



# **SG6000 storage appliances**

## StorageGRID

NetApp  
October 03, 2025

This PDF was generated from <https://docs.netapp.com/us-en/storagegrid-115/sg6000/sg6060-overview.html> on October 03, 2025. Always check [docs.netapp.com](https://docs.netapp.com) for the latest.

# Table of Contents

SG6000 storage appliances .....	1
SG6000 appliances overview .....	1
SG6060 overview .....	1
SGF6024 overview .....	5
Controllers in the SG6000 appliances .....	7
Installation and deployment overview .....	12
Installation and deployment tasks .....	12
Preparing for installation .....	13
Preparing the site (SG6000) .....	13
Unpacking the boxes (SG6000) .....	14
Obtaining additional equipment and tools (SG6000) .....	18
Web browser requirements .....	20
Reviewing appliance network connections .....	21
Gathering installation information (SG6000) .....	24
Installing the hardware .....	29
Registering the hardware .....	30
SG6060: Installing 60-drive shelves into a cabinet or rack .....	30
SG6060: Installing the drives .....	33
SGF6024: Installing 24-drive shelves into a cabinet or rack .....	34
SG6000-CN: Installing into a cabinet or rack .....	36
Cabling the appliance (SG6000) .....	38
SG6060: Cabling the optional expansion shelves .....	42
Connecting power cords and applying power (SG6000) .....	44
Viewing status indicators and buttons on the SG6000-CN controller .....	45
Viewing boot-up status codes for the SG6000 storage controllers .....	46
Configuring the hardware .....	47
Configuring StorageGRID connections .....	48
Accessing and Configuring SANtricity System Manager .....	69
Configuring the BMC interface .....	77
Optional: Enabling node encryption .....	84
Optional: Changing the RAID mode (SG6000 only) .....	86
Optional: Remapping network ports for the appliance .....	87
Deploying an appliance Storage Node .....	88
Monitoring the storage appliance installation .....	91
Automating appliance installation and configuration .....	92
Automating appliance configuration using the StorageGRID Appliance Installer .....	93
Automating installation and configuration of appliance nodes using the configure-sga.py script .....	95
Automating the configuration of StorageGRID .....	99
Overview of installation REST APIs .....	100
StorageGRID Installation API .....	100
StorageGRID Appliance Installer API .....	101
Troubleshooting the hardware installation .....	101
Viewing boot-up codes for the SG6000-CN controller .....	102

Viewing error codes for the SG6000-CN controller . . . . .	104
Hardware setup appears to hang . . . . .	106
Troubleshooting connection issues . . . . .	107
Rebooting the SG6000-CN controller while the StorageGRID Appliance Installer is running . . . . .	109
<b>Maintaining the SG6000 appliance . . . . .</b>	<b>109</b>
Placing an appliance into maintenance mode . . . . .	110
Upgrading SANtricity OS on the storage controllers . . . . .	113
Upgrading drive firmware using SANtricity System Manager . . . . .	122
Adding an expansion shelf to a deployed SG6060 . . . . .	127
Turning the controller identify LED on and off . . . . .	133
Locating the controller in a data center . . . . .	134
Replacing a storage controller . . . . .	135
Replacing hardware components in the storage controller shelf . . . . .	141
Replacing hardware components in the optional 60-drive expansion shelf . . . . .	142
Shutting down the SG6000-CN controller . . . . .	143
Powering on the SG6000-CN controller and verifying operation . . . . .	145
Replacing the SG6000-CN controller . . . . .	148
Replacing a power supply in the SG6000-CN controller . . . . .	149
Removing the SG6000-CN controller from a cabinet or rack . . . . .	151
Reinstalling the SG6000-CN controller into a cabinet or rack . . . . .	152
Removing the SG6000-CN controller cover . . . . .	154
Reinstalling the SG6000-CN controller cover . . . . .	154
Replacing the Fibre Channel HBA in the SG6000-CN controller . . . . .	155
Changing the link configuration of the SG6000-CN controller . . . . .	159
Changing the MTU setting . . . . .	161
Checking the DNS server configuration . . . . .	164
Monitoring node encryption in maintenance mode . . . . .	166

# SG6000 storage appliances

Learn how to install and maintain the StorageGRID SG6060 and SGF6024 appliances.

- [SG6000 appliances overview](#)
- [Installation and deployment overview](#)
- [Preparing for installation](#)
- [Installing the hardware](#)
- [Configuring the hardware](#)
- [Deploying an appliance Storage Node](#)
- [Monitoring the storage appliance installation](#)
- [Automating appliance installation and configuration](#)
- [Overview of installation REST APIs](#)
- [Troubleshooting the hardware installation](#)
- [Maintaining the SG6000 appliance](#)

## SG6000 appliances overview

The StorageGRID SG6000 appliances are integrated storage and computing platforms that operate as Storage Nodes in a StorageGRID system. These appliances can be used in a hybrid grid environment that combines appliance Storage Nodes and virtual (software-based) Storage Nodes.

The SG6000 appliances provide the following features:

- Available in two models:
  - SG6060, which includes 60 drives and supports expansion shelves.
  - SGF6024, which offers 24 solid state drives (SSDs).
- Integrate the storage and computing elements for a StorageGRID Storage Node.
- Include the StorageGRID Appliance Installer to simplify Storage Node deployment and configuration.
- Include SANtricity System Manager for managing and monitoring the storage controllers and drives.
- Include a baseboard management controller (BMC) for monitoring and diagnosing the hardware in the compute controller.
- Support up to four 10-GbE or 25-GbE connections to the StorageGRID Grid Network and Client Network.
- Support Federal Information Processing Standard (FIPS) drives. When these drives are used with the Drive Security feature in SANtricity System Manager, unauthorized access to data is prevented.

## SG6060 overview

The StorageGRID SG6060 appliance includes a compute controller and a storage controller shelf that contains two storage controllers and 60 drives. Optionally, 60-drive expansion shelves can be added to the appliance.

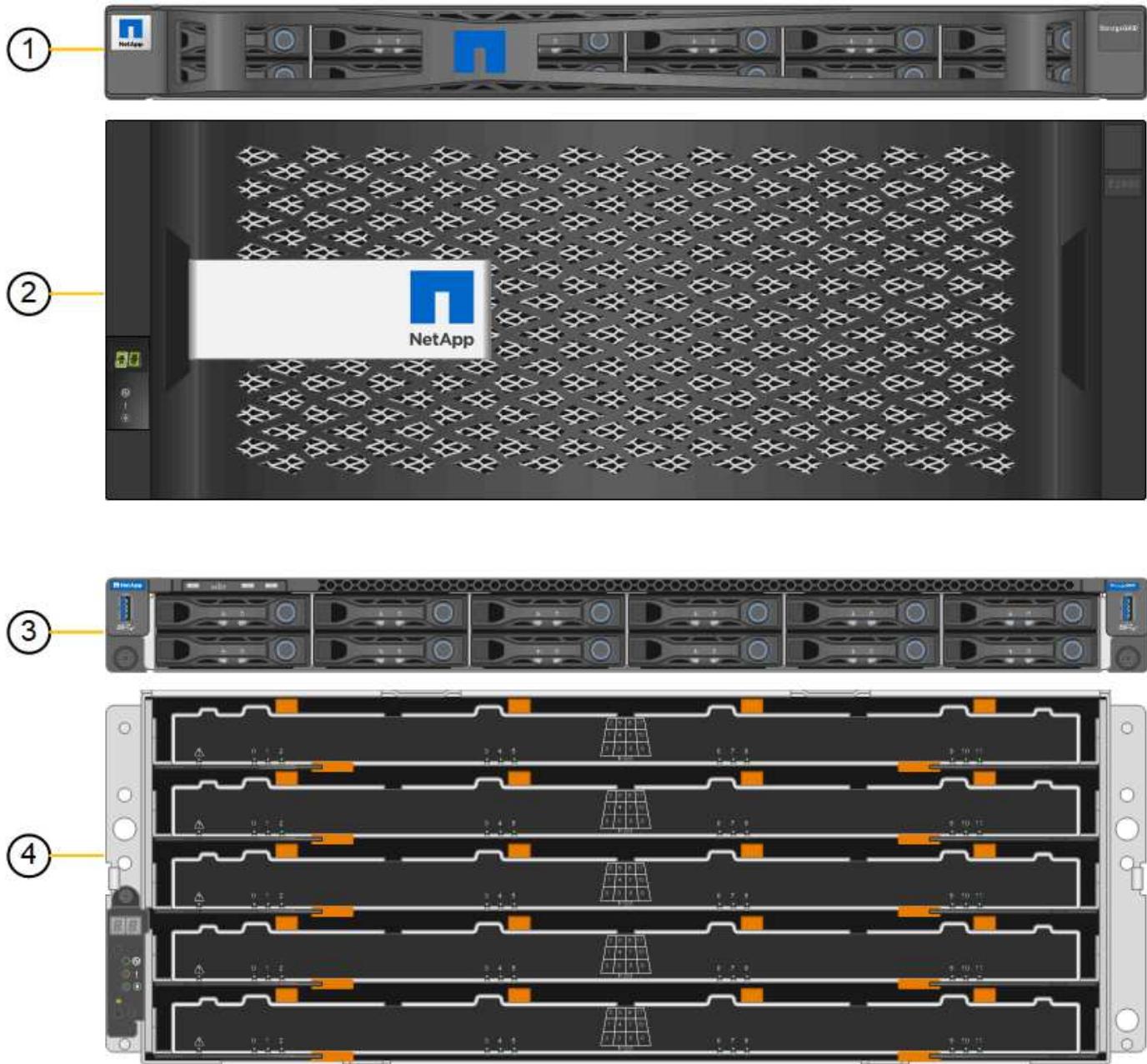
## SG6060 components

The SG6060 appliance includes the following components:

Component	Description
Compute controller	<p>SG6000-CN controller, a one-rack unit (1U) server that includes:</p> <ul style="list-style-type: none"><li>• 40 cores (80 threads)</li><li>• 192 GB RAM</li><li>• Up to 4 × 25 Gbps aggregate Ethernet bandwidth</li><li>• 4 × 16 Gbps Fibre Channel (FC) interconnect</li><li>• Baseboard management controller (BMC) that simplifies hardware management</li><li>• Redundant power supplies</li></ul>
Storage controller shelf	<p>E-Series E2860 controller shelf (storage array), a 4U shelf that includes:</p> <ul style="list-style-type: none"><li>• Two E-Series E2800 controllers (duplex configuration) to provide storage controller failover support</li><li>• Five-drawer drive shelf that holds sixty 3.5-inch drives (2 solid-state drives, or SSDs, and 58 NL-SAS drives)</li><li>• Redundant power supplies and fans</li></ul>
Optional: Storage expansion shelves  <b>Note:</b> Expansion shelves can be installed during initial deployment or added later.	<p>E-Series DE460C enclosure, a 4U shelf that includes:</p> <ul style="list-style-type: none"><li>• Two input/output modules (IOMs)</li><li>• Five drawers, each holding 12 NL-SAS drives, for a total of 60 drives</li><li>• Redundant power supplies and fans</li></ul> <p>Each SG6060 appliance can have one or two expansion shelves for a total of 180 drives.</p>

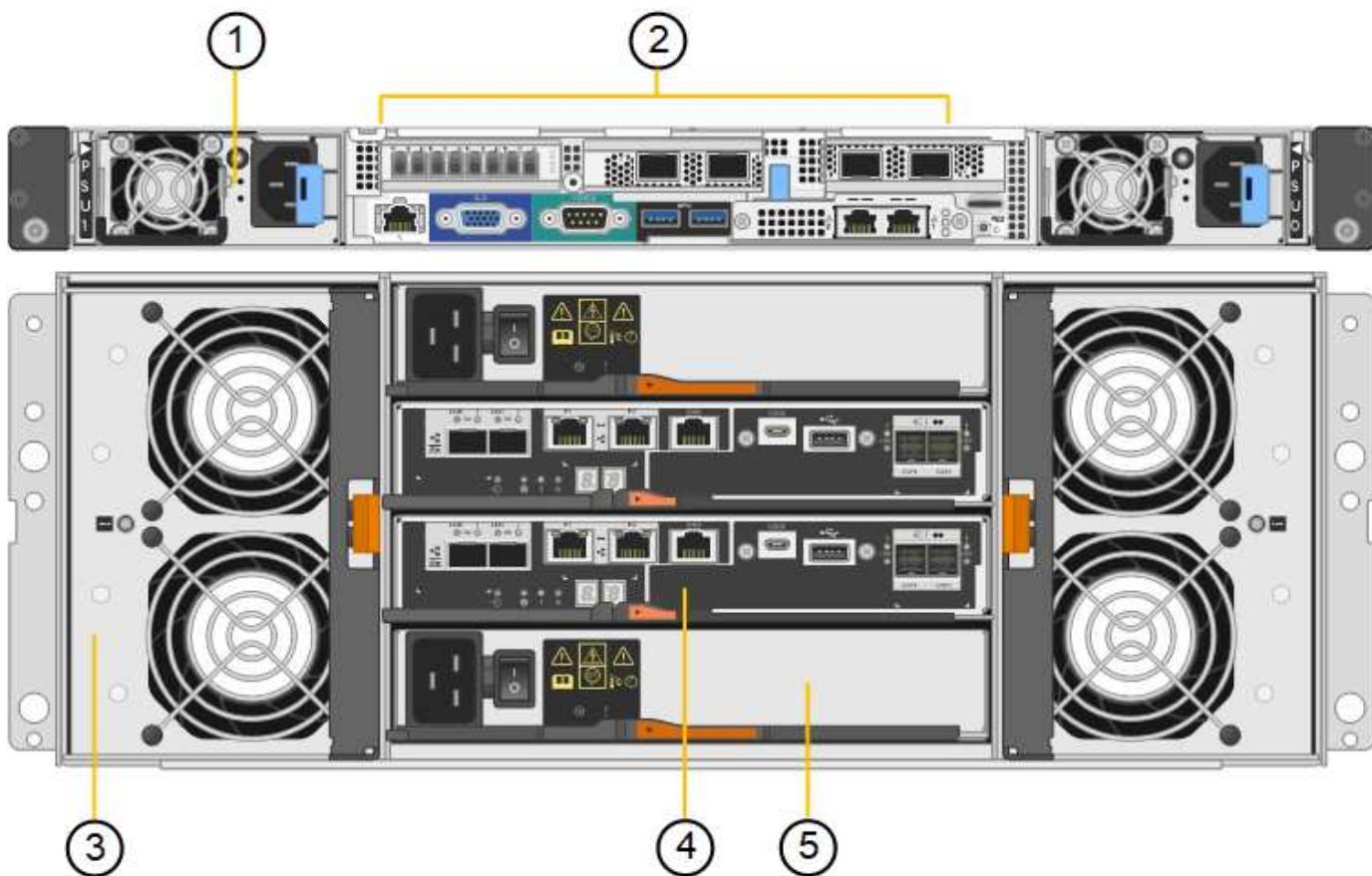
## SG6060 diagrams

This figure shows the front of the SG6060, which includes a 1U compute controller and a 4U shelf containing two storage controllers and 60 drives in five drive drawers.



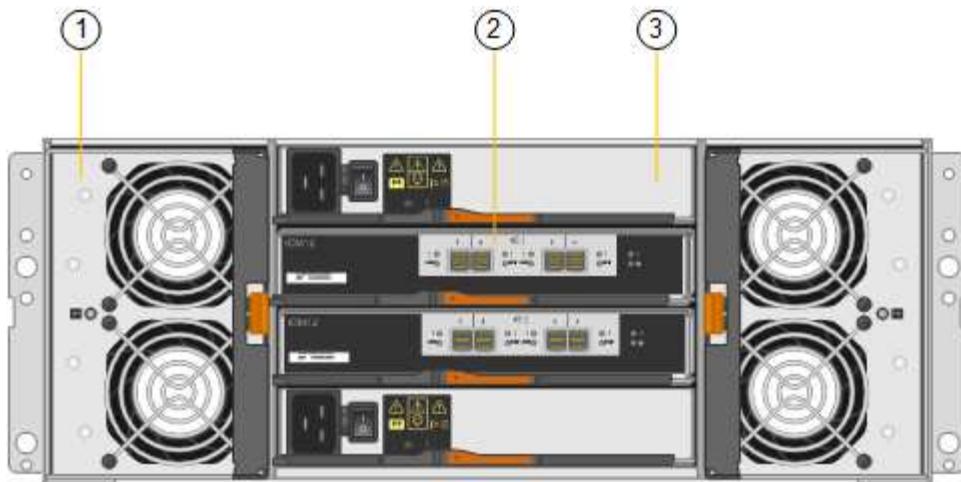
	Description
1	SG6000-CN compute controller with front bezel
2	E2860 controller shelf with front bezel (optional expansion shelf looks identical)
3	SG6000-CN compute controller with front bezel removed
4	E2860 controller shelf with front bezel removed (optional expansion shelf looks identical)

This figure shows the back of the SG6060, including the compute and storage controllers, fans, and power supplies.



	Description
1	Power supply (1 of 2) for SG6000-CN compute controller
2	Connectors for SG6000-CN compute controller
3	Fan (1 of 2) for E2860 controller shelf
4	E-Series E2800 storage controller (1 of 2) and connectors
5	Power supply (1 of 2) for E2860 controller shelf

This figure shows the back of the optional expansion shelf for the SG6060, including the input/output modules (IOMs), fans, and power supplies. Each SG6060 can be installed with one or two expansion shelves, which can be included in the initial installation or added later.



	Description
1	Fan (1 of 2) for expansion shelf
2	IOM (1 of 2) for expansion shelf
3	Power supply (1 of 2) for expansion shelf

## SGF6024 overview

The StorageGRID SGF6024 includes a compute controller and a storage controller shelf that holds 24 solid state drives.

### SGF6024 components

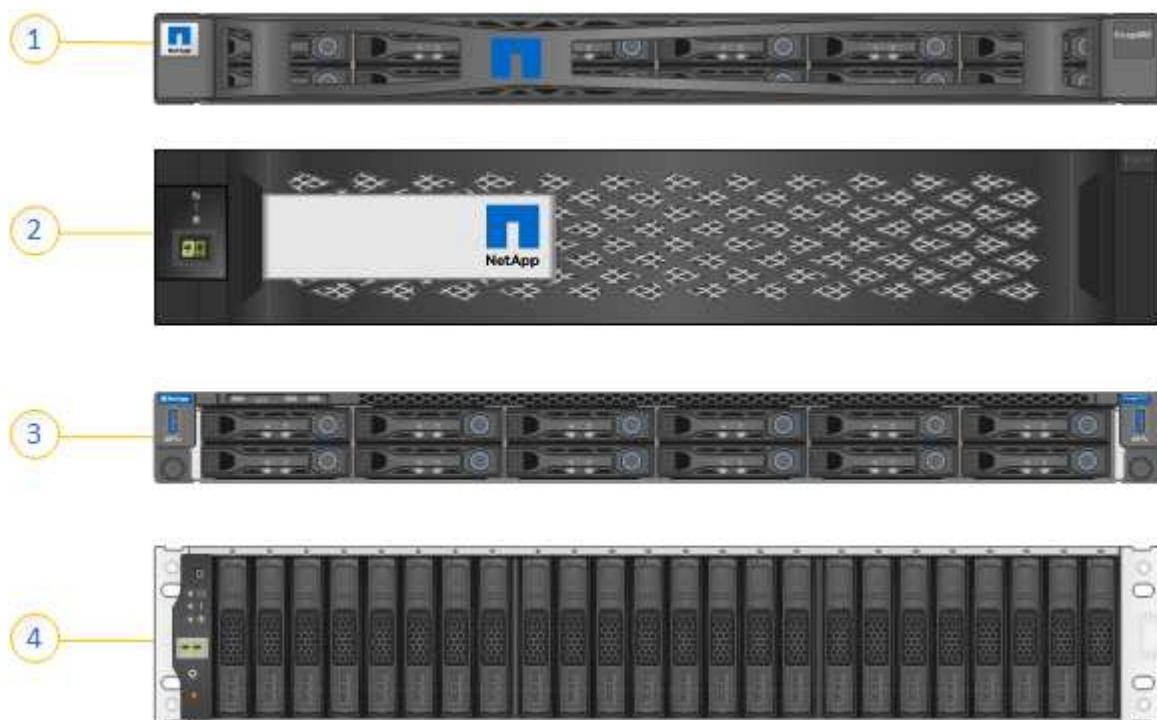
The SGF6024 appliance includes the following components:

Component	Description
Compute controller	SG6000-CN controller, a one-rack unit (1U) server that includes: <ul style="list-style-type: none"> <li>• 40 cores (80 threads)</li> <li>• 192 GB RAM</li> <li>• Up to 4 × 25 Gbps aggregate Ethernet bandwidth</li> <li>• 4 × 16 Gbps Fibre Channel (FC) interconnect</li> <li>• Baseboard management controller (BMC) that simplifies hardware management</li> <li>• Redundant power supplies</li> </ul>

Component	Description
Flash array (controller shelf)	E-Series EF570 flash array (also known as a controller shelf), a 2U shelf that includes: <ul style="list-style-type: none"> <li>Two E-Series EF570 controllers (duplex configuration) to provide storage controller failover support</li> <li>24 solid state drives (also known as SSDs or flash drives)</li> <li>Redundant power supplies and fans</li> </ul>

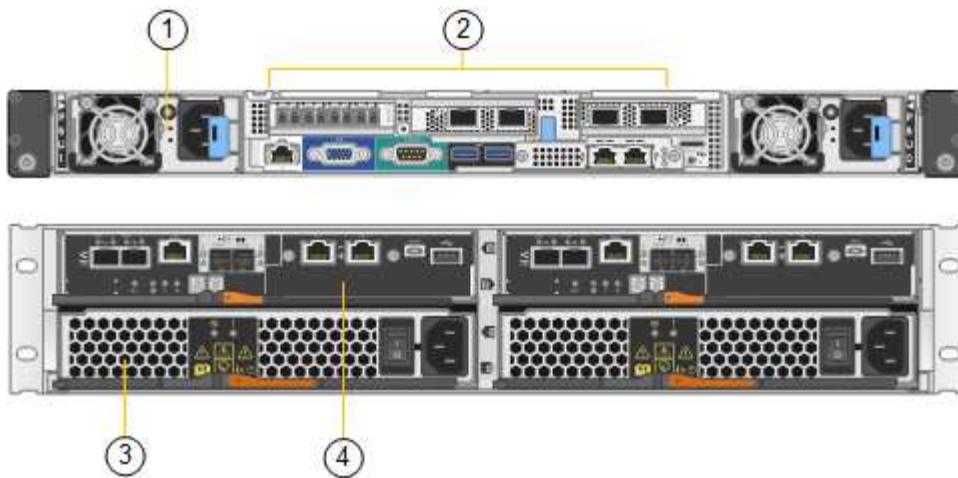
## SGF6024 diagrams

This figure shows the front of the SGF6024, which includes a 1U compute controller and a 2U enclosure containing two storage controllers and 24 flash drives.



	Description
1	SG6000-CN compute controller with front bezel
2	EF570 flash array with front bezel
3	SG6000-CN compute controller with front bezel removed
4	EF570 flash array with front bezel removed

This figure shows the back of the SGF6024, including the compute and storage controllers, fans, and power supplies.



	Description
1	Power supply (1 of 2) for SG6000-CN compute controller
2	Connectors for SG6000-CN compute controller
3	Power supply (1 of 2) for EF570 flash array
4	E-Series EF570 storage controller (1 of 2) and connectors

## Controllers in the SG6000 appliances

Each model of the StorageGRID SG6000 appliance includes an SG6000-CN compute controller in a 1U enclosure and duplex E-Series storage controllers in a 2U or 4U enclosure, depending on the model. Review the diagrams to learn more about each type of controller.

### All appliances: SG6000-CN compute controller

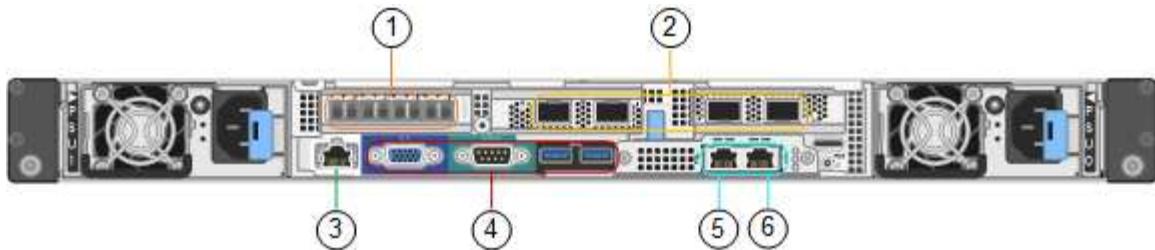
- Provides compute resources for the appliance.
- Includes the StorageGRID Appliance Installer.



StorageGRID software is not preinstalled on the appliance. This software is retrieved from the Admin Node when you deploy the appliance.

- Can connect to all three StorageGRID networks, including the Grid Network, the Admin Network, and the Client Network.
- Connects to the E-Series storage controllers and operates as the initiator.

This figure shows the connectors on the back of the SG6000-CN.



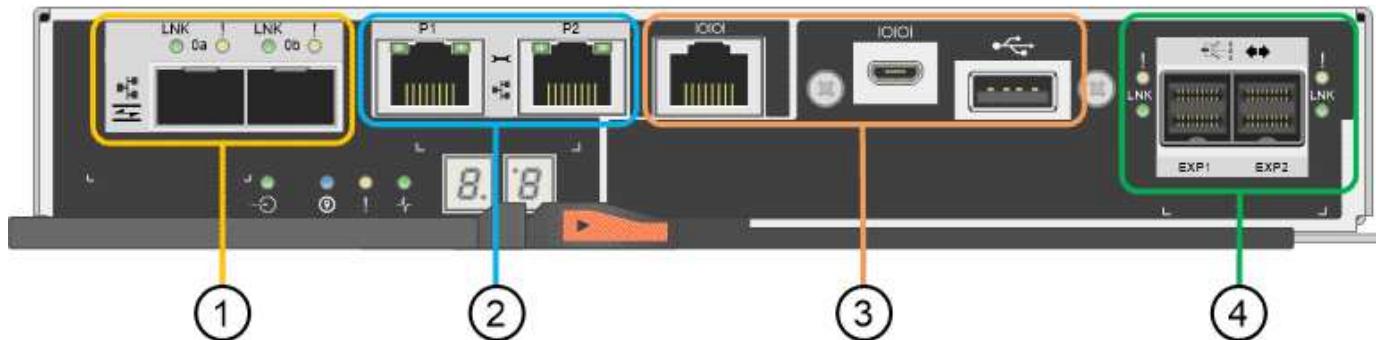
	Port	Type	Use
1	Interconnect ports 1-4	16-Gb/s Fibre Channel (FC), with integrated optics	Connect the SG6000-CN controller to the E2800 controllers (two connections to each E2800).
2	Network ports 1-4	10-GbE or 25-GbE, based on cable or SFP transceiver type, switch speed, and configured link speed	Connect to the Grid Network and the Client Network for StorageGRID.
3	BMC management port	1-GbE (RJ-45)	Connect to the SG6000-CN baseboard management controller.
4	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• VGA</li> <li>• Serial, 115200 8-N-1</li> <li>• USB</li> </ul>	Reserved for technical support use.
5	Admin Network port 1	1-GbE (RJ-45)	Connect the SG6000-CN to the Admin Network for StorageGRID.

	Port	Type	Use
6	Admin Network port 2	1-GbE (RJ-45)	<p>Options:</p> <ul style="list-style-type: none"> <li>• Bond with management port 1 for a redundant connection to the Admin Network for StorageGRID.</li> <li>• Leave unwired and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, use port 2 for IP configuration if DHCP-assigned IP addresses are not available.</li> </ul>

### SG6060: E2800 storage controllers

- Two controllers for failover support.
- Manage the storage of data on the drives.
- Function as standard E-Series controllers in a duplex configuration.
- Include SANtricity OS Software (controller firmware).
- Include SANtricity System Manager for monitoring storage hardware and for managing alerts, the AutoSupport feature, and the Drive Security feature.
- Connect to the SG6000-CN controller and provide access to the storage.

This figure shows the connectors on the back of each of the E2800 controllers.

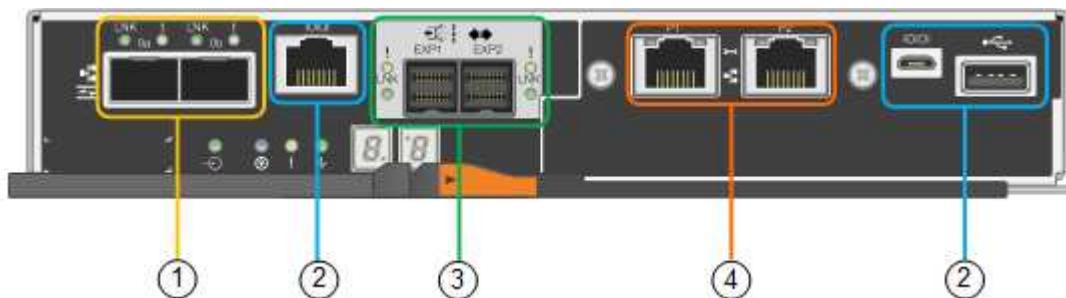


	Port	Type	Use
1	Interconnect ports 1 and 2	16-Gb/s FC optical SFPa	<p>Connect each of the E2800 controllers to the SG6000-CN controller.</p> <p>There are four connections to the SG6000-CN controller (two from each E2800).</p>
2	Management ports 1 and 2	1-Gb (RJ-45) Ethernet	<ul style="list-style-type: none"> <li>• Port 1 connects to the network where you access SANtricity System Manager on a browser.</li> <li>• Port 2 is reserved for technical support use.</li> </ul>
3	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• RJ-45 serial port</li> <li>• Micro USB serial port</li> <li>• USB port</li> </ul>	Reserved for technical support use.
4	Drive expansion ports 1 and 2	12Gb/s SAS	Connect the ports to the drive expansion ports on the IOMs in the expansion shelf.

### SGF6024: EF570 storage controllers

- Two controllers for failover support.
- Manage the storage of data on the drives.
- Function as standard E-Series controllers in a duplex configuration.
- Include SANtricity OS Software (controller firmware).
- Include SANtricity System Manager for monitoring storage hardware and for managing alerts, the AutoSupport feature, and the Drive Security feature.
- Connect to the SG6000-CN controller and provide access to the flash storage.

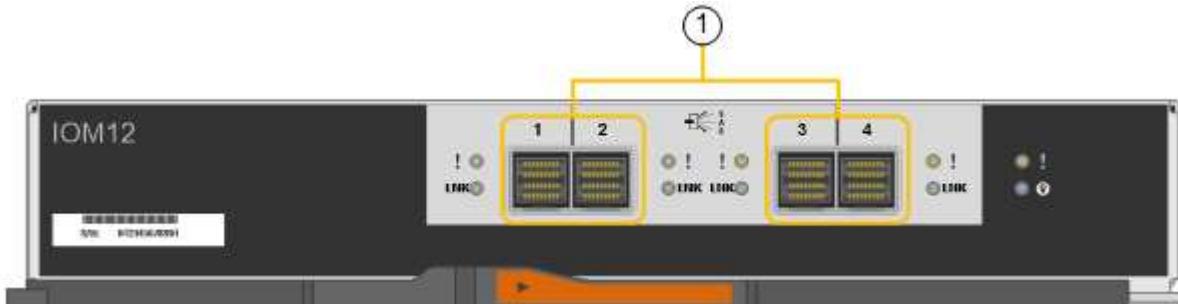
This figure shows the connectors on the back of each of the EF570 controllers.



	Port	Type	Use
1	Interconnect ports 1 and 2	16-Gb/s FC optical SFPa	Connect each of the EF570 controllers to the SG6000-CN controller.  There are four connections to the SG6000-CN controller (two from each EF570).
2	Diagnostic and support ports	<ul style="list-style-type: none"> <li>• RJ-45 serial port</li> <li>• Micro USB serial port</li> <li>• USB port</li> </ul>	Reserved for technical support use.
3	Drive expansion ports	12Gb/s SAS	Not used. The SGF6024 appliance does not support expansion drive shelves.
4	Management ports 1 and 2	1-Gb (RJ-45) Ethernet	<ul style="list-style-type: none"> <li>• Port 1 connects to the network where you access SANtricity System Manager on a browser.</li> <li>• Port 2 is reserved for technical support use.</li> </ul>

### SG6060: Input/output modules for optional expansion shelves

The expansion shelf contains two input/output modules (IOMs) that connect to the storage controllers or to other expansion shelves.



	Port	Type	Use
1	Drive expansion ports 1-4	12Gb/s SAS	Connect each port to the storage controllers or additional expansion shelf (if any).

# Installation and deployment overview

You can install one or more StorageGRID storage appliances when you first deploy StorageGRID, or you can add appliance Storage Nodes later as part of an expansion. You might also need to install an appliance Storage Node as part of a recovery operation.

## What you'll need

Your StorageGRID system is using the required version of StorageGRID software.

Appliance	Required StorageGRID version
SG6060 with no expansion shelves	11.1.1 or later
SG6060 with expansion shelves (one or two)	11.3 or later  <b>Note:</b> If you add expansion shelves after the initial deployment, you must use version 11.4 or later.
SGF6024	11.3 or later

## Installation and deployment tasks

Adding a StorageGRID storage appliance to a StorageGRID system includes four primary steps:

1. Preparing for installation:
  - Preparing the installation site
  - Unpacking the boxes and checking the contents
  - Obtaining additional equipment and tools
  - Gathering IP addresses and network information
  - Optional: Configuring an external key management server (KMS) if you plan to encrypt all appliance data. See details about external key management in the instructions for administering StorageGRID.
2. Installing the hardware:
  - Registering the hardware
  - Installing the appliance into a cabinet or rack
  - Installing the drives
  - Installing optional expansion shelves (model SG6060 only; maximum of two expansion shelves)
  - Cabling the appliance
  - Connecting the power cords and applying power
  - Viewing boot-up status codes
3. Configuring the hardware:
  - Accessing SANtricity System Manager to configure SANtricity System Manager settings
  - Accessing StorageGRID Appliance Installer, setting a static IP address for management port 1 on the storage controller, and configuring the link and network IP settings required to connect to StorageGRID networks

- Accessing the baseboard management controller (BMC) interface on the SG6000-CN controller
- Optional: Enabling node encryption if you plan to use an external KMS to encrypt appliance data.
- Optional: Changing the RAID mode.

#### 4. Deploying the appliance as a Storage Node:

Task	Instructions
Deploying an appliance Storage Node in a new StorageGRID system	<a href="#">Deploying an appliance Storage Node</a>
Adding an appliance Storage Node to an existing StorageGRID system	Instructions for expanding a StorageGRID system
Deploying an appliance Storage Node as part of a Storage Node recovery operation	Instructions for recovery and maintenance

#### Related information

[Preparing for installation](#)

[Installing the hardware](#)

[Configuring the hardware](#)

[Expand your grid](#)

[Maintain & recover](#)

[Administer StorageGRID](#)

## Preparing for installation

Preparing to install a StorageGRID appliance entails preparing the site and obtaining all required hardware, cables, and tools. You should also gather IP addresses and network information.

#### Steps

- [Preparing the site \(SG6000\)](#)
- [Unpacking the boxes \(SG6000\)](#)
- [Obtaining additional equipment and tools \(SG6000\)](#)
- [Web browser requirements](#)
- [Reviewing appliance network connections](#)
- [Gathering installation information \(SG6000\)](#)

### Preparing the site (SG6000)

Before installing the appliance, you must make sure that the site and the cabinet or rack

you plan to use meet the specifications for a StorageGRID appliance.

## Steps

1. Confirm that the site meets the requirements for temperature, humidity, altitude range, airflow, heat dissipation, wiring, power, and grounding. See the NetApp Hardware Universe for more information.
2. Confirm that your location provides 240-volt AC power for the SG6060 or 120-volt AC power for the SGF6024.
3. Obtain a 19-inch (48.3-cm) cabinet or rack to fit shelves of this size (without cables):

Type of shelf	Height	Width	Depth	Maximum weight
<b>E2860 controller shelf</b> for SG6060	6.87 in. (17.46 cm)	17.66 in. (44.86 cm)	38.25 in. (97.16 cm)	250 lb. (113 kg)
<b>Optional expansion shelf</b> for SG6060 (one or two)	6.87 in. (17.46 cm)	17.66 in. (44.86 cm)	38.25 in. (97.16 cm)	250 lb. (113 kg)
<b>EF570 controller shelf</b> for SGF6024	3.35 in. (8.50 cm)	17.66 in. (44.86 cm)	19.00 in. (48.26 cm)	51.74 lb. (23.47 kg)
<b>SG6000-CN controller</b> for each appliance	1.70 in. (4.32 cm)	17.32 in. (44.0 cm)	32.0 in. (81.3 cm)	39 lb. (17.7 kg)

4. Decide where you are going to install the appliance.



When installing the E2860 controller shelf or optional expansion shelves, install hardware from the bottom to the top of the rack or cabinet to prevent the equipment from tipping over. To ensure that the heaviest equipment is at the bottom of the cabinet or rack, install the SG6000-CN controller above the E2860 controller shelf and expansion shelves.



Before committing to the installation, verify that the 0.5m optic cables shipped with the appliance, or cables that you supply, are long enough for the planned layout.

## Related information

[NetApp Hardware Universe](#)

[NetApp Interoperability Matrix Tool](#)

## Unpacking the boxes (SG6000)

Before installing the StorageGRID appliance, unpack all boxes and compare the contents to the items on the packing slip.

## SG6060

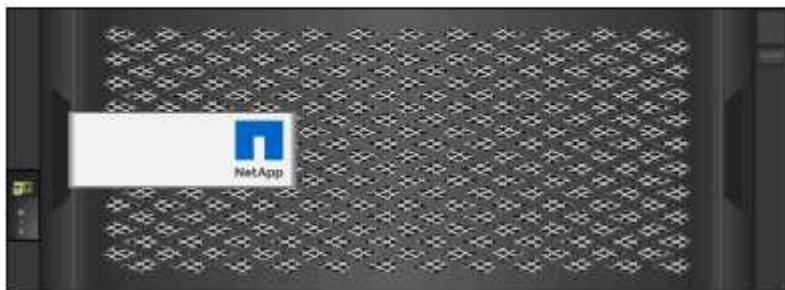
- SG6000-CN controller



- E2860 controller shelf with no drives installed



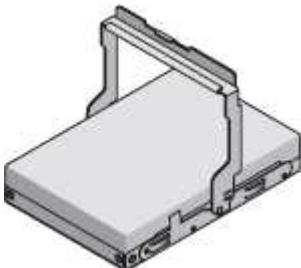
- Two front bezels



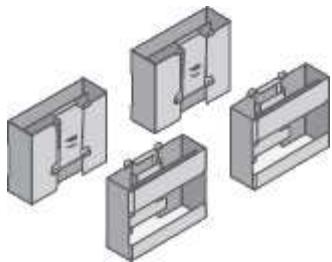
- Two rail kits with instructions



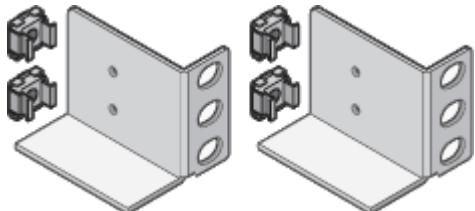
- 60 drives (2 SSD and 58 NL-SAS)



- Four handles

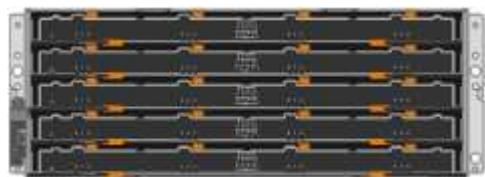


- Back brackets and cage nuts for square-hole rack installation



### SG6060 expansion shelf

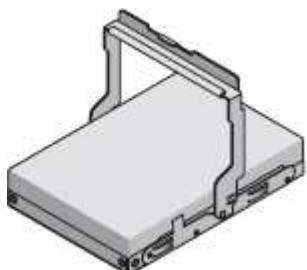
- Expansion shelf with no drives installed



- Front bezel



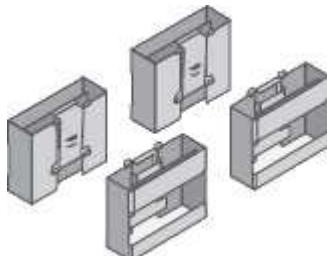
- 60 NL-SAS drives



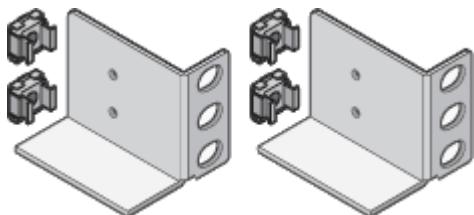
- One rail kit with instructions



- Four handles



- Back brackets and cage nuts for square-hole rack installation



## SGF6024

- SG6000-CN controller



- EF570 flash array with 24 solid state (flash) drives installed



- Two front bezels



- Two rail kits with instructions



- **Shelf endcaps**



## Cables and connectors

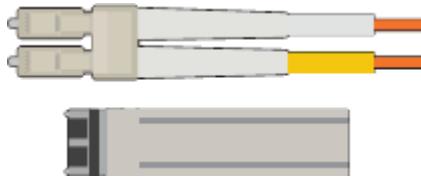
The shipment for the StorageGRID appliance includes the following cables and connectors:

- **Four power cords for your country**



Your cabinet might have special power cords that you use instead of the power cords that ship with the appliance.

- **Optical cables and SFP transceivers**



Four optical cables for the FC interconnect ports

Four SFP+ transceivers, which support 16-Gb/s FC

- **Optional: Two SAS cables for connecting each SG6060 expansion shelf**

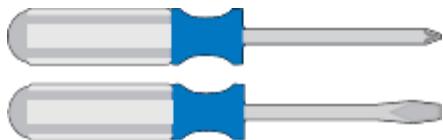


## Obtaining additional equipment and tools (SG6000)

Before installing the StorageGRID appliance, confirm you have all of the additional equipment and tools that you need.

You need the following additional equipment to install and configure the hardware:

- **Screwdrivers**



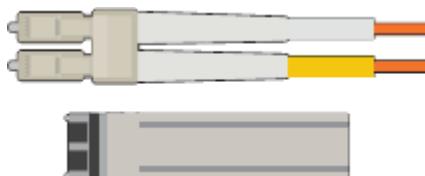
Phillips No. 2 screwdriver

Medium flat-blade screwdriver

- **ESD wrist strap**



- **Optical cables and SFP transceivers**



You need one of the following options:

- One to four TwinAx cables or optical cables for the 10/25-GbE ports you plan to use on the SG6000-CN controller
- One to four SFP+ transceivers for the 10/25-GbE ports if you will use optical cables and 10-GbE link speed
- One to four SFP28 transceivers for the 10/25-GbE ports if you will use optical cables and 25-GbE link speed

- **RJ-45 (Cat5/Cat5e/Cat6) Ethernet cables**



- **Service laptop**



Supported web browser

1-GbE (RJ-45) port

- **Optional tools**



Power drill with Phillips head bit

Flashlight

Mechanized lift for 60-drive shelves

## 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

## Reviewing appliance network connections

Before installing the StorageGRID appliance, you should understand which networks can be connected to the appliance.

When you deploy a StorageGRID appliance as a Storage Node in a StorageGRID system, you can connect it to the following networks:

- **Grid Network for StorageGRID:** The Grid Network is used for all internal StorageGRID traffic. It provides connectivity between all nodes in the grid, across all sites and subnets. The Grid Network is required.
- **Admin Network for StorageGRID:** The Admin Network is a closed network used for system administration and maintenance. The Admin Network is typically a private network and does not need to be routable between sites. The Admin Network is optional.
- **Client Network for StorageGRID:** The Client Network is an open network used to provide access to client applications, including S3 and Swift. The Client Network provides client protocol access to the grid, so the Grid Network can be isolated and secured. The Client Network is optional.
- **Management network for SANtricity System Manager:** This network provides access to SANtricity System Manager on the storage controller, allowing you to monitor and manage the hardware components in the storage controller shelf. This management network can be the same as the Admin Network for StorageGRID, or it can be an independent management network.
- **BMC management network for the SG6000-CN controller:** This network provides access to the baseboard management controller in the SG6000-CN, allowing you to monitor and manage the hardware components in the SG6000-CN controller. This management network can be the same as the Admin Network for StorageGRID, or it can be an independent management network.



For detailed information about StorageGRID networks, see the *Grid Primer*.

### Related information

[Gathering installation information \(SG6000\)](#)

[Cabling the appliance \(SG6000\)](#)

[Port bond modes for the SG6000-CN controller](#)

[Network guidelines](#)

### Port bond modes for the SG6000-CN controller

When configuring network links for the SG6000-CN, you can use port bonding for the 10/25-GbE ports that connect to the Grid Network and optional Client Network, and the 1-GbE management ports that connect to the optional Admin Network. Port bonding helps protect your data by providing redundant paths between StorageGRID networks and the appliance.

### Related information

[Configuring network links \(SG6000\)](#)

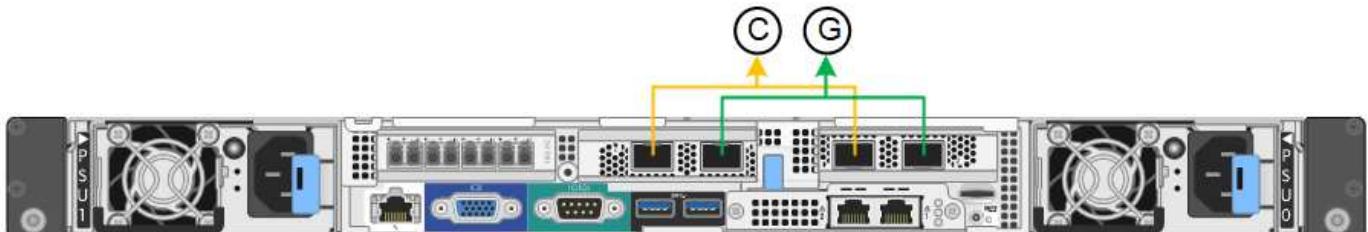
[Network bond modes for the 10/25-GbE ports](#)

The 10/25-GbE networking ports on the SG6000-CN controller support Fixed port bond

mode or Aggregate port bond mode for the Grid Network and Client Network connections.

### Fixed port bond mode

Fixed mode is the default configuration for the 10/25-GbE networking ports.



Which ports are bonded	
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

When using Fixed port bond mode, the ports can be bonded using active-backup mode or Link Aggregation Control Protocol mode (LACP 802.3ad).

- In active-backup mode (default), only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Port 4 provides a backup path for port 2 (Grid Network), and port 3 provides a backup path for port 1 (Client Network).
- In LACP mode, each pair of ports forms a logical channel between the controller and the network, allowing for higher throughput. If one port fails, the other port continues to provide the channel. Throughput is reduced, but connectivity is not impacted.

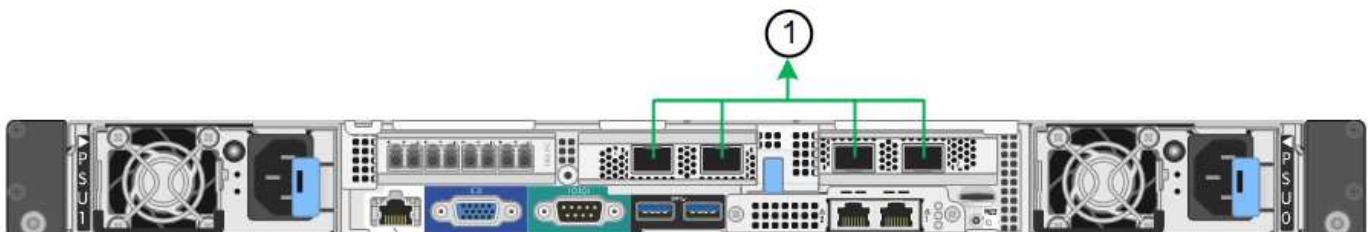
If you do not need redundant connections, you can use only one port for each network.

 However, be aware that an alert will be triggered in the Grid Manager after StorageGRID is installed, indicating that the link is down. Because this port is disconnected on purpose, you can safely disable this alert.

From the Grid Manager, select **Alert > Rules**, select the rule, and click **Edit rule**. Then, uncheck the **Enabled** check box.

### Aggregate port bond mode

Aggregate port bond mode significantly increases the throughput for each StorageGRID network and provides additional failover paths.



Which ports are bonded	
1	All connected ports are grouped in a single LACP bond, allowing all ports to be used for Grid Network and Client Network traffic.

If you plan to use aggregate port bond mode:

- You must use LACP network bond mode.
- You must specify a unique VLAN tag for each network. This VLAN tag will be added to each network packet to ensure that network traffic is routed to the correct network.
- The ports must be connected to switches that can support VLAN and LACP. If multiple switches are participating in the LACP bond, the switches must support multi-chassis link aggregation groups (MLAG), or equivalent.
- You must understand how to configure the switches to use VLAN, LACP, and MLAG, or equivalent.

If you do not want to use all four 10/25-GbE ports, you can use one, two, or three ports. Using more than one port maximizes the chance that some network connectivity will remain available if one of the 10/25-GbE ports fails.



If you choose to use fewer than four ports, be aware that one or more alarms will be raised in the Grid Manager after StorageGRID is installed, indicating that cables are unplugged. You can safely acknowledge the alarms to clear them.

#### Network bond modes for the 1-GbE management ports

For the two 1-GbE management ports on the SG6000-CN controller, you can choose Independent network bond mode or Active-Backup network bond mode to connect to the optional Admin Network.

In Independent mode, only the management port on the left is connected to the Admin Network. This mode does not provide a redundant path. The management port on the right is unconnected and available for temporary local connections (uses IP address 169.254.0.1)

In Active-Backup mode, both management ports are connected to the Admin Network. Only one port is active at a time. If the active port fails, its backup port automatically provides a failover connection. Bonding these two physical ports into one logical management port provides a redundant path to the Admin Network.



If you need to make a temporary local connection to the SG6000-CN controller when the 1-GbE management ports are configured for Active-Backup mode, remove the cables from both management ports, plug your temporary cable into the management port on the right, and access the appliance using IP address 169.254.0.1.



Network bond mode	
A	Both management ports are bonded into one logical management port connected to the Admin Network.
I	The port on the left is connected to the Admin Network. The port on the right is available for temporary local connections (IP address 169.254.0.1).

## Gathering installation information (SG6000)

As you install and configure the StorageGRID appliance, you must make decisions and gather information about Ethernet switch ports, IP addresses, and port and network bond modes.

### About this task

You can use the following tables to record the required information for each network you connect to the appliance. These values are required to install and configure the hardware.

### Information needed to connect to SANtricity System Manager on the storage controllers

You must connect both of the storage controllers in the appliance (either the E2800 controllers or the EF570 controllers) to the management network you will use for SANtricity System Manager. The controllers are located in each appliance as follows:

- SG6060: Controller A is on the top, and controller B is on the bottom.
- SGF6024: Controller A is on the left, and controller B is on the right.

Information needed	Your value for controller A	Your value for controller B
Ethernet switch port you will connect to management port 1 (labeled as P1 on the controller)		
MAC address for management port 1 (printed on a label near port P1)		
DHCP-assigned IP address for management port 1, if available after power on		
<b>Note:</b> If the network you will connect to the storage controller includes a DHCP server, the network administrator can use the MAC address to determine the IP address that was assigned by the DHCP server.		

Information needed	Your value for controller A	Your value for controller B
Static IP address you plan to use for the appliance on the management network	For IPv4: <ul style="list-style-type: none"> <li>IPv4 address:</li> <li>Subnet mask:</li> <li>Gateway:</li> </ul> For IPv6: <ul style="list-style-type: none"> <li>IPv6 address:</li> <li>Routable IP address:</li> <li>storage controller router IP address:</li> </ul>	For IPv4: <ul style="list-style-type: none"> <li>IPv4 address:</li> <li>Subnet mask:</li> <li>Gateway:</li> </ul> For IPv6: <ul style="list-style-type: none"> <li>IPv6 address:</li> <li>Routable IP address:</li> <li>storage controller router IP address:</li> </ul>
IP address format	Choose one: <ul style="list-style-type: none"> <li>IPv4</li> <li>IPv6</li> </ul>	Choose one: <ul style="list-style-type: none"> <li>IPv4</li> <li>IPv6</li> </ul>
Speed and duplex mode	Must be: <ul style="list-style-type: none"> <li>Autonegotiate (default)</li> </ul>	Must be: <ul style="list-style-type: none"> <li>Autonegotiate (default)</li> </ul>

### Information needed to connect the SG6000-CN controller to the Admin Network

The Admin Network for StorageGRID is an optional network, used for system administration and maintenance. The appliance connects to the Admin Network using the following 1-GbE management ports on the SG6000-CN controller.



Information needed	Your value
Admin Network enabled	Choose one: <ul style="list-style-type: none"> <li>No</li> <li>Yes (default)</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>Independent (default)</li> <li>Active-Backup</li> </ul>

Information needed	Your value
Switch port for the left port in the red circle in the diagram (default active port for Independent network bond mode)	
Switch port for the right port in the red circle in the diagram (Active-Backup network bond mode only)	
<p>MAC address for the Admin Network port</p> <p><b>Note:</b> The MAC address label on the front of the SG6000-CN controller lists the MAC address for the BMC management port. To determine the MAC address for the Admin Network port, you must add <b>2</b> to the hexadecimal number on the label. For example, if the MAC address on the label ends in <b>09</b>, the MAC address for the Admin Port would end in <b>0B</b>. If the MAC address on the label ends in <b>(y)FF</b>, the MAC address for the Admin Port would end in <b>(y+1)01</b>. You can easily make this calculation by opening Calculator in Windows, setting it to Programmer mode, selecting Hex, typing the MAC address, then typing <b>+ 2 =</b>.</p>	
<p>DHCP-assigned IP address for the Admin Network port, if available after power on</p> <p><b>Note:</b> You can determine the DHCP-assigned IP address by using the MAC address to look up the assigned IP.</p>	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
<p>Static IP address you plan to use for the appliance Storage Node on the Admin Network</p> <p><b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.</p>	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>
Admin Network subnets (CIDR)	

### Information needed to connect and configure the 10/25-GbE ports on the SG6000-CN controller

The four 10/25-GbE ports on the SG6000-CN controller connect to the StorageGRID Grid Network and the optional Client Network.

Information needed	Your value
Link speed	Choose one: <ul style="list-style-type: none"> <li>• Auto (default)</li> <li>• 10 GbE</li> <li>• 25 GbE</li> </ul>
Port bond mode	Choose one: <ul style="list-style-type: none"> <li>• Fixed (default)</li> <li>• Aggregate</li> </ul>
Switch port for port 1 (Client Network for Fixed mode)	
Switch port for port 2 (Grid Network for Fixed mode)	
Switch port for port 3 (Client Network for Fixed mode)	
Switch port for port 4 (Grid Network for Fixed mode)	

#### Information needed to connect the SG6000-CN controller to the Grid Network

The Grid Network for StorageGRID is a required network, used for all internal StorageGRID traffic. The appliance connects to the Grid Network using the 10/25-GbE ports on the SG6000-CN controller.

Information needed	Your value
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>• Active-Backup (default)</li> <li>• LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>• No (default)</li> <li>• Yes</li> </ul>
VLAN tag(if VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Grid Network, if available after power on	<ul style="list-style-type: none"> <li>• IPv4 address (CIDR):</li> <li>• Gateway:</li> </ul>

Information needed	Your value
Static IP address you plan to use for the appliance Storage Node on the Grid Network  <b>Note:</b> If your network does not have a gateway, specify the same static IPv4 address for the gateway.	<ul style="list-style-type: none"> <li>IPv4 address (CIDR):</li> <li>Gateway:</li> </ul>
Grid Network subnets (CIDRs)	

### Information needed to connect the SG6000-CN controller to the Client Network

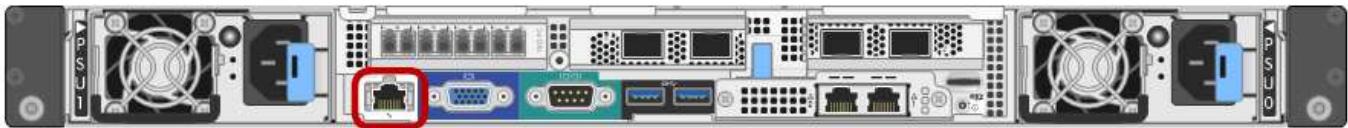
The Client Network for StorageGRID is an optional network, typically used to provide client protocol access to the grid. The appliance connects to the Client Network using the 10/25-GbE ports on the SG6000-CN controller.

Information needed	Your value
Client Network enabled	Choose one: <ul style="list-style-type: none"> <li>No (default)</li> <li>Yes</li> </ul>
Network bond mode	Choose one: <ul style="list-style-type: none"> <li>Active-Backup (default)</li> <li>LACP (802.3ad)</li> </ul>
VLAN tagging enabled	Choose one: <ul style="list-style-type: none"> <li>No (default)</li> <li>Yes</li> </ul>
VLAN tag (If VLAN tagging is enabled)	Enter a value between 0 and 4095:
DHCP-assigned IP address for the Client Network, if available after power on	<ul style="list-style-type: none"> <li>IPv4 address (CIDR):</li> <li>Gateway:</li> </ul>
Static IP address you plan to use for the appliance Storage Node on the Client Network  <b>Note:</b> If the Client Network is enabled, the default route on the controller will use the gateway specified here.	<ul style="list-style-type: none"> <li>IPv4 address (CIDR):</li> <li>Gateway:</li> </ul>

### Information needed to connect the SG6000-CN controller to the BMC management network

You can access the BMC interface on the SG6000-CN controller using the following 1-GbE management port. This port supports remote management of the controller hardware over Ethernet using the Intelligent Platform

Management Interface (IPMI) standard.



Information needed	Your value
Ethernet switch port you will connect to the BMC management port (circled in the diagram)	
DHCP-assigned IP address for the BMC management network, if available after power on	<ul style="list-style-type: none"><li>• IPv4 address (CIDR):</li><li>• Gateway:</li></ul>
Static IP address you plan to use for the BMC management port	<ul style="list-style-type: none"><li>• IPv4 address (CIDR):</li><li>• Gateway:</li></ul>

#### Related information

[Controllers in the SG6000 appliances](#)

[Reviewing appliance network connections](#)

[Port bond modes for the SG6000-CN controller](#)

[Cabling the appliance \(SG6000\)](#)

[Configuring StorageGRID IP addresses](#)

## Installing the hardware

Hardware installation entails installing the SG6000-CN controller and the storage controller shelf into a cabinet or rack, connecting the cables, and applying power.

### Steps

- [Registering the hardware](#)
- [SG6060: Installing 60-drive shelves into a cabinet or rack](#)
- [SG6060: Installing the drives](#)
- [SGF6024: Installing 24-drive shelves into a cabinet or rack](#)
- [SG6000-CN: Installing into a cabinet or rack](#)
- [Cabling the appliance \(SG6000\)](#)
- [SG6060: Cabling the optional expansion shelves](#)
- [Connecting power cords and applying power \(SG6000\)](#)
- [Viewing status indicators and buttons on the SG6000-CN controller](#)
- [Viewing boot-up status codes for the SG6000 storage controllers](#)

## Registering the hardware

Registering the appliance hardware provides support benefits.

### Steps

1. Locate the chassis serial number for the storage controller shelf.

You can find the number on the packing slip, in your confirmation email, or on the appliance after you unpack it.



There are several serial numbers on the storage appliance. The serial number on the storage controller shelf is the one that must be registered and used if you call for service or support on the appliance.

2. Go to the NetApp Support Site at [mysupport.netapp.com](http://mysupport.netapp.com).
3. Determine whether you need to register the hardware:

If you are a...	Follow these steps...
Existing NetApp customer	<ol style="list-style-type: none"><li>Sign in with your username and password.</li><li>Select <b>Products &gt; My Products</b>.</li><li>Confirm that the new serial number is listed.</li><li>If it is not, follow the instructions for new NetApp customers.</li></ol>
New NetApp customer	<ol style="list-style-type: none"><li>Click <b>Register Now</b>, and create an account.</li><li>Select <b>Products &gt; Register Products</b>.</li><li>Enter the product serial number and requested details.</li></ol> <p>After your registration is approved, you can download any required software. The approval process might take up to 24 hours.</p>

## SG6060: Installing 60-drive shelves into a cabinet or rack

You must install a set of rails for the E2860 controller shelf in your cabinet or rack, and then slide the controller shelf onto the rails. If you are installing 60-drive expansion shelves, the same procedure applies.

### What you'll need

- You have reviewed the Safety Notices document included in the box, and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.

-  Each 60-drive shelf weighs approximately 132 lb (60 kg) without drives installed. Four people or a mechanized lift are required to safely move the shelf.
-  To avoid damaging the hardware, never move the shelf if drives are installed. You must remove all drives before moving the shelf.
-  When installing the E2860 controller shelf or optional expansion shelves, install hardware from the bottom to the top of the rack or cabinet to prevent the equipment from tipping over. To ensure that the heaviest equipment is at the bottom of the cabinet or rack, install the SG6000-CN controller above the E2860 controller shelf and expansion shelves.
-  Before committing to the installation, verify that the 0.5m optic cables shipped with the appliance, or cables that you supply, are long enough for the planned layout.

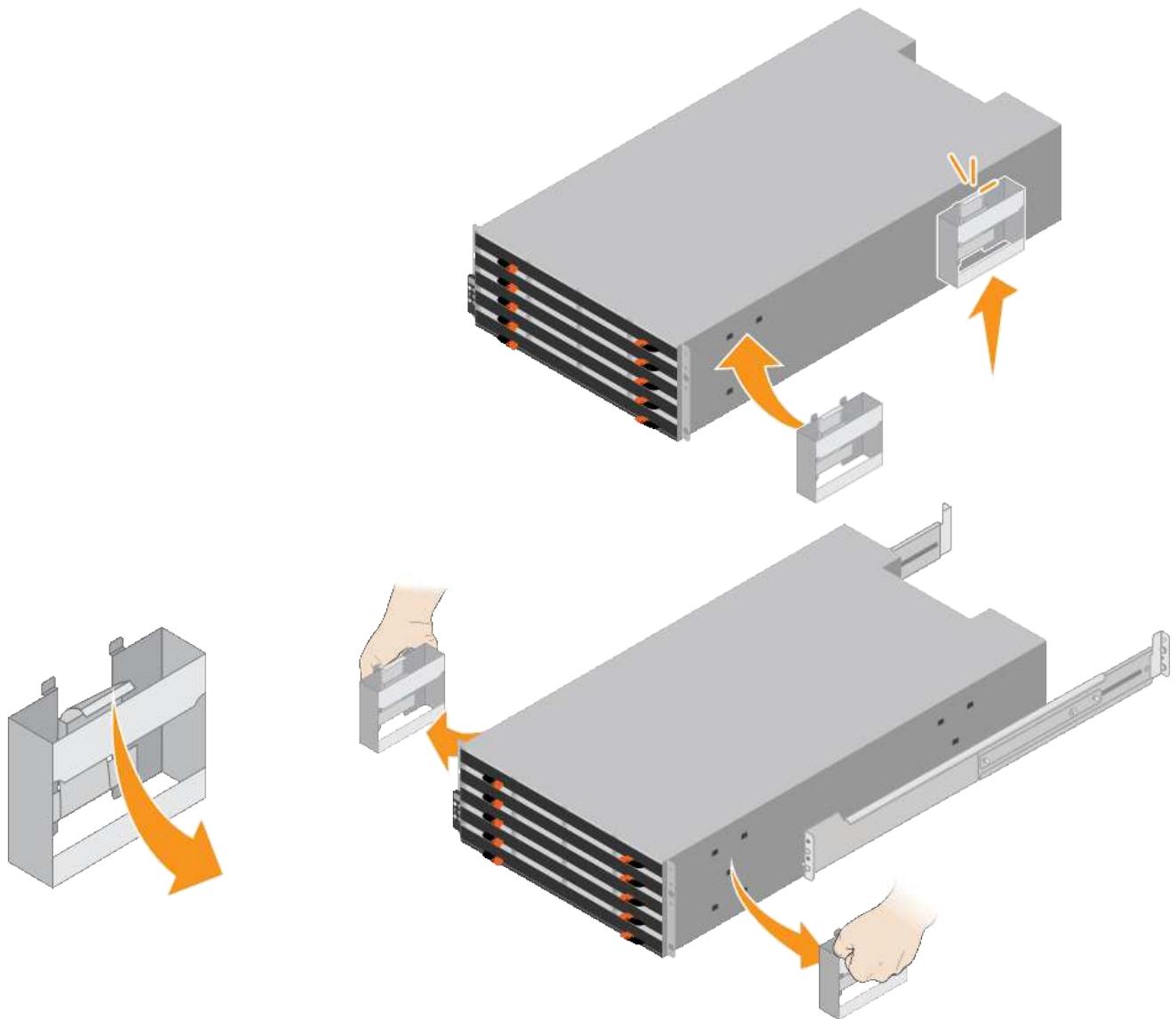
## Steps

1. Carefully follow the instructions for the rail kit to install the rails in your cabinet or rack.

For square hole cabinets, you must first install the provided cage nuts to secure the front and rear of the shelf with screws.

2. Remove the outer packing box for the appliance. Then, fold down the flaps on the inner box.
3. If you are lifting the appliance by hand, attach the four handles to the sides of the chassis.

Push up on each handle until it clicks into place.



4. Place the back of the shelf (the end with the connectors) on the rails.
5. Supporting the shelf from the bottom, slide it into the cabinet. If you are using the handles, use the thumb latches to detach one handle at a time as you slide the shelf in.

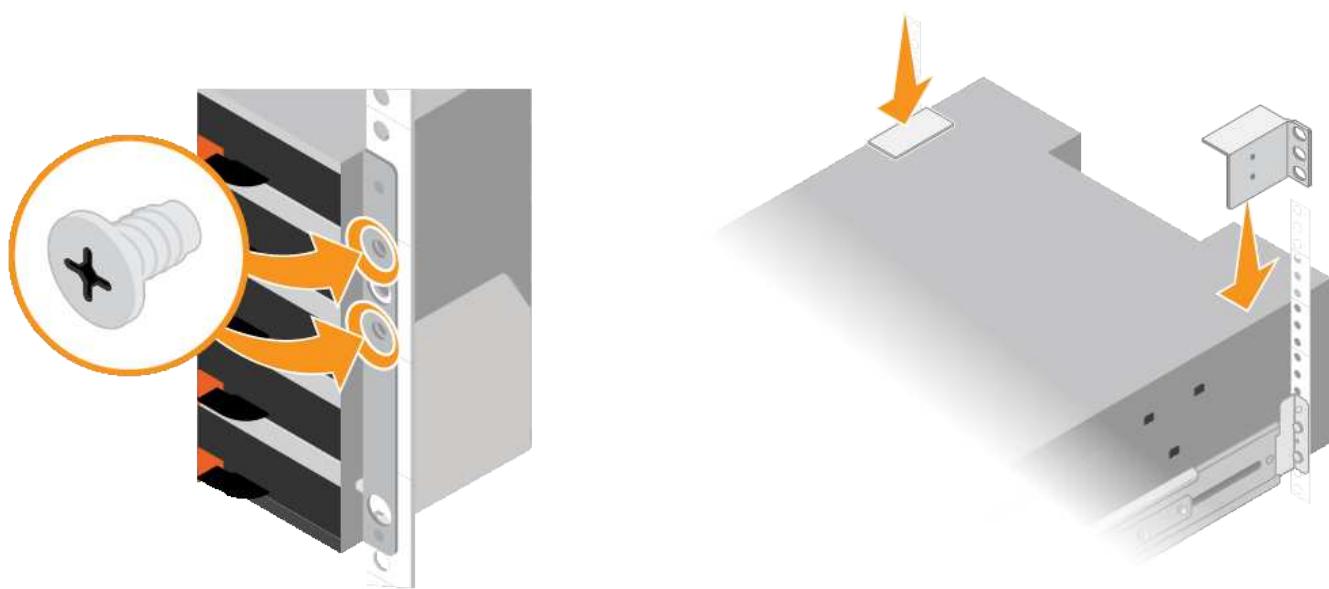
To remove the handles, pull back on the release latch, push down, then pull away from the shelf.

6. Secure the shelf to the front of the cabinet.

Insert screws into the first and third holes from the top of the shelf on both sides.

7. Secure the shelf to the rear of the cabinet.

Place two back brackets on each side of the upper rear section of the shelf. Insert screws into the first and third holes of each bracket.



8. Repeat these steps for any expansion shelves.

## SG6060: Installing the drives

After installing the 60-drive shelf into a cabinet or rack, you must install all 60 drives into the shelf. The shipment for the E2860 controller shelf includes two SSD drives, which you should install in the top drawer of the controller shelf. Each optional expansion shelf includes 60 HDD drives and no SSD drives.

### What you'll need

You have installed the E2860 controller shelf or optional expansion shelves (one or two) in the cabinet or rack.



To avoid damaging the hardware, never move the shelf if drives are installed. You must remove all drives before moving the shelf.

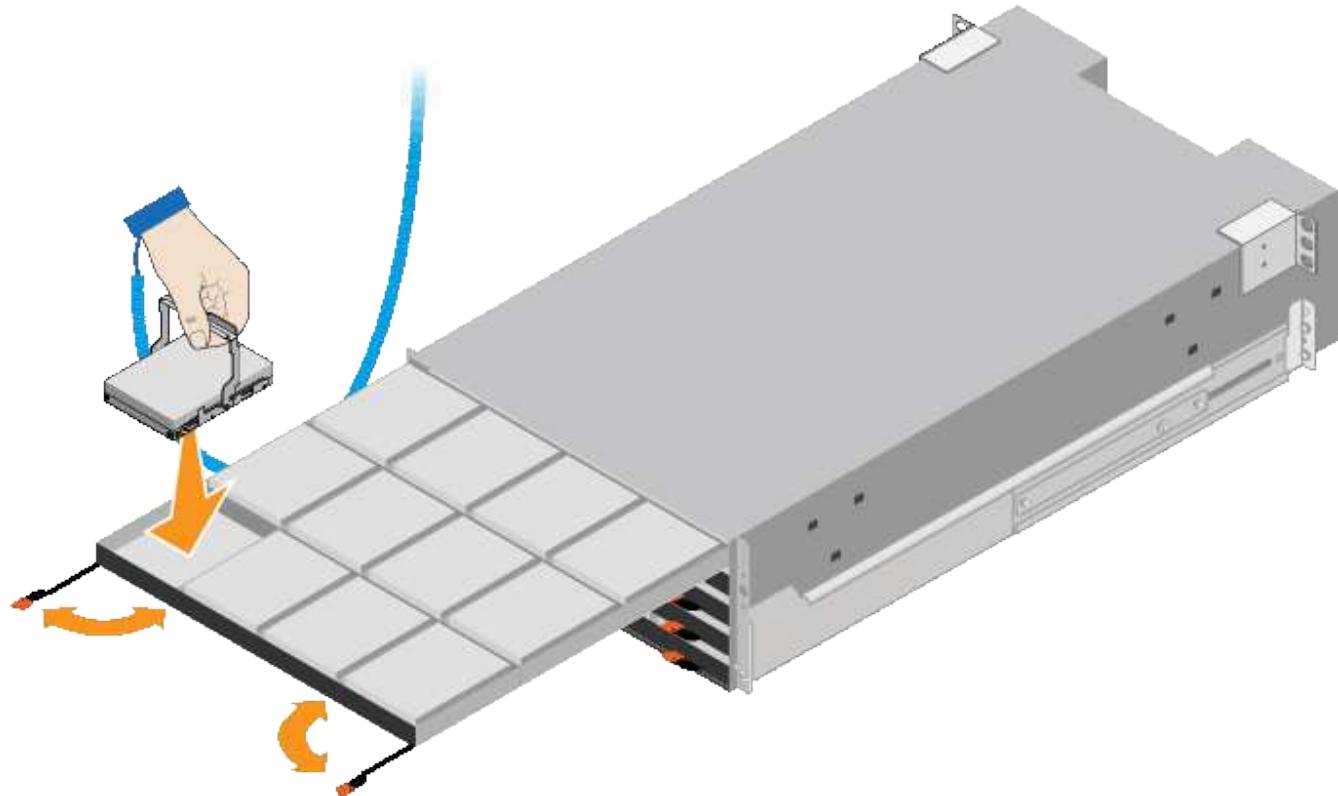
### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Remove the drives from their packaging.
3. Release the levers on the top drive drawer, and slide the drawer out using the levers.
4. Locate the two SSD drives.



Expansion shelves do not use SSD drives.

5. Raise each drive handle to a vertical position.
6. Install the two SSD drives in slots 0 and 1 (the first two slots along the lefthand side of the drawer).
7. Gently position each drive into its slot, and lower the raised drive handle until it clicks into place.



8. Install 10 HDD drives into the top drawer.

9. Slide the drawer back in by pushing on the center and closing both levers gently.



Stop pushing the drawer if you feel binding. Use the release levers at the front of the drawer to slide the drawer back out. Then, carefully reinsert the drawer into the slot.

10. Repeat these steps to install HDD drives into the other four drawers.



You must install all 60 drives to ensure correct operation.

11. Attach the front bezel to the shelf.

12. If you have expansion shelves, repeat these steps to install 12 HDD drives into each drawer of each expansion shelf.

13. Proceed to the instructions for installing the SG6000-CN into a cabinet or rack.

## SGF6024: Installing 24-drive shelves into a cabinet or rack

You must install a set of rails for the EF570 controller shelf in your cabinet or rack, and then slide the array onto the rails.

### What you'll need

- You have reviewed the Safety Notices document included in the box, and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.

### Steps

1. Carefully follow the instructions for the rail kit to install the rails in your cabinet or rack.

For square hole cabinets, you must first install the provided cage nuts to secure the front and rear of the shelf with screws.

2. Remove the outer packing box for the appliance. Then, fold down the flaps on the inner box.

3. Place the back of the shelf (the end with the connectors) on the rails.



A fully loaded shelf weighs approximately 52 lb (24 kg). Two persons are required to safely move the enclosure.

4. Carefully slide the enclosure all the way onto the rails.



You might need to adjust the rails to ensure that the enclosure slides all the way onto the rails.

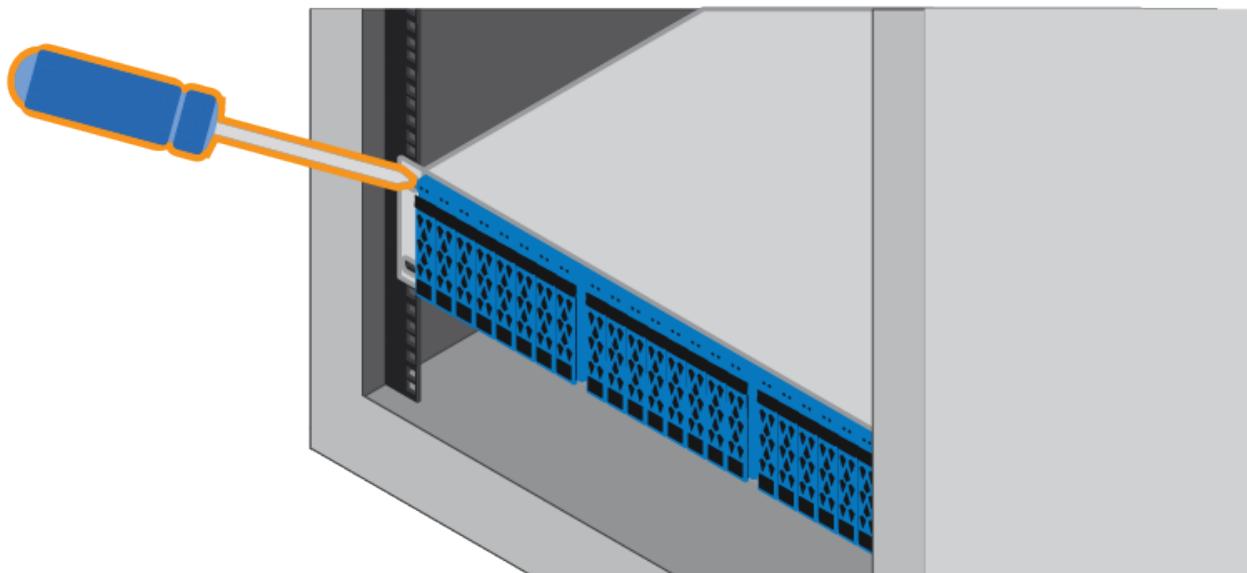


Do not place additional equipment on the rails after you finish installing the enclosure. The rails are not designed to bear additional weight.



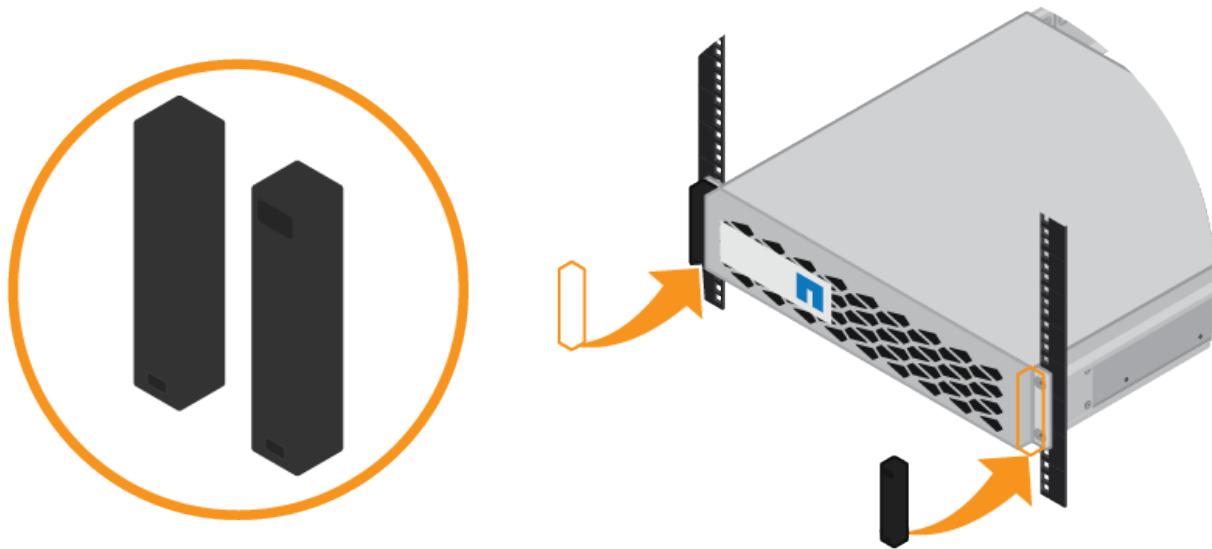
If applicable, you might need to remove the shelf end caps or the system bezel to secure the enclosure to the rack post; if so, you need to replace the end caps or bezel when you are done.

5. Secure the enclosure to the front of the cabinet or rack and rails by inserting two M5 screws through the mounting brackets (preinstalled on either side of the front of the enclosure), the holes on the rack or system cabinet, and the holes on the front of rails.



6. Secure the enclosure to the back of the rails by inserting two M5 screws through the brackets at the enclosure and the rail kit bracket.

7. If applicable, replace the shelf end caps or the system bezel.



## SG6000-CN: Installing into a cabinet or rack

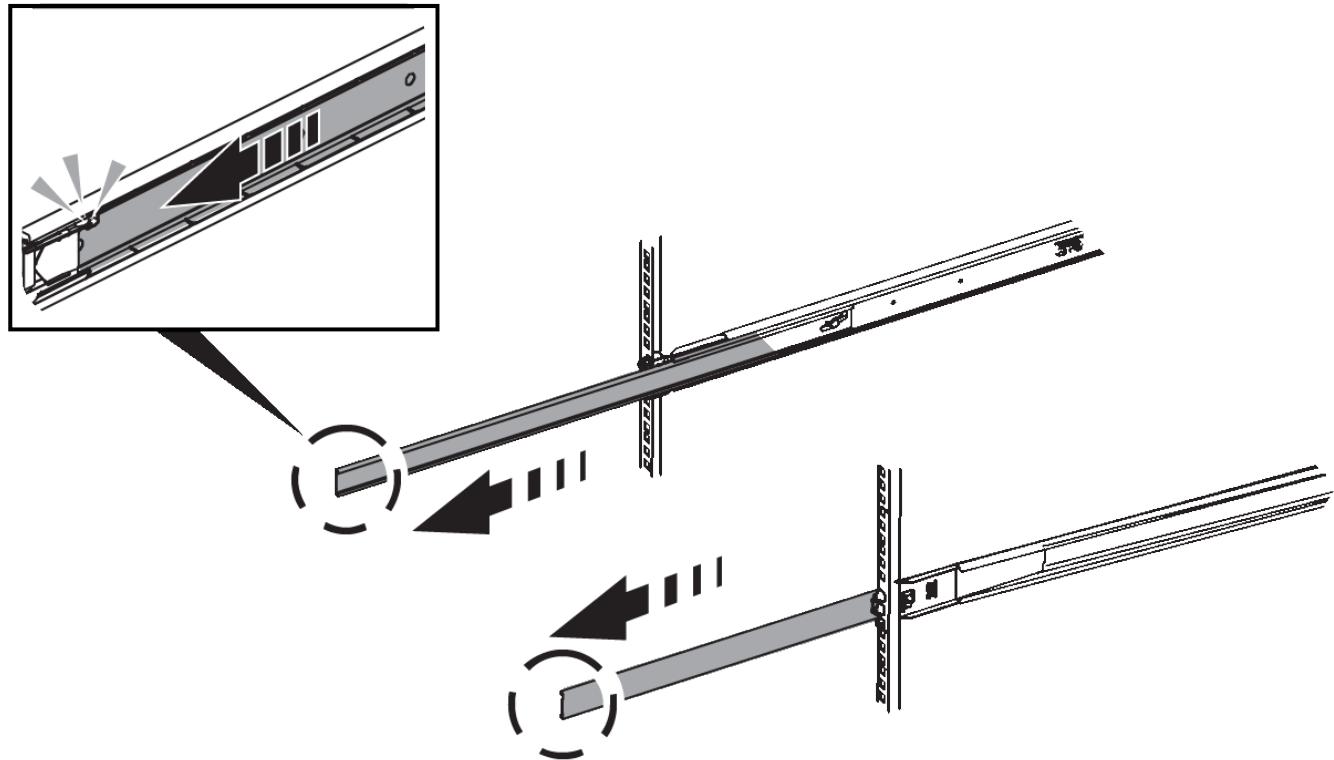
You must install a set of rails for the SG6000-CN controller in your cabinet or rack, and then slide the controller onto the rails.

### What you'll need

- You have reviewed the Safety Notices document included in the box, and understand the precautions for moving and installing hardware.
- You have the instructions packaged with the rail kit.
- You have installed the E2860 controller shelf and drives or the EF570 controller shelf.

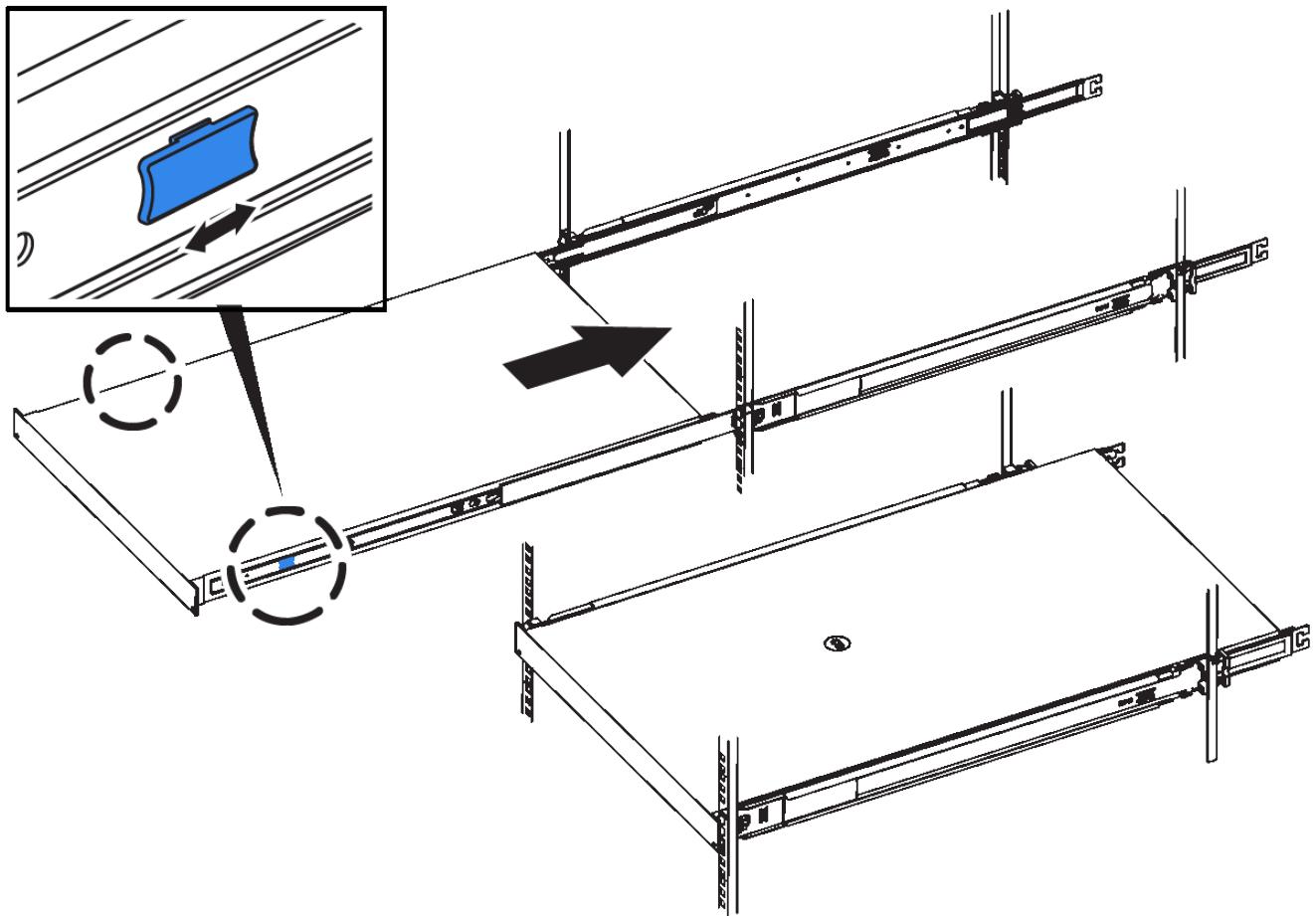
### Steps

1. Carefully follow the instructions for the rail kit to install the rails in your cabinet or rack.
2. On the two rails installed in the cabinet or rack, extend the movable parts of the rails until you hear a click.



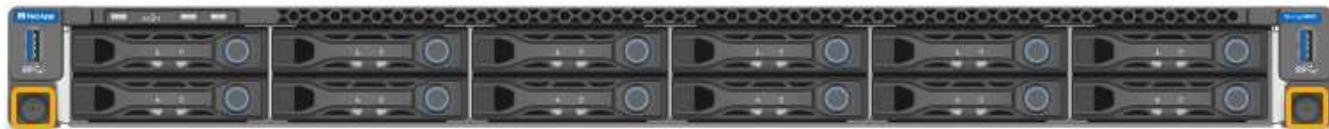
3. Insert the SG6000-CN controller into the rails.
4. Slide the controller into the cabinet or rack.

When you cannot move the controller any further, pull the blue latches on both sides of the chassis to slide the controller all the way in.



Do not attach the front bezel until after you power on the controller.

5. Tighten the captive screws on the controller front panel to secure the controller in the rack.



## Cabling the appliance (SG6000)

You must connect the storage controllers to the SG6000-CN controller, connect the management ports on all three controllers, and connect the network ports on the SG6000-CN controller to the Grid Network and optional Client Network for StorageGRID.

### What you'll need

- You have the four optical cables provided with the appliance for connecting the two storage controllers to the SG6000-CN controller.
- You have RJ-45 Ethernet cables (four minimum) for connecting the management ports.
- You have one of the following options for the network ports. These items are not provided with the appliance.
  - One to four TwinAx cables for connecting the four network ports.

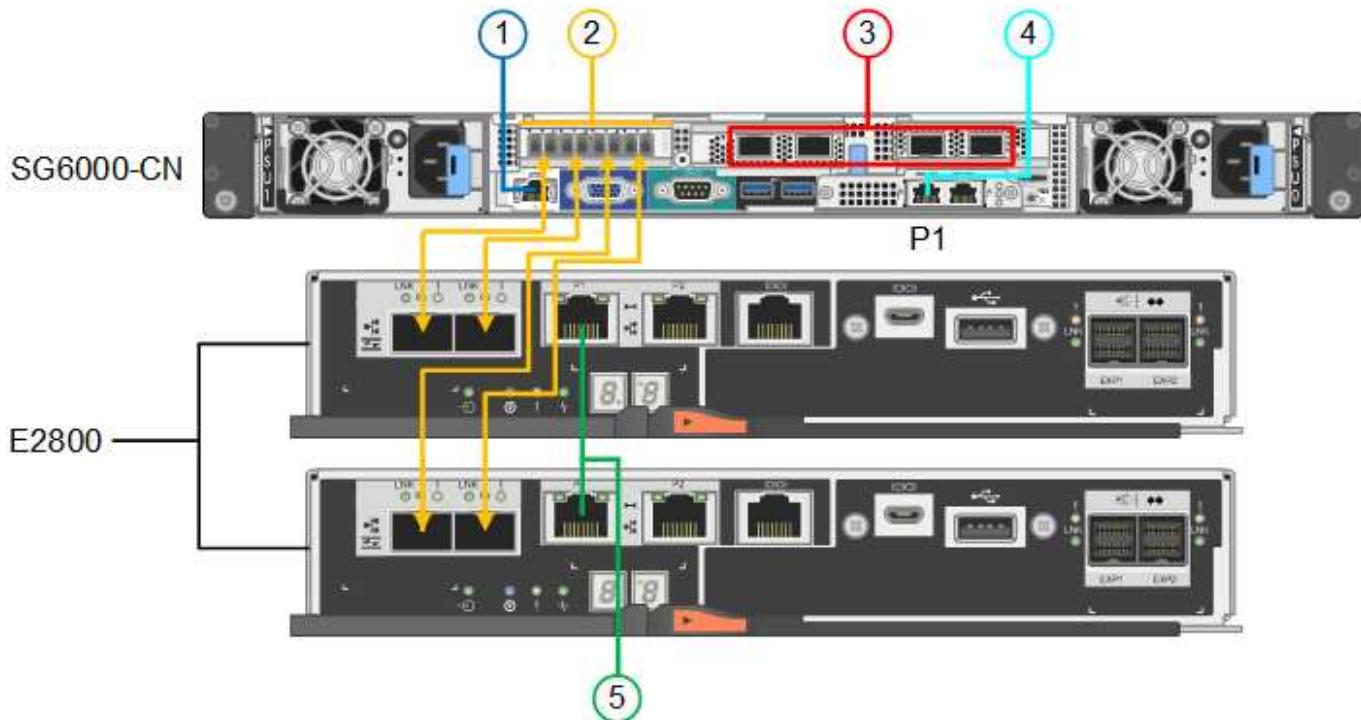
- One to four SFP+ or SFP28 transceivers if you plan to use optical cables for the ports.



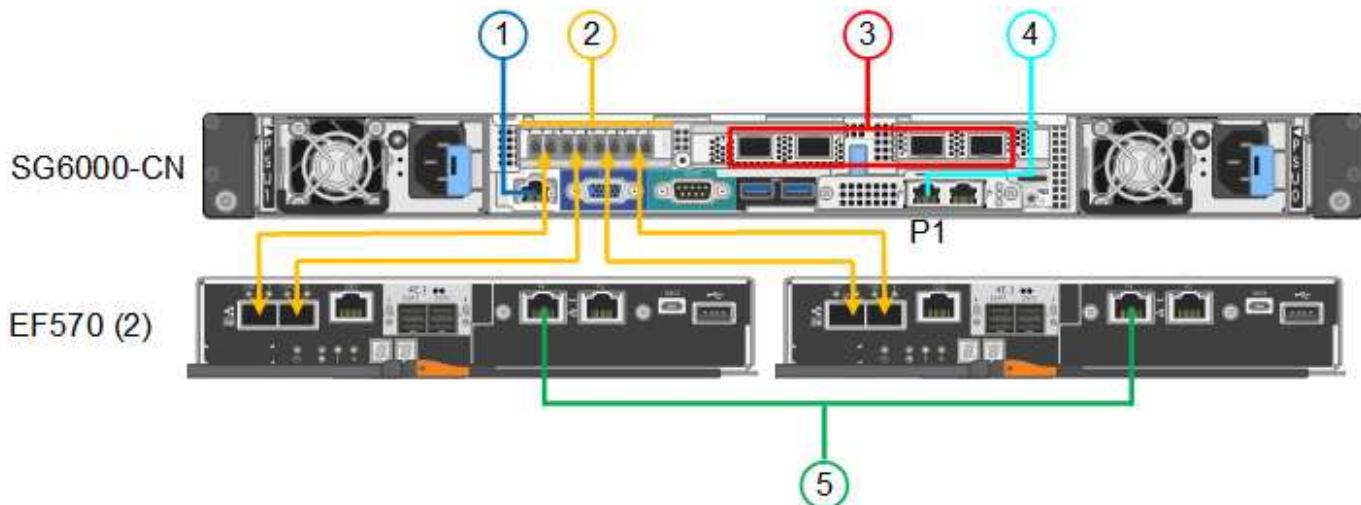
**Risk of exposure to laser radiation** — Do not disassemble or remove any part of an SFP transceiver. You might be exposed to laser radiation.

## About this task

The following figure shows the three controllers in the SG6060 appliance, with the SG6000-CN compute controller on the top and the two E2800 storage controllers on the bottom.



The following figure shows the three controllers in the SGF6024 appliance, with the SG6000-CN compute controller on the top and the two EF570 storage controllers side by side below the compute controller.



	Port	Type of port	Function
1	BMC management port on the SG6000-CN controller	1-GbE (RJ-45)	Connects to the network where you access the BMC interface.
2	FC connection ports: <ul style="list-style-type: none"> <li>• 4 on the SG6000-CN controller</li> <li>• 2 on each storage controller</li> </ul>	16-Gb/s FC optical SFP+	Connect each storage controller to the SG6000-CN controller.
3	Four network ports on the SG6000-CN controller	10/25-GbE	Connect to the Grid Network and the Client Network for StorageGRID.
4	Admin Network port on the SG6000-CN controller (labelled P1 in the figure)	1-GbE (RJ-45)  <b>Important:</b> This port operates only at 1000 baseT/full and does not support 10- or 100-megabit speeds.	Connects the SG6000-CN controller to the Admin Network for StorageGRID.
4	Rightmost RJ-45 port on the SG6000-CN controller	1-GbE (RJ-45)  <b>Important:</b> This port operates only at 1000 baseT/full and does not support 10- or 100-megabit speeds.	<ul style="list-style-type: none"> <li>• Can be bonded with management port 1 if you want a redundant connection to the Admin Network.</li> <li>• Can be left unwired and available for temporary local access (IP 169.254.0.1).</li> <li>• During installation, can be used to connect the SG6000-CN controller to a service laptop if DHCP-assigned IP addresses are not available.</li> </ul>
5	Management port 1 on each storage controller	1-GbE (RJ-45)	Connects to the network where you access SANtricity System Manager.

	Port	Type of port	Function
5	Management port 2 on each storage controller	1-GbE (RJ-45)	Reserved for technical support.

## Steps

1. Connect the BMC management port on the SG6000-CN controller to the management network, using an Ethernet cable.
2. Connect the two FC ports on each storage controller to the FC ports on the SG6000-CN controller, using four optical cables and four SFP+ transceivers for the storage controllers.
3. Connect the network ports on the SG6000-CN controller to the appropriate network switches, using TwinAx cables or optical cables and SFP+ or SFP28 transceivers.



The four network ports must use the same link speed. Install SFP+ transceivers if you plan to use 10-GbE link speeds. Install SFP28 transceivers if you plan to use 25-GbE link speeds.

- If you plan to use Fixed port bond mode (default), connect the ports to the StorageGRID Grid and Client Networks, as shown in the table.

Port	Connects to...
Port 1	Client Network (optional)
Port 2	Grid Network
Port 3	Client Network (optional)
Port 4	Grid Network

- If you plan to use the Aggregate port bond mode, connect one or more of the network ports to one or more switches. You should connect at least two of the four ports to avoid having a single point of failure. If you use more than one switch for a single LACP bond, the switches must support MLAG or equivalent.

4. If you plan to use the Admin Network for StorageGRID, connect the Admin Network port on the SG6000-CN controller to the Admin Network, using an Ethernet cable.
5. Connect management port 1 (P1) on each storage controller (the RJ-45 port on the left) to the management network for SANtricity System Manager, using an Ethernet cable.

Do not use management port 2 (P2) on the storage controllers (the RJ-45 port on the right). This port is reserved for technical support.

## Related information

[Port bond modes for the SG6000-CN controller](#)

[Reinstalling the SG6000-CN controller into a cabinet or rack](#)

## SG6060: Cabling the optional expansion shelves

If you are using expansion shelves, you must connect them to the E2860 controller shelf. You can have a maximum of two expansion shelves for each SG6060 appliance.

### What you'll need

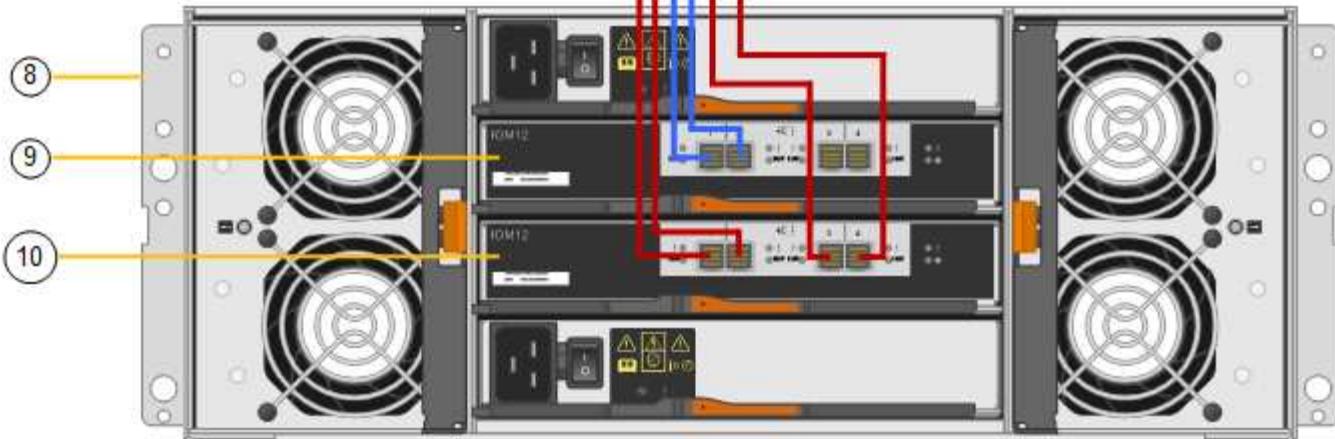
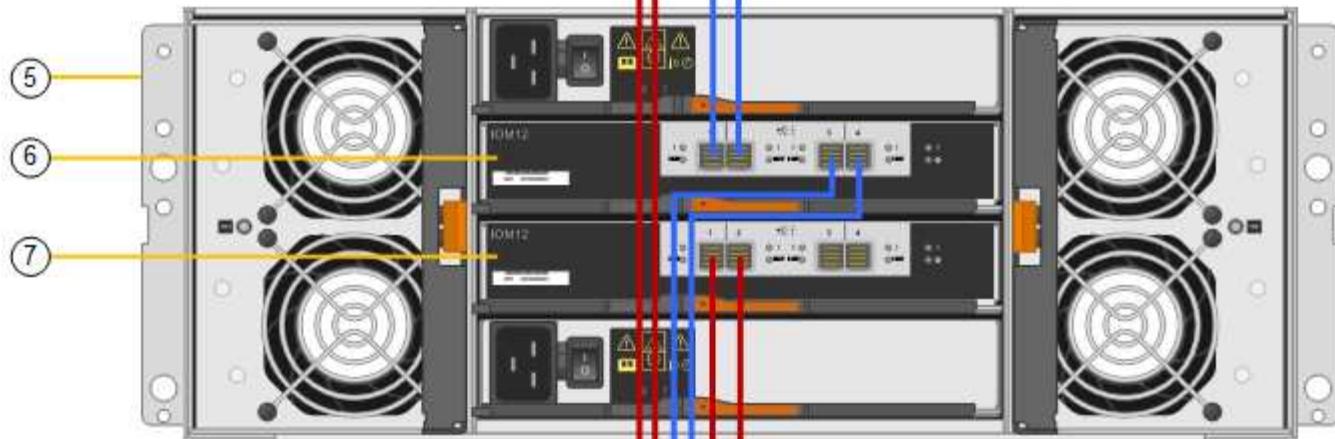
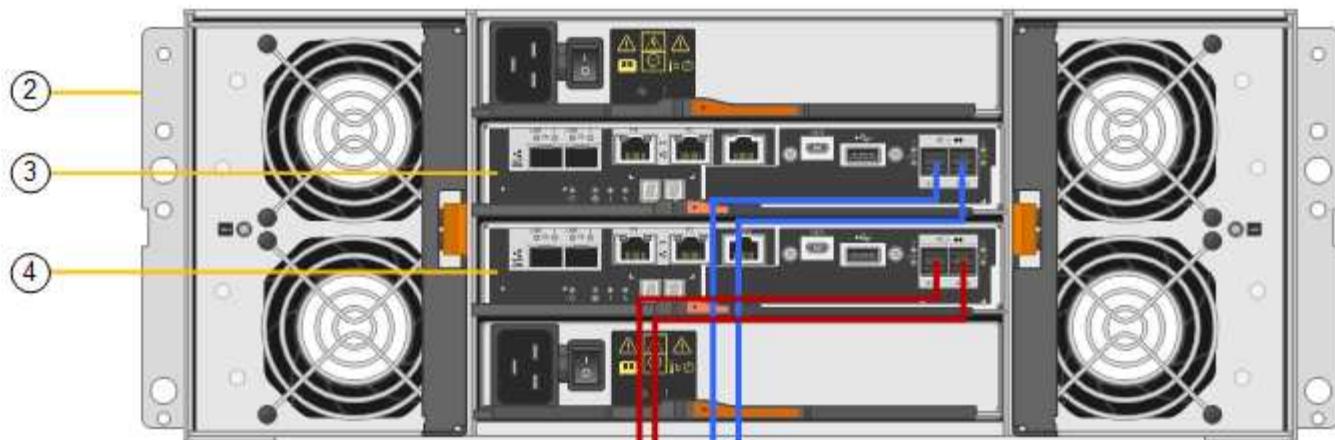
- You have the two SAS cables shipped with each expansion shelf.
- You have installed the expansion shelves in the cabinet or rack that contains the E2860 controller shelf.

[SG6060: Installing 60-drive shelves into a cabinet or rack](#)

### Step

Connect each expansion shelf to the E2860 controller shelf as shown in the diagram.

This drawing shows two expansion shelves. If you have only one, connect IOM A to controller A and connect IOM B to controller B.



	Description
1	SG6000-CN

	<b>Description</b>
2	E2860 controller shelf
3	Controller A
4	Controller B
5	Expansion shelf 1
6	IOM A for expansion shelf 1
7	IOM B for expansion shelf 1
8	Expansion shelf 2
9	IOM A for expansion shelf 2
10	IOM B for expansion shelf 2

## Connecting power cords and applying power (SG6000)

After connecting the network cables, you are ready to apply power to the SG6000-CN controller and to the two storage controllers or optional expansion shelves.

### Steps

1. Confirm that both controllers in the storage controller shelf are off.
 

 **Risk of electrical shock** — Before connecting the power cords, make sure that the power switches for each of the two storage controllers are off.
2. If you have expansion shelves, confirm that both of the IOM power switches are off.
 

 **Risk of electrical shock** — Before connecting the power cords, make sure that the two power switches for each of the expansion shelves are off.
3. Connect a power cord to each of the two power supply units in the SG6000-CN controller.
4. Connect these two power cords to two different power distribution units (PDUs) in the cabinet or rack.
5. Connect a power cord to each of the two power supply units in the storage controller shelf.
6. If you have expansion shelves, connect a power cord to each of the two power supply units in each expansion shelf.
7. Connect the two power cords in each storage shelf (including the optional expansion shelves) to two different PDUs in the cabinet or rack.
8. If the power button on the front of the SG6000-CN controller is not currently illuminated blue, press the button to turn on power to the controller.

Do not press the power button again during the power-on process.

9. Turn on the two power switches on the back of the storage controller shelf. If you have expansion shelves, turn on the two power switches for each shelf.
  - Do not turn off the power switches during the power-on process.
  - The fans in the storage controller shelf and optional expansion shelves might be very loud when they first start up. The loud noise during start-up is normal.
10. After the components have booted up, check their status.
  - Check the seven-segment display on the back of each storage controller. Refer to the article about viewing boot-up status codes for more information.
  - Verify that the power button on the front of the SG6000-CN controller is lit.
11. If errors occur, correct any issues.
12. Attach the front bezel to the SG6000-CN controller.

#### Related information

[Viewing boot-up status codes for the SG6000 storage controllers](#)

[Viewing status indicators and buttons on the SG6000-CN controller](#)

[Reinstalling the SG6000-CN controller into a cabinet or rack](#)

### Viewing status indicators and buttons on the SG6000-CN controller

The SG6000-CN controller includes indicators that help you determine the status of the controller, including the following indicators and buttons.



	Display	Description
1	Power button	<ul style="list-style-type: none"><li>• Blue: The controller is powered on.</li><li>• Off: The controller is powered off.</li></ul>
2	Reset button	<p><i>No indicator</i></p> <p>Use this button to perform a hard reset of the controller.</p>

	Display	Description
3	Identify button	<ul style="list-style-type: none"> <li>• Blinking or solid blue: Identifies the controller in the cabinet or rack.</li> <li>• Off: The controller is not visually identifiable in the cabinet or rack.</li> </ul> <p>This button can be set to Blink, On (Solid), or Off.</p>
4	Alarm LED	<ul style="list-style-type: none"> <li>• Amber: An error has occurred.</li> </ul> <p><b>Note:</b> To view the boot-up and error codes, you must access the BMC interface.</p> <ul style="list-style-type: none"> <li>• Off: No errors are present.</li> </ul>

## General boot-up codes

During boot-up or after a hard reset of the SG6000-CN controller, the following occurs:

1. The baseboard management controller (BMC) logs codes for the boot-up sequence, including any errors that occur.
2. The power button lights up.
3. If any errors occur during boot-up, the alarm LED lights up.

To view the boot-up and error codes, you must access the BMC interface.

## Related information

[Troubleshooting the hardware installation](#)

[Configuring the BMC interface](#)

[Powering on the SG6000-CN controller and verifying operation](#)

## Viewing boot-up status codes for the SG6000 storage controllers

Each storage controller has a seven-segment display that provides status codes as the controller powers up. The status codes are the same for both the E2800 controller and the EF570 controller.

### About this task

For descriptions of these codes, see the E-Series system monitoring information for your storage controller type.

### Steps

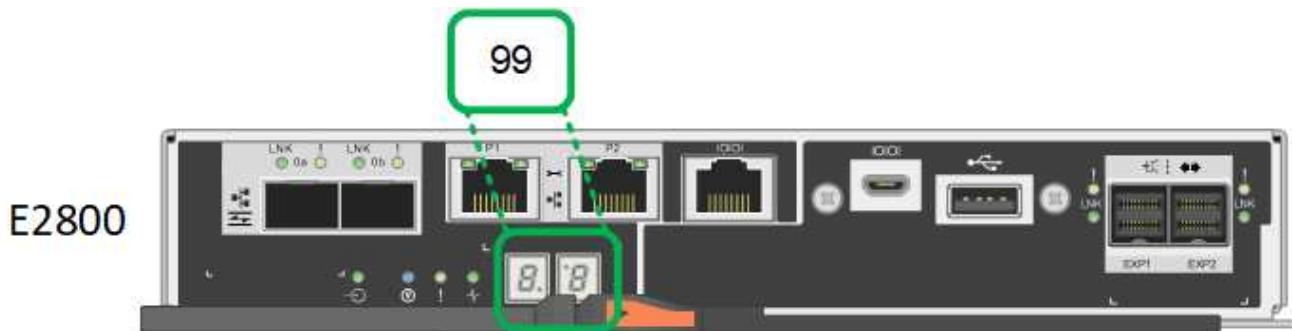
1. During boot-up, monitor progress by viewing the codes shown on the seven-segment display for each

storage controller.

The seven-segment display on each storage controller shows the repeating sequence **OS, Sd, blank** to indicate that the controller is performing start-of-day processing.

2. After the controllers have booted up, confirm that each storage controller shows 99, which is the default ID for an E-Series controller shelf.

Make sure this value is displayed on both storage controllers, as shown in this example E2800 controller.



3. If one or both controllers show other values, see the information about troubleshooting the hardware installation, and confirm you completed the installation steps correctly. If you are unable to resolve the problem, contact technical support.

#### Related information

[E5700 and E2800 System Monitoring Guide](#)

[Troubleshooting the hardware installation](#)

[NetApp Support](#)

[Powering on the SG6000-CN controller and verifying operation](#)

## Configuring the hardware

After applying power to the appliance, you must configure the network connections that will be used by StorageGRID. You must configure SANtricity System Manager, which is the software you will use to monitor the storage controllers and other hardware in the controller shelf. You must also ensure that you can access the BMC interface for the SG6000-CN controller.

#### Steps

- [Configuring StorageGRID connections](#)
- [Accessing and Configuring SANtricity System Manager](#)
- [Configuring the BMC interface](#)
- [Optional: Enabling node encryption](#)
- [Optional: Changing the RAID mode \(SG6000 only\)](#)
- [Optional: Remapping network ports for the appliance](#)

## Configuring StorageGRID connections

Before you can deploy a StorageGRID appliance as a Storage Node in a StorageGRID system, you must configure the connections between the appliance and the networks you plan to use. You can configure networking by browsing to the StorageGRID Appliance Installer, which is pre-installed on the SG6000-CN controller (the compute controller).

### Steps

- [Accessing the StorageGRID Appliance Installer](#)
- [Verifying and upgrading the StorageGRID Appliance Installer version](#)
- [Configuring network links \(SG6000\)](#)
- [Configuring StorageGRID IP addresses](#)
- [Verifying network connections](#)
- [Verifying port-level network connections](#)

### Accessing the StorageGRID Appliance Installer

You must access the StorageGRID Appliance Installer to verify the installer version and configure the connections between the appliance and the three StorageGRID networks: the Grid Network, the Admin Network (optional), and the Client Network (optional).

#### What you'll need

- You are using any management client that can connect to the StorageGRID Admin Network, or you have a service laptop.
- The client or service laptop has a supported web browser.
- The SG6000-CN controller is connected to all of the StorageGRID networks you plan to use.
- You know the IP address, gateway, and subnet for the SG6000-CN controller on these networks.
- You have configured the network switches you plan to use.

#### About this task

To initially access the StorageGRID Appliance Installer, you can use the DHCP-assigned IP address for the Admin Network port on the SG6000-CN controller (assuming the controller is connected to the Admin Network), or you can connect a service laptop directly to the SG6000-CN controller.

### Steps

1. If possible, use the DHCP address for the Admin Network port on the SG6000-CN controller to access the StorageGRID Appliance Installer.



- a. Locate the MAC address label on the front of the SG6000-CN controller, and determine the MAC address for the Admin Network port.

The MAC address label lists the MAC address for the BMC management port.

To determine the MAC address for the Admin Network port, you must add **2** to the hexadecimal number

on the label. For example, if the MAC address on the label ends in **09**, the MAC address for the Admin Port would end in **0B**. If the MAC address on the label ends in **(y)FF**, the MAC address for the Admin Port would end in **(y+1)01**. You can easily make this calculation by opening Calculator in Windows, setting it to Programmer mode, selecting Hex, typing the MAC address, then typing **+ 2 =**.

- b. Provide the MAC address to your network administrator, so they can look up the DHCP address for the appliance on the Admin Network.
- c. From the client, enter this URL for the StorageGRID Appliance Installer:  
**[https://Appliance\\_Controller\\_IP:8443](https://Appliance_Controller_IP:8443)**

For *SG6000-CN\_Controller\_IP*, use the DHCP address.

- d. If you are prompted with a security alert, view and install the certificate using the browser's installation wizard.

The alert will not appear the next time you access this URL.

The StorageGRID Appliance Installer Home page appears. The information and messages shown when you first access this page depend on how your appliance is currently connected to StorageGRID networks. Error messages might appear that will be resolved in later steps.

# NetApp® StorageGRID® Appliance Installer

[Home](#)[Configure Networking](#)[Configure Hardware](#)[Monitor Installation](#)[Advanced](#)

## Home

**ⓘ** The installation is ready to be started. Review the settings below, and then click Start Installation.

### This Node

Node type

Storage

Node name

MM-2-108-SGA-lab25

[Cancel](#)

[Save](#)

### Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

172.16.1.178

Connection state

Connection to 172.16.1.178 ready

[Cancel](#)

[Save](#)

### Installation

Current state

Ready to start installation of MM-2-108-SGA-lab25 into grid with Admin Node 172.16.1.178 running StorageGRID 11.2.0, using StorageGRID software downloaded from the Admin Node.

[Start Installation](#)

2. If you cannot obtain an IP address using DHCP, you can use a link-local connection.

- Connect a service laptop directly to the rightmost RJ-45 port on the SG6000-CN controller, using an Ethernet cable.



- Open a web browser on the service laptop.
- Enter this URL for the StorageGRID Appliance Installer:

<https://169.254.0.1:8443>

The StorageGRID Appliance Installer Home page appears. The information and messages shown when you first access this page depend on how your appliance is currently connected.



If you cannot access the Home page over a link-local connection, configure the service laptop IP address as 169.254.0.2, and try again.

## After you finish

After accessing the StorageGRID Appliance Installer:

- Verify that the StorageGRID Appliance Installer version on the appliance matches the software version installed on your StorageGRID system. Upgrade StorageGRID Appliance Installer, if necessary.

### [Verifying and upgrading the StorageGRID Appliance Installer version](#)

- Review any messages displayed on the StorageGRID Appliance Installer Home page and configure the link configuration and the IP configuration, as required.

## Related information

[Web browser requirements](#)

## Verifying and upgrading the StorageGRID Appliance Installer version

The StorageGRID Appliance Installer version on the appliance must match the software version installed on your StorageGRID system to ensure that all StorageGRID features are supported.

### What you'll need

You have accessed the StorageGRID Appliance Installer.

### About this task

StorageGRID appliances come from the factory preinstalled with the StorageGRID Appliance Installer. If you are adding an appliance to a recently upgraded StorageGRID system, you might need to manually upgrade the StorageGRID Appliance Installer before installing the appliance as a new node.

The StorageGRID Appliance Installer automatically upgrades when you upgrade to a new StorageGRID version. You do not need to upgrade the StorageGRID Appliance Installer on installed appliance nodes. This procedure is only required when you are installing an appliance that contains an earlier version of the StorageGRID Appliance Installer.

### Steps

- From the StorageGRID Appliance Installer, select **Advanced > Upgrade Firmware**.
- Compare the Current Firmware version to the software version installed on your StorageGRID system (from the Grid Manager select **Help > About**).

The second digit in the two versions should match. For example, if your StorageGRID system is running version 11.5.x.y, the StorageGRID Appliance Installer version should be 3.5.z.

- If the appliance has a down-level version of the StorageGRID Appliance Installer, go to the NetApp Downloads page for StorageGRID.

## NetApp Downloads: StorageGRID

Sign in with the username and password for your NetApp account.

4. Download the appropriate version of the **Support file for StorageGRID Appliances** and the corresponding checksum file.

The Support file for StorageGRID Appliances file is a `.zip` archive that contains the current and previous firmware versions for all StorageGRID appliance models, in subdirectories for each controller type.

After downloading the Support file for StorageGRID Appliances file, extract the `.zip` archive and see the `README` file for important information about installing the StorageGRID Appliance Installer.

5. Follow the instructions on the Upgrade Firmware page of the StorageGRID Appliance Installer to perform these steps:
  - a. Upload the appropriate support file (firmware image) for your controller type and the checksum file.
  - b. Upgrade the inactive partition.
  - c. Reboot and swap partitions.
  - d. Upgrade the second partition.

### Related information

[Accessing the StorageGRID Appliance Installer](#)

### Configuring network links (SG6000)

You can configure network links for the ports used to connect the appliance to the Grid Network, the Client Network, and the Admin Network. You can set the link speed as well as the port and network bond modes.

#### What you'll need

If you are cloning an appliance node, configure network links for the target appliance for all links used by the source appliance node.

If you plan to use the 25-GbE link speed:

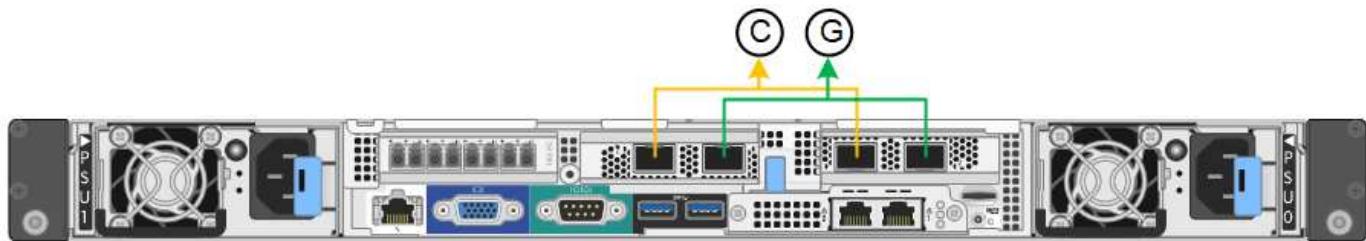
- You are using SFP28 TwinAx cables, or you have installed SFP28 transceivers in the network ports you plan to use.
- You have connected the network ports to switches that can support these features.
- You understand how to configure the switches to use this higher speed.

If you plan to use Aggregate port bond mode, LACP network bond mode, or VLAN tagging:

- You have connected the network ports on the appliance to switches that can support VLAN and LACP.
- If multiple switches are participating in the LACP bond, the switches support multi-chassis link aggregation groups (MLAG), or equivalent.
- You understand how to configure the switches to use VLAN, LACP, and MLAG or equivalent.
- You know the unique VLAN tag to use for each network. This VLAN tag will be added to each network packet to ensure that network traffic is routed to the correct network.

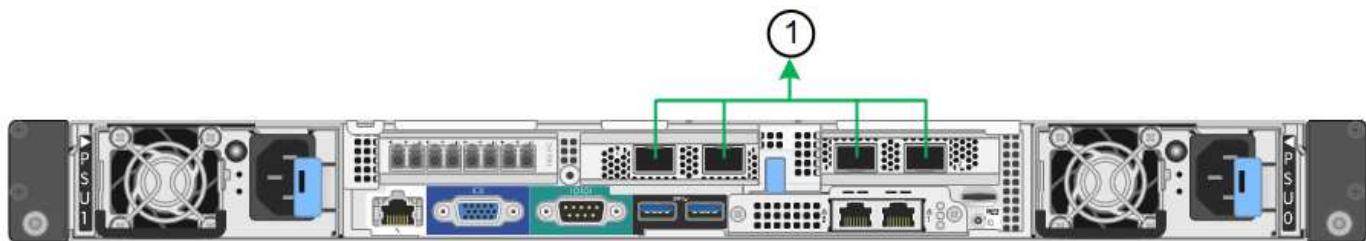
### About this task

This figure shows how the four network ports are bonded in fixed port bond mode (default configuration).



Which ports are bonded	
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

This figure shows how the four network ports are bonded in aggregate port bond mode.



Which ports are bonded	
1	All four ports are grouped in a single LACP bond, allowing all ports to be used for Grid Network and Client Network traffic.

The table summarizes the options for configuring the four network ports. The default settings are shown in bold. You only need to configure the settings on the Link Configuration page if you want to use a non-default setting.

- **Fixed (default) port bond mode**

Network bond mode	Client Network disabled (default)	Client Network enabled
<b>Active-Backup (default)</b>	<ul style="list-style-type: none"> <li>• Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>• Ports 1 and 3 are not used.</li> <li>• A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>• Ports 2 and 4 use an active-backup bond for the Grid Network.</li> <li>• Ports 1 and 3 use an active-backup bond for the Client Network.</li> <li>• VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad)	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 are not used.</li> <li>A VLAN tag is optional.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 2 and 4 use an LACP bond for the Grid Network.</li> <li>Ports 1 and 3 use an LACP bond for the Client Network.</li> <li>VLAN tags can be specified for both networks for the convenience of the network administrator.</li> </ul>

- Aggregate port bond mode

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network.</li> <li>A single VLAN tag identifies Grid Network packets.</li> </ul>	<ul style="list-style-type: none"> <li>Ports 1-4 use a single LACP bond for the Grid Network and the Client Network.</li> <li>Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.</li> </ul>

See “Network port connections for the SG6000-CN controller” for more information about port bond and network bond modes.

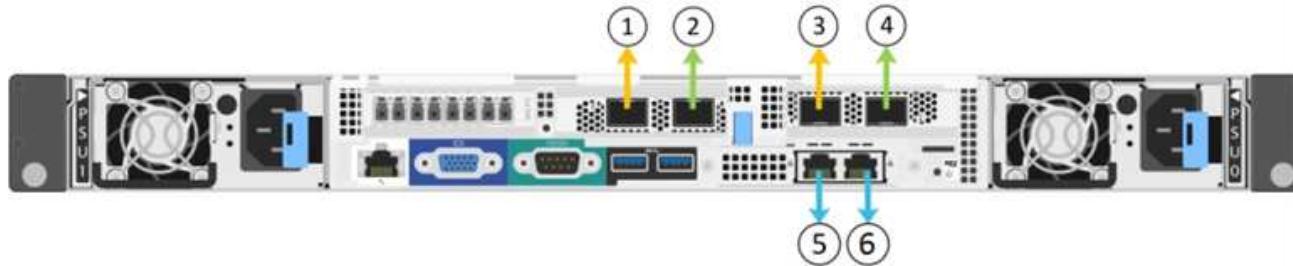
This figure shows how the two 1-GbE management ports on the SG6000-CN controller are bonded in Active-Backup network bond mode for the Admin Network.



### Steps

- From the StorageGRID Appliance Installer, click **Configure Networking > Link Configuration**.

The Network Link Configuration page displays a diagram of your appliance with the network and management ports numbered.



**⚠** You might lose your connection if you make changes to the network or link you are connected through. If you are not reconnected within 1 minute, re-enter the URL using one of the other IP addresses assigned to the appliance.

The Link Status table lists the link state (up/down) and speed (1/10/25/40/100 Gbps) of the numbered ports.

#### Link Status

Link	State	Speed (Gbps)
1	Up	10
2	Up	10
3	Down	N/A
4	Down	N/A
5	Up	1
6	Up	1

The first time you access this page:

- **Link Speed** is set to **10GbE**.
- **Port bond mode** is set to **Fixed**.
- **Network bond mode** is set to **Active-Backup** for the Grid Network.
- The **Admin Network** is enabled, and the network bond mode is set to **Independent**.
- The **Client Network** is disabled.

## Link Settings

Link speed

Port bond mode  Fixed  Aggregate  
Choose Fixed port bond mode if you want to use ports 2 and 4 for the Grid Network and ports 1 and 3 for the Client Network (if enabled). Choose Aggregate port bond mode if you want all connected ports to share a single LACP bond for both the Grid and Client Networks.

## Grid Network

Enable network

Network bond mode  Active-Backup  LACP (802.3ad)

Enable VLAN (802.1q) tagging

MAC Addresses 50:6b:4b:42:d7:00 50:6b:4b:42:d7:01 50:6b:4b:42:d7:24 50:6b:4b:42:d7:25  
If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

## Admin Network

Enable network

Network bond mode  Independent  Active-Backup  
Connect the Admin Network to port 5. Leave port 6 unconnected. If necessary, you can make a temporary direct Ethernet connection to port 6 and use link-local IP address 169.254.0.1 for access.

MAC Addresses d8:c4:97:2a:e4:95  
If you are using DHCP, it is recommended that you configure a permanent DHCP reservation. Use all of these MAC addresses in the reservation to assign one IP address to this network interface.

## Client Network

Enable network

Enabling the Client Network causes the default gateway for this node to move to the Client Network. Before enabling the Client Network, ensure that you've added all necessary subnets to the Grid Network Subnet List. Otherwise, the connection to the node might be lost.

2. If you plan to use the 25-GbE link speed for the network ports, select **25GbE** from the Link speed drop-down list.

The network switches you are using for the Grid Network and the Client Network must also support and be configured for this speed. You must use SFP28 TwinAx cables or optical cables and SFP28 transceivers.

3. Enable or disable the StorageGRID networks you plan to use.

The Grid Network is required. You cannot disable this network.

- a. If the appliance is not connected to the Admin Network, unselect the **Enable network** check box for the Admin Network.

#### **Admin Network**

Enable network

- b. If the appliance is connected to the Client Network, select the **Enable network** check box for the Client Network.

The Client Network settings for the network ports are now shown.

4. Refer to the table, and configure the port bond mode and the network bond mode.

This example shows:

- **Aggregate** and **LACP** selected for the Grid and the Client networks. You must specify a unique VLAN tag for each network. You can select values between 0 and 4095.
- **Active-Backup** selected for the Admin Network.

## Link Settings

Link speed	10GbE
Port bond mode	<input type="radio"/> Fixed <input checked="" type="radio"/> Aggregate
Choose Fixed port bond mode if you want to use ports 2 and 4 for the Grid Network and ports 1 and 3 for the Client Network (if enabled). Choose Aggregate port bond mode if you want all connected ports to share a single LACP bond for both the Grid and Client Networks.	
<b>Grid Network</b>	
Enable network	<input checked="" type="checkbox"/>
Network bond mode	<input type="radio"/> Active-Backup <input checked="" type="radio"/> LACP (802.3ad)
If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.	
Enable VLAN (802.1q) tagging	<input checked="" type="checkbox"/>
VLAN (802.1q) tag	328
<b>Admin Network</b>	
Enable network	<input checked="" type="checkbox"/>
Network bond mode	<input type="radio"/> Independent <input checked="" type="radio"/> Active-Backup
Connect the Admin Network to ports 5 and 6. If necessary, you can make a temporary direct Ethernet connection by disconnecting ports 5 and 6, then connecting to port 6 and using link-local IP address 169.254.0.1 for access.	
<b>Client Network</b>	
Enable network	<input checked="" type="checkbox"/>
Network bond mode	<input type="radio"/> Active-Backup <input checked="" type="radio"/> LACP (802.3ad)
If the port bond mode is Aggregate, all bonds must be in LACP (802.3ad) mode.	
Enable VLAN (802.1q) tagging	<input checked="" type="checkbox"/>
VLAN (802.1q) tag	332

5. When you are satisfied with your selections, click **Save**.



You might lose your connection if you made changes to the network or link you are connected through. If you are not reconnected within 1 minute, re-enter the URL for the StorageGRID Appliance Installer using one of the other IP addresses assigned to the appliance:

**[https://SG6000-CN\\_Controller\\_IP:8443](https://SG6000-CN_Controller_IP:8443)**

## Related information

[Port bond modes for the SG6000-CN controller](#)

[Configuring StorageGRID IP addresses](#)

## Configuring StorageGRID IP addresses

You use the StorageGRID Appliance Installer to configure the IP addresses and routing information used for the appliance Storage Node on the StorageGRID Grid, Admin, and Client Networks.

### About this task

You must either assign a static IP for the appliance on each connected network or assign a permanent lease for the address on the DHCP server.

If you want to change the link configuration, see the instructions for changing the link configuration of the SG6000-CN controller.

### Steps

1. In the StorageGRID Appliance Installer, select **Configure Networking > IP Configuration**.  
The IP Configuration page appears.
2. To configure the Grid Network, select either **Static** or **DHCP** in the **Grid Network** section of the page.

## Grid Network

The Grid Network is used for all internal StorageGRID traffic. The Grid Network provides connectivity between all nodes in the grid, across all sites and subnets. All hosts on the Grid Network must be able to talk to all other hosts. The Grid Network can consist of multiple subnets. Networks containing critical grid services, such as NTP, can also be added as Grid subnets.

IP  Static  DHCP

Assignment

IPv4 Address (CIDR)

Gateway

**⚠ All required Grid Network subnets must also be defined in the Grid Network Subnet List on the Primary Admin Node before starting installation.**

Subnets (CIDR)	<input type="text" value="172.18.0.0/21"/> <span style="color: red;">×</span>
	<input type="text" value="172.18.0.0/21"/> <span style="color: red;">×</span>
	<input type="text" value="192.168.0.0/21"/> <span style="color: green;">+ ×</span>
MTU	<input type="text" value="1500"/> <span style="border: 1px solid black; padding: 2px;">▼</span>

Cancel Save

3. If you selected **Static**, follow these steps to configure the Grid Network:

- Enter the static IPv4 address, using CIDR notation.
- Enter the gateway.

If your network does not have a gateway, re-enter the same static IPv4 address.

- If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.



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.

d. Click **Save**.

When you change the IP address, the gateway and list of subnets might also change.

If you lose your connection to the StorageGRID Appliance Installer, re-enter the URL using the new static IP address you just assigned. For example,

**`https://services_appliance_IP:8443`**

e. Confirm that the list of Grid Network subnets is correct.

If you have grid subnets, the Grid Network gateway is required. All grid subnets specified must be reachable through this gateway. These Grid Network subnets must also be defined in the Grid Network Subnet List on the primary Admin Node when you start StorageGRID installation.



The default route is not listed. If the Client Network is not enabled, the default route will use the Grid Network gateway.

- To add a subnet, click the insert icon  to the right of the last entry.
- To remove an unused subnet, click the delete icon .

f. Click **Save**.

4. If you selected **DHCP**, follow these steps to configure the Grid Network:

a. After you select the **DHCP** radio button, click **Save**.

The **IPv4 Address**, **Gateway**, and **Subnets** fields are automatically populated. If the DHCP server is set up to assign an MTU value, the **MTU** field is populated with that value, and the field becomes read-only.

Your web browser is automatically redirected to the new IP address for the StorageGRID Appliance Installer.

b. Confirm that the list of Grid Network subnets is correct.

If you have grid subnets, the Grid Network gateway is required. All grid subnets specified must be reachable through this gateway. These Grid Network subnets must also be defined in the Grid Network Subnet List on the primary Admin Node when you start StorageGRID installation.



The default route is not listed. If the Client Network is not enabled, the default route will use the Grid Network gateway.

- To add a subnet, click the insert icon  to the right of the last entry.
- To remove an unused subnet, click the delete icon .

c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.



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.

d. Click **Save**.

5. To configure the Admin Network, select either **Static** or **DHCP** in the **Admin Network** section of the page.



To configure the Admin Network, you must enable the Admin Network on the Link Configuration page.

## Admin Network

The Admin Network is a closed network used for system administration and maintenance. The Admin Network is typically a private network and does not need to be routable between sites.

IP Assignment  Static  DHCP

IPv4 Address (CIDR)

Gateway

Subnets (CIDR)  +

MTU  ▼

Cancel Save

6. If you selected **Static**, follow these steps to configure the Admin Network:

a. Enter the static IPv4 address, using CIDR notation, for Management Port 1 on the appliance.

Management Port 1 is the left of the two 1-GbE RJ45 ports on the right end of the appliance.

b. Enter the gateway.

If your network does not have a gateway, re-enter the same static IPv4 address.

c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as

9000. Otherwise, keep the default value of 1500.



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.

d. Click **Save**.

When you change the IP address, the gateway and list of subnets might also change.

If you lose your connection to the StorageGRID Appliance Installer, re-enter the URL using the new static IP address you just assigned. For example,

**`https://services_appliance:8443`**

e. Confirm that the list of Admin Network subnets is correct.

You must verify that all subnets can be reached using the gateway you provided.



The default route cannot be made to use the Admin Network gateway.

- To add a subnet, click the insert icon  to the right of the last entry.
- To remove an unused subnet, click the delete icon .

f. Click **Save**.

7. If you selected **DHCP**, follow these steps to configure the Admin Network:

a. After you select the **DHCP** radio button, click **Save**.

The **IPv4 Address**, **Gateway**, and **Subnets** fields are automatically populated. If the DHCP server is set up to assign an MTU value, the **MTU** field is populated with that value, and the field becomes read-only.

Your web browser is automatically redirected to the new IP address for the StorageGRID Appliance Installer.

b. Confirm that the list of Admin Network subnets is correct.

You must verify that all subnets can be reached using the gateway you provided.



The default route cannot be made to use the Admin Network gateway.

- To add a subnet, click the insert icon  to the right of the last entry.
- To remove an unused subnet, click the delete icon .

c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.



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.

d. Click **Save**.

8. To configure the Client Network, select either **Static** or **DHCP** in the **Client Network** section of the page.



To configure the Client Network, you must enable the Client Network on the Link Configuration page.

## Client Network

The Client Network is an open network used to provide access to client applications, including S3 and Swift. The Client Network enables grid nodes to communicate with any subnet reachable through the Client Network gateway. The Client Network does not become operational until you complete the StorageGRID configuration steps.

IP Assignment

Static     DHCP

IPv4 Address (CIDR)

Gateway

MTU

9. If you selected **Static**, follow these steps to configure the Client Network:

- Enter the static IPv4 address, using CIDR notation.
- Click **Save**.
- Confirm that the IP address for the Client Network gateway is correct.



If the Client Network is enabled, the default route is displayed. The default route uses the Client Network gateway and cannot be moved to another interface while the Client Network is enabled.

- If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.



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.

10. If you selected **DHCP**, follow these steps to configure the Client Network:

- After you select the **DHCP** radio button, click **Save**.

The **IPv4 Address** and **Gateway** fields are automatically populated. If the DHCP server is set up to assign an MTU value, the **MTU** field is populated with that value, and the field becomes read-only.

Your web browser is automatically redirected to the new IP address for the StorageGRID Appliance Installer.

b. Confirm that the gateway is correct.



If the Client Network is enabled, the default route is displayed. The default route uses the Client Network gateway and cannot be moved to another interface while the Client Network is enabled.

c. If you want to use jumbo frames, change the MTU field to a value suitable for jumbo frames, such as 9000. Otherwise, keep the default value of 1500.



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.

## Related information

[Changing the link configuration of the SG6000-CN controller](#)

## Verifying network connections

You should confirm you can access the StorageGRID networks you are using from the appliance. To validate routing through network gateways, you should test connectivity between the StorageGRID Appliance Installer and IP addresses on different subnets. You can also verify the MTU setting.

### Steps

1. From the menu bar of the StorageGRID Appliance Installer, click **Configure Networking > Ping and MTU Test**.

The Ping and MTU Test page appears.

### Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

#### Ping and MTU Test

Network	<input type="text" value="Grid"/> <span>▼</span>
Destination IPv4 Address or FQDN	<input type="text"/>
Test MTU	<input type="checkbox"/>
<span>Test Connectivity</span>	

2. From the **Network** drop-down box, select the network you want to test: Grid, Admin, or Client.

3. Enter the IPv4 address or fully qualified domain name (FQDN) for a host on that network.

For example, you might want to ping the gateway on the network or the primary Admin Node.

4. Optionally, select the **Test MTU** check box to verify the MTU setting for the entire path through the network to the destination.

For example, you can test the path between the appliance node and a node at a different site.

5. Click **Test Connectivity**.

If the network connection is valid, the "Ping test passed" message appears, with the ping command output listed.

### Ping and MTU Test

Use a ping request to check the appliance's connectivity to a remote host. Select the network you want to check connectivity through, and enter the IP address of the host you want to reach. To verify the MTU setting for the entire path through the network to the destination, select Test MTU.

#### Ping and MTU Test

Network	<input type="text" value="Grid"/> <input type="button" value="▼"/>
Destination IPv4 Address or FQDN	<input type="text" value="10.96.104.223"/>
Test MTU	<input checked="" type="checkbox"/>
<input type="button" value="Test Connectivity"/>	

Ping test passed

Ping command output

```
PING 10.96.104.223 (10.96.104.223) 1472(1500) bytes of data.
1480 bytes from 10.96.104.223: icmp_seq=1 ttl=64 time=0.318 ms

--- 10.96.104.223 ping statistics ---
1 packets transmitted, 1 received, 0% packet loss, time 0ms
rtt min/avg/max/mdev = 0.318/0.318/0.318/0.000 ms

Found MTU 1500 for 10.96.104.223 via br0
```

### Related information

[Configuring network links \(SG6000\)](#)

[Changing the MTU setting](#)

### Verifying port-level network connections

To ensure that access between the StorageGRID Appliance Installer and other nodes is

not obstructed by firewalls, confirm that the StorageGRID Appliance Installer can connect to a specific TCP port or set of ports at the specified IP address or range of addresses.

### About this task

Using the list of ports provided in the StorageGRID Appliance Installer, you can test the connectivity between the appliance and the other nodes in your Grid Network.

Additionally, you can test connectivity on the Admin and Client Networks and on UDP ports, such as those used for external NFS or DNS servers. For a list of these ports, see the port reference in the StorageGRID networking guidelines.



The Grid Network ports listed in the port connectivity table are valid only for StorageGRID version 11.5.0. To verify which ports are correct for each node type, you should always consult the networking guidelines for your version of StorageGRID.

### Steps

1. From the StorageGRID Appliance Installer, click **Configure Networking > Port Connectivity Test (nmap)**.

The Port Connectivity Test page appears.

The port connectivity table lists node types that require TCP connectivity on the Grid Network. For each node type, the table lists the Grid Network ports that should be accessible to your appliance.

The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

You can test the connectivity between the appliance ports listed in the table and the other nodes in your Grid Network.

2. From the **Network** drop-down, select the network you want to test: **Grid**, **Admin**, or **Client**.
3. Specify a range of IPv4 addresses for the hosts on that network.

For example, you might want to probe the gateway on the network or the primary Admin Node.

Specify a range using a hyphen, as shown in the example.

4. Enter a TCP port number, a list of ports separated by commas, or a range of ports.

The following node types require TCP connectivity on the Grid Network.

Node Type	Grid Network Ports
Admin Node	22,80,443,1504,1505,1506,1508,7443,9999
Storage Node without ADC	22,1139,1502,1506,1511,7001,9042,9999,18002,18017,18019,18082,18083,18200
Storage Node with ADC	22,1139,1501,1502,1506,1511,7001,9042,9999,18000,18001,18002,18003,18017,18019,18082,18083,18200,19000
API Gateway	22,1506,1507,9999
Archive Node	22,1506,1509,9999,11139

#### Port Connectivity Test

Network

IPv4 Address Ranges

Port Ranges

Protocol  TCP  UDP

#### 5. Click **Test Connectivity**.

- If the selected port-level network connections are valid, the “Port connectivity test passed” message appears in a green banner. The nmap command output is listed below the banner.

Port connectivity test passed

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Fri Nov 13 18:32:03 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,2022 10.224.6.160-161
Nmap scan report for 10.224.6.160
Host is up (0.00072s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

Nmap scan report for 10.224.6.161
Host is up (0.00060s latency).

PORT      STATE SERVICE
22/tcp    open  ssh
2022/tcp  open  down

# Nmap done at Fri Nov 13 18:32:04 2020 -- 2 IP addresses (2 hosts up) scanned in 0.55 seconds
```

- If a port-level network connection is made to the remote host, but the host is not listening on one or more of the selected ports, the “Port connectivity test failed” message appears in a yellow banner. The nmap command output is listed below the banner.

Any remote port the host is not listening to has a state of “closed.” For example, you might see this yellow banner when the node you are trying to connect to is in a pre-installed state and the StorageGRID NMS service is not yet running on that node.

 Port connectivity test failed  
Connection not established. Services might not be listening on target ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:07:02 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,80,443,1504,1505,1506,1508,7443,9999
Nmap scan report for 172.16.4.71
Host is up (0.00020s latency).

PORT      STATE    SERVICE
22/tcp    open     ssh
80/tcp    open     http
443/tcp   open     https
1504/tcp  closed   evb-elm
1505/tcp  open     funkproxy
1506/tcp  open     utcd
1508/tcp  open     diagmond
7443/tcp  open     oracleas-https
9999/tcp  open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:07:03 2020 -- 1 IP address (1 host up) scanned in 0.59 seconds
```

- If a port-level network connection cannot be made for one or more selected ports, the “Port connectivity test failed” message appears in a red banner. The nmap command output is listed below the banner.

The red banner indicates that a TCP connection attempt to a port on the remote host was made, but nothing was returned to the sender. When no response is returned, the port has a state of “filtered” and is likely blocked by a firewall.



Ports with “closed” are also listed.

 Port connectivity test failed  
Connection failed to one or more ports.

Nmap command output. Note: Unreachable hosts will not appear in the output.

```
# Nmap 7.70 scan initiated Sat May 16 17:11:01 2020 as: /usr/bin/nmap -n -oN - -e br0 -p 22,79,80,443,1504,1505,1506,1508,7443,9999 172.16.4.71
Nmap scan report for 172.16.4.71
Host is up (0.00029s latency).

PORT      STATE    SERVICE
22/tcp    open     ssh
79/tcp    filtered finger
80/tcp    open     http
443/tcp   open     https
1504/tcp  closed   evb-elm
1505/tcp  open     funkproxy
1506/tcp  open     utcd
1508/tcp  open     diagmond
7443/tcp  open     oracleas-https
9999/tcp  open     abyss
MAC Address: 00:50:56:87:39:AE (VMware)

# Nmap done at Sat May 16 17:11:02 2020 -- 1 IP address (1 host up) scanned in 1.60 seconds
```

## Related information

[Network guidelines](#)

## Accessing and Configuring SANtricity System Manager

You can use SANtricity System Manager to monitor the status of the storage controllers, storage disks, and other hardware components in the storage controller shelf. You can

also configure a proxy for E-Series AutoSupport that enables you to send AutoSupport messages from the appliance without the use of the management port.

## Steps

- [Setting up and Accessing SANtricity System Manager](#)
- [Reviewing the hardware status in SANtricity System Manager](#)
- [Setting the IP addresses for the storage controllers using the StorageGRID Appliance Installer](#)

### Setting up and Accessing SANtricity System Manager

You might need to access SANtricity System Manager on the storage controller to monitor the hardware in the storage controller shelf or to configure E-Series AutoSupport.

#### What you'll need

- You are using a supported web browser.
- To access SANtricity System Manager through Grid Manager, you must have installed StorageGRID, and you must have the Storage Appliance Administrator permission or Root Access permission.
- To access SANtricity System Manager using the StorageGRID Appliance Installer, you must have the SANtricity System Manager administrator username and password.
- To access SANtricity System Manager directly using a web browser, you must have the SANtricity System Manager administrator username and password.



You must have SANtricity firmware 8.70 or higher to access SANtricity System Manager using the Grid Manager or the StorageGRID Appliance Installer. You can check your firmware version by using the StorageGRID Appliance Installer and selecting **Help > About**.



Accessing SANtricity System Manager from the Grid Manager or from the Appliance Installer is generally meant only for monitoring your hardware and configuring E-Series AutoSupport. Many features and operations within SANtricity System Manager such as upgrading firmware do not apply to monitoring your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance.

#### About this task

There are three ways to access SANtricity System Manager, depending upon what stage of the installation and configuration process you are in:

- If the appliance has not yet been deployed as a node in your StorageGRID system, you should use the Advanced tab in the StorageGRID Appliance Installer.  
  
 Once the node is deployed, you can no longer use the StorageGRID Appliance Installer to access SANtricity System Manager.
- If the appliance has been deployed as a node in your StorageGRID system, use the SANtricity System Manager tab on the Nodes page in Grid Manager.
- If you cannot use the StorageGRID Appliance Installer or Grid Manager, you can access SANtricity System Manager directly using a web browser connected to the management port.

This procedure includes steps for your initial access to SANtricity System Manager. If you have already set up SANtricity System Manager, go to the [configure hardware alerts](#) step.



Using either the Grid Manager or the StorageGRID Appliance Installer enables you to access SANtricity System Manager without having to configure or connect the management port of the appliance.

You use SANtricity System Manager to monitor the following:

- Performance data such as storage array level performance, I/O latency, CPU utilization, and throughput
- Hardware component status
- Support functions including viewing diagnostic data

You can use SANtricity System Manager to configure the following settings:

- Email alerts, SNMP alerts, or syslog alerts for the components in the storage controller shelf
- E-Series AutoSupport settings for the components in the storage controller shelf.

For additional details on E-Series AutoSupport, see the E-Series documentation center.

#### [NetApp E-Series Systems Documentation Site](#)

- Drive Security keys, which are needed to unlock secured drives (this step is required if the Drive Security feature is enabled)
- Administrator password for accessing SANtricity System Manager

### Steps

1. Do one of the following:

- Use the StorageGRID Appliance Installer and select **Advanced > SANtricity System Manager**
- Use the Grid Manager and select **Nodes > *appliance Storage Node* > SANtricity System Manager**



If these options are not available or the login page does not appear, you must use the IP address of the storage controller. Access SANtricity System Manager by browsing to the storage controller IP:

**`https://Storage_Controller_IP`**

The login page for SANtricity System Manager appears.

2. Set or enter the administrator password.



SANtricity System Manager uses a single administrator password that is shared among all users.

The Set Up wizard appears.

## Set Up SANtricity® System Manager



More (10 total) >

1 Welcome

2 Verify Hardware

3 Verify Hosts

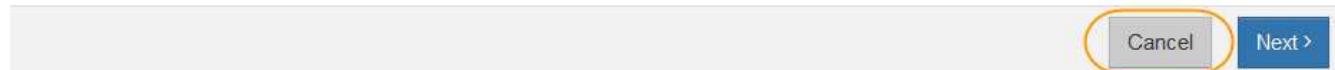
4 Select Applications

5 Define Workloads

6 Ac

Welcome to the SANtricity® System Manager! With System Manager, you can...

- Configure your storage array and set up alerts.
- Monitor and troubleshoot any problems when they occur.
- Keep track of how your system is performing in real time.



3. Select **Cancel** to close the wizard.



Do not complete the Set Up wizard for a StorageGRID appliance.

The SANtricity System Manager home page appears.

The SANtricity System Manager home page features a navigation menu on the left with options: Home, Storage, Hardware, Settings, and Support. The main content area includes:

- Storage Array Level Performance:** A graph showing IOPS (Ready) and IOPS (Write) over time. The graph shows a peak around 10:30 AM.
- CAPACITY:** A circular progress bar showing 0% Free, with a total capacity of 223531.39 GB.
- STORAGE HIERARCHY:** A diagram showing the storage structure: Storage Array (1 Shelf, 80 Drives) -> 8 Pools -> 8 Volume Groups -> 8 Volumes -> 8 Host Clusters -> 8 Hosts -> 8 Workloads.

4. Configure hardware alerts.

- a. Select **Help** to access the online help for SANtricity System Manager.
- b. Use the **Settings > Alerts** section of the online help to learn about alerts.
- c. Follow the “How To” instructions to set up email alerts, SNMP alerts, or syslog alerts.

5. Manage AutoSupport for the components in the storage controller shelf.
  - a. Select **Help** to access the online help for SANtricity System Manager.
  - b. Use the **Support > Support Center** section of the online help to learn about the AutoSupport feature.
  - c. Follow the “How To” instructions to manage AutoSupport.

For specific instructions on configuring a StorageGrid proxy for sending E-Series AutoSupport messages without using the management port, go to the instructions for administering StorageGRID and search for "proxy settings for E-Series AutoSupport."

#### [Administer StorageGRID](#)

6. If the Drive Security feature is enabled for the appliance, create and manage the security key.
  - a. Select **Help** to access the online help for SANtricity System Manager.
  - b. Use the **Settings > System > Security key management** section of the online help to learn about Drive Security.
  - c. Follow the “How To” instructions to create and manage the security key.
7. Optionally, change the administrator password.
  - a. Select **Help** to access the online help for SANtricity System Manager.
  - b. Use the **Home > Storage array administration** section of the online help to learn about the administrator password.
  - c. Follow the “How To” instructions to change the password.

#### **Related information**

##### [Web browser requirements](#)

##### [Setting the IP addresses for the storage controllers using the StorageGRID Appliance Installer](#)

#### **Reviewing the hardware status in SANtricity System Manager**

You can use SANtricity System Manager to monitor and manage the individual hardware components in the storage controller shelf and to review hardware diagnostic and environmental information, such as component temperatures, as well as issues related to the drives.

#### **What you'll need**

- You are using a supported web browser.
- To access SANtricity System Manager through Grid Manager, you must have the Storage Appliance Administrator permission or Root Access permission.
- To access SANtricity System Manager using the StorageGRID Appliance Installer, you must have the SANtricity System Manager administrator username and password.
- To access SANtricity System Manager directly using a web browser, you must have the SANtricity System Manager administrator username and password.



You must have SANtricity firmware 8.70 or higher to access SANtricity System Manager using the Grid Manager or the StorageGRID Appliance Installer.



Accessing SANtricity System Manager from the Grid Manager or from the Appliance Installer is generally meant only for monitoring your hardware and configuring E-Series AutoSupport. Many features and operations within SANtricity System Manager such as upgrading firmware do not apply to monitoring your StorageGRID appliance. To avoid issues, always follow the hardware installation and maintenance instructions for your appliance.

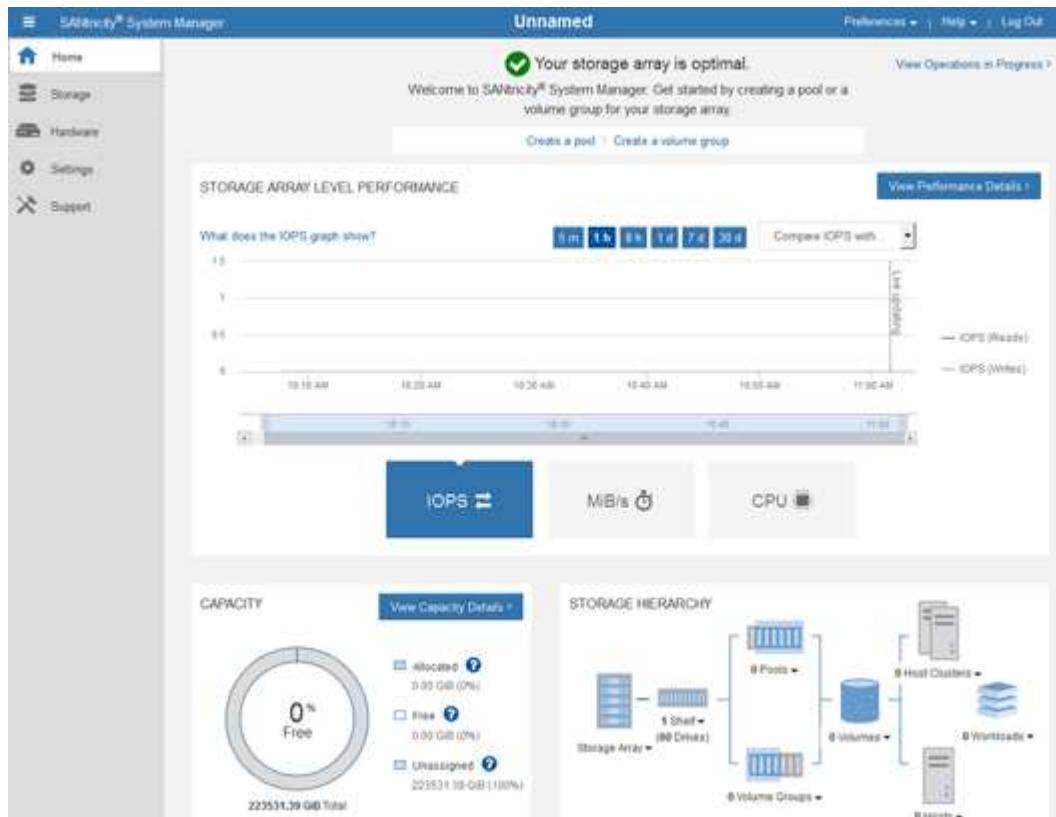
## Steps

1. Access SANtricity System Manager.

### Setting up and Accessing SANtricity System Manager

2. Enter the administrator username and password if required.
3. Click **Cancel** to close the Set Up wizard and to display the SANtricity System Manager home page.

The SANtricity System Manager home page appears. In SANtricity System Manager, the controller shelf is referred to as a storage array.



4. Review the information displayed for appliance hardware and confirm that all hardware components have a status of Optimal.
  - a. Click the **Hardware** tab.
  - b. Click **Show back of shelf**.

## HARDWARE

[Learn More >](#)

### Legend ▾

Show status icon details 

Controller Shelf 99 ▾ |     

[Show front of shelf](#)



From the back of the shelf, you can view both storage controllers, the battery in each storage controller, the two power canisters, the two fan canisters, and expansion shelves (if any). You can also view component temperatures.

- c. To see the settings for each storage controller, select the controller, and select **View settings** from the context menu.
- d. To see the settings for other components in the back of the shelf, select the component you want to view.
- e. Click **Show front of shelf**, and select the component you want to view.

From the front of the shelf, you can view the drives and the drive drawers for the storage controller shelf or the expansion shelves (if any).

If the status of any component is Needs Attention, follow the steps in the Recovery Guru to resolve the issue or contact technical support.

### Setting the IP addresses for the storage controllers using the StorageGRID Appliance Installer

Management port 1 on each storage controller connects the appliance to the management network for SANtricity System Manager. If you cannot access to the SANtricity System Manager from the StorageGRID Appliance Installer, you must set a static IP address for each storage controller to ensure that you do not lose your management connection to the hardware and the controller firmware in the controller shelf.

#### What you'll need

- You are using any management client that can connect to the StorageGRID Admin Network, or you have a service laptop.
- The client or service laptop has a supported web browser.

## About this task

DHCP-assigned addresses can change at any time. Assign static IP addresses to the controllers to ensure consistent accessibility.



Follow this procedure only if you do not have access to SANtricity System Manager from the StorageGRID Appliance Installer (**Advanced > SANtricity System Manager**) or Grid Manager (**Nodes > SANtricity System Manager**).

## Steps

1. From the client, enter the URL for the StorageGRID Appliance Installer:

**https://Appliance\_Controller\_IP:8443**

For *Appliance\_Controller\_IP*, use the IP address for the appliance on any StorageGRID network.

The StorageGRID Appliance Installer Home page appears.

2. Select **Configure Hardware > Storage Controller Network Configuration**.

The Storage Controller Network Configuration page appears.

3. Depending on your network configuration, select **Enabled** for IPv4, IPv6, or both.
4. Make a note of the IPv4 address that is automatically displayed.

DHCP is the default method for assigning an IP address to the storage controller management port.



It might take a few minutes for the DHCP values to appear.

IPv4 Address Assignment	<input type="radio"/> Static <input checked="" type="radio"/> DHCP
IPv4 Address (CIDR)	10.224.5.166/21
Default Gateway	10.224.0.1

5. Optionally, set a static IP address for the storage controller management port.



You should either assign a static IP for the management port or assign a permanent lease for the address on the DHCP server.

- a. Select **Static**.
- b. Enter the IPv4 address, using CIDR notation.
- c. Enter the default gateway.

IPv4 Address Assignment  Static  DHCP

IPv4 Address (CIDR)	10.224.2.200/21
Default Gateway	10.224.0.1

d. Click **Save**.

It might take a few minutes for your changes to be applied.

When you connect to SANtricity System Manager, you will use the new static IP address as the URL:  
[https://Storage\\_Controller\\_IP](https://Storage_Controller_IP)

## Configuring the BMC interface

The user interface for the baseboard management controller (BMC) on the SG6000-CN controller provides status information about the hardware and allows you to configure SNMP settings and other options for the SG6000-CN controller.

### Steps

- [Changing the root password for the BMC interface](#)
- [Setting the IP address for the BMC management port](#)
- [Accessing the BMC interface](#)
- [Configuring SNMP settings for the SG6000-CN controller](#)
- [Setting up email notifications for alerts](#)

### Changing the root password for the BMC interface

For security, you must change the password for the BMC's root user.

#### What you'll need

- The management client is using a supported web browser.

#### About this task

When you first install the appliance, the BMC uses a default password for the root user (root/calvin). You must change the password for the root user to secure your system.

### Steps

1. From the client, enter the URL for the StorageGRID Appliance Installer:  
[https://Appliance\\_Controller\\_IP:8443](https://Appliance_Controller_IP:8443)

For *Appliance\_Controller\_IP*, use the IP address for the appliance on any StorageGRID network.

The StorageGRID Appliance Installer Home page appears.

2. Select **Configure Hardware > BMC Configuration**.

NetApp® StorageGRID® Appliance Installer

Home	Configure Networking	Configure Hardware	Monitor Installation
Home	<a href="#">BMC Configuration</a> <a href="#">Storage Controller Network Configuration</a>		

The Baseboard Management Controller Configuration page appears.

3. Enter a new password for the root account in the two fields provided.

### Baseboard Management Controller Configuration

#### User Settings

Root Password

.....

Confirm Root Password

.....

4. Click **Save**.

#### Setting the IP address for the BMC management port

Before you can access the BMC interface, you must configure the IP address for the BMC management port on the SG6000-CN controller.

#### What you'll need

- The management client is using a supported web browser.
- You are using any management client that can connect to a StorageGRID network.
- The BMC management port is connected to the management network you plan to use.



#### About this task

For support purposes, the BMC management port allows low-level hardware access.



You should only connect this port to a secure, trusted, internal management network. If no such network is available, leave the BMC port unconnected or blocked, unless a BMC connection is requested by technical support.

#### Steps

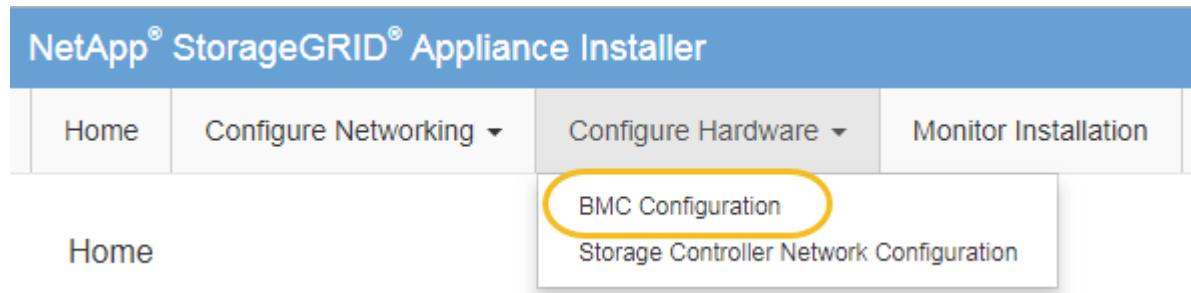
1. From the client, enter the URL for the StorageGRID Appliance Installer:

**[https://SG6000-CN\\_Controller\\_IP:8443](https://SG6000-CN_Controller_IP:8443)**

For SG6000-CN\_Controller\_IP, use the IP address for the appliance on any StorageGRID network.

The StorageGRID Appliance Installer Home page appears.

2. Select **Configure Hardware > BMC Configuration**.



The screenshot shows the 'NetApp® StorageGRID® Appliance Installer' interface. The top navigation bar has tabs for 'Home', 'Configure Networking', 'Configure Hardware', and 'Monitor Installation'. The 'Configure Hardware' tab is selected, and its dropdown menu is open, showing 'BMC Configuration' and 'Storage Controller Network Configuration', with 'BMC Configuration' highlighted by a yellow circle. Below the navigation bar, the word 'Home' is displayed.

The Baseboard Management Controller Configuration page appears.

3. Make a note of the IPv4 address that is automatically displayed.

DHCP is the default method for assigning an IP address to this port.



It might take a few minutes for the DHCP values to appear.

#### Baseboard Management Controller Configuration

##### LAN IP Settings

IP Assignment

Static

DHCP

MAC Address

d8:c4:97:28:50:62

IPv4 Address (CIDR)

10.224.3.225/21

Default gateway

10.224.0.1

Cancel

Save

4. Optionally, set a static IP address for the BMC management port.



You should either assign a static IP for the BMC management port or assign a permanent lease for the address on the DHCP server.

a. Select **Static**.

b. Enter the IPv4 address, using CIDR notation.

c. Enter the default gateway.

## Baseboard Management Controller Configuration

### LAN IP Settings

IP Assignment  Static  DHCP

MAC Address d8:c4:97:28:50:62

IPv4 Address (CIDR) 10.224.3.225/21

Default gateway 10.224.0.1

**Cancel** **Save**

d. Click **Save**.

It might take a few minutes for your changes to be applied.

## Accessing the BMC interface

You can access the BMC interface on the SG6000-CN controller using the DHCP or static IP address for the BMC management port.

### What you'll need

- The BMC management port on the SG6000-CN controller is connected to the management network you plan to use.



- The management client is using a supported web browser.

### Steps

- Enter the URL for the BMC interface:

**`https://BMC_Port_IP`**

For `BMC_Port_IP`, use the DHCP or static IP address for the BMC management port.

The BMC sign-in page appears.

- Enter the root username and password, using the password you set when you changed the default root password:

**`root`**

**`password`**



root  
\*\*\*\*\*  
 Remember Username  
**Sign me in**

[I forgot my password](#)

# NetApp®

3. Select **Sign me in**.

The BMC dashboard appears.

The screenshot shows the BMC Control Panel Dashboard. The left sidebar includes links for BMC, Dashboard, Sensor, System Inventory, FRU Information, BIOS POST Code, Server Identify, Logs & Reports, Settings, Remote Control, Power Control, Maintenance, and Sign out. The main dashboard features a 'Device Information' card with BMC Date&Time (17 Sep 2018 18:05:48) and a 'System Up Time' card showing 62 d 13 hrs. Below these are two 'Login Info' cards: one for Today (4 events) and one for 30 days (64 events). A green box on the right indicates 'Threshold Sensor Monitoring' is active with 'All threshold sensors are normal.'

4. Optionally, create additional users by selecting **Settings > User Management** and clicking on any "disabled" user.



When users sign in for the first time, they might be prompted to change their password for increased security.

## Related information

[Changing the root password for the BMC interface](#)

## Configuring SNMP settings for the SG6000-CN controller

If you are familiar with configuring SNMP for hardware, you can use the BMC interface to configure the SNMP settings for the SG6000-CN controller. You can provide secure community strings, enable SNMP Trap, and specify up to five SNMP destinations.

### What you'll need

- You know how to access the BMC dashboard.
- You have experience in configuring SNMP settings for SNMPv1-v2c equipment.

### Steps

1. From the BMC dashboard, select **Settings > SNMP Settings**.
2. On the SNMP Settings page, select **Enable SNMP V1/V2**, and then provide a Read-Only Community String and a Read-Write Community String.

The Read-Only Community String is like a user ID or password. You should change this value to prevent intruders from getting information about your network setup. The Read-Write Community String protects the device against unauthorized changes.
3. Optionally, select **Enable Trap**, and enter the required information.



Enter the Destination IP for each SNMP trap using an IP address. Fully qualified domain names are not supported.

Enable traps if you want the SG6000-CN controller to send immediate notifications to an SNMP console when it is in an unusual state. Traps might indicate hardware failures of various components or temperature thresholds being exceeded.

4. Optionally, click **Send Test Trap** to test your settings.
5. If the settings are correct, click **Save**.

### Setting up email notifications for alerts

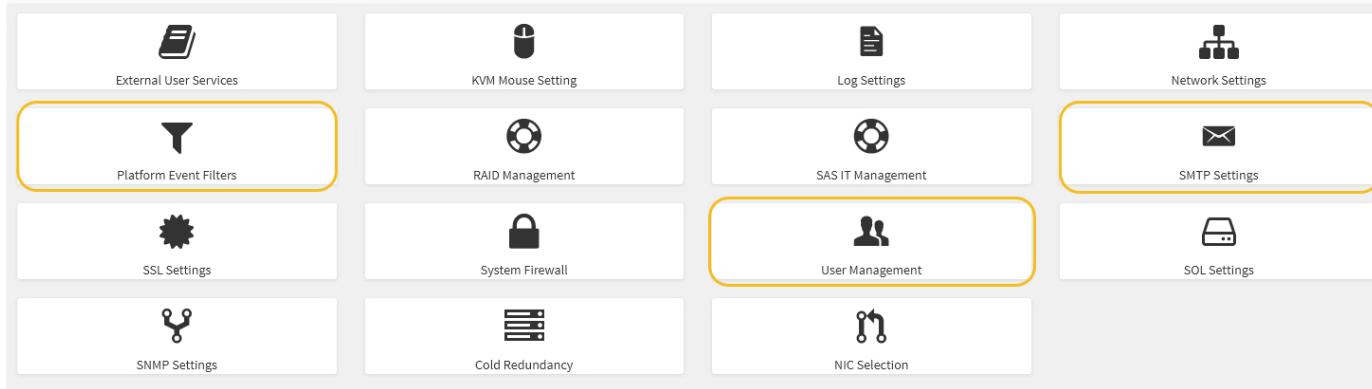
If you want email notifications to be sent when alerts occur, you must use the BMC interface to configure SMTP settings, users, LAN destinations, alert policies, and event filters.

### What you'll need

You know how to access the BMC dashboard.

### About this task

In the BMC interface, you use the **SMTP Settings**, **User Management**, and **Platform Event Filters** options on the Settings page to configure email notifications.



## Steps

1. Configure the SMTP settings.
  - a. Select **Settings > SMTP Settings**.
  - b. For Sender Email ID, enter a valid email address.

This email address is provided as the From address when the BMC sends email.

2. Set up users to receive alerts.
  - a. From the BMC dashboard, select **Settings > User Management**.
  - b. Add at least one user to receive alert notifications.

The email address you configure for a user is the address the BMC sends alert notifications to. For example, you could add a generic user, such as “notification-user,” and use the email address of a technical support team email distribution list.

3. Configure the LAN destination for alerts.
  - a. Select **Settings > Platform Event Filters > LAN Destinations**.
  - b. Configure at least one LAN destination.
    - Select **Email** as the Destination Type.
    - For BMC Username, select a user name that you added earlier.
    - If you added multiple users and want all of them to receive notification emails, you must add a LAN Destination for each user.
  - c. Send a test alert.
4. Configure alert policies so you can define when and where the BMC sends alerts.
  - a. Select **Settings > Platform Event Filters > Alert Policies**.
  - b. Configure at least one alert policy for each LAN destination.
    - For Policy Group Number, select **1**.
    - For Policy Action, select **Always send alert to this destination**.
    - For LAN Channel, select **1**.
    - In the Destination Selector, select the LAN destination for the policy.
5. Configure event filters to direct alerts for different event types to the appropriate users.

- a. Select **Settings > Platform Event Filters > Event Filters**.
- b. For Alert Policy Group Number, enter 1.
- c. Create filters for every event you want the Alert Policy Group to be notified about.
  - You can create event filters for power actions, specific sensor events, or all events.
  - If you are uncertain which events to monitor, select **All Sensors** for Sensor Type and **All Events** for Event Options. If you receive unwanted notifications, you can change your selections later.

## Optional: Enabling node encryption

If you enable node encryption, the disks in your appliance can be protected by secure key management server (KMS) encryption against physical loss or removal from the site. You must select and enable node encryption during appliance installation and cannot unselect node encryption once the KMS encryption process starts.

### What you'll need

Review the information about KMS in the instructions for administering StorageGRID.

### About this task

An appliance that has node encryption enabled connects to the external key management server (KMS) that is configured for the StorageGRID site. Each KMS (or KMS cluster) manages the encryption keys for all appliance nodes at the site. These keys encrypt and decrypt the data on each disk in an appliance that has node encryption enabled.

A KMS can be set up in Grid Manager before or after the appliance is installed in StorageGRID. See the information about KMS and appliance configuration in the instructions for administering StorageGRID for additional details.

- If a KMS is set up before installing the appliance, KMS-controlled encryption begins when you enable node encryption on the appliance and add it to a StorageGRID site where KMS is configured.
- If a KMS is not set up before you install the appliance, KMS-controlled encryption is performed on each appliance that has node encryption enabled as soon as a KMS is configured and available for the site that contains the appliance node.

 Any data that exists before an appliance that has node encryption enabled connects to the configured KMS is encrypted with a temporary key that is not secure. The appliance is not protected from removal or theft until the key is set to a value provided by the KMS.

Without the KMS key needed to decrypt the disk, data on the appliance cannot be retrieved and is effectively lost. This is the case whenever the decryption key cannot be retrieved from the KMS. The key becomes inaccessible if a customer clears the KMS configuration, a KMS key expires, connection to the KMS is lost, or the appliance is removed from the StorageGRID system where its KMS keys are installed.

### Steps

1. Open a browser, and enter one of the IP addresses for the appliance's compute controller.

**`https://Controller_IP:8443`**

`Controller_IP` is the IP address of the compute controller (not the storage controller) on any of the three StorageGRID networks.

The StorageGRID Appliance Installer Home page appears.



After the appliance has been encrypted with a KMS key, the appliance disks cannot be decrypted without using the same KMS key.

## 2. Select **Configure Hardware > Node Encryption**.

NetApp® StorageGRID® Appliance Installer

Help ▾

Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

**Node Encryption**

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

**Encryption Status**

⚠ You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption

Save

**Key Management Server Details**

## 3. Select **Enable node encryption**.

You can unselect **Enable node encryption** without risk of data loss until you select **Save** and the appliance node accesses the KMS encryption keys in your StorageGRID system and begins disk encryption. You are not able to disable node encryption after the appliance is installed.



After you add an appliance that has node encryption enabled to a StorageGRID site that has a KMS, you cannot stop using KMS encryption for the node.

## 4. Select **Save**.

## 5. Deploy the appliance as a node in your StorageGRID system.

KMS-controlled encryption begins when the appliance accesses the KMS keys configured for your StorageGRID site. The installer displays progress messages during the KMS encryption process, which might take a few minutes depending on the number of disk volumes in the appliance.



Appliances are initially configured with a random non-KMS encryption key assigned to each disk volume. The disks are encrypted using this temporary encryption key, that is not secure, until the appliance that has node encryption enabled accesses the KMS keys configured for your StorageGRID site.

## After you finish

You can view node-encryption status, KMS details, and the certificates in use when the appliance node is in maintenance mode.

## Related information

[Administer StorageGRID](#)

[Monitoring node encryption in maintenance mode](#)

## Optional: Changing the RAID mode (SG6000 only)

You can change to a different RAID mode on the appliance to accommodate your storage and recovery requirements. You can only change the mode before deploying the appliance Storage Node.

### What you'll need

- You are using any client that can connect to StorageGRID.
- The client has a supported web browser.

### About this task

Before deploying the appliance as a Storage Node, you can choose one of the following volume configuration options:

- **DDP:** This mode uses two parity drives for every eight data drives. This is the default and recommended mode for all appliances. When compared to RAID6, DDP delivers better system performance, reduced rebuild times after drive failures, and ease of management. DDP also provides drawer loss protection in 60-drive appliances.
- **DDP16:** This mode uses two parity drives for every 16 data drives, which results in higher storage efficiency compared to DDP. When compared to RAID6, DDP16 delivers better system performance, reduced rebuild times after drive failures, ease of management, and comparable storage efficiency. To use DDP16 mode, your configuration must contain at least 20 drives. DDP16 does not provide drawer loss protection.
- **RAID6:** This mode uses two parity drives for every 16 or more data drives. To use RAID 6 mode, your configuration must contain at least 20 drives. Although RAID6 can increase storage efficiency of the appliance when compared to DDP, it is not recommended for most StorageGRID environments.

 If any volumes have already been configured or if StorageGRID was previously installed, changing the RAID mode causes the volumes to be removed and replaced. Any data on those volumes will be lost.

### Steps

1. Open a browser, and enter one of the IP addresses for the appliance's compute controller.

**`https://Controller_IP:8443`**

`Controller_IP` is the IP address of the compute controller (not the storage controller) on any of the three StorageGRID networks.

The StorageGRID Appliance Installer Home page appears.

2. Select **Advanced > RAID Mode**.
3. On the **Configure RAID Mode** page, select the desired RAID mode from the Mode drop-down list.
4. Click **Save**.

### Related information

[NetApp E-Series Systems Documentation Site](#)

## Optional: Remapping network ports for the appliance

You might need to remap the internal ports on the appliance Storage Node to different external ports. For example, you might need to remap ports because of a firewall issue.

### What you'll need

- You have previously accessed the StorageGRID Appliance Installer.
- You have not configured and do not plan to configure load balancer endpoints.



If you remap any ports, you cannot use the same ports to configure load balancer endpoints. If you want to configure load balancer endpoints and have already remapped ports, follow the steps in the recovery and maintenance instructions for removing port remaps.

### Steps

1. From the StorageGRID Appliance Installer, click **Configure Networking > Remap Ports**.

The Remap Port page appears.

2. From the **Network** drop-down box, select the network for the port you want to remap: Grid, Admin, or Client.
3. From the **Protocol** drop-down box, select the IP protocol: TCP or UDP.
4. From the **Remap Direction** drop-down box, select which traffic direction you want to remap for this port: Inbound, Outbound, or Bi-directional.
5. For **Original Port**, enter the number of the port you want to remap.
6. For **Mapped-To Port**, enter the number of the port you want to use instead.
7. Click **Add Rule**.

The new port mapping is added to the table, and the remapping takes effect immediately.

### Remap Ports

If required, you can remap the internal ports on the appliance Storage Node to different external ports. For example, you might need to remap ports because of a firewall issue.

Network	Protocol	Remap Direction	Original Port	Mapped-To Port
Grid	TCP	Bi-directional	1800	1801

8. To remove a port mapping, select the radio button for the rule you want to remove, and click **Remove Selected Rule**.

# Deploying an appliance Storage Node

After installing and configuring the storage appliance, you can deploy it as a Storage Node in a StorageGRID system. When you deploy an appliance as a Storage Node, you use the StorageGRID Appliance Installer included on the appliance.

## What you'll need

- If you are cloning an appliance node, continue following the process in recovery and maintenance.

### Maintain & recover

- The appliance has been installed in a rack or cabinet, connected to your networks, and powered on.
- Network links, IP addresses, and port remapping (if necessary) have been configured for the appliance using the StorageGRID Appliance Installer.
- You know one of the IP addresses assigned to the appliance's compute controller. You can use the IP address for any attached StorageGRID network.
- The primary Admin Node for the StorageGRID system has been deployed.
- All Grid Network subnets listed on the IP Configuration page of the StorageGRID Appliance Installer have been defined in the Grid Network Subnet List on the primary Admin Node.
- You have a service laptop with a supported web browser.

## About this task

Each storage appliance functions as a single Storage Node. Any appliance can connect to the Grid Network, the Admin Network, and the Client Network.

To deploy an appliance Storage Node in a StorageGRID system, you access the StorageGRID Appliance Installer and perform the following steps:

- You specify or confirm the IP address of the primary Admin Node and the name of the Storage Node.
- You start the deployment and wait as volumes are configured and the software is installed.
- When the installation pauses partway through the appliance installation tasks, you resume the installation by signing into the Grid Manager, approving all grid nodes, and completing the StorageGRID installation and deployment processes.



If you need to deploy multiple appliance nodes at one time, you can automate the installation process by using the `configure-sga.py` Appliance Installation script.

- If you are performing an expansion or recovery operation, follow the appropriate instructions:
  - To add an appliance Storage Node to an existing StorageGRID system, see the instructions for expanding a StorageGRID system.
  - To deploy an appliance Storage Node as part of a recovery operation, see instructions for recovery and maintenance.

## Steps

1. Open a browser, and enter one of the IP addresses for the appliance's compute controller.

**`https://Controller_IP:8443`**

The StorageGRID Appliance Installer Home page appears.

# NetApp® StorageGRID® Appliance Installer

[Home](#)[Configure Networking](#)[Configure Hardware](#)[Monitor Installation](#)[Advanced](#)

## Home

ⓘ The installation is ready to be started. Review the settings below, and then click Start Installation.

### Primary Admin Node connection

Enable Admin Node discovery

Primary Admin Node IP

Connection state Connection to 172.16.4.210 ready

[Cancel](#)[Save](#)

### Node name

Node name

[Cancel](#)[Save](#)

### Installation

Current state Ready to start installation of NetApp-SGA into grid with Admin Node 172.16.4.210.

[Start Installation](#)

2. In the **Primary Admin Node connection** section, determine whether you need to specify the IP address for the primary Admin Node.

If you have previously installed other nodes in this data center, the StorageGRID Appliance Installer can discover this IP address automatically, assuming the primary Admin Node, or at least one other grid node with ADMIN\_IP configured, is present on the same subnet.

3. If this IP address is not shown or you need to change it, specify the address:

Option	Description
Manual IP entry	<ol style="list-style-type: none"> <li>Unselect the <b>Enable Admin Node discovery</b> check box.</li> <li>Enter the IP address manually.</li> <li>Click <b>Save</b>.</li> <li>Wait for the connection state for the new IP address to become ready.</li> </ol>
Automatic discovery of all connected primary Admin Nodes	<ol style="list-style-type: none"> <li>Select the <b>Enable Admin Node discovery</b> check box.</li> <li>Wait for the list of discovered IP addresses to be displayed.</li> <li>Select the primary Admin Node for the grid where this appliance Storage Node will be deployed.</li> <li>Click <b>Save</b>.</li> <li>Wait for the connection state for the new IP address to become ready.</li> </ol>

4. In the **Node name** field, enter the name you want to use for this appliance node, and click **Save**.

The node name is assigned to this appliance node in the StorageGRID system. It is shown on the Nodes page (Overview tab) in the Grid Manager. If required, you can change the name when you approve the node.

5. In the **Installation** section, confirm that the current state is "Ready to start installation of *node name* into grid with primary Admin Node *admin\_ip*" and that the **Start Installation** button is enabled.

If the **Start Installation** button is not enabled, you might need to change the network configuration or port settings. For instructions, see the installation and maintenance instructions for your appliance.



If you are deploying the Storage Node appliance as a node cloning target, stop the deployment process here and continue the node cloning procedure in recovery and maintenance.

[Maintain & recover](#)

6. From the StorageGRID Appliance Installer home page, click **Start Installation**.

The Current state changes to "Installation is in progress," and the Monitor Installation page is displayed.



If you need to access the Monitor Installation page manually, click **Monitor Installation**.

7. If your grid includes multiple appliance Storage Nodes, repeat these steps for each appliance.



If you need to deploy multiple appliance Storage Nodes at one time, you can automate the installation process by using the `configure-sga.py` Appliance Installation script. This script applies only to Storage Nodes.

## Related information

[Expand your grid](#)

[Maintain & recover](#)

# Monitoring the storage appliance installation

The StorageGRID Appliance Installer provides status until installation is complete. When the software installation is complete, the appliance is rebooted.

## Steps

1. To monitor the installation progress, click **Monitor Installation**.

The Monitor Installation page shows the installation progress.

Monitor Installation		
Step	Progress	Status
1. Configure storage	<div style="width: 100%; background-color: #2e7131; height: 10px;"></div>	Running
Connect to storage controller	<div style="width: 100%; background-color: #2e7131; height: 10px;"></div>	Complete
Clear existing configuration	<div style="width: 100%; background-color: #2e7131; height: 10px;"></div>	Complete
Configure volumes	<div style="width: 10%; background-color: #0072bc; height: 10px;"></div>	Creating volume StorageGRID-obj-00
Configure host settings	<div style="width: 0%; background-color: #cccccc; height: 10px;"></div>	Pending
2. Install OS		
3. Install StorageGRID		Pending
4. Finalize installation		Pending

The blue status bar indicates which task is currently in progress. Green status bars indicate tasks that have completed successfully.



The installer ensures that tasks completed in a previous install are not re-run. If you are re-running an installation, any tasks that do not need to be re-run are shown with a green status bar and a status of "Skipped."

2. Review the progress of the first two installation stages.

### 1. Configure storage

During this stage, the installer connects to the storage controller, clears any existing configuration, communicates with SANtricity software to configure volumes, and configures host settings.

### 2. Install OS

During this stage, the installer copies the base operating system image for StorageGRID to the appliance.

3. Continue monitoring the installation progress until the **Install StorageGRID** stage pauses and a message appears on the embedded console, prompting you to approve this node on the Admin Node using the Grid Manager. Go to the next step.

Home	Configure Networking ▾	Configure Hardware ▾	Monitor Installation	Advanced ▾	
------	------------------------	----------------------	----------------------	------------	--

## Monitor Installation

1. Configure storage	Complete
2. Install OS	Complete
3. Install StorageGRID	Running
4. Finalize installation	Pending

Connected (unencrypted) to: QEMU

```
/platform.type=: Device or resource busy
[2017-07-31T22:09:12.362566]    INFO -- [INSG] NOTICE: seeding /var/local with c
ontainer data
[2017-07-31T22:09:12.366205]    INFO -- [INSG] Fixing permissions
[2017-07-31T22:09:12.369633]    INFO -- [INSG] Enabling syslog
[2017-07-31T22:09:12.511533]    INFO -- [INSG] Stopping system logging: syslog-n
g.
[2017-07-31T22:09:12.570096]    INFO -- [INSG] Starting system logging: syslog-n
g.
[2017-07-31T22:09:12.576360]    INFO -- [INSG] Beginning negotiation for downloa
d of node configuration
[2017-07-31T22:09:12.581363]    INFO -- [INSG]
[2017-07-31T22:09:12.585066]    INFO -- [INSG]
[2017-07-31T22:09:12.588314]    INFO -- [INSG]
[2017-07-31T22:09:12.591851]    INFO -- [INSG]
[2017-07-31T22:09:12.594886]    INFO -- [INSG]
[2017-07-31T22:09:12.598360]    INFO -- [INSG]
[2017-07-31T22:09:12.601324]    INFO -- [INSG]
[2017-07-31T22:09:12.604759]    INFO -- [INSG]
[2017-07-31T22:09:12.607800]    INFO -- [INSG]
[2017-07-31T22:09:12.610985]    INFO -- [INSG]
[2017-07-31T22:09:12.614597]    INFO -- [INSG]
[2017-07-31T22:09:12.618282]    INFO -- [INSG] Please approve this node on the A
dmin Node GMI to proceed...
```

4. Go to the Grid Manager, approve the pending storage node, and complete the StorageGRID installation process.

When you click **Install** from the Grid Manager, Stage 3 completes and stage 4, **Finalize Installation**, begins. When stage 4 completes, the controller is rebooted.

## Automating appliance installation and configuration

You can automate the installation and configuration of your appliances and configuration of the whole StorageGRID system.

### About this task

Automating installation and configuration can be useful for deploying multiple StorageGRID instances or one large, complex StorageGRID instance.

To automate installation and configuration, use one or more of the following options:

- Create a JSON file that specifies the configuration settings for your appliances. Upload the JSON file using the StorageGRID Appliance Installer.



You can use the same file to configure more than one appliance.

- Use the `StorageGRIDconfigure-sga.py` Python script to automate the configuration of your appliances.
- Use additional Python scripts to configure other components of the whole StorageGRID system (the "grid").



You can use StorageGRID automation Python scripts directly, or you can use them as examples of how to use the StorageGRID Installation REST API in grid deployment and configuration tools you develop yourself. See the information about downloading and extracting the StorageGRID installation files in the Recovery and Maintenance instructions.

## Automating appliance configuration using the StorageGRID Appliance Installer

You can automate the configuration of an appliance by using a JSON file that contains the configuration information. You upload the file using the StorageGRID Appliance Installer.

### What you'll need

- Your appliance must be on the latest firmware compatible with StorageGRID 11.5 or higher.
- You must be connected to the StorageGRID Appliance Installer on the appliance you are configuring using a supported browser.

### About this task

You can automate appliance configuration tasks such as configuring the following:

- Grid Network, Admin Network, and Client Network IP addresses
- BMC interface
- Network links
  - Port bond mode
  - Network bond mode
  - Link speed

Configuring your appliance using an uploaded JSON file is often more efficient than performing the configuration manually using multiple pages in the StorageGRID Appliance Installer, especially if you have to configure many nodes. You must apply the configuration file for each node one at a time.



Experienced users who want to automate both the installation and configuration of their appliances can use the `configure-sga.py` script.

[Automating installation and configuration of appliance nodes using the configure-sga.py script](#)

### Steps

1. Generate the JSON file using one of the following methods:

- The ConfigBuilder application

[ConfigBuilder.netapp.com](https://ConfigBuilder.netapp.com)

- The `configure-sga.py` appliance configuration script. You can download the script from StorageGRID Appliance Installer (**Help > Appliance Configuration Script**). See the instructions on automating the configuration using the `configure-sga.py` script.

[Automating installation and configuration of appliance nodes using the `configure-sga.py` script](#)

The node names in the JSON file must follow these requirements:

- Must be a valid hostname containing at least 1 and no more than 32 characters
- Can use letters, numbers, and hyphens are allowed
- Cannot start or end with a hyphen or contain only numbers



Ensure that the node names (the top-level names) in the JSON file are unique, or you will not be able to configure more than one node using the JSON file.

2. Select **Advanced > Update Appliance Configuration**.

The Update Appliance Configuration page appears.

#### Update Appliance Configuration

Use a JSON file to update this appliance's configuration. You can generate the JSON file from the [ConfigBuilder](#) application or from the [appliance configuration script](#).

**⚠** You might lose your connection if the applied configuration from the JSON file includes "link\_config" and/or "networks" sections. If you are not reconnected within 1 minute, re-enter the URL using one of the other IP addresses assigned to the appliance.

#### Upload JSON

JSON configuration	<input type="button" value="Browse"/>
Node name	<input type="button" value="-- Upload a file"/>
<input type="button" value="Apply JSON configuration"/>	

3. Select the JSON file with the configuration you want to upload.

- Select **Browse**.
- Locate and select the file.
- Select **Open**.

The file is uploaded and validated. When the validation process is complete, the file name is shown

next to a green check mark.



You might lose connection to the appliance if the configuration from the JSON file includes sections for "link\_config", "networks", or both. If you are not reconnected within 1 minute, re-enter the appliance URL using one of the other IP addresses assigned to the appliance.

#### Upload JSON

JSON configuration	<input type="button" value="Browse"/> <span>✓ appliances.orig.json</span>
Node name	-- Select a node ▾
<input type="button" value="Apply JSON configuration"/>	

The **Node name** drop down is populated with the top-level node names defined in the JSON file.



If the file is not valid, the file name is shown in red and an error message is displayed in a yellow banner. The invalid file is not applied to the appliance. You can use ConfigBuilder to ensure you have a valid JSON file.

4. Select a node from the list in the **Node name** drop down.

The **Apply JSON configuration** button is enabled.

#### Upload JSON

JSON configuration	<input type="button" value="Browse"/> <span>✓ appliances.orig.json</span>
Node name	Lab-80-1000 ▾
<input type="button" value="Apply JSON configuration"/>	

5. Select **Apply JSON configuration**.

The configuration is applied to the selected node.

## Automating installation and configuration of appliance nodes using the `configure-sga.py` script

You can use the `configure-sga.py` script to automate many of the installation and configuration tasks for StorageGRID appliance nodes, including installing and configuring a primary Admin Node. This script can be useful if you have a large number of appliances to configure. You can also use the script to generate a JSON file that contains appliance

configuration information.

## What you'll need

- The appliance has been installed in a rack, connected to your networks, and powered on.
- Network links and IP addresses have been configured for the primary Admin Node using the StorageGRID Appliance Installer.
- If you are installing the primary Admin Node, you know its IP address.
- If you are installing and configuring other nodes, the primary Admin Node has been deployed, and you know its IP address.
- For all nodes other than the primary Admin Node, all Grid Network subnets listed on the IP Configuration page of the StorageGRID Appliance Installer have been defined in the Grid Network Subnet List on the primary Admin Node.
- You have downloaded the `configure-sga.py` file. The file is included in the installation archive, or you can access it by clicking **Help > Appliance Installation Script** in the StorageGRID Appliance Installer.



This procedure is for advanced users with some experience using command-line interfaces. Alternatively, you can also use the StorageGRID Appliance Installer to automate the configuration.

[Automating appliance configuration using the StorageGRID Appliance Installer](#)

## Steps

1. Log in to the Linux machine you are using to run the Python script.
2. For general help with the script syntax and to see a list of the available parameters, enter the following:

```
configure-sga.py --help
```

The `configure-sga.py` script uses five subcommands:

- `advanced` for advanced StorageGRID appliance interactions, including BMC configuration and creating a JSON file containing the current configuration of the appliance
- `configure` for configuring the RAID mode, node name, and networking parameters
- `install` for starting a StorageGRID installation
- `monitor` for monitoring a StorageGRID installation
- `reboot` for rebooting the appliance

If you enter a subcommand (advanced, configure, install, monitor, or reboot) argument followed by the `--help` option you will get a different help text providing more detail on the options available within that subcommand:

```
configure-sga.py subcommand --help
```

3. To confirm the current configuration of the appliance node, enter the following where `SGA-install-ip` is any one of the IP addresses for the appliance node:

```
configure-sga.py configure SGA-INSTALL-IP
```

The results show current IP information for the appliance, including the IP address of the primary Admin Node and information about the Admin, Grid, and Client Networks.

```
Connecting to +https://10.224.2.30:8443+ (Checking version and
connectivity.)
2021/02/25 16:25:11: Performing GET on /api/versions... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-info... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/admin-connection...
Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/link-config... Received
200
2021/02/25 16:25:11: Performing GET on /api/v2/networks... Received 200
2021/02/25 16:25:11: Performing GET on /api/v2/system-config... Received
200
```

#### StorageGRID Appliance

```
Name: LAB-SGA-2-30
Node type: storage
```

#### StorageGRID primary Admin Node

```
IP: 172.16.1.170
State: unknown
Message: Initializing...
Version: Unknown
```

#### Network Link Configuration

##### Link Status

Link	State	Speed (Gbps)
1	Up	10
2	Up	10
3	Up	10
4	Up	10
5	Up	1
6	Down	N/A

##### Link Settings

```
Port bond mode: FIXED
Link speed: 10GBE
```

```
Grid Network: ENABLED
Bonding mode: active-backup
VLAN: novlan
MAC Addresses: 00:a0:98:59:8e:8a 00:a0:98:59:8e:82
```

```
Admin Network: ENABLED
Bonding mode: no-bond
MAC Addresses: 00:80:e5:29:70:f4
```

```
Client Network:      ENABLED
      Bonding mode:    active-backup
        VLAN:          novlan
  MAC Addresses:    00:a0:98:59:8e:89  00:a0:98:59:8e:81
```

#### Grid Network

```
CIDR:      172.16.2.30/21 (Static)
MAC:       00:A0:98:59:8E:8A
Gateway:   172.16.0.1
Subnets:   172.17.0.0/21
           172.18.0.0/21
           192.168.0.0/21
MTU:      1500
```

#### Admin Network

```
CIDR:      10.224.2.30/21 (Static)
MAC:       00:80:E5:29:70:F4
Gateway:   10.224.0.1
Subnets:   10.0.0.0/8
           172.19.0.0/16
           172.21.0.0/16
MTU:      1500
```

#### Client Network

```
CIDR:      47.47.2.30/21 (Static)
MAC:       00:A0:98:59:8E:89
Gateway:   47.47.0.1
MTU:      2000
```

```
#####
##### If you are satisfied with this configuration, #####
##### execute the script with the "install" sub-command. #####
#####
```

4. If you need to change any of the values in the current configuration, use the `configure` subcommand to update them. For example, if you want to change the IP address that the appliance uses for connection to the primary Admin Node to 172.16.2.99, enter the following:

```
configure-sga.py configure --admin-ip 172.16.2.99 SGA-INSTALL-IP
```

5. If you want to back up the appliance configuration to a JSON file, use the `advanced` and `backup-file` subcommands. For example, if you want to back up the configuration of an appliance with IP address *SGA-INSTALL-IP* to a file named `appliance-SG1000.json`, enter the following:

```
configure-sga.py advanced --backup-file appliance-SG1000.json SGA-INSTALL-IP
```

The JSON file containing the configuration information is written to the same directory you executed the script from.



Check that the top-level node name in the generated JSON file matches the appliance name. Do not make any changes to this file unless you are an experienced user and have a thorough understanding of StorageGRID APIs.

6. When you are satisfied with the appliance configuration, use the `install` and `monitor` subcommands to install the appliance:

```
configure-sga.py install --monitor SGA-INSTALL-IP
```

7. If you want to reboot the appliance, enter the following:

```
configure-sga.py reboot SGA-INSTALL-IP
```

## 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
<code>configure-storagegrid.py</code>	Python script used to automate the configuration
<code>configure-storagegrid.sample.json</code>	Sample configuration file for use with the script
<code>configure-storagegrid.blank.json</code>	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`, `rpm`, or `vsphere`.

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

For example:

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

## After you finish

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.
```

## Overview of installation REST APIs

StorageGRID provides two REST APIs for performing installation tasks: the StorageGRID Installation API and the StorageGRID Appliance Installer API.

Both APIs use 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.

## StorageGRID Appliance Installer API

The StorageGRID Appliance Installer API can be accessed over HTTPS from *Controller\_IP*:8443.

To access the API documentation, go to the StorageGRID Appliance Installer on the appliance and select **Help > API Docs** from the menu bar.

The StorageGRID Appliance Installer API includes the following sections:

- **clone** — Operations to configure and control node cloning.
- **encryption** — Operations to manage encryption and view encryption status.
- **hardware configuration** — Operations to configure system settings on attached hardware.
- **installation** — Operations for starting the appliance installation and for monitoring installation status.
- **networking** — Operations related to the Grid, Admin, and Client Network configuration for a StorageGRID appliance and appliance port settings.
- **setup** — Operations to help with initial appliance installation setup including requests to get information about the system and update the primary Admin Node IP.
- **support** — Operations for rebooting the controller and getting logs.
- **upgrade** — Operations related to upgrading appliance firmware.
- **uploadsg** — Operations for uploading StorageGRID installation files.

## Troubleshooting the hardware installation

If you encounter issues during the installation, you might find it helpful to review troubleshooting information related to hardware setup and connectivity issues.

### Related information

[Hardware setup appears to hang](#)

[Troubleshooting connection issues](#)

## Viewing boot-up codes for the SG6000-CN controller

When you apply power to the appliance, the BMC logs a series of boot-up codes for the SG6000-CN controller. You can view these codes in several ways.

### What you'll need

- You know how to access the BMC dashboard.
- If you want to use a kernel-based virtual machine (KVM), you have experience deploying and using KVM applications.
- If you want to use serial-over-LAN (SOL), you have experience using IPMI SOL console applications.

### Steps

1. Select one of the following methods for viewing the boot-up codes for the appliance controller, and gather the required equipment.

Method	Required equipment
VGA console	<ul style="list-style-type: none"><li>• VGA-capable monitor</li><li>• VGA cable</li></ul>
KVM	<ul style="list-style-type: none"><li>• KVM application</li><li>• RJ-45 cable</li></ul>
Serial port	<ul style="list-style-type: none"><li>• DB-9 serial cable</li><li>• Virtual serial terminal</li></ul>
SOL	<ul style="list-style-type: none"><li>• Virtual serial terminal</li></ul>

2. If you are using a VGA console, perform these steps:
  - a. Connect a VGA-capable monitor to the VGA port on the back of the appliance.
  - b. View the codes displayed on the monitor.
3. If you are using BMC KVM, perform these steps:
  - a. Connect to the BMC management port and log into the BMC web interface.
  - b. Select **Remote Control**.
  - c. Launch the KVM.
  - d. View the codes on the virtual monitor.
4. If you are using a serial port and terminal, perform these steps:
  - a. Connect to the DB-9 serial port on the back of the appliance.
  - b. Use settings 115200 8-N-1.
  - c. View the codes printed over the serial terminal.

5. If you are using SOL, perform these steps:

- Connect to the IPMI SOL using the BMC IP address and login credentials.

```
ipmitool -I lanplus -H 10.224.3.91 -U root -P calvin sol activate
```

- View the codes on the virtual serial terminal.

6. Use the table to look up the codes for your appliance.

Code	Indicates
HI	The master boot script has started.
HP	The system is checking to see if the network interface card (NIC) firmware needs to be updated.
RB	The system is rebooting after applying firmware updates.
FP	The hardware subsystem firmware update checks have been completed. Inter-controller communication services are starting.
HE	For an appliance Storage Node only:  The system is awaiting connectivity with the storage controllers and synchronizing with the SANtricity operating system.  <b>Note:</b> If the boot-up procedure does not progress past this stage, perform these steps: <ol style="list-style-type: none"><li>Confirm that the four interconnect cables between the SG6000-CN controller and the two storage controllers are securely connected.</li><li>As required, replace one or more of the cables, and try again.</li><li>If this does not resolve the issue, contact technical support.</li></ol>
HC	The system is checking for existing StorageGRID installation data.
HO	The StorageGRID Appliance Installer is running.
HA	StorageGRID is running.

## Viewing error codes for the SG6000-CN controller

If a hardware error occurs when the SG6000-CN controller is booting up, the BMC logs an error code. As required, you can view these error codes using the BMC interface, and then work with technical support to resolve the issue.

### What you'll need

- You know how to access the BMC dashboard.

### Steps

1. From the BMC dashboard, select **BIOS POST Code**.
2. Review the information displayed for Current Code and the Previous Code.

If any of the following error codes are shown, work with technical support to resolve the issue.

Code	Indicates
0x0E	Microcode not found
0x0F	Microcode not loaded
0x50	Memory initialization error. Invalid memory type or incompatible memory speed.
0x51	Memory initialization error. SPD reading has failed.
0x52	Memory initialization error. Invalid memory size or memory modules do not match.
0x53	Memory initialization error. No usable memory detected.
0x54	Unspecified memory initialization error
0x55	Memory not installed
0x56	Invalid CPU type or speed
0x57	CPU mismatch
0x58	CPU self-test failed, or possible CPU cache error
0x59	CPU micro-code is not found, or micro-code update failed
0x5A	Internal CPU error

Code	Indicates
0x5B	Reset PPI is not available
0x5C	PEI phase BMC self-test failure
0xD0	CPU initialization error
0xD1	North bridge initialization error
0xD2	South bridge initialization error
0xD3	Some architectural protocols are not available
0xD4	PCI resource allocation error. Out of resources.
0xD5	No space for legacy option ROM
0xD6	No console output devices are found
0xD7	No console input devices are found
0xD8	Invalid password
0xD9	Error loading boot option (LoadImage returned error)
0xDA	Boot option failed (StartImage returned error)
0xDB	Flash update failed
0xDC	Reset protocol is not available
0xDD	DXE phase BMC self-test failure
0xE8	MRC: ERR_NO_MEMORY
0xE9	MRC: ERR_LT_LOCK
0xEA	MRC: ERR_DDR_INIT
0xEB	MRC: ERR_MEM_TEST
0xEC	MRC: ERR_VENDOR_SPECIFIC

Code	Indicates
0xED	MRC: ERR_DIMM_COMPAT
0xEE	MRC: ERR_MRC_COMPATIBILITY
0xEF	MRC: ERR_MRC_STRUCT
0xF0	MRC: ERR_SET_VDD
0xF1	MRC: ERR_IOT_MEM_BUFFER
0xF2	MRC: ERR_RC_INTERNAL
0xF3	MRC: ERR_INVALID_REG_ACCESS
0xF4	MRC: ERR_SET_MC_FREQ
0xF5	MRC: ERR_READ_MC_FREQ
0x70	MRC: ERR_DIMM_CHANNEL
0x74	MRC: ERR_BIST_CHECK
0xF6	MRC: ERR_SMBUS
0xF7	MRC: ERR_PCU
0xF8	MRC: ERR_NGN
0xF9	MRC: ERR_INTERLEAVE_FAILURE

## Hardware setup appears to hang

The StorageGRID Appliance Installer might not be available if hardware faults or cabling errors prevent the storage controllers or the SG6000-CN controller from completing their boot-up processing.

### Steps

1. For the storage controllers, watch the codes on the seven-segment displays.

While the hardware is initializing during power up, the two seven-segment displays show a sequence of codes. When the hardware boots successfully, both seven-segment displays show 99.

2. Review the LEDs on the SG6000-CN controller and the boot-up and error codes displayed in the BMC.
3. If you need help resolving an issue, contact technical support.

## Related information

[Viewing boot-up status codes for the SG6000 storage controllers](#)

[E5700 and E2800 System Monitoring Guide](#)

[Viewing status indicators and buttons on the SG6000-CN controller](#)

[Viewing boot-up codes for the SG6000-CN controller](#)

[Viewing error codes for the SG6000-CN controller](#)

## Troubleshooting connection issues

If you encounter connection issues during the StorageGRID appliance installation, you should perform the corrective action steps listed.

### Unable to connect to the appliance

If you cannot connect to the appliance, there might be a network issue, or the hardware installation might not have been completed successfully.

#### Steps

1. If you are unable to connect to SANtricity System Manager:

a. Try to ping the appliance using the IP address for either storage controller on the management network for SANtricity System Manager:

**`ping Storage_Controller_IP`**

b. If you receive no response from the ping, confirm you are using the correct IP address.

Use the IP address for management port 1 on either storage controller.

c. If the IP address is correct, check appliance cabling and the network setup.

If that does not resolve the issue, contact technical support.

d. If the ping was successful, open a web browser.

e. Enter the URL for SANtricity System Manager:

**`https://Storage_Controller_IP`**

The log in page for SANtricity System Manager appears.

2. If you are unable to connect to the SG6000-CN controller:

a. Try to ping the appliance using the IP address for the SG6000-CN controller:

**`ping SG6000-CN_Controller_IP`**

b. If you receive no response from the ping, confirm you are using the correct IP address.

You can use the IP address of the appliance on the Grid Network, the Admin Network, or the Client Network.

c. If the IP address is correct, check appliance cabling, SFP transceivers, and the network setup.

If that does not resolve the issue, contact technical support.

- d. If the ping was successful, open a web browser.
- e. Enter the URL for the StorageGRID Appliance Installer:  
**[https://SG6000-CN\\_Controller\\_IP:8443](https://SG6000-CN_Controller_IP:8443)**

The Home page appears.

### Expansion shelves do not appear in Appliance Installer

If you have installed expansion shelves for the SG6060 and they do not appear in the StorageGRID Appliance Installer, you should verify that the shelves have been completely installed and powered on.

#### About this task

You can verify that the expansion shelves are connected to the appliance by viewing the following information in the StorageGRID Appliance Installer:

- The **Home** page contains a message about expansion shelves.

 The storage system contains 2 expansion shelves.

- The **Advanced > RAID Mode** page indicates by number of drives whether or not the appliance includes expansion shelves. For example, in the following screen shot, two SSDs and 178 HDDs are shown. An SG6060 with two expansion shelves contains 180 total drives.

### Configure RAID Mode

This appliance contains the following drives.

Type	Size	Number of drives
SSD	800 GB	2
HDD	11.8 TB	178

If the StorageGRID Appliance Installer pages do not indicate that expansion shelves are present, follow this procedure.

#### Steps

1. Verify that all required cables have been firmly connected.
2. Verify that you have powered on the expansion shelves.
3. If you need help resolving an issue, contact technical support.

#### Related information

[SG6060: Cabling the optional expansion shelves](#)

[Connecting power cords and applying power \(SG6000\)](#)

## Rebooting the SG6000-CN controller while the StorageGRID Appliance Installer is running

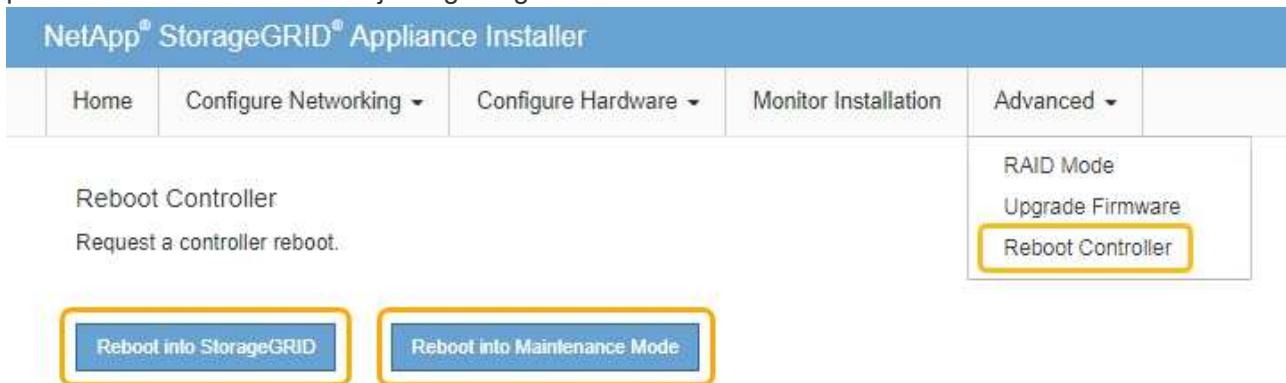
You might need to reboot the SG6000-CN controller while the StorageGRID Appliance Installer is running. For example, you might need to reboot the controller if the installation fails.

### About this task

This procedure only applies when the SG6000-CN controller is running the StorageGRID Appliance Installer. Once the installation is completed, this step no longer works because the StorageGRID Appliance Installer is no longer available.

### Steps

1. From the StorageGRID Appliance Installer, click **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



The SG6000-CN controller is rebooted.

## Maintaining the SG6000 appliance

You might need to perform maintenance procedures on the SG6000 appliance. The procedures in this section assume that the appliance has already been deployed as a Storage Node in a StorageGRID system.

### Steps

- Placing an appliance into maintenance mode
- Upgrading SANtricity OS on the storage controllers
- Upgrading drive firmware using SANtricity System Manager

- Adding an expansion shelf to a deployed SG6060
- Turning the controller identify LED on and off
- Locating the controller in a data center
- Replacing a storage controller
- Replacing hardware components in the storage controller shelf
- Replacing hardware components in the optional 60-drive expansion shelf
- Shutting down the SG6000-CN controller
- Powering on the SG6000-CN controller and verifying operation
- Replacing the SG6000-CN controller
- Replacing a power supply in the SG6000-CN controller
- Removing the SG6000-CN controller from a cabinet or rack
- Reinstalling the SG6000-CN controller into a cabinet or rack
- Removing the SG6000-CN controller cover
- Reinstalling the SG6000-CN controller cover
- Replacing the Fibre Channel HBA in the SG6000-CN controller
- Changing the link configuration of the SG6000-CN controller
- Changing the MTU setting
- Checking the DNS server configuration
- Monitoring node encryption in maintenance mode

## Placing an appliance into maintenance mode

You must place the appliance into maintenance mode before performing specific maintenance procedures.

### What you'll need

- You must be signed in to the Grid Manager using a supported browser.
- You must have the Maintenance or Root Access permission. For details, see the instructions for administering StorageGRID.

### About this task

Placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.



The password and host key for a StorageGRID appliance in maintenance mode remain the same as they were when the appliance was in service.

### Steps

1. From the Grid Manager, select **Nodes**.
2. From the tree view of the Nodes page, select the appliance Storage Node.
3. Select **Tasks**.

## Reboot

Shuts down and restarts the node.

**Reboot**

## Maintenance Mode

Places the appliance's compute controller into maintenance mode.

**Maintenance Mode**

### 4. Select **Maintenance Mode**.

A confirmation dialog box appears.

#### **⚠ Enter Maintenance Mode on SGA-106-15**

You must place the appliance's compute controller into maintenance mode to perform certain maintenance procedures on the appliance.

Attention: All StorageGRID services on this node will be shut down. Wait a few minutes for the node to reboot into maintenance mode.

If you are ready to start, enter the provisioning passphrase and click **OK**.

Provisioning Passphrase

**Cancel**

**OK**

### 5. Enter the provisioning passphrase, and select **OK**.

A progress bar and a series of messages, including "Request Sent," "Stopping StorageGRID," and "Rebooting," indicate that the appliance is completing the steps for entering maintenance mode.

## Reboot

Shuts down and restarts the node.

Reboot

## Maintenance Mode

**Attention:** Your request has been sent, but the appliance might take 10-15 minutes to enter maintenance mode. Do not perform maintenance procedures until this tab indicates maintenance mode is ready, or data could become corrupted.



Request Sent

When the appliance is in maintenance mode, a confirmation message lists the URLs you can use to access the StorageGRID Appliance Installer.

## Reboot

Shuts down and restarts the node.

Reboot

## Maintenance Mode

This node is currently in maintenance mode. Navigate to one of the URLs listed below and perform any necessary maintenance procedures.

- <https://172.16.2.106:8443>
- <https://10.224.2.106:8443>
- <https://47.47.2.106:8443>
- <https://169.254.0.1:8443>

When you are done with any required maintenance procedures, you must exit maintenance mode by clicking Reboot Controller from the StorageGRID Appliance Installer.

6. To access the StorageGRID Appliance Installer, browse to any of the URLs displayed.

If possible, use the URL containing the IP address of the appliance's Admin Network port.

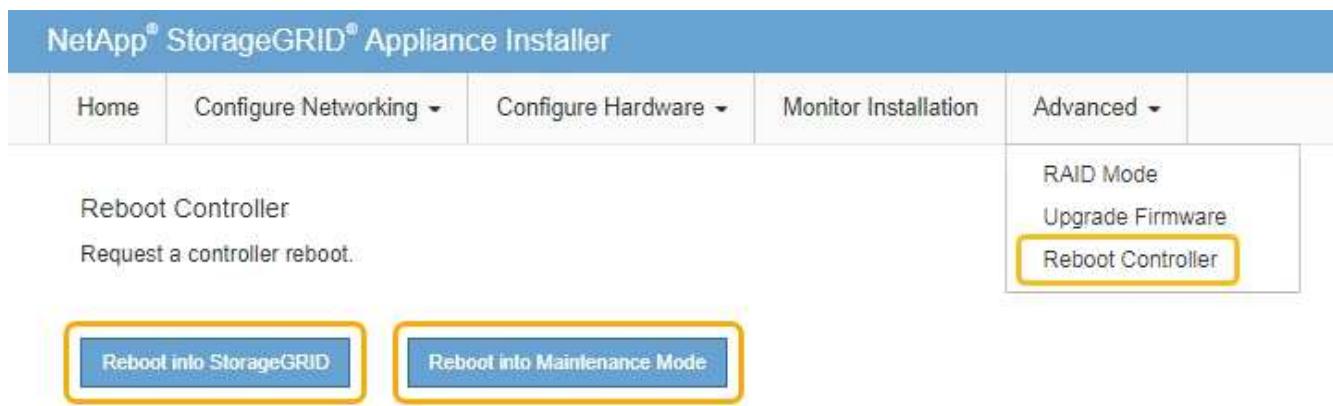


Accessing <https://169.254.0.1:8443> requires a direct connection to the local management port.

7. From the StorageGRID Appliance Installer, confirm that the appliance is in maintenance mode.

**⚠** This node is in maintenance mode. Perform any required maintenance procedures. If you want to exit maintenance mode manually to resume normal operation, go to Advanced > Reboot Controller to **reboot** the controller.

8. Perform any required maintenance tasks.
9. After completing maintenance tasks, exit maintenance mode and resume normal node operation. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select **Reboot into StorageGRID**.



NetApp® StorageGRID® Appliance Installer

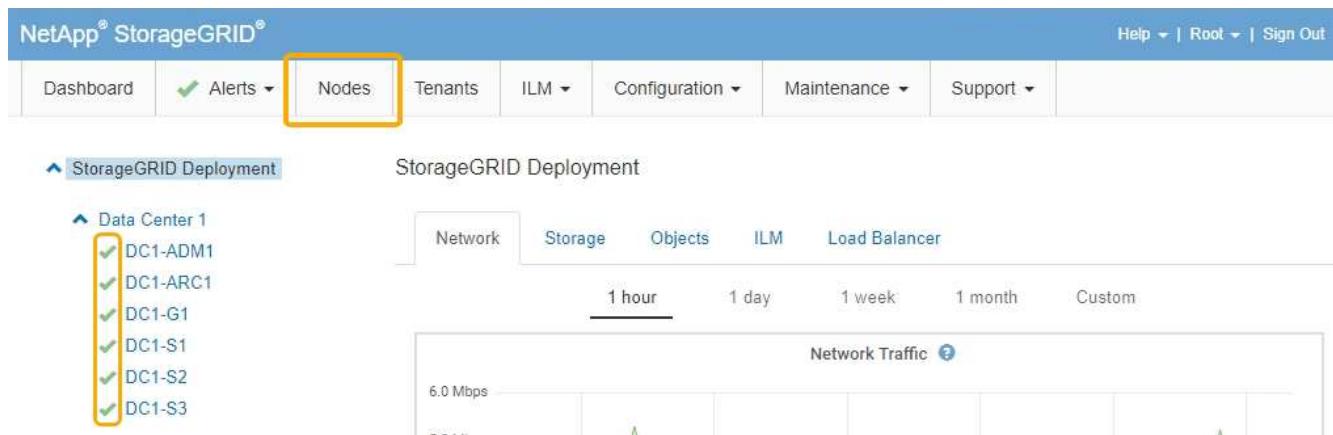
Home Configure Networking ▾ Configure Hardware ▾ Monitor Installation Advanced ▾

RAID Mode  
Upgrade Firmware  
**Reboot Controller**

Reboot Controller  
Request a controller reboot.

**Reboot into StorageGRID** **Reboot into Maintenance Mode**

It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **Nodes** tab should display a normal status **✓** for the appliance node, indicating that no alerts are active and the node is connected to the grid.



NetApp® StorageGRID®

Help ▾ | Root ▾ | Sign Out

Dashboard Alerts ▾ **Nodes** Tenants ILM ▾ Configuration ▾ Maintenance ▾ Support ▾

▲ StorageGRID Deployment StorageGRID Deployment

▲ Data Center 1

- ✓ DC1-ADM1
- ✓ DC1-ARC1
- ✓ DC1-G1
- ✓ DC1-S1
- ✓ DC1-S2
- ✓ DC1-S3

Network Storage Objects ILM Load Balancer

1 hour 1 day 1 week 1 month Custom

6.0 Mbps

Network Traffic

## Upgrading SANtricity OS on the storage controllers

To ensure optimal functioning of the storage controller, you must upgrade to the latest maintenance release of the SANtricity OS that is qualified for your StorageGRID appliance. Consult the NetApp Interoperability Matrix Tool (IMT) to determine which version you should be using. If you need assistance, contact technical support.

Use one of the following procedures based on the version of SANtricity OS currently installed:

- If the storage controller is using SANtricity OS 08.42.20.00 (11.42) or newer, use the Grid Manager to perform the upgrade.

### [Upgrading SANtricity OS on the storage controllers using the Grid Manager](#)

- If the storage controller is using a SANtricity OS version older than 08.42.20.00 (11.42), use maintenance mode to perform the upgrade.

### [Upgrading SANtricity OS on the storage controllers using maintenance mode](#)



When upgrading the SANtricity OS for your storage appliance, you must follow the instructions in the StorageGRID documentation. If you use any other instructions, your appliance could become inoperable.

#### **Related information**

[NetApp Interoperability Matrix Tool](#)

[NetApp Downloads: SANtricity OS](#)

[Monitor & troubleshoot](#)

### **Upgrading SANtricity OS on the storage controllers using the Grid Manager**

For storage controllers currently using SANtricity OS 08.42.20.00 (11.42) or newer, you must use the Grid Manager to apply an upgrade.

#### **What you'll need**

- You have consulted the NetApp Interoperability Matrix Tool (IMT) to confirm that the SANtricity OS version you are using for the upgrade is compatible with your appliance.
- You must have the Maintenance permission.
- You must be signed in to the Grid Manager using a supported browser.
- You must have the provisioning passphrase.
- You must have access to the NetApp downloads page for SANtricity OS.

#### **About this task**

You cannot perform other software updates (StorageGRID software upgrade or a hotfix) until you have completed the SANtricity OS upgrade process. If you attempt to start a hotfix or a StorageGRID software upgrade before the SANtricity OS upgrade process has finished, you are redirected to the SANtricity OS upgrade page.

The procedure will not be complete until the SANtricity OS upgrade has been successfully applied to all applicable nodes. It might take more than 30 minutes to load the SANtricity OS on each node and up to 90 minutes to reboot each StorageGRID storage appliance.



The following steps are only applicable when you are using the Grid Manager to perform the upgrade. The storage controllers in the SG6000 series appliances cannot be upgraded using the Grid Manager when the controllers are using SANtricity OS older than 08.42.20.00 (11.42).



This procedure will automatically upgrade the NVSRAM to the most recent version associated with the SANtricity OS upgrade. You do not need to apply a separate NVSRAM upgrade file.

## Steps

1. From a service laptop, download the new SANtricity OS Software file from the NetApp support site.

Be sure to choose the correct SANtricity OS version for the storage controllers in your appliance. The SG6060 uses the E2800 controller, and the SGF6024 uses the EF570 controller.

### NetApp Downloads: SANtricity OS

2. Sign in to the Grid Manager using a supported browser.
3. Select **Maintenance**. Then, in the System section of the menu, select **Software Update**.

The Software Update page appears.

#### Software Update

You can upgrade StorageGRID software, apply a hotfix, or upgrade the SANtricity OS software on StorageGRID storage appliances.

- To perform a major version upgrade of StorageGRID, see the [Instructions for upgrading StorageGRID](#), and then select **StorageGRID Upgrade**.
- To apply a hotfix to all nodes in your system, see "Hotfix procedure" in the [recovery and maintenance instructions](#), and then select **StorageGRID Hotfix**.
- To upgrade SANtricity OS software on a storage controller, see "Upgrading SANtricity OS Software on the storage controllers" in the installation and maintenance instructions for your storage appliance, and then select **SANtricity OS**:
  - SG6000 appliance installation and maintenance
  - SG5700 appliance installation and maintenance
  - SG5600 appliance installation and maintenance



StorageGRID Upgrade

StorageGRID Hotfix

SANtricity OS

4. Click **SANtricity OS**.

The SANtricity OS page appears.

## SANtricity OS

You can use this page to upgrade the SANtricity OS software on storage controllers in a storage appliance. Before installing the new software, confirm the storage controllers are Nominal (**Nodes > appliance node > Hardware**) and ready for an upgrade. A health check is automatically performed as part of the upgrade process and valid NVSRAM is automatically installed based on the appliance type and new software version. The software upgrade can take up to 30 minutes per appliance. When the upgrade is complete, the node will be automatically rebooted to activate the SANtricity OS on the storage controllers. If you have multiple types of appliances, repeat this procedure to install the appropriate OS software for each type.

### SANtricity OS Upgrade File

SANtricity OS Upgrade File 

### Passphrase

Provisioning Passphrase 

 Start

5. Select the SANtricity OS upgrade file you downloaded from the NetApp support site.

- a. Click **Browse**.
- b. Locate and select the file.
- c. Click **Open**.

The file is uploaded and validated. When the validation process is done, the file name is shown in the Details field.



Do not change the file name since it is part of the verification process.

## SANtricity OS

You can use this page to upgrade the SANtricity OS software on storage controllers in a storage appliance. Before installing the new software, confirm the storage controllers are Nominal (**Nodes > appliance node > Hardware**) and ready for an upgrade. A health check is automatically performed as part of the upgrade process and valid NVSRAM is automatically installed based on the appliance type and new software version. The software upgrade can take up to 30 minutes per appliance. When the upgrade is complete, the node will be automatically rebooted to activate the SANtricity OS on the storage controllers. If you have multiple types of appliances, repeat this procedure to install the appropriate OS software for each type.

### SANtricity OS Upgrade File

The screenshot shows the SANtricity OS Upgrade File page. It includes a 'SANtricity OS Upgrade File' section with a 'Browse' button and a checked file entry 'RC\_...dlp'. Below it is a 'Details' section with a file entry 'RC\_...dlp'. The next section is 'Passphrase' with a 'Provisioning Passphrase' field and a 'Start' button.

6. Enter the provisioning passphrase.

The **Start** button is enabled.

## SANtricity OS

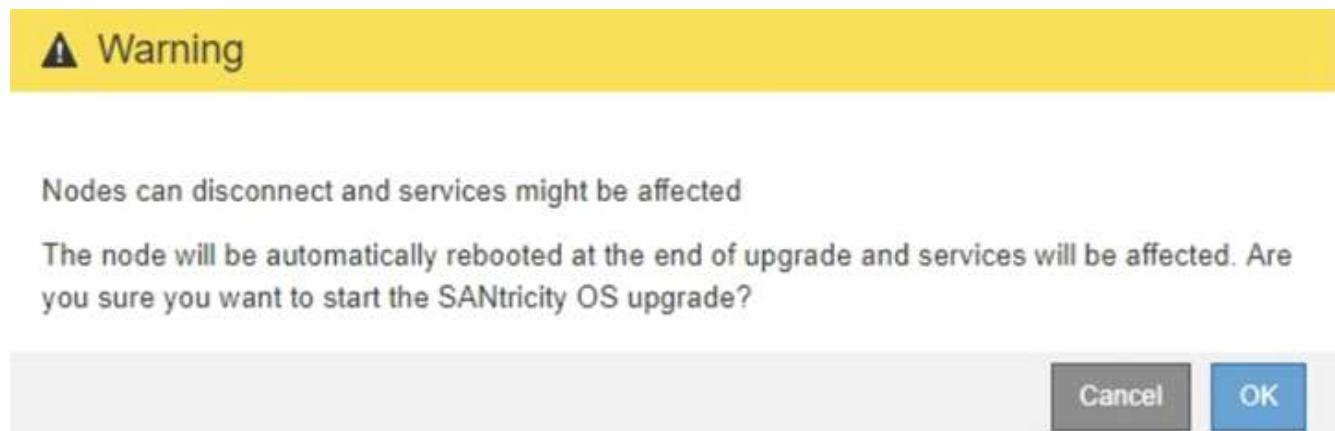
You can use this page to upgrade the SANtricity OS software on storage controllers in a storage appliance. Before installing the new software, confirm the storage controllers are Nominal (**Nodes > appliance node > Hardware**) and ready for an upgrade. A health check is automatically performed as part of the upgrade process and valid NVSRAM is automatically installed based on the appliance type and new software version. The software upgrade can take up to 30 minutes per appliance. When the upgrade is complete, the node will be automatically rebooted to activate the SANtricity OS on the storage controllers. If you have multiple types of appliances, repeat this procedure to install the appropriate OS software for each type.

### SANtricity OS Upgrade File

The screenshot shows the SANtricity OS Upgrade File page. It includes a 'SANtricity OS Upgrade File' section with a 'Browse' button and a checked file entry 'RC\_...dlp'. Below it is a 'Details' section with a file entry 'RC\_...dlp'. The next section is 'Passphrase' with a 'Provisioning Passphrase' field containing redacted text and a 'Start' button.

7. Click **Start**.

A warning box appears stating that your browser's connection might be lost temporarily as services on nodes that are upgraded are restarted.



8. Click **OK** to stage the SANtricity OS upgrade file to the primary Admin Node.

When the SANtricity OS upgrade starts:

- a. The health check is run. This process checks that no nodes have the status of Needs Attention.



If any errors are reported, resolve them and click **Start** again.

- b. The SANtricity OS Upgrade Progress table appears. This table shows all Storage Nodes in your grid and the current stage of the upgrade for each node.



The table shows all Storage Nodes, including software-based Storage Nodes. You must approve the upgrade for all Storage Nodes, even though a SANtricity OS upgrade has no effect on software-based Storage Nodes. The upgrade message returned for software-based Storage Nodes is "SANtricity OS upgrade is not applicable to this node."

#### SANtricity OS Upgrade Progress

Storage Nodes - 0 out of 4 completed							Approve All	Remove All
Site	Name	Progress	Stage	Details	Action		Search	
RTP Lab 1	DT-10-224-1-181-S1		Waiting for you to approve		<a href="#">Approve</a>			
RTP Lab 1	DT-10-224-1-182-S2		Waiting for you to approve		<a href="#">Approve</a>			
RTP Lab 1	DT-10-224-1-183-S3		Waiting for you to approve		<a href="#">Approve</a>			
RTP Lab 1	NetApp-SGA-Lab2-002-024		Waiting for you to approve		<a href="#">Approve</a>			

9. Optionally, sort the list of nodes in ascending or descending order by **Site**, **Name**, **Progress**, **Stage**, or **Details**. Or, enter a term in the **Search** box to search for specific nodes.

You can scroll through the list of nodes by using the left and right arrows at the bottom right corner of the section.

10. 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.



Do not approve the SANtricity OS upgrade for an appliance storage node unless you are sure the node is ready to be stopped and rebooted. When the SANtricity OS upgrade is approved on a node, the services on that node are stopped. Later, when the node is upgraded, the appliance node is rebooted. These operations might cause service interruptions for clients that are communicating with the node.

- Click either of the **Approve All** buttons to add all Storage Nodes to the SANtricity OS upgrade queue.



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(s).

- Click one or more **Approve** buttons to add one or more nodes to the SANtricity OS upgrade queue.



You can delay applying a SANtricity OS upgrade to a node, but the SANtricity OS upgrade process will not be complete until you approve the SANtricity OS upgrade on all the listed Storage Nodes.

After you click **Approve**, the upgrade process determines if the node can be upgraded. If a node can be upgraded, it is added to the upgrade queue.

For some nodes, the selected upgrade file is intentionally not applied and you can complete the upgrade process without upgrading these specific nodes. For nodes intentionally not upgraded, the process will show stage of Complete with one of the following messages in the Details column:

- Storage Node was already upgraded.
- SANtricity OS upgrade is not applicable to this node.
- SANtricity OS file is not compatible with this node.

The message “SANtricity OS upgrade is not applicable to this node” indicates that the node does not have a storage controller that can be managed by the StorageGRID system. This message will appear for non-appliance Storage Nodes. You can complete the SANtricity OS upgrade process without upgrading the node displaying this message.

The message “SANtricity OS file is not compatible with this node” indicates that the node requires a SANtricity OS file different than the one the process is attempting to install. After you complete the current SANtricity OS upgrade, download the SANtricity OS appropriate for the node and repeat the upgrade process.

11. If you need to remove a node or all nodes from the SANtricity OS upgrade queue, click **Remove** or **Remove All**.

As shown in the example, when the stage progresses beyond Queued, the **Remove** button is hidden and you can no longer remove the node from the SANtricity OS upgrade process.

▲ Storage Nodes - 1 out of 9 completed

Approve All Remove All

Search 

Site	Name	Progress	Stage	Details	Action
Raleigh	RAL-S1-101-196	Queued			
Raleigh	RAL-S2-101-197	Complete			
Raleigh	RAL-S3-101-198	Queued			
Sunnyvale	SVL-S1-101-199	Queued			
Sunnyvale	SVL-S2-101-93		Waiting for you to approve		
Sunnyvale	-SVL-S3-101-94		Waiting for you to approve		
Vancouver	VTC-S1-101-193		Waiting for you to approve		
Vancouver	-VTC-S2-101-194		Waiting for you to approve		
Vancouver	-VTC-S3-101-195		Waiting for you to approve		

12. Wait while the SANtricity OS upgrade is applied to each approved grid node.



If any node shows a stage of Error while the SANtricity OS upgrade is being applied, the upgrade has failed for that node. The appliance might need to be placed in maintenance mode to recover from the failure. Contact technical support before continuing.

If the firmware on the node is too old to be upgraded with the Grid Manager, the node shows a stage of Error with the details: "You must use maintenance mode to upgrade SANtricity OS on this node. See the installation and maintenance instructions for your appliance. After the upgrade, you can use this utility for future upgrades." To resolve the error, do the following:

- Use maintenance mode to upgrade SANtricity OS on the node that shows a stage of Error.
- Use the Grid Manager to re-start and complete the SANtricity OS upgrade.

When the SANtricity OS upgrade is complete on all approved nodes, the SANtricity OS Upgrade Progress table closes and a green banner shows the date and time the SANtricity OS upgrade was completed.

SANtricity OS upgrade completed at 2020-04-07 13:26:02 EDT.

SANtricity OS Upgrade File

SANtricity OS Upgrade File 

Passphrase

Provisioning Passphrase 

13. Repeat this upgrade procedure for any nodes with a stage of Complete that require a different SANtricity OS upgrade file.



For any nodes with a status of Needs Attention, use maintenance mode to perform the upgrade.

## Related information

[NetApp Interoperability Matrix Tool](#)

[Upgrading SANtricity OS on the storage controllers using maintenance mode](#)

### Upgrading SANtricity OS on the storage controllers using maintenance mode

For storage controllers currently using SANtricity OS older than 08.42.20.00 (11.42), you must use the maintenance mode procedure to apply an upgrade.

#### What you'll need

- You have consulted the NetApp Interoperability Matrix Tool (IMT) to confirm that the SANtricity OS version you are using for the upgrade is compatible with your appliance.
- If the StorageGRID appliance is running in a StorageGRID system, the SG6000-CN controller has been placed in maintenance mode.



Maintenance mode interrupts the connection to the storage controller.

[Placing an appliance into maintenance mode](#)

#### About this task

Do not upgrade the SANtricity OS or NVSRAM in the E-Series controller on more than one StorageGRID appliance at a time.



Upgrading more than one StorageGRID appliance at a time might cause data unavailability, depending on your deployment model and ILM policies.

#### Steps

1. From a service laptop, access SANtricity System Manager and sign in.
2. Download the new SANtricity OS Software file and NVSRAM file to the management client.



The NVSRAM is specific to the StorageGRID appliance. Do not use the standard NVSRAM download.

3. Follow the instructions in the *Upgrading SANtricity OS* guide or the SANtricity System Manager online help to upgrade the firmware and NVSRAM.



Activate the upgrade files immediately. Do not defer activation.

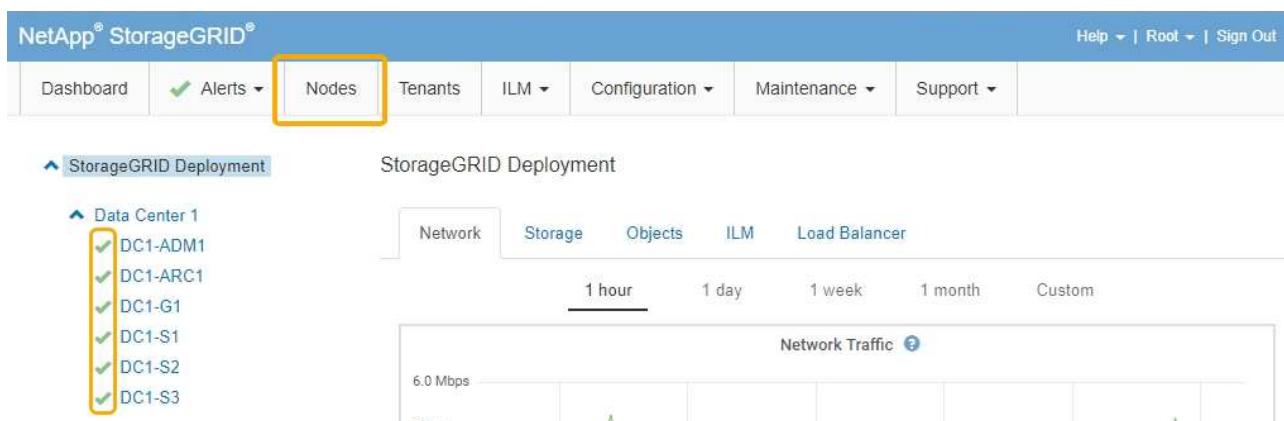
4. Once the upgrade operation has completed, reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in

maintenance mode. Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



The screenshot shows the 'Reboot Controller' section of the StorageGRID Appliance Installer. It includes a 'Reboot Controller' button, a 'Request a controller reboot.' link, and a 'Reboot Controller' link in the 'Advanced' dropdown menu, all highlighted with yellow boxes.

It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **Nodes** tab should display a normal status  for the appliance node, indicating that no alerts are active and the node is connected to the grid.



The screenshot shows the StorageGRID Grid Manager interface with the 'Nodes' tab selected, highlighted with a yellow box. The 'Nodes' tab displays a list of nodes under 'Data Center 1', including DC1-ADM1, DC1-ARC1, DC1-G1, DC1-S1, DC1-S2, and DC1-S3, all of which have a green checkmark icon next to them, indicating they are connected to the grid.

#### Related information

[NetApp Interoperability Matrix Tool](#)

[Upgrading SANtricity OS on the storage controllers using the Grid Manager](#)

## Upgrading drive firmware using SANtricity System Manager

You upgrade your drive firmware to make sure you have all the latest features and bug fixes.

#### What you'll need

- The storage appliance has an Optimal status.
- All drives have an Optimal status.
- You have the latest version of SANtricity System Manager installed that is compatible with your StorageGRID version.
- You have placed the StorageGRID appliance in maintenance mode.

## Placing an appliance into maintenance mode



Maintenance mode interrupts the connection to the storage controller, stopping all I/O activity and placing all drives offline.



Do not upgrade the drive firmware on more than one StorageGRID appliance at a time. Doing so might cause data unavailability, depending on your deployment model and ILM policies.

### Steps

1. Access SANtricity System Manager using one of these methods:
  - Use the StorageGRID Appliance Installer and select **Advanced > SANtricity System Manager**
  - Use the Grid Manager and select **Nodes > appliance Storage Node > SANtricity System Manager**



If these options are not available or the SANtricity System Manager login page does not appear, access SANtricity System Manager by browsing to the storage controller IP:  
**[https://Storage\\_Controller\\_IP](https://Storage_Controller_IP)**

2. Enter the SANtricity System Manager administrator username and password, if required.

3. Verify the drive firmware version currently installed in the storage appliance:

- a. From SANtricity System Manager, select **Support > Upgrade Center**.
- b. Under Drive Firmware upgrade, select **Begin Upgrade**.

The Upgrade Drive Firmware displays the drive firmware files currently installed.

- c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.

Upgrade Drive Firmware

**1 Select Upgrade Files** **2 Select Drives**

Review your current drive firmware and select upgrade files below...

What do I need to know before upgrading drive firmware?

Current Drive Firmware	Associated Drives
MS02, KPM51VUG800G	<a href="#">View drives</a>

Total rows: 1

Select up to four drive firmware files. [Browse...](#)

In this example:

- The drive firmware revision is **MS02**.
- The drive identifier is **KPM51VUG800G**.

Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.

d. Close the Upgrade Drive Firmware window.

4. Download and prepare the available drive firmware upgrade:

- Under Drive Firmware upgrade, select **NetApp Support**.
- On the NetApp Support web site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

The E-Series Disk Firmware page displays.

- Search for each **Drive Identifier** installed in your storage appliance and verify that each drive identifier has the latest firmware revision.
  - If the firmware revision is not a link, this drive identifier has the latest firmware revision.
  - If one or more drive part numbers are listed for a drive identifier, a firmware upgrade is available for these drives. You can select any link to download the firmware file.

Drive Part Number	Descriptions	Drive Identifier	Firmware Rev. (Download)	Notes and Config Info	Release Date
E-X4041C	SSD, 800GB, SAS, PI	KPM51VUG800G	<a href="#">Firmware Rev. (Download)</a>	MS02 Fixes Bug 1194908 MS03 Fixes Bug 1334862	04-Sep-2020

- If a later firmware revision is listed, select the link in the Firmware Rev. (Download) column to download a .zip archive containing the firmware file.
- Extract (unzip) the drive firmware archive files you downloaded from the Support site.

5. Install the drive firmware upgrade:

- From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.
- Select **Browse**, and select the new drive firmware files that you downloaded from the Support site.

Drive firmware files have a filename similar to

D\_HUC101212CSS600\_30602291\_MS01\_2800\_0002.dlp.

You can select up to four drive firmware files, one at a time. If more than one drive firmware file is compatible with the same drive, you get a file conflict error. Decide which drive firmware file you want to use for the upgrade and remove the other one.

- Select **Next**.

**Select Drives** lists the drives that you can upgrade with the selected firmware files.

Only drives that are compatible appear.

The selected firmware for the drive appears in **Proposed Firmware**. If you must change this firmware, select **Back**.

- d. Select **Offline (parallel)** upgrade.

You can use the offline upgrade method because the appliance is in maintenance mode, where I/O activity is stopped for all drives and all volumes.

- e. In the first column of the table, select the drive or drives you want to upgrade.

The best practice is to upgrade all drives of the same model to the same firmware revision.

- f. Select **Start**, and confirm that you want to perform the upgrade.

If you need to stop the upgrade, select **Stop**. Any firmware downloads currently in progress complete. Any firmware downloads that have not started are canceled.



Stopping the drive firmware upgrade might result in data loss or unavailable drives.

- g. (Optional) To see a list of what was upgraded, select **Save Log**.

The log file is saved in the downloads folder for your browser with the name `latest-upgrade-log-timestamp.txt`.

If any of the following errors occur during the upgrade procedure, take the appropriate recommended action.

- **Failed assigned drives**

One reason for the failure might be that the drive does not have the appropriate signature. Make sure that the affected drive is an authorized drive. Contact technical support for more information.

When replacing a drive, make sure that the replacement drive has a capacity equal to or greater than the failed drive you are replacing.

You can replace the failed drive while the storage array is receiving I/O.

- **Check storage array**

- Make sure that an IP address has been assigned to each controller.
- Make sure that all cables connected to the controller are not damaged.
- Make sure that all cables are tightly connected.

- **Integrated hot spare drives**

This error condition must be corrected before you can upgrade the firmware.

- **Incomplete volume groups**

If one or more volume groups or disk pools are incomplete, you must correct this error condition before you can upgrade the firmware.

- **Exclusive operations (other than background media/parity scan) currently running on any**

## volume groups

If one or more exclusive operations are in progress, the operations must complete before the firmware can be upgraded. Use System Manager to monitor the progress of the operations.

- **Missing volumes**

You must correct the missing volume condition before the firmware can be upgraded.

- **Either controller in a state other than Optimal**

One of the storage array controllers needs attention. This condition must be corrected before the firmware can be upgraded.

- **Mismatched Storage Partition information between Controller Object Graphs**

An error occurred while validating the data on the controllers. Contact technical support to resolve this issue.

- **SPM Verify Database Controller check fails**

A storage partitions mapping database error occurred on a controller. Contact technical support to resolve this issue.

- **Configuration Database Validation (If supported by the storage array's controller version)**

A configuration database error occurred on a controller. Contact technical support to resolve this issue.

- **MEL Related Checks**

Contact technical support to resolve this issue.

- **More than 10 DDE Informational or Critical MEL events were reported in the last 7 days**

Contact technical support to resolve this issue.

- **More than 2 Page 2C Critical MEL Events were reported in the last 7 days**

Contact technical support to resolve this issue.

- **More than 2 Degraded Drive Channel Critical MEL events were reported in the last 7 days**

Contact technical support to resolve this issue.

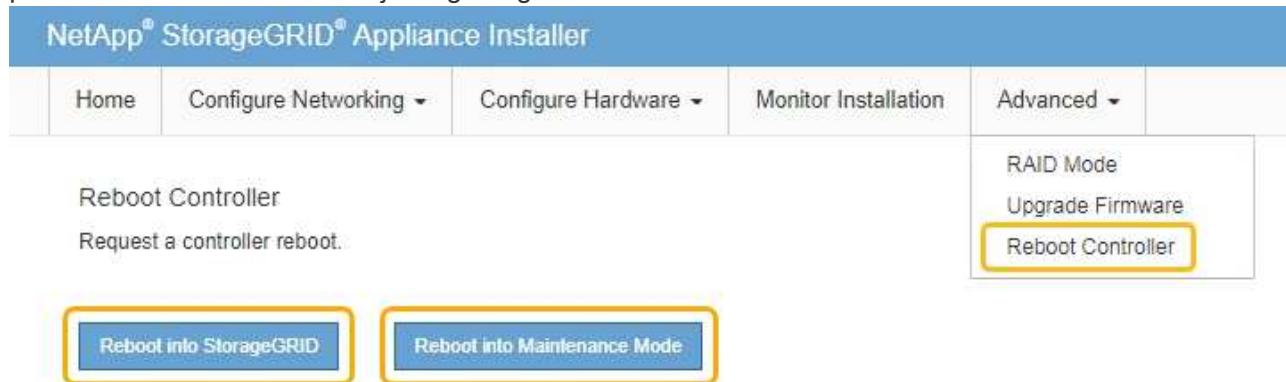
- **More than 4 critical MEL entries in the last 7 days**

Contact technical support to resolve this issue.

6. Once the upgrade operation has completed, reboot the appliance. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:

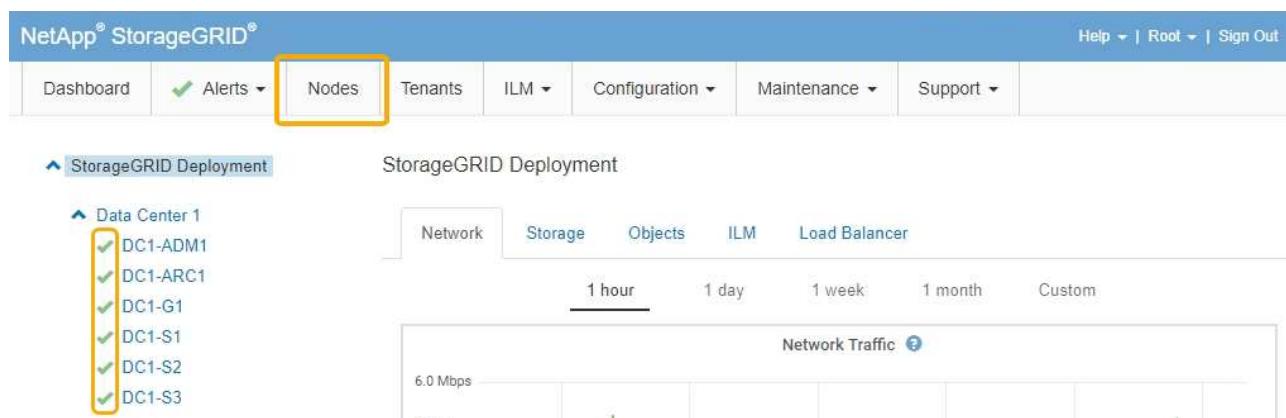
- Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
- Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in

maintenance mode. Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



The screenshot shows the 'Reboot Controller' section of the StorageGRID Appliance Installer. It includes a 'Reboot Controller' button, a 'Request a controller reboot.' link, and a 'Reboot Controller' link in the 'Advanced' dropdown menu, all highlighted with yellow boxes.

It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **Nodes** tab should display a normal status  for the appliance node, indicating that no alerts are active and the node is connected to the grid.



The screenshot shows the StorageGRID Grid Manager interface. The 'Nodes' tab is selected and highlighted with a yellow box. The 'Data Center 1' section lists nodes: DC1-ADM1, DC1-ARC1, DC1-G1, DC1-S1, DC1-S2, and DC1-S3, all of which have green checkmarks indicating they are connected. The 'Network' tab is selected in the navigation bar.

#### Related information

[Upgrading SANtricity OS on the storage controllers](#)

## Adding an expansion shelf to a deployed SG6060

To increase storage capacity, you can add one or two expansion shelves to an SG6060 that is deployed in a StorageGRID system.

#### What you'll need

- You must have the provisioning passphrase.
- You must be running StorageGRID 11.4 or later.
- You have the expansion shelf and two SAS cables for each expansion shelf.
- You have physically located the storage appliance where you are adding the expansion shelf in the data center.

[Locating the controller in a data center](#)

## About this task

To add an expansion shelf, you perform these high-level steps:

- Install the hardware in the cabinet or rack.
- Place the SG6060 into maintenance mode.
- Connect the expansion shelf to the E2860 controller shelf or to another expansion shelf.
- Start the expansion using the StorageGRID Appliance Installer
- Wait until the new volumes are configured.

Completing the procedure for one or two expansion shelves should take one hour or less per appliance node. To minimize downtime, the following steps instruct you to install the new expansion shelves and drives before placing the SG6060 into maintenance mode. The remaining steps should take approximately 20 to 30 minutes per appliance node.

### Steps

1. Follow the instructions for installing 60-drive shelves into a cabinet or rack.

[SG6060: Installing 60-drive shelves into a cabinet or rack](#)

2. Follow the instructions for installing the drives.

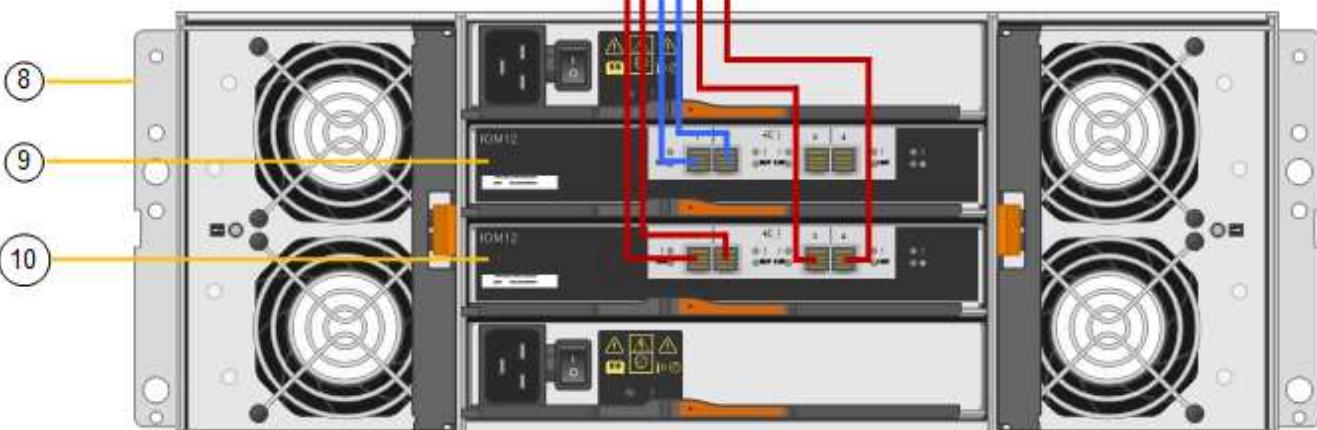
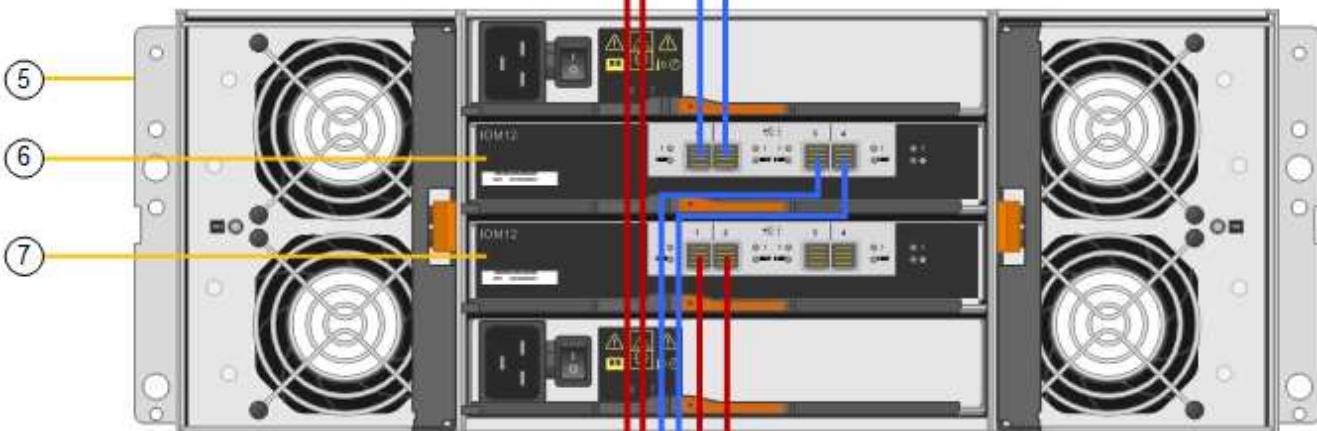
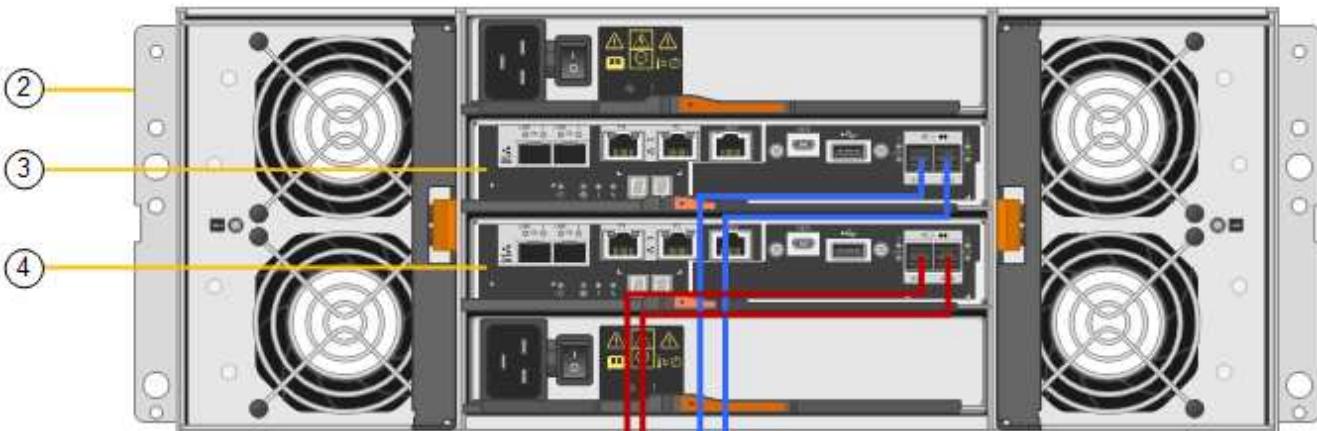
[SG6060: Installing the drives](#)

3. From the Grid Manager, place the SG6000-CN controller into maintenance mode.

[Placing an appliance into maintenance mode](#)

4. Connect each expansion shelf to the E2860 controller shelf as shown in the diagram.

This drawing shows two expansion shelves. If you have only one, connect IOM A to controller A and connect IOM B to controller B.



	Description
1	SG6000-CN

	<b>Description</b>
2	E2860 controller shelf
3	Controller A
4	Controller B
5	Expansion shelf 1
6	IOM A for expansion shelf 1
7	IOM B for expansion shelf 1
8	Expansion shelf 2
9	IOM A for expansion shelf 2
10	IOM B for expansion shelf 2

5. Connect the power cords and apply power to the expansion shelves.
  - a. Connect a power cord to each of the two power supply units in each expansion shelf.
  - b. Connect the two power cords in each expansion shelf to two different PDUs in the cabinet or rack.
  - c. Turn on the two power switches for each expansion shelf.
    - Do not turn off the power switches during the power-on process.
    - The fans in the expansion shelves might be very loud when they first start up. The loud noise during start-up is normal.
6. Monitor the Home page of the StorageGRID Appliance Installer.

In approximately five minutes, the expansion shelves finish powering up and are detected by the system. The Home page shows the number of new expansion shelves detected, and the Start Expansion button is enabled.

The screenshot shows examples of the messages that could appear on the Home page, depending on the number of existing or new expansion shelves, as follows:

- The banner circled at the top of the page indicates the total number of expansion shelves detected.
  - The banner indicates the total number of expansion shelves, whether the shelves are configured and deployed or new and unconfigured.
  - If no expansion shelves are detected, the banner will not appear.
- The message circled at the bottom of the page indicates an expansion is ready to be started.
  - The message indicates the number of new expansion shelves StorageGRID detects. “Attached” indicates that the shelf is detected. “Unconfigured” indicates that the shelf is new and not yet configured using the StorageGRID Appliance Installer.



Expansion shelves that are already deployed are not included in this message. They are included in the count in the banner at the top of the page.

- The message will not appear if new expansion shelves are not detected.

The screenshot shows a configuration page for adding expansion shelves. At the top, there are two informational messages:

- 1 The expansion is ready to be started. Make sure this page accurately indicates the number of new storage shelves you are trying to add, then click Start Expansion.
- 2 The storage system contains 2 expansion shelves.

The main configuration area is titled "This Node". It includes fields for "Node type" (Storage) and "Node name" (NetApp-SGA), with "Save" and "Cancel" buttons.

The "Primary Admin Node connection" section includes "Enable Admin Node discovery" (unchecked), "Primary Admin Node IP" (172.16.4.71), and "Connection state" (Connection to 172.16.4.71 ready), with "Save" and "Cancel" buttons.

The "Installation" section shows "Current state" (Ready to start configuration of 1 attached but unconfigured expansion shelf) and a "Start Expansion" button, which is highlighted with a yellow box.

7. As necessary, resolve any issues described in the messages on the Home page.

For example, use SANtricity System Manager to resolve any storage hardware issues.

8. Verify that the number of expansion shelves displayed on the Home page matches the number of expansion shelves you are adding.



If the new expansion shelves have not been detected, verify that they are properly cabled and powered up.

9. Click **Start Expansion** to configure the expansion shelves and make them available for object storage.

10. Monitor the progress of the expansion shelf configuration.

Progress bars appear on the web page, just as they do during initial installation.

1. Configure storage			Running
Step	Progress	Status	
Connect to storage controller	<div style="width: 100%; background-color: #2e7131;"></div>	Complete	
Clear existing configuration	<div style="width: 100%; background-color: #2e7131;"></div>	Skipped	
Configure volumes	<div style="width: 20%; background-color: #0070C0;"></div>	Creating volume StorageGRID-obj-22	
Configure caching	<div style="width: 0%; background-color: #D9D9D9;"></div>	Pending	
Configure host settings	<div style="width: 0%; background-color: #D9D9D9;"></div>	Pending	

2. Complete storage expansion	Pending
-------------------------------	---------

When configuration is complete, the appliance automatically reboots to exit maintenance mode and rejoin the grid. This process can take up to 20 minutes.



If the appliance does not rejoin the grid, go to the StorageGRID Appliance Installer Home page, select **Advanced > Reboot Controller**, and then select **Reboot into Maintenance Mode**.

When the reboot is complete, the **Tasks** tab looks like the following screenshot:

The screenshot shows the StorageGRID Appliance Installer interface with the **Tasks** tab selected. Below the tabs, there are two main sections: **Reboot** and **Maintenance Mode**.

**Reboot** section: Describes the action as "Shuts down and restarts the node." with a **Reboot** button.

**Maintenance Mode** section: Describes the action as "Places the appliance's compute controller into maintenance mode." with a **Maintenance Mode** button.

## 11. Verify the status of the appliance Storage Node and the new expansion shelves.

- In the Grid Manager, select **Nodes** and verify that the appliance Storage Node has a green checkmark icon.

The green checkmark icon means that no alerts are active and the node is connected to the grid. For a description of node icons, see the instructions for monitoring and troubleshooting StorageGRID.

- Select the **Storage** tab and confirm that 16 new object stores are shown in the Object Storage table for each expansion shelf you added.
- Verify that each new expansion shelf has a shelf status of Nominal and a configuration status of Configured.

Storage Shelves												
Shelf Chassis Serial Number	Shelf ID	Shelf Status	IOM Status	Power Supply Status	Drawer Status	Fan Status	Drive Slots	Data Drives	Data Drive Size	Cache Drives	Cache Drive Size	Configuration Status
721924500063	99	Nominal 	N/A	Nominal	Nominal	Nominal	60	58	9.80 TB	2	800.17 GB	Configured (in use)
721929500038	0	Nominal 	Nominal	Nominal	Nominal	Nominal	60	60	9.80 TB	0	0 bytes	Configured (in use)
721929500039	1	Nominal 	Nominal	Nominal	Nominal	Nominal	60	60	9.80 TB	0	0 bytes	Configured (in use)

## Related information

[Unpacking the boxes \(SG6000\)](#)

[SG6060: Installing 60-drive shelves into a cabinet or rack](#)

[SG6060: Installing the drives](#)

[Monitor & troubleshoot](#)

## Turning the controller identify LED on and off

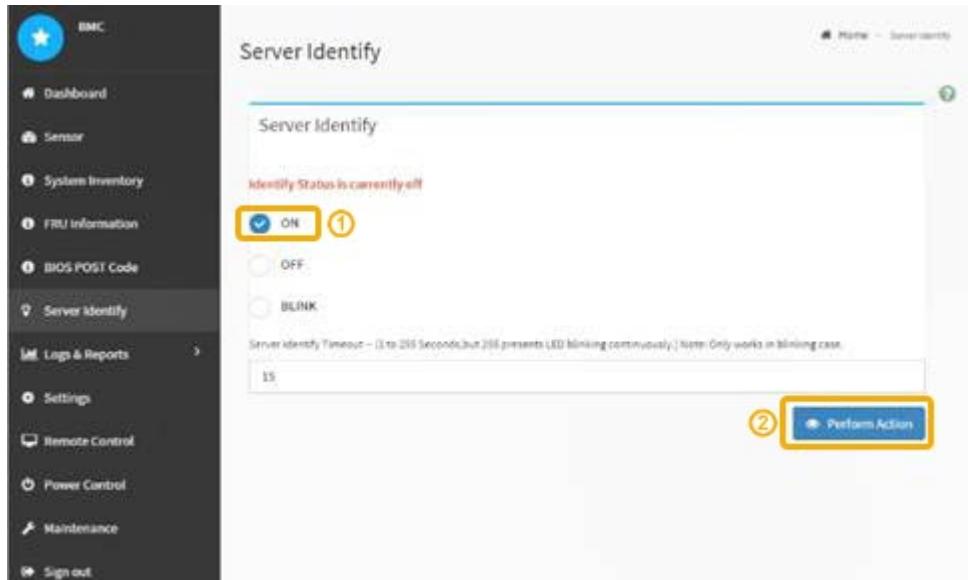
The blue identify LED on the front and back of the controller can be turned on to help locate the appliance in a data center.

### What you'll need

You must have the BMC IP address of the controller you want to identify.

### Steps

1. Access the controller BMC interface.
2. Select **Server Identify**.
3. Select **ON** and then select **Perform Action**.



### Result

The blue identify LEDs light on the front (shown) and rear of the controller.



If a bezel is installed on the controller, it might be difficult to see the front identify LED.

#### After you finish

To turn off the controller identify LED:

- Press the identify LED switch on the controller front panel.
- From the controller BMC interface, select **Server Identify**, select **OFF** and then select **Perform Action**.

The blue identify LEDs on the front and rear of the controller go off.



#### Related information

[Verifying the Fibre Channel HBA to replace](#)

[Locating the controller in a data center](#)

[Accessing the BMC interface](#)

## Locating the controller in a data center

Locate the controller so that you can perform hardware maintenance or upgrades.

#### What you'll need

- You have determined which controller requires maintenance.

(Optional) To help locate the controller in your data center, turn on the blue identify LED.

## Turning the controller identify LED on and off

### Steps

#### 1. Find the controller requiring maintenance in the data center.

- Look for a lit blue identify LED on the front or rear of the controller.

The front identify LED is behind the controller front bezel and might be difficult to see if the bezel is installed.



- Check the tags attached to the front of each controller for a matching part number.

#### 2. Remove the controller front bezel, if one is installed, to access the front panel controls and indicators.

#### 3. Optional: Turn off the blue identify LED if you used it to locate the controller.

- Press the identify LED switch on the controller front panel.
- Use the controller BMC interface.

## Turning the controller identify LED on and off

### Related information

[Removing the Fibre Channel HBA](#)

[Removing the SG6000-CN controller from a cabinet or rack](#)

[Shutting down the SG6000-CN controller](#)

## Replacing a storage controller

You might need to replace an E2800 controller or an EF570 controller if it is not functioning optimally or if it has failed.

### What you'll need

- You have a replacement controller with the same part number as the controller you are replacing.
- You have labels to identify each cable that is connected to the controller.
- You have an ESD wristband, or you have taken other antistatic precautions.
- You have a #1 Phillips screwdriver.
- You have the E-Series instructions for replacing a controller in duplex configuration.



Refer to the E-Series instructions only when directed or if you need more details to perform a specific step. Do not rely on the E-Series instructions to replace a controller in the StorageGRID appliance, because the procedures are not the same.

- You have physically located the storage appliance where you are replacing the controller in the data center.

### [Locating the controller in a data center](#)

#### **About this task**

You can determine if you have a failed controller in two ways:

- The Recovery Guru in SANtricity System Manager directs you to replace the controller.
- The amber Attention LED on the controller is on, indicating that the controller has a fault.



If both controllers in the shelf have their Attention LEDs on, contact technical support for assistance.

Because the storage controller shelf contains two storage controllers, you can replace one of the controllers while your appliance is powered on and performing read/write operations, as long as the following conditions are true:

- The second controller in the shelf has Optimal status.
- The “OK to remove” field in the Details area of the Recovery Guru in SANtricity System Manager displays Yes, indicating that it is safe to remove this component.



If the second controller canister in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the controller canister, contact technical support.

When you replace a controller, you must remove the battery from the original controller and install it in the replacement controller.



The storage controllers in the appliance do not include host interface cards (HIC).

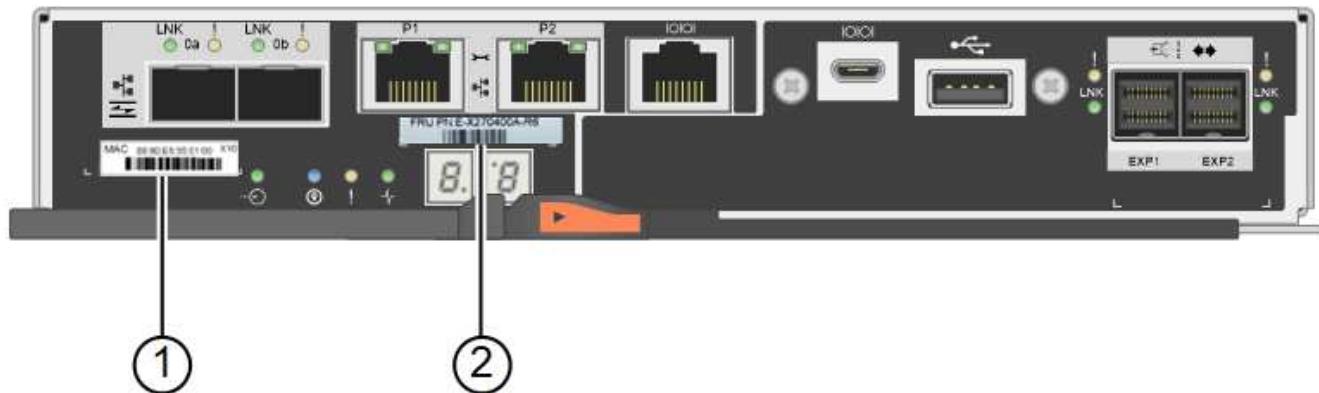
#### **Steps**

1. Unpack the new controller, and set it on a flat, static-free surface.

Save the packing materials to use when shipping the failed controller.

2. Locate the MAC address and FRU part number labels on the back of the replacement controller.

This figure shows the E2800 controller. The procedure for replacing the EF570 controller is identical.



Label	Label	Description
1	MAC address	The MAC address for management port 1 ("P1"). If you used DHCP to obtain the original controller's IP address, you will need this address to connect to the new controller.
2	FRU part number	The FRU part number. This number must match the replacement part number for the currently installed controller.

### 3. Prepare to remove the controller.

You use SANtricity System Manager to perform these steps. As needed for additional details, reference the E-Series instructions for replacing the storage controller.

- Confirm that the replacement part number for the failed controller is the same as the FRU part number for the replacement controller.

When a controller has a fault and needs to be replaced, the replacement part number is displayed in the Details area of the Recovery Guru. If you need to find this number manually, you can look on the **Base** tab for the controller.



**Possible loss of data access** -- If the two part numbers are not the same, do not attempt this procedure.

- Back up the configuration database.

If a problem occurs when you remove a controller, you can use the saved file to restore your configuration.

- Collect support data for the appliance.



Collecting support data before and after replacing a component ensures you can send a full set of logs to technical support in case the replacement does not resolve the problem.

d. Take the controller you plan to replace offline.

4. Remove the controller from the appliance:

- Put on an ESD wristband or take other antistatic precautions.
- Label the cables and then disconnect the cables and SFPs.

 To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

- Release the controller from the appliance by squeezing the latch on the cam handle until it releases, and then open the cam handle to the right.
- Using two hands and the cam handle, slide the controller out of the appliance.

 Always use two hands to support the weight of the controller.

- Place the controller on a flat, static-free surface with the removable cover facing up.
- Remove the cover by pressing down on the button and sliding the cover off.

5. Remove the battery from the failed controller, and install it into the replacement controller:

a. Confirm that the green LED inside the controller (between the battery and the DIMMs) is off.

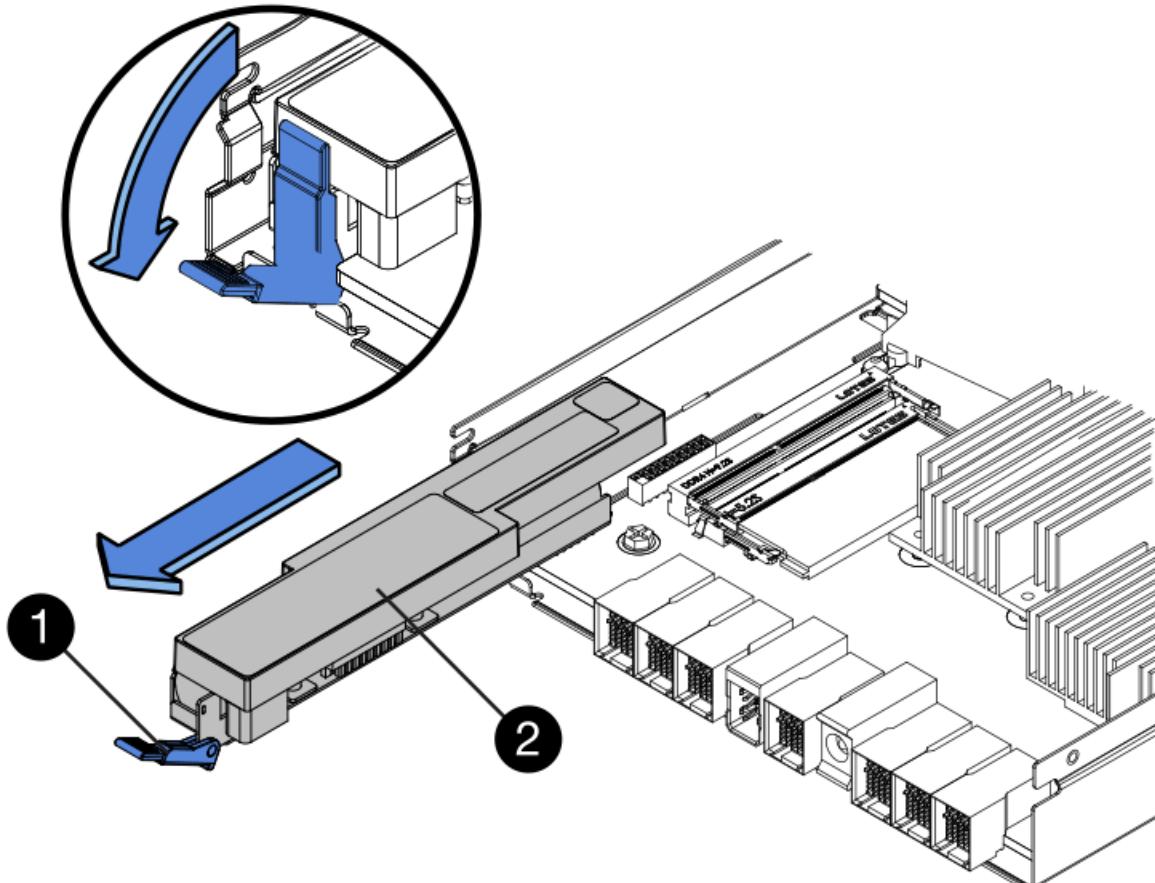
If this green LED is on, the controller is still using battery power. You must wait for this LED to go off before removing any components.



Item	Description
	Internal Cache Active LED

Item	Description
	Battery

- b. Locate the blue release latch for the battery.
- c. Unlatch the battery by pushing the release latch down and away from the controller.



Item	Description
	Battery release latch
	Battery

- d. Lift up on the battery, and slide it out of the controller.
- e. Remove the cover from the replacement controller.
- f. Orient the replacement controller so that the slot for the battery faces toward you.
- g. Insert the battery into the controller at a slight downward angle.

You must insert the metal flange at the front of the battery into the slot on the bottom of the controller, and slide the top of the battery beneath the small alignment pin on the left side of the controller.

- h. Move the battery latch up to secure the battery.

When the latch clicks into place, the bottom of the latch hooks into a metal slot on the chassis.

- i. Turn the controller over to confirm that the battery is installed correctly.



**Possible hardware damage**— The metal flange at the front of the battery must be completely inserted into the slot on the controller (as shown in the first figure). If the battery is not installed correctly (as shown in the second figure), the metal flange might contact the controller board, causing damage.

- **Correct**—The battery's metal flange is completely inserted in the slot on the controller:



- **Incorrect**—The battery's metal flange is not inserted into the slot on the controller:



- j. Replace the controller cover.

6. Install the replacement controller into the appliance.

- a. Turn the controller over, so that the removable cover faces down.

- b. With the cam handle in the open position, slide the controller all the way into the appliance.

- c. Move the cam handle to the left to lock the controller in place.
- d. Replace the cables and SFPs.
- e. If the original controller used DHCP for the IP address, locate the MAC address on the label on the back of the replacement controller. Ask your network administrator to associate the DNS/network and IP address for the controller you removed with the MAC address for the replacement controller.



If the original controller did not use DHCP for the IP address, the new controller will adopt the IP address of the controller you removed.

## 7. Bring the controller online using SANtricity System Manager:

- a. Select **Hardware**.
- b. If the graphic shows the drives, select **Show back of shelf**.
- c. Select the controller you want to place online.
- d. Select **Place Online** from the context menu, and confirm that you want to perform the operation.
- e. Verify that the seven-segment display shows a state of 99.

## 8. Confirm that the new controller is Optimal, and collect support data.

### Related information

[NetApp E-Series Systems Documentation Site](#)

## Replacing hardware components in the storage controller shelf

If a hardware problem occurs, you might need to replace a component in the storage controller shelf.

### What you'll need

- You have the E-Series hardware replacement procedure.
- You have physically located the storage appliance where you are replacing storage shelf hardware components in the data center.

### [Locating the controller in a data center](#)

### About this task

To replace the battery in the storage controller, see the instructions in these instructions for replacing a storage controller. Those instructions describe how to remove a controller from the appliance, remove the battery from the controller, install the battery, and replace the controller.

For instructions for the other field replaceable units (FRUs) in the controller shelves, access the E-Series procedures for system maintenance.

FRU	See instructions
Battery	StorageGRID (these instructions): Replacing a storage controller

FRU	See instructions
Drive	E-Series: <ul style="list-style-type: none"> <li>Replace drive (60-drive)</li> <li>Replace drive (12-drive or 24-drive)</li> </ul>
Power canister	E-Series <ul style="list-style-type: none"> <li>Replace power canister (60-drive)</li> <li>Replace power supply (12-drive or 24-drive)</li> </ul>
Fan canister (60-drive shelves only)	E-Series: Replace fan canister (60-drive)
Drive drawer (60-drive shelves only)	E-Series: Replace drive drawer (60-drive)

#### Related information

[NetApp E-Series Systems Documentation Site](#)

[Replacing a storage controller](#)

## Replacing hardware components in the optional 60-drive expansion shelf

You might need to replace an input/output module, a power supply, or a fan in the expansion shelf.

#### What you'll need

- You have the E-Series hardware replacement procedure.
- You have physically located the storage appliance where you are replacing expansion shelf hardware components in the data center.

[Locating the controller in a data center](#)

#### About this task

To replace an input/output module (IOM) in a 60-drive expansion shelf, see the instructions in these instructions for replacing a storage controller.

To replace a power supply or a fan in a 60-drive expansion shelf, access the E-Series procedures for maintaining 60-drive hardware.

FRU	See E-Series instructions for
Input/output module (IOM)	Replacing an IOM
Power canister	Replace power canister (60-drive)
Fan canister	Replace fan canister (60-drive)

## Shutting down the SG6000-CN controller

Shut down the SG6000-CN controller to perform hardware maintenance.

### What you'll need

- You have physically located the SG6000-CN controller requiring maintenance in the data center.

#### [Locating the controller in a data center](#)

- The appliance has been placed maintenance mode.

#### [Placing an appliance into maintenance mode](#)

### About this task

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before shutting down the controller or shut down the controller during a scheduled maintenance window when periods of service disruption are normally expected. See the information about determining node connection states in the instructions for managing objects with information lifecycle management.

 If you have ever used an ILM rule that creates only one copy of an object, you must shut down the controller during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure.

See information about managing objects with information lifecycle management.

### Steps

1. When the appliance has been placed maintenance mode, shut down the SG6000-CN controller:



You must perform a controlled shut down of the controller by entering the commands specified below. Shutting down the controller using the power switch will result in data loss.

- a. Log in to the grid node using PuTTY or another ssh client:

- i. Enter the following command: `ssh admin@grid_node_IP`
- ii. Enter the password listed in the `Passwords.txt` file.
- iii. Enter the following command to switch to root: `su -`
- iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

- b. Shut down the SG6000-CN controller:

**`shutdown -h now`**

This command might take up to 10 minutes to complete.

2. Use one of the following methods to verify that the SG6000-CN controller is powered off:

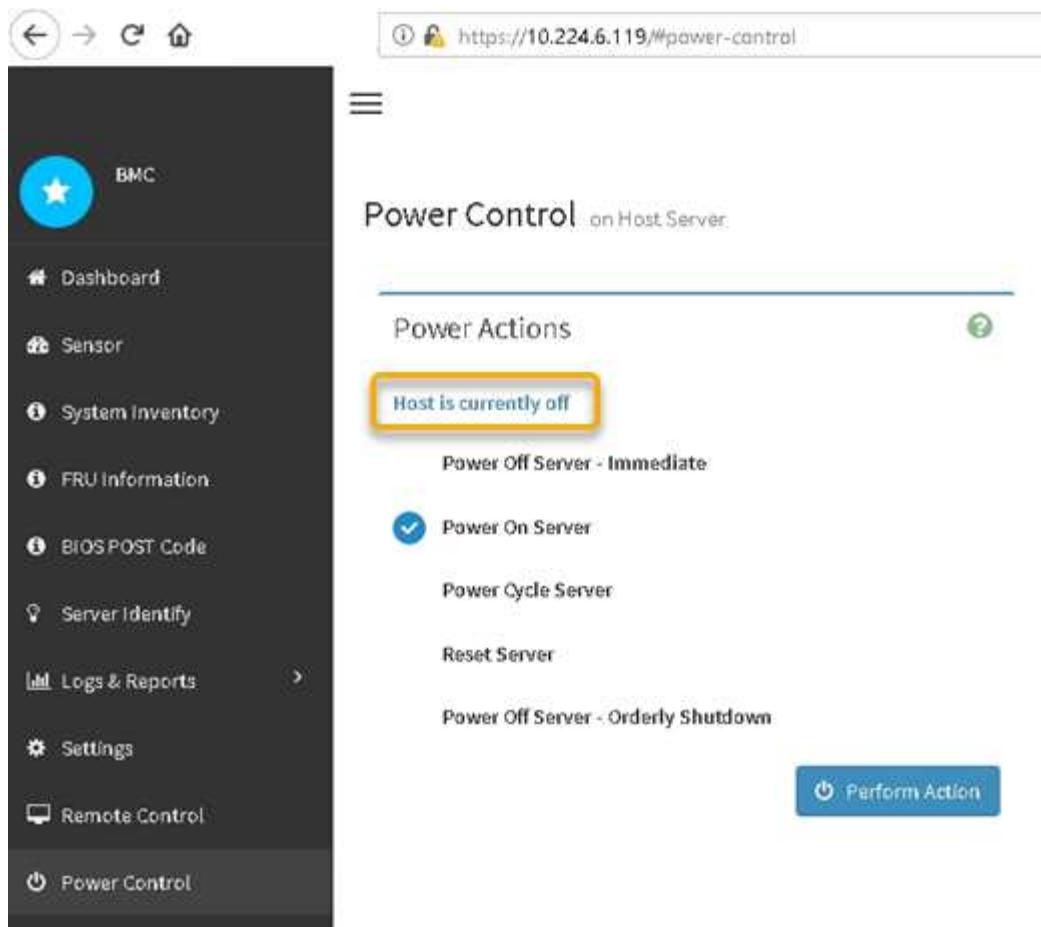
- Look at the blue power LED on the front of the controller and confirm that it is off.



- Look at the green LEDs on both power supplies in the rear of the controller and confirm that they blink at a regular rate (approximately one blink per second).



- Use the controller BMC interface:
  - i. Access the controller BMC interface.  
[Accessing the BMC interface](#)
  - ii. Select **Power Control**.
  - iii. Verify that the Power Actions indicates that the host is currently off.



#### Related information

[Removing the SG6000-CN controller from a cabinet or rack](#)

### Powering on the SG6000-CN controller and verifying operation

Power on the controller after completing maintenance.

#### What you'll need

- You have installed the controller in a cabinet or rack and connected the data and power cables.

[Reinstalling the SG6000-CN controller into a cabinet or rack](#)

- You have physically located the controller in the data center.

[Locating the controller in a data center](#)

#### Steps

1. Power on the SG6000-CN controller and monitor the controller LEDs and boot-up codes using one of the following methods:
  - Press the power switch on the front of the controller.



- Use the controller BMC interface:
  - i. Access the controller BMC interface.

#### Accessing the BMC interface

- ii. Select **Power Control**.
- iii. Select **Power On Server** and then select **Perform Action**.

A screenshot of the BMC interface. The top navigation bar shows a back arrow, forward arrow, refresh, and home icon, with the URL https://10.224.6.119/#power-control. The left sidebar has a 'BMC' icon and a list of options: Dashboard, Sensor, System Inventory, FRU Information, BIOS POST Code, Server Identify, Logs &amp; Reports, Settings, Remote Control, and Power Control (which is highlighted with a blue bar). The main content area is titled 'Power Control on Host Server'. It shows 'Power Actions' with a note 'Host is currently off'. Under 'Power Off Server - Immediate', the 'Power On Server' button is highlighted with a yellow box and a circled '1'. Under 'Power Off Server - Orderly Shutdown', the 'Perform Action' button is highlighted with a yellow box and a circled '2'.

Use the BMC interface to monitor start-up status.

2. Confirm that the appliance controller displays in the Grid Manager and with no alerts.

It might take up to 20 minutes for the controller to display in the Grid Manager.

3. Confirm that the new SG6000-CN controller is fully operational:

a. Log in to the grid node using PuTTY or another ssh client:

- i. Enter the following command: `ssh admin@grid_node_IP`
- ii. Enter the password listed in the `Passwords.txt` file.
- iii. Enter the following command to switch to root: `su -`
- iv. Enter the password listed in the `Passwords.txt` file.

When you are logged in as root, the prompt changes from `$` to `#`.

b. Enter the following command and verify that it returns the expected output:

```
cat /sys/class/fc_host/*/port_state
```

Expected output:

```
Online  
Online  
Online
```

If the expected output is not returned, contact technical support.

c. Enter the following command and verify that it returns the expected output:

```
cat /sys/class/fc_host/*/speed
```

Expected output:

```
16 Gbit  
16 Gbit  
16 Gbit16 Gbit  
16 Gbit
```

If the expected output is not returned, contact technical support.

d. From the Nodes page in Grid Manager, make sure that the appliance node is connected to the grid and does not have any alerts.



Do not take another appliance node offline unless this appliance has a green icon.

4. Optional: Install the front bezel, if one was removed.

#### Related information

[Viewing status indicators and buttons on the SG6000-CN controller](#)

[Viewing boot-up status codes for the SG6000 storage controllers](#)

## Replacing the SG6000-CN controller

You might need to replace the SG6000-CN controller if it is not functioning optimally or if it has failed.

### What you'll need

- You have a replacement controller with the same part number as the controller you are replacing.
- You have labels to identify each cable that is connected to the controller.
- You have physically located the controller to replace in the data center.

### [Locating the controller in a data center](#)

### About this task

The appliance Storage Node will not be accessible when you replace the SG6000-CN controller. If the SG6000-CN controller is functioning sufficiently, you can perform a controlled shutdown at the start of this procedure.

If you are replacing the controller before installing StorageGRID software, you might not be able to access the StorageGRID Appliance Installer immediately after completing this procedure.



While you can access the StorageGRID Appliance Installer from other hosts on the same subnet as the appliance, you cannot access it from hosts on other subnets. This condition should resolve itself within 15 minutes (when any ARP cache entries for the original controller time out), or you can clear the condition immediately by purging any old ARP cache entries manually from the local router or gateway.

### Steps

1. If the SG6000-CN controller is functioning sufficiently to allow for a controlled shutdown, shut down the SG6000-CN controller.

### [Shutting down the SG6000-CN controller](#)

The green Cache Active LED on the back of the E2800 controller is on when cached data needs to be written to the drives. You must wait for this LED to turn off.

2. Use one of two methods to verify that the power for the SG6000-CN controller is off:
  - The power indicator LED on the front of the controller is off.
  - The Power Control page of the BMC interface indicates that the controller is off.
3. If the StorageGRID networks attached to the controller use DHCP servers, update DNS/network and IP address settings.
  - a. Locate the MAC address label on the front of the SG6000-CN controller, and determine the MAC address for the Admin Network port.



The MAC address label lists the MAC address for the BMC management port. To determine the MAC address for the Admin Network port, you must add **2** to the hexadecimal number on the label. For example, if the MAC address on the label ends in **09**, the MAC address for the Admin Port would end in **0B**. If the MAC address on the label ends in **(y)FF**, the MAC address for the Admin Port would end in **(y+1)01**. You can easily make this calculation by opening Calculator in Windows, setting it to Programmer mode, selecting Hex, typing the MAC address, then typing **+ 2 =**.

b. Ask your network administrator to associate the DNS/network and IP address for the controller you removed with the MAC address for the replacement controller.



You must ensure that all IP addresses for the original controller have been updated before you apply power to the replacement controller. Otherwise, the controller will obtain new DHCP IP addresses when it boots up and might not be able to reconnect to StorageGRID. This step applies to all StorageGRID networks that are attached to the controller.



If the original controller used static IP address, the new controller will automatically adopt the IP addresses of the controller you removed.

4. Remove and replace the SG6000-CN controller:

a. Label the cables and then disconnect the cables and any SFP+ or SFP28 transceivers.



To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

b. Remove the failed controller from the cabinet or rack.  
c. Install the replacement controller into the cabinet or rack.  
d. Replace the cables and any SFP+ or SFP28 transceivers.  
e. Power on the controller and monitor the controller LEDs and boot-up codes.

5. Confirm that the appliance Storage Node appears in the Grid Manager and that no alarms appear.

6. From the Grid Manager, select **Nodes**, and verify that the BMC IP address for the node controller is correct.

If the node controller IP address is not valid or is not in the expected range, reconfigure the IP address as described in the recovery and maintenance instructions.

#### [Maintain & recover](#)

#### **Related information**

[SG6000-CN: Installing into a cabinet or rack](#)

[Viewing status indicators and buttons on the SG6000-CN controller](#)

[Viewing boot-up codes for the SG6000-CN controller](#)

### **Replacing a power supply in the SG6000-CN controller**

The SG6000-CN controller has two power supplies for redundancy. If one of the power supplies fails, you must replace it as soon as possible to ensure that the compute controller has redundant power.

#### **What you'll need**

- You have unpacked the replacement power supply unit.
- You have physically located the controller where you are replacing the power supply in the data center.

[Locating the controller in a data center](#)

- You have confirmed that the other power supply is installed and running.

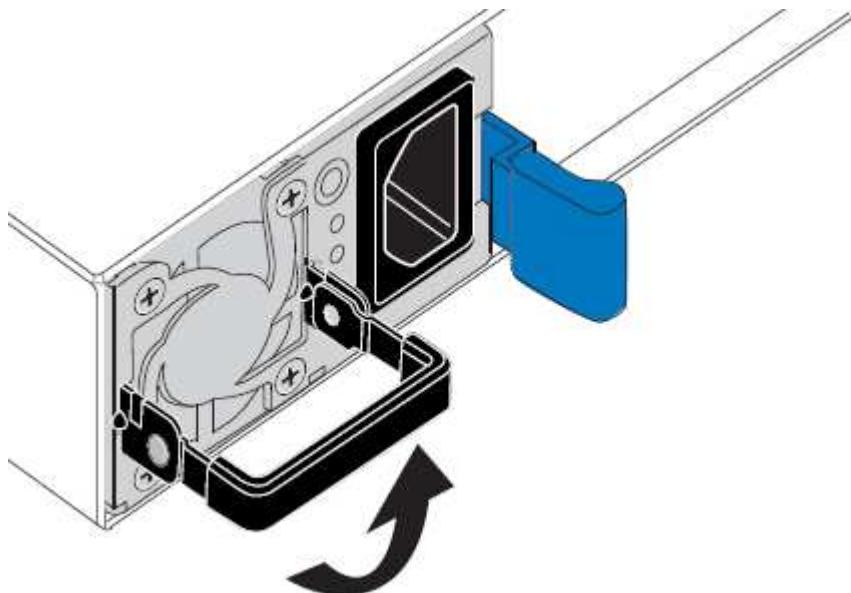
## About this task

The figure shows the two power supply units for the SG6000-CN controller, which are accessible from the back of the controller.

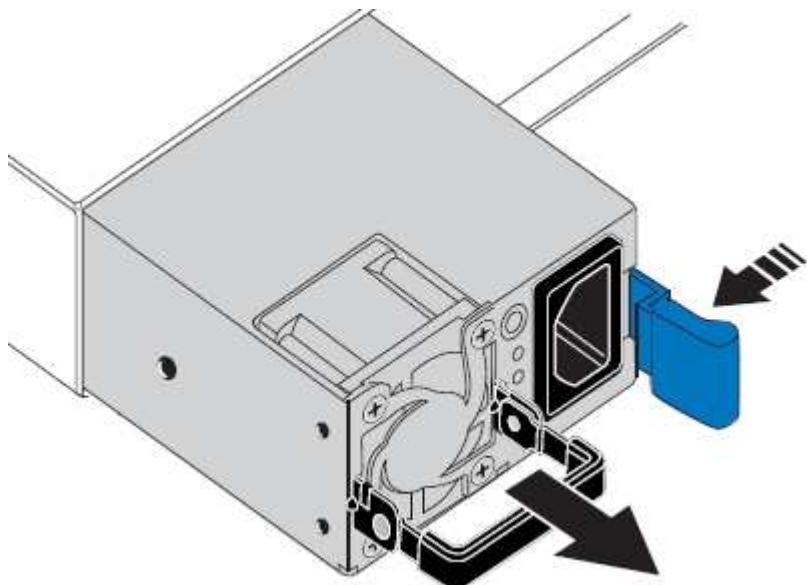


## Steps

1. Unplug the power cord from the power supply.
2. Lift the cam handle.

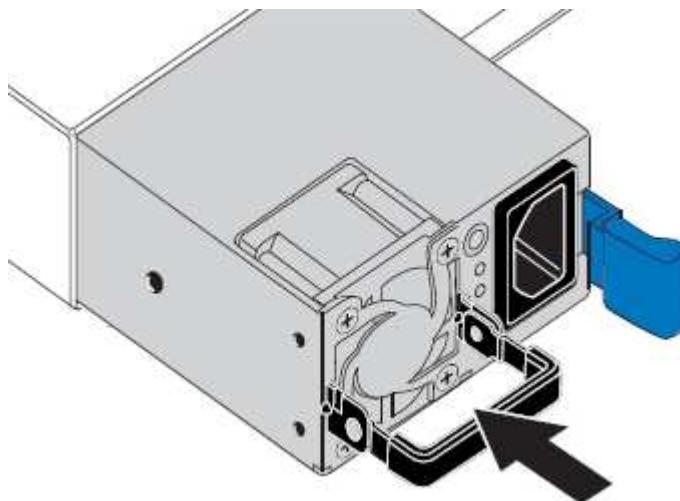


3. Press the blue latch and pull the power supply out.



4. Slide the replacement power supply into the chassis.

Ensure that the blue latch is on the right side when you slide the unit in.



5. Push the cam handle down to secure the power supply.

6. Attach the power cord to the power supply, and ensure that the green LED comes on.

## Removing the SG6000-CN controller from a cabinet or rack

Remove the SG6000-CN controller from a cabinet or rack to access the top cover or to move the controller to a different location.

### What you'll need

- You have labels to identify each cable that is connected to the SG6000-CN controller.
- You have physically located the SG6000-CN controller where you are performing maintenance in the data center.

#### Locating the controller in a data center

- You have shut down the SG6000-CN controller.

#### Shutting down the SG6000-CN controller



Do not shut down the controller using the power switch.

### Steps

1. Label and then disconnect the controller power cables.
2. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
3. Label and then disconnect the controller data cables and any SFP+ or SFP28 transceivers.



To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

4. Loosen the two captive screws on the controller front panel.



5. Slide the SG6000-CN controller forward out of the rack until the mounting rails are fully extended and you hear the latches on both sides click.

The controller top cover is accessible.

6. Optional: If you are fully removing the controller from the cabinet or rack, follow the instructions for the rail kit to remove the controller from the rails.

#### Related information

[Removing the SG6000-CN controller cover](#)

## Reinstalling the SG6000-CN controller into a cabinet or rack

Reinstall the controller into a cabinet or rack when hardware maintenance is complete.

#### What you'll need

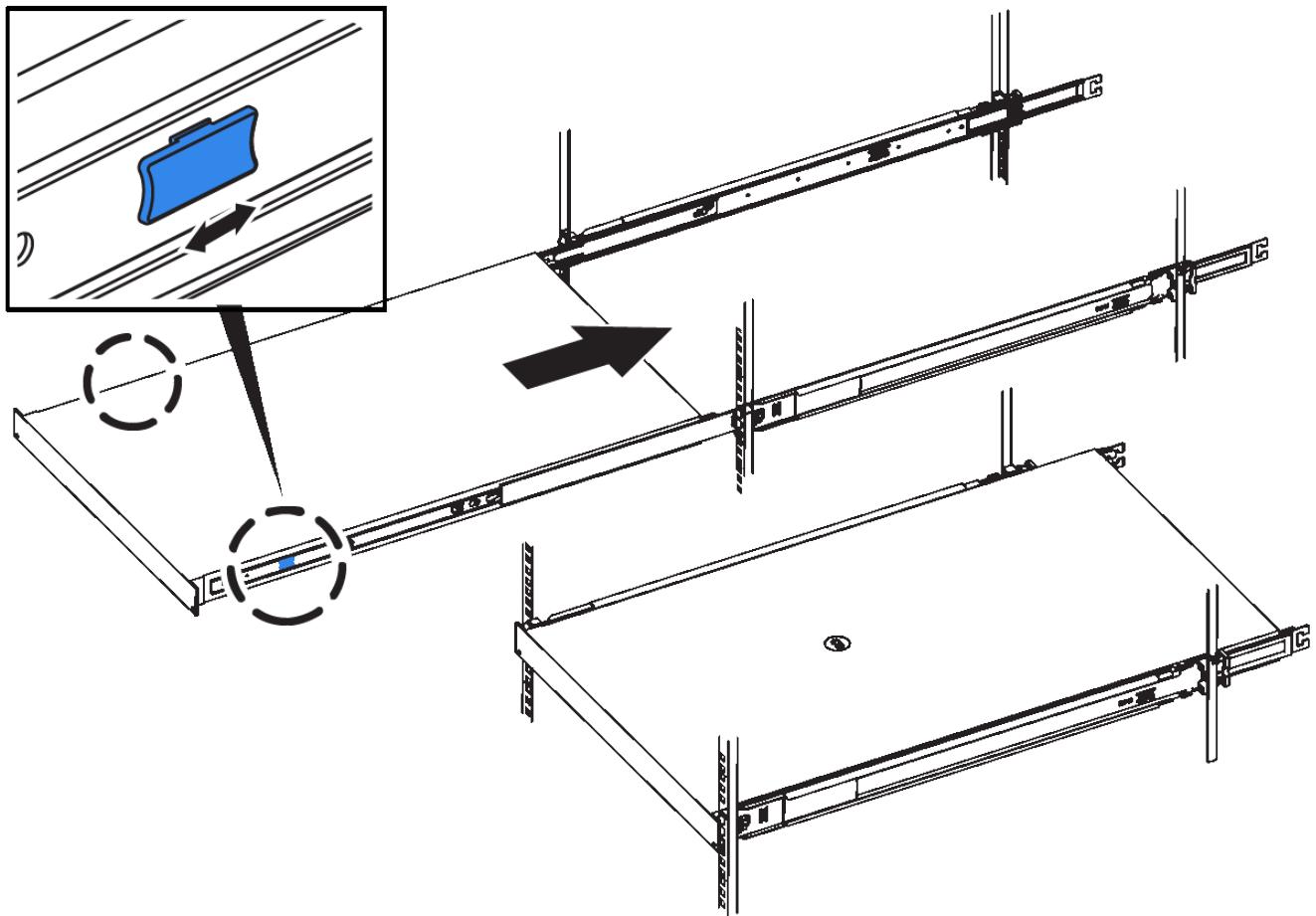
You have reinstalled the controller cover.

[Reinstalling the SG6000-CN controller cover](#)

#### Steps

1. Press the blue rail releases both rack rails at the same time and slide the SG6000-CN controller into the rack until it is fully seated.

When you cannot move the controller any further, pull the blue latches on both sides of the chassis to slide the controller all the way in.



Do not attach the front bezel until after you power on the controller.

2. Tighten the captive screws on the controller front panel to secure the controller in the rack.



3. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
4. Reconnect the controller data cables and any SFP+ or SFP28 transceivers.



To prevent degraded performance, do not twist, fold, pinch, or step on the cables.

#### [Cabling the appliance \(SG6000\)](#)

5. Reconnect the controller power cables.

#### [Connecting power cords and applying power \(SG6000\)](#)

#### **After you finish**

The controller can be restarted.

#### [Powering on the SG6000-CN controller and verifying operation](#)

## Removing the SG6000-CN controller cover

Remove the controller cover to access internal components for maintenance.

### What you'll need

Remove the controller from the cabinet or rack to access the top cover.

### Removing the SG6000-CN controller from a cabinet or rack

#### Steps

1. Make sure that the SG6000-CN controller cover latch is not locked. If necessary, turn the blue plastic latch lock one-quarter turn in the unlock direction, as shown on the latch lock.
2. Rotate the latch up and back toward the rear of the SG6000-CN controller chassis until it stops; then, carefully lift the cover from the chassis and set it aside.



Wrap the strap end of an ESD wristband around your wrist and secure the clip end to a metal ground to prevent static discharge when working inside the SG6000-CN controller.

#### Related information

##### [Removing the Fibre Channel HBA](#)

## Reinstalling the SG6000-CN controller cover

Reinstall the controller cover when internal hardware maintenance is complete.

### What you'll need

You have completed all maintenance procedures inside the controller.

#### Steps

1. With the cover latch open, hold the cover above the chassis and align the hole in the top cover latch with the pin in the chassis. When the cover is aligned, lower it onto the chassis.



2. Rotate the cover latch forward and down until it stops and the cover fully seats into the chassis. Verify that there are no gaps along the front edge of the cover.

If the cover is not fully seated, you might not be able to slide the SG6000-CN controller into the rack.

3. Optional: Turn the blue plastic latch lock one-quarter turn in the lock direction, as shown on the latch lock, to lock it.

#### After you finish

Reinstall the controller in the cabinet or rack.

### [Reinstalling the SG6000-CN controller into a cabinet or rack](#)

## Replacing the Fibre Channel HBA in the SG6000-CN controller

You might need to replace the Fibre Channel host bus adapter (HBA) in the SG6000-CN controller if it is not functioning optimally or if it has failed.

#### Verifying the Fibre Channel HBA to replace

If you are unsure which Fibre Channel host bus adapter (HBA) to replace, complete this procedure to identify it.

#### What you'll need

- You have the serial number of the storage appliance or SG6000-CN controller where the Fibre Channel HBA needs to be replaced.



If the serial number of the storage appliance containing the Fibre Channel HBA you are replacing starts with the letter Q, it will not be listed in the Grid Manager. You must check the tags attached to the front of each SG6000-CN controller in the data center until you find a match.

- You must be signed in to the Grid Manager using a supported browser.

#### Steps

1. From the Grid Manager, select **Nodes**.
2. From the tree view of the Nodes page, select an appliance Storage Node.
3. Select the **Hardware** tab.

Check the Storage Appliance Chassis Serial Number and the Compute Controller Serial Number in the StorageGRID Appliance section to see if one of these serial numbers matches the serial number of the storage appliance where you are replacing the Fibre Channel HBA. If either serial number matches, you have found the correct appliance.

Storage Appliance Chassis Serial Number	721005600100
Appliance Model	SG6060
Storage Controller Name	StorageGRID-xcb-3-228-sn
Storage Controller A Management IP	10.224.9.230
Storage Controller B Management IP	10.224.9.234
Storage Controller WWID	600009800001c25000000000544a0003
Storage Appliance Chassis Serial Number	721005600100
Storage Hardware	Nominal
Storage Controller Failed Drive Count	0
Storage Controller A	Nominal
Storage Controller B	Nominal
Storage Controller Power Supply A	Nominal
Storage Controller Power Supply B	Nominal
Storage Data Drive Type	NL-SAS HDD
Storage Data Drive Size	8.00 TB
Storage RAID Mode	DOP
Storage Connectivity	Nominal
Overall Power Supply	Nominal
Compute Controller BMC IP	10.224.9.109
Compute Controller Serial Number	721005600009
Compute Hardware	Nominal
Compute Controller CPU Temperature	Nominal
Compute Controller Chassis Temperature	Nominal

- If the StorageGRID Appliance section does not display, the node selected is not a StorageGRID appliance. Select a different node from the tree view.
- If the Appliance Model is not SG6060, select a different node from the tree view.
- If the serial numbers do not match, select a different node from the tree view.

4. After you locate the node where the Fibre Channel HBA needs to be replaced, write down the Compute Controller BMC IP address listed the StorageGRID Appliance section.

You can use this IP address to turn on the compute controller identify LED, to help you locate the appliance in the data center.

#### Turning the controller identify LED on and off

#### Related information

##### [Removing the Fibre Channel HBA](#)

#### Removing the Fibre Channel HBA

You might need to replace the Fibre Channel host bus adapter (HBA) in the SG6000-CN controller if it is not functioning optimally or if it has failed.

#### What you'll need

- You have the correct replacement Fibre Channel HBA.

- You have determined which SG6000-CN controller contains the Fibre Channel HBA to replace.

#### [Verifying the Fibre Channel HBA to replace](#)

- You have physically located the SG6000-CN controller where you are replacing the Fibre Channel HBA in the data center.

#### [Locating the controller in a data center](#)

- You have removed the controller cover.

#### [Removing the SG6000-CN controller cover](#)

### **About this task**

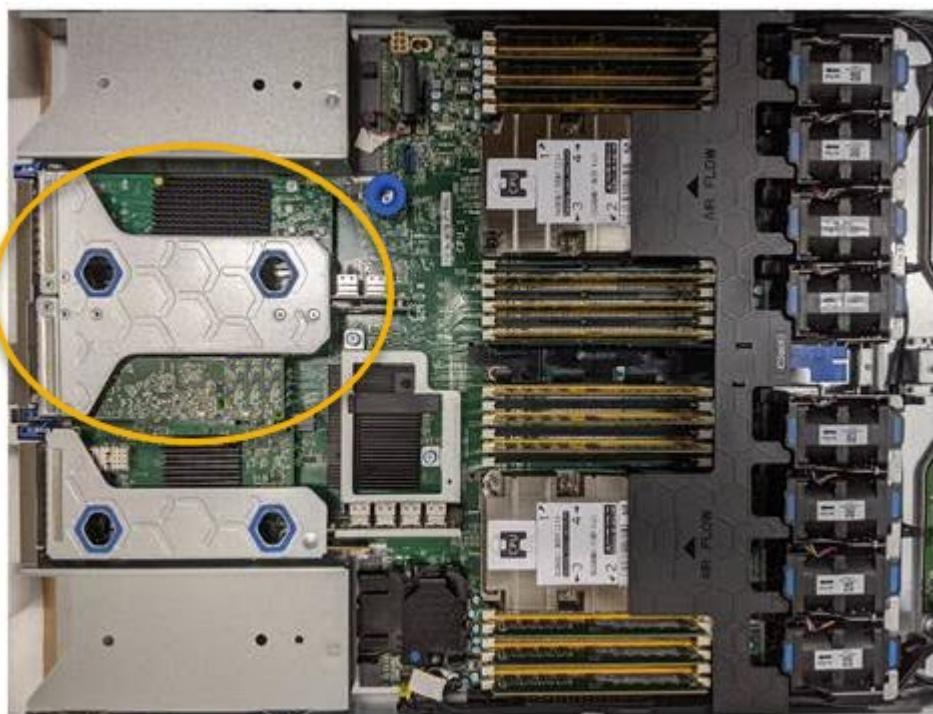
To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before starting the Fibre Channel HBA replacement or replace the adapter during a scheduled maintenance window when periods of service disruption are normally expected. See the information about determining node connection states in the instructions for managing objects with information lifecycle management.

**i** If you have ever used an ILM rule that creates only one copy of an object, you must replace the Fibre Channel HBA during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure.

See information about managing objects with information lifecycle management.

### **Steps**

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Locate the riser assembly at the rear of the controller that contains the Fibre Channel HBA.



3. Grasp the riser assembly through the blue-marked holes and carefully lift it upwards. Move the riser assembly toward the front of the chassis as you lift it to allow the external connectors in its installed

adapters to clear the chassis.

4. Place the riser card on a flat anti-static surface with the metal frame side down to access the adapters.



There are two adapters in the riser assembly: a Fibre Channel HBA and an Ethernet network adapter. The Fibre Channel HBA is indicated in the illustration.

5. Open the blue adapter latch (circled) and carefully remove the Fibre Channel HBA from the riser assembly. Rock the adapter slightly to help remove the adapter from its connector. Do not use excessive force.
6. Place the adapter on a flat anti-static surface.

#### After you finish

Install the replacement Fibre Channel HBA.

#### [Reinstalling the Fibre Channel HBA](#)

#### Related information

[Reinstalling the Fibre Channel HBA](#)

[Administer StorageGRID](#)

[Monitor & troubleshoot](#)

[Manage objects with ILM](#)

#### **Reinstalling the Fibre Channel HBA**

The replacement Fibre Channel HBA is installed into the same location as the one that was removed.

#### What you'll need

- You have the correct replacement Fibre Channel HBA.
- You have removed the existing Fibre Channel HBA.

#### [Removing the Fibre Channel HBA](#)

#### Steps

1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.

2. Remove the replacement Fibre Channel HBA from its packaging.
3. With the blue adapter latch in the open position, align the Fibre Channel HBA with its connector on the riser assembly; then, carefully press the adapter into the connector until it is fully seated.



There are two adapters in the riser assembly: a Fibre Channel HBA and an Ethernet network adapter. The Fibre Channel HBA is indicated in the illustration.

4. Locate the alignment hole on the riser assembly (circled) that aligns with a guide pin on the system board to ensure correct riser assembly positioning.



5. Position the riser assembly in the chassis, making sure that it aligns with the connector and guide pin on the system board; then, insert the riser assembly.
6. Carefully press the riser assembly in place along its center line, next to the blue-marked holes, until it is fully seated.
7. Remove the protective caps from the Fibre Channel HBA ports where you will be reinstalling cables.

#### **After you finish**

If you have no other maintenance procedures to perform in the controller, reinstall the controller cover.

#### [Reinstalling the SG6000-CN controller cover](#)

### **Changing the link configuration of the SG6000-CN controller**

You can change the Ethernet link configuration of the SG6000-CN controller. You can change the port bond mode, the network bond mode, and the link speed.

## What you'll need

The appliance has been placed maintenance mode.

### Placing an appliance into maintenance mode

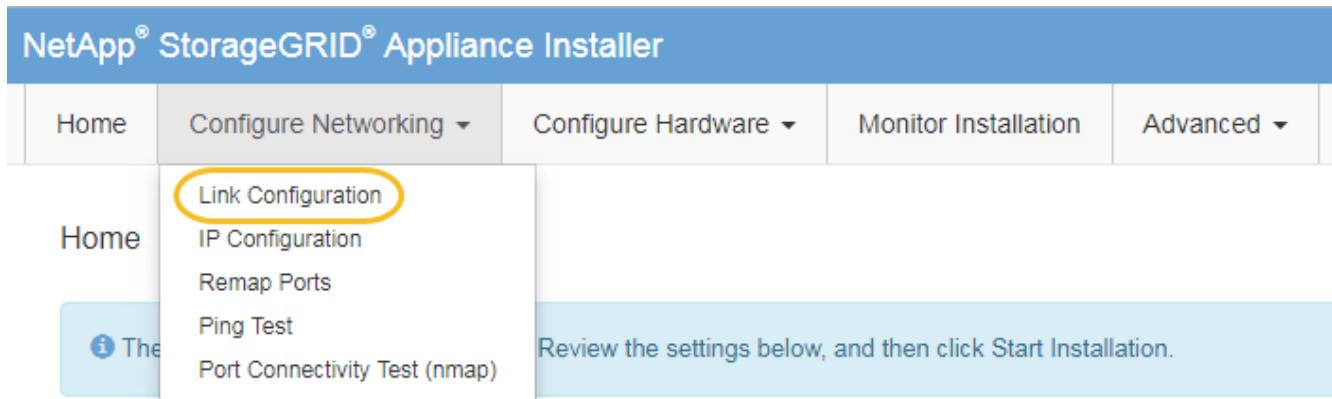
#### About this task

Options for changing the Ethernet link configuration of the SG6000-CN controller include:

- Changing **Port bond mode** from Fixed to Aggregate, or from Aggregate to Fixed
- Changing **Network bond mode** from Active-Backup to LACP, or from LACP to Active-Backup
- Enabling or disabling VLAN tagging, or changing the value of a VLAN tag
- Changing the link speed.

#### Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking > Link Configuration**.



2. Make the desired changes to the link configuration.

For more information on the options, see [Configuring network links \(SG6000\)](#).

3. When you are satisfied with your selections, click **Save**.



You might lose your connection if you made changes to the network or link you are connected through. If you are not reconnected within 1 minute, re-enter the URL for the StorageGRID Appliance Installer using one of the other IP addresses assigned to the appliance:

**[https://Appliance\\_Controller\\_IP:8443](https://Appliance_Controller_IP:8443)**

If you made changes to the VLAN settings, the subnet for the appliance might have changed. If you need to change the IP addresses for the appliance, follow the instructions for configuring IP addresses.

### Configuring StorageGRID IP addresses

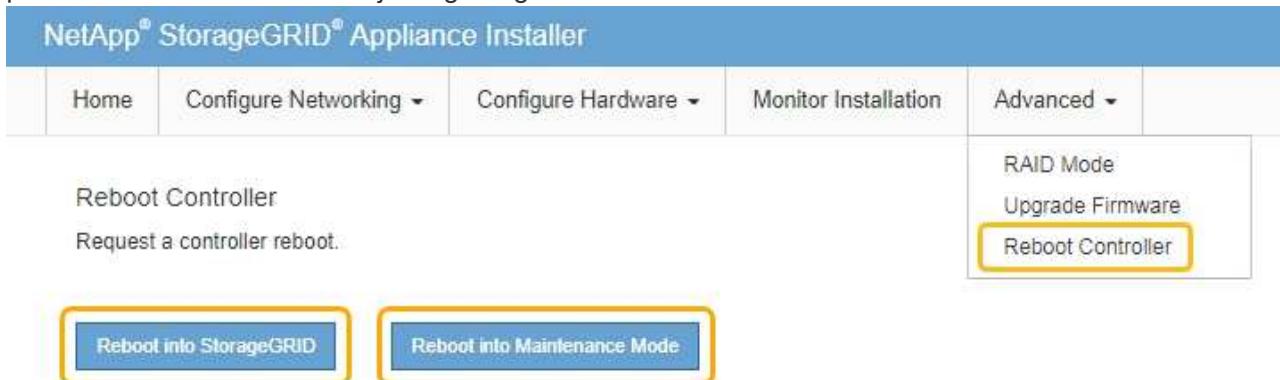
4. Select **Configure Networking > Ping Test** from the menu.
5. Use the Ping Test tool to check connectivity to IP addresses on any networks that might have been affected by the link configuration changes you made in the [link configuration changes](#) step.

In addition to any other tests you choose to perform, confirm that you can ping the Grid Network IP address

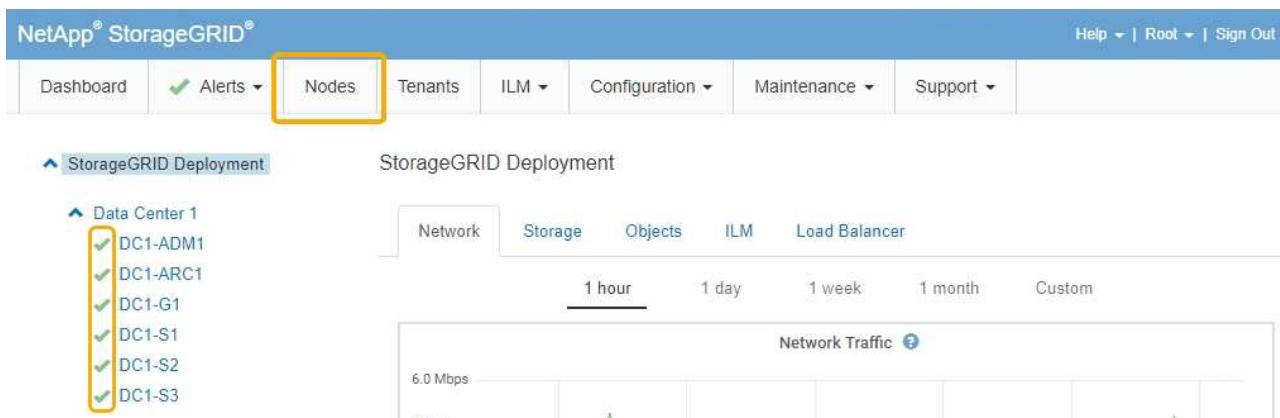
of the primary Admin Node, and the Grid Network IP address of at least one other Storage Node. If necessary, return to the [link configuration changes](#) step and correct any link configuration issues.

6. When you are satisfied that your link configuration changes are working, reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:

- Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
- Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **Nodes** tab should display a normal status  for the appliance node, indicating that no alerts are active and the node is connected to the grid.



## Changing the MTU setting

You can change the MTU setting that you assigned when you configured IP addresses for the appliance node.

### What you'll need

The appliance has been placed maintenance mode.

## Placing an appliance into maintenance mode

### Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking > IP Configuration**.
2. Make the desired changes to the MTU settings for the Grid Network, Admin Network, and Client Network.

#### Grid Network

The Grid Network is used for all internal StorageGRID traffic. The Grid Network provides connectivity between all nodes in the grid, across all sites and subnets. All hosts on the Grid Network must be able to talk to all other hosts. The Grid Network can consist of multiple subnets. Networks containing critical grid services, such as NTP, can also be added as Grid subnets.

IP  Static  DHCP

Assignment

IPv4 Address (CIDR)

Gateway

**⚠** All required Grid Network subnets must also be defined in the Grid Network Subnet List on the Primary Admin Node before starting installation.

Subnets (CIDR)	<input type="text" value="172.18.0.0/21"/> <span style="color: red;">×</span>
	<input type="text" value="172.18.0.0/21"/> <span style="color: red;">×</span>
	<input type="text" value="192.168.0.0/21"/> <span style="color: green;">+ ×</span>
MTU	<input type="text" value="1500"/> <span style="border: 1px solid black; padding: 2px;">▼</span>
	<span style="background-color: #668d4c; color: white; padding: 5px 10px; border-radius: 5px;">Cancel</span>
	<span style="background-color: #337ab7; color: white; padding: 5px 10px; border-radius: 5px; border: 1px solid #337ab7;">Save</span>



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.

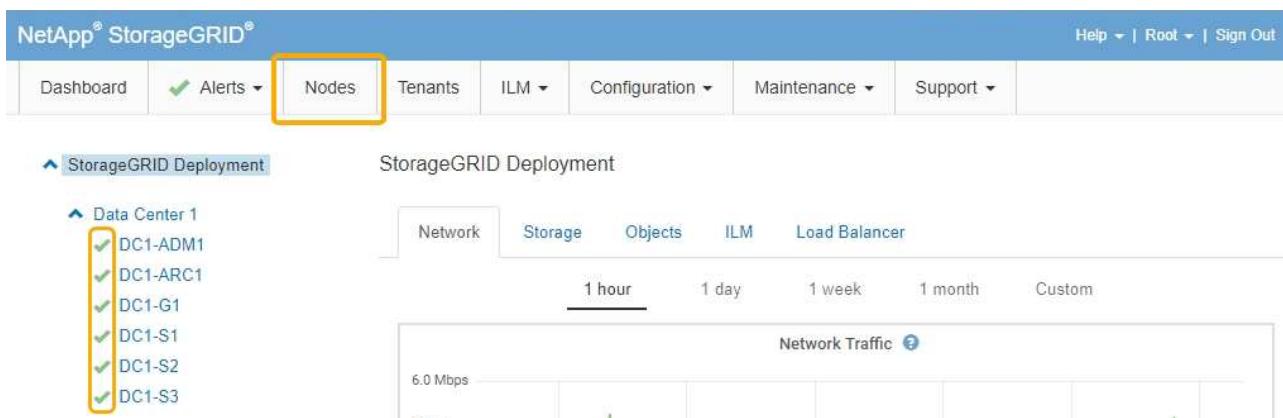


For the best network performance, all nodes should be configured with similar MTU values on their Grid Network interfaces. The **Grid Network MTU mismatch** alert is triggered if there is a significant difference in MTU settings for the Grid Network on individual nodes. The MTU values do not have to be the same for all network types.

3. When you are satisfied with the settings, select **Save**.
4. Reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:
  - Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
  - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **Nodes** tab should display a normal status for the appliance node, indicating that no alerts are active and the node is connected to the grid.



## Related information

[Administer StorageGRID](#)

## Checking the DNS server configuration

You can check and temporarily change the domain name system (DNS) servers that are currently in use by this appliance node.

### What you'll need

The appliance has been placed maintenance mode.

#### [Placing an appliance into maintenance mode](#)

### About this task

You might need to change the DNS server settings if an encrypted appliance cannot connect to the key management server (KMS) or KMS cluster because the hostname for the KMS was specified as a domain name instead of an IP address. Any changes that you make to the DNS settings for the appliance are temporary and are lost when you exit maintenance mode. To make these changes permanent, specify the DNS servers in Grid Manager (**Maintenance > Network > DNS Servers**).

- Temporary changes to the DNS configuration are necessary only for node-encrypted appliances where the KMS server is defined using a fully qualified domain name, instead of an IP address, for the hostname.
- When a node-encrypted appliance connects to a KMS using a domain name, it must connect to one of the DNS servers defined for the grid. One of these DNS servers then translates the domain name into an IP address.
- If the node cannot reach a DNS server for the grid, or if you changed the grid-wide DNS settings when a node-encrypted appliance node was offline, the node is unable to connect to the KMS. Encrypted data on the appliance cannot be decrypted until the DNS issue is resolved.

To resolve a DNS issue preventing KMS connection, specify the IP address of one or more DNS servers in the StorageGRID Appliance Installer. These temporary DNS settings allow the appliance to connect to the KMS and decrypt data on the node.

For example, if the DNS server for the grid changes while an encrypted node was offline, the node will not be able to reach the KMS when it comes back online, since it is still using the previous DNS values. Entering the new DNS server IP address in the StorageGRID Appliance Installer allows a temporary KMS connection to decrypt the node data.

### Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking > DNS Configuration**.
2. Verify that the DNS servers specified are correct.

## DNS Servers

⚠ Configuration changes made on this page will not be passed to the StorageGRID software after appliance installation.

Servers	
Server 1	10.224.223.135
Server 2	10.224.223.136

**Cancel** **Save**

3. If required, change the DNS servers.



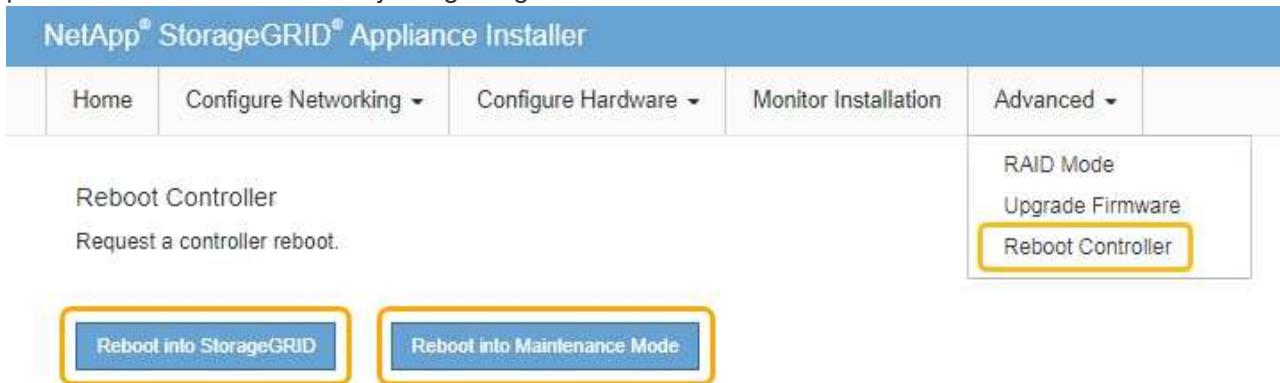
Changes made to the DNS settings are temporary and are lost when you exit maintenance mode.

4. When you are satisfied with the temporary DNS settings, select **Save**.

The node uses the DNS server settings specified on this page to reconnect to the KMS, allowing data on the node to be decrypted.

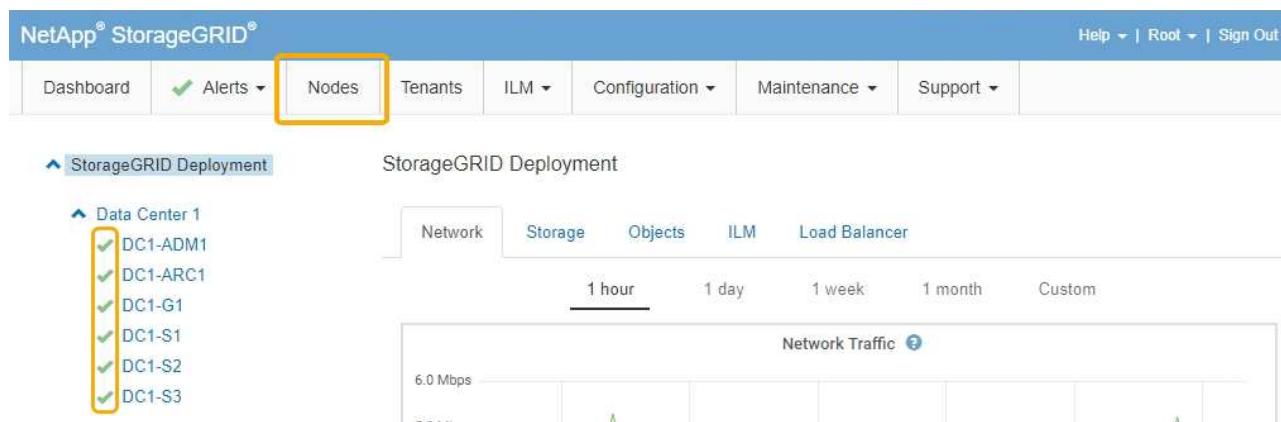
5. After node data is decrypted, reboot the node. From the StorageGRID Appliance Installer, select **Advanced > Reboot Controller**, and then select one of these options:

- Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
- Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



When the node reboots and rejoins the grid, it uses the system-wide DNS servers listed in the Grid Manager. After rejoining the grid, the appliance will no longer use the temporary DNS servers specified in the StorageGRID Appliance Installer while the appliance was in maintenance mode.

It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **Nodes** tab should display a normal status  for the appliance node, indicating that no alerts are active and the node is connected to the grid.



## Monitoring node encryption in maintenance mode

If you enabled node encryption for the appliance during installation, you can monitor the node-encryption status of each appliance node, including the node-encryption state and key management server (KMS) details.

### What you'll need

- Node encryption must have been enabled for the appliance during installation. You cannot enable node encryption after the appliance is installed.
- The appliance has been placed into maintenance mode.

#### [Placing an appliance into maintenance mode](#)

### Steps

1. From the StorageGRID Appliance Installer, select **Configure Hardware > Node Encryption**.

## Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

### Encryption Status

**⚠** You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption

**Save**

### Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name	thales
External key UID	41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57
Hostnames	10.96.99.164 10.96.99.165
Port	5696

**Server certificate** 

**Client certificate** 

### Clear KMS Key

**⚠** Do not clear the KMS key if you need to access or preserve any data on this appliance.

If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

**Clear KMS Key and Delete Data**

The Node Encryption page includes these three sections:

- Encryption Status shows whether node encryption is enabled or disabled for the appliance.
- Key Management Server Details shows information about the KMS being used to encrypt the appliance. You can expand the server and client certificate sections to view certificate details and status.
  - To address issues with the certificates themselves, such as renewing expired certificates, see the information about KMS in the instructions for administering StorageGRID.
  - If there are unexpected problems connecting to KMS hosts, verify that the domain name system (DNS) servers are correct and that appliance networking is correctly configured.

#### Checking the DNS server configuration

- If you are unable to resolve your certificate issues, contact technical support.
- Clear KMS Key disables node encryption for the appliance, removes the association between the appliance and the key management server that was configured for the StorageGRID site, and deletes

all data from the appliance. You must clear the KMS key before you can install the appliance into another StorageGRID system.

#### [Clearing the key management server configuration](#)



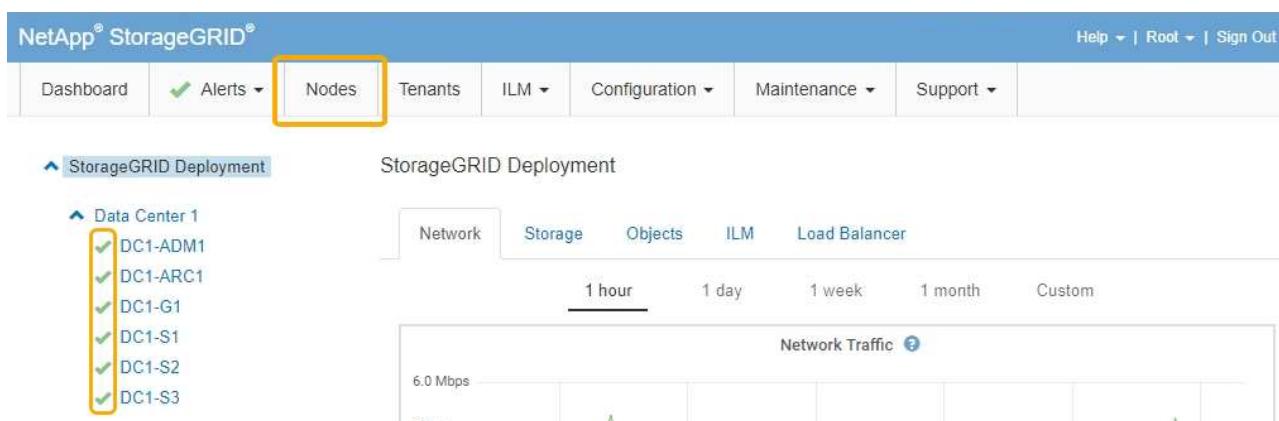
Clearing the KMS configuration deletes data from the appliance, rendering it permanently inaccessible. This data is not recoverable.

2. When you are done checking node-encryption status, reboot the node. From the StorageGRID Appliance Installer, select **Advanced** > **Reboot Controller**, and then select one of these options:

- Select **Reboot into StorageGRID** to reboot the controller with the node rejoining the grid. Select this option if you are done working in maintenance mode and are ready to return the node to normal operation.
- Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if there are additional maintenance operations you need to perform on the node before rejoining the grid.



It can take up to 20 minutes for the appliance to reboot and rejoin the grid. To confirm that the reboot is complete and that the node has rejoined the grid, go back to the Grid Manager. The **Nodes** tab should display a normal status for the appliance node, indicating that no alerts are active and the node is connected to the grid.



#### **Related information**

[Administer StorageGRID](#)

## Clearing the key management server configuration

Clearing the key management server (KMS) configuration disables node encryption on your appliance. After clearing the KMS configuration, the data on your appliance is permanently deleted and is no longer accessible. This data is not recoverable.

### What you'll need

If you need to preserve data on the appliance, you must perform a node decommission procedure before you clear the KMS configuration.



When KMS is cleared, data on the appliance will be permanently deleted and no longer accessible. This data is not recoverable.

Decommission the node to move any data it contains to other nodes in StorageGRID. See the recovery and maintenance instructions for grid node decommissioning.

### About this task

Clearing the appliance KMS configuration disables node encryption, removing the association between the appliance node and the KMS configuration for the StorageGRID site. Data on the appliance is then deleted and the appliance is left in a pre-install state. This process cannot be reversed.

You must clear the KMS configuration:

- Before you can install the appliance into another StorageGRID system, that does not use a KMS or that uses a different KMS.



Do not clear the KMS configuration if you plan to reinstall an appliance node in a StorageGRID system that uses the same KMS key.

- Before you can recover and reinstall a node where the KMS configuration was lost and the KMS key is not recoverable.
- Before returning any appliance that was previously in use at your site.
- After decommissioning a appliance that had node encryption enabled.



Decommission the appliance before clearing KMS to move its data to other nodes in your StorageGRID system. Clearing KMS before decommissioning the appliance will result in data loss and might render the appliance inoperable.

### Steps

1. Open a browser, and enter one of the IP addresses for the appliance's compute controller.

**[https://Controller\\_IP:8443](https://Controller_IP:8443)**

*Controller\_IP* is the IP address of the compute controller (not the storage controller) on any of the three StorageGRID networks.

The StorageGRID Appliance Installer Home page appears.

2. Select **Configure Hardware > Node Encryption**.

## Node Encryption

Node encryption allows you to use an external key management server (KMS) to encrypt all StorageGRID data on this appliance. If node encryption is enabled for the appliance and a KMS is configured for the site, you cannot access any data on the appliance unless the appliance can communicate with the KMS.

### Encryption Status

**⚠** You can only enable node encryption for an appliance during installation. You cannot enable or disable the node encryption setting after the appliance is installed.

Enable node encryption

**Save**

### Key Management Server Details

View the status and configuration details for the KMS that manages the encryption key for this appliance. You must use the Grid Manager to make configuration changes.

KMS display name thales

External key UID 41b0306abcce451facfce01b1b4870ae1c1ec6bd5e3849d790223766baf35c57

Hostnames 10.96.99.164  
10.96.99.165

Port 5696

**Server certificate** **>**

**Client certificate** **>**

### Clear KMS Key

**⚠** Do not clear the KMS key if you need to access or preserve any data on this appliance.

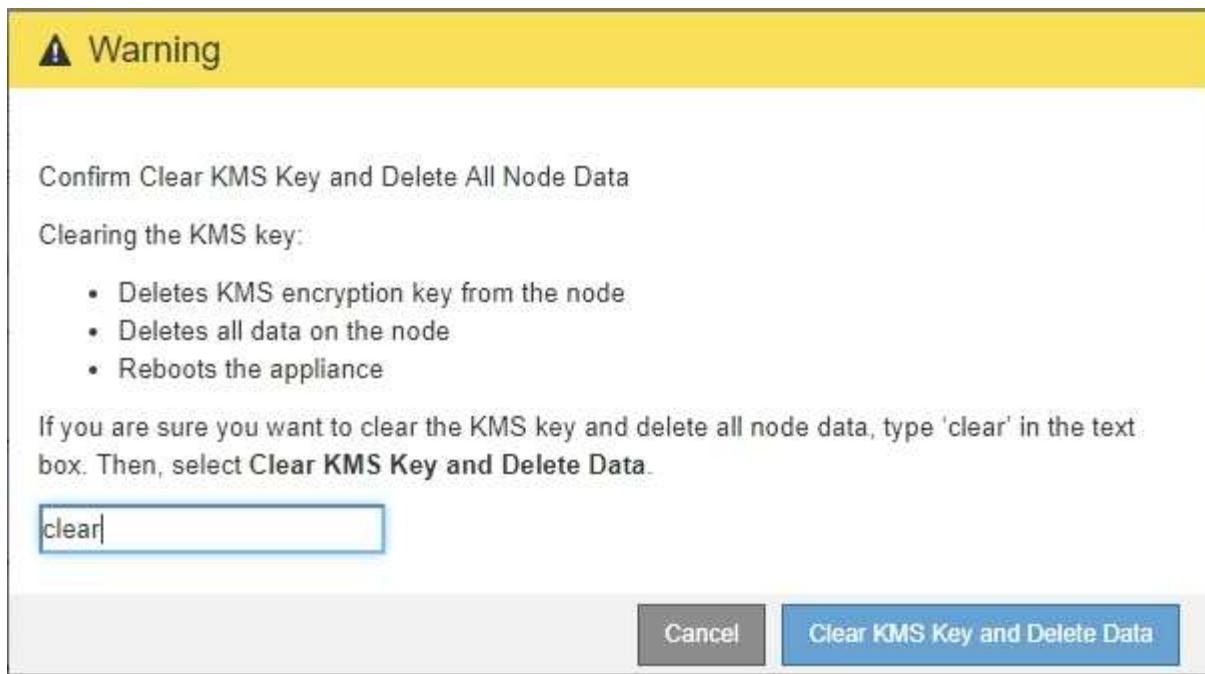
If you want to reinstall this appliance node (for example, in another grid), you must clear the KMS key. When the KMS key is cleared, all data on this appliance is deleted.

**Clear KMS Key and Delete Data**



If the KMS configuration is cleared, data on the appliance will be permanently deleted. This data is not recoverable.

3. At the bottom of the window, select **Clear KMS Key and Delete Data**.
4. If you are sure that you want to clear the KMS configuration, type **clear** and select **Clear KMS Key and Delete Data**.



The KMS encryption key and all data are deleted from the node, and the appliance reboots. This can take up to 20 minutes.

5. Open a browser, and enter one of the IP addresses for the appliance's compute controller.

[https://Controller\\_IP:8443](https://Controller_IP:8443)

*Controller\_IP* is the IP address of the compute controller (not the storage controller) on any of the three StorageGRID networks.

The StorageGRID Appliance Installer Home page appears.

6. Select **Configure Hardware > Node Encryption**.
7. Verify that node encryption is disabled and that the key and certificate information in **Key Management Server Details** and the **Clear KMS Key and Delete Data** control are removed from the window.

Node encryption cannot be reenabled on the appliance until it is reinstalled in a grid.

### After you finish

After the appliance reboots and you have verified that KMS has been cleared and that the appliance is in a pre-install state, you can physically remove the appliance from your StorageGRID system. See the recovery and maintenance instructions for information about preparing an appliance for reinstallation.

### Related information

[Administer StorageGRID](#)

[Maintain & recover](#)

## 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—with 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.