted), StorageGRID can now perform an automatic compaction on that Storage Node. This background process only runs if the load on the system is low—that is, when there is available CPU, disk space, and memory. The new compaction process removes metadata for deleted objects sooner than in previous releases and helps to free up space for new objects to be stored.

Learn more

- Administer StorageGRID

Changes to S3 REST API support

- You can now use the S3 REST API to specify S3 Object Lock settings:
  - To create a bucket with S3 Object Lock enabled, use a PUT Bucket request with the `x-amz-bucket-object-lock-enabled` header.
  - To determine if S3 Object Lock is enabled for a bucket, use a GET Object Lock Configuration request.
  - When adding an object version to a bucket with S3 Object Lock enabled, use the following request headers to specify the retention and legal hold settings: `x-amz-object-lock-mode`, `x-amz-object-lock-retain-until-date`, and `x-amz-object-lock-legal-hold`.
- You can now use DELETE Multiple Objects on a versioned bucket.
- You can now use PUT, GET, and DELETE Bucket encryption requests to manage encryption for an existing S3 bucket.
- A minor change was made to a field name for the `Expiration` parameter. This parameter is included in the response to a PUT Object, HEAD Object, or GET Object request if an expiration rule in the lifecycle configuration applies to a specific object. The field that indicates which expiration rule was matched was previously named `rule_id`. This field was renamed to `rule-id` to match the AWS implementation.
- By default, the S3 GET Storage Usage request now attempts to retrieve the storage used by a tenant account and its buckets using strong-global consistency. If strong-global consistency cannot be achieved, StorageGRID attempts to retrieve the usage information using strong-site consistency.
- The `Content-MD5` request header is now correctly supported.

Learn more

- Use S3

Maximum size for CloudMirror objects increased to 5 TB

The maximum size for objects that can be replicated to a destination bucket by the CloudMirror replication service was increased to 5 TB, which is the maximum object size supported by StorageGRID.

Learn more

- Use S3
- Use Swift

New alerts added

The following new alerts were added for StorageGRID 11.5:

- Appliance BMC communication error
- Appliance Fibre Channel fault detected
- Appliance Fibre Channel HBA port failure
- Appliance LACP port missing
- Cassandra auto-compactor error
- Cassandra auto-compactor metrics out of date
- Cassandra compactions overloaded
- Disk I/O is very slow
- KMS CA certificate expiration
- KMS client certificate expiration
- KMS configuration failed to load
- KMS connectivity error
- KMS encryption key name not found
- KMS encryption key rotation failed
- KMS is not configured
- KMS key failed to decrypt an appliance volume
- KMS server certificate expiration
- Low free space for storage pool
- Node network reception frame error
- Services appliance storage connectivity degraded
- Storage appliance storage connectivity degraded (previously named Appliance storage connectivity degraded)
- Tenant quota usage high
- Unexpected node reboot

Learn more

- Monitor & troubleshoot

TCP support for SNMP traps

You can now select Transmission Control Protocol (TCP) as the protocol for SNMP trap destinations.

Previously, only the User Datagram Protocol (UDP) protocol was supported.

Learn more

- Monitor & troubleshoot

Installation and networking enhancements

- **MAC address cloning**: You can now use MAC address cloning to enhance the security of certain environments. MAC address cloning enables you to use a dedicated virtual NIC for the Grid Network, Admin Network, and Client Network. Having the Docker container use the MAC address of the dedicated NIC on the host allows you to avoid using promiscuous mode network configurations. Three new MAC address cloning keys were added to the node configuration file for Linux-based (bare metal) nodes.
- **Automatic discovery of DNS and NTP host routes**: Previously, there were restrictions on which network your NTP and DNS servers had to connect to, such as the requirement that you could not have all of your NTP and DNS servers on the Client Network. Now, those restrictions are removed.

Learn more

- Install Red Hat Enterprise Linux or CentOS
- Install Ubuntu or Debian

Support for rebalancing erasure-coded (EC) data after Storage Node expansion

The EC rebalance procedure is a new command-line script that might be required after you add new Storage Nodes. When you perform the procedure, StorageGRID redistributes erasure-coded fragments among the existing and the newly expanded Storage Nodes at a site.

> You should only perform the EC rebalance procedure in limited cases. For example, if you cannot add the recommended number of Storage Nodes in an expansion, you can use the EC rebalance procedure to allow additional erasure-coded objects to be stored.

Learn more

- Expand your grid

New and revised maintenance procedures

- **Site decommission**: You can now remove an operational site from your StorageGRID system. The connected site decommission procedure removes an operational site and preserves data. The new Decommission Site wizard guides you through the process (**Maintenance** > **Decommission** > **Decommission Site**).
- **Appliance node cloning**: You can now clone an existing appliance node to upgrade the node to a new appliance model. For example, you can clone a smaller-capacity appliance node to a larger-capacity appliance. You can also clone an appliance node to implement new functionality, such as the new **Node Encryption** setting that is required for the KMS encryption.
- **Ability to change the provisioning passphrase**: You can now change the provisioning passphrase (**Configuration** > **Access Control** > **Grid Passwords**). The passphrase is required for recovery, expansion, and maintenance procedures.
- **Enhanced SSH password behavior**: To enhance the security of StorageGRID appliances, the SSH password is no longer changed when you place an appliance into maintenance mode. In addition, new SSH host certificates and host keys are generated when you upgrade a node to StorageGRID 11.5.

If you use SSH to log in to a node after upgrading to StorageGRID 11.5, you will receive a warning that the host key has changed. This behavior is expected and you can safely approve the new key.

Learn more

- Maintain & recover

Changes to StorageGRID appliances

- **Direct access to SANtricity System Manager for storage appliances**: You can now access the E-Series SANtricity System Manager user interface from the StorageGRID Appliance Installer and from the Grid Manager. Using these new methods enables access to SANtricity System Manager without using the management port on the appliance. Users who need to access SANtricity System Manager from the Grid Manager must have the new Storage Appliance Administrator permission.
- **Node encryption**: As part of the new KMS encryption feature, a new **Node Encryption** setting was added to the StorageGRID Appliance Installer. If you want to use encryption key management to protect appliance data, you must enable this setting during the hardware configuration stage of appliance installation.
- **UDP port connectivity**: You can now test the network connectivity of a StorageGRID appliance to UDP ports, such as those used for an external NFS or DNS server. From the StorageGRID Appliance Installer, select **Configure Networking** > **Port Connectivity Test (nmap)**.
- **Automating installation and configuration**: A new JSON configuration upload page was added to the StorageGRID Appliance Installer (**Advanced** > **Update Appliance Configuration**). This page enables you to use one file to configure multiple appliances in large grids. Additionally, the `configure-sga.py` Python script has been updated to match the capabilities of the StorageGRID Appliance Installer.

Learn more

- SG100 & SG1000 services appliances
- SG6000 storage appliances
- SG5700 storage appliances
- SG5600 storage appliances

Changes to audit messages

- **Automatic cleanup of overwritten objects**: Previously, objects that were overwritten were not removed from disk in specific cases, which resulted in additional space consumption. These overwritten objects, which are inaccessible to users, are now automatically removed to save storage space. Refer to the LKCU audit message for more information.
- **New audit codes for S3 Object Lock**: Four new audit codes were added to the SPUT audit message to include S3 Object Lock request headers:
  - LKEN: Object Lock Enabled
  - LKLH: Object Lock Legal Hold
  - LKMD: Object Lock Retention Mode
  - LKRU: Object Lock Retain Until Date
- **New fields for Last Modified Time and Previous Object Size**: You can now track when an object was overwritten as well as the original object size.
  - The MTME (Last Modified Time) field was added to the following audit messages:

        - SDEL (S3 DELETE)
        - SPUT (S3 PUT)
        - WDEL (Swift DELETE)
        - WPUT (Swift PUT)
    - The CSIZ (Previous Object Size) field was added to the OVWR (Object Overwrite) audit message.

Learn more

- Review audit logs

New nms.requestlog file

A new log file, `/var/local/log/nms.requestlog`, is maintained on all Admin Nodes. This file contains information about outgoing connections from the Management API to internal StorageGRID services.

Learn more

- Monitor & troubleshoot

StorageGRID documentation changes

- To make networking information and requirements easier to find and to clarify that the information also applies to StorageGRID appliance nodes, the networking documentation was moved from the software-based installation guides (RedHat Enterprise Linux/CentOS, Ubuntu/Debian, and VMware) to a new networking guide.

  Network guidelines

- To make ILM-related instructions and examples easier to find, the documentation for managing objects with information lifecycle management was moved from the *Administrator Guide* to a new ILM guide.

  Manage objects with ILM

- A new FabricPool guide provides an overview of configuring StorageGRID as a NetApp FabricPool cloud tier and describes the best practices for configuring ILM and other StorageGRID options for a FabricPool workload.

  Configure StorageGRID for FabricPool

- You can now access several instructional videos from the Grid Manager. The current videos provide instructions for managing alerts, custom alerts, ILM rules, and ILM policies.

Removed or deprecated features

Some features were removed or deprecated in StorageGRID 11.5. You must review these items to understand whether you need to update client applications or modify your configuration before you upgrade.

Weak consistency control removed

The Weak consistency control was removed for StorageGRID 11.5. After you upgrade, the following behaviors will apply:

- Requests to set Weak consistency for an S3 bucket or Swift container will succeed, but the consistency

level will actually be set to Available.

- Existing buckets and containers that use Weak consistency will be silently updated to use Available consistency.
- Requests that have a Weak consistency-control header will actually use Available consistency, if applicable.

The Available consistency control behaves the same as the “read-after-new-write” consistency level, but only provides eventual consistency for HEAD operations. The Available consistency control offers higher availability for HEAD operations than “read-after-new-write” if Storage Nodes are unavailable.

Alarm for grid health deprecated

The `/grid/health/topology` API, which checks for active *alarms* on nodes, is deprecated. In its place, a new `/grid/node-health` endpoint was added. This API returns the current status of each node by checking for active *alerts* on nodes.

Compliance feature deprecated

The S3 Object Lock feature in StorageGRID 11.5 replaces the Compliance feature that was available in previous StorageGRID versions. Because the new S3 Object Lock feature conforms to Amazon S3 requirements, it deprecates the proprietary StorageGRID Compliance feature, which is now referred to as “legacy Compliance.”

If you previously enabled the global Compliance setting, the new global S3 Object Lock setting is enabled automatically when you upgrade to StorageGRID 11.5. Tenant users will no longer be able to create new buckets with Compliance enabled in StorageGRID; however, as required, tenant users can continue to use and manage any existing legacy Compliant buckets.

In the Tenant Manager, a shield icon indicates a legacy Compliant bucket. Legacy Compliant buckets might also have a hold badge HOLD to indicate that the bucket is under a legal hold.

KB: How to manage legacy Compliant buckets in StorageGRID 11.5

Manage objects with ILM

“S3 multipart part too small” alert removed

The **S3 multipart part too small** alert was removed. Previous, this alert was triggered if an S3 client attempted to complete a multipart upload with parts that did not meet Amazon S3 size limits. After the upgrade to StorageGRID 11.5, any multipart upload requests that do not meet the following size limits will fail:

- Each part in a multipart upload must be between 5 MiB (5,242,880 bytes) and 5 GiB (5,368,709,120 bytes).
- The last part can be smaller than 5 MiB (5,242,880 bytes).
- In general, part sizes should be as large as possible. For example, use part sizes of 5 GiB for a 100 GiB object. Since each part is considered a unique object, using large part sizes reduces StorageGRID metadata overhead.
- For objects smaller than 5 GiB, consider using non-multipart upload instead.

"Appliance link down on Grid Network" alerts removed

The following alerts were removed. If the Grid Network is down, the metrics that would trigger these alerts are not accessible:

- Services appliance link down on Grid Network
- Storage appliance link down on Grid Network

Support for fully qualified domain name removed from SNMP configuration

When configuring an SNMP server in the baseboard management controller (BMC) for the SG6000, SG100, or SG1000, you must now specify an IP address instead of a fully qualified domain name. If a fully qualified domain name was previously configured, change it to an IP address before upgrading to StorageGRID 11.5.

Legacy attributes removed

The following legacy attributes were removed. As applicable, equivalent information is provided by Prometheus metrics:

Legacy attribute	Equivalent Prometheus metric
BREC	storagegrid_service_network_received_bytes
BTRA	storagegrid_service_network_transmitted_bytes
CQST	storagegrid_metadata_queries_average_latency_milliseconds
HAIS	storagegrid_http_sessions_incoming_attempted
HCCS	storagegrid_http_sessions_incoming_currently_established
HEIS	storagegrid_http_sessions_incoming_failed
HISC	storagegrid_http_sessions_incoming_successful
LHAC	*none*
NREC	*none*
NTSO (Chosen Time Source Offset)	storagegrid_ntp_chosen_time_source_offset_milliseconds
NTRA	*none*
SLOD	storagegrid_service_load
SMEM	storagegrid_service_memory_usage_bytes
SUTM	storagegrid_service_cpu_seconds
SVUT	storagegrid_service_uptime_seconds

Legacy attribute	Equivalent Prometheus metric
TRBS (Total bits per second received)	*none*
TRXB	storagegrid_network_received_bytes
TTBS (Total bits per second transmitted)	*none*
TTXB	storagegrid_network_transmitted_bytes

The following related changes were also made:

- The `network_received_bytes` and `network_transmitted_bytes` Prometheus metrics were changed from gauges to counters because the values of these metrics only increase. If you are currently using these metrics in Prometheus queries, you should start using the `increase()` function in the query.
- The Network Resources table was removed from the Resources tab for StorageGRID services. (Select **Support** > **Tools** > **Grid Topology**.Then, select ***node*** > ***service*** > **Resources**.)
- The HTTP Sessions page was removed for Storage Nodes. Previously, you could access this page by selecting **Support** > **Tools** > **Grid Topology** and then selecting ***Storage Node*** > **LDR** > **HTTP**.
- The HCCS (Currently Established Incoming Sessions) alarm was removed.
- The NTSO (Chosen Time Source Offset) alarm was removed.

Changes to the Grid Management API

StorageGRID 11.5 uses version 3 of the Grid Management API. Version 3 deprecates version 2; however, version 1 and version 2 are still supported.

> You can continue to use version 1 and version 2 of the management API with StorageGRID 11.5; however, support for these versions of the API will be removed in a future release of StorageGRID. After upgrading to StorageGRID 11.5, the deprecated v1 and v2 APIs can be deactivated using the `PUT /grid/config/management` API.

New client-certificates section

The new section, `/grid/client-certificates`, allows you to configure client certificates to provide secure, authenticated access to the StorageGRID Prometheus database. For example, you can monitor StorageGRID externally using Grafana.

Legacy compliance endpoints moved to new s3-object-lock section

With the introduction of StorageGRID S3 Object Lock, the APIs used to manage the legacy compliance settings for the grid were moved to a new section of the Swagger user interface. The **s3-object-lock** section includes the two `/grid/compliance-global` API endpoints, which now control the global S3 Object Lock setting. The endpoint URIs remain unchanged for compatibility with existing applications.

Swift-admin-password Accounts endpoint removed

The following Accounts API endpoint, which was deprecated in StorageGRID 10.4, has now been removed:

```
https://<IP-Address>/api/v1/grid/accounts/<AccountID>/swift-admin-password
```

New grid-passwords section

The **grid-passwords** section enables operations for grid password management. The section includes two `/grid/change-provisioning-passphrase` API endpoints. The endpoints allow users to change the StorageGRID provisioning passphrase and retrieve the status of the passphrase change.

storageAdmin permission added to Groups API

The `/grid/groups` API now includes the storageAdmin permission.

New parameter for Storage Usage API

The `GET /grid/accounts/{id}/usage` API now has a `strictConsistency` parameter. To enforce a strong-global consistency when retrieving storage usage information across Storage Nodes, set this parameter to `true`. When this parameter is set to `false` (default), StorageGRID attempts to retrieve usage information using strong-global consistency, but falls back to strong-site consistency if strong-global consistency cannot be met.

New Node Health API

A new `/grid/node-health` endpoint was added. This API returns the current status of each node by checking for active *alerts* on the nodes. The `/grid/health/topology` API, which checks for active *alarms* on nodes, is deprecated.

Change to "ApplianceStorageShelvesPowerSupplyDegraded" alert rule ID

The alert rule ID "ApplianceStorageShelvesPowerSupplyDegraded" has been renamed to "ApplianceStorageShelvesDegraded" to better reflect the alert's actual behavior.

Related information

Administer StorageGRID

Changes to the Tenant Management API

StorageGRID 11.5 uses version 3 of the Tenant Management API. Version 3 deprecates version 2; however, version 1 and version 2 are still supported.

> You can continue to use version 1 and version 2 of the management API with StorageGRID 11.5; however, support for these versions of the API will be removed in a future release of StorageGRID. After upgrading to StorageGRID 11.5, the deprecated v1 and v2 APIs can be deactivated using the `PUT /grid/config/management` API.

New parameter for tenant Storage Usage API

The `GET /org/usage` API now has a `strictConsistency` parameter. To enforce a strong-global consistency when retrieving storage usage information across Storage Nodes, set this parameter to `true`.

When this parameter is set to `false` (default), StorageGRID attempts to retrieve usage information using strong-global consistency, but falls back to strong-site consistency if strong-global consistency cannot be met.

Related information

Use S3

Use a tenant account

Upgrade planning and preparation

You must plan the upgrade of your StorageGRID system to ensure that the system is ready for the upgrade, and that the upgrade can be completed with minimal disruption.

Steps

1. Estimating the time to complete an upgrade
2. How your system is affected during the upgrade
3. Impact of an upgrade on groups and user accounts
4. Verifying the installed version of StorageGRID
5. Obtaining the required materials for a software upgrade
6. Downloading the StorageGRID upgrade files
7. Downloading the Recovery Package
8. Checking the system's condition before upgrading software

Estimating the time to complete an upgrade

When planning an upgrade to StorageGRID 11.5, you must consider when to upgrade, based on how long the upgrade might take. You must also be aware of which operations you can and cannot perform during each stage of the upgrade.

About this task

The time required to complete a StorageGRID upgrade depends on a variety of factors such as client load and hardware performance.

The table summarizes the main upgrade tasks and lists the approximate time required for each task. The steps after the table provide instructions you can use to estimate the upgrade time for your system.

> During the upgrade from StorageGRID 11.4 to 11.5, Cassandra database tables on Storage Nodes will be upgraded. The **Upgrade Database** task occurs in the background, but might require an extensive amount of time to complete. While the database is being upgraded, you can safely use new features, apply hotfixes, and perform node recovery operations. However, you might be prevented from performing other maintenance procedures.

> If an expansion is urgently required, perform the expansion before upgrading to 11.5.

Upgrade task	Description	Approximate time required	During this task
Start Upgrade Service	Upgrade prechecks are run, the software file is distributed, and the upgrade service is started.	3 minutes per grid node, unless validation errors are reported	As required, you can run the upgrade prechecks manually before the scheduled upgrade maintenance window.
Upgrade Grid Nodes (primary Admin Node)	The primary Admin Node is stopped, upgraded, and restarted.	Up to 30 minutes	You cannot access the primary Admin Node. Connection errors are reported, which you can ignore.
Upgrade Grid Nodes (all other nodes)	The software on all other grid nodes is upgraded, in the order in which you approve the nodes. Every node in your system will be brought down one at a time for several minutes each.	15 to 45 minutes per node, with appliance Storage Nodes requiring the most time **Note:** For appliance nodes, the StorageGRID Appliance Installer is automatically updated to the latest release.	• Do not change the grid configuration. • Do not change the audit level configuration. • Do not update the ILM configuration. • Do not perform another maintenance procedure, such as hotfix, decommission, or expansion. **Note:** If you need to perform a recovery procedure, contact technical support.
Enable Features	The new features for the new version are enabled.	Less than 5 minutes	• Do not change the grid configuration. • Do not change the audit level configuration. • Do not update the ILM configuration. • Do not perform another maintenance procedure.

Upgrade task	Description	Approximate time required	During this task
Upgrade Database	Cassandra database tables, which exist on all Storage Nodes, are upgraded.	Hours or days, based on the amount of metadata in your system	During the **Upgrade Database** task, the upgraded grid will operate normally; however, the upgrade will still be in progress. During this task, you can: • Use the new features in the new StorageGRID version. • Change the audit level configuration. • Update the ILM configuration. • Apply a hotfix. • Recover a node. **Note:** You cannot perform a decommission or expansion procedure until the **Final Upgrade Steps** complete.
Final Upgrade Steps	Temporary files are removed and the upgrade to the new release completes.	5 minutes	When the **Final Upgrade Steps** task completes, you can perform all maintenance procedures.

Steps

1. Estimate the time required to upgrade all grid nodes (consider all upgrade tasks except for **Upgrade Database**).
   a. Multiply the number of nodes in your StorageGRID system by 30 minutes/node (average).
   b. Add 1 hour to this time to account for the time required to download the `.upgrade` file, run precheck validations, and complete the final upgrade steps.
2. If you have Linux nodes, add 15 minutes for each node to account for the time required to download and install the RPM or DEB package.
3. Estimate the time required to upgrade the database.
   a. From the Grid Manager, select **Nodes**.
   b. Select the first entry in the tree (entire grid), and select the **Storage** tab.
   c. Hover your cursor over the **Storage Used - Object Metadata** chart, and locate the **Used** value, which indicates how many bytes of object metadata are on your grid.
   d. Divide the **Used** value by 1.5 TB/day to determine how many days will be needed to upgrade the database.

4. Calculate the total estimated time for the upgrade by adding the results of steps 1, 2, and 3.

Example: Estimating the time to upgrade from StorageGRID 11.4 to 11.5

Suppose your system has 14 grid nodes, of which 8 are Linux nodes. Also, assume that the **Used** value for object metadata is 6 TB.

1. Multiply 14 by 30 minutes/node and add 1 hour. The estimated time to upgrade all nodes is 8 hours.
2. Multiple 8 by 15 minutes/node to account for the time to install the RPM or DEB package on the Linux nodes. The estimated time for this step is 2 hours.
3. Divide 6 by 1.5 TB/day. The estimated number of days for the **Upgrade Database** task is 4 days.

> While the **Upgrade Database** task is running, you can safely use new features, apply hotfixes, and perform node recovery operations.

4. Add the values together. You should allow 5 days to complete the upgrade of your system to StorageGRID 11.5.0.

How your system is affected during the upgrade

You must understand how your StorageGRID system will be affected during the upgrade.

StorageGRID upgrades are non-disruptive

The StorageGRID system can ingest and retrieve data from client applications throughout the upgrade process. Grid nodes are brought down one at a time during the upgrade, so there is not a time when all grid nodes are unavailable.

To allow for continued availability, you must ensure that objects are stored redundantly using the appropriate ILM policies. You must also ensure that all external S3 or Swift clients are configured to send requests to one of the following:

- A StorageGRID endpoint configured as a high availability (HA) group
- A high availability third-party load balancer
- Multiple Gateway Nodes for each client
- Multiple Storage Nodes for each client

Appliance firmware is upgraded

During the StorageGRID 11.5 upgrade:

- All StorageGRID appliance nodes are automatically upgraded to StorageGRID Appliance Installer firmware version 3.5.
- SG6060 and SGF6024 appliances are automatically upgraded to BIOS firmware version 3B03.EX and BMC firmware version BMC 3.90.07.
- SG100 and SG1000 appliances are automatically upgraded to BIOS firmware version 3B08.EC and BMC firmware version 4.64.07.

Alerts might be triggered

Alerts might be triggered when services start and stop and when the StorageGRID system is operating as a

mixed-version environment (some grid nodes running an earlier version, while others have been upgraded to a later version). For example, you might see the **Unable to communicate with node** alert when services are stopped, or you might see the **Cassandra communication error** alert when some nodes have been upgraded to StorageGRID 11.5 but other nodes are still running StorageGRID 11.4.

In general, these alerts will clear when the upgrade completes.

After the upgrade completes, you can review any upgrade-related alerts by selecting **Recently resolved alerts** from the Grid Manager Dashboard.

> During the upgrade to StorageGRID 11.5, the **ILM placement unachievable** alert might be triggered when Storage Nodes are stopped. This alert might persist for 1 day after the upgrade is completed successfully.

Many SNMP notifications are generated

Be aware that a large number of SNMP notifications might be generated when grid nodes are stopped and restarted during the upgrade. To avoid excessive notifications, unselect the **Enable SNMP Agent Notifications** check box (**Configuration** > **Monitoring** > **SNMP Agent**) to disable SNMP notifications before you start the upgrade. Then, re-enable notifications after the upgrade is complete.

Configuration changes are restricted

Until the **Enable New Feature** task completes:

- Do not make any grid configuration changes.
- Do not change the audit level configuration.
- Do not enable or disable any new features.
- Do not update the ILM configuration. Otherwise, you might experience inconsistent and unexpected ILM behavior.
- Do not apply a hotfix or recover a grid node.

Until the **Final Upgrade Steps** task completes:

- Do not perform an expansion procedure.
- Do not perform a decommission procedure.

Impact of an upgrade on groups and user accounts

You must understand the impact of the StorageGRID upgrade, so that you can update groups and user accounts appropriately after the upgrade is complete.

Changes to group permissions and options

After upgrading to StorageGRID 11.5, optionally select the following new permissions and options (**Configuration** > **Access Control** > **Admin Groups**).

Permission or option	Description
Storage Appliance Administrator	Required to access the SANtricity System Manager user interface from Grid Manager.

Permission or option	Description
Access Mode	When managing groups, you can select **Read-only** for this new option to prevent users from changing the settings and features that are selected for the group. Users in groups with read-only access mode can view settings, but they cannot change them.

Related information

Administer StorageGRID

Verifying the installed version of StorageGRID

Before starting the upgrade, you must verify that the previous version of StorageGRID is currently installed with the latest available hotfix applied.

Steps

1. Sign in to the Grid Manager using a supported browser.
2. Select **Help** > **About**.
3. Verify that the **Version** is 11.4.*x.y*.

   In the StorageGRID 11.4.*x.y* version number:

   - The major release has an *x* value of 0 (11.4.0).
   - A minor release, if available, has an *x* value other than 0 (for example, 11.4.1).
   - A hotfix, if available, has a *y* value (for example, 11.4.0.1).

   > If you have an earlier version of StorageGRID, you must upgrade to any 11.4 version before upgrading to StorageGRID 11.5. You do not need to be at the highest 11.4 minor-version release to upgrade to StorageGRID 11.5.

4. If you are not at a StorageGRID 11.4 version you must upgrade to version 11.4, one release at a time, using the instructions for each release.

   You must also apply the latest hotfix for each StorageGRID version before upgrading to the next level.

   One possible upgrade path is shown in the example.

5. Once you are at StorageGRID 11.4, go to the NetApp Downloads page for StorageGRID and see if any hotfixes are available for your StorageGRID 11.4.*x* version.

   NetApp Downloads: StorageGRID

6. Verify that your StorageGRID 11.4.*x* version has the latest hotfix applied.
7. If necessary, download and apply the latest StorageGRID 11.4.*x.y* hotfix for your StorageGRID 11.4.*x* version.

   See the recovery and maintenance instructions for information about applying hotfixes.

Example: Preparing to upgrade to StorageGRID 11.5 from version 11.3.0.8

The following example shows the upgrade steps to prepare for an upgrade from StorageGRID version 11.3.0.8 to version 11.5. Before you can upgrade to StorageGRID 11.5, your system must have a StorageGRID 11.4 version installed with the latest hotfix.

Download and install software in the following sequence to prepare your system for upgrade:

1. Apply the latest StorageGRID 11.3.0.*y* hotfix.
2. Upgrade to the StorageGRID 11.4.0 major release. (You do not need to install any 11.4.*x* minor releases.)
3. Apply the latest StorageGRID 11.4.0.*y* hotfix.

Related information

Administer StorageGRID

Maintain & recover

Obtaining the required materials for a software upgrade

Before you begin the software upgrade, you must obtain all required materials so you can complete the upgrade successfully.

Item	Notes
StorageGRID upgrade files	You must download the required files to your service laptop: • **All platforms**: `.upgrade` file • **Any node on Red Hat Enterprise Linux or CentOS**: `.upgrade` file and RPM file (`.zip` or `.tgz`) • **Any node on Ubuntu or Debian**: `.upgrade` file and DEB file (`.zip` or `.tgz`)
Service laptop	The service laptop must have: • Network port • SSH client (for example, PuTTY)
Supported web browser	You must confirm that the web browser on the service laptop is supported for use with StorageGRID 11.5. Web browser requirements **Note:** Browser support has changed for StorageGRID 11.5. Confirm you are using a supported version.

Item	Notes
Recovery Package (`.zip`) file	Before upgrading, you should download the most recent Recovery Package file in case any problems occur during the upgrade. After you upgrade the primary Admin Node, you must download a new copy of the Recovery Package file and save it in a safe location. The updated Recovery Package file allows you to restore the system if a failure occurs. Downloading the Recovery Package
`Passwords.txt` file	This file is included in the SAID package, which is part of the Recovery Package `.zip` file. You must obtain the latest version of the Recovery Package.
Provisioning passphrase	The passphrase is created and documented when the StorageGRID system is first installed. The provisioning passphrase is not listed in the `Passwords.txt` file.
Related documentation	• Release notes for StorageGRID 11.5. Be sure to read these carefully before starting the upgrade. • Instructions for administering StorageGRID • If you are upgrading a Linux deployment, the StorageGRID installation instructions for your Linux platform. • Other StorageGRID documentation, as required.

Related information

Web browser requirements

Administer StorageGRID

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

Install VMware

Downloading the StorageGRID upgrade files

Downloading the Recovery Package

Release notes

Web browser requirements

You must use a supported web browser.

Web browser	Minimum supported version
Google Chrome	87

Web browser	Minimum supported version
Microsoft Edge	87
Mozilla Firefox	84

You should set the browser window to a recommended width.

Browser width	Pixels
Minimum	1024
Optimum	1280

Downloading the StorageGRID upgrade files

You must download the required files to a service laptop before you upgrade your StorageGRID system.

What you'll need

You must have installed all required hotfixes for the StorageGRID software version you are upgrading. See the hotfix procedure in the recovery and maintenance instructions.

About this task

You must download the `.upgrade` archive for any platform. If any nodes are deployed on Linux hosts, you must also download an RPM or DEB archive, which you will install before you start the upgrade.

Steps

1. Go to the NetApp Downloads page for StorageGRID.

   NetApp Downloads: StorageGRID

2. Select the button for downloading the latest release, or select another version from the drop-down menu and select **Go**.

   StorageGRID software versions have this format: 11.*x.y*. StorageGRID hotfixes have this format: 11.*x.y.z*.

3. Sign in with the username and password for your NetApp account.
4. If a Caution/MustRead statement appears, read it and select the check box.

   This statement appears if there is a required hotfix for the release.

5. Read the End User License Agreement, select the check box, and then select **Accept & Continue**.

   The downloads page for the version you selected appears. The page contains three columns:

   - Install StorageGRID
   - Upgrade StorageGRID
   - Support files for StorageGRID Appliances

6. In the **Upgrade StorageGRID** column, select and download the `.upgrade` archive.

   Every platform requires the `.upgrade` archive.

7. If any nodes are deployed on Linux hosts, also download the RPM or DEB archive in either `.tgz` or `.zip` format.

   You must install the RPM or DEB archive on all Linux nodes before you start the upgrade.

   > No additional files are required for the SG100 or SG1000.

   > Select the `.zip` file if you are running Windows on the service laptop.

   - Red Hat Enterprise Linux or CentOS
     `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip`
     `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
   - Ubuntu or Debian
     `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip`
     `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

Related information

Linux: Installing the RPM or DEB package on all hosts

Maintain & recover

Downloading the Recovery Package

The Recovery Package file allows you to restore the StorageGRID system if a failure occurs.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have the provisioning passphrase.
- You must have specific access permissions.

About this task

Download the current Recovery Package file before making grid topology changes to the StorageGRID system or before upgrading software. Then, download a new copy of the Recovery Package after making grid topology changes or after upgrading software.

Steps

1. Select **Maintenance** > **System** > **Recovery Package**.
2. Enter the provisioning passphrase, and select **Start Download**.

   The download starts immediately.

3. When the download completes:
   a. Open the `.zip` file.

b. Confirm it includes a `gpt-backup` directory and an inner `.zip` file.

c. Extract the inner `.zip` file.

d. Confirm you can open the `Passwords.txt` file.

4. Copy the downloaded Recovery Package file (`.zip`) to two safe, secure, and separate locations.

> The Recovery Package file must be secured because it contains encryption keys and passwords that can be used to obtain data from the StorageGRID system.

Related information

Administer StorageGRID

Checking the system's condition before upgrading software

Before upgrading a StorageGRID system, you must verify the system is ready to accommodate the upgrade. You must ensure that the system is running normally and that all grid nodes are operational.

Steps

1. Sign in to the Grid Manager using a supported browser.
2. Check for and resolve any active alerts.

   For information about specific alerts, see the monitoring and troubleshooting instructions.

3. Confirm that no conflicting grid tasks are active or pending.

   a. Select **Support** > **Tools** > **Grid Topology**.

   b. Select ***site*** > ***primary Admin Node*** > **CMN** > **Grid Tasks** > **Configuration**.

      Information lifecycle management evaluation (ILME) tasks are the only grid tasks that can run concurrently with the software upgrade.

   c. If any other grid tasks are active or pending, wait for them to finish or release their lock.

      > Contact technical support if a task does not finish or release its lock.

4. Refer to the lists of internal and external ports in the 11.5 version of the networking guidelines, and ensure that all required ports are opened before you upgrade.

   > If you have opened any custom firewall ports, you are notified during the upgrade precheck. You must contact technical support before proceeding with the upgrade.

Related information

Monitor & troubleshoot

Administer StorageGRID

Maintain & recover

Network guidelines

Performing the upgrade

The Software Upgrade page guides you through the process of uploading the required file and upgrading all of the grid nodes in your StorageGRID system.

What you'll need

You are aware of the following:

- You must upgrade all grid nodes for all data center sites from the primary Admin Node, using the Grid Manager.
- To detect and resolve issues, you can manually run the upgrade prechecks before starting the actual upgrade. The same prechecks are performed when you start the upgrade. Precheck failures will stop the upgrade process and might require technical support involvement to resolve.
- When you start the upgrade, the primary Admin Node is upgraded automatically.
- After the primary Admin Node has been upgraded, you can select which grid nodes to upgrade next.
- You must upgrade all grid nodes in your StorageGRID system to complete the upgrade, but you can upgrade individual grid nodes in any order. You can select individual grid nodes, groups of grid nodes, or all grid nodes. You can repeat the process of selecting grid nodes as many times as necessary, until all grid nodes at all sites are upgraded.
- When the upgrade starts on a grid node, the services on that node are stopped. Later, the grid node is rebooted. Do not approve the upgrade for a grid node unless you are sure that node is ready to be stopped and rebooted.
- When all grid nodes have been upgraded, new features are enabled and you can resume operations; however, you must wait to perform a decommission or expansion procedure until the background **Upgrade Database** task and the **Final Upgrade Steps** task have completed.
- You must complete the upgrade on the same hypervisor platform you started with.

Steps

1. Linux: Installing the RPM or DEB package on all hosts
2. Starting the upgrade
3. Upgrading grid nodes and completing the upgrade
4. Increasing the Metadata Reserved Space setting

Related information

Administer StorageGRID

Estimating the time to complete an upgrade

Linux: Installing the RPM or DEB package on all hosts

If any StorageGRID nodes are deployed on Linux hosts, you must install an additional RPM or DEB package on each of these hosts before you start the upgrade.

What you'll need

You must have downloaded one of the following `.tgz` or `.zip` files from the NetApp Downloads page for StorageGRID.

Use the `.zip` file if you are running Windows on the service laptop.

Linux platform	Additional file (choose one)
Red Hat Enterprise Linux or CentOS	• `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.zip` • `StorageGRID-Webscale-`*`version`*`-RPM-`*`uniqueID`*`.tgz`
Ubuntu or Debian	• `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.zip` • `StorageGRID-Webscale-`*`version`*`-DEB-`*`uniqueID`*`.tgz`

Steps

1. Extract the RPM or DEB packages from the installation file.
2. Install the RPM or DEB packages on all Linux hosts.

   See the steps for installing StorageGRID host services in the installation instructions for your Linux platform.

   Install Red Hat Enterprise Linux or CentOS

   Install Ubuntu or Debian

   The new packages are installed as additional packages. Do not remove the existing packages.

Starting the upgrade

When you are ready to perform the upgrade, you select the downloaded file and enter the provisioning passphrase. As an option, you can run the upgrade prechecks before performing the actual upgrade.

What you'll need

You have reviewed all of the considerations and completed all steps in Upgrade planning and preparation.

Steps

1. Sign in to the Grid Manager using a supported browser.
2. Select **Maintenance** > **System** > **Software Update**.

   The Software Update page appears.

3. Select **StorageGRID Upgrade**.

   The StorageGRID Upgrade page appears and shows the date and time of the most recently completed upgrade, unless the primary Admin Node has been rebooted or the management API restarted since that upgrade was performed.

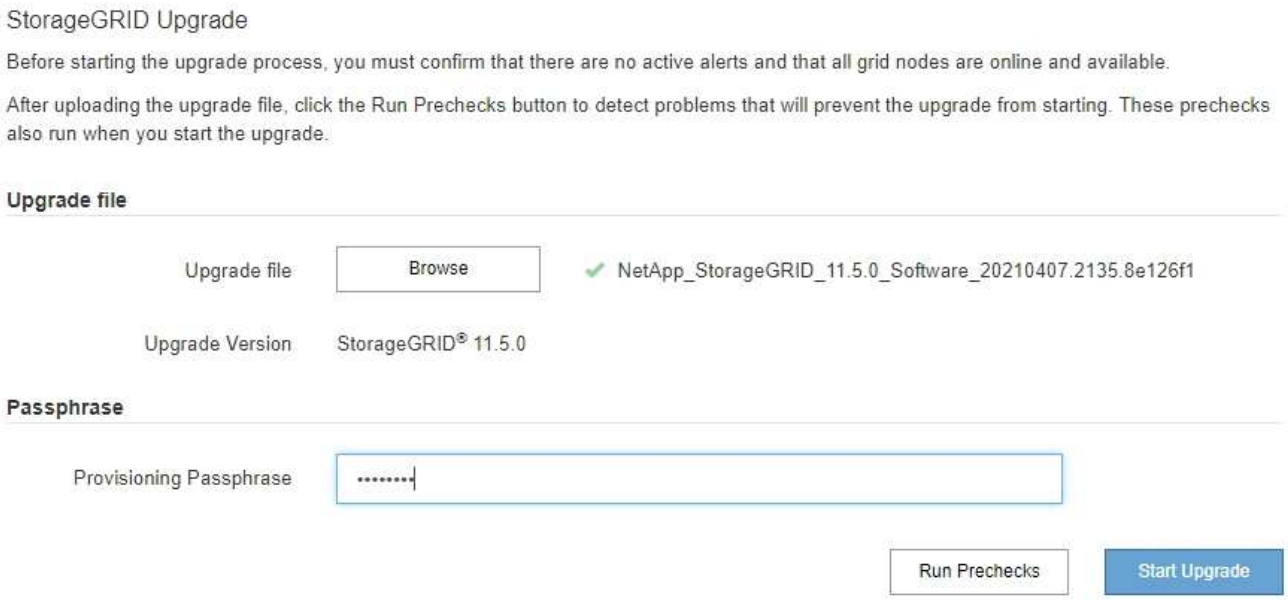
4. Select the `.upgrade` file you downloaded.
   a. Select **Browse**.
   b. Locate and select the file: `NetApp_StorageGRID_version_Software_uniqueID.upgrade`

c. Select **Open**.

The file is uploaded and validated. When the validation process is done, a green checkmark appears next to the upgrade file name.

5. Enter the provisioning passphrase in the text box.

The **Run Prechecks** and **Start Upgrade** buttons become enabled.



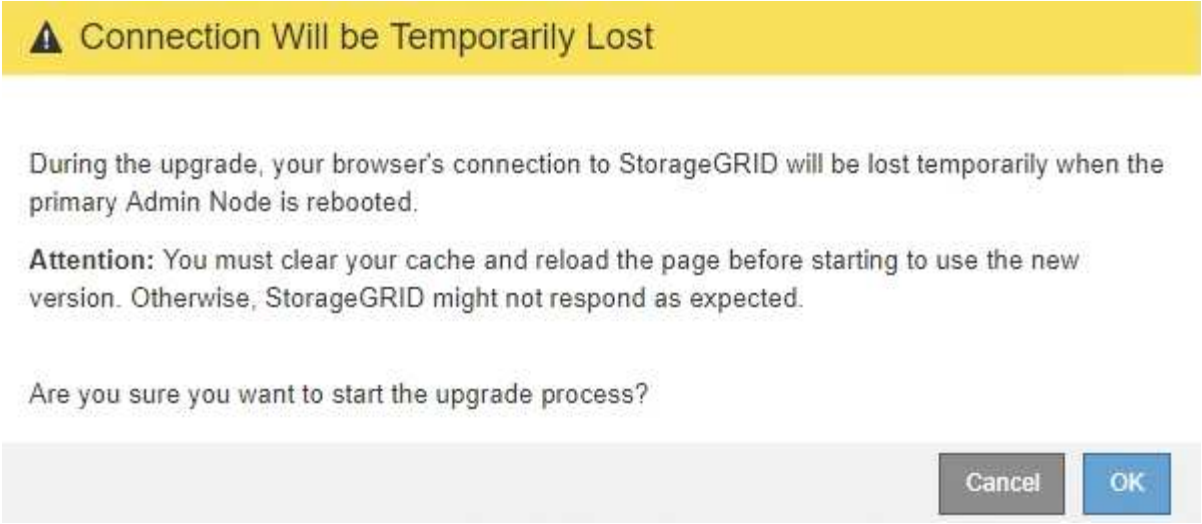
6. If you want to validate the condition of your system before you start the actual upgrade, select **Run Prechecks**. Then, resolve any precheck errors that are reported.

> If you have opened any custom firewall ports, you are notified during the precheck validation. You must contact technical support before proceeding with the upgrade.

> The same prechecks are performed when you select **Start Upgrade**. Selecting **Run Prechecks** allows you to detect and resolve issues before starting the upgrade.

7. When you are ready to perform the upgrade, select **Start Upgrade**.

A warning appears to remind you that your browser's connection will be lost when the primary Admin Node is rebooted. When the primary Admin Node is available again, you need to clear your web browser's cache and reload the Software Upgrade page.



8. Select **OK** to acknowledge the warning and start the upgrade process.

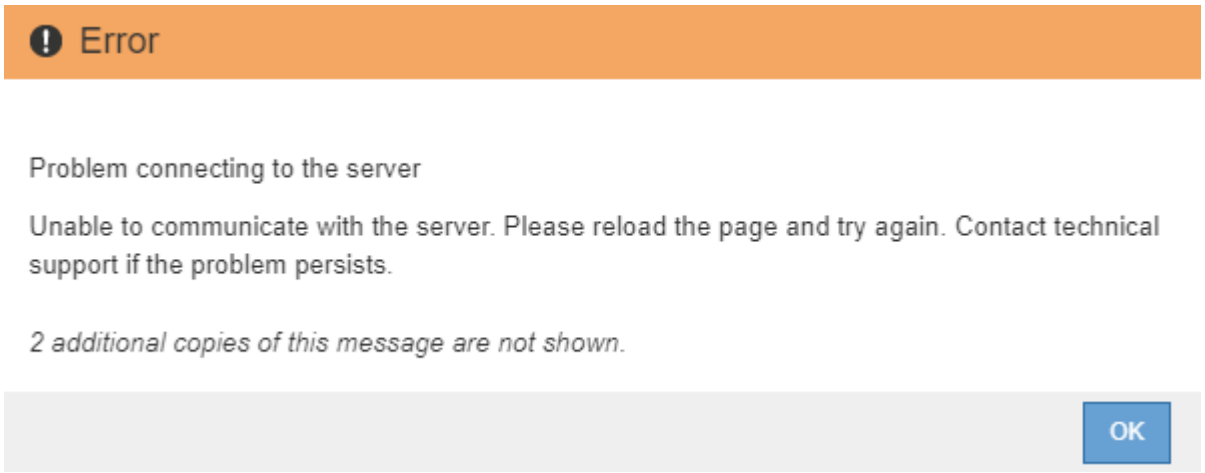
   When the upgrade starts:

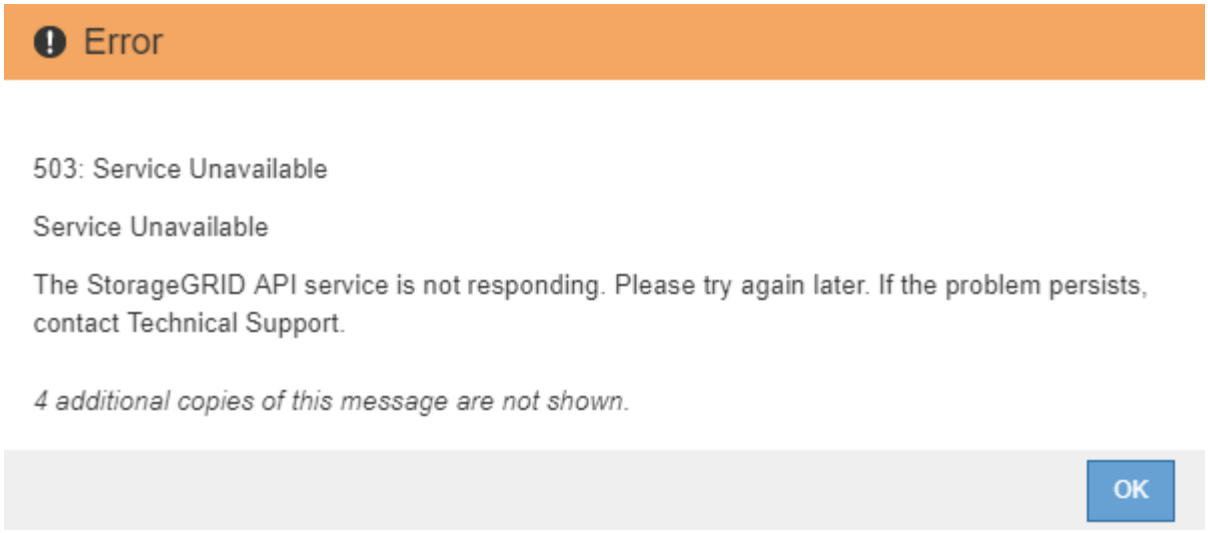
   a. The upgrade prechecks are run.

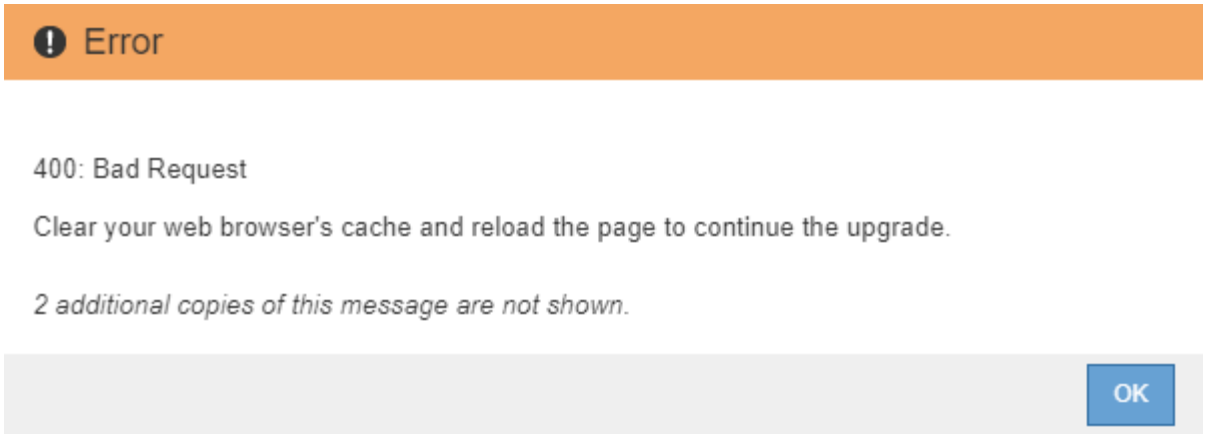
      > If any precheck errors are reported, resolve them and select **Start Upgrade** again.

   b. The primary Admin Node is upgraded, which includes stopping services, upgrading the software, and restarting services. You will not be able to access the Grid Manager while the primary Admin Node is being upgraded. Audit logs will also be unavailable. This upgrade can take up to 30 minutes.

      > While the primary Admin Node is being upgraded, multiple copies of the following error messages appear, which you can ignore.







9. After the primary Admin Node has been upgraded, clear your web browser's cache, sign back in, and reload the Software Upgrade page.

   For instructions, see the documentation for your web browser.

   > You must clear the web browser's cache to remove outdated resources used by the previous version of the software.

Related information

Upgrade planning and preparation

Upgrading grid nodes and completing the upgrade

After the primary Admin Node has been upgraded, you must upgrade all other grid nodes in your StorageGRID system. You can customize the upgrade sequence by selecting to upgrade individual grid nodes, groups of grid nodes, or all grid nodes.

Steps

1. Review the Upgrade Progress section on the Software Upgrade page, which provides information about each major upgrade task.
   a. **Start Upgrade Service** is the first upgrade task. During this task, the software file is distributed to the grid nodes, and the upgrade service is started.

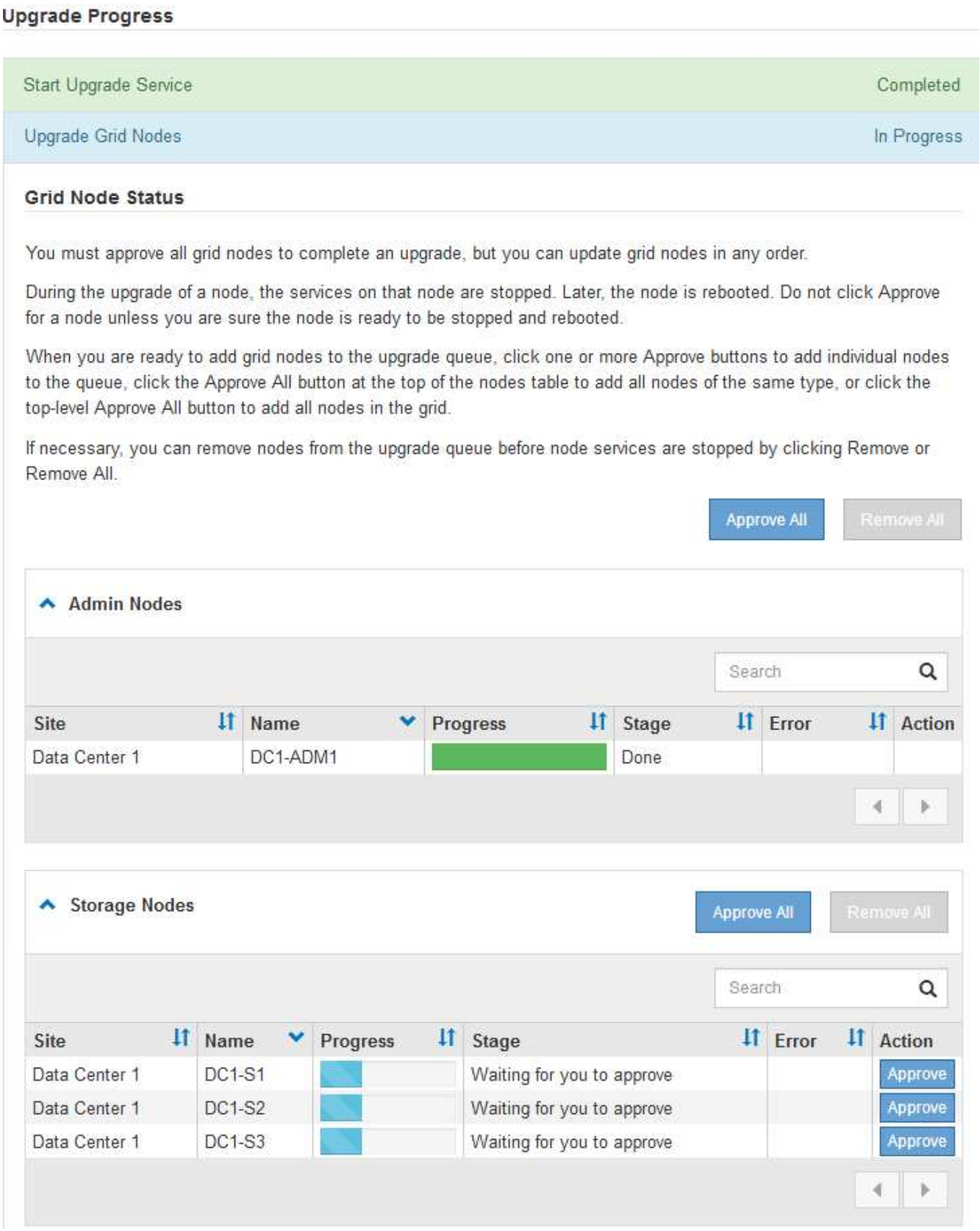
b. When the **Start Upgrade Service** task is complete, the **Upgrade Grid Nodes** task starts.

c. While the **Upgrade Grid Nodes** task is in progress, the Grid Node Status table appears and shows the upgrade stage for each grid node in your system.

2. After the grid nodes appear in the Grid Node Status table, but before approving any grid nodes, download a new copy of the Recovery Package.

> You must download a new copy of the Recovery Package file after you upgrade the software version on the primary Admin Node. The Recovery Package file allows you to restore the system if a failure occurs.

3. Review the information in the Grid Node Status table. Grid nodes are arranged in sections by type: Admin Nodes, API Gateway Nodes, Storage Nodes, and Archive Nodes.



A grid node can be in one of these stages when this page first appears:

- Done (primary Admin Node only)
- Preparing upgrade

- Software download queued
- Downloading
- Waiting for you to approve

4. Approve the grid nodes you are ready to add to the upgrade queue. Approved nodes of the same type are upgraded one at a time.

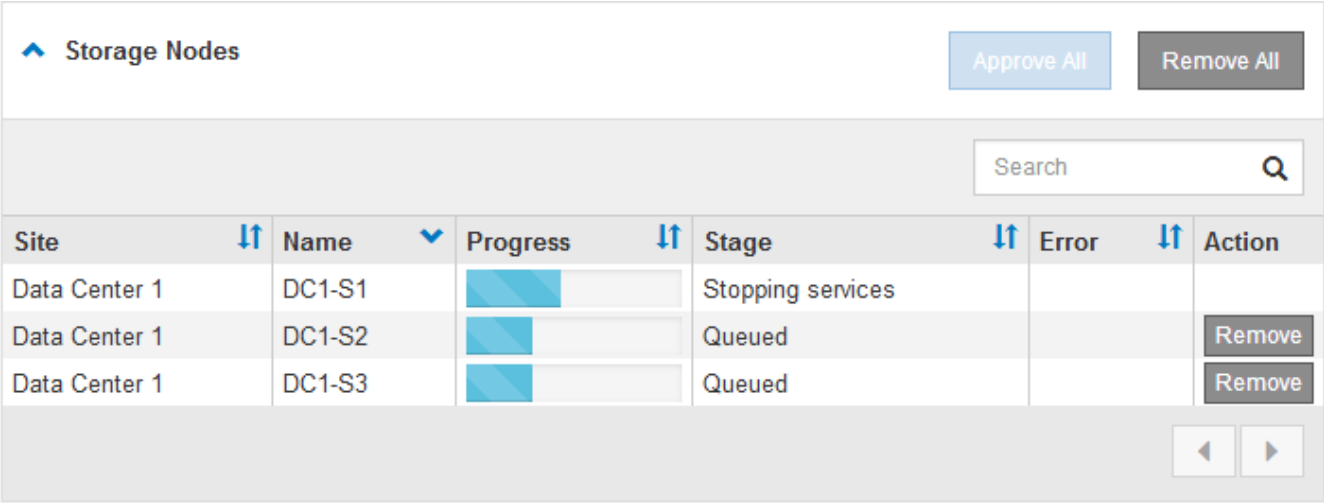
   If the order in which nodes are upgraded is important, approve nodes or groups of nodes one at a time and wait until the upgrade is complete on each node before approving the next node or group of nodes.

   > When the upgrade starts on a grid node, the services on that node are stopped. Later, the grid node is rebooted. These operations might cause service interruptions for clients that are communicating with the node. Do not approve the upgrade for a node unless you are sure that node is ready to be stopped and rebooted.

   - Select one or more **Approve** buttons to add one or more individual nodes to the upgrade queue.
   - Select the **Approve All** button within each section to add all nodes of the same type to the upgrade queue.
   - Select the top-level **Approve All** button to add all nodes in the grid to the upgrade queue.

5. If you need to remove a node or all nodes from the upgrade queue, select **Remove** or **Remove All**.

   As shown in the example, when the Stage reaches **Stopping services**, the **Remove** button is hidden and you can no longer remove the node.



6. Wait for each node to proceed through the upgrade stages, which include Queued, Stopping services, Stopping container, Cleaning up Docker images, Upgrading base OS packages, Rebooting, and Starting services.

   > When an appliance node reaches the Upgrading base OS packages stage, the StorageGRID Appliance Installer software on the appliance is updated. This automated process ensures that the StorageGRID Appliance Installer version remains in sync with the StorageGRID software version.

   When all grid nodes have been upgraded, the **Upgrade Grid Nodes** task is shown as Completed. The remaining upgrade tasks are performed automatically and in the background.

7. As soon as the **Enable Features** task is complete (which occurs quickly), you can start using the new features in the upgraded StorageGRID version.

   For example, if you are upgrading to StorageGRID 11.5, you can now enable S3 Object Lock, configure a key management server, or increase the Metadata Reserved Space setting.

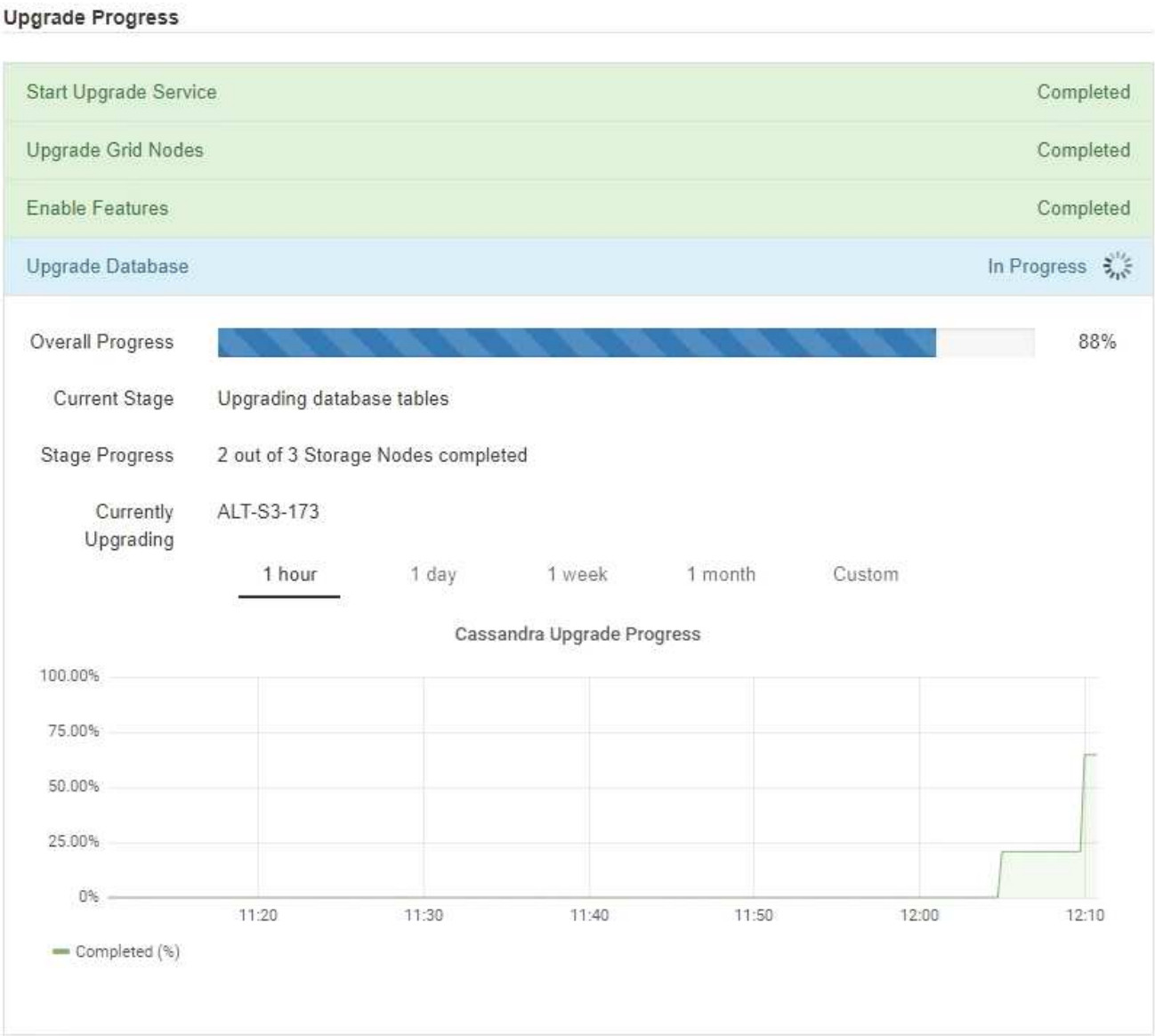
   Increasing the Metadata Reserved Space setting

8. Periodically monitor the progress of the **Upgrade Database** task.

   During this task, the Cassandra database is upgraded on each Storage Node.

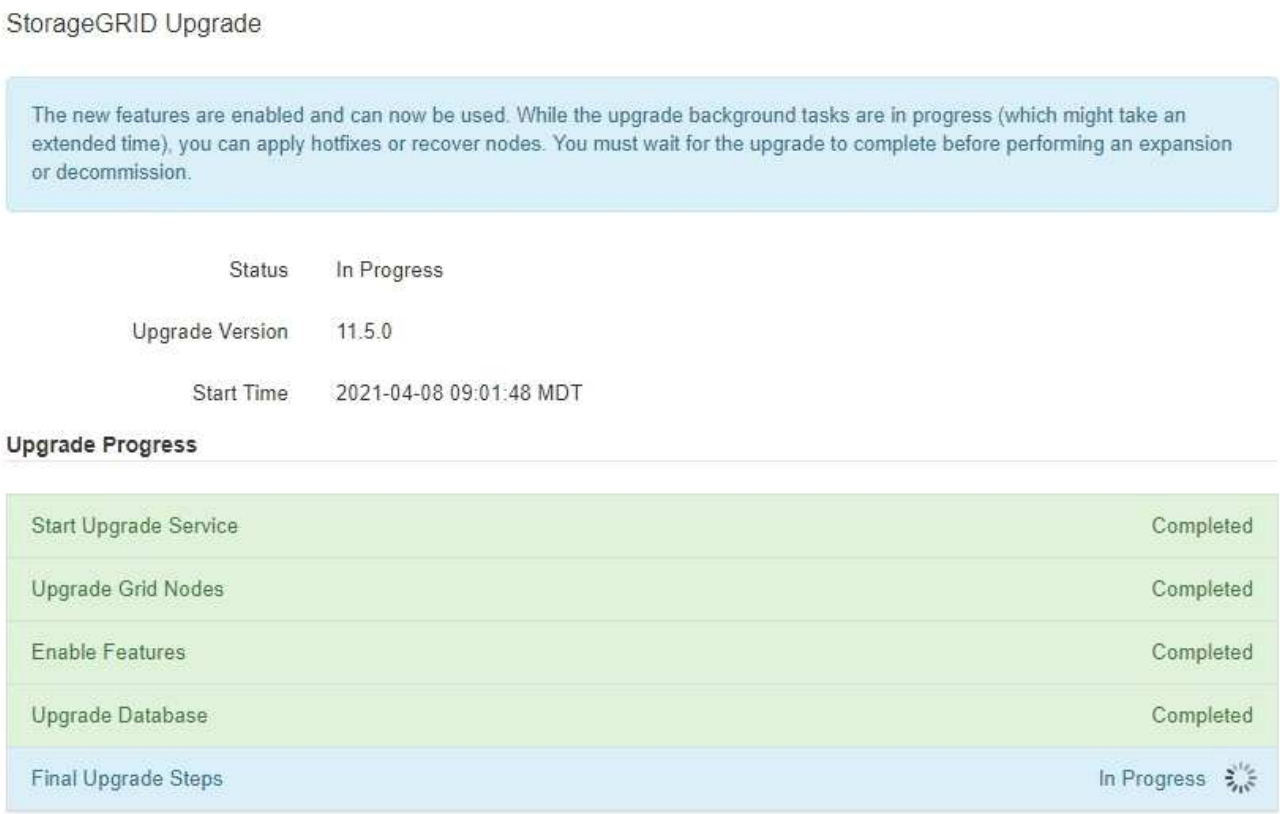
   > The **Upgrade Database** task might take days to complete. As this background task runs, you can apply hotfixes or recover nodes. However, you must wait for the **Final Upgrade Steps** task to complete before performing an expansion or decommission procedure.

   You can review the graph to monitor the progress for each Storage Node.



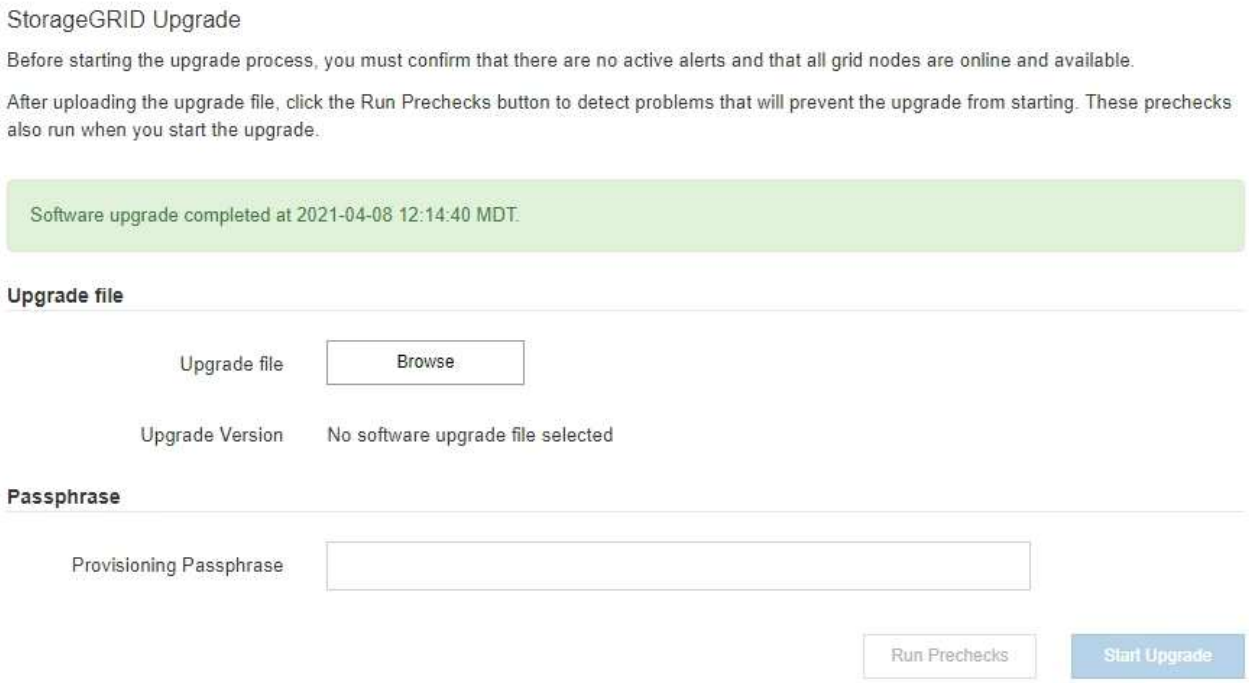
9. When the **Upgrade Database** task has completed, wait a few minutes for the **Final Upgrade Steps** task to

complete.



When the Final Upgrade Steps task has completed, the upgrade is done.

10. Confirm that the upgrade completed successfully.
    a. Sign in to the Grid Manager using a supported browser.
    b. Select **Help** > **About**.
    c. Confirm that the displayed version is what you would expect.
    d. Select **Maintenance** > **System** > **Software Update**. Then, select **StorageGRID Upgrade**.
    e. Confirm that the green banner shows that the software upgrade was completed on the date and time you expected.



11. Verify that grid operations have returned to normal:
    a. Check that the services are operating normally and that there are no unexpected alerts.
    b. Confirm that client connections to the StorageGRID system are operating as expected.
12. Check the NetApp Downloads page for StorageGRID to see if any hotfixes are available for the StorageGRID version that you just installed.

    NetApp Downloads: StorageGRID

    In the StorageGRID 11.5.*x.y* version number:

    - The major release has an *x* value of 0 (11.5.0).
    - A minor release, if available, has an *x* value other than 0 (for example, 11.5.1).
    - A hotfix, if available, has a *y* value (for example, 11.5.0.1).
13. If available, download and apply the latest hotfix for your StorageGRID version.

    See the recovery and maintenance instructions for information about applying hotfixes.

Related information

Downloading the Recovery Package

Maintain & recover

Increasing the Metadata Reserved Space setting

After you upgrade to StorageGRID 11.5, you might be able to increase the Metadata Reserved Space system setting if your Storage Nodes meet specific requirements for RAM and available space.

What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have the Root Access permission or the Grid Topology Page Configuration and Other Grid Configuration permissions.
- You have started the StorageGRID 11.5 upgrade and the **Enable New Features** upgrade task has completed.

About this task

You might be able to manually increase the system-wide Metadata Reserved Space setting up to 8 TB after upgrading to StorageGRID 11.5. Reserving additional metadata space after the 11.5 upgrade will simplify future hardware and software upgrades.

You can only increase the value of the system-wide Metadata Reserved Space setting if both of these statements are true:

- The Storage Nodes at any site in your system each have 128 GB or more RAM.
- The Storage Nodes at any site in your system each have sufficient available space on storage volume 0.

Be aware that if you increase this setting, you will simultaneously reduce the space available for object storage on storage volume 0 of all Storage Nodes. For this reason, you might prefer to set the Metadata Reserved Space to a value smaller than 8 TB, based on your expected object metadata requirements.

> In general, it is better to use a higher value instead of a lower value. If the Metadata Reserved Space setting is too large, you can decrease it later. In contrast, if you increase the value later, the system might need to move object data to free up space.

For a detailed explanation of how the Metadata Reserved Space setting affects the allowed space for object metadata storage on a particular Storage Node, go to the instructions for administering StorageGRID and search for “managing object metadata storage.”

Administer StorageGRID

Steps

1. Sign in to the Grid Manager using a supported browser.
2. Determine the current Metadata Reserved Space setting.
   a. Select **Configuration** > **System Settings** > **Storage Options**.
   b. In the Storage Watermarks section, note the value of **Metadata Reserved Space**.
3. Ensure you have enough available space on storage volume 0 of each Storage Node to increase this value.
   a. Select **Nodes**.
   b. Select the first Storage Node in the grid.
   c. Select the Storage tab.
   d. In the Volumes section, locate the **/var/local/rangedb/0** entry.
   e. Confirm that the Available value is equal to or greater than difference between the new value you want to use and the current Metadata Reserved Space value.

      For example, if the Metadata Reserved Space setting is currently 4 TB and you want to increase it to 6 TB, the Available value must be 2 TB or greater.

f. Repeat these steps for all Storage Nodes.

- If one or more Storage Nodes do not have enough available space, the Metadata Reserved Space value cannot be increased. Do not continue with this procedure.
- If each Storage Node has enough available space on volume 0, go to the next step.

4. Ensure you have at least 128 GB of RAM on each Storage Node.

   a. Select **Nodes**.

   b. Select the first Storage Node in the grid.

   c. Select the **Hardware** tab.

   d. Hover your cursor over the Memory Usage chart. Ensure that **Total Memory** is at least 128 GB.

   e. Repeat these steps for all Storage Nodes.

   - If one or more Storage Nodes do not have enough available total memory, the Metadata Reserved Space value cannot be increased. Do not continue with this procedure.
   - If each Storage Node has at least 128 GB of total memory, go to the next step.

5. Update the Metadata Reserved Space setting.

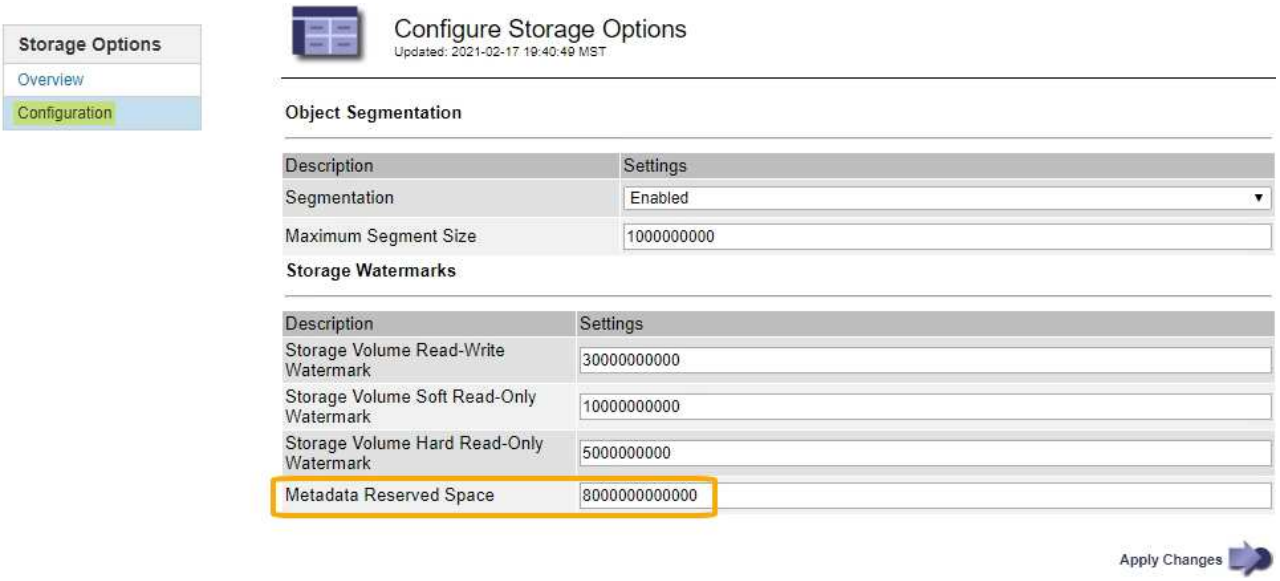
   a. Select **Configuration** > **System Settings** > **Storage Options**.

   b. Select the Configuration tab.

   c. In the Storage Watermarks section, select **Metadata Reserved Space**.

   d. Enter the new value.

   For example, to enter 8 TB, which is the maximum supported value, enter **8000000000000** (8, followed by 12 zeros)



   e. Select **Apply Changes**.

Troubleshooting upgrade issues

If the upgrade does not complete successfully, you might able to resolve the issue yourself. If you cannot resolve an issue, you should gather the required information before contacting technical support.

The following sections describe how to recover from situations where the upgrade has partially failed. Contact technical support if you cannot resolve an upgrade issue.

Upgrade precheck errors

To detect and resolve issues, you can manually run the upgrade prechecks before starting the actual upgrade. Most precheck errors provide information about how to resolve the issue. If you need help, contact technical support.

Provisioning failures

If the automatic provisioning process fails, contact technical support.

Grid node crashes or fails to start

If a grid node crashes during the upgrade process or fails to start successfully after the upgrade finishes, contact technical support to investigate and to correct any underlying issues.

Ingest or data retrieval is interrupted

If data ingest or retrieval is unexpectedly interrupted when you are not upgrading a grid node, contact technical support.

Database upgrade errors

If the database upgrade fails with an error, retry the upgrade. If it fails again, contact technical support.

Related information

Checking the system's condition before upgrading software

Troubleshooting user interface issues

You might see issues with the Grid Manager or the Tenant Manager after upgrading to a new version of StorageGRID software.

Web interface does not respond as expected

The Grid Manager or the Tenant Manager might not respond as expected after StorageGRID software is upgraded.

If you experience issues with the web interface:

- Make sure you are using a supported browser.

  > Browser support has changed for StorageGRID 11.5. Confirm you are using a supported version.

- Clear your web browser cache.

  Clearing the cache removes outdated resources used by the previous version of StorageGRID software, and permits the user interface to operate correctly again. For instructions, see the documentation for your web browser.

Related information

Web browser requirements

“Docker image availability check” error messages

When attempting to start the upgrade process, you might receive an error message that states “The following issues were identified by the Docker image availability check validation suite.” All issues must be resolved before you can complete the upgrade.

Contact technical support if you are unsure of the changes required to resolve the identified issues.

Message	Cause	Solution
Unable to determine upgrade version. Upgrade version info file `{file_path}` did not match the expected format.	The upgrade package is corrupt.	Re-upload the upgrade package, and try again. If the problem persists, contact technical support.
Upgrade version info file `{file_path}` was not found. Unable to determine upgrade version.	The upgrade package is corrupt.	Re-upload the upgrade package, and try again. If the problem persists, contact technical support.
Unable to determine currently installed release version on `{node_name}`.	A critical file on the node is corrupt.	Contact technical support.
Connection error while attempting to list versions on `{node_name}`	The node is offline or the connection was interrupted.	Check to make sure that all nodes are online and reachable from the primary Admin Node, and try again.
The host for node `{node_name}` does not have StorageGRID `{upgrade_version}` image loaded. Images and services must be installed on the host before the upgrade can proceed.	The RPM or DEB packages for the upgrade have not been installed on the host where the node is running, or the images are still in the process of being imported. **Note:** This error only applies to nodes that are running as containers on Linux.	Check to make sure that the RPM or DEB packages have been installed on all Linux hosts where nodes are running. Make sure the version is correct for both the service and the images file. Wait a few minutes, and try again. For more information, see the installation instructions for your Linux platform.
Error while checking node `{node_name}`	An unexpected error occurred.	Wait a few minutes, and try again.
Uncaught error while running prechecks. `{error_string}`	An unexpected error occurred.	Wait a few minutes, and try again.

Related information

Install Red Hat Enterprise Linux or CentOS

Install Ubuntu or Debian

Copyright information

Copyright © 2025 NetApp, Inc. All Rights Reserved. Printed in the U.S. No part of this document covered by copyright may be reproduced in any form or by any means—graphic, electronic, or mechanical, including photocopying, recording, taping, or storage in an electronic retrieval system—without prior written permission of the copyright owner.

Software derived from copyrighted NetApp material is subject to the following license and disclaimer:

THIS SOFTWARE IS PROVIDED BY NETAPP “AS IS” AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, WHICH ARE HEREBY DISCLAIMED. IN NO EVENT SHALL NETAPP BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

NetApp reserves the right to change any products described herein at any time, and without notice. NetApp assumes no responsibility or liability arising from the use of products described herein, except as expressly agreed to in writing by NetApp. The use or purchase of this product does not convey a license under any patent rights, trademark rights, or any other intellectual property rights of NetApp.

The product described in this manual may be protected by one or more U.S. patents, foreign patents, or pending applications.

LIMITED RIGHTS LEGEND: Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (b)(3) of the Rights in Technical Data -Noncommercial Items at DFARS 252.227-7013 (FEB 2014) and FAR 52.227-19 (DEC 2007).

Data contained herein pertains to a commercial product and/or commercial service (as defined in FAR 2.101) and is proprietary to NetApp, Inc. All NetApp technical data and computer software provided under this Agreement is commercial in nature and developed solely at private expense. The U.S. Government has a non-exclusive, non-transferrable, nonsublicensable, worldwide, limited irrevocable license to use the Data only in connection with and in support of the U.S. Government contract under which the Data was delivered. Except as provided herein, the Data may not be used, disclosed, reproduced, modified, performed, or displayed without the prior written approval of NetApp, Inc. United States Government license rights for the Department of Defense are limited to those rights identified in DFARS clause 252.227-7015(b) (FEB 2014).

Trademark information

NETAPP, the NETAPP logo, and the marks listed at http://www.netapp.com/TM are trademarks of NetApp, Inc. Other company and product names may be trademarks of their respective owners.