NetApp

Configure hardware (SG6000)

StorageGRID

NetApp
March 03, 2022

Table of Contents

Configure hardware (SG6000)

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.

Configure StorageGRID connections (SG6000)

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).

Access 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

   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.

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

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

    b. Open a web browser on the service laptop.

    c. 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.

  Verify and upgrade 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

Verify and upgrade 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

1. From the StorageGRID Appliance Installer, select **Advanced** > **Upgrade Firmware**.

2. Compare the Current Firmware version to the software version installed on your StorageGRID system. (From the top of the Grid Manager, select the help icon and select **About**.)

   The second digit in the two versions should match. For example, if your StorageGRID system is running version 11.**6**.*x.y*, the StorageGRID Appliance Installer version should be 3.**6**.*z*.

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

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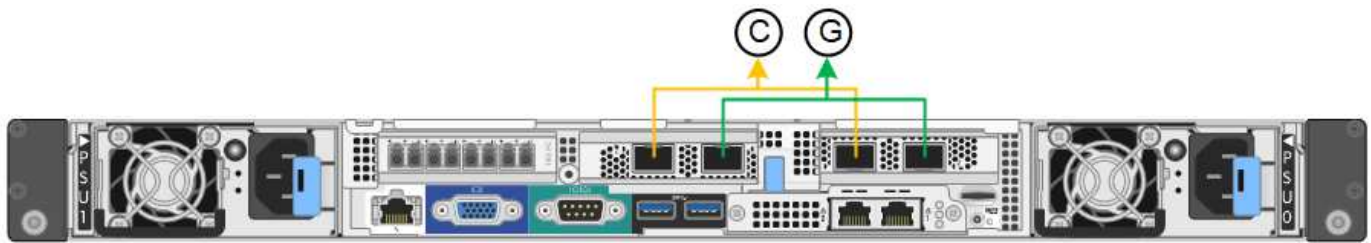
Callout	Which ports are bonded
C	Ports 1 and 3 are bonded together for the Client Network, if this network is used.
G	Ports 2 and 4 are bonded together for the Grid Network.

This figure shows how the four network ports are bonded in aggregate port bond mode.
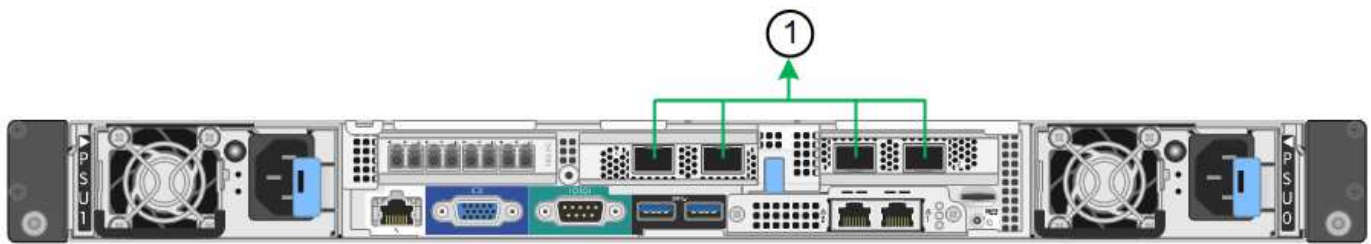
Callout	Which ports are bonded
1	All four ports are grouped in a single LACP bond, allowing all ports to be used for Grid Network and Client Network traffic.

The tables summarize 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
Active-Backup (default)	- Ports 2 and 4 use an active-backup bond for the Grid Network. - Ports 1 and 3 are not used. - A VLAN tag is optional.	- Ports 2 and 4 use an active-backup bond for the Grid Network. - Ports 1 and 3 use an active-backup bond for the Client Network. - VLAN tags can be specified for both networks for the convenience of the network administrator.

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad)	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 are not used. • A VLAN tag is optional.	• Ports 2 and 4 use an LACP bond for the Grid Network. • Ports 1 and 3 use an LACP bond for the Client Network. • VLAN tags can be specified for both networks for the convenience of the network administrator.

• **Aggregate port bond mode**

Network bond mode	Client Network disabled (default)	Client Network enabled
LACP (802.3ad) only	• Ports 1-4 use a single LACP bond for the Grid Network. • A single VLAN tag identifies Grid Network packets.	• Ports 1-4 use a single LACP bond for the Grid Network and the Client Network. • Two VLAN tags allow Grid Network packets to be segregated from Client Network packets.

See Port bond modes for 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.
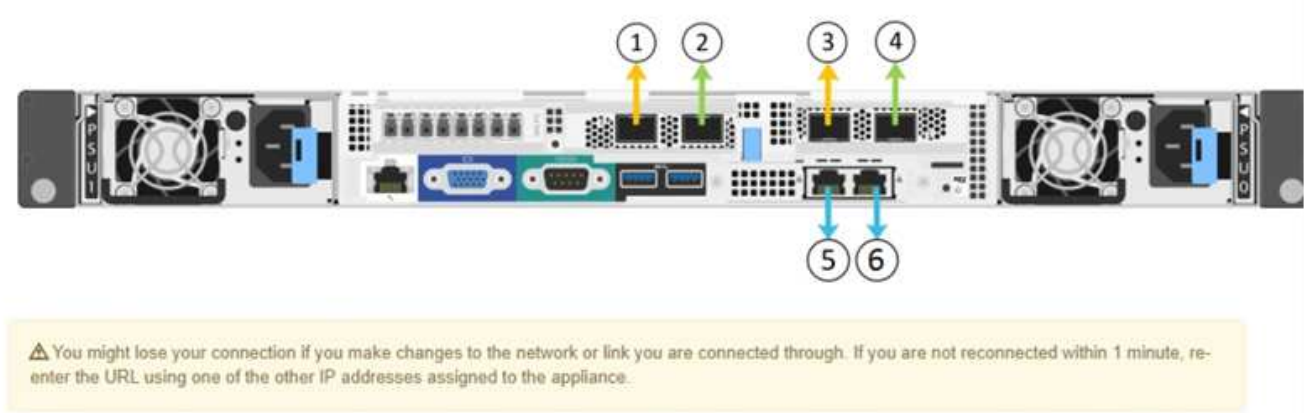

Steps

1. 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.

Network Link Configuration

⚠ 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	100
2	Up	100
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 **Auto**.
- **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   Auto

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 **Auto** 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.

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`

Configure 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.

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

a. Enter the static IPv4 address, using CIDR notation.

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.

> (i) 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.

> (i) 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.

> (i) 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)	10.224.3.72/21
Gateway	10.224.0.1
Subnets (CIDR)	0.0.0.0/32 ➕
MTU	1500 ⬍

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.

> (i) 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.

> (i) 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)	47.47.7.183/21
Gateway	47.47.0.1
MTU	1500

Cancel

Save

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

a. Enter the static IPv4 address, using CIDR notation.

b. Click **Save**.

c. Confirm that the IP address for the Client Network gateway is correct.

> (i) 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.

d. 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.

> ℹ️ 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.

    e. Click **Save**.

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

    a. 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.

> ℹ️ 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.

> ℹ️ 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.

Verify 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	Grid ⌄
Destination IPv4 Address or FQDN	
Test MTU	☐

Test Connectivity

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	Grid
Destination IPv4 Address or FQDN	10.96.104.223
Test MTU	☑

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

Configure network links (SG6000)

Change MTU setting

Verify 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.

> (i) The Grid Network ports listed in the port connectivity table are valid only for StorageGRID version 11.6.0. 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.

   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.

Port Connectivity Test

Network	Grid ▾
IPv4 Address Ranges	10.224.6.160-161
Port Ranges	22,2022
Protocol	⦿ TCP ◯ UDP
	Test Connectivity

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

Networking guidelines

Access and Configure SANtricity System Manager (SG6000)

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.

Set up and access 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**.

> ℹ️ 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.

  > ℹ️ 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.

> ℹ️ 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 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

> ℹ️ If these options are not available or the login page does not appear, you must use the IP addresses for the storage controllers. Access SANtricity System Manager by browsing to the storage controller IP.

2. Set or enter the administrator password.

SANtricity System Manager uses a single administrator password that is shared among all users.
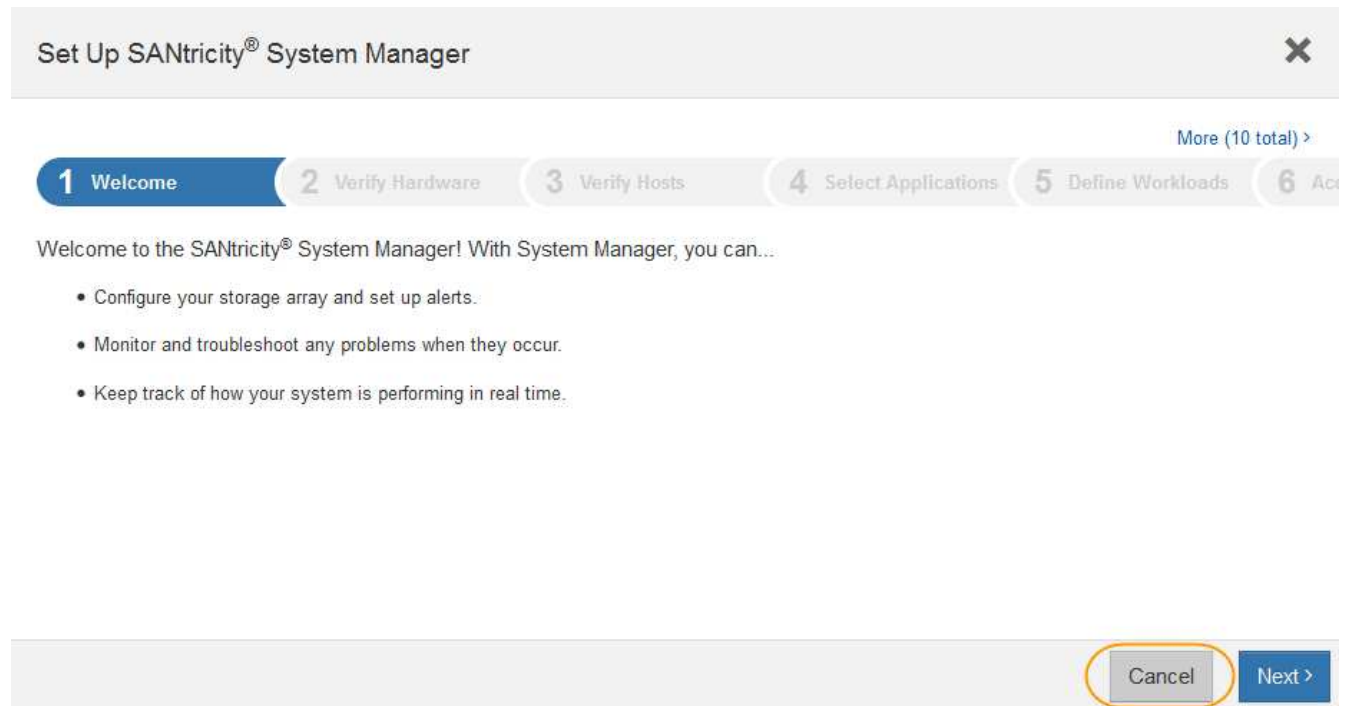
3. Select **Cancel** to close the wizard.

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

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 configuring storage proxy settings.

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.

Review 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.

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

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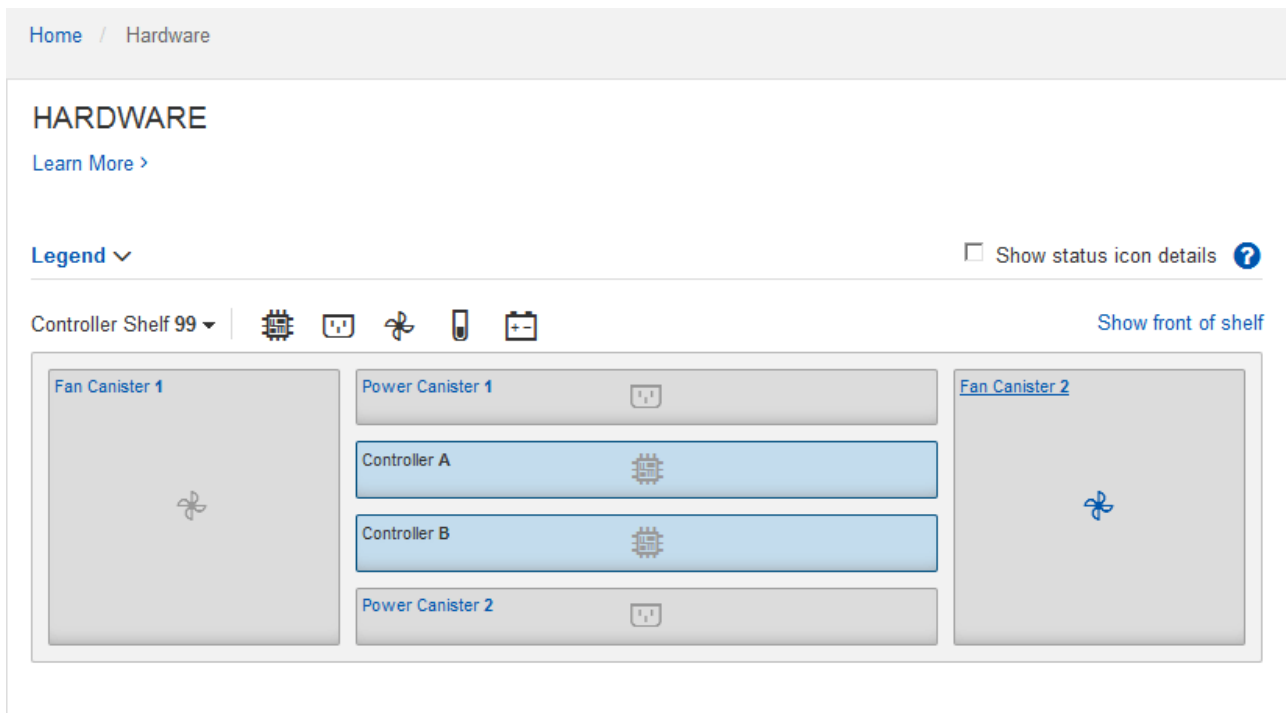
From the back of the shelf, you can view both storage controllers, the battery in each storage controller, the two power canisters, the two fan canisters, and expansion shelves (if any). You can also view

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.

Set IP addresses for storage controllers using 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.

> (i) 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.

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

IPv4 Address Assignment	◯ Static	⦿ 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.

   > ℹ️ 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*

Configure BMC interface (SG6000)

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.

Change root password for 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.
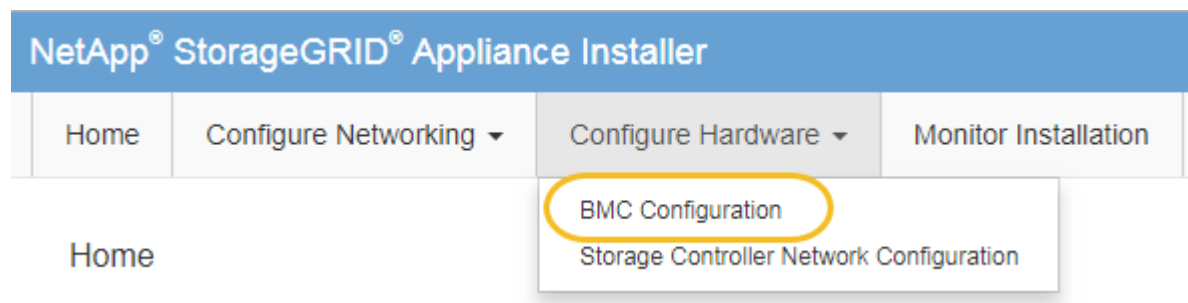
Steps

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

   https://*Appliance_Controller_IP*:8443

   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**.

   The Baseboard Management Controller Configuration page appears.

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

4. Click **Save**.

Set IP address for 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.

> (i) 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.
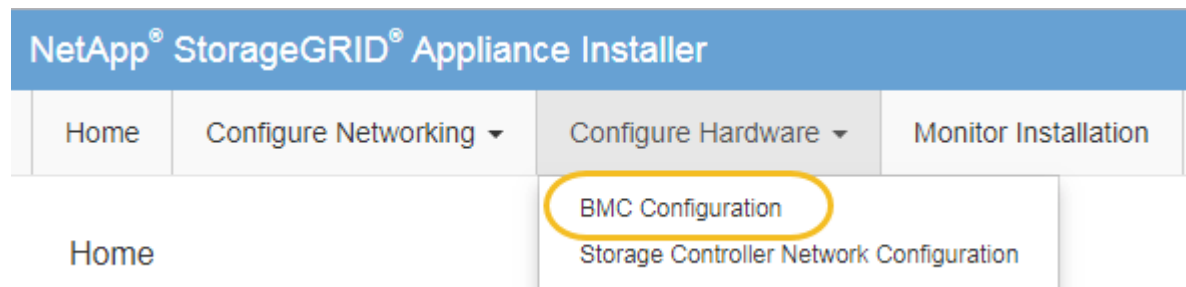
Steps

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

   https://*SG6000-CN_Controller_IP*:8443

   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 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.

   > (i) 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.

> ℹ️ 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.

Access 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

1. 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.

   > (i) If you haven't yet configured `BMC_Port_IP`, follow the instructions in Configure BMC interface (SG6000). If you are unable to follow that procedure due to a hardware problem, and have not yet configured a BMC IP address, you might still be able to access the BMC. By default, the BMC obtains an IP address using DHCP. If DHCP is enabled on the BMC network, your network administrator can provide the IP address assigned to the BMC MAC, which is printed on the label on the front of the SG6000-CN controller. If DHCP is not enabled on the BMC network, the BMC will not respond after a few minutes and assign itself the default static IP `192.168.0.120`. You might need to connect your laptop directly to the BMC port, and change the networking setting to assign your laptop an IP such as `192.168.0.200/24`, in order to browse to `192.168.0.120`.

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

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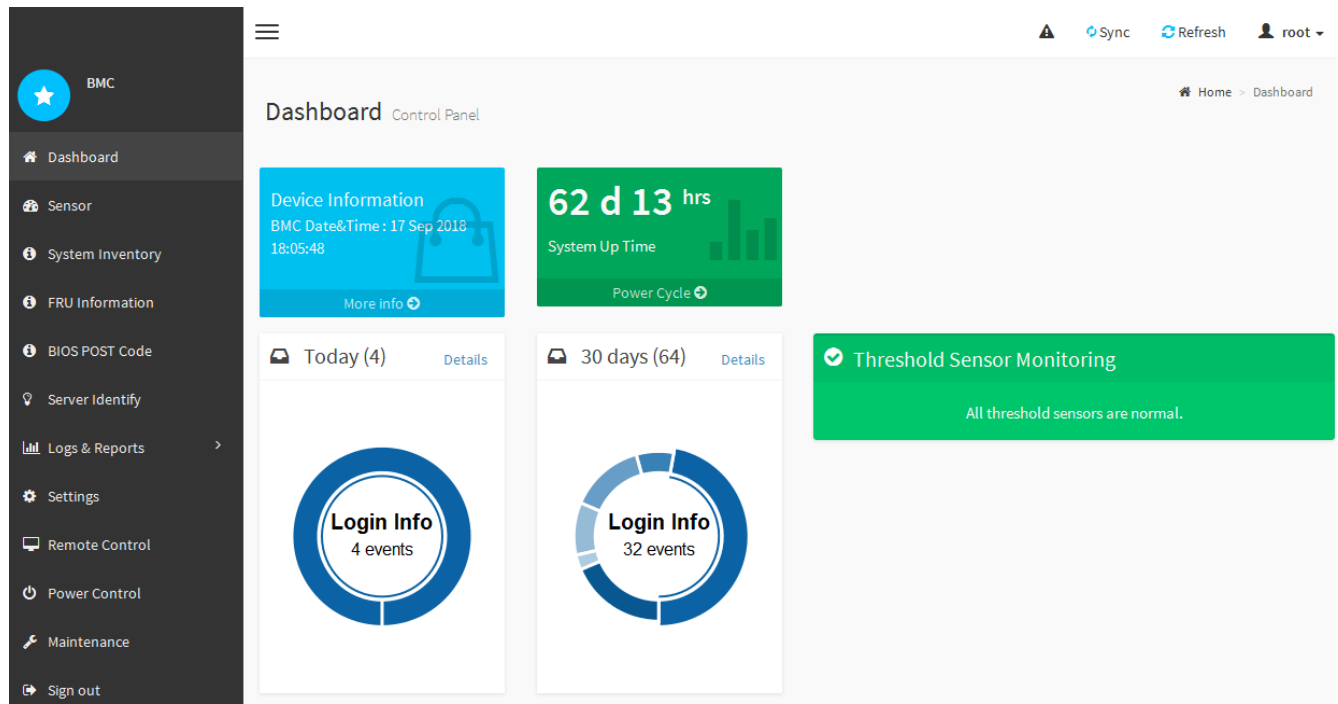
4. Optionally, create additional users by selecting **Settings** > **User Management** and clicking on any "disabled" user.

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

Configure SNMP settings for 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.

> ⓘ BMC settings made by this procedure might not be preserved if the SG6000-CN fails and has to be replaced. Make sure you have a record of all settings you have applied, so they can be easily reapplied after a hardware replacement if necessary.

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**.

Set 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.

> ⓘ BMC settings made by this procedure might not be preserved if the SG6000-CN fails and has to be replaced. Make sure you have a record of all settings you have applied, so they can be easily reapplied after a hardware replacement if necessary.

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.
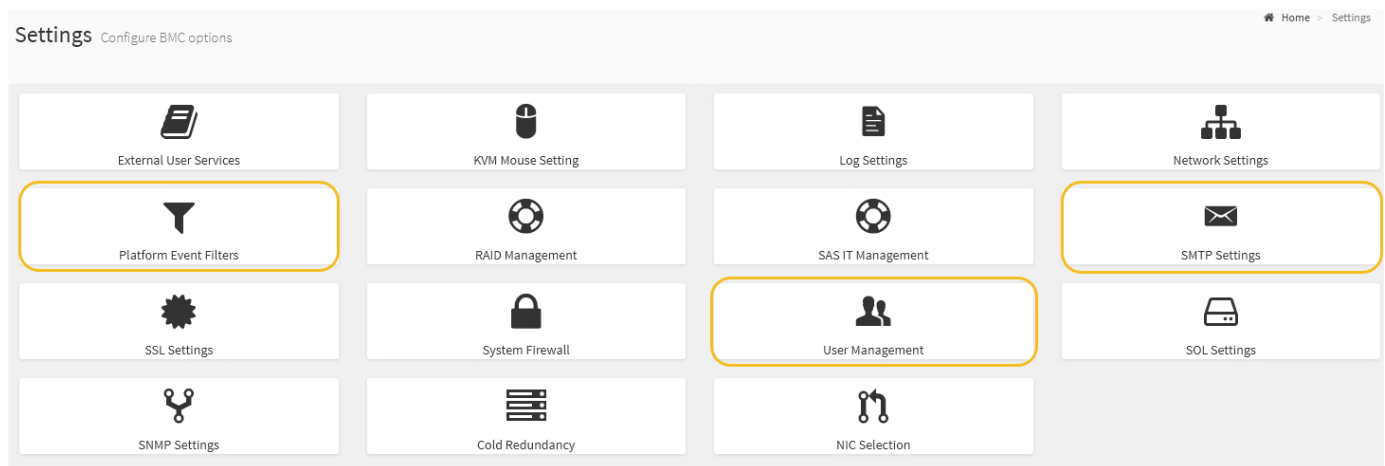
Steps

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: Enable 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.

> (i) Data that exists prior to connecting to the KMS on an appliance that has node encryption enabled 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.

   > (i) 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**.

3. Select **Enable node encryption**.

   Prior to appliance installation you can unselect **Enable node encryption** without risk of data loss. When the installation begins 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

Monitor node encryption in maintenance mode (SG6000)

Optional: Change 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.

- **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: Remap network ports for 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 Remove 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**.