Maintain appliance hardware

StorageGRID Appliances

NetApp
April 11, 2024

Table of Contents

Maintain appliance hardware

Maintain appliance configuration

Common procedures for node maintenance: Overview

Use these instructions to maintain your StorageGRID system.

About these instructions

These instructions describe procedures common to all nodes such as how to apply a software hotfix, recover grid nodes, recover a failed site, decommission grid nodes or an entire site, perform network maintenance, perform host-level and middleware maintenance procedures, and perform grid node procedures.

> In these instructions, “Linux” refers to a Red Hat® Enterprise Linux®, Ubuntu®, or Debian® deployment. Use the NetApp Interoperability Matrix Tool (IMT) to get a list of supported versions.

Before you begin

- You have a broad understanding of the StorageGRID system.
- You have reviewed your StorageGRID system’s topology and you understand the grid configuration.
- You understand that you must follow all instructions exactly and heed all warnings.
- You understand that maintenance procedures not described aren’t supported or require a services engagement.

Maintenance procedures for appliances

Specific maintenance procedures for each type of StorageGRID appliance are in the appliance maintenance sections:

- Maintain SG6100 appliance
- Maintain SG6000 appliance
- Maintain SG5700 appliance
- Maintain SG100 and SG1000 appliances

Place appliance into maintenance mode

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

Before you begin

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

About this task

In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

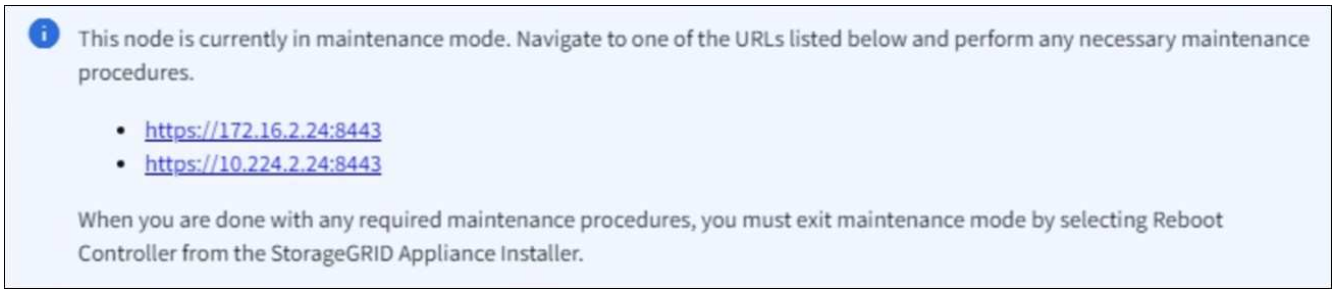
The admin account password and SSH host keys for a StorageGRID appliance in maintenance mode remain the same as they were when the appliance was in service.

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**.
4. Select **Maintenance mode**. A confirmation dialog box appears.
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.

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



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

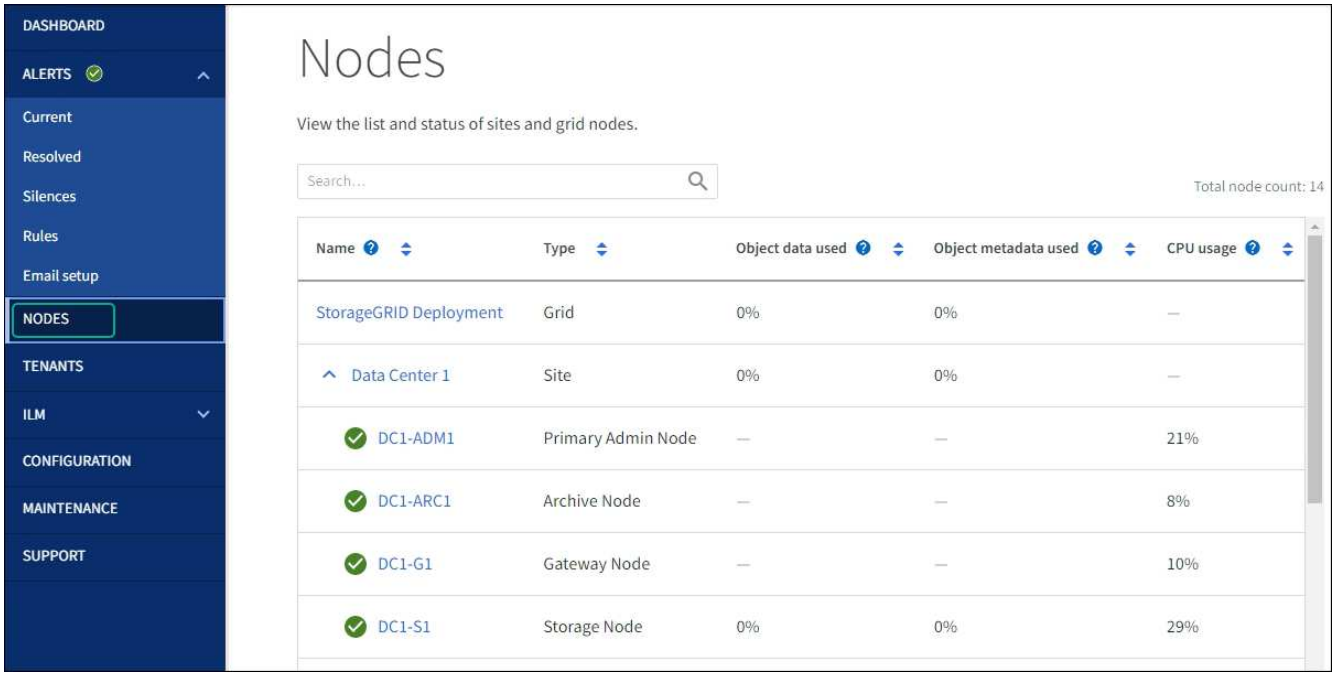
   If possible, use the URL containing the IP address of the appliance's Admin Network port.

   If you have a direct connection to the appliance's management port, use `https://169.254.0.1:8443` to access the StorageGRID Appliance Installer page.

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

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**.

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** page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Change MTU setting

You can change the MTU setting that you assigned when you configured IP addresses for the appliance node.

About this task

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 don't have to be the same for all network types.

To change the MTU setting without rebooting the appliance node, use the Change IP tool.

If the Client or Admin Network was not configured in the StorageGRID Appliance Installer during the initial installation, change the MTU setting using maintenance mode.

Change the MTU setting using the Change IP tool

Before you begin

You have the `Passwords.txt` file to use the Change IP tool.

Steps

Access the Change IP tool and update the MTU settings as described in Change node network configuration.

Change the MTU setting using maintenance mode

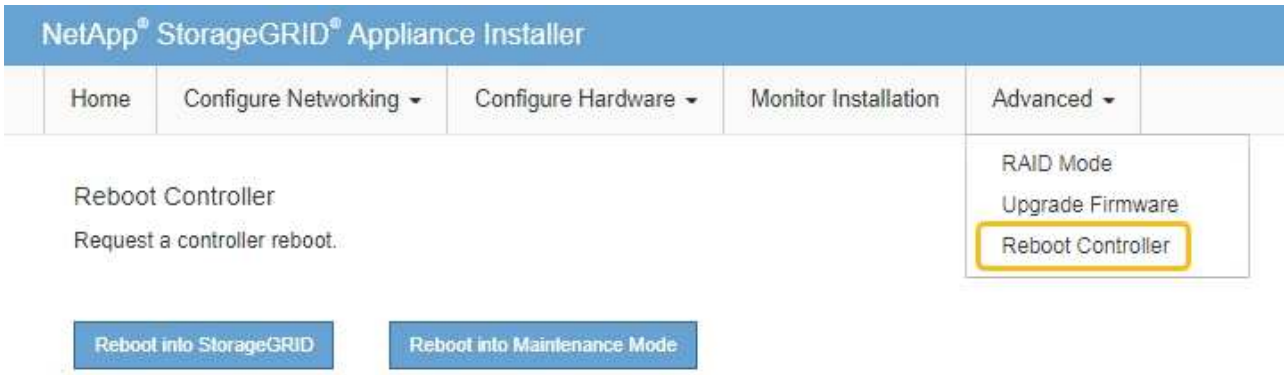
Change the MTU setting using maintenance mode if you are unable to access these settings using the Change IP tool.

Before you begin

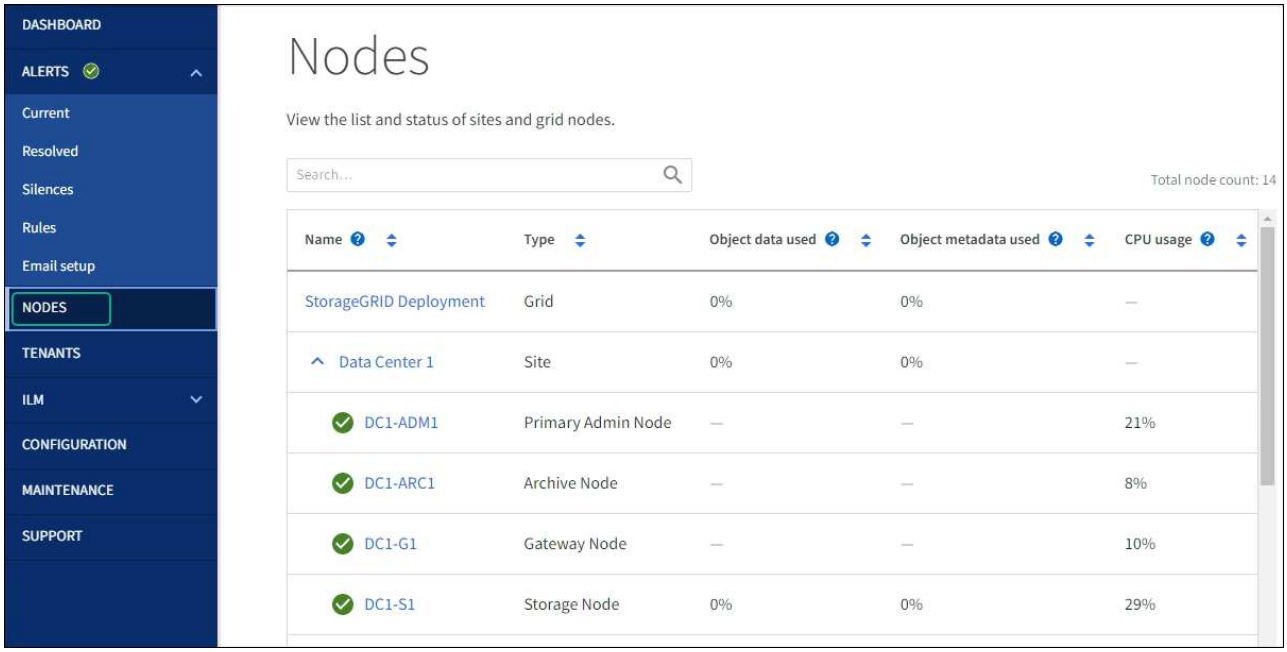
The appliance has been placed maintenance mode.

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.
3. When you are satisfied with the settings, select **Save**.
4. If this procedure completed successfully and you have additional procedures to perform while the node is in maintenance mode, perform them now. When you are done, or if you experienced any failures and want to start over, select **Advanced** > **Reboot Controller**, and then select one of these options:
   - Select **Reboot into StorageGRID**
   - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if you experienced any failures during the procedure and want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.



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** page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Check DNS server configuration

You can check and temporarily change the DNS servers that are currently in use by this appliance node.

Before you begin

The appliance has been placed maintenance mode.

About this task

You might need to change the DNS server settings if an encrypted appliance can't 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**).

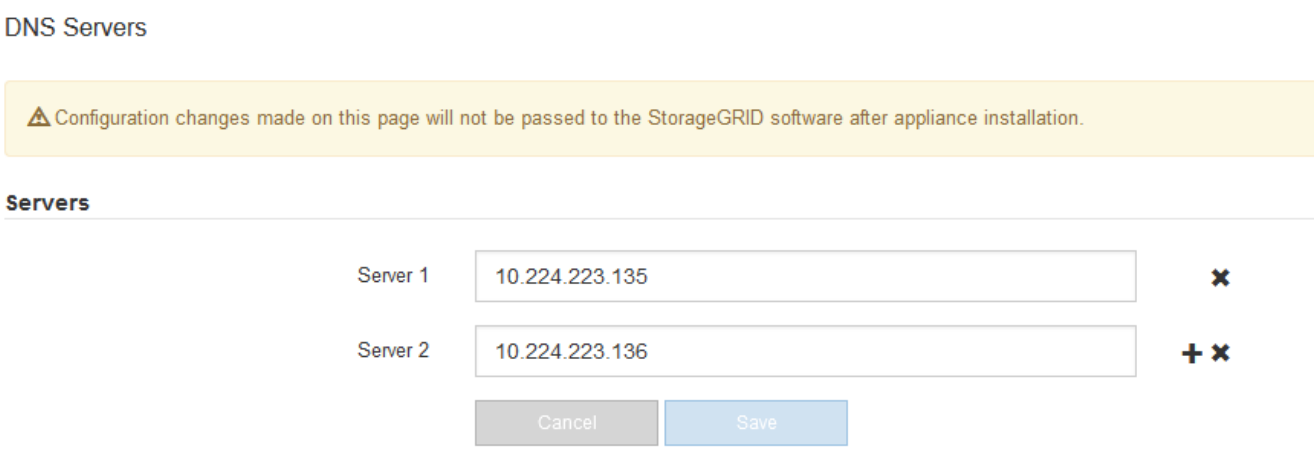
- Temporary changes to the DNS configuration are necessary only for node-encrypted appliances where the KMS server is defined using a fully qualified domain name, instead of an IP address, for the hostname.
- When a node-encrypted appliance connects to a KMS using a domain name, it must connect to one 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 can't 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 can't 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, because 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.



3. If required, change the DNS servers.

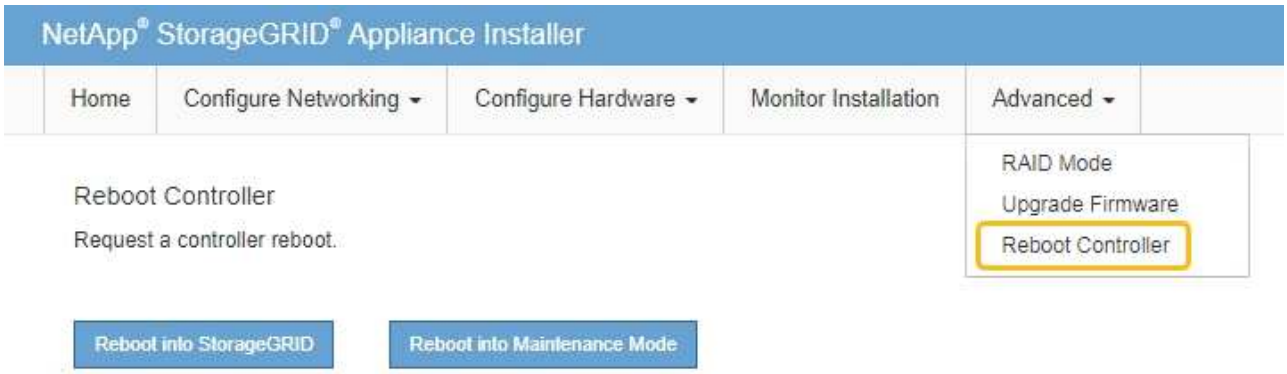
> Changes made to the DNS settings are temporary and are lost when you exit maintenance mode.

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.

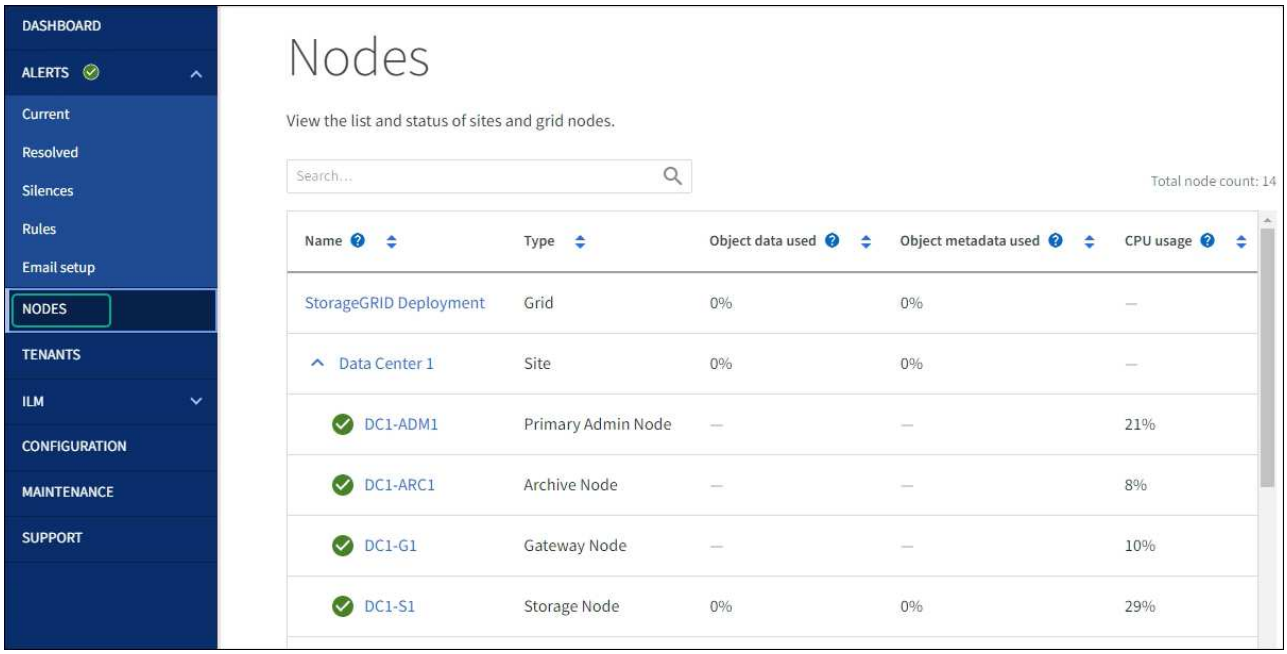
5. After node data is decrypted, reboot the node. From the StorageGRID Appliance Installer, select **Advanced** > **Reboot Controller**, and then select one of these options:

- 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. (This option is available only when the controller is 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** page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Update MAC address references

In some cases you might need to update MAC address references after the replacement of an appliance.

About this task

If any of the network interfaces on an appliance you are replacing are configured for DHCP, you might need to update the permanent DHCP lease assignments on the DHCP servers to reference the MAC addresses of the replacement appliance. The update ensures the replacement appliance is assigned the expected IP addresses.

Steps

1. Locate the label on the front of the appliance. The label lists the MAC address for the BMC management port of the appliance.
2. 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 =**.

3. Ask your network administrator to associate the DNS/network and IP address for the appliance you removed with the MAC address for the replacement appliance.

   > You must ensure that all IP addresses for the original appliance have been updated before you apply power to the replacement appliance. Otherwise, the appliance 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 appliance.

   > If the original appliance used static IP address, the new appliance will automatically adopt the IP addresses of the appliance you removed.

Monitor 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.

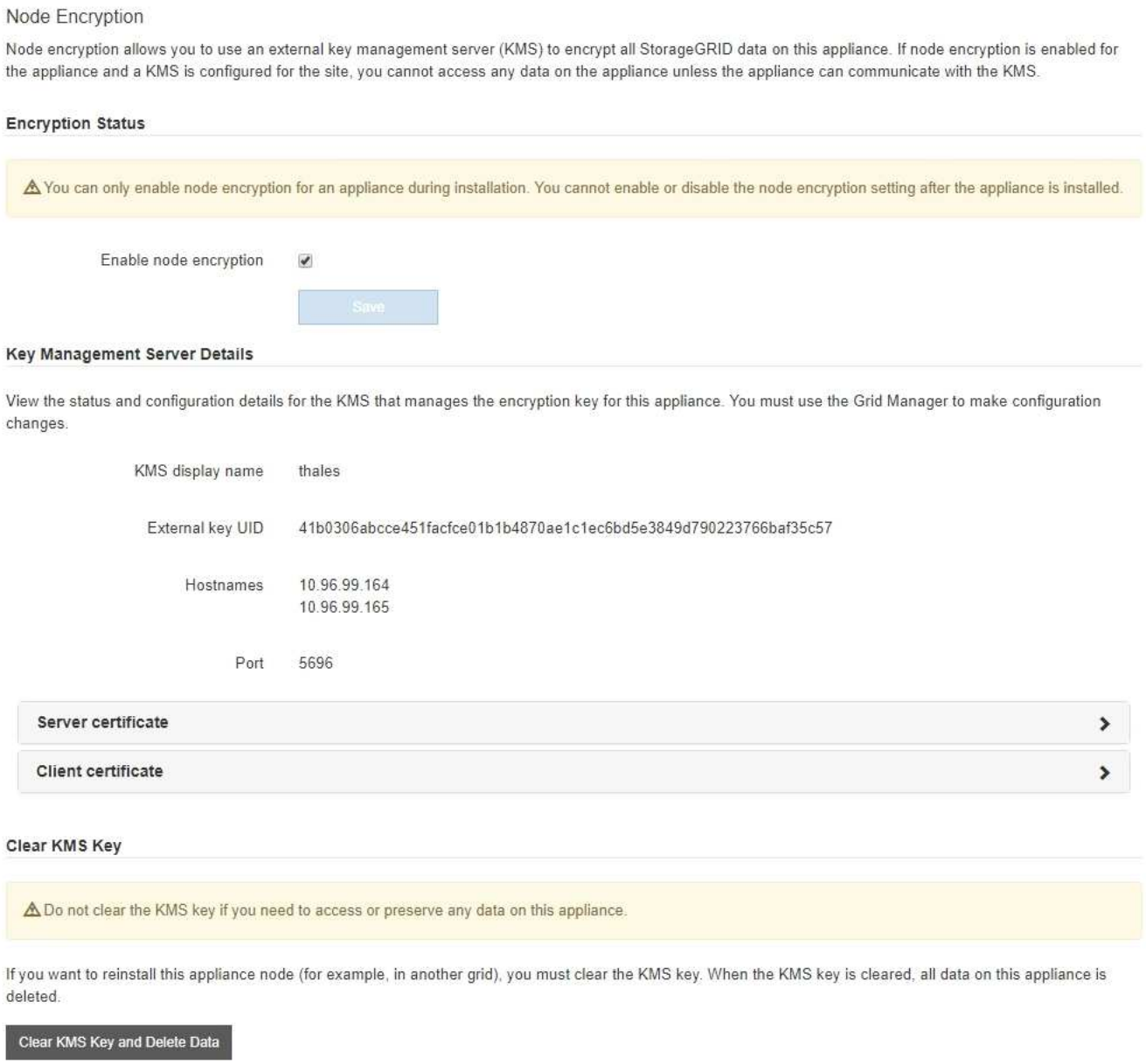
See Configure key management servers for information about implementing KMS for StorageGRID appliances.

Before you begin

- You enabled node encryption for the appliance during installation. You can't enable node encryption after the appliance is installed.
- You have placed the appliance into maintenance mode.

Steps

1. From the StorageGRID Appliance Installer, select **Configure Hardware** > **Node Encryption**.

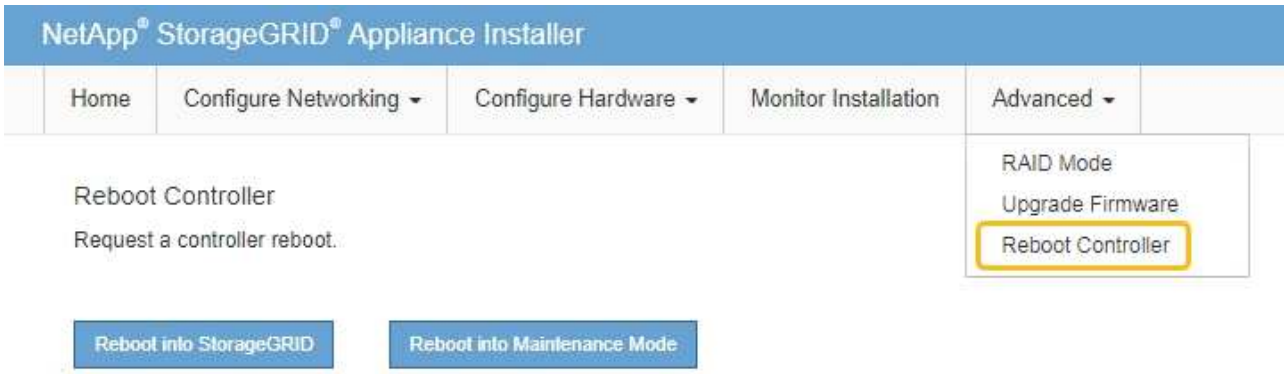


The Node Encryption page includes three sections:

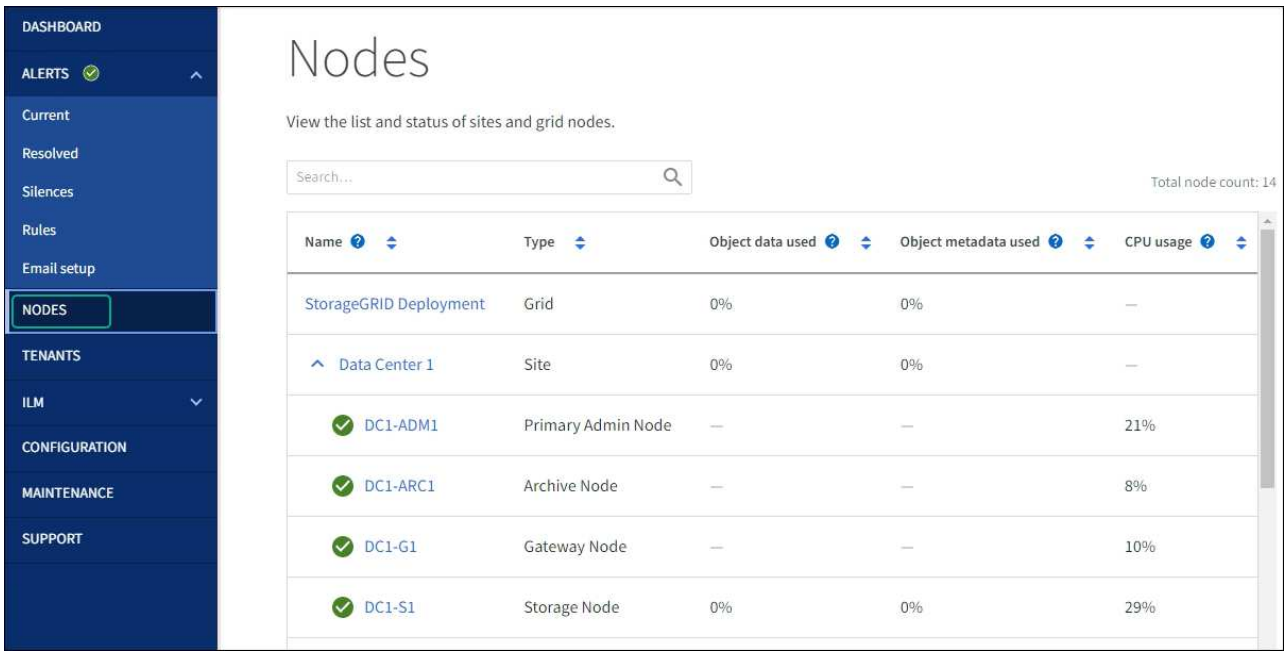
- Encryption Status shows whether node encryption is enabled or disabled for the appliance.
- Key Management Server Details shows information about the KMS being used to encrypt the appliance. You can expand the server and client certificate sections to view certificate details and status.
  - To address issues with the certificates themselves, such as renewing expired certificates, see the instructions for configuring KMS.
  - If there are unexpected problems connecting to KMS hosts, verify that the DNS servers are correct and that appliance networking is correctly configured.
  - 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 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. (This option is available only when the controller is 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** page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Clear 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.

Before you begin

If you need to preserve data on the appliance, you must either perform a node decommission procedure or clone the node 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.

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 can't 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.

  > Don't 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`

   `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**.

   > 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`** in the warning dialog box 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`

   `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 can't 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 instructions for preparing the appliance for reinstallation.

Appliance node cloning

Appliance node cloning: Overview

You can clone an appliance node in StorageGRID to use an appliance of newer design or increased capabilities. Cloning transfers all information about the existing node to the new appliance, provides a hardware-upgrade process that is easy to perform, and provides an alternative to decommissioning and expansion for replacing appliances.

Appliance node cloning lets you easily replace an existing appliance node (source) in your grid with a compatible appliance (target) that is part of the same logical StorageGRID site. The process transfers all data to the new appliance, placing it in service to replace the old appliance node and leaving the old appliance in a pre-install state.

Why clone an appliance node?

You can clone an appliance node if you need to:

- Replace appliances that are reaching end-of-life.
- Upgrade existing nodes to take advantage of improved appliance technology.
- Increase grid storage capacity without changing the number of Storage Nodes in your StorageGRID system.
- Improve storage efficiency, such as by changing the RAID mode from DDP-8 to DDP-16, or to RAID-6.

- Efficiently implement node encryption to allow the use of external key management servers (KMS).

Which StorageGRID network is used?

Cloning transfers data from the source node directly to the target appliance over any of the three StorageGRID networks. The Grid Network is typically used, but you can also use the Admin Network or the Client Network if the source appliance is connected to these networks. Choose the network to use for cloning traffic that provides the best data-transfer performance without degrading StorageGRID network performance or data availability.

When you install the replacement appliance, you must specify temporary IP addresses for StorageGRID connection and data transfer. Because the replacement appliance will be part of the same networks as the appliance node it replaces, you must specify temporary IP addresses for each of these networks on the replacement appliance.

Target appliance compatibility

Replacement appliances must be the same type as the source node they are replacing and both must be part of the same logical StorageGRID site.

- A replacement services appliance can be different than the Admin Node or Gateway Node it is replacing.
  - You can clone an SG100 source node appliance to an SG1000 services target appliance to give the Admin Node or Gateway Node greater capability.
  - You can clone an SG1000 source node appliance to an SG100 services target appliance to redeploy the SG1000 for a more demanding application.

    For example, if an SG1000 source node appliance is being used as an Admin Node and you want to use it as a dedicated load-balancing node.

  - Replacing an SG1000 source node appliance with an SG100 services target appliance reduces the maximum speed of the network ports from 100-GbE to 25-GbE.
  - The services appliances have different network connectors. Changing the appliance type might require replacing the cables or SFP modules.
- A replacement storage appliance must have greater capacity than the Storage Node it is replacing.
  - If the target storage appliance has the same number of drives as the source node, the drives in the target appliance must have greater capacity (in TB).
  - If you plan to use the same RAID mode on the target node as was used on the source node, or a less storage efficient RAID mode (for example, switching from RAID 6 to DDP), the drives in the target appliance must be larger (in TB) than the drives in the source appliance.
  - If the number of standard drives installed in a target storage appliance is less than the number of drives in the source node, due to installation of solid-state drives (SSDs), the overall storage capacity of the standard drives in the target appliance (in TB) must exceed the total functional drive capacity of all drives in the source Storage Node.

    For example, when cloning an SG5760 source Storage Node appliance with 60 drives to an SG6060 target appliance with 58 standard drives, larger drives should be installed in the SG6060 target appliance before cloning to maintain storage capacity. (The two drive slots containing SSDs in the target appliance aren’t included in the total appliance-storage capacity.)

    However, if a 60-drive SG5760 source node appliance is configured with SANtricity Dynamic Disk Pools DDP-8, configuring a 58-drive same-size-drive SG6060 target appliance with DDP-16 might

make the SG6060 appliance a valid clone target due to its improved storage efficiency.

You can view information about the current RAID mode of the source appliance node on the **NODES** page in Grid Manager. Select the **Storage** tab for the appliance.

- The number of volumes in a target storage appliance must be greater than or equal to the number of volumes in the source node. You cannot clone a source node with 16 object store volumes (rangedb) to a target storage appliance with 12 object store volumes even if the target appliance has larger capacity than the source node. Most storage appliances have 16 object store volumes, except the SGF6112 storage appliance that has only 12 object store volumes.

What information is not cloned?

The following appliance configurations don't transfer to the replacement appliance during cloning. You must configure them during initial set up of the replacement appliance.

- BMC interface
- Network links
- Node encryption status
- SANtricity System Manager (for Storage Nodes)
- RAID mode (for Storage Nodes)

What issues prevent cloning?

If any of the following issues are encountered while cloning, the cloning process halts and an error message is generated:

- Wrong network configuration
- Lack of connectivity between the source and target appliances
- Source and target appliance incompatibility
- For Storage Nodes, a replacement appliance of insufficient capacity

You must resolve each issue for cloning to continue.

Considerations and requirements for appliance node cloning

Before cloning an appliance node, you must understand the considerations and requirements.

Hardware requirements for the replacement appliance

Ensure that the replacement appliance meets the following criteria:

- The source node (appliance being replaced) and the target (new) appliance must be the same type of appliance:
  - You can only clone an Admin Node appliance or a Gateway Node appliance to a new services appliance.
  - You can only clone a Storage Node appliance to a new storage appliance.
- For Admin Node or Gateway Node appliances, the source node appliance and the target appliance don't need to be the same appliance model; however, changing the appliance model might require replacing the

cables or SFP modules.

For example, you can replace a SG1000 node appliance with a SG100 or replace a SG100 appliance with a SG1000 appliance.

- For Storage Node appliances, the source node appliance and the target appliance don't need to be the same type of appliance; however:
  - The target appliance must have greater storage capacity than the source appliance.

    For example, you can replace a SG5700 node appliance with a SG6000 appliance.

  - The target appliance must have an equal or greater number of object storage volumes than the source appliance.

    For example, you cannot replace a SG6000 node appliance (16 object store volumes) with a SGF6112 appliance (12 object store volumes).

Contact your StorageGRID sales representative for help choosing compatible replacement appliances to clone specific appliance nodes in your StorageGRID installation.

Prepare to clone an appliance node

You must have the following information before you clone an appliance node:

- Obtain a temporary IP address for the Grid Network from your network administrator for use with the target appliance during initial installation. If the source node belongs to an Admin Network or Client Network, obtain temporary IP addresses for these networks.

  Temporary IP addresses are normally on the same subnet as the source node appliance being cloned and aren't needed after cloning completes. The source and target appliances must both connect to the primary Admin Node of your StorageGRID to establish a cloning connection.

- Determine which network to use for cloning data-transfer traffic that provides the best data-transfer performance without degrading StorageGRID network performance or data availability.

  Using the 1-GbE Admin Network for clone data transfer results in slower cloning.

- Determine if node encryption using a key management server (KMS) will be used on the target appliance, so that you can enable node encryption during initial target appliance installation before cloning. You can check if node encryption is enabled on the source appliance node as described in the enabling node encryption.

  The source node and target appliance can have different node-encryption settings. Data decryption and encryption is performed automatically during data transfer and when the target node restarts and joins the grid.

- Determine if the RAID mode on the target appliance should be changed from its default setting, so you can specify this information during initial target appliance installation before cloning. You can view information about the current RAID mode of the source appliance node on the **NODES** page in Grid Manager. Select the **Hardware** tab for the appliance.

  The source node and target appliance can have different RAID settings.

- Plan for sufficient time to complete the node cloning process. Several days might be required to transfer

data from an operational Storage Node to a target appliance. Schedule cloning at a time that minimizes the impact to your business.

- You should only clone one appliance node at a time. Cloning can prevent you from performing other StorageGRID maintenance functions at the same time.
- After you have cloned an appliance node, you can use the source appliance that was returned to a pre-install state as the target to clone another compatible node appliance.

Clone appliance node

The cloning process might take several days to transfer data between the source node (appliance being replaced) and the target (new) appliance.

Before you begin

- You have installed the compatible target appliance into a cabinet or rack, connected all cables, and applied power.
- You have verified that the StorageGRID Appliance Installer version on the replacement appliance matches the software version of your StorageGRID system, upgrading and downgrading the StorageGRID Appliance Installer firmware, if necessary.
- You have configured the target appliance, including configuring StorageGRID connections, SANtricity System Manager (storage appliances only), and the BMC interface.
  - When configuring StorageGRID connections, use the temporary IP addresses.
  - When configuring network links, use the final link configuration.

> Leave the StorageGRID Appliance Installer open after you complete initial target appliance configuration. You will return to the target appliance's installer page after you start the node cloning process.

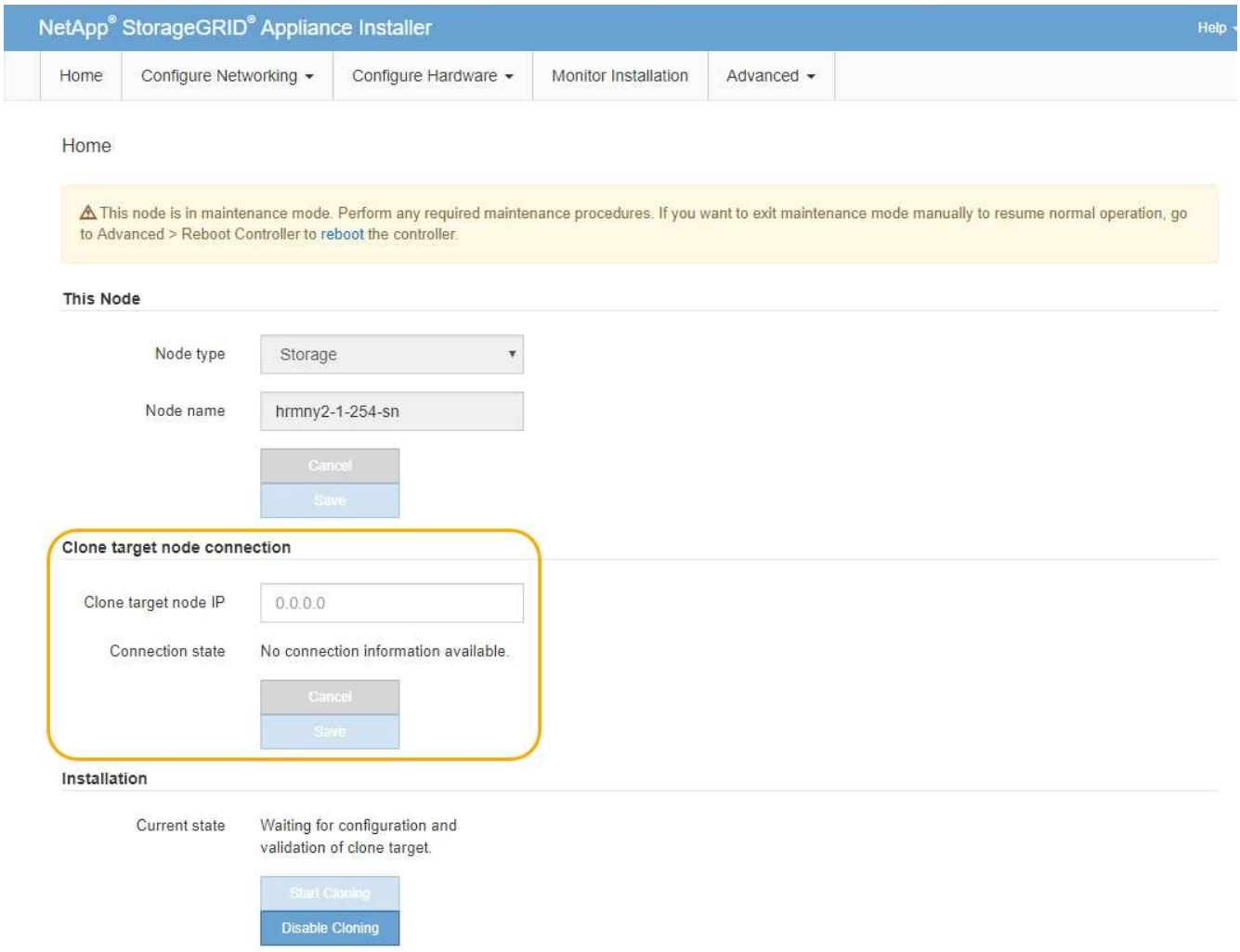
- You have optionally enabled node encryption for the target appliance.
- You have optionally set the RAID mode for the target appliance (storage appliances only).
- You have reviewed the considerations and requirements for appliance node cloning.

You should clone only one appliance node at a time to maintain StorageGRID network performance and data availability.

Steps

1. Place the source node you are cloning into maintenance mode.
2. From the StorageGRID Appliance Installer on the source node, in the Installation section of the Home page, select **Enable Cloning**.

   The Primary Admin Node connection section is replaced with the Clone target node connection section.



3. For **Clone target node IP**, enter the temporary IP address assigned to the target node for the network to use for clone data-transfer traffic, and then select **Save**.

   Typically, you enter the IP address for the Grid Network, but if you need to use a different network for clone data-transfer traffic, enter the IP address of the target node on that network.

   > Using the 1-GbE Admin Network for clone data transfer results in slower cloning.

   After the target appliance is configured and validated, in the Installation section, **Start Cloning** is enabled on the source node.

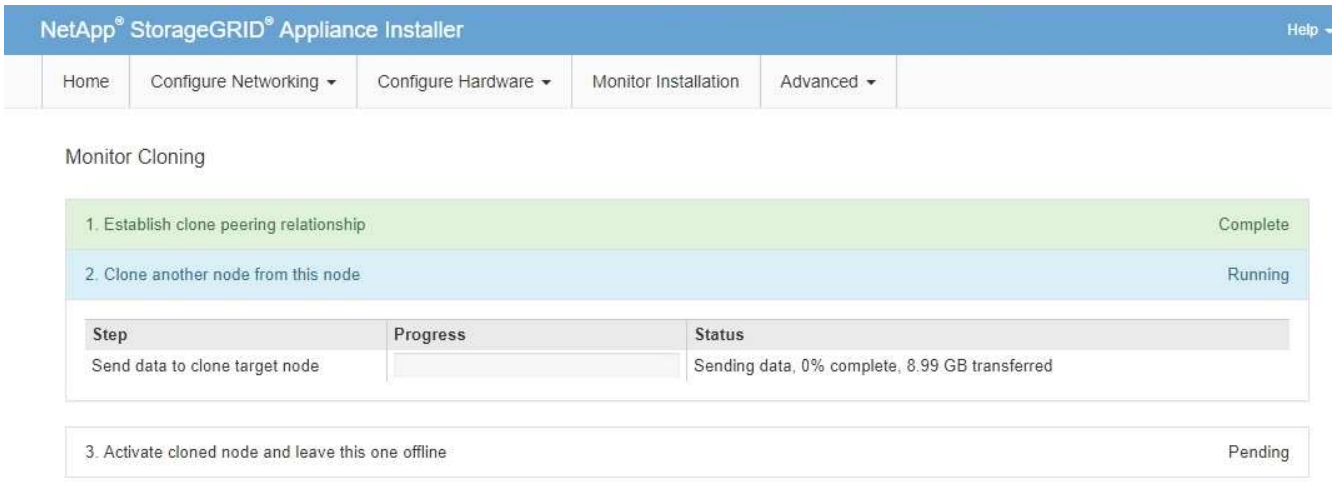
   If issues exist that prevent cloning, **Start Cloning** is not enabled and issues that you must resolve are listed as the **Connection state**. These issues are listed on the StorageGRID Appliance Installer Home page of both the source node and the target appliance. Only one issue displays at a time and the state automatically updates as conditions change. Resolve all cloning issues to enable **Start Cloning**.

   When **Start Cloning** is enabled, the **Current state** indicates the StorageGRID network that was selected for cloning traffic, along with information about using that network connection. See Considerations and requirements for appliance node cloning.

4. Select **Start Cloning** on the source node.
5. Monitor the cloning progress using the StorageGRID Appliance Installer on either the source or target

node.

The StorageGRID Appliance Installer on both the source and target nodes indicate similar status.



The Monitor Cloning page provides detailed progress for each stage of the cloning process:

- **Establish clone peering relationship** shows the progress of cloning set up and configuration.
- **Clone another node from this node** shows the progress of data transfer. (This part of the cloning process can take several days to complete.)
- **Activate cloned node and leave this one offline** shows the progress of transferring control to the target node and placing the source node in a pre-install state, after data transfer is complete.

6. If you need to terminate the cloning process and return the source node to service before cloning is complete, on the source node go to the StorageGRID Appliance Installer Home page and select **Advanced** > **Reboot Controller**, and then select **Reboot into StorageGRID**.

   If the cloning process is terminated:

   - The source node exits maintenance mode and rejoins StorageGRID.
   - The target node remains in the pre-install state.
     To restart cloning the source node, start the cloning process again from step 1.

When cloning successfully completes:

- The source and target nodes swap IP addresses:
  - The target node now uses the IP addresses originally assigned to the source node for the Grid, Admin, and Client Networks.
  - The source node now uses the temporary IP address initially assigned to the target node.
- The target node exits maintenance mode and joins StorageGRID, replacing the source node.
- The source appliance is in a pre-installed state, as if you had prepared it for reinstallation.

> If the target appliance does not join the grid, go to the StorageGRID Appliance Installer Home page for the source node, select **Advanced** > **Reboot Controller**, and then select **Reboot into Maintenance Mode**. After the source node reboots in maintenance mode, repeat the node cloning procedure.

- User data remains on the source appliance as a recovery option if an unexpected issue occurs with the target node. After the target node has successfully joined StorageGRID, user data on the source appliance is outdated and is no longer needed.

  Outdated user data is overwritten when you install or expand the source appliance as a new node in another grid.

  You can also reset the controller configuration on the source appliance to make this data inaccessible:

  1. Open the StorageGRID Appliance Installer for the source appliance using the temporary IP address initially assigned to the target node.
  2. Select **Help** > **Support and Debug Tools**.
  3. Select **Reset Storage Controller Configuration**.

  > If needed, contact technical support for assistance resetting the storage controller configuration.

  > Overwriting the data or resetting the controller configuration makes the outdated data difficult or impossible to retrieve; however, neither method securely removes the data from the source appliance. If a secure erase is required, use a data-wiping tool or service to permanently and securely remove data from the source appliance.

You can:

- Use the source appliance as a target for additional cloning operations: no additional configuration is required. This appliance already has the temporary IP address assigned that were originally specified for the first clone target.
- Install and set up the source appliance as a new appliance node.
- Discard the source appliance if it is no longer of use with StorageGRID.

Maintain SG1000 and SG100 services appliance hardware

Maintain SG100 and SG1000 appliances

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

Procedures specific to maintaining your SG100 or SG1000 appliance are in this section.

See Common procedures for maintenance procedures that are used by all appliances.

See Set up hardware for maintenance procedures that are also performed during initial appliance installation and configuration.

Maintenance configuration procedures

Turn SG100 or SG1000 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.

Before you begin

You have the BMC IP address of the controller you want to identify.

Steps

1. Access the appliance BMC interface.
2. Select **Server Identify**.

   The current status of the identify LED is selected.

3. Select **ON** or **OFF**, and then select **Perform Action**.

   When you select **ON**, the blue identify LEDs light on the front (shown) and rear of the appliance.

   If a bezel is installed on the controller, it might be difficult to see the front identify LED.

4. Turn the LED on and off as needed.

Related information

Locate controller in data center

Access BMC interface

Locate SG100 or SG1000 in data center

Locate the controller so that you can perform hardware maintenance or upgrades.

Before you begin

- You have determined which controller requires maintenance.
- (Optional) To help locate the controller in your data center, turn on the blue identify LED.

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.

Shut down the SG100 or SG1000

Shut down the services appliance to perform hardware maintenance.

Before you begin

- You have physically located the services appliance requiring maintenance in the data center.

About this task

To prevent service interruptions, shut down the services appliance during a scheduled maintenance window when periods of service disruption are acceptable.

Steps

1. Shut down the appliance:

> You must perform a controlled shut down of the appliance by entering the commands specified below. It is a best practice to perform a controlled shutdown when possible to avoid unnecessary alerts, ensure full logs are available, and avoid service disruptions.

   a. If you have not already logged into the grid node, log in 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 services appliance:
```
shutdown -h now
```
This command might take up to 10 minutes to complete.

2. Use one of the following methods to verify that the appliance is powered off:
   - Look at the power LED on the front of the appliance and confirm that it is off.
   - Check the Power Control page of the BMC interface to confirm the appliance is off.

Change link configuration of SG100 or SG1000

You can change the Ethernet link configuration of the services appliance. You can change the port bond mode, the network bond mode, and the link speed.

Before you begin

- You have placed the appliance into maintenance mode.

> In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

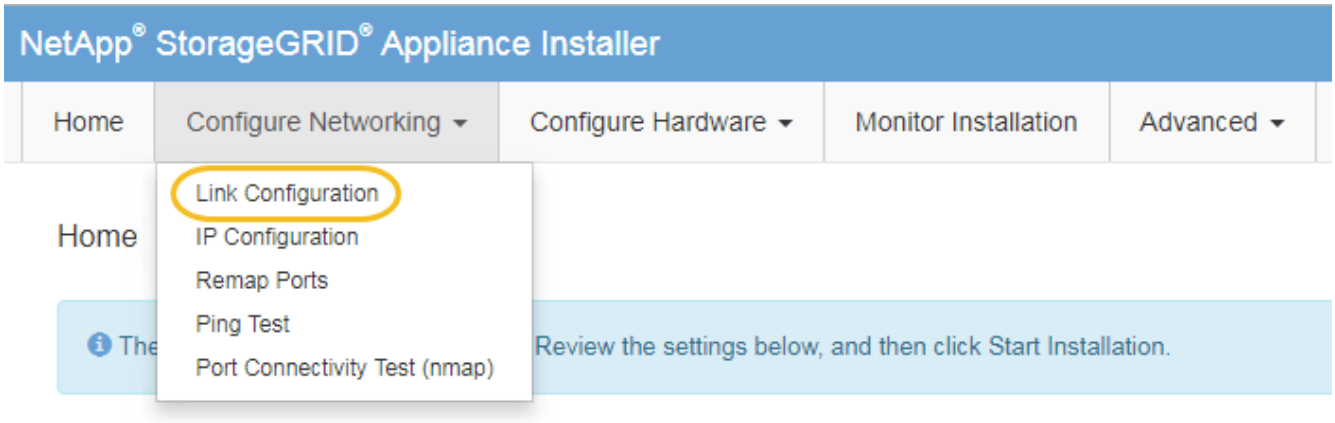
About this task

Options for changing the Ethernet link configuration of the services appliance 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 about the options, see Configure network links.

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 aren't 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://services_appliance_IP:8443`

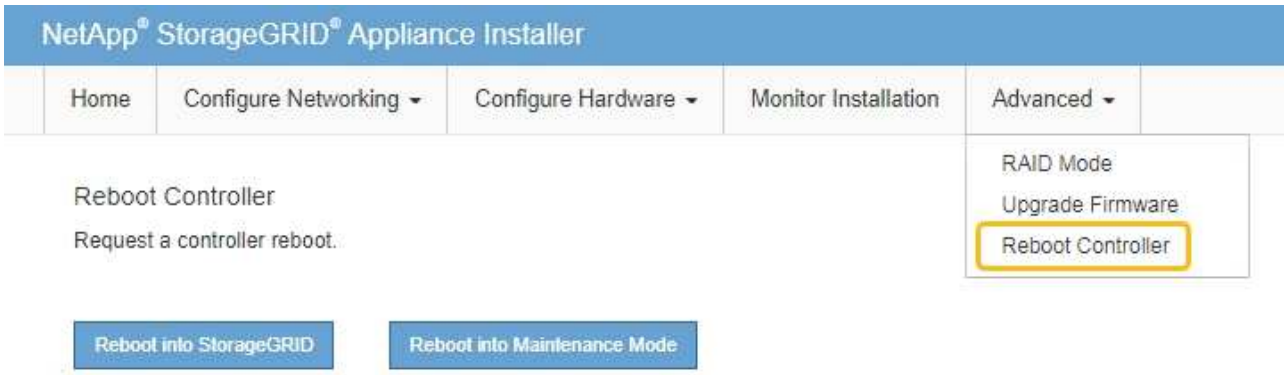
4. Make any necessary changes to the IP addresses for the appliance.

   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, see Configure StorageGRID IP addresses.

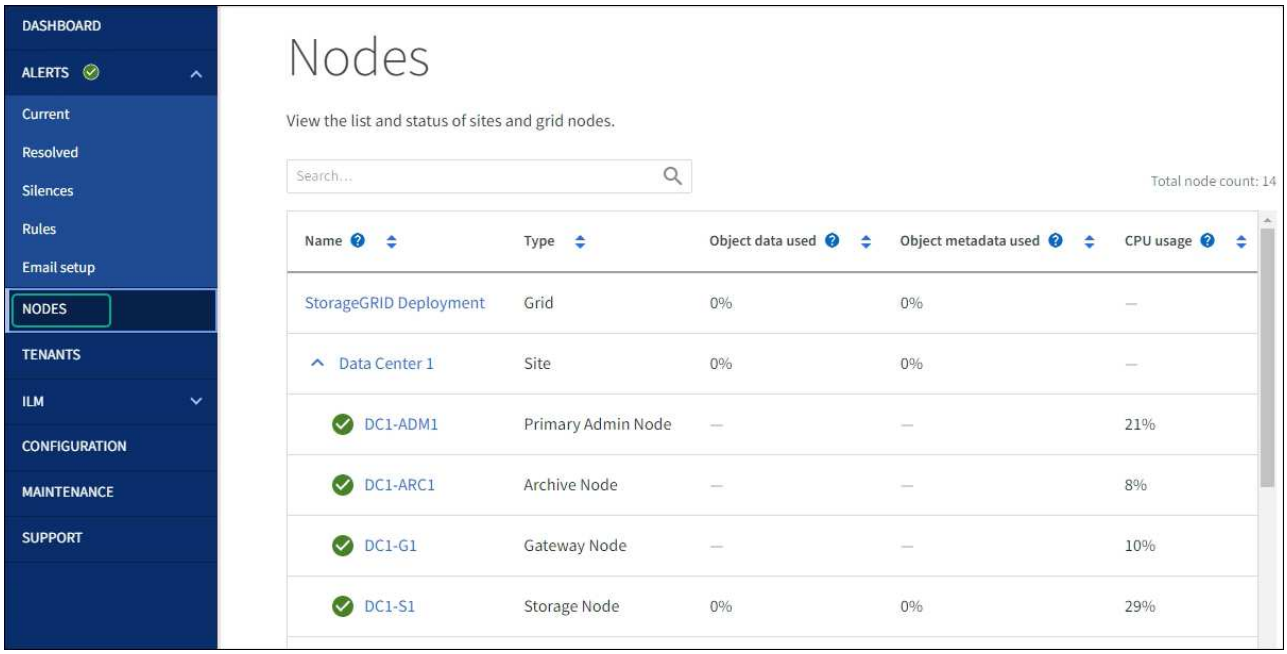
5. Select **Configure Networking** > **Ping Test** from the menu.
6. Use the Ping Test tool to check connectivity to IP addresses on any networks that might have been affected by the link configuration changes you made when configuring the appliance.

   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 node. If necessary, return to the instructions for configuring network links, and correct any issues.

7. Once 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. (This option is available only when the controller is 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** page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Hardware procedures

Replace one or both power supplies in the SG100 or SG1000

The services appliance 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. Both power supplies operating in the controller must be the same model and wattage.

Before you begin

- You have physically located the controller with the power supply to be replaced.
- If you are replacing only one power supply:
  - You have unpacked the replacement power supply unit and ensured that it is the same model and wattage as the power supply unit you are replacing.
  - You have confirmed that the other power supply is installed and running.
- If you are replacing both power supplies at the same time:
  - You have unpacked the replacement power supply units and ensured they are the same model and wattage.

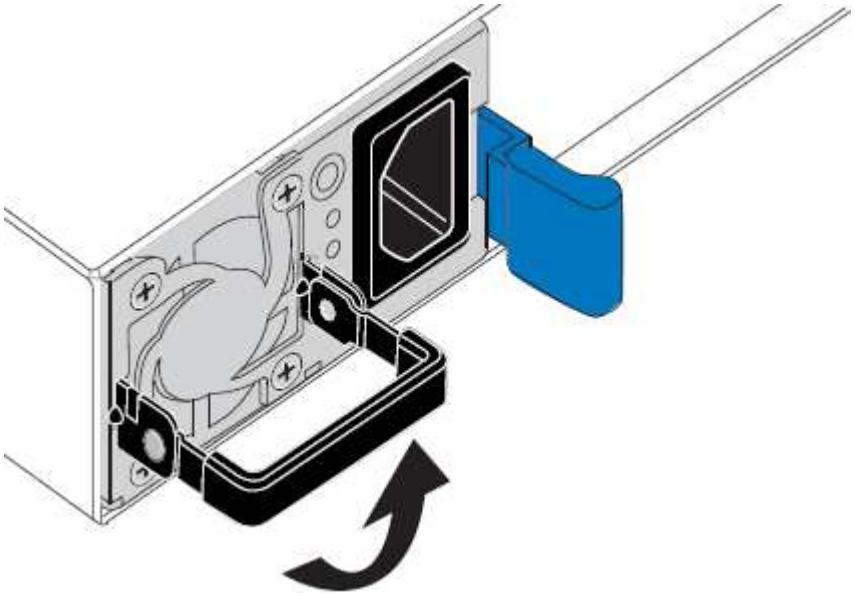
About this task

The figure shows the two power supply units for the SG100, which are accessible from the back of the appliance.

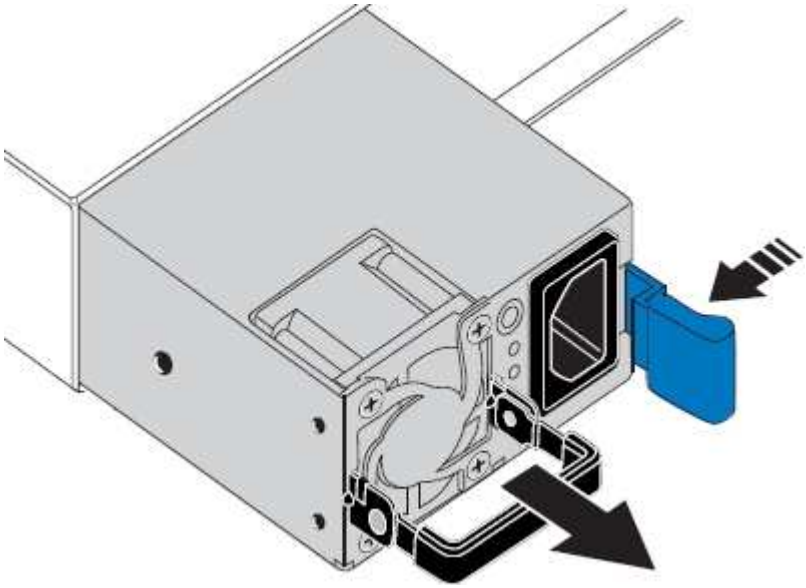
The power supplies for the SG1000 are identical.

Steps

1. If you are replacing only one power supply, you don't need to shut down the appliance. Go to the Unplug the power cord step. If you are replacing both power supplies at the same time, do the following before unplugging the power cords:
   a. Shut down the appliance.
2. Unplug the power cord from each power supply to be replaced.
3. Lift the cam handle on the first supply to be replaced.



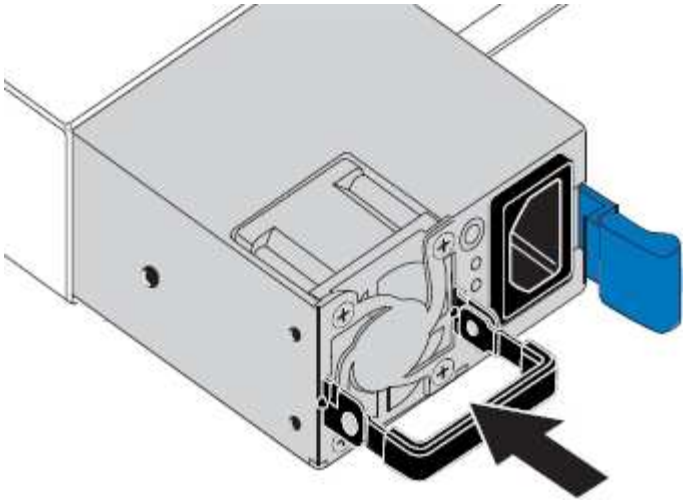
4. Press the blue latch and pull the power supply out.



5. With the blue latch on the right, slide the replacement power supply into the chassis.

   Both power supplies must be the same model and wattage.

   Ensure that the blue latch is on the right side when you slide the replacement unit in.



6. Push the cam handle down to secure the replacement power supply.
7. If you are replacing both power supplies, repeat steps 2 though 6 to replace the second power supply.
8. Connect the power cords to the replaced units and apply power.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace fan in SG100 or SG1000

The services appliance has eight cooling fans. If one of the fans fails, you must replace it as soon as possible to ensure that the appliance has proper cooling.

Before you begin

- You have unpacked the replacement fan.
- You have physically located the appliance.
- You have confirmed that the other fans are installed and running.

About this task

The appliance node will not be accessible while you replace the fan.

The photograph shows a fan for the services appliance. The cooling fans are accessible after you take the top cover off the appliance.

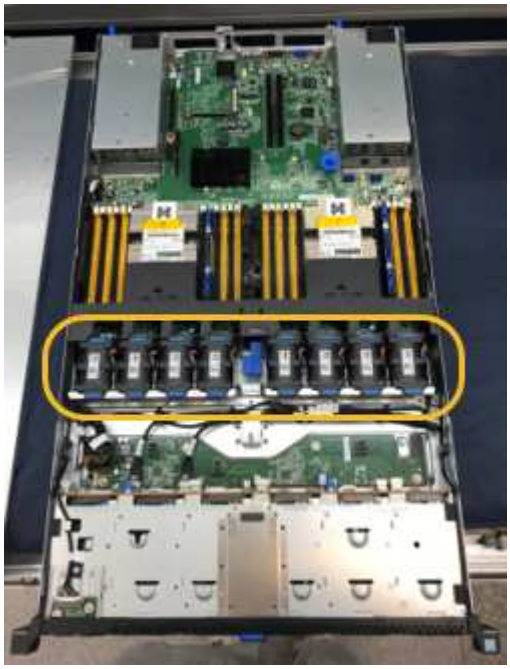
> Each of the two power supply units also contain a fan. Those fans aren't included in this procedure.

Steps

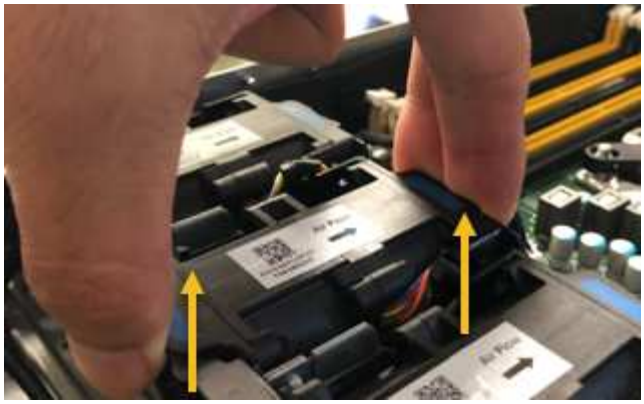
1. Shut down the appliance.
   a. Log in to the grid node:
      i. Enter the following command: `ssh admin@grid_node_IP`
      ii. Enter the password listed in the `Passwords.txt` file.
      iii. Enter the following command to switch to root: `su -`
      iv. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

   b. Shut down the services appliance:
      `shutdown -h now`
2. Use one of two methods to verify that the power for the services appliance is off:
   - The power indicator LED on the front of the appliance is off.
   - The Power Control page of the BMC interface indicates that the appliance is off.
3. Pull the appliance out of the rack.
4. Lift the latch on the top cover and remove the cover from the appliance.
5. Locate the fan that failed.

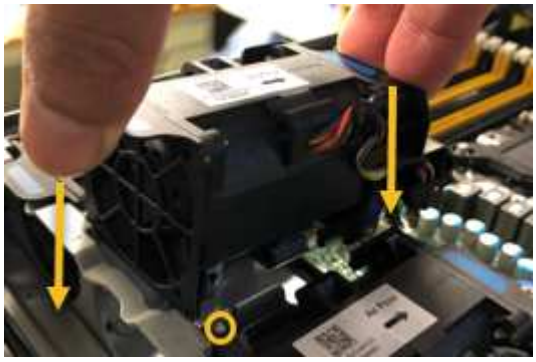


6. Lift the failed fan out of the chassis.

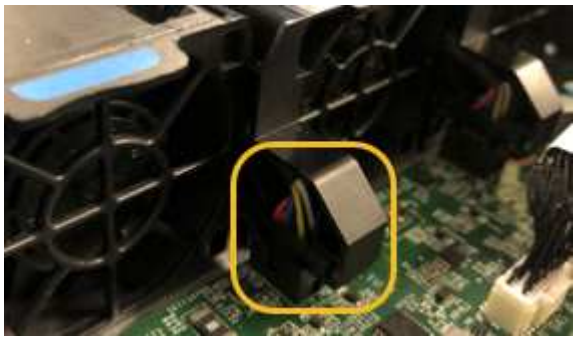


7. Slide the replacement fan into the open slot in the chassis.

   Line up the edge of the fan with the guide pin. The pin is circled in the photograph.



8. Press the fan's connector firmly into the circuit board.



9. Put the top cover back on the appliance, and press the latch down to secure the cover in place.
10. Power on the appliance and monitor the controller LEDs and boot-up codes.

    Use the BMC interface to monitor boot-up status.

11. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace drive in SG100 or SG1000

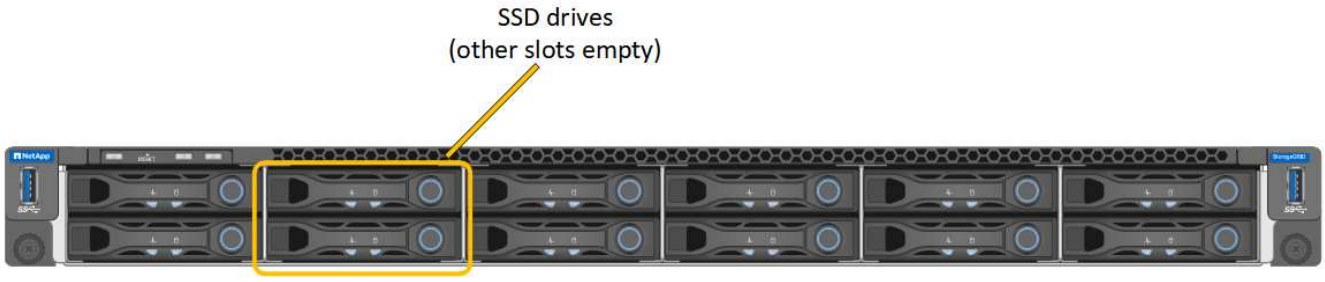
The SSDs in the services appliance contain the StorageGRID operating system. Additionally, when the appliance is configured as an Admin Node, the SSDs also contain

audit logs, metrics, and database tables. The drives are mirrored using RAID1 for redundancy. If one of the drives fails, you must replace it as soon as possible to ensure redundancy.

Before you begin

- You have physically located the appliance.
- You have verified which drive has failed by noting that its left LED is blinking amber.

  The two SSDs are placed in the slots as shown in the following diagram:



> If you remove the working drive, you will bring down the appliance node. See the information about viewing status indicators to verify the failure.

- You have obtained the replacement drive.
- You have obtained proper ESD protection.

Steps

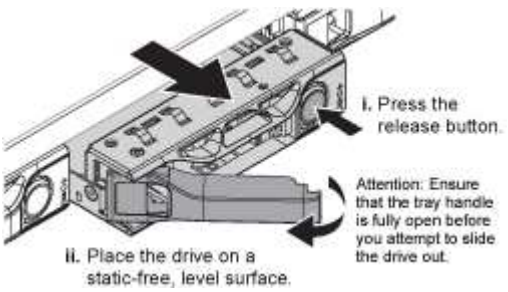
1. Verify that the drive to be replaced has the left LED blinking amber. If a drive issue was reported in the Grid Manager or BMC UIs, HDD02 or HDD2 refer to the drive in the upper slot, and HDD03 or HDD3 refer to the drive in the lower slot.

   You can also use the Grid Manager to monitor the status of the SSDs. Select **NODES**. Then select **`Appliance Node`** > **Hardware**. If a drive has failed, the Storage RAID Mode field contains a message about which drive has failed.

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. Unpack the replacement drive, and set it on a static-free, level surface near the appliance.

   Save all packing materials.

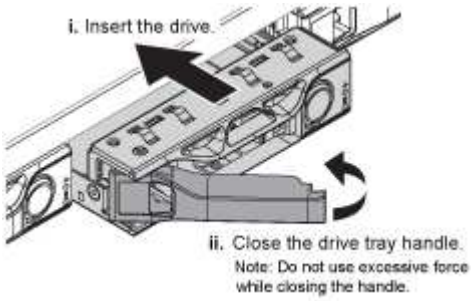
4. Press the release button on the failed drive.



   The handle on the drive springs open partially, and the drive releases from the slot.

5. Open the handle, slide the drive out, and place it on a static-free, level surface.
6. Press the release button on the replacement drive before you insert it into the drive slot.

   The latch springs open.



7. Insert the replacement drive in the slot, and then close the drive handle.

   Don’t use excessive force while closing the handle.

   When the drive is fully inserted, you hear a click.

   The drive is automatically rebuilt with mirrored data from the working drive. You can check the status of the rebuild by using the Grid Manager. Select **NODES**. Then select **`Appliance Node`** > **Hardware**. The Storage RAID Mode field contains a “rebuilding” message until the drive is completely rebuilt.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace an SG100 or SG1000

You might need to replace the appliance if it is not functioning optimally or if it has failed.

Before you begin

- You have a replacement appliance with the same part number as the appliance you are replacing.
- You have labels to identify each cable that is connected to the appliance.
- You have physically located the appliance.

About this task

The StorageGRID node will not be accessible while you replace the appliance. If the appliance is functioning sufficiently, you can perform a controlled shutdown at the start of this procedure.

If you are replacing the appliance 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 can’t access it from hosts on other subnets. This condition should resolve itself within 15 minutes (when any ARP cache entries for the original appliance 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. Display the current configurations of the appliance and record them.

a. Log in to the appliance to be replaced:

   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: **`run-host-command ipmitool lan print`** to display the current BMC configurations for the appliance.

2. Shut down the appliance: `shutdown -h now`

3. If any of the network interfaces on this StorageGRID appliance are configured for DHCP, you might need to update the permanent DHCP lease assignments on the DHCP servers to reference the MAC addresses of the replacement appliance. The update ensures the appliance is assigned the expected IP addresses. See Update MAC address references.

4. Remove and replace the appliance:

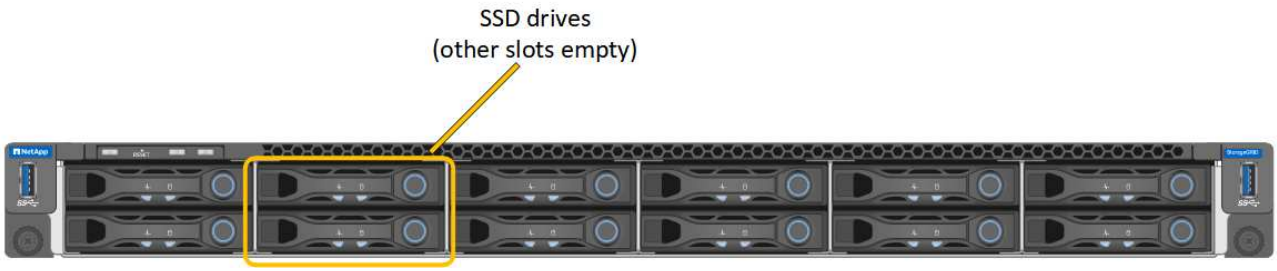
   a. Label the cables and then disconnect the cables and any network transceivers.

   To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

   b. Remove the failed appliance from the cabinet or rack.

   c. Transfer the two power supplies, eight cooling fans, and two SSDs from the failed appliance to the replacement appliance.

   The two SSDs are placed in the slots as shown in the following diagram:



   HDD02 or HDD2 refer to the drive in the upper slot, and HDD03 or HDD3 refer to the drive in the lower slot.

   Follow the instructions provided for replacing these components.

   d. Install the replacement appliance into the cabinet or rack.

   e. Replace the cables and any optical transceivers.

   f. Power on the appliance and wait for it to rejoin the grid.

   g. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

5. Log in to the replaced appliance:

   a. Enter the following command: `ssh admin@grid_node_IP`

b. Enter the password listed in the `Passwords.txt` file.

c. Enter the following command to switch to root: `su -`

d. Enter the password listed in the `Passwords.txt` file.

6. Restore BMC network connectivity for the replaced appliance. There are two options:
   - Use static IP, netmask, and gateway
   - Use DHCP to obtain an IP, netmask, and gateway

   a. To restore the BMC configuration to use a static IP, netmask, and gateway, enter the following commands:

   ```
   run-host-command ipmitool lan set 1 ipsrc static

   run-host-command ipmitool lan set 1 ipaddr Appliance_IP

   run-host-command ipmitool lan set 1 netmask Netmask_IP

   run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
   ```

   b. To restore the BMC configuration to use DHCP to obtain an IP, netmask, and gateway, enter the following command:

   ```
   run-host-command ipmitool lan set 1 ipsrc dhcp
   ```

7. After restoring BMC network connectivity, connect to the BMC interface to audit and restore any additional custom BMC configuration you might have applied. For example, you should confirm the settings for SNMP trap destinations and email notifications. See Configure BMC interface.
8. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Related information

View status indicators

View boot-up codes for appliance

Maintain SG5600 hardware

Maintain SG5600 appliance

The SG5600 appliance has reached End Of Support. Contact your NetApp Sales Representative for hardware refresh options.

If you need to perform maintenance procedures on SG5600 hardware, use the StorageGRID 11.6 instructions.

Maintain SG5700 storage appliance hardware

Maintain SG5700 appliance

You might need to upgrade the SANtricity OS Software on the E2800 controller, change the Ethernet link configuration of the E5700SG controller, replace the E2800 controller or the E5700SG controller, or replace specific components. The procedures in this section assume that the appliance has already been deployed as a Storage Node in a StorageGRID system.

Procedures specific to maintaining your SG5700 appliance are in this section.

See Common procedures for maintenance procedures that are used by all appliances.

See Set up hardware for maintenance procedures that are also performed during initial appliance installation and configuration.

Maintenance configuration procedures

Upgrade SANtricity OS on SG5700 storage controller

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.

Download the new SANtricity OS Software file from NetApp Downloads: StorageGRID Appliance.

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.

  Upgrade SANtricity OS on storage controllers using 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.

  Upgrade SANtricity OS on E2800 controller using maintenance mode

Upgrade SANtricity OS on SG5700 storage controllers using 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.

Before you begin

- 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 have the Maintenance or Root access permission.
- You are signed in to the Grid Manager using a supported web browser.
- You have the provisioning passphrase.

- You have access to NetApp Downloads: StorageGRID Appliance.

About this task

You can't 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 that have been selected for the upgrade. It might take more than 30 minutes to load the SANtricity OS on each node (sequentially) and up to 90 minutes to reboot each StorageGRID storage appliance. Any nodes in your grid that don't use SANtricity OS will not be affected by this procedure.

The following steps are only applicable when you are using the Grid Manager to perform the upgrade. The storage controllers in the appliance can't 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 don't need to apply a separate NVSRAM upgrade file.

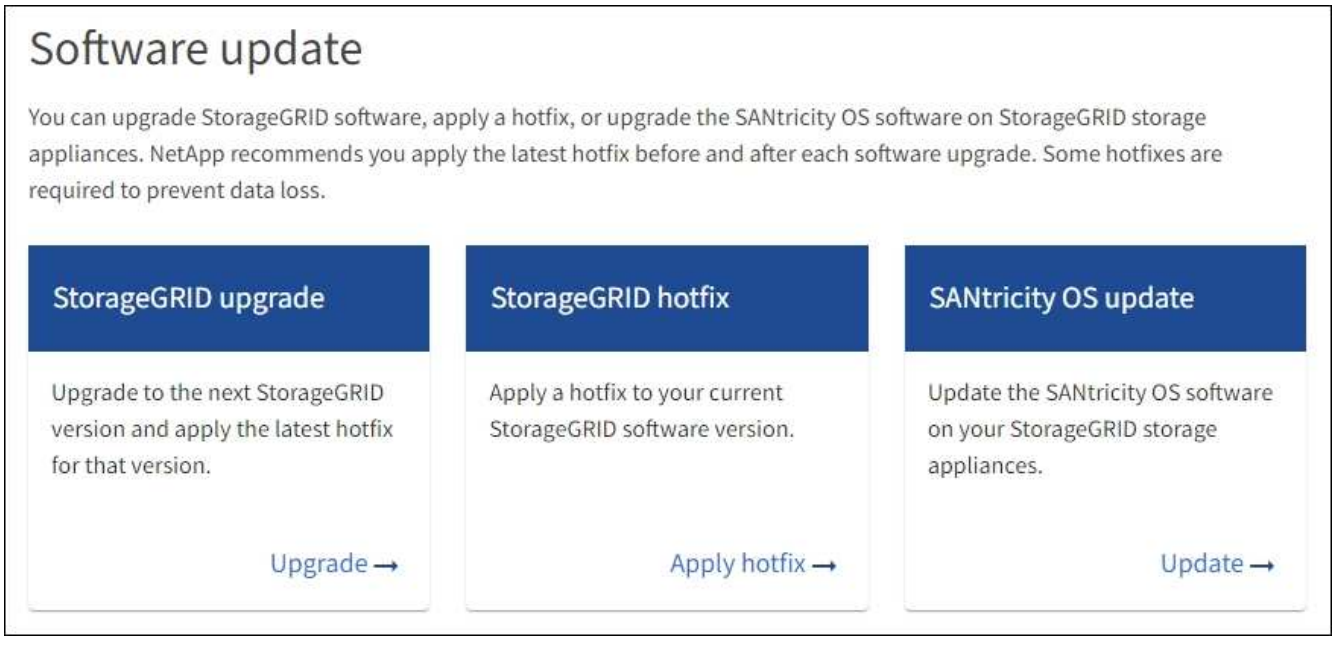
Be sure to apply the latest StorageGRID hotfix before you begin this procedure. See StorageGRID hotfix procedure for details.

Steps

1. Download the new SANtricity OS Software file from NetApp Downloads: StorageGRID Appliance.

   Be sure to choose the SANtricity OS version for your storage controllers.

2. Select **MAINTENANCE** > **System** > **Software update**.



3. In the SANtricity OS update section, select **Update**.

   The SANtricity OS upgrade page appears and lists the details for each appliance node including:

- Node name
- Site
- Appliance model
- SANtricity OS version
- Status
- Last upgrade status

4. Review the information in the table for all of your upgradable appliances. Confirm that all storage controllers have **Nominal** status. If the status for any controller is **Unknown**, go to **Nodes** > ***appliance node*** > **Hardware** to investigate and resolve the issue.
5. Select the SANtricity OS upgrade file you downloaded from the NetApp Support Site.

   a. Select **Browse**.
   b. Locate and select the file.
   c. Select **Open**.

   The file is uploaded and validated. When the validation process is done, the file name is shown with a green check mark next to the **Browse** button. Don't change the file name because it is part of the verification process.

6. Enter the provisioning passphrase and select **Continue**.

   A warning box appears stating that your browser's connection might be lost temporarily as services on nodes that are upgraded are restarted.

7. Select **Yes** to stage the SANtricity OS upgrade file to the primary Admin Node.

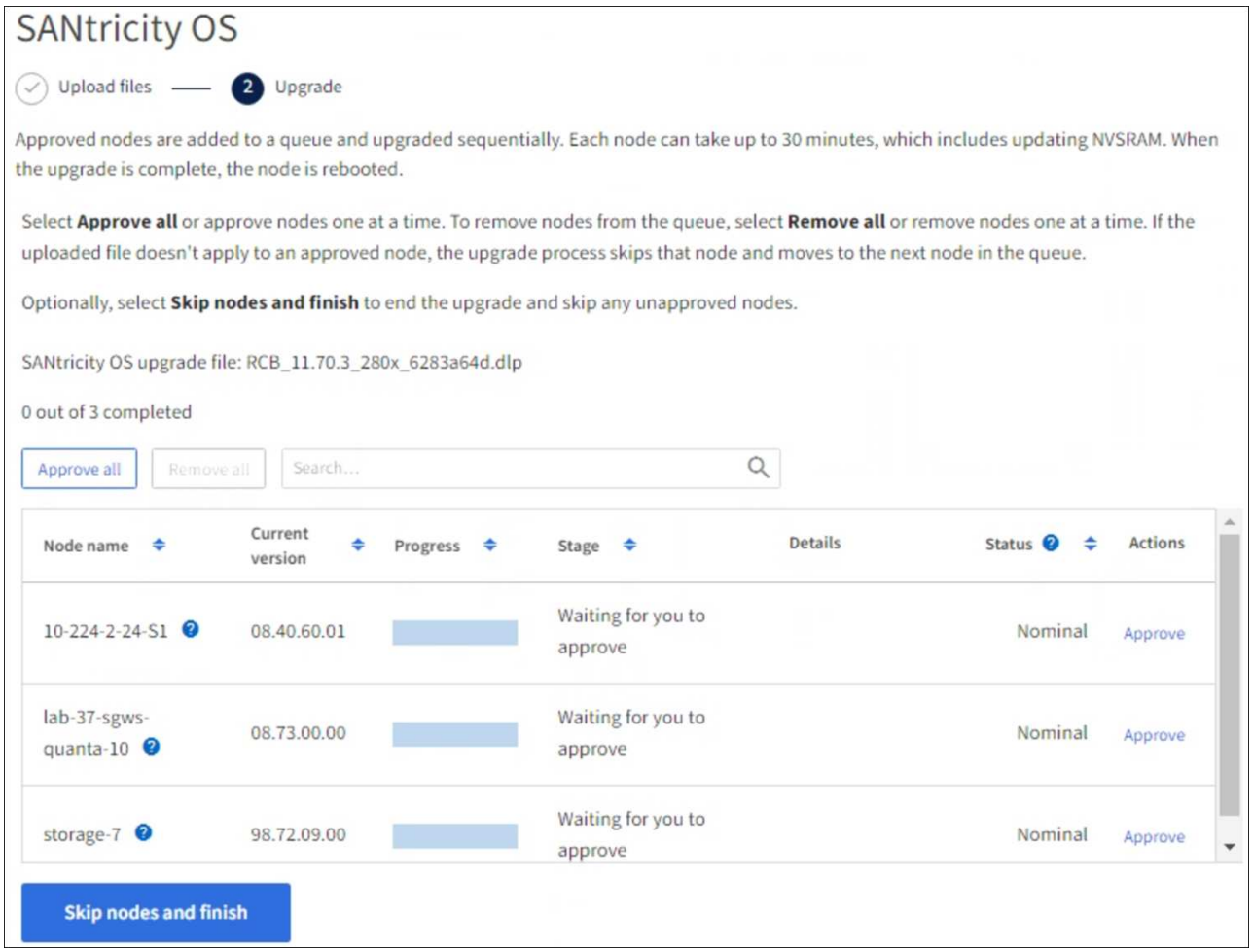
   When the SANtricity OS upgrade starts:

   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 select **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 appliance Storage Nodes. Software-based Storage Nodes aren't displayed. Select **Approve** for all nodes that require the upgrade.



8. Optionally, sort the list of nodes in ascending or descending order by:
   - Node name
   - Current version
   - Progress
   - Stage
   - Status

   You can also enter a term in the Search box to search for specific nodes.

9. Approve the grid nodes you are ready to add to the upgrade queue. Approved nodes are upgraded one at a time.

   > Don’t 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 and the upgrade process begins. Later, when the node is finished upgrading, the appliance node is rebooted. These operations might cause service interruptions for clients that are communicating with the node.

   - Select the **Approve All** button 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.

- Select one or more **Approve** buttons to add one or more nodes to the SANtricity OS upgrade queue. The **Approve** button is disabled if the Status is not Nominal.

  After you select **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. Nodes intentionally not upgraded show a stage of Complete (upgrade attempted) and list the reason the node was not upgraded in the Details column.

10. If you need to remove a node or all nodes from the SANtricity OS upgrade queue, select **Remove** or **Remove All**.

    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.

11. 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 applied, the upgrade has failed for the node. With the assistance of technical support, you might need to place the appliance in maintenance mode to recover it.
    - 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 that you must use maintenance mode to upgrade SANtricity OS on the node. To resolve the error, do the following:
      a. Use maintenance mode to upgrade SANtricity OS on the node that shows a stage of Error.
      b. Use the Grid Manager to restart 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 number of nodes upgraded, and the date and time the upgrade completed.

12. If a node can't be upgraded, note the reason shown in the Details column and take the appropriate action.

    The SANtricity OS upgrade process will not be complete until you approve the SANtricity OS upgrade on all the listed Storage Nodes.

Reason	Recommended action
Storage Node was already upgraded.	No further action required.
SANtricity OS upgrade is not applicable to this node.	The node does not have a storage controller that can be managed by the StorageGRID system. Complete the upgrade process without upgrading the node displaying this message.

Reason	Recommended action
SANtricity OS file is not compatible with this node.	The node requires a SANtricity OS file different than the one you selected. After completing the current upgrade, download the correct SANtricity OS file for the node and repeat the upgrade process.

13. If you want to end approving nodes and return to the SANtricity OS page to allow for an upload of a new SANtricity OS file, do the following:
    a. Select **Skip Nodes and Finish**.

       A warning appears asking if you are sure you want to finish the upgrade process without upgrading all applicable nodes.

    b. Select **OK** to return to the **SANtricity OS** page.
    c. When you are ready to continue approving nodes, download the SANtricity OS to restart the upgrade process.

       Nodes already approved and upgraded without errors remain upgraded.

14. 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

Upgrade SANtricity OS on E2800 controller using maintenance mode

Upgrade SANtricity OS on E2800 controller 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.

Before you begin

- 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 place the E5700SG controller into maintenance mode, which interrupts the connection to the E2800 controller.

  In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

About this task

Don’t 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. Confirm the appliance is in maintenance mode.
2. From a service laptop, access SANtricity System Manager and sign in.
3. Download the new SANtricity OS Software file and NVSRAM file to the management client.

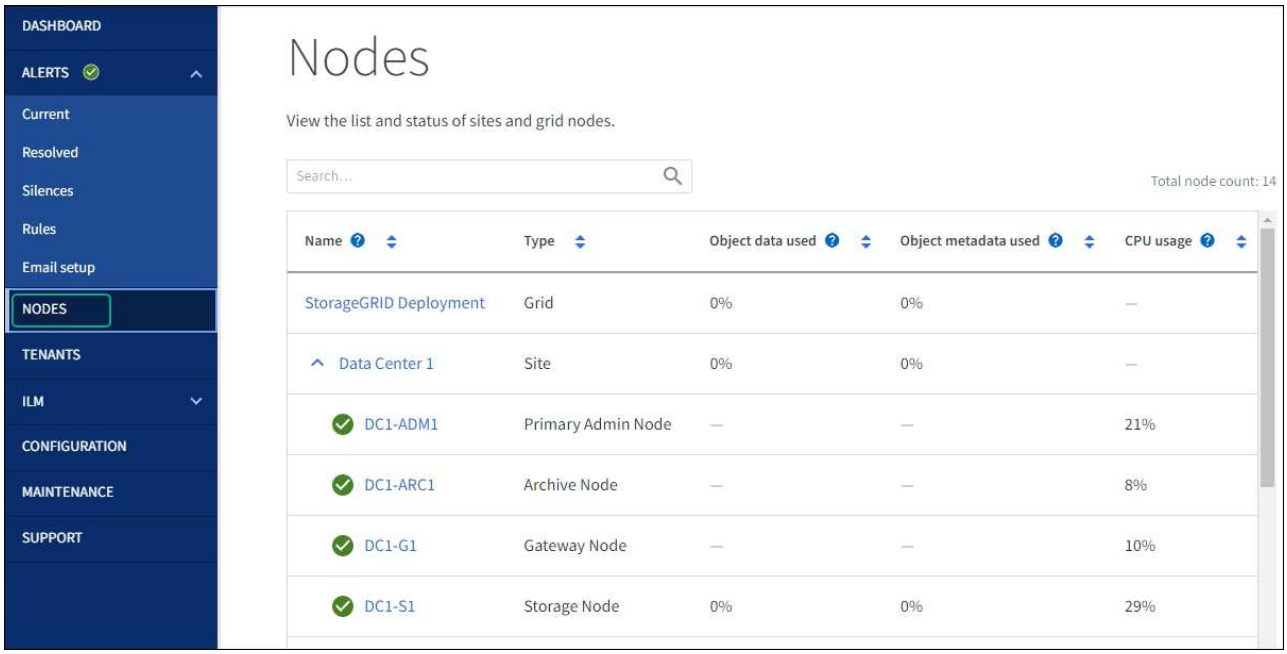
   The NVSRAM is specific to the StorageGRID appliance. Don't use the standard NVSRAM download.

4. Follow the instructions in the *E2800 and E5700 SANtricity Software and Firmware Upgrade Guide* or the SANtricity System Manager online help to upgrade the E2800 controller's firmware and NVSRAM.

   Activate the upgrade files immediately. Don't defer activation.

5. If this procedure completed successfully and you have additional procedures to perform while the node is in maintenance mode, perform them now. When you are done, or if you experienced any failures and want to start over, select **Advanced** > **Reboot Controller**, and then select one of these options:
   - Select **Reboot into StorageGRID**
   - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if you experienced any failures during the procedure and want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.

   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 page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Related information

Upgrade SANtricity OS on storage controllers using Grid Manager

Upgrade drive firmware using SANtricity System Manager

Upgrade SG5700 drive firmware using SANtricity System Manager online method

Use the SANtricity System Manager online method to upgrade the firmware on the drives in your appliance to make sure you have all the latest features and bug fixes.

Before you begin

- The storage appliance has an Optimal status.
- All drives have an Optimal status.

> Don't 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 policy.

About this task

The drives are upgraded one at a time while the appliance is performing I/O. This method does not require you to place the appliance in maintenance mode. However, system performance might be impacted and the upgrade might take several hours longer than the offline method.

> Drives belonging to volumes that don't have redundancy must be updated using the offline method. The offline method should be used for any drive associated with flash read cache, or any pool or volume group that is currently degraded.
>
> You must use the offline method when upgrading SSD drives.

Steps

1. Access SANtricity System Manager using one of these methods:
   - Use the StorageGRID Appliance Installer and select **Advanced** > **SANtricity System Manager**

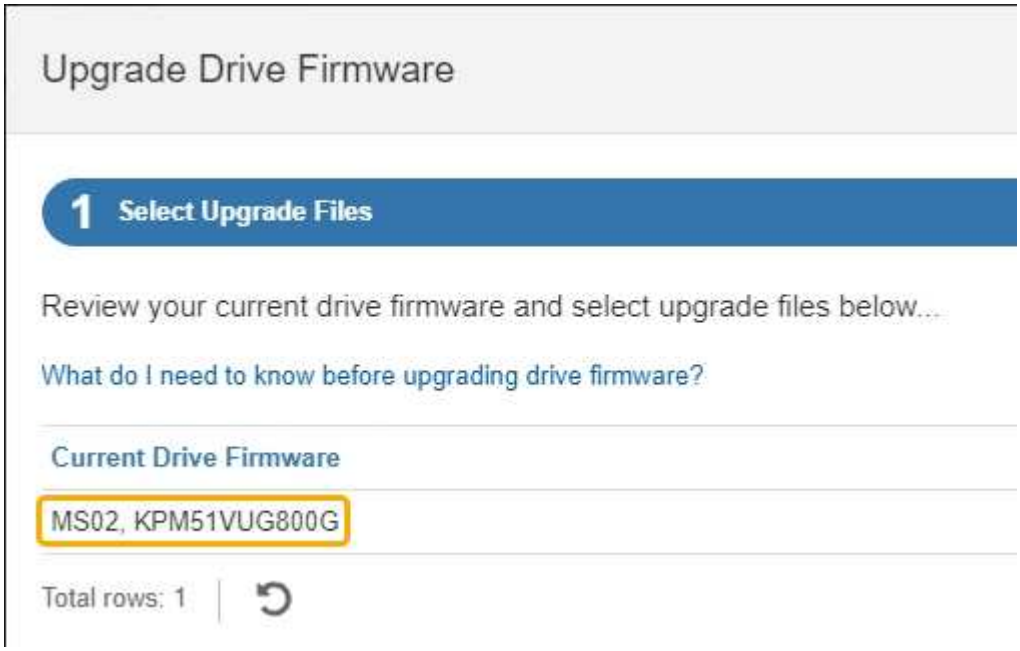
- Use the Grid Manager and select **NODES** > ***Storage Node*** > **SANtricity System Manager**
- Use SANtricity System Manager by browsing to the storage controller IP:

  `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 page displays the drive firmware files currently installed.

   c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.



      In this example:

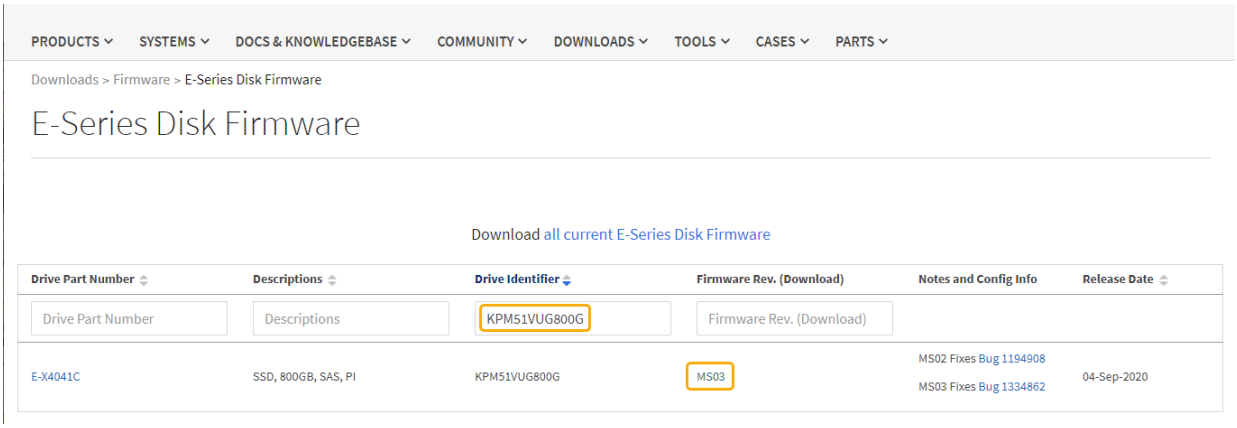
      - The drive firmware revision is **MS02**.
      - The drive identifier is **KPM51VUG800G**.

   d. Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.
   e. Close the Upgrade Drive Firmware window.
4. Download and prepare the available drive firmware upgrade:
   a. Under Drive Firmware upgrade, select **NetApp Support**.
   b. On the NetApp Support Site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

      The E-Series Disk Firmware page displays.

   c. 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.



d. 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.

e. Extract (unzip) the drive firmware archive files you downloaded from the Support site.

5. Install the drive firmware upgrade:

a. From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.

b. 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.

c. 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 the **Proposed Firmware** column. If you must change this firmware, select **Back**.

d. Select **Upgrade all drives online** — Upgrades the drives that can support a firmware download while the storage array is processing I/O. You don't have to stop I/O to the associated volumes using these drives when you select this upgrade method.

> An online upgrade can take several hours longer than an offline upgrade.

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 required, troubleshoot driver firmware upgrade errors.

Upgrade SG5700 drive firmware using SANtricity System Manager using offline method

Use the SANtricity System Manager online method to upgrade the firmware on the drives in your appliance to make sure you have all the latest features and bug fixes.

Before you begin

- The storage appliance has an Optimal status.
- All drives have an Optimal status.
- You have placed the StorageGRID appliance into maintenance mode.

> While the appliance is in maintenance mode, I/O (input/output) activity to the storage controller is stopped to make disruptive storage operations safe.

> Don’t 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 policy.

About this task

The drives are upgraded in parallel while the appliance is in maintenance mode. If the pool or volume group does not support redundancy or is degraded, you must use the offline method to upgrade the drive firmware. You should also use the offline method for any drive associated with flash read cache, or any pool or volume group that is currently degraded. The offline method upgrades firmware only while all I/O activity is stopped on the drives to be upgraded. To stop I/O activity, place the node into maintenance mode.

The offline method is faster than the online method and will be significantly faster when many drives in a single appliance need upgrades. However, it requires that nodes be taken out of service, which might require scheduling a maintenance window and monitoring progress. Choose the method that is the best fit for your operational procedures and the number of drives that need to be upgraded.

Steps

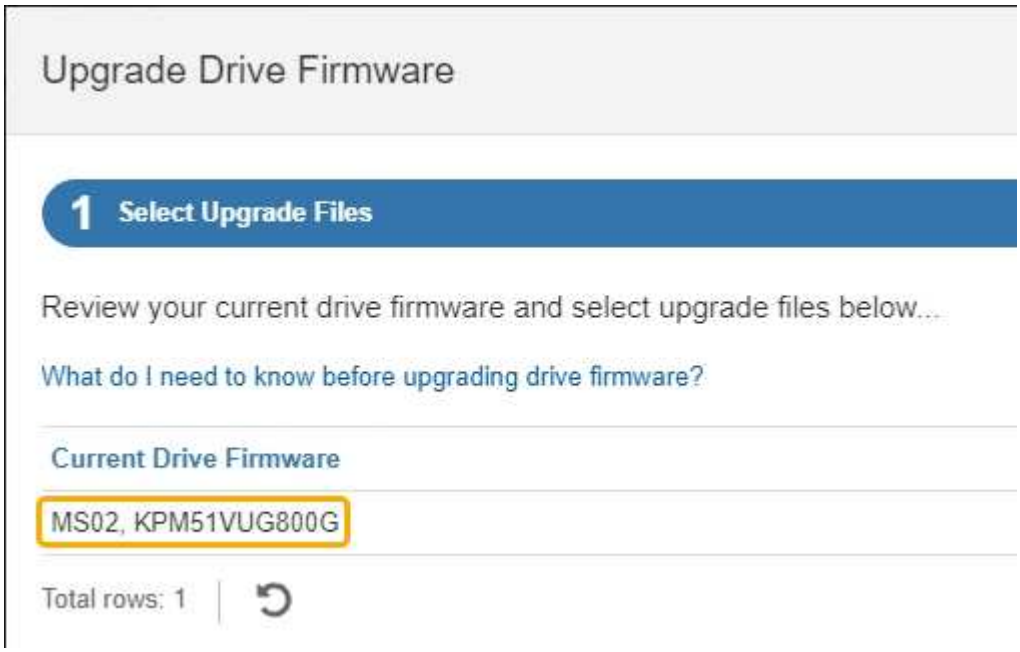
1. Confirm that the appliance is in maintenance mode.
2. Access SANtricity System Manager using one of these methods:
   - Use the StorageGRID Appliance Installer and select **Advanced** > **SANtricity System Manager**
   - Use the Grid Manager and select **NODES** > ***Storage Node*** > **SANtricity System Manager**
   - Use SANtricity System Manager by browsing to the storage controller IP:

     `https://Storage_Controller_IP`

3. Enter the SANtricity System Manager administrator username and password, if required.
4. 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 page displays the drive firmware files currently installed.

   c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.



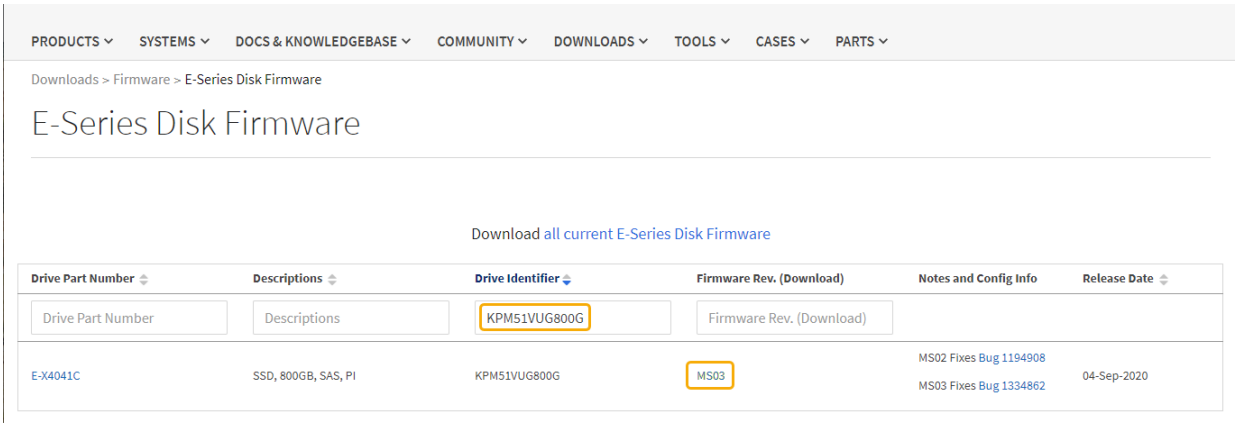
      In this example:

      - The drive firmware revision is **MS02**.
      - The drive identifier is **KPM51VUG800G**.

   d. Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.
   e. Close the Upgrade Drive Firmware window.
5. Download and prepare the available drive firmware upgrade:
   a. Under Drive Firmware upgrade, select **NetApp Support**.
   b. On the NetApp Support Site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

      The E-Series Disk Firmware page displays.

   c. 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.



d. 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.

e. Extract (unzip) the drive firmware archive files you downloaded from the Support site.

6. Install the drive firmware upgrade:

a. From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.

b. 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.

c. 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 the **Proposed Firmware** column. If you must change this firmware, select **Back**.

d. Select **Upgrade all drives offline (parallel)** — Upgrades the drives that can support a firmware download only while all I/O activity is stopped on any volumes that use the drives.

You must place the appliance into maintenance mode before using this method. You should use the **Offline** method to upgrade the drive firmware.

If you want to use the Offline (parallel) upgrade, don't proceed unless you are certain that the appliance is in maintenance mode. Failure to place the appliance into maintenance mode before initiating an offline drive firmware update might cause data loss.

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.

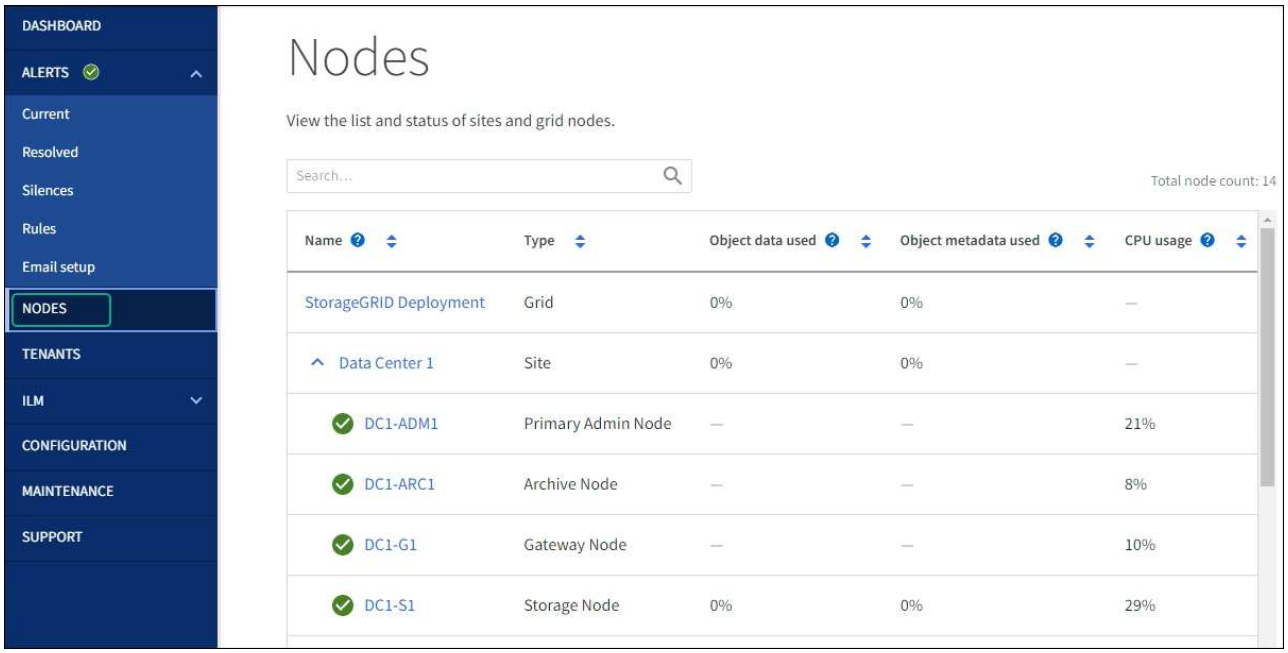
g. (Optional) To see a list of what was upgraded, select **Save Log**.

The log file is saved in the downloads folder for your browser with the name `latest-upgrade-log-timestamp.txt`.

If required, troubleshoot driver firmware upgrade errors.

7. After the procedure completes successfully, perform any additional maintenance procedures while the node is in maintenance mode. When you are done, or if you experienced any failures and want to start over, go to the StorageGRID Appliance Installer and select **Advanced** > **Reboot Controller**. Then select one of these options:
   - **Reboot into StorageGRID**.
   - **Reboot into Maintenance Mode**. Reboot the controller and keep the node in maintenance mode. Select this option if there were any failures during the procedure and you want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.

   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 page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Troubleshoot drive firmware upgrade errors

Troubleshoot errors that can occur when using SANtricity System Manager to upgrade the firmware on the drives in your appliance.

- **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 aren't 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.

Change link configuration of E5700SG controller

You can change the Ethernet link configuration of the E5700SG controller. You can change the port bond mode, the network bond mode, and the link speed.

Before you begin

Place E5700SG controller into maintenance mode.

> In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

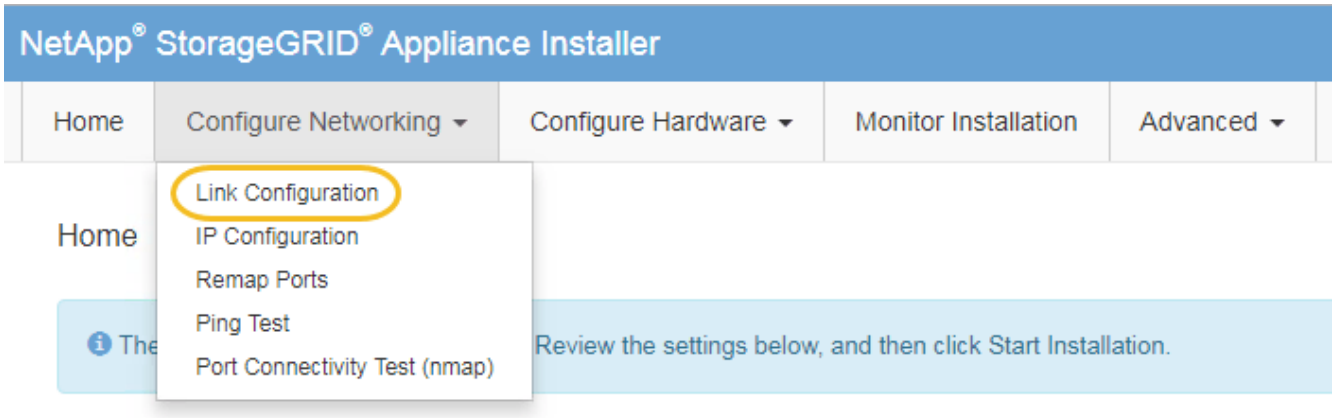
About this task

Options for changing the Ethernet link configuration of the E5700SG 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 from 10-GbE to 25-GbE, or from 25-GbE to 10-GbE

Steps

1. Select **Configure Networking** > **Link Configuration** from the menu.



2. Make the desired changes to the link configuration.

   For more information about the options, see Configure network links.

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 aren't 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://E5700SG_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 configure StorageGRID IP addresses instructions.

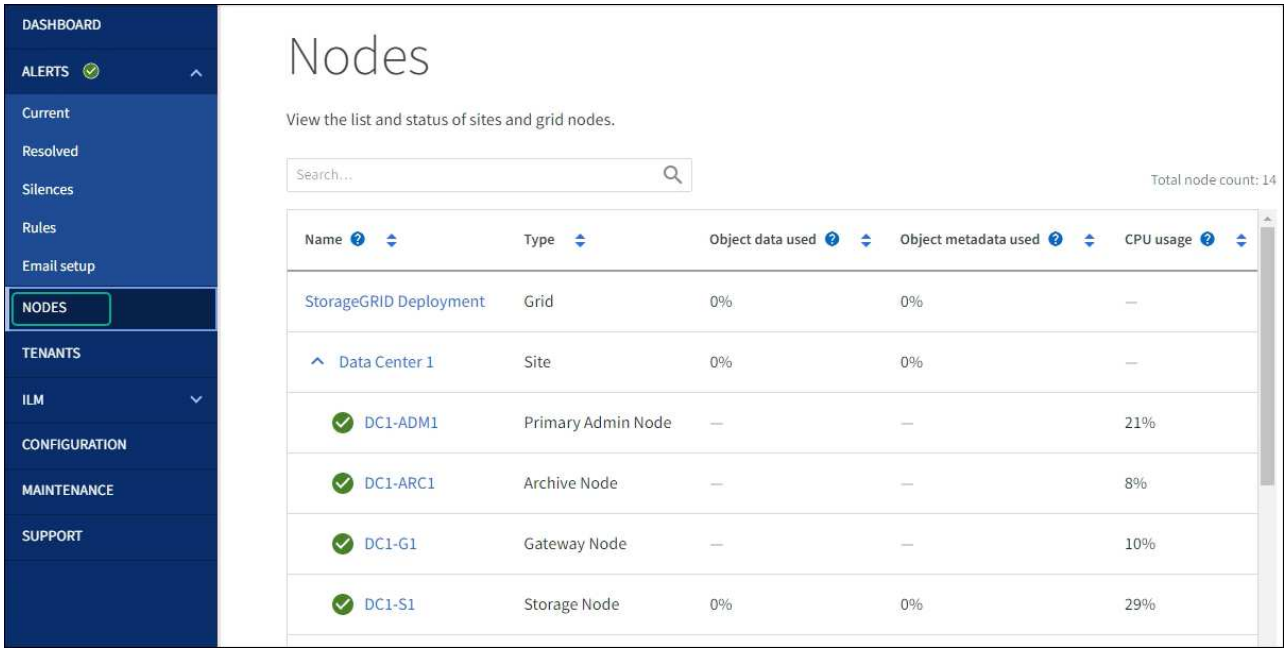
4. From the StorageGRID Appliance Installer, select **Configure Networking** > **Ping Test**.
5. Use the Ping Test tool to check connectivity to IP addresses on any networks that might have been affected by the link configuration changes you made in the Change link configuration step.

   In addition to any other tests you choose to perform, confirm that you can ping the grid IP address of the primary Admin Node, and the grid IP address of at least one other Storage Node. If necessary, correct any link configuration issues.

6. Once 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. (This option is available only when the controller is 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** page should display a normal status (green check mark icon to the left of the node name) for the

appliance node, indicating that no alerts are active and the node is connected to the grid.



Hardware procedures

Replace E2800 series storage controller in the SG5700

You might need to replace the E2800 series controller if it is not functioning optimally or if it has failed.

Before you begin

- You have a replacement controller with the same part number as the controller you are replacing.

> Don’t rely on the E-Series instructions to replace a controller in the StorageGRID appliance, because the procedures aren’t the same.

- You have labels to identify each cable that is connected to the controller.
- If all drives are secured, you have reviewed the steps in the simplex E2800 series controller replacement procedure, which include downloading and installing E-Series SANtricity System Manager from the NetApp Support Site and then using the Enterprise Management Window (EMW) to unlock the secured drives after you have replaced the controller.

> You will not be able to use the appliance until you unlock the drives with the saved key.

- You must have specific access permissions.
- You must be signed in to the Grid Manager using a supported web browser.

About this task

You can determine if you have a failed controller canister 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.

The appliance Storage Node will not be accessible when you replace the controller. If the E2800 series controller is functioning sufficiently, you can place the E5700SG controller into maintenance mode.

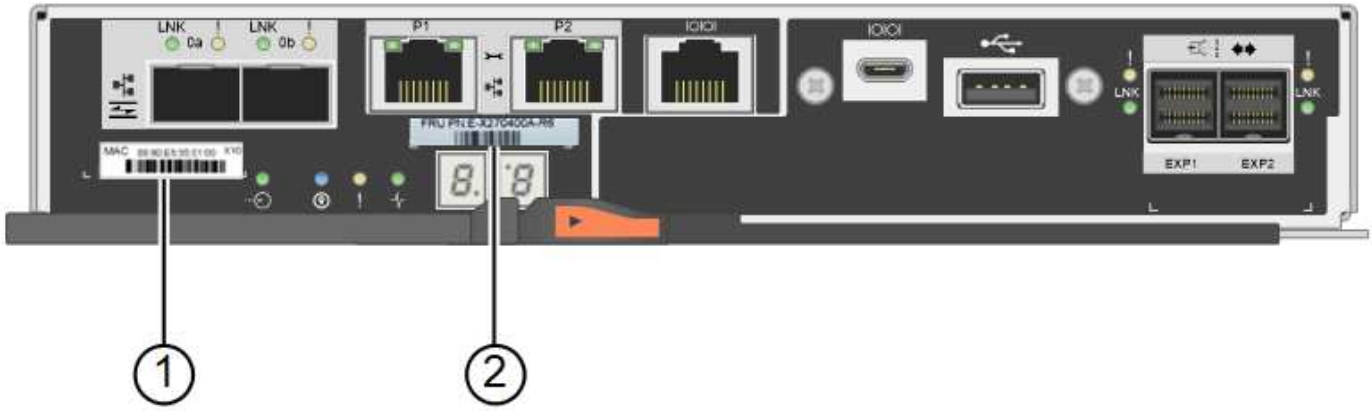
When you replace a controller, you must remove the battery from the original controller and install it in the replacement controller. In some cases, you might also need to remove the host interface card from the original controller and install it in the replacement controller.

The storage controllers in most appliance models don't include host interface cards (HIC).

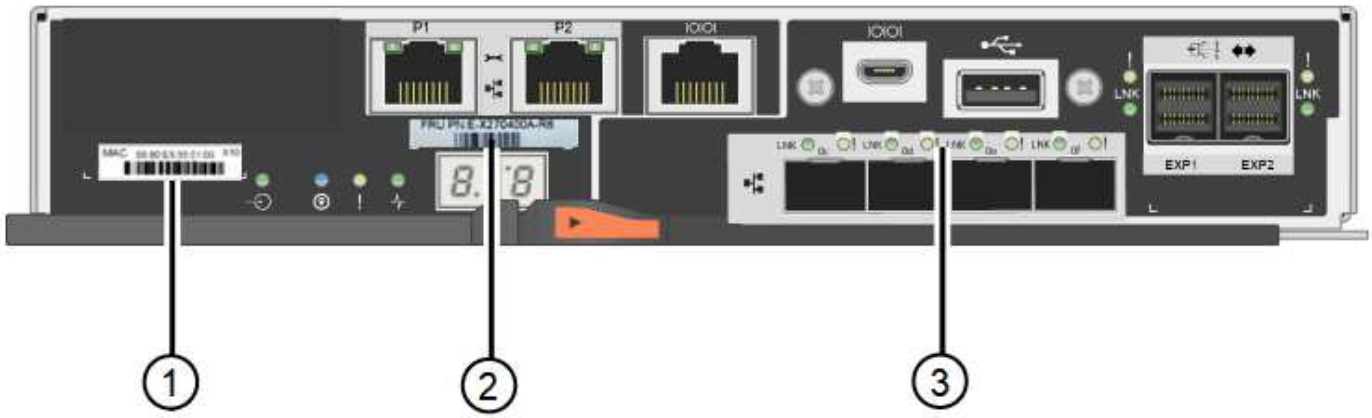
Step 1: Prepare to remove the controller

These figures show the E2800A controller and the E2800B controller. The procedure for replacing the E2800 series controllers and the EF570 controller is identical.

E2800A storage controller:



E2800B storage controller:



Label	component	Description
1	MAC address	The MAC address for management port 1 ("P1 on the E2800A and 0a on the E2800B"). If you used DHCP to obtain the original controller's IP address, you will need this address to connect to the new controller.

Label	component	Description
2	FRU part number	The FRU part number. This number must match the replacement part number for the currently installed controller.
3	4-port HIC	The 4-port host interface card (HIC). This card must be moved to the new controller when you perform the replacement. **Note**: the E2800A controller does not have a HIC.

Follow the instructions in the E2800 controller replacement procedure to prepare to remove the controller.

You use SANtricity System Manager to perform the following steps.

Steps

1. Make a note of which version of SANtricity OS software is currently installed on the controller.
2. Make a note of which version of NVSRAM is currently installed.
3. If the Drive Security feature is enabled, be sure a saved key exists and that you know the pass phrase required to install it.

> **Possible loss of data access —** If all drives in the appliance are security enabled, the new controller will not be able to access the appliance until you unlock the secured drives using the Enterprise Management Window in SANtricity System Manager.

4. Back up the configuration database.

   If a problem occurs when you remove a controller, you can use the saved file to restore your configuration.

5. 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 if the replacement does not resolve the problem.

Step 2: Take the controller offline

Take the controller offline and confirm that all operations are complete.

Steps

1. If the StorageGRID appliance is running in a StorageGRID system, place the E5700SG controller into maintenance mode.
2. If the E2800 controller is functioning sufficiently to allow for a controlled shutdown, confirm that all operations have completed.
   a. From the home page of SANtricity System Manager, select **View Operations in Progress**.
   b. Confirm that all operations have completed.
3. Power off the controller shelf.

Step 3: Remove the controller

Remove the failed controller from the appliance.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label the cables and then disconnect the cables and SFPs.

   To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

3. 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.
4. 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.

5. Place the controller on a flat, static-free surface with the removable cover facing up.
6. Remove the cover by pressing down on the button and sliding the cover off.

Step 4: Move battery to the new controller

Remove the battery from the failed controller, and install it into the replacement controller.

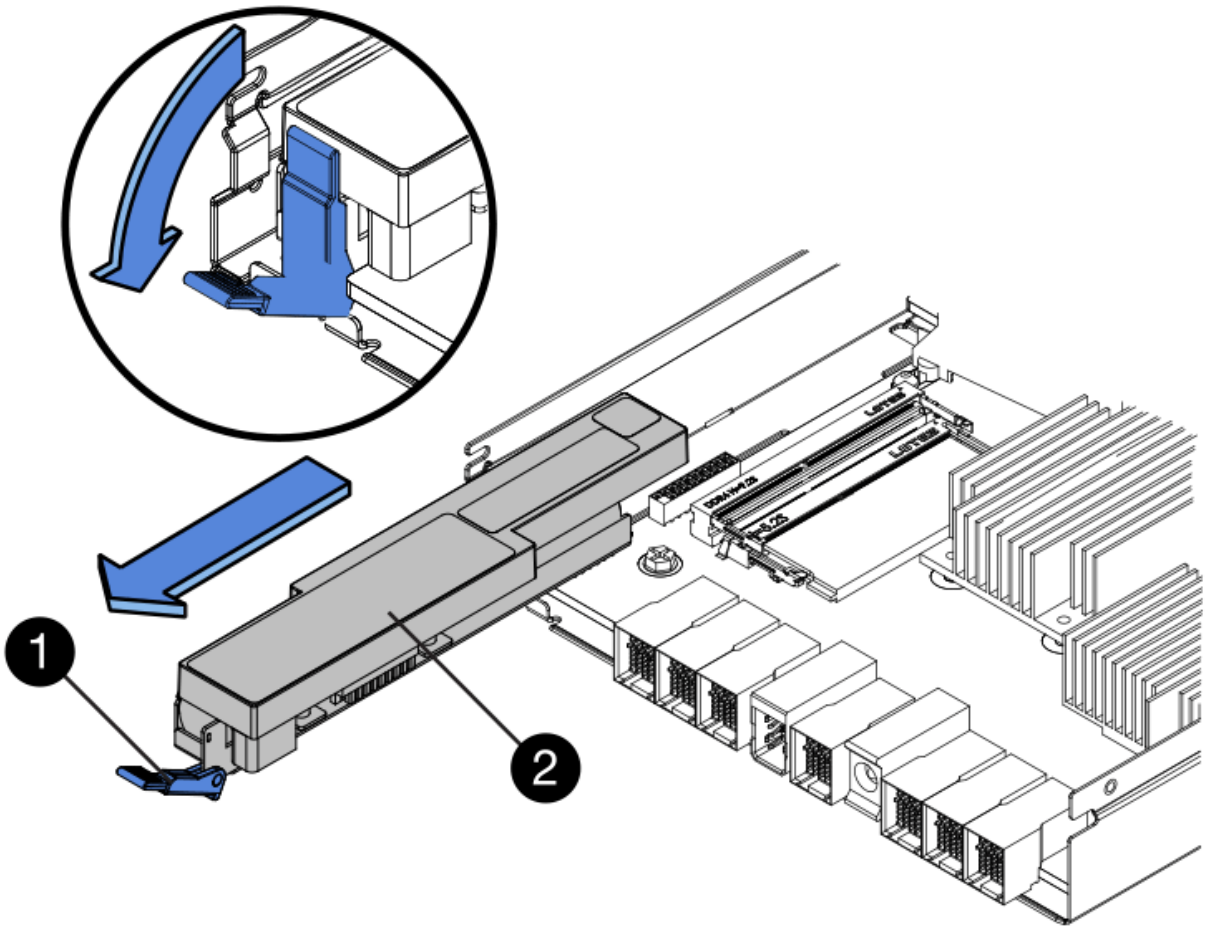
Steps

1. 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
1	Internal Cache Active LED
2	Battery

2. Locate the blue release latch for the battery.
3. Unlatch the battery by pushing the release latch down and away from the controller.



Item	Description
1	Battery release latch
2	Battery

4. Lift up on the battery, and slide it out of the controller.
5. Remove the cover from the replacement controller.
6. Orient the replacement controller so that the slot for the battery faces toward you.
7. 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.

8. Move the battery latch up to secure the battery.

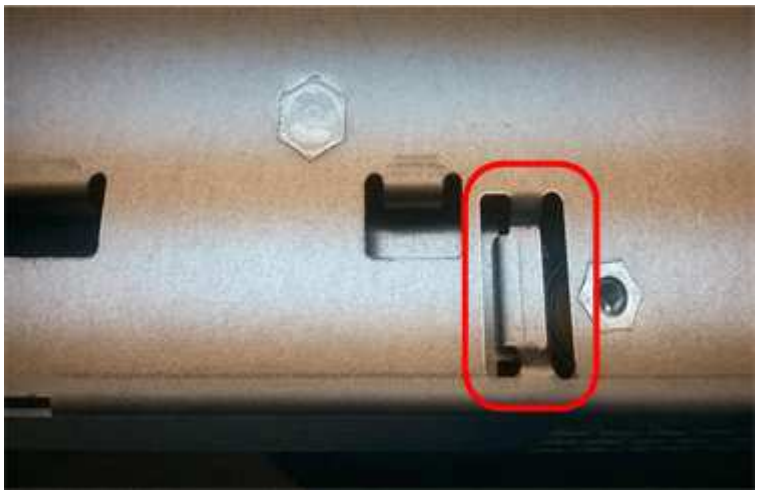
   When the latch clicks into place, the bottom of the latch hooks into a metal slot on the chassis.

9. 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 into the slot on the controller:**

- **Incorrect — The battery's metal flange is not inserted into the slot on the controller:**



10. Replace the controller cover.

Step 5: Move HIC to new controller, if needed

If the failed controller includes a host interface card (HIC), move the HIC from the failed controller to the replacement controller.

A separate HIC is used for the E2800B controller only. The HIC is mounted to the main controller board and includes two SPF connectors.

The illustrations in this procedure show a 2-port HIC. The HIC in your controller might have a different number of ports.

E2800A

An E2800A controller does not have a HIC.

Replace the E2800A controller cover, and go to Step 6: Replace controller

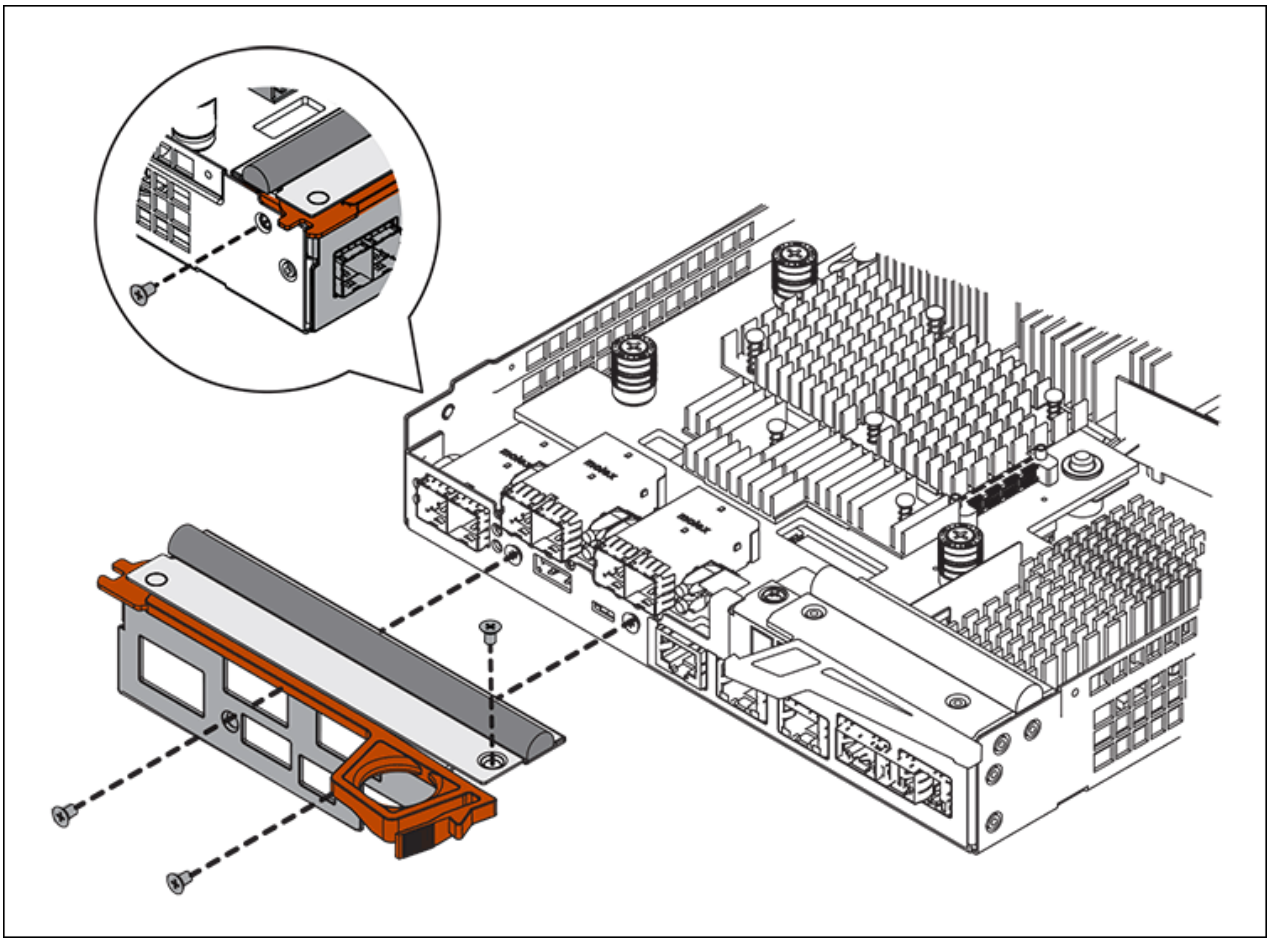
E2800B

Move the HIC from the failed E2800B controller to the replacement controller.

Steps

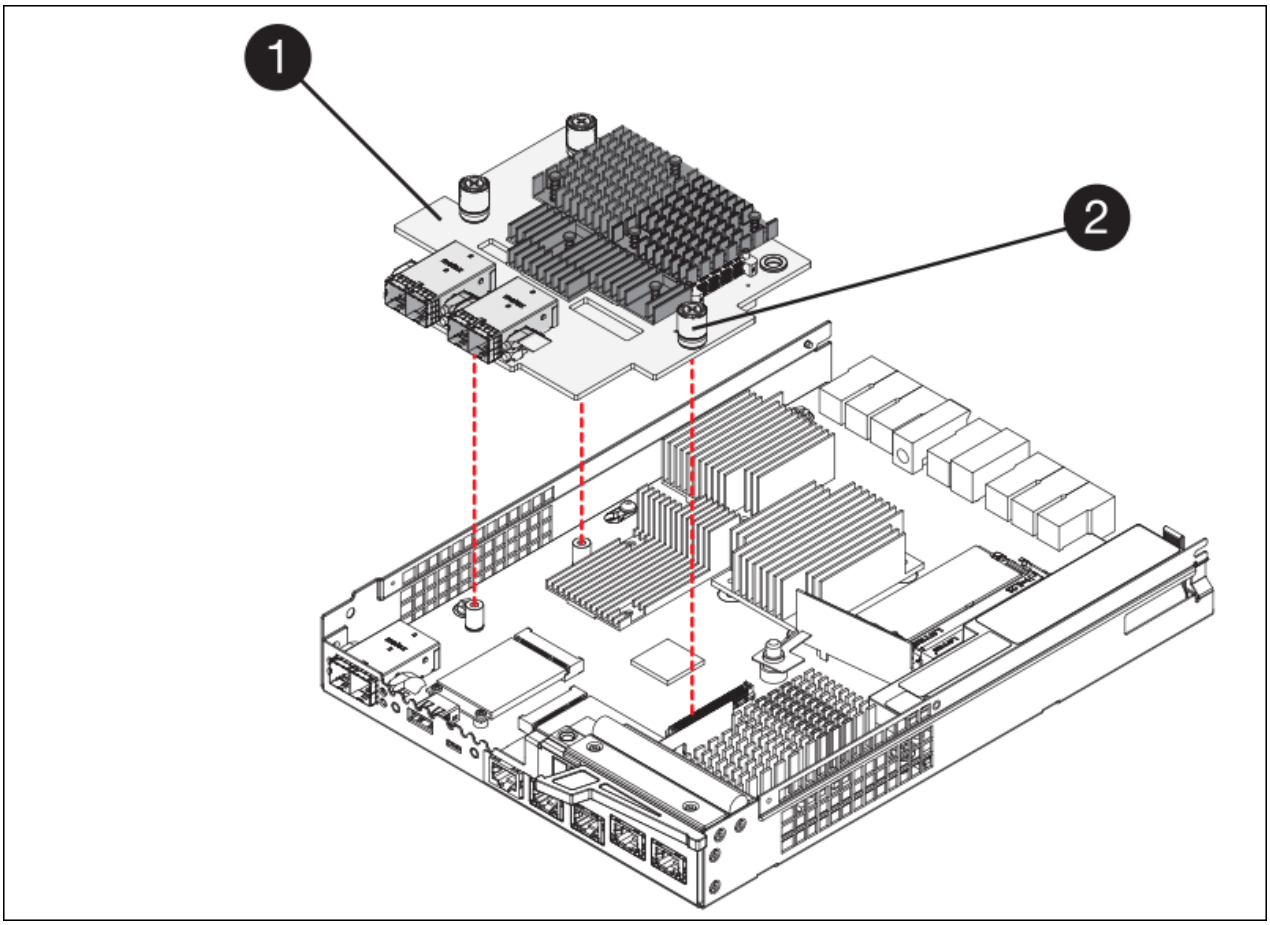
1. Remove any SFPs from the HIC.
2. Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller.

   There are four screws: one on the top, one on the side, and two on the front.



3. Remove the HIC faceplate.
4. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
5. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.

> Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



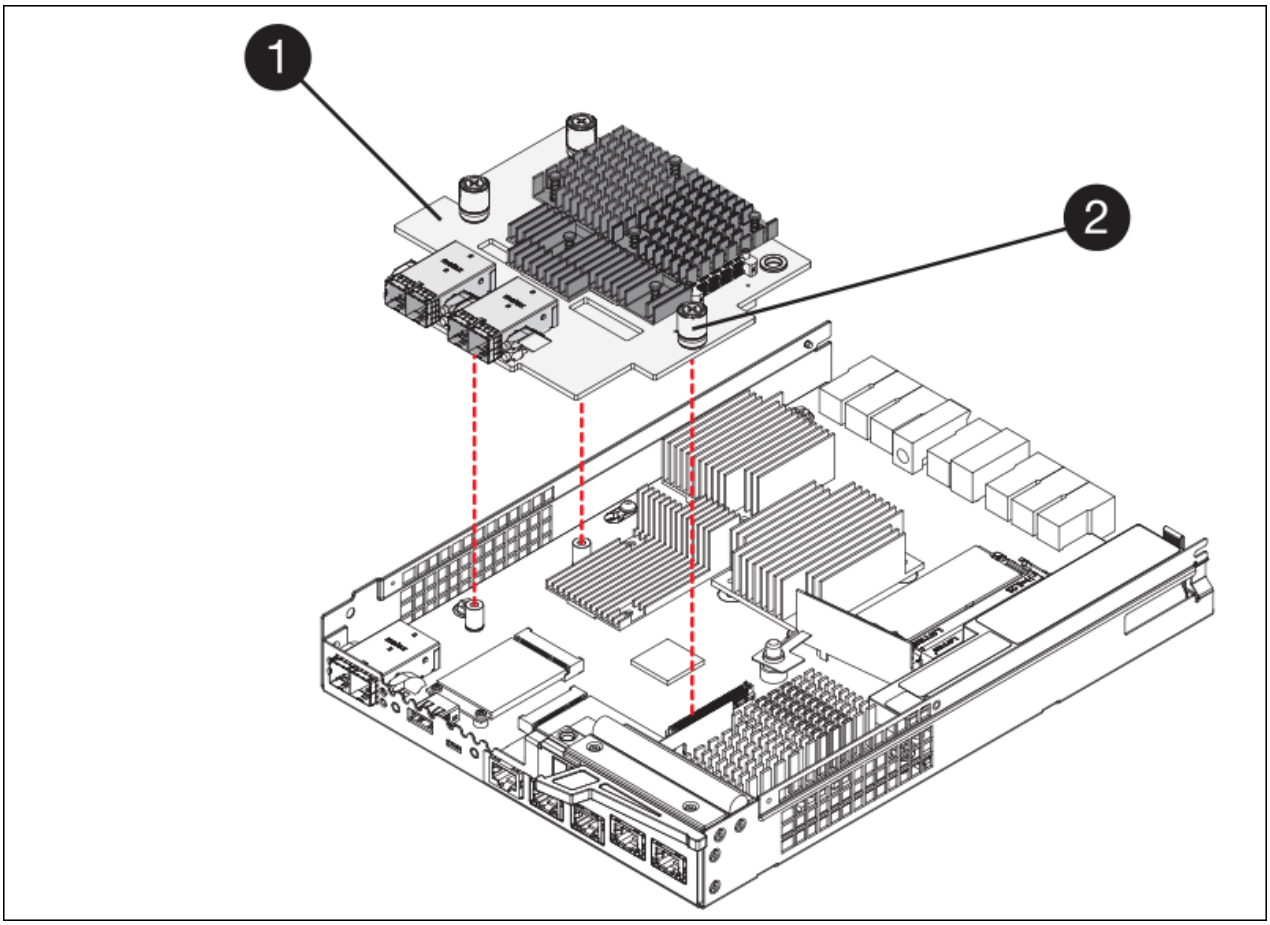
Label	Description
1	Host interface card
2	Thumbscrews

6. Place the HIC on a static-free surface.
7. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the replacement controller, and remove the faceplate.
8. Align the three thumbscrews on the HIC with the corresponding holes on the replacement controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

   Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

9. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.

Possible equipment damage — Be careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.

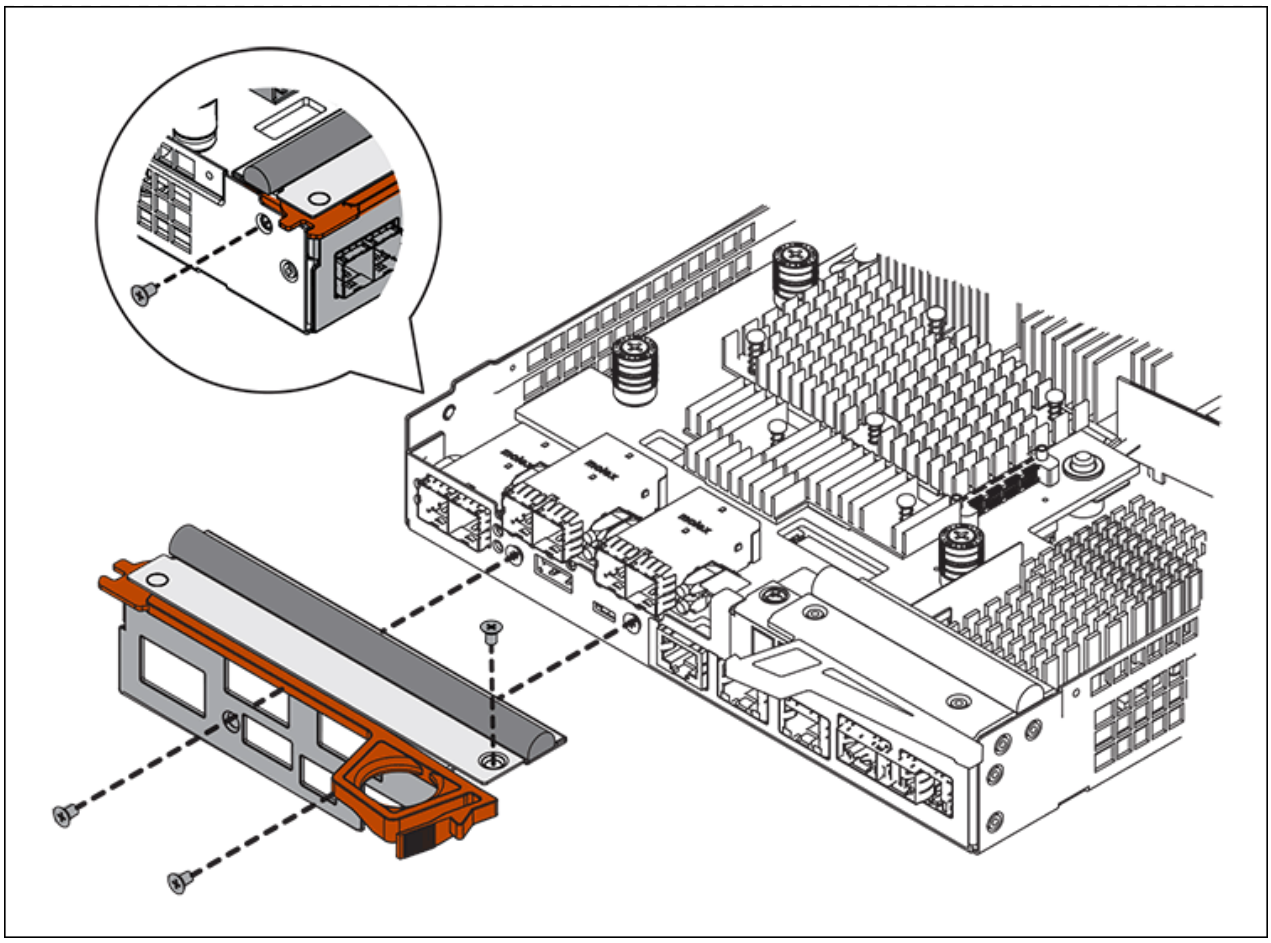


Label	Description
1	Host interface card
2	Thumbscrews

10. Hand-tighten the HIC thumbscrews.

    Don’t use a screwdriver, or you might over tighten the screws.

11. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller to the new controller with four screws.



12. Reinstall any removed SFPs into the HIC.

Step 6: Replace controller

Install the replacement controller and verify that it has rejoined the grid.

Steps

1. 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. Power on the controller shelf.
   f. Wait for the E2800 controller to reboot. Verify that the seven-segment display shows a state of `99`.
   g. Determine how you will assign an IP address to the replacement controller.

> The steps for assigning an IP address to the replacement controller depend on whether you connected management port 1 to a network with a DHCP server and on whether all drives are secured.

If management port 1 is connected to a network with a DHCP server, the new controller will obtain its

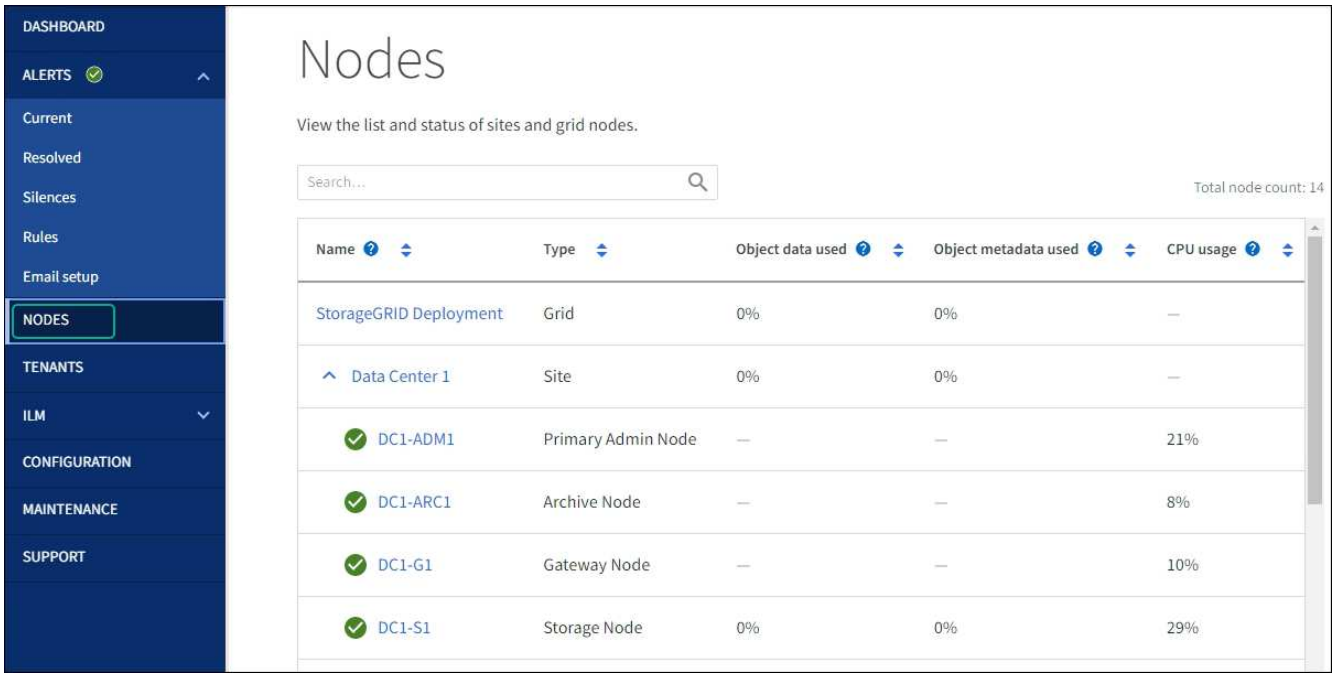
IP address from the DHCP server. This value might be different than the original controller's IP address.

2. If the appliance uses secured drives, follow the instructions in the E2800 controller replacement procedure to import the drive security key.
3. Return the appliance to normal operating mode. From the StorageGRID Appliance Installer, select **Advanced** > **Reboot Controller**, and then select **Reboot into StorageGRID**.

4. During the reboot, monitor the node's status to determine when it has rejoined the grid.

   The appliance reboots and rejoins the grid. This process can take up to 20 minutes.

5. Confirm that the reboot is complete and that the node has rejoined the grid. In the Grid Manager, verify that the Nodes page displays a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



6. From SANtricity System Manager, confirm that the new controller is Optimal, and collect support data.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace E5700SG compute controller

You might need to replace the E5700SG controller if it is not functioning optimally or if it has failed.

Before you begin

- You have a replacement controller with the same part number as the controller you are replacing.
- You have downloaded the E-Series instructions for replacing a failed E5700 controller.

> Use the E-Series instructions for reference only if you need more details to perform a specific step. Don't rely on the E-Series instructions to replace a controller in the StorageGRID appliance, because the procedures aren't the same. For example, the E-Series instructions for the E5700 controller describe how to remove the battery and the host interface card (HIC) from a failed controller and install them in a replacement controller. These steps don't apply to the E5700SG controller.

- You have labels to identify each cable that is connected to the controller.

About this task

The appliance Storage Node will not be accessible when you replace the controller. If the E5700SG 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 can't 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. Shut down the E5700SG controller.
   a. Log in to the grid node:
      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 E5700SG controller:
      `shutdown -h now`
   c. Wait for any data in cache memory to be written to the drives.

      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. Turn off the power.
   a. From the home page of SANtricity System Manager, select **View Operations in Progress**.
   b. Confirm that all operations have completed.
   c. Turn off both power switches on the appliance.
   d. Wait for all LEDs to turn off.
3. If the StorageGRID networks attached to the controller use DHCP servers:
   a. Note the MAC addresses for the ports on the replacement controller (located on labels on the controller).
   b. Ask your network administrator to update the IP address settings for the original controller to reflect the MAC addresses for the replacement controller.

   > You must ensure that the 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.

4. Remove the controller from the appliance:
   a. Put on an ESD wristband or take other antistatic precautions.
   b. Label the cables and then disconnect the cables and SFPs.

      To prevent degraded performance, don’t twist, fold, pinch, or step on the cables.

   c. 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.
   d. 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.

5. 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.
6. Power on the appliance, and monitor the controller LEDs and seven-segment displays.

   After the controllers have successfully booted up, the seven-segment displays should show the following:

   - E2800 series controller:

     The final state is `99`.

   - E5700SG controller:

The final state is `HA`.

7. Confirm that the appliance Storage Node appears in the Grid Manager and that no alarms appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Related information

NetApp E-Series Systems Documentation Site

Replace other hardware components in the SG5700

You might need to replace a controller battery, drive, fan, or power supply, in the StorageGRID appliance.

Before you begin

- You have the E-Series hardware replacement procedure.
- The appliance has been placed into maintenance mode if the component replacement procedure requires that you shut down the appliance.

About this task

To replace the battery in the E2800 controller, see the instructions in these instructions for replacing the E2800 controller. Those instructions describe how to remove the controller from the appliance, remove the battery from the controller, install the battery, and replace the controller.

To replace a drive, power-fan canister, fan canister, power canister, or drive drawer in the appliance, access the E-Series procedures for maintaining E2800 hardware.

SG5712 component replacement instructions

FRU	See E-Series instructions for
Drive	Replacing a drive in E2800 12-drive or 24-drive shelves
Power-fan canister	Replacing a power-fan canister in E2800 shelves

SG5760 component replacement instructions

FRU	See E-Series instructions for
Drive	Replacing a drive in E2860 shelves
Power canister	Replacing a power canister in E2860 shelves
Fan canister	Replacing a fan canister in E2860 shelves
Drive drawer	Replacing a drive drawer in E2860 shelves

Maintain SG6000 storage appliance hardware

Maintain SG6000 appliance

You might need to perform maintenance procedures on the SG6000 appliance.

Procedures specific to maintaining your SG6000 appliance are in this section and assume that the appliance has already been deployed as a Storage Node in a StorageGRID system.

See Common procedures for maintenance procedures that are used by all appliances.

See Set up hardware for maintenance procedures that are also performed during initial appliance installation and configuration.

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before shutting down the appliance or shut down the appliance during a scheduled maintenance window when periods of service disruption are acceptable. See the information about monitoring node connection states.

> If you have ever used an ILM rule that creates only one copy of an object, you must shut down the appliance during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during any maintenance procedure that takes a storage node out of service. See the information about managing objects with information lifecycle management.

Maintenance configuration procedures

Upgrade SANtricity OS on SG6000 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.

Download the new SANtricity OS Software file from NetApp Downloads: StorageGRID Appliance.

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.

  Upgrade SANtricity OS on storage controllers using 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.

  Upgrade SANtricity OS on 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.

Upgrade SANtricity OS on SG6000 storage controllers using 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.

Before you begin

- 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 have the Maintenance or Root access permission.
- You are signed in to the Grid Manager using a supported web browser.
- You have the provisioning passphrase.
- You have access to NetApp Downloads: StorageGRID Appliance.

About this task

You can't 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 that have been selected for the upgrade. It might take more than 30 minutes to load the SANtricity OS on each node (sequentially) and up to 90 minutes to reboot each StorageGRID storage appliance. Any nodes in your grid that don't use SANtricity OS will not be affected by this procedure.

> The following steps are only applicable when you are using the Grid Manager to perform the upgrade. The storage controllers in the appliance can't 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 don't need to apply a separate NVSRAM upgrade file.

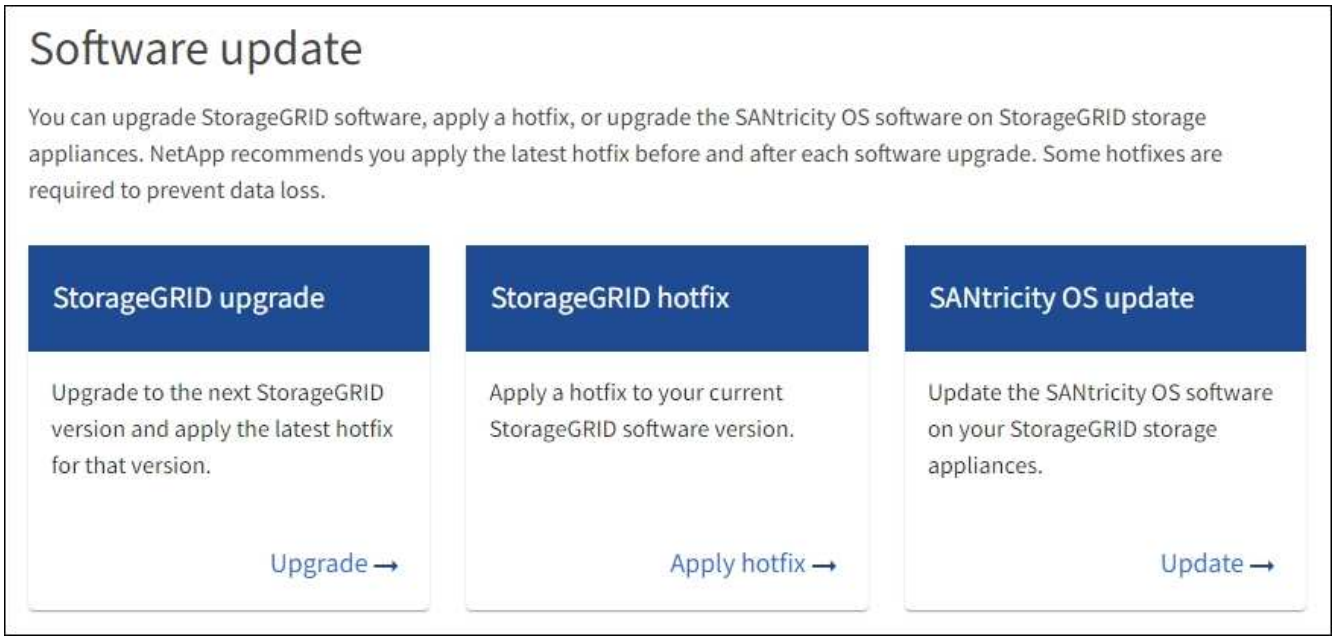
> Be sure to apply the latest StorageGRID hotfix before you begin this procedure. See StorageGRID hotfix procedure for details.

Steps

1. Download the new SANtricity OS Software file from NetApp Downloads: StorageGRID Appliance.

   Be sure to choose the SANtricity OS version for your storage controllers.

2. Select **MAINTENANCE** > **System** > **Software update**.



3. In the SANtricity OS update section, select **Update**.

   The SANtricity OS upgrade page appears and lists the details for each appliance node including:

   - Node name
   - Site
   - Appliance model
   - SANtricity OS version
   - Status
   - Last upgrade status

4. Review the information in the table for all of your upgradable appliances. Confirm that all storage controllers have **Nominal** status. If the status for any controller is **Unknown**, go to **Nodes** > ***appliance node*** > **Hardware** to investigate and resolve the issue.
5. Select the SANtricity OS upgrade file you downloaded from the NetApp Support Site.

   a. Select **Browse**.
   b. Locate and select the file.
   c. Select **Open**.

   The file is uploaded and validated. When the validation process is done, the file name is shown with a green check mark next to the **Browse** button. Don't change the file name because it is part of the verification process.

6. Enter the provisioning passphrase and select **Continue**.

   A warning box appears stating that your browser's connection might be lost temporarily as services on nodes that are upgraded are restarted.

7. Select **Yes** to stage the SANtricity OS upgrade file to the primary Admin Node.

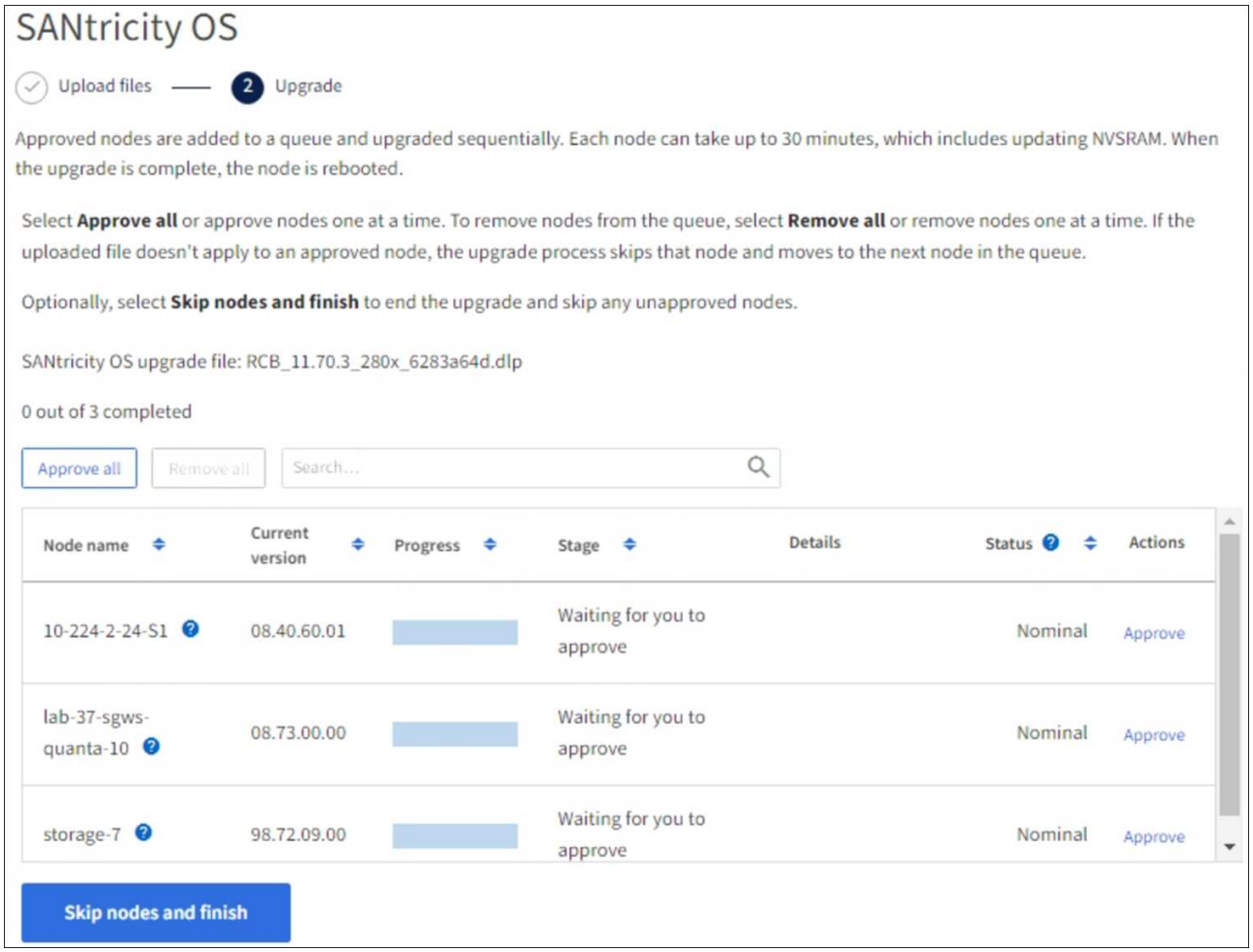
   When the SANtricity OS upgrade starts:

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 select **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 appliance Storage Nodes. Software-based Storage Nodes aren't displayed. Select **Approve** for all nodes that require the upgrade.



8. Optionally, sort the list of nodes in ascending or descending order by:
   - Node name
   - Current version
   - Progress
   - Stage
   - Status

   You can also enter a term in the Search box to search for specific nodes.

9. Approve the grid nodes you are ready to add to the upgrade queue. Approved nodes are upgraded one at a time.

Don’t 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 and the upgrade process begins. Later, when the node is finished upgrading, the appliance node is rebooted. These operations might cause service interruptions for clients that are communicating with the node.

- Select the **Approve All** button 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.

- Select one or more **Approve** buttons to add one or more nodes to the SANtricity OS upgrade queue. The **Approve** button is disabled if the Status is not Nominal.

  After you select **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. Nodes intentionally not upgraded show a stage of Complete (upgrade attempted) and list the reason the node was not upgraded in the Details column.

10. If you need to remove a node or all nodes from the SANtricity OS upgrade queue, select **Remove** or **Remove All**.

    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.

11. 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 applied, the upgrade has failed for the node. With the assistance of technical support, you might need to place the appliance in maintenance mode to recover it.
    - 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 that you must use maintenance mode to upgrade SANtricity OS on the node. To resolve the error, do the following:
      a. Use maintenance mode to upgrade SANtricity OS on the node that shows a stage of Error.
      b. Use the Grid Manager to restart 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 number of nodes upgraded, and the date and time the upgrade completed.

12. If a node can’t be upgraded, note the reason shown in the Details column and take the appropriate action.

    The SANtricity OS upgrade process will not be complete until you approve the SANtricity OS upgrade on all the listed Storage Nodes.

Reason	Recommended action
Storage Node was already upgraded.	No further action required.
SANtricity OS upgrade is not applicable to this node.	The node does not have a storage controller that can be managed by the StorageGRID system. Complete the upgrade process without upgrading the node displaying this message.
SANtricity OS file is not compatible with this node.	The node requires a SANtricity OS file different than the one you selected. After completing the current upgrade, download the correct SANtricity OS file for the node and repeat the upgrade process.

13. If you want to end approving nodes and return to the SANtricity OS page to allow for an upload of a new SANtricity OS file, do the following:
    a. Select **Skip Nodes and Finish**.

       A warning appears asking if you are sure you want to finish the upgrade process without upgrading all applicable nodes.

    b. Select **OK** to return to the **SANtricity OS** page.
    c. When you are ready to continue approving nodes, download the SANtricity OS to restart the upgrade process.

       Nodes already approved and upgraded without errors remain upgraded.

14. 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

Upgrade SANtricity OS on storage controllers using maintenance mode

Upgrade SANtricity OS on SG6000 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.

Before you begin

- 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, you have placed the SG6000-CN controller into maintenance mode.

Maintenance mode interrupts the connection to the storage controller.

About this task

Don't 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

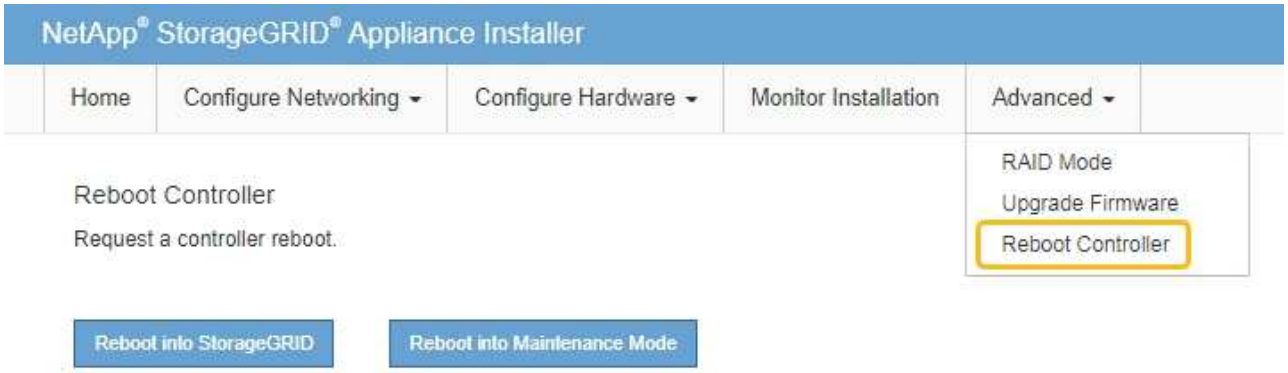
1. Confirm that the appliance is in maintenance mode.
2. From a service laptop, access SANtricity System Manager and sign in.
3. Download the new SANtricity OS Software file and NVSRAM file to the management client.

   The NVSRAM is specific to the StorageGRID appliance. Don't use the standard NVSRAM download.

4. Follow the instructions in the *Upgrading SANtricity OS* guide or the SANtricity System Manager online help to upgrade the firmware and NVSRAM.

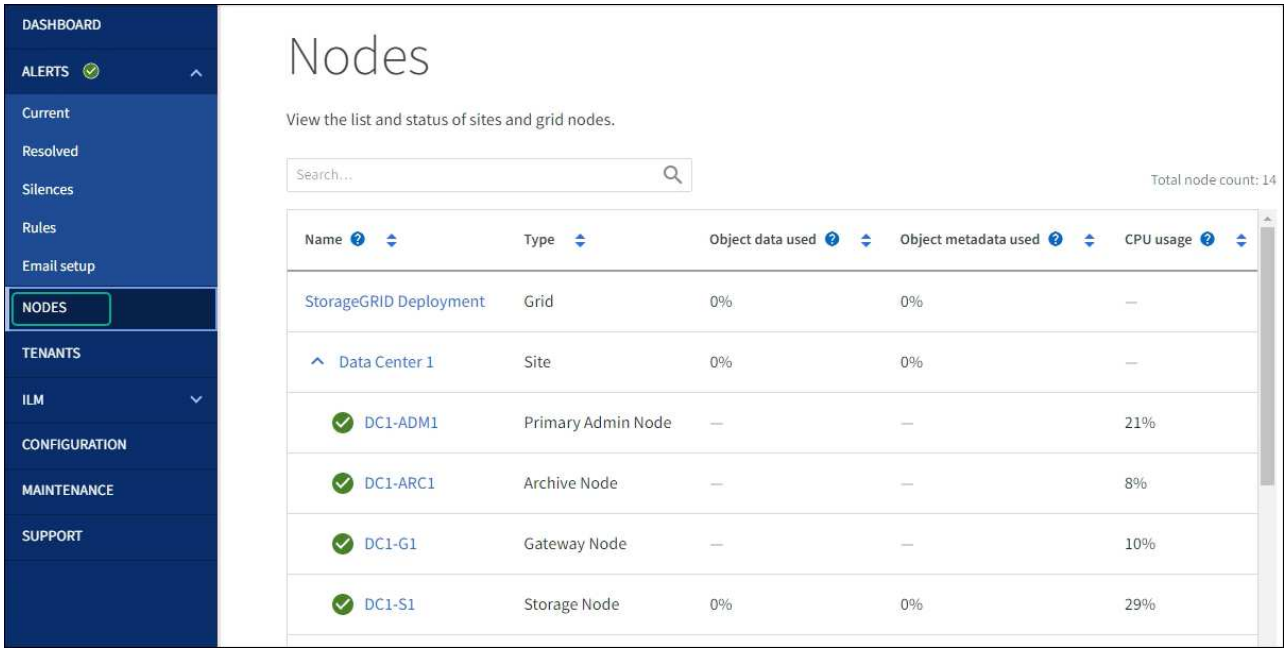
   Activate the upgrade files immediately. Don't defer activation.

5. If this procedure completed successfully and you have additional procedures to perform while the node is in maintenance mode, perform them now. When you are done, or if you experienced any failures and want to start over, select **Advanced** > **Reboot Controller**, and then select one of these options:
   - Select **Reboot into StorageGRID**
   - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if you experienced any failures during the procedure and want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.



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 page should display a normal status (green check mark icon to the left of the node name) for the

appliance node, indicating that no alerts are active and the node is connected to the grid.



Related information

NetApp Interoperability Matrix Tool

Upgrade SANtricity OS on storage controllers using Grid Manager

Upgrade drive firmware using SANtricity System Manager

Upgrade SG6000 drive firmware using SANtricity System Manager using the online method

Use the SANtricity System Manager online method to upgrade the firmware on the drives in your appliance to make sure you have all the latest features and bug fixes.

Before you begin

- The storage appliance has an Optimal status.
- All drives have an Optimal status.

> Don’t 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 policy.

About this task

The drives are upgraded one at a time while the appliance is performing I/O. This method does not require you to place the appliance in maintenance mode. However, system performance might be impacted and the upgrade might take several hours longer than the offline method.

Drives belonging to volumes that don't have redundancy must be updated using the offline method. The offline method should be used for any drive associated with flash read cache (for example, SSD drives in the SG6060), or any pool or volume group that is currently degraded.

There are two types of drives: SSD and HDD. You must use the offline method to upgrade the firmware on the SSDs (for example, SSD drives in the SG6060). You can use either the online or offline method to upgrade the firmware on HDDs.

Steps

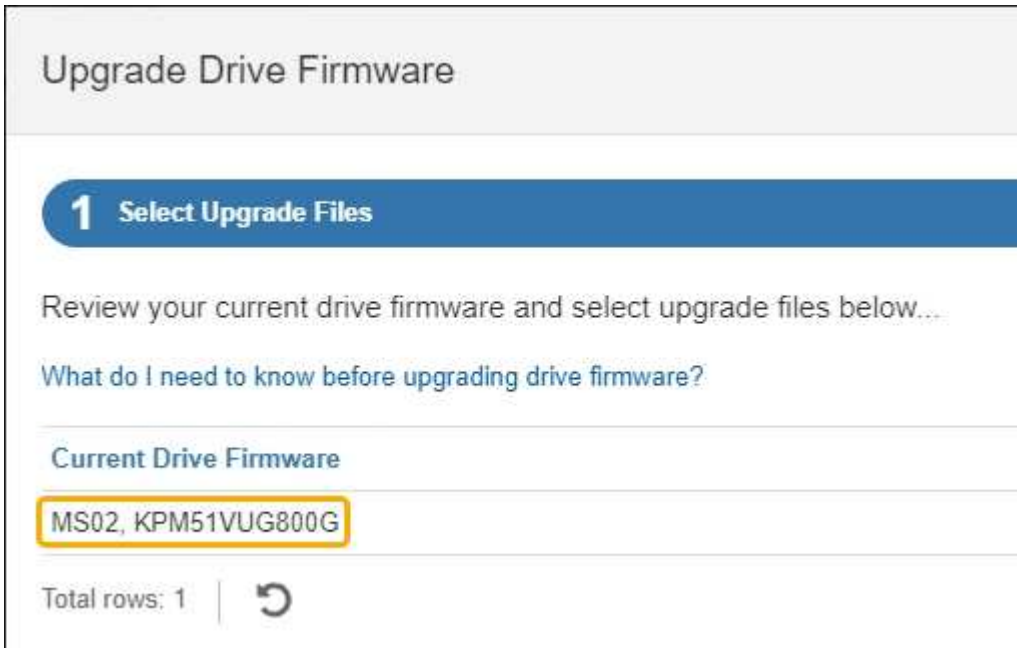
1. Access SANtricity System Manager using one of these methods:
   - Use the StorageGRID Appliance Installer and select **Advanced** > **SANtricity System Manager**
   - Use the Grid Manager and select **NODES** > ***Storage Node*** > **SANtricity System Manager**
   - Use SANtricity System Manager by browsing to the 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 page displays the drive firmware files currently installed.

   c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.



      In this example:

      - The drive firmware revision is **MS02**.
      - The drive identifier is **KPM51VUG800G**.

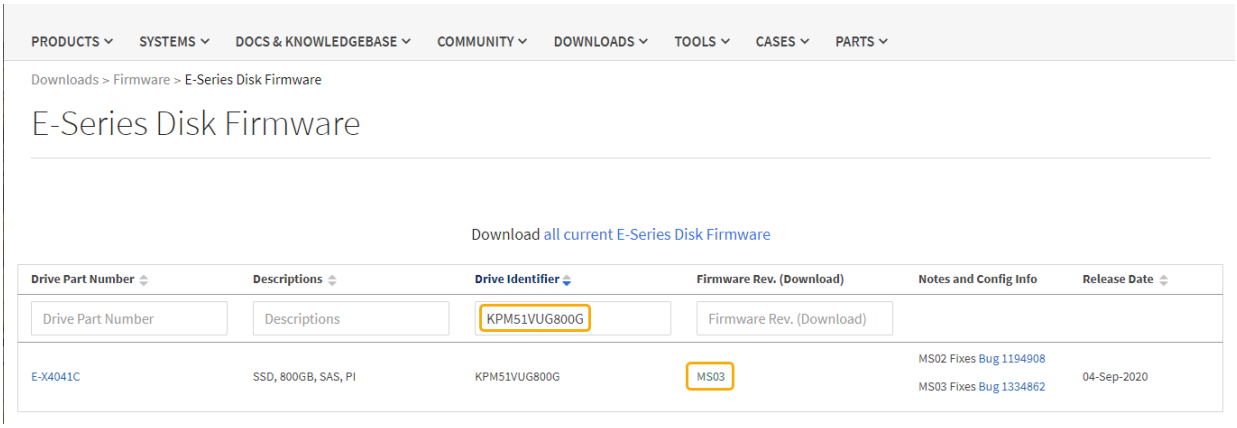
   d. Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.

e. Close the Upgrade Drive Firmware window.

4. Download and prepare the available drive firmware upgrade:
   a. Under Drive Firmware upgrade, select **NetApp Support**.
   b. On the NetApp Support Site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

      The E-Series Disk Firmware page displays.

   c. 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.



   d. 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.
   e. Extract (unzip) the drive firmware archive files you downloaded from the Support site.

5. Install the drive firmware upgrade:
   a. From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.
   b. 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.

   c. 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 the **Proposed Firmware** column. If you must change this firmware, select **Back**.

d. Select **Upgrade all drives online** — Upgrades the drives that can support a firmware download while the storage array is processing I/O. You don't have to stop I/O to the associated volumes using these drives when you select this upgrade method.

> An online upgrade can take several hours longer than an offline upgrade.
>
> You must use the offline method to upgrade the firmware on SSDs.

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 required, troubleshoot driver firmware upgrade errors.

Upgrade SG6000 drive firmware using SANtricity System Manager using the offline method

Use the SANtricity System Manager offline method to upgrade the firmware on the drives in your appliance to make sure you have all the latest features and bug fixes.

Before you begin

- The storage appliance has an Optimal status.
- All drives have an Optimal status.
- You have placed the StorageGRID appliance into maintenance mode.

> While the appliance is in maintenance mode, I/O (input/output) activity to the storage controller is stopped to make disruptive storage operations safe.

> Don't 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 policy.

About this task

The drives are upgraded in parallel while the appliance is in maintenance mode. If the pool or volume group does not support redundancy or is degraded, you must use the offline method to upgrade the drive firmware. You should also use the offline method for any drive associated with flash read cache, or any pool or volume group that is currently degraded. The offline method upgrades firmware only while all I/O activity is stopped on the drives to be upgraded. To stop I/O activity, place the node into maintenance mode.

The offline method is faster than the online method and will be significantly faster when many drives in a single

appliance need upgrades. However, it requires that nodes be taken out of service, which might require scheduling a maintenance window and monitoring progress. Choose the method that is the best fit for your operational procedures and the number of drives that need to be upgraded.

> There are two types of drives: SSD and HDD. You must use the offline method to upgrade the firmware on the SSDs (for example, SSD drives in the SG6060). You can use either the online or offline method to upgrade the firmware on HDDs.

Steps

1. Confirm that the appliance is in maintenance mode.

   > If you are upgrading the firmware in SSD drives that are part of a cache group, you must ensure that no I/O is sent to any cached volumes while the upgrade is in progress. When the appliance is in maintenance mode, no I/O is sent to any volumes while the upgrade is in progress.

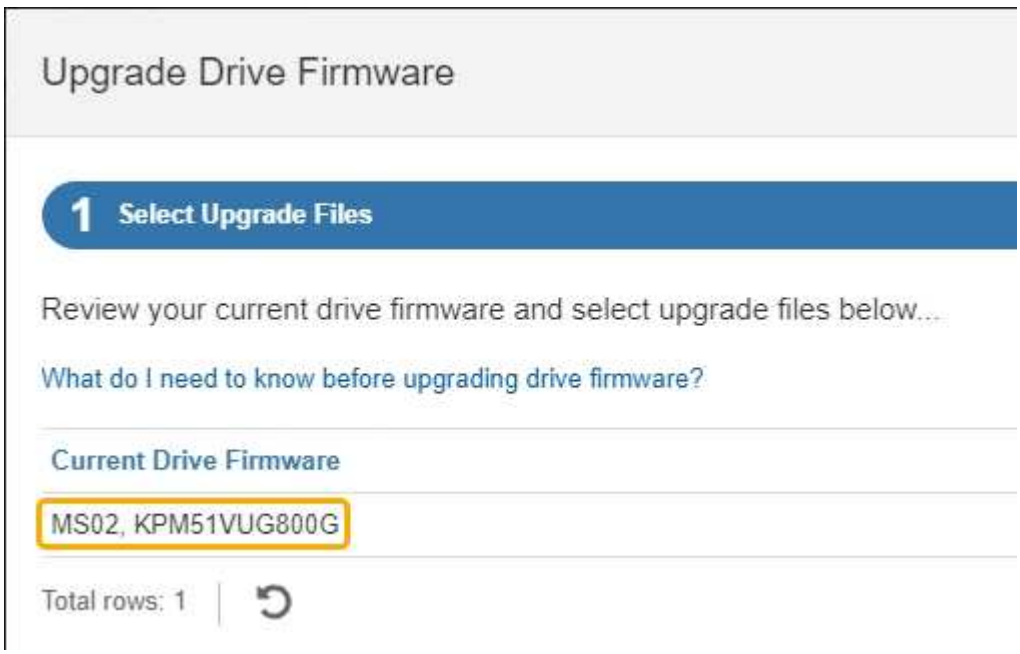
2. Access SANtricity System Manager using one of these methods:
   - Use the StorageGRID Appliance Installer and select **Advanced** > **SANtricity System Manager**
   - Use the Grid Manager and select **NODES** > ***Storage Node*** > **SANtricity System Manager**
   - Use SANtricity System Manager by browsing to the storage controller IP:

     `https://Storage_Controller_IP`

3. Enter the SANtricity System Manager administrator username and password, if required.
4. 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 page displays the drive firmware files currently installed.

   c. Note the current drive firmware revisions and drive identifiers in the Current Drive Firmware column.



In this example:

- The drive firmware revision is **MS02**.
- The drive identifier is **KPM51VUG800G**.

d. Select **View drives** in the Associated Drives column to display where these drives are installed in your storage appliance.

e. Close the Upgrade Drive Firmware window.

5. Download and prepare the available drive firmware upgrade:

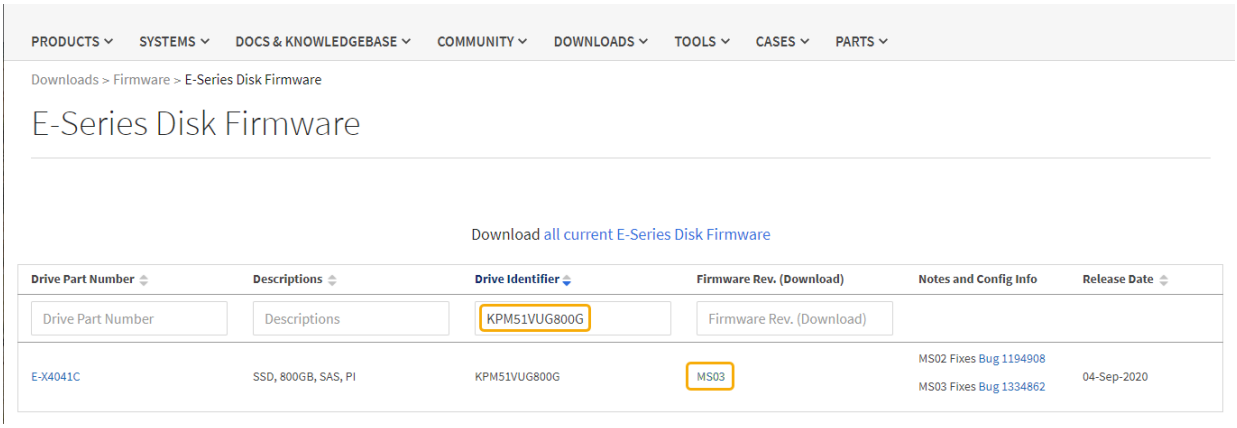
a. Under Drive Firmware upgrade, select **NetApp Support**.

b. On the NetApp Support Site, select the **Downloads** tab, and then select **E-Series Disk Drive Firmware**.

The E-Series Disk Firmware page displays.

c. 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.



d. 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.

e. Extract (unzip) the drive firmware archive files you downloaded from the Support site.

6. Install the drive firmware upgrade:

a. From SANtricity System Manager, under Drive Firmware upgrade, select **Begin Upgrade**.

b. 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.

c. 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 the **Proposed Firmware** column. If you must change this firmware, select **Back**.

d. Select **Upgrade all drives offline (parallel)** — Upgrades the drives that can support a firmware download only while all I/O activity is stopped on any volumes that use the drives.

> You must place the appliance into maintenance mode before using this method. You should use the **Offline** method to upgrade the drive firmware.

> If you want to use the Offline (parallel) upgrade, don't proceed unless you are certain that the appliance is in maintenance mode. Failure to place the appliance into maintenance mode before initiating an offline drive firmware update might cause data loss.

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.

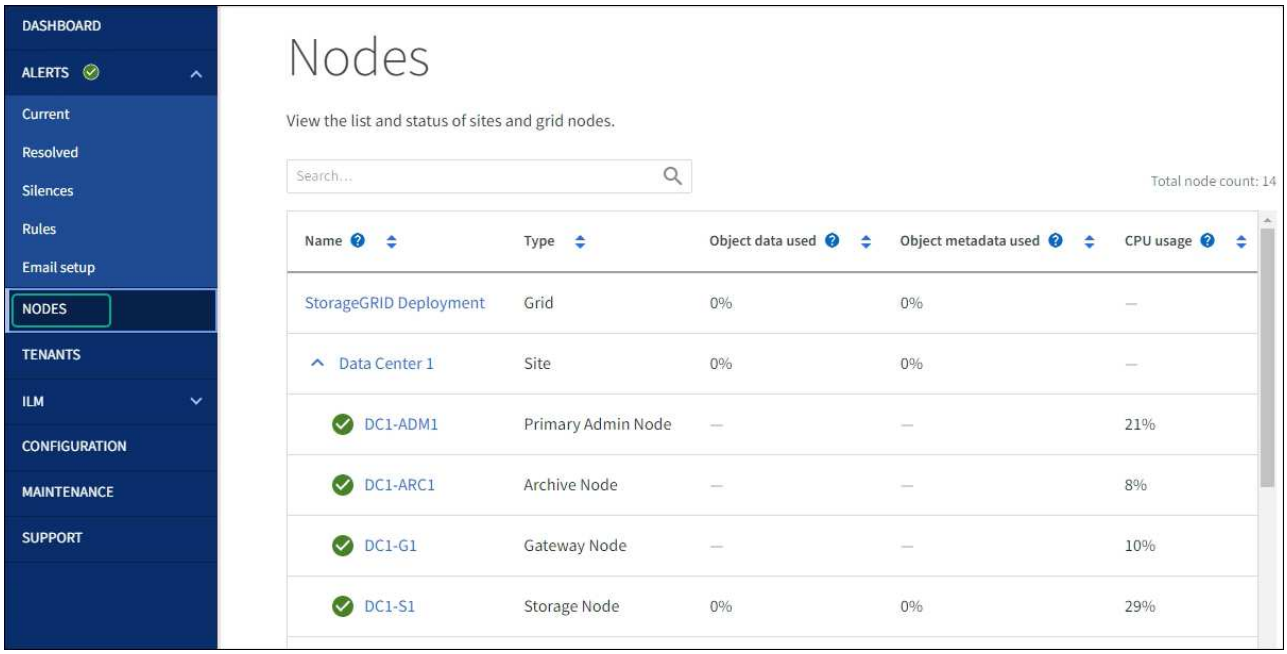
g. (Optional) To see a list of what was upgraded, select **Save Log**.

The log file is saved in the downloads folder for your browser with the name `latest-upgrade-log-timestamp.txt`.

If required, troubleshoot driver firmware upgrade errors.

7. After the procedure completes successfully, perform any additional maintenance procedures while the node is in maintenance mode. When you are done, or if you experienced any failures and want to start over, go to the StorageGRID Appliance Installer and select **Advanced** > **Reboot Controller**. Then select one of these options:
   - **Reboot into StorageGRID**.
   - **Reboot into Maintenance Mode**. Reboot the controller and keep the node in maintenance mode. Select this option if there were any failures during the procedure and you want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.

   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 page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Troubleshoot drive firmware upgrade errors

Troubleshoot errors that can occur when using SANtricity System Manager to upgrade the firmware on the drives in your appliance.

- **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 aren't 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.

Turn SG6000-CN 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.

Before you begin

You have the BMC IP address of the controller you want to identify.

Steps

1. Access the controller BMC interface.
2. Select **Server Identify**.

The current status of the identify LED is selected.

3. Select **ON** or **OFF**, and then select **Perform Action**.

   When you select **ON**, the blue identify LEDs light on the front (shown) and rear of the appliance.

   If a bezel is installed on the controller, it might be difficult to see the front identify LED.

4. Turn the LED on and off as needed.

Related information

Verify Fibre Channel HBA to replace

Locate controller in data center

Access BMC interface

Locate SG6000-CN controller in data center

Locate the controller so that you can perform hardware maintenance or upgrades.

Before you begin

- You have determined which controller requires maintenance.

  (Optional) To help locate the controller in your data center, turn on the blue identify LED.

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.

Related information

Remove Fibre Channel HBA

Remove SG6000-CN controller from cabinet or rack

Shut down SG6000-CN controller

Power SG6000-CN controller off and on

You can shut down the SG6000-CN controller and power it back on to perform maintenance.

Shut down SG6000-CN controller

Shut down the SG6000-CN controller to perform hardware maintenance.

Before you begin

- You have physically located the SG6000-CN controller requiring maintenance in the data center. See Locate controller in data center.

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 acceptable. See the information about monitoring node connection states.

> 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. Shut down the SG6000-CN controller.

   > You must perform a controlled shut down of the appliance by entering the commands specified below. It is a best practice to perform a controlled shutdown when possible to avoid unnecessary alerts, ensure full logs are available, and avoid service disruptions.

   a. If you have not already logged into the grid node, log in 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.

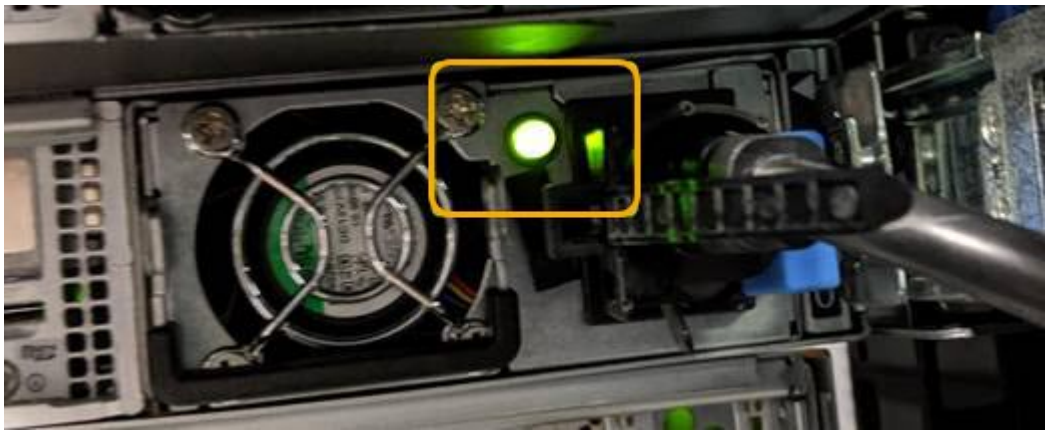
      When you are logged in as root, the prompt changes from `$` to `#`.

   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.

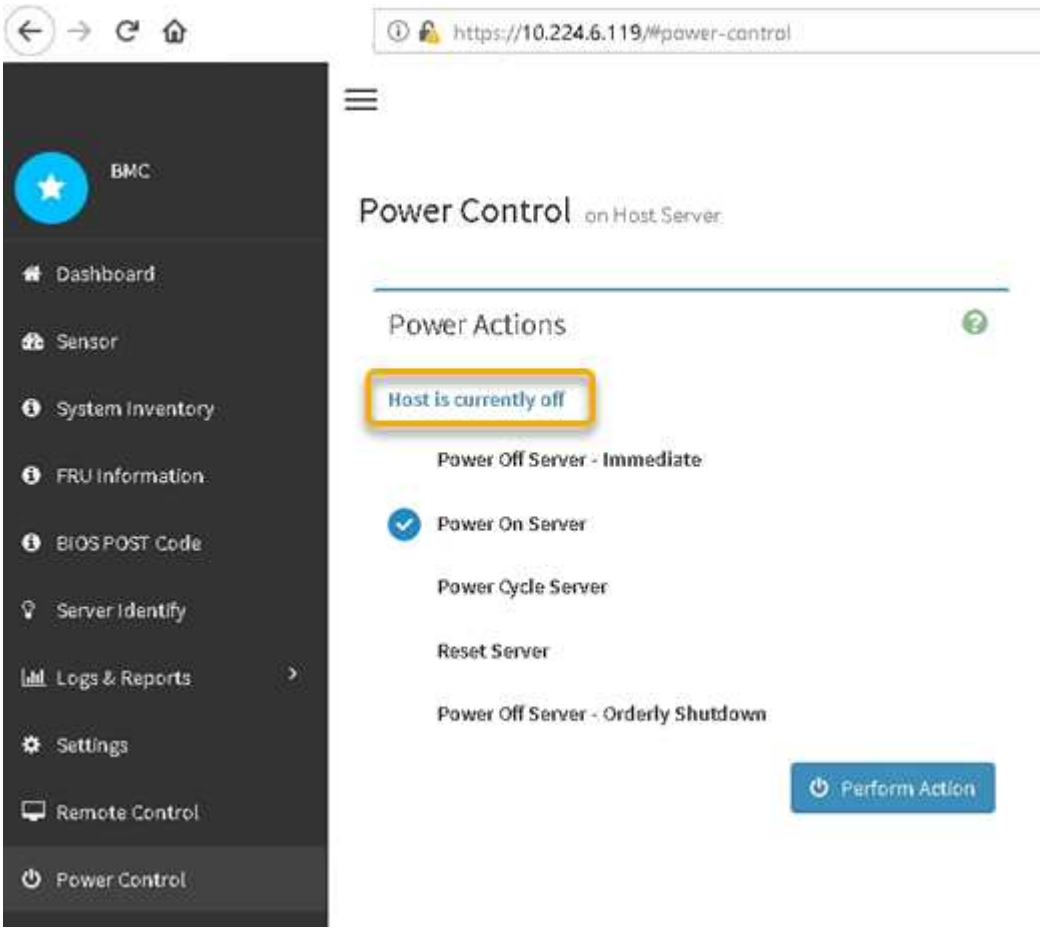
   - Look at the green LEDs on both power supplies in the rear of the controller and confirm that they blink at a regular rate (approximately one blink per second).



- Use the controller BMC interface:
  i. Access the controller BMC interface.

     Access BMC interface

  ii. Select **Power Control**.
  iii. Verify that the Power Actions indicates that the host is currently off.



Power on SG6000-CN controller and verify operation

Power on the controller after completing maintenance.

Before you begin

- You have installed the controller in a cabinet or rack and connected the data and power cables.

  Reinstall SG6000-CN controller into cabinet or rack

- You have physically located the controller in the data center.

  Locate controller in data center

Steps

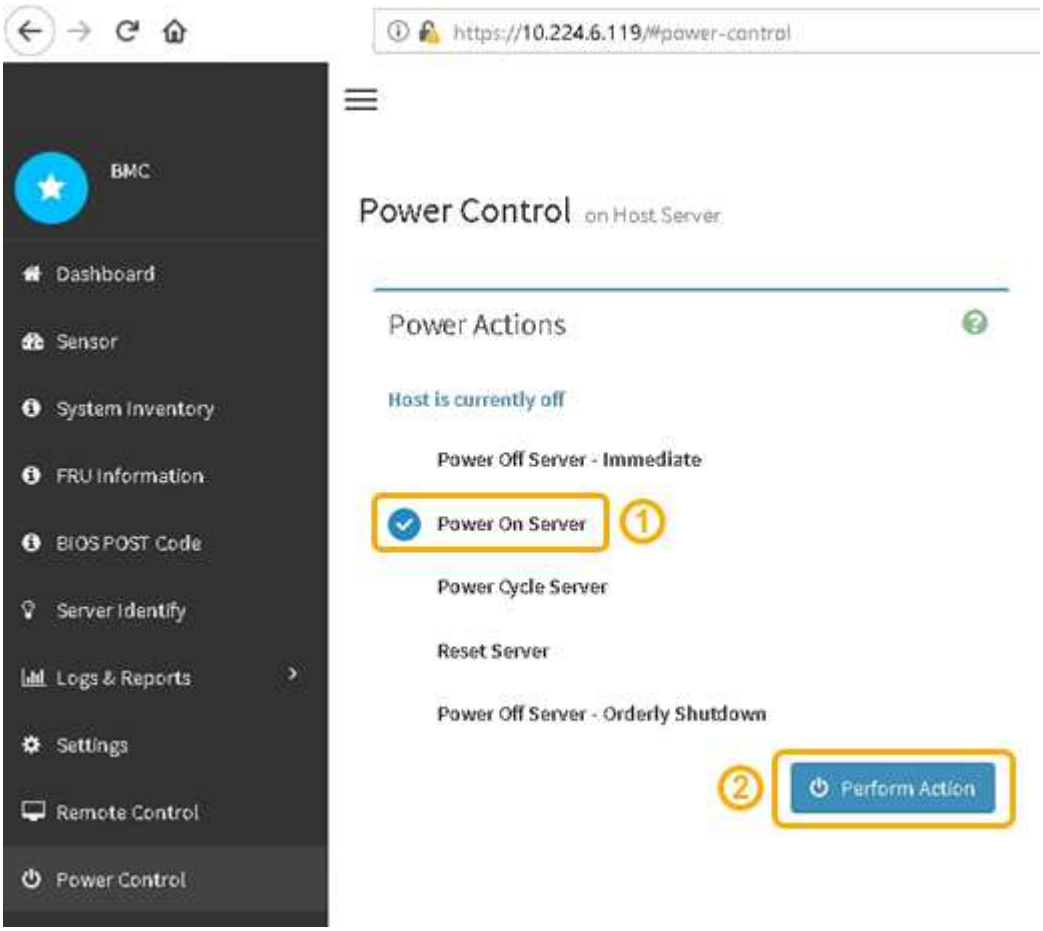
1. Power on the SG6000-CN controller and monitor the controller LEDs and boot-up codes using one of the following methods:

- Press the power switch on the front of the controller.

- Use the controller BMC interface:
  i. Access the controller BMC interface.

     Access BMC interface

  ii. Select **Power Control**.
  iii. Select **Power On Server** and then select **Perform Action**.



  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
      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 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.

      Don’t take another appliance node offline unless this appliance has a green icon.

4. Optional: Install the front bezel, if one was removed.

Related information

- Remove SG6000-CN controller from cabinet or rack
- View status indicators

Change link configuration of 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.

Before you begin

The appliance has been placed maintenance mode.

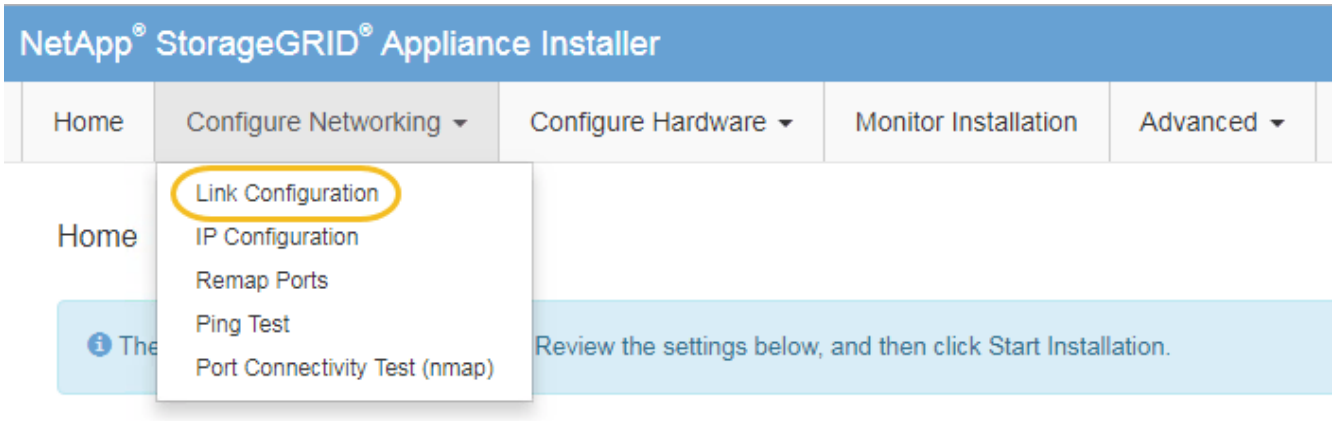
About this task

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 about the options, see Configure network links.

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 aren't 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`

   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 Configure IP addresses instructions.

   Configure StorageGRID IP addresses

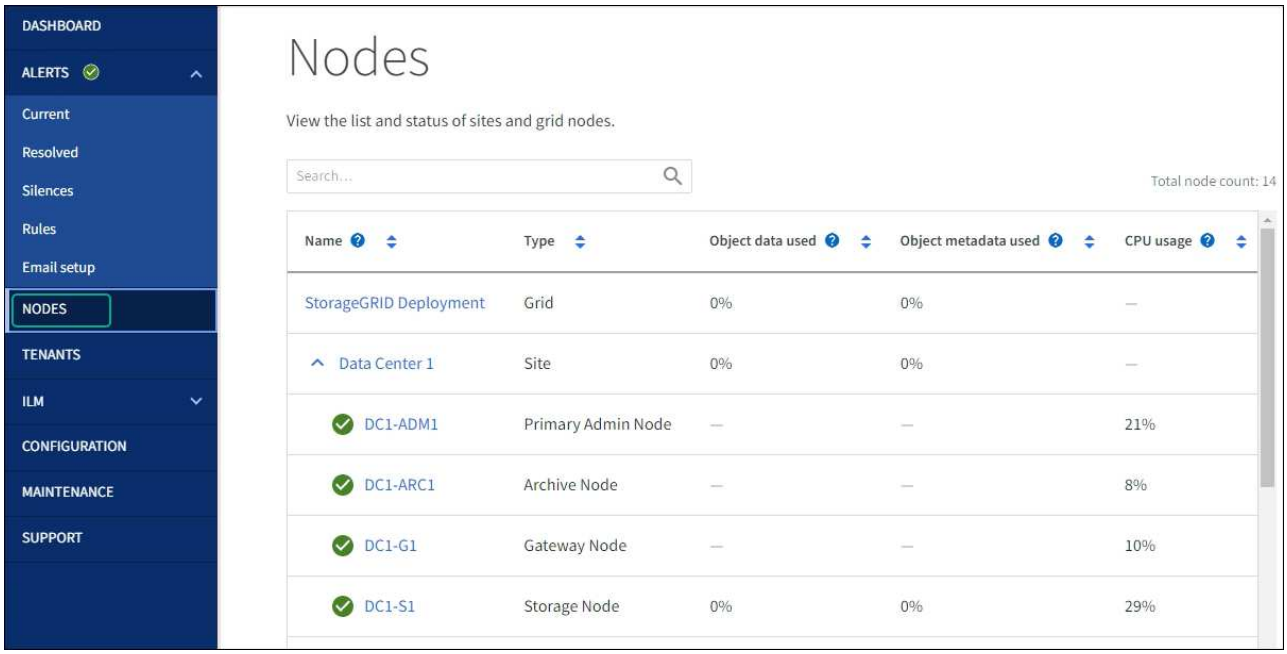
4. Select **Configure Networking** > **Ping Test** from the menu.
5. Use the Ping Test tool to check connectivity to IP addresses on any networks that might have been

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 and you have additional procedures to perform while the node is in maintenance mode, perform them now. When you are done, or if you experienced any failures and want to start over, select **Advanced** > **Reboot Controller**, and then select one of these options:
   - Select **Reboot into StorageGRID**
   - Select **Reboot into Maintenance Mode** to reboot the controller with the node remaining in maintenance mode. Select this option if you experienced any failures during the procedure and want to start over. After the node finishes rebooting into maintenance mode, restart from the appropriate step in the procedure that failed.

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** page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Hardware procedures

Add expansion shelf to deployed SG6060

To increase storage capacity, you can add one or two expansion shelves to an SG6060 that is already deployed in a StorageGRID system.

Before you begin

- 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.

  Locate controller in data center

About this task

To add an expansion shelf, you perform these high-level steps:

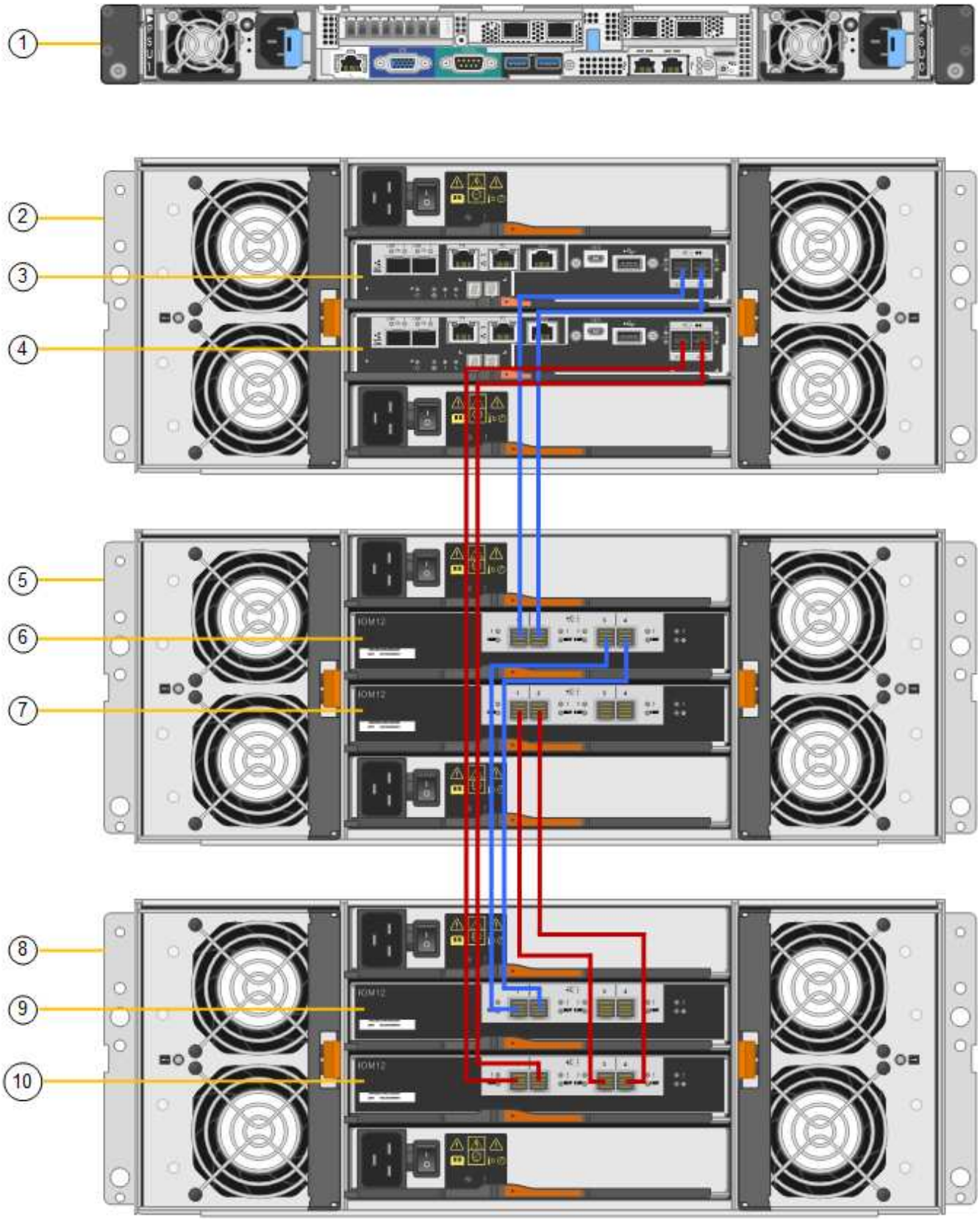
- Install the hardware in the cabinet or rack.
- Place the SG6060 into maintenance mode.
- Connect the expansion shelf to the E2860 controller shelf or to another expansion shelf.
- Start the expansion using the StorageGRID Appliance Installer
- Wait until the new volumes are configured.

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.
2. Follow the instructions for installing the drives.
3. From the Grid Manager, place the SG6000-CN controller 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.



Callout	Description
1	SG6000-CN

Callout	Description
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.
      - Don’t 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.

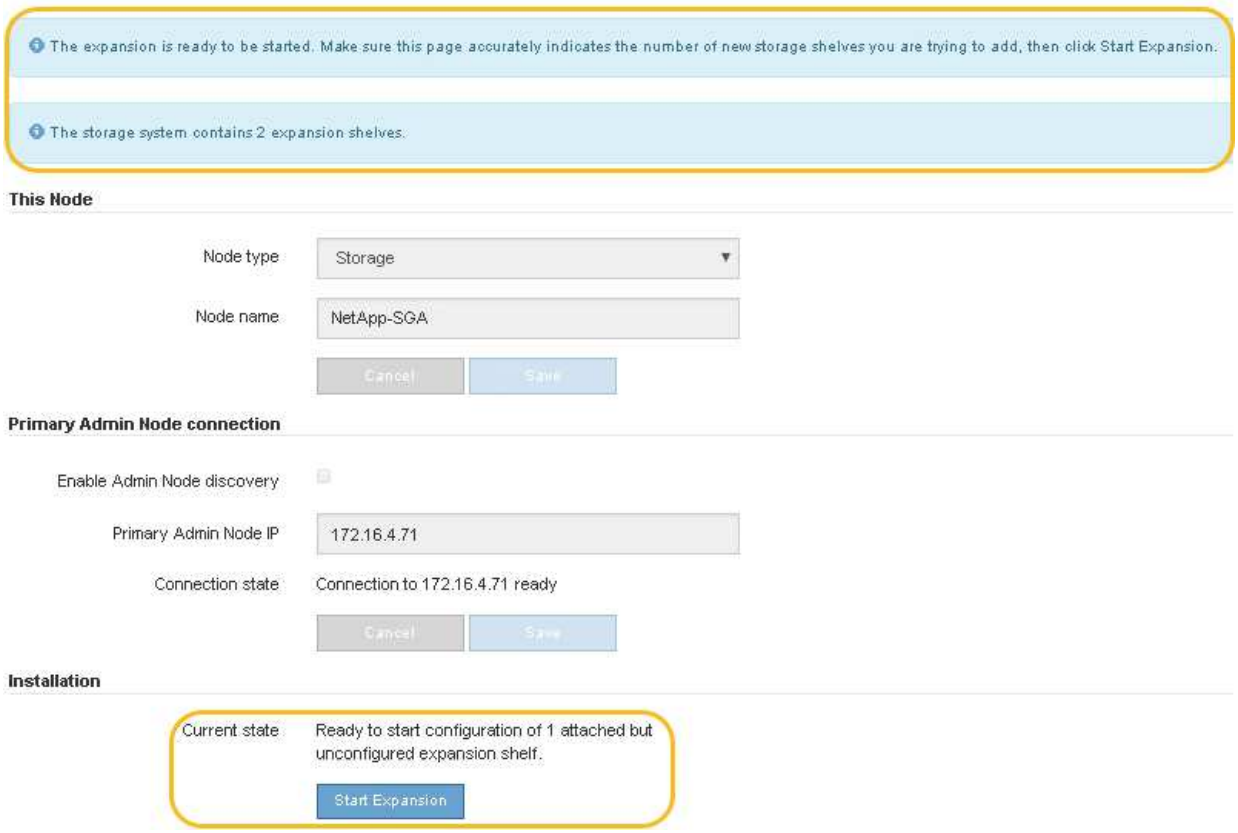
   In approximately five minutes, the expansion shelves finish powering up and are detected by the system. The Home page shows the number of new expansion shelves detected, and the Start Expansion button is enabled.

   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 aren't 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 aren't detected.



7. As necessary, resolve any issues described in the messages on the Home page.

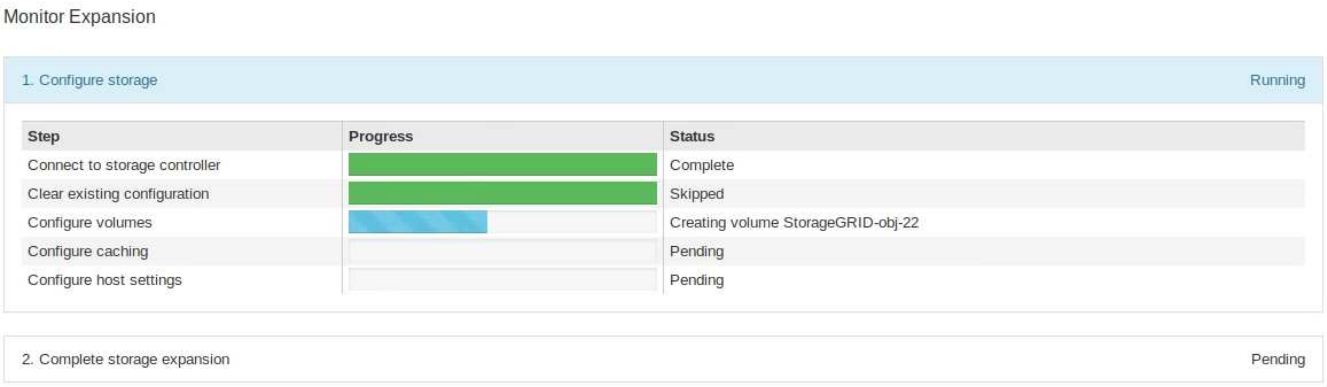
   For example, use SANtricity System Manager to resolve any storage hardware issues.

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.



When configuration is complete, the appliance automatically reboots to exit maintenance mode and rejoin the grid. This process can take up to 20 minutes.

> To retry the expansion shelf configuration if it fails, go to the StorageGRID Appliance Installer, select **Advanced** > **Reboot Controller**, and then select **Reboot into Maintenance Mode**. After the node reboots, retry the expansion shelf configuration.

When the reboot is complete, the **Tasks** tab looks like the following screenshot:

11. Verify the status of the appliance Storage Node and the new expansion shelves.
    a. In the Grid Manager, select **NODES** and verify that the appliance Storage Node has a green check mark icon.

       The green check mark icon means that no alerts are active and the node is connected to the grid. For a description of node icons, see Monitor node connection states.

    b. Select the **Storage** tab and confirm that 16 new object stores are shown in the Object Storage table for each expansion shelf you added.
    c. Verify that each new expansion shelf has a shelf status of Nominal and a configuration status of Configured.

Replace storage controller in the SG6000

You might need to replace an E2800 series controller or an EF570 controller if it is not functioning optimally or if it has failed.

Before you begin

- 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 physically located the storage appliance where you are replacing the controller in the data center.

  Locate controller in data center

> Don't rely on the E-Series instructions to replace a controller in the StorageGRID appliance, because the procedures aren't the same.

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.

If your appliance 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.

> When possible, place the appliance into maintenance mode for this replacement procedure to minimize the potential impact of unforeseen errors or failures.

> If the second controller in the shelf does not have Optimal status or if the Recovery Guru indicates that it is not OK to remove the controller, contact technical support.

When you replace a controller, you must remove the battery from the original controller and install it in the replacement controller. In some cases, you might also need to remove the host interface card from the original controller and install it in the replacement controller.

> The storage controllers in most appliance models don't include host interface cards (HIC).

Step 1: Prepare the replacement controller

Prepare the replacement E2800A or E2800B controller.

Steps

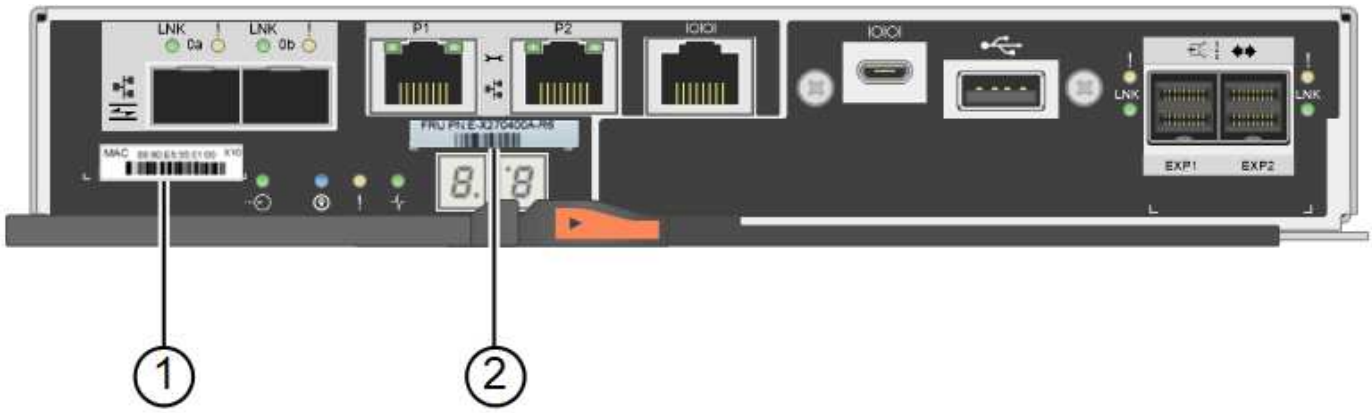
1. Unpack the new controller, and set it on a flat, static-free surface.

   Save the packing materials to use when shipping the failed controller.

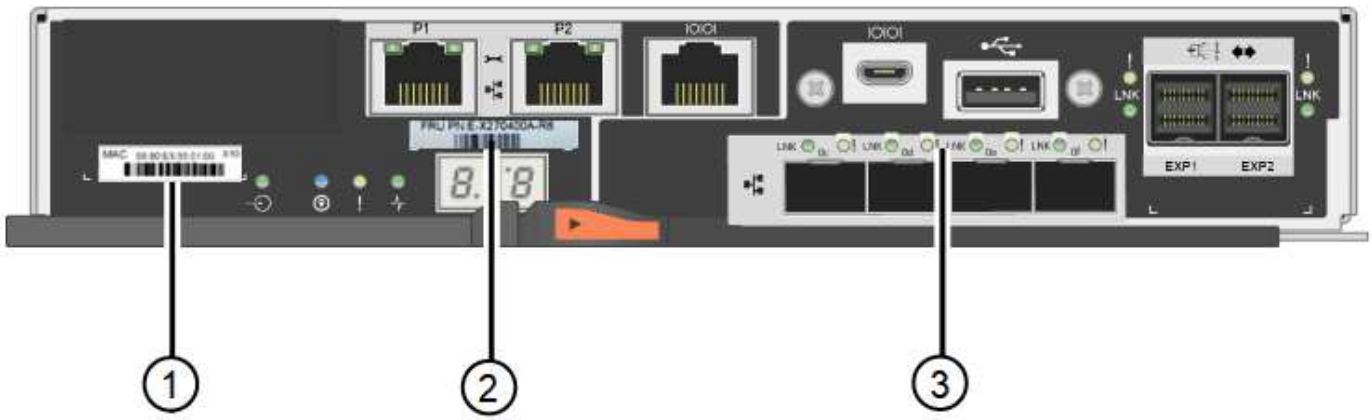
2. Locate the MAC address and FRU part number labels on the back of the replacement controller.

These figures show the E2800A controller and the E2800B controller. The procedure for replacing the E2800 series controllers and the EF570 controller is identical.

E2800A storage controller:



E2800B storage controller:



Label	component	Description
1	MAC address	The MAC address for management port 1 (“P1 on the E2800A and 0a on the E2800B”). 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	4-port HIC	The 4-port host interface card (HIC). This card must be moved to the new controller when you perform the replacement. **Note**: the E2800A controller does not have a HIC.

Step 2: Take the controller offline

Prepare to remove the failed controller and and take it offline.

Steps

1. Prepare to remove the controller. You use SANtricity System Manager to perform these steps.
   a. 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 aren't the same, don't attempt this procedure.

   b. Back up the configuration database.

      If a problem occurs when you remove a controller, you can use the saved file to restore your configuration.

   c. 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 if the replacement does not resolve the problem.

   d. Take the controller you plan to replace offline.
2. Power off the controller shelf.

Step 3: Remove the controller

Remove the failed controller from the appliance.

Steps

1. Put on an ESD wristband or take other antistatic precautions.
2. Label the cables and then disconnect the cables and SFPs.

   To prevent degraded performance, don't twist, fold, pinch, or step on the cables.
3. 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.
4. 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.
5. Place the controller on a flat, static-free surface with the removable cover facing up.
6. Remove the cover by pressing down on the button and sliding the cover off.

Step 4: Move battery to the new controller

Remove the battery from the failed controller, and install it into the replacement controller.

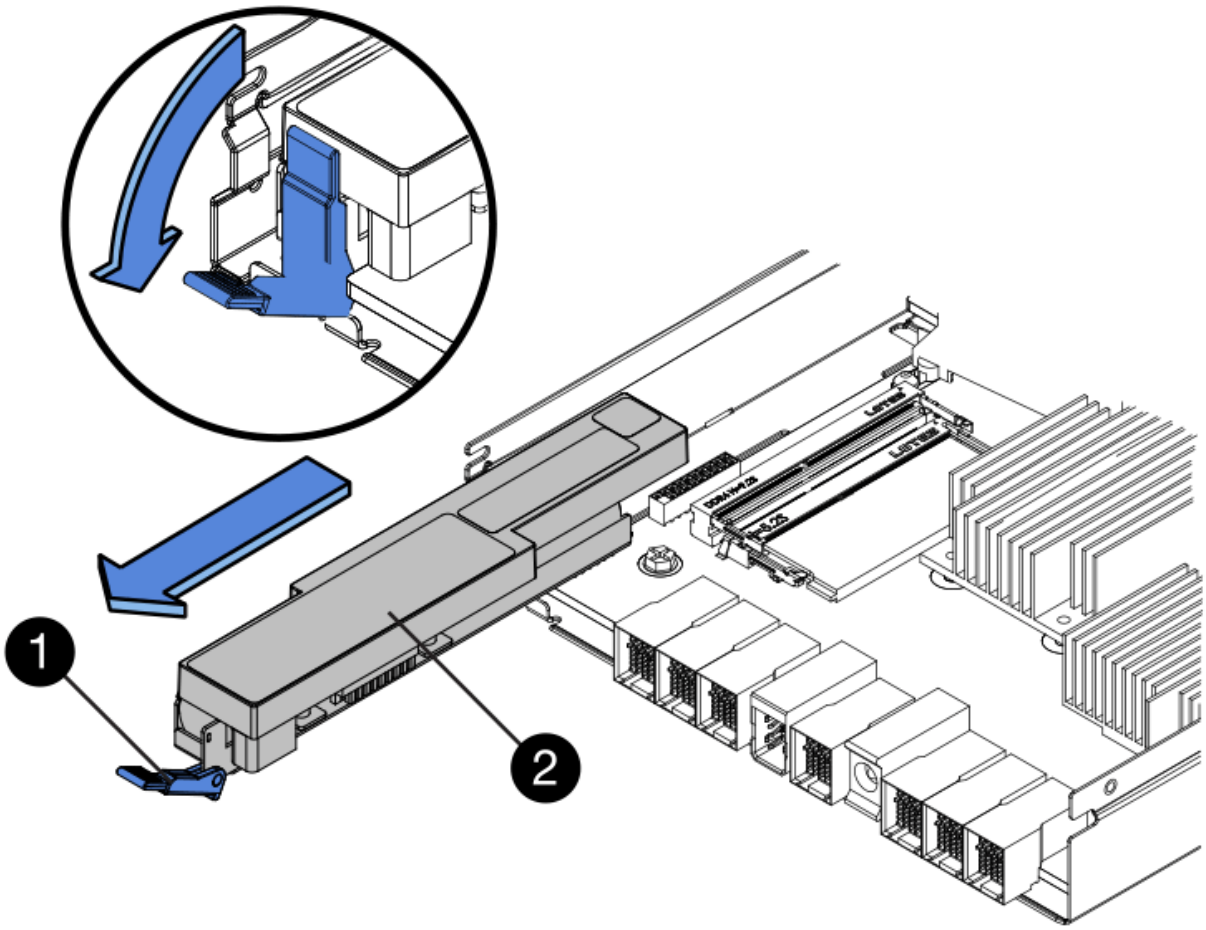
Steps

1. 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
1	Internal Cache Active LED
2	Battery

2. Locate the blue release latch for the battery.
3. Unlatch the battery by pushing the release latch down and away from the controller.



Item	Description
1	Battery release latch
2	Battery

4. Lift up on the battery, and slide it out of the controller.
5. Remove the cover from the replacement controller.
6. Orient the replacement controller so that the slot for the battery faces toward you.
7. 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.

8. Move the battery latch up to secure the battery.

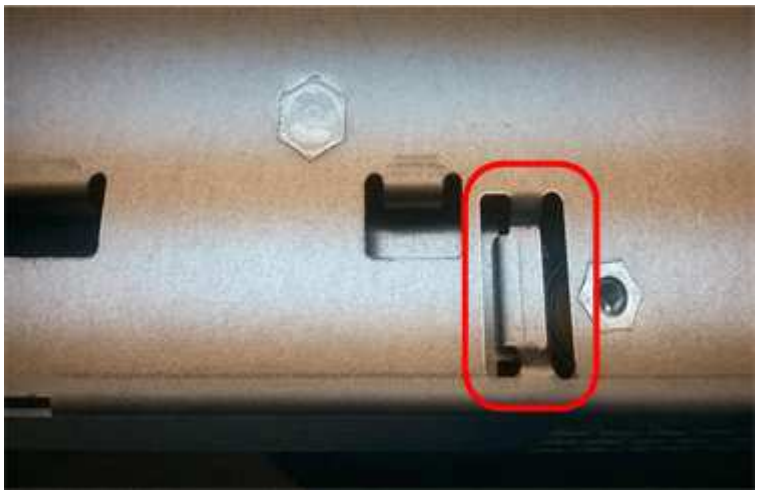
   When the latch clicks into place, the bottom of the latch hooks into a metal slot on the chassis.

9. 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 into the slot on the controller:**

- **Incorrect — The battery's metal flange is not inserted into the slot on the controller:**



10. Replace the controller cover.

Step 5: Move HIC to new controller, if needed

If the failed controller includes a host interface card (HIC), move the HIC from the failed controller to the replacement controller.

A separate HIC is used for the E2800B controller only. The HIC is mounted to the main controller board and includes two SPF connectors.

The illustrations in this procedure show a 2-port HIC. The HIC in your controller might have a different number of ports.

E2800A

An E2800A controller does not have a HIC.

Replace the E2800A controller cover, and go to Step 6: Replace controller

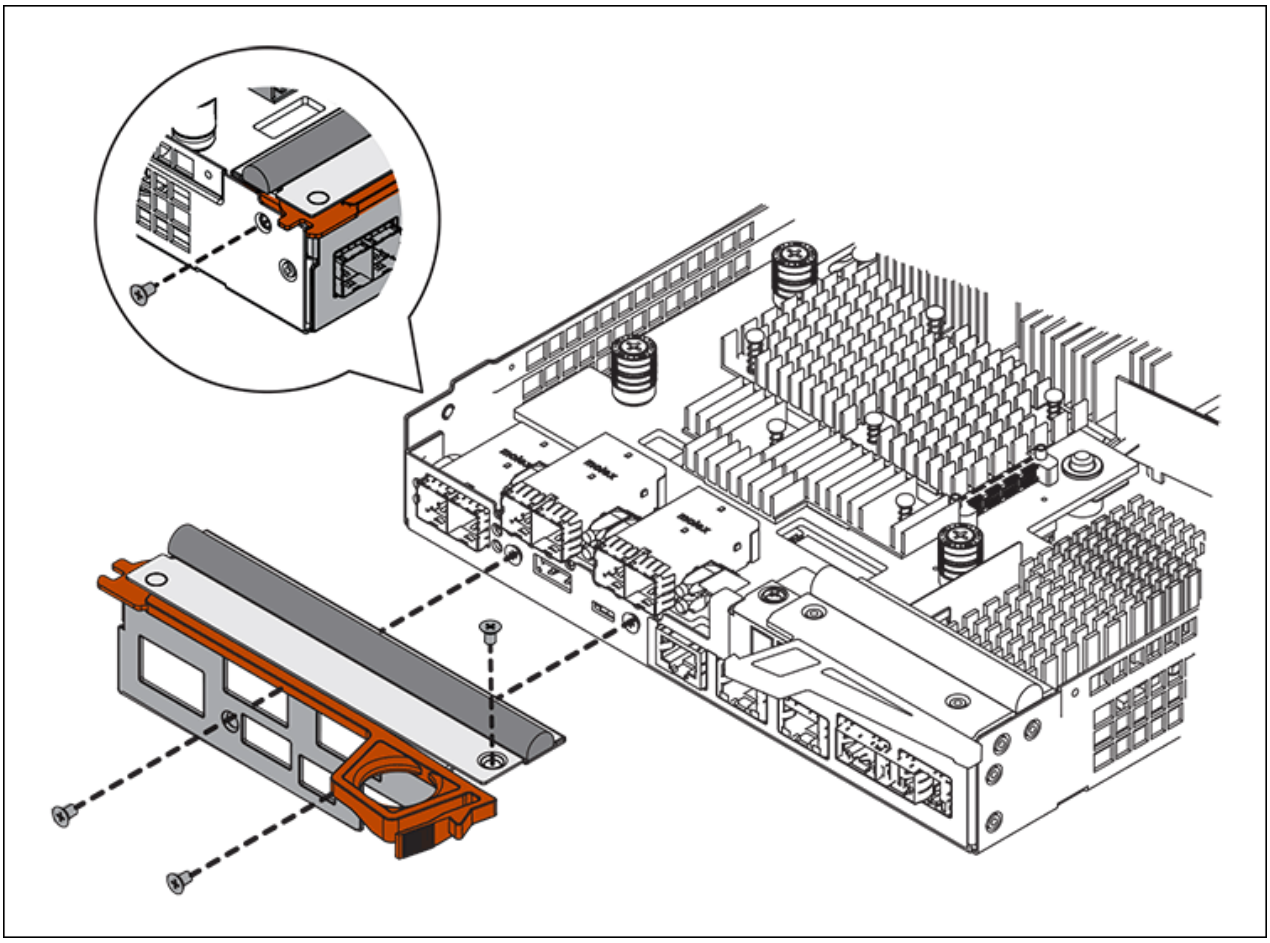
E2800B

Move the HIC from the failed E2800B controller to the replacement controller.

Steps

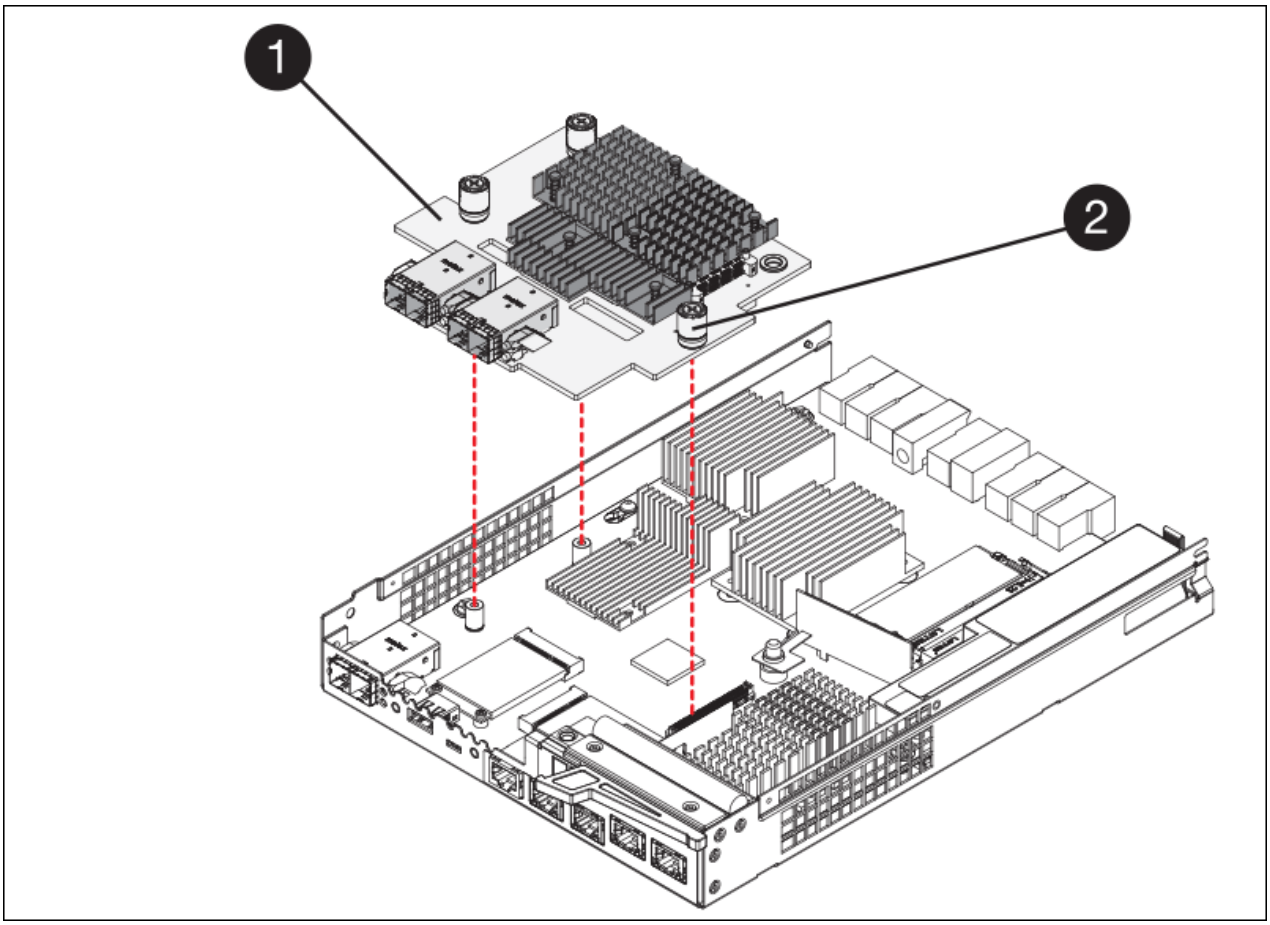
1. Remove any SFPs from the HIC.
2. Using a #1 Phillips screwdriver, remove the screws that attach the HIC faceplate to the controller.

   There are four screws: one on the top, one on the side, and two on the front.



3. Remove the HIC faceplate.
4. Using your fingers or a Phillips screwdriver, loosen the three thumbscrews that secure the HIC to the controller card.
5. Carefully detach the HIC from the controller card by lifting the card up and sliding it back.

> Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.



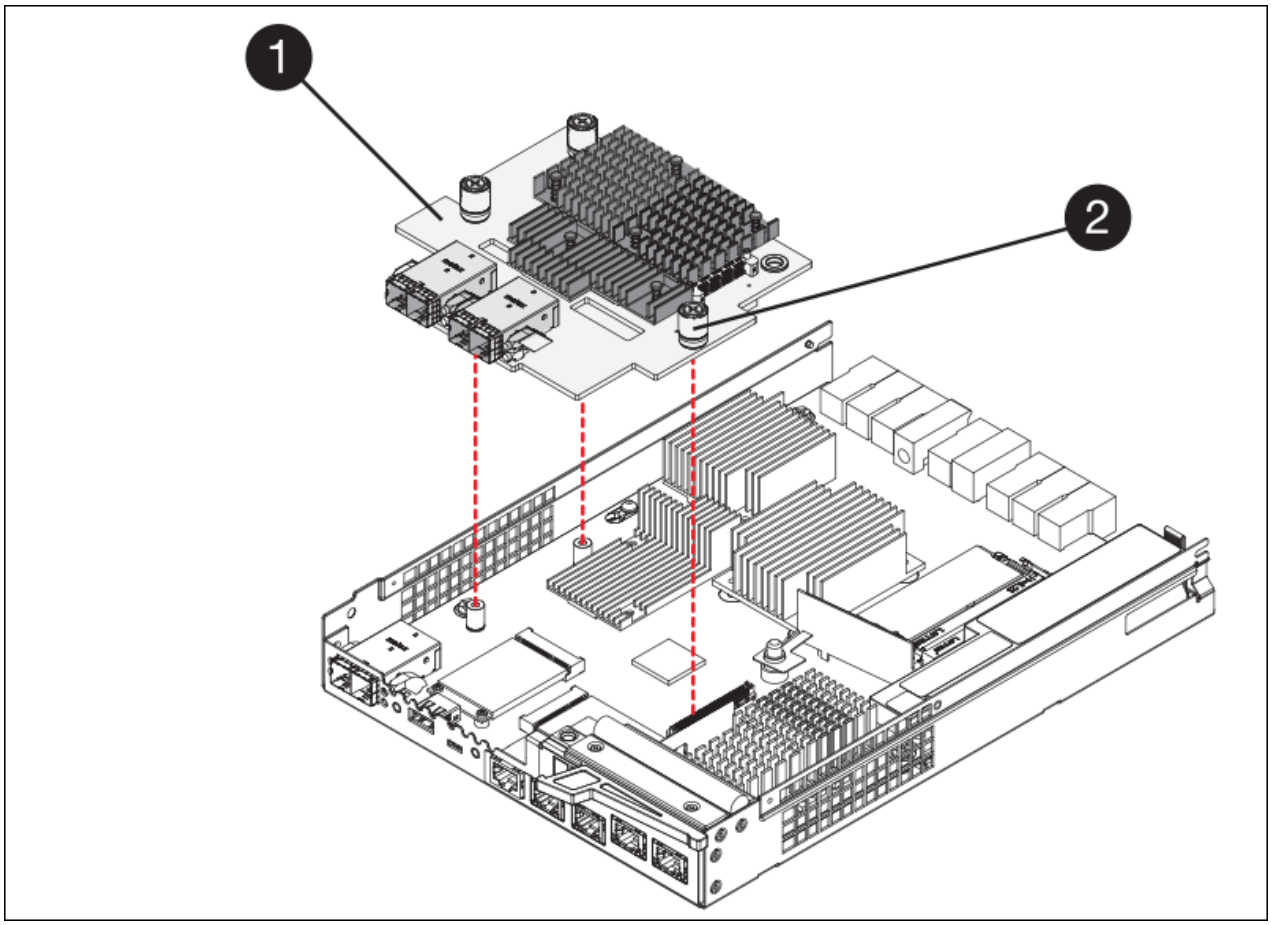
Label	Description
1	Host interface card
2	Thumbscrews

6. Place the HIC on a static-free surface.
7. Using a #1 Phillips screwdriver, remove the four screws that attach the blank faceplate to the replacement controller, and remove the faceplate.
8. Align the three thumbscrews on the HIC with the corresponding holes on the replacement controller, and align the connector on the bottom of the HIC with the HIC interface connector on the controller card.

   Be careful not to scratch or bump the components on the bottom of the HIC or on the top of the controller card.

9. Carefully lower the HIC into place, and seat the HIC connector by pressing gently on the HIC.

Possible equipment damage — Be careful not to pinch the gold ribbon connector for the controller LEDs between the HIC and the thumbscrews.

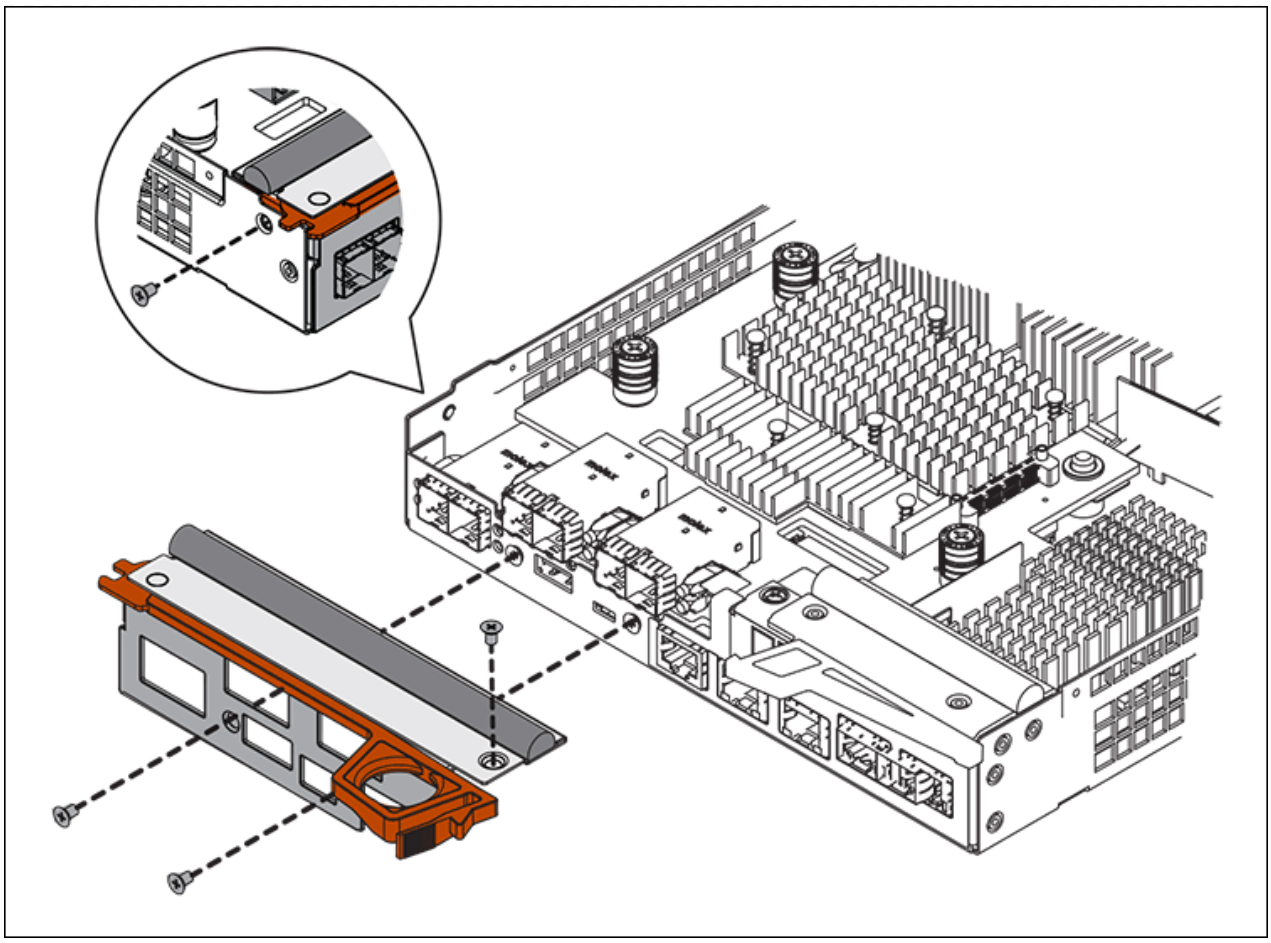


Label	Description
1	Host interface card
2	Thumbscrews

10. Hand-tighten the HIC thumbscrews.

    Don’t use a screwdriver, or you might over tighten the screws.

11. Using a #1 Phillips screwdriver, attach the HIC faceplate you removed from the original controller to the new controller with four screws.



12. Reinstall any removed SFPs into the HIC.

Step 6: Replace controller

Install the replacement controller and verify that it has rejoined the grid.

Steps

1. 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. Power on the controller shelf.
   f. 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.

2. 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`.

3. Confirm that the new controller is Optimal, and collect support data.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace hardware components in SG6000 storage controller shelf

If a hardware problem occurs, you might need to replace a component in the storage controller shelf.

Before you begin

- 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.

  Locate controller in data center

About this task

To replace the battery in the storage controller, see the steps in the 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
Drive	E-Series: • Replace drive (60-drive) • Replace drive (12-drive or 24-drive)
Power canister	E-Series • Replace power canister (60-drive) • Replace power supply (12-drive or 24-drive)
Fan canister (60-drive shelves only)	E-Series: Replace fan canister (60-drive)

FRU	See instructions
Drive drawer (60-drive shelves only)	E-Series: Replace drive drawer (60-drive)

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace hardware components in optional SG6000 60-drive expansion shelf

You might need to replace an input/output module, a power supply, or a fan in the expansion shelf.

Before you begin

- 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.

  Locate controller in data center

About this task

To replace an input/output module (IOM) in a 60-drive expansion shelf, see the steps in the 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)

Replace SG6000-CN controller

You might need to replace the SG6000-CN controller if it is not functioning optimally or if it has failed.

Before you begin

- 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.

  Locate controller in 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 can't 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. Display the current configurations of the appliance and record them.
   a. Log in to the appliance to be replaced:
      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: **`run-host-command ipmitool lan print`** to display the current BMC configurations for the appliance.
2. If the SG6000-CN controller is functioning sufficiently to allow for a controlled shutdown, shut down the SG6000-CN controller.
3. If any of the network interfaces on this StorageGRID appliance are configured for DHCP, you might need to update the permanent DHCP lease assignments on the DHCP servers to reference the MAC addresses of the replacement appliance. The update ensures the appliance is assigned the expected IP addresses. See Update MAC address references.
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, don't 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.

      When the controller starts, it automatically installs pending updates for the controller and appliance components. Installation of these updates can take an hour or more to complete, and the controller might reboot multiple times.

      > Do not manually reboot the appliance unless you are certain that it is *not* in the middle of a firmware update.

You can connect a monitor or service laptop to the SG6000-CN controller to monitor update installation progress.

> A service-laptop connection might not be available at some stages of the installation process.

5. If the appliance where you replaced the controller used a key management server (KMS) to encrypt data, additional configuration might be required before the node can join the grid. If the node does not automatically join the grid, make sure that these configuration settings have transferred to the new controller and manually configure any settings that don't have the expected configuration:
   - Configure network links
   - Configure StorageGRID IP addresses
   - Configure node encryption for the appliance
6. Log in to the appliance with the replaced controller:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
7. Restore BMC network connectivity for the appliance. There are two options:
   - Use static IP, netmask, and gateway
   - Use DHCP to obtain an IP, netmask, and gateway
     a. To restore the BMC configuration to use a static IP, netmask, and gateway, enter the following commands:

     ```
     run-host-command ipmitool lan set 1 ipsrc static

     run-host-command ipmitool lan set 1 ipaddr Appliance_IP

     run-host-command ipmitool lan set 1 netmask Netmask_IP

     run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
     ```

     b. To restore the BMC configuration to use DHCP to obtain an IP, netmask, and gateway, enter the following command:

     ```
     run-host-command ipmitool lan set 1 ipsrc dhcp
     ```
8. After restoring BMC network connectivity, connect to the BMC interface to audit and restore any additional custom BMC configuration you might have applied. For example, you should confirm the settings for SNMP trap destinations and email notifications. See Configure BMC interface.
9. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Related information

Install SG6000-CN into cabinet or rack

View status indicators

View boot-up codes for SG6000-CN controller

Replace one or both power supplies 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. Both power supplies operating in the controller must be the same model and wattage.

Before you begin

- You have determined the physical location in the data center of the controller with the power supply to be replaced.

  Locating the controller in a data center

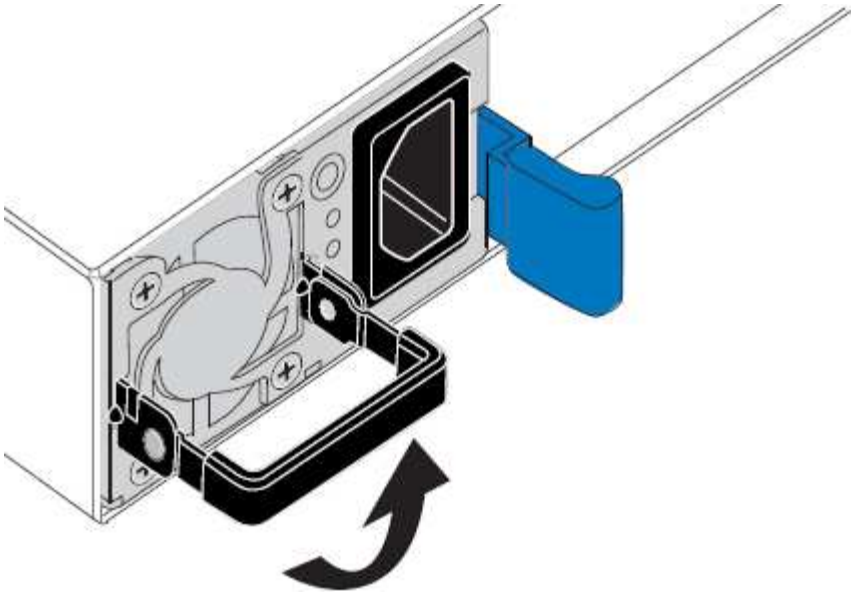
- If you are replacing only one power supply:
  - You have unpacked the replacement power supply unit and ensured that it is the same model and wattage as the power supply unit you are replacing.
  - You have confirmed that the other power supply is installed and running.
- If you are replacing both power supplies at the same time:
  - You have unpacked the replacement power supply units and ensured they are the same model and wattage.

About this task

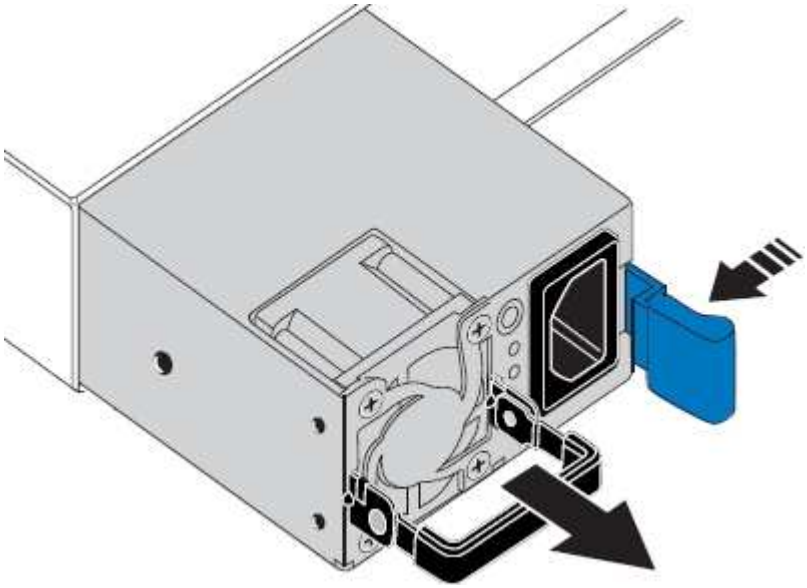
The figure shows the two power supply units for the SG6000-CN controller, which are accessible from the back of the controller. Use this procedure to replace one or both of the power supplies. If you are replacing both power supplies, you must first perform a controlled shut down of the appliance.

Steps

1. If you are replacing only one power supply, you don't need to shut down the appliance. Go to the Unplug the power cord step. If you are replacing both power supplies at the same time, do the following before unplugging the power cords:
   a. Shut down the appliance.
2. Unplug the power cord from each power supply to be replaced.
3. Lift the cam handle on the first supply to be replaced.



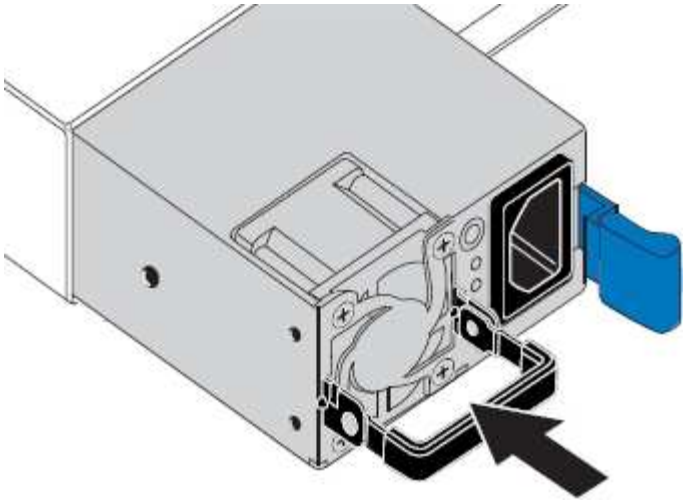
4. Press the blue latch and pull the power supply out.



5. With the blue latch on the right, slide the replacement power supply into the chassis.

   Both power supplies must be the same model and wattage.

   Ensure that the blue latch is on the right side when you slide the replacement unit in.



6. Push the cam handle down to secure the replacement power supply.
7. If you are replacing both power supplies, repeat steps 2 though 6 to replace the second power supply.
8. Connect the power cords to the replaced units and apply power.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Relocate SG6000-CN controller in cabinet or rack

Remove the SG6000-CN controller from a cabinet or rack to access the top cover or to move the appliance to a different location, then reinstall the controller into a cabinet or rack when hardware maintenance is complete.

Remove SG6000-CN controller from 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.

Before you begin

- 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.

  Locate controller in data center

- You have shut down the SG6000-CN controller.

  Don’t 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, don’t 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.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Reinstall SG6000-CN controller into cabinet or rack

Reinstall the controller into a cabinet or rack when hardware maintenance is complete.

Before you begin

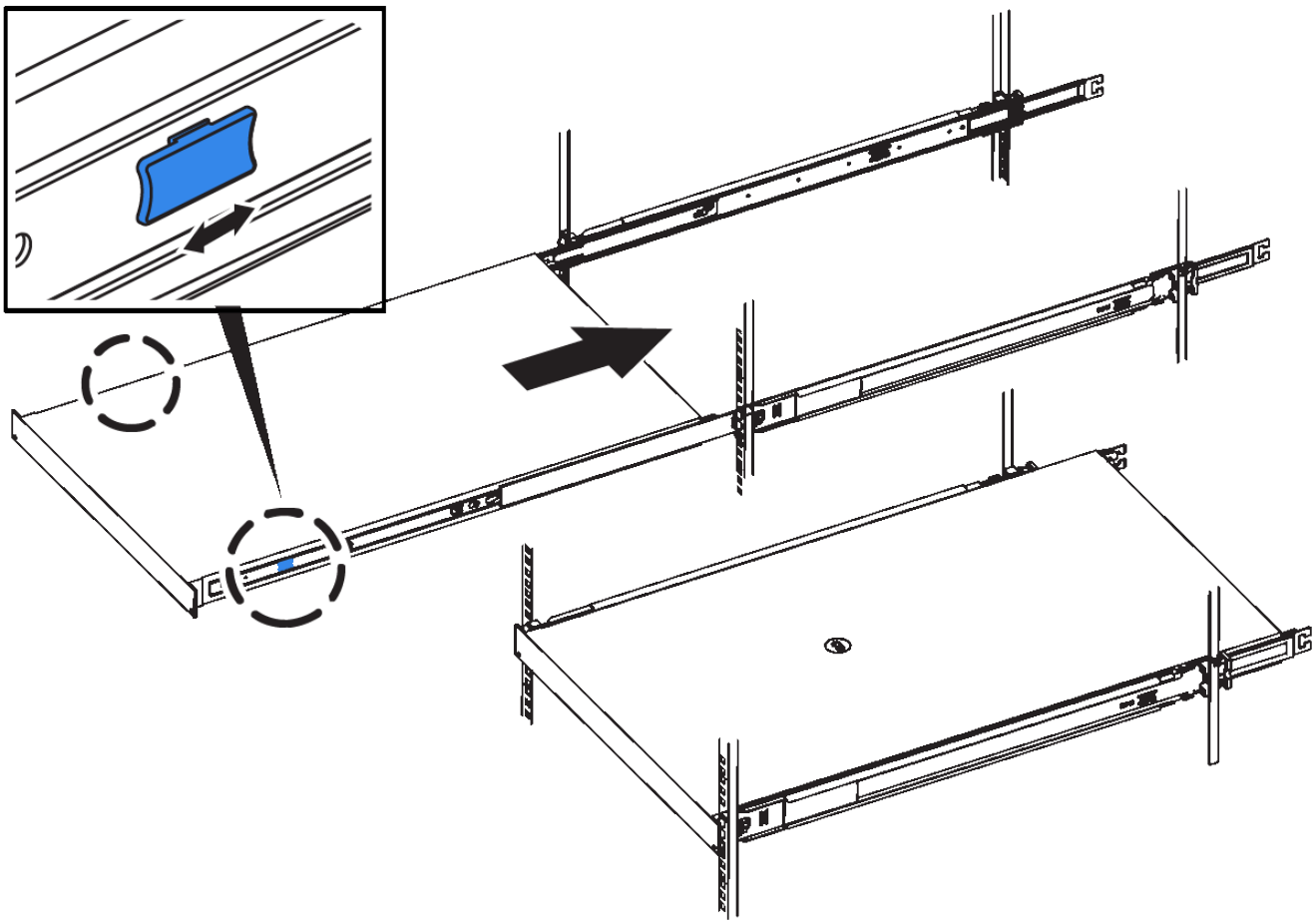
You have reinstalled the controller cover.

Reinstall 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 can’t move the controller any further, pull the blue latches on both sides of the chassis to slide the controller all the way in.



Don’t 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, don’t twist, fold, pinch, or step on the cables.

Cable appliance

5. Reconnect the controller power cables.

Connect power cords and apply power (SG6000)

After you finish

The controller can be restarted restarted.

Replace SG6000 controller cover

Remove the appliance cover to access internal components for maintenance, and replace the cover when you are finished.

Remove SG6000-CN controller cover

Remove the controller cover to access internal components for maintenance.

Before you begin

Remove the controller from the cabinet or rack to access the top cover.

Remove SG6000-CN controller from 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.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Reinstall SG6000-CN controller cover

Reinstall the controller cover when internal hardware maintenance is complete.

Before you begin

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.

Replace Fibre Channel HBA in SG6000

You might need to replace a Fibre Channel HBA if it is not functioning optimally or if it has failed.

Verify Fibre Channel HBA to replace

If you are unsure which Fibre Channel host bus adapter (HBA) to replace, complete this procedure to identify it.

Before you begin

- 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.

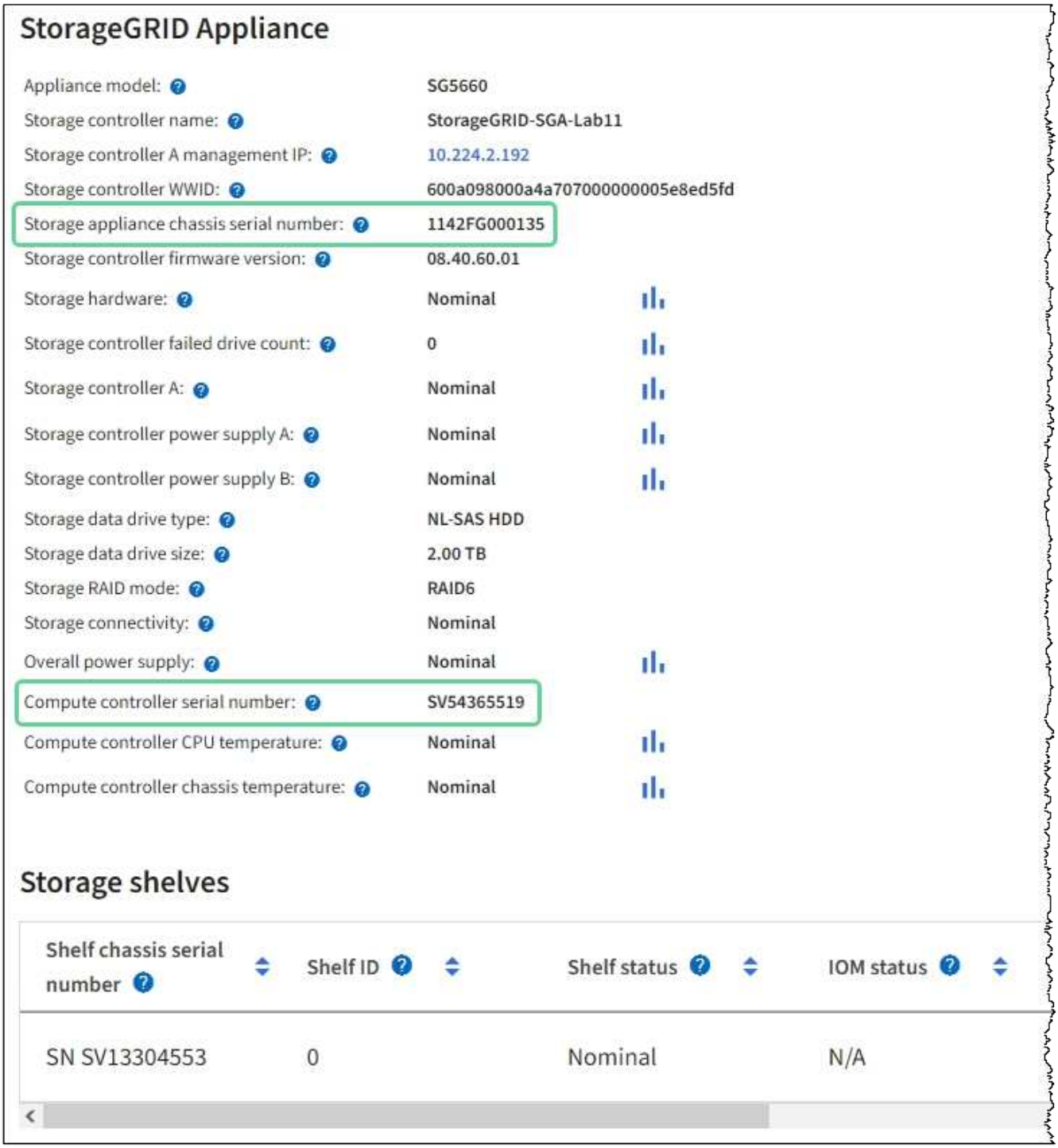
- You are signed in to the Grid Manager using a supported web browser.

Steps

1. From the Grid Manager, select **NODES**.
2. From the table on 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. 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.



   - 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 or SG6060X, select a different node from the tree view.
   - If the serial numbers don't 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.

Remove 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.

Before you begin

- You have the correct replacement Fibre Channel HBA.
- You have determined which SG6000-CN controller contains the Fibre Channel HBA to replace.
- You have physically located the SG6000-CN controller in the data center.
- You have shut down the SG6000-CN controller.

  A controlled shutdown is required before you remove the controller from the rack.

- You have removed the controller from the cabinet or rack.
- You have removed the controller cover.

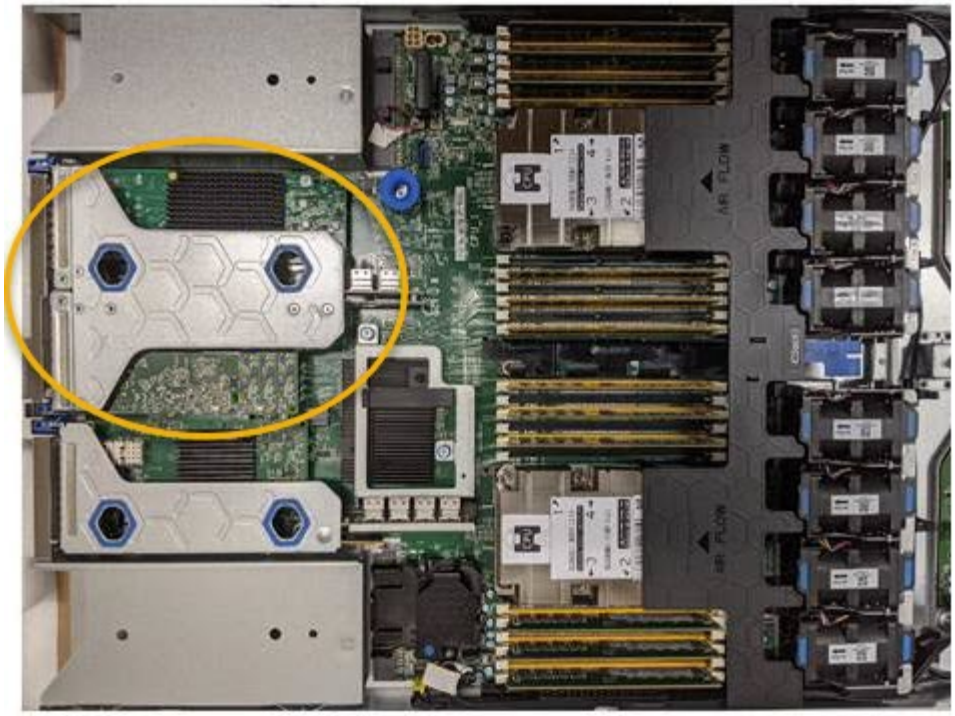
About this task

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 acceptable. See the information about monitoring node connection states.

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 why you should not use single-copy replication.

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. Don’t use excessive force.
6. Place the adapter on a flat anti-static surface.

After you finish

Install the replacement Fibre Channel HBA.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Reinstall Fibre Channel HBA

The replacement Fibre Channel HBA is installed into the same location as the one that was removed.

Before you begin

- You have the correct replacement Fibre Channel HBA.
- You have removed the existing Fibre Channel HBA.

  Remove 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.

Maintain SG6100 storage appliance hardware

Maintain SG6100 appliance

You might need to perform maintenance procedures on your appliance. Procedures specific to maintaining your SG6100 appliance are in this section.

The procedures in this section assume that the appliance has already been deployed as a Storage Node in a StorageGRID system.

Configuration maintenance procedures are performed using the Appliance Installer, Grid Manager, or BMC interface. These procedures include:

- Turn appliance identify LED on and off
- Locate appliance in data center
- Shut down the appliance
- Change link configuration of the appliance

Hardware maintenance procedures require the physical manipulation of specific SGF6112 components.

Drive firmware upgrade

The firmware on the drives in the SGF6112 is automatically checked every time the appliance is rebooted. When necessary, the firmware is automatically upgraded to the version expected by the current StorageGRID release. Usually, firmware upgrades occur during StorageGRID software upgrades. Any necessary drive firmware upgrades for existing StorageGRID versions will be included in hotfixes. Follow the instructions provided with each hotfix to ensure that the upgrade is applied to all drives that could benefit from it.

SANtricity System Manager is not needed to maintain the SGF6112 appliance.

General Maintenance procedures

See Common maintenance procedures for procedures that are the same for all appliances, such as applying a hotfix, recovering a node or site, and performing network maintenance.

See Set up appliance hardware for appliance maintenance procedures that are also performed during initial appliance installation and configuration.

Configuration maintenance procedures

Use the Manage drives tab

You can use the Manage drives tab in the Grid Manager to perform troubleshooting and

maintenance tasks on the drives in the SGF6112 appliance.

Before you begin

- You are signed in to the Grid Manager using a supported web browser.

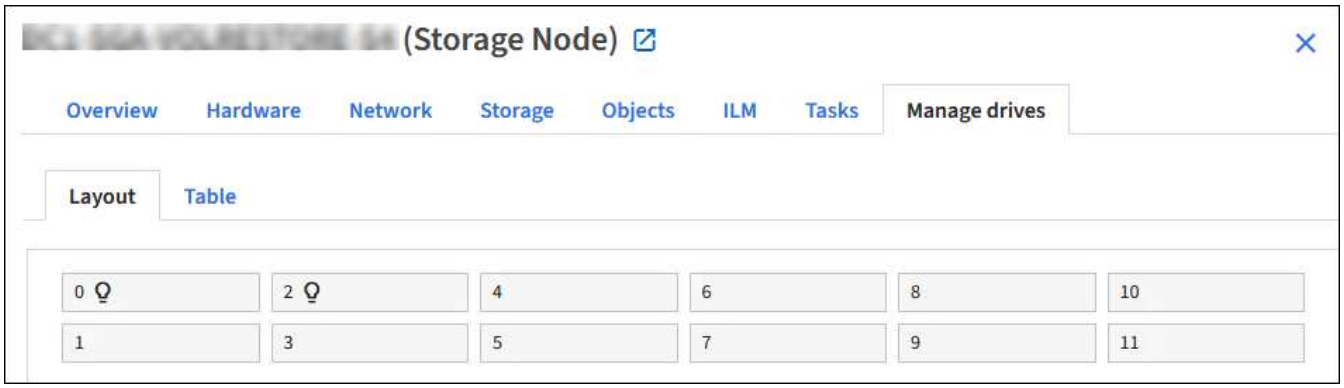
About this task

If you have an SGF6112 appliance and either the Storage appliance administrator or Root access permission, a Manage drives tab appears on the appliance details page.

The Manage drives tab contains the following views:

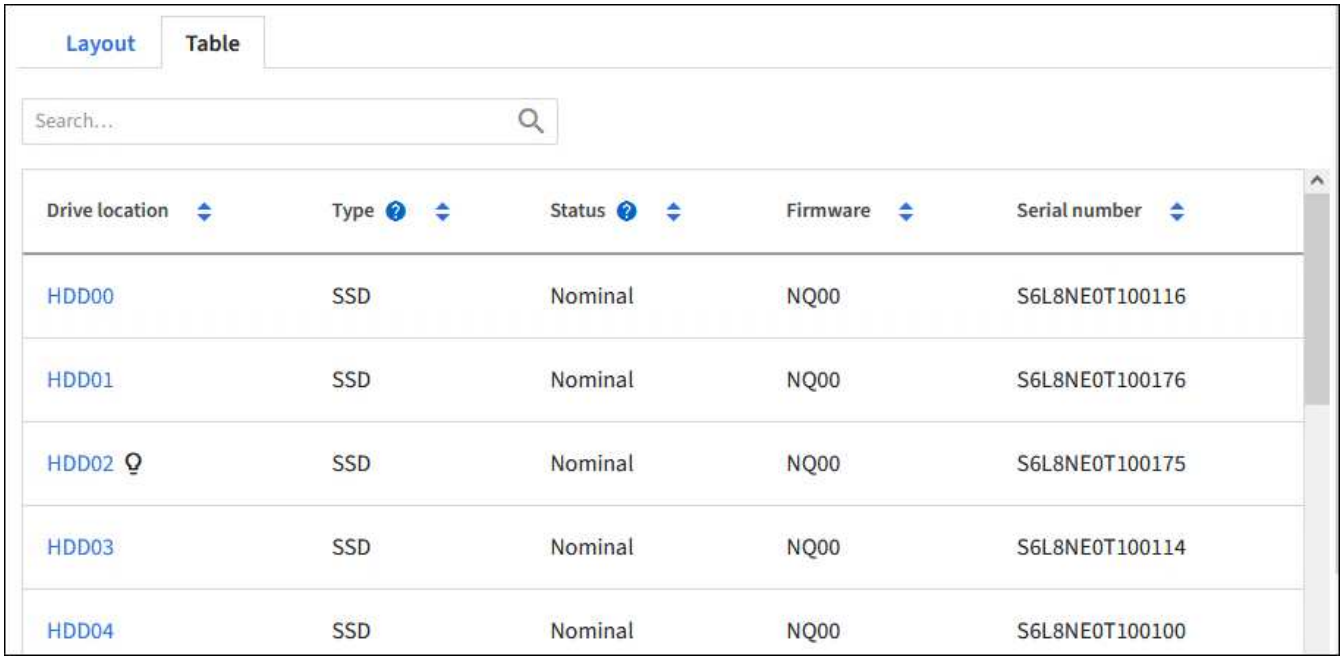
Layout

Layout of data storage drives in the appliance. Select a drive to view drive details.



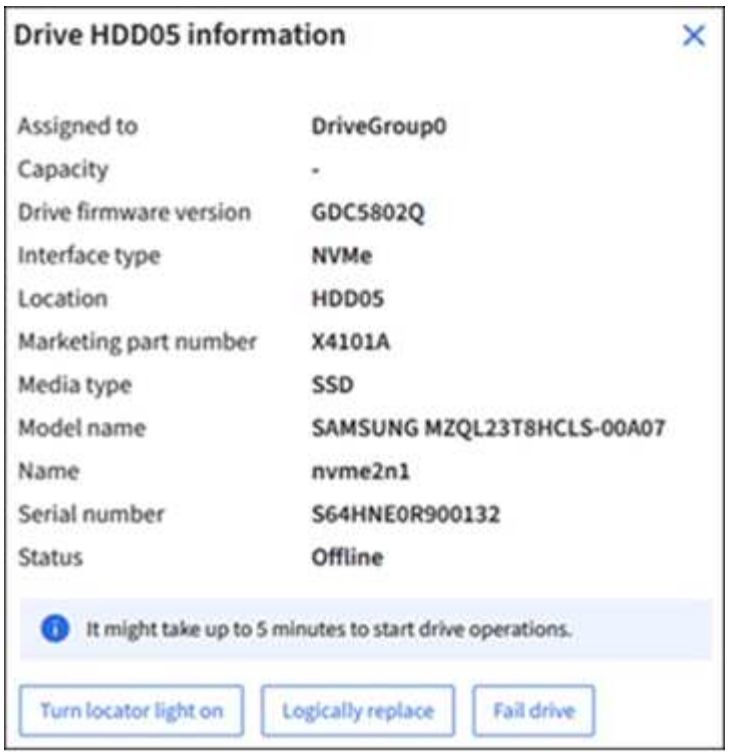
Table

Lists information for each drive. Select a drive to view drive details.



Drive details

Summary for each drive. Select the appropriate task button, as described in the steps below.



Turn locator light on or off

To physically locate a drive in the appliance:

1. From the Grid Manager, select **NODES** > ***data center***.
2. Select ***appliance storage node*** > **Manage drives** > **Layout** > ***drive***.

   The drive details panel appears.

3. Select **Turn locator light on**.
   - A light bulb icon appears for the drive.
   - An amber LED blinks on the physical drive.
4. When you want to turn off the locator light, select **Turn locator light off**.

Logically replace drive

If a drive in the storage appliance needs to be rebuilt or reinitialized:

1. From the Grid Manager, select **NODES** > ***data center***.
2. Select ***appliance storage node*** > **Manage drives** > **Layout** > ***drive***.

   The drive details panel appears.

3. Select **Logically replace**.

   On the drive details panel, the drive's status indicates *Rebuilding*. Rebuilding a drive could take up to 5 minutes.

Fail drive

For troubleshooting, you can manually "fail" a drive that you suspect is faulty. The system will then run without that drive.

1. From the Grid Manager, select **NODES** > ***data center***.
2. Select ***appliance storage node*** > **Manage drives** > **Layout** > ***drive***.

   The drive details panel appears.

3. Select **Fail drive**.

After you fail a drive, you must either physically replace the drive or logically replace the drive.

Turn SGF6112 appliance identify LED on and off

The blue identify LED on the front and back of the appliance can be turned on to help locate the appliance in a data center.

Before you begin

You have the BMC IP address of the appliance you want to identify.

Steps

1. Access the appliance BMC interface.
2. Select **Server Identify**.

   The current status of the identify LED is selected.

3. Select **ON** or **OFF**, and then select **Perform Action**.

   When you select **ON**, the blue identify LEDs light on the front (typical shown) and rear of the appliance.

   If a bezel is installed on the controller, it might be difficult to see the front identify LED.

   The rear identify LED is at the center of the appliance below the Micro-SD slot.

4. Turn the identify LEDs on and off as needed.

Related information

Locate appliance in data center

Locate SGF6112 appliance in data center

Locate the appliance so that you can perform hardware maintenance or upgrades.

Before you begin

- You have determined which appliance requires maintenance.
- To help locate the appliance in your data center, turn on the blue identify LED.

Steps

1. Find the appliance in the data center.
   - Look for a lit blue identify LED on the front or rear of the appliance.

     The front identify LED is behind the front bezel and might be difficult to see if the bezel is installed.

     The rear identify LED is at the center of the appliance below the Micro-SD slot.

   - Check the tags attached to the front of the appliance for a matching part number to confirm you have found the correct appliance.
2. Remove the front bezel, if one is installed, to access the front panel controls and indicators.

After you finish

Turn off the blue identify LED if you used it to locate the appliance.
Press the identify LED switch on the appliance front panel.
Use the appliance BMC interface.

Power SGF6112 appliance off and on

You can shut down the SGF6112 appliance and power it back on to perform maintenance.

Shut down the SGF6112 appliance

Shut down the appliance to perform hardware maintenance.

Before you begin

- You have physically located the appliance.

About this task

To prevent service interruptions, shut down the appliance during a scheduled maintenance window when periods of service disruption are acceptable.

Steps

1. Shut down the appliance:

   > You must perform a controlled shut down of the appliance by entering the commands specified below. It is a best practice to perform a controlled shutdown when possible to avoid unnecessary alerts, ensure full logs are available, and avoid service disruptions.

   a. If you have not already logged into the grid node, log in 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 appliance:
      `shutdown -h now`

      This command might take up to 10 minutes to complete.

2. Use one of the following methods to verify that the appliance is powered off:
   - Look at the power LED on the front of the appliance and confirm that it is off.
   - Check the Power Control page of the BMC interface to confirm the appliance is off.

Power on SGF6112 and verify operation

Power on the controller after completing maintenance.

Before you begin

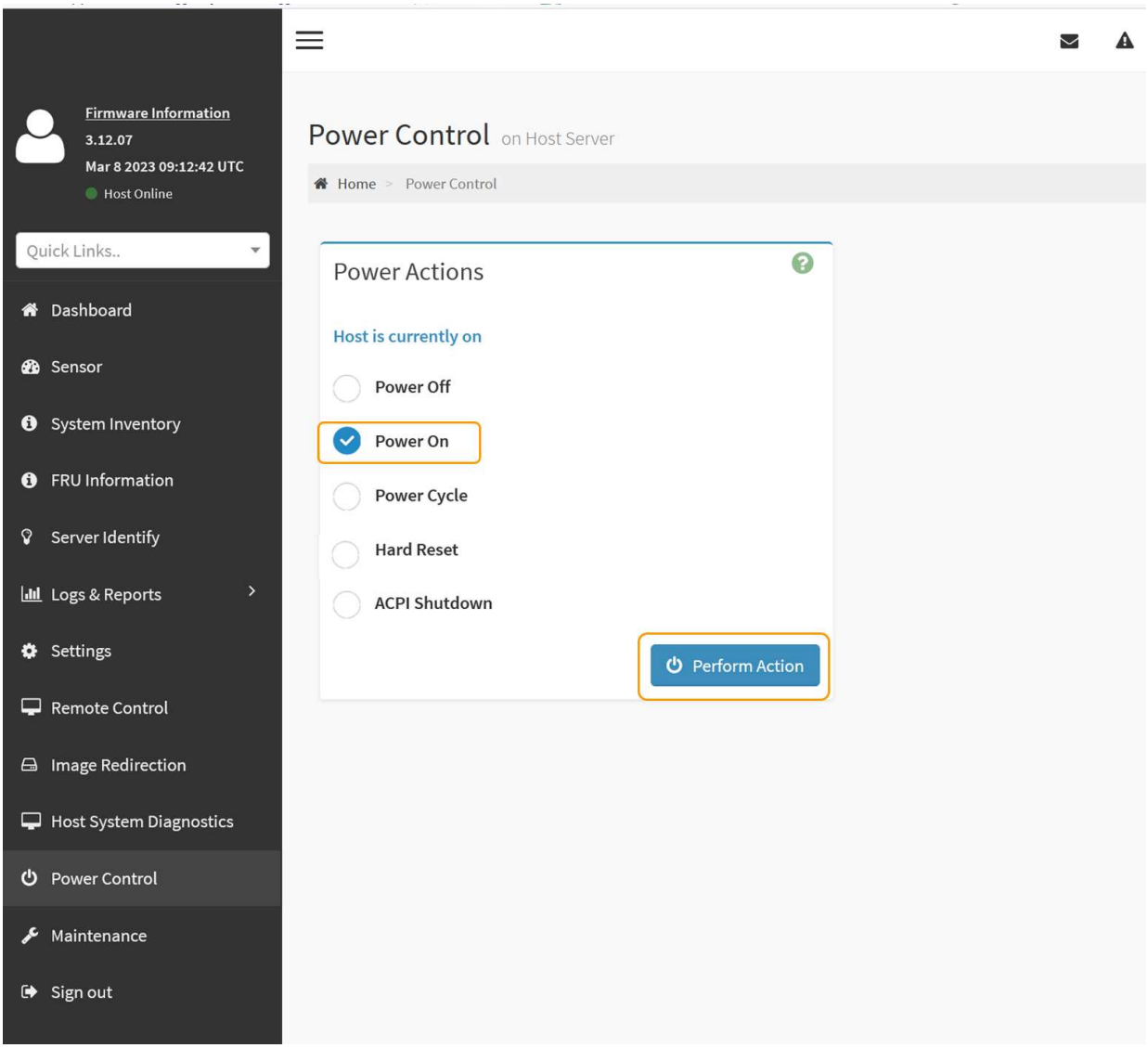
- You have installed the controller in a cabinet or rack and connected the data and power cables.
- You have physically located the controller in the data center.

Steps

1. Power on the appliance.

   You might have to remove the bezel to access the power switch; if so, remember to reinstall it afterwards.

2. 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.
      ii. Select **Power Control**.
      iii. Select **Power On** and then select **Perform Action**.



Use the BMC interface to monitor start-up status.

3. 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.

   > Don't take another appliance node offline unless this appliance has a green icon.

4. Confirm that the new appliance is fully operational by logging in to the grid node using PuTTY or another ssh client:
   a. Enter the following command: `ssh Appliance_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.

      When you are logged in as root, the prompt changes from `$` to `#`.

Related information

View status indicators

Change link configuration of SGF6112 appliance

You can change the Ethernet link configuration of the appliance including the port bond mode, the network bond mode, and the link speed.

Before you begin

- You have placed the appliance into maintenance mode.

> In rare instances, placing a StorageGRID appliance into maintenance mode might make the appliance unavailable for remote access.

Steps

1. From the StorageGRID Appliance Installer, select **Configure Networking** > **Link Configuration**.
2. Make the desired changes to the link configuration.

   For more information about the options, see Configure network links.

   > IP configuration changes made while the appliance is in maintenance mode are not applied to the installed StorageGRID environment. Run the `change-ip` command after rebooting the appliance into StorageGRID.

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 aren't 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_IP:8443`**

4. Make any necessary changes to the IP addresses for the appliance.

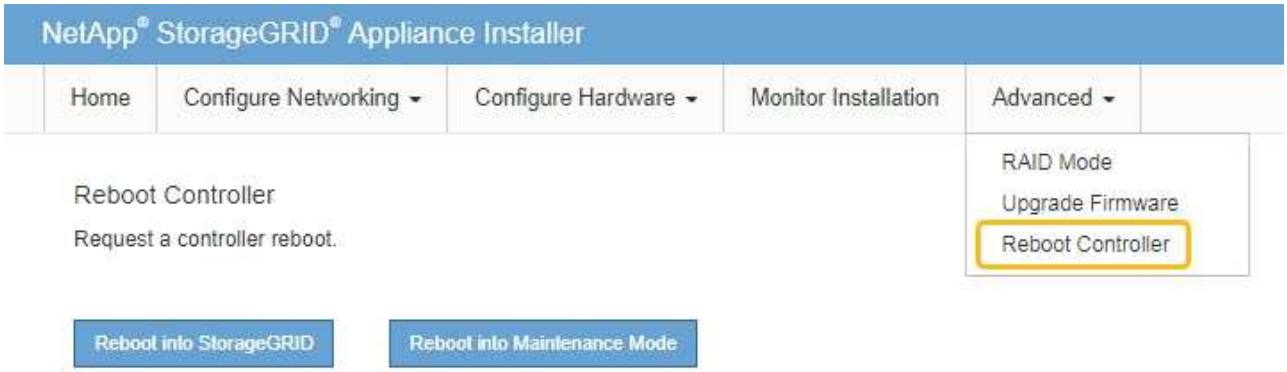
   If you made changes to the VLAN settings, the subnet for the appliance might have changed. If you need to change the IP addresses for the appliance, see Configure StorageGRID IP addresses.

5. Select **Configure Networking** > **Ping Test** from the menu.
6. 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 when configuring the appliance.

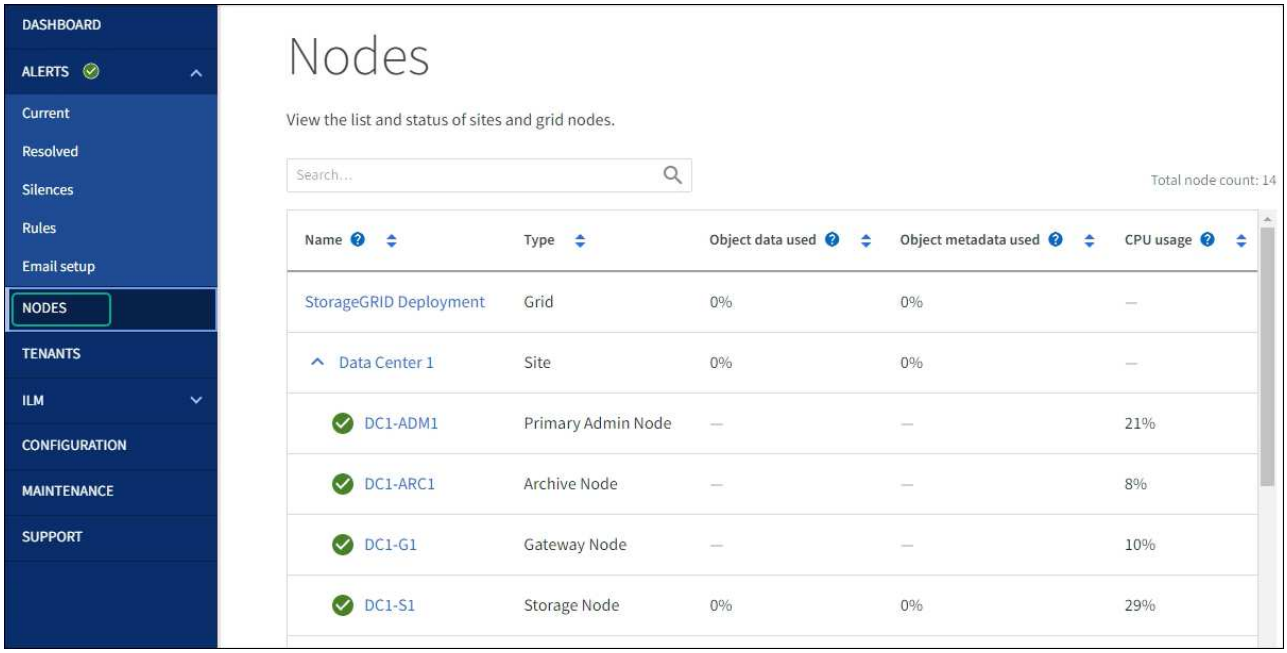
   In addition to any other tests you choose to perform, confirm that you can ping the Grid Network IP address of the primary Admin Node, and the Grid Network IP address of at least one other node. If necessary, return to the instructions for configuring network links and correct any issues.

7. After 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 compute 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 compute controller with the node remaining in

maintenance mode. (This option is available only when the controller is in maintenance mode.) Select this option if there are additional maintenance operations you need to perform on the node before it rejoins 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 page should display a normal status (green check mark icon to the left of the node name) for the appliance node, indicating that no alerts are active and the node is connected to the grid.



Hardware maintenance procedures

Verify component to replace in the SGF6112

If you are unsure which hardware component to replace in your appliance, complete this procedure to identify the component and the location of the appliance in the data center.

Before you begin

- You have the serial number of the storage appliance where the component needs to be replaced.

- You are signed in to the Grid Manager using a supported web browser.

About this task

Use this procedure to identify the appliance with failed hardware and which of the replaceable hardware components is not operating properly. Components that might be identified for replacement include:

- Power supplies
- Fans
- Solid state drives (SSDs)
- Network Interface Cards (NICs)
- CMOS battery

Steps

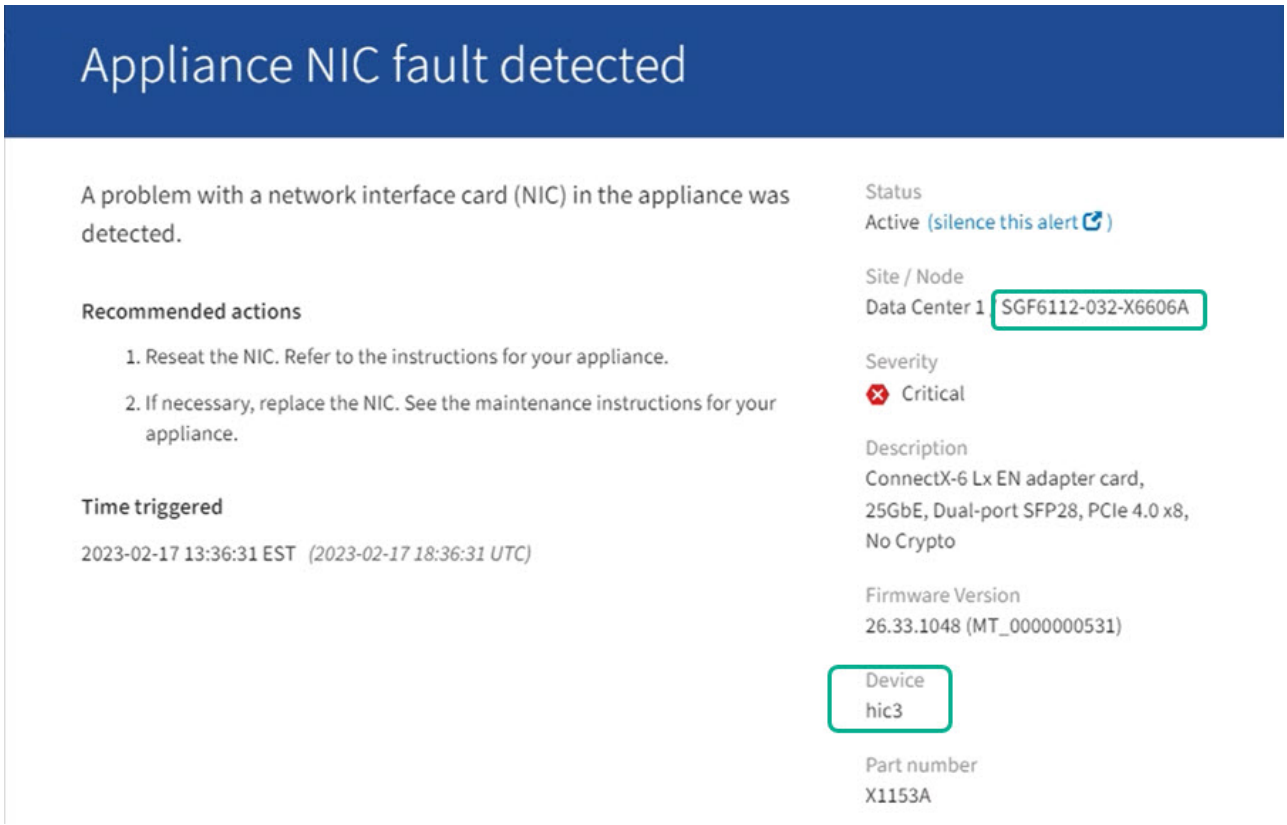
1. Identify the failed component and the name of the appliance that it is installed in.
   a. In Grid Manager, Select **ALERTS** > **Current**.

      The Alerts page appears.

   b. Select the alert to see the alert details.

      Select the alert, not the heading for a group of alerts.

   c. Record the node name and unique identifying label of the component that has failed.



2. Identify the chassis with the component that needs to be replaced.
   a. From the Grid Manager, select **NODES**.

b. From the table on the Nodes page, select the appliance Storage Node name with the failed component.

c. Select the **Hardware** tab.

   Check the **Compute controller serial number** in the StorageGRID Appliance section. Check if the serial number matches the serial number of the storage appliance where you are replacing the component. If the serial number matches, you have found the correct appliance.

   - If the StorageGRID Appliance section in Grid Manager does not display, the node selected is not a StorageGRID appliance. Select a different node from the tree view.
   - If the serial numbers don't match, select a different node from the tree view.

3. After you locate the node where the component needs to be replaced, write down the appliance BMC IP address listed the StorageGRID Appliance section.

   To help you locate the appliance in the data center, you can use the BMC IP address to turn on the appliance identify LED.

Related information

Turn on the appliance identify LED

Replace one or both power supplies in the SGF6112

The SGF6112 appliance 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 appliance has redundant power. Both power supplies operating in the appliance must be of the same model and wattage.

Before you begin

- You have physically located the appliance with the power supply to be replaced.
- You have determined the location of the power supply to replace.
- If you are replacing only one power supply:
  - You have unpacked the replacement power supply unit and ensured that it is the same model and wattage as the power supply unit you are replacing.
  - You have confirmed that the other power supply is installed and running.
- If you are replacing both power supplies at the same time:
  - You have unpacked the replacement power supply units and ensured they are the same model and wattage.

About this task

The figure shows the two power supply units for the SGF6112. The power supplies are accessible from the back of the appliance.

Steps

1. If you are replacing only one power supply, you don't need to shut down the appliance. Go to the Unplug

the power cord step. If you are replacing both power supplies at the same time, do the following before unplugging the power cords:

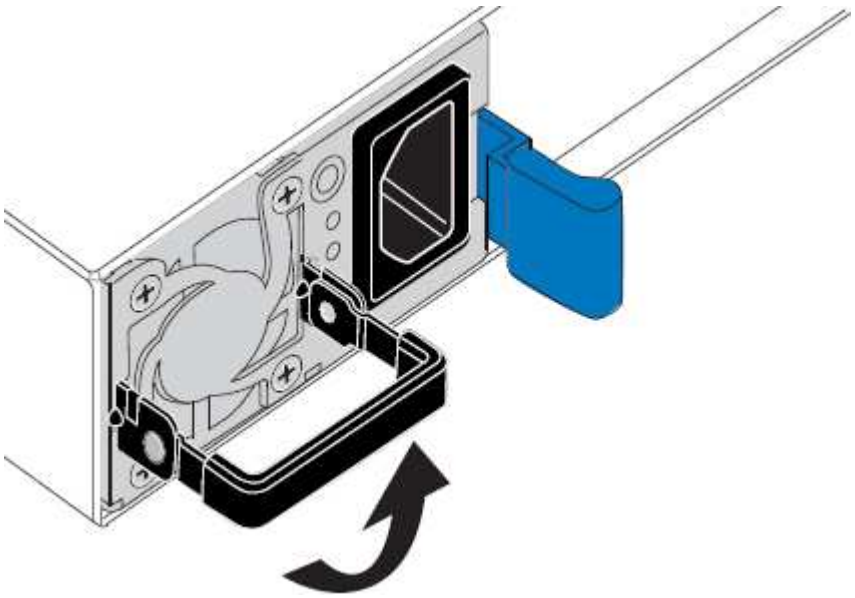
a. Shut down the appliance.

> If you have ever used an ILM rule that creates only one copy of an object and you are replacing both power supplies at the same time, you must replace the power supplies during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about why you should not use single-copy replication.

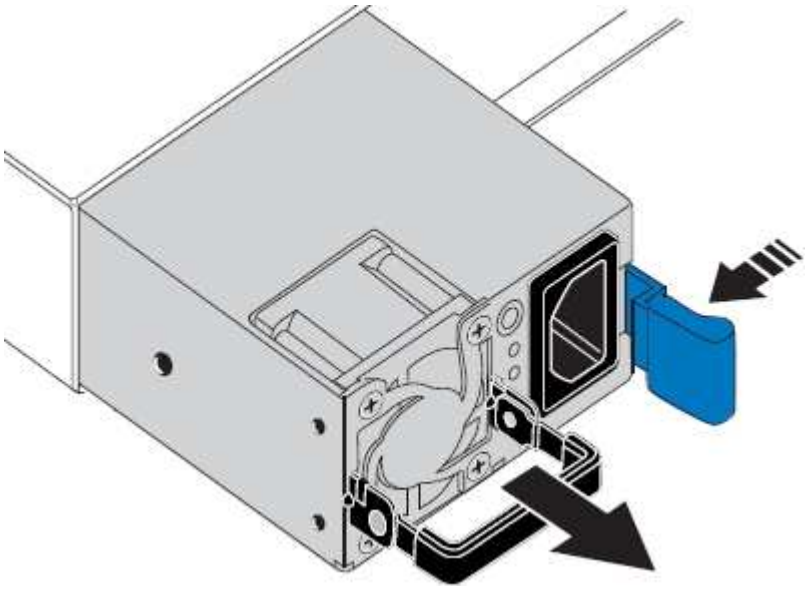
2. Unplug the power cord from each power supply to be replaced.

When viewed from the rear of the appliance, power supply A (PSU0) is on the right and power supply B (PSU1) is on the left.

3. Lift the handle on the first supply to be replaced.



4. Press the blue latch and pull the power supply out.

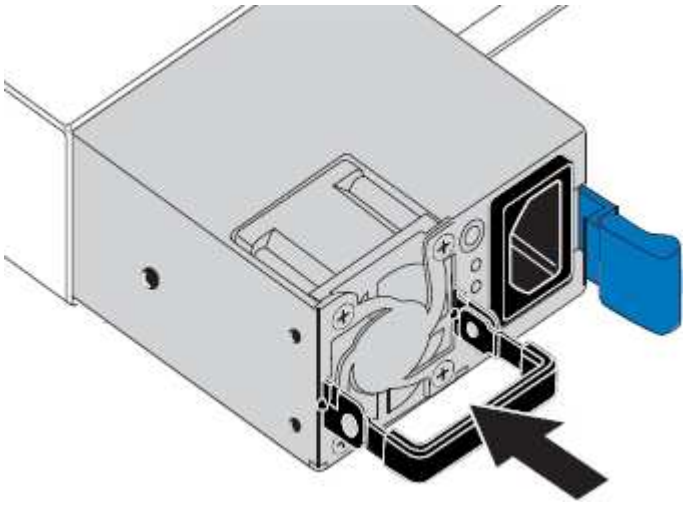


5. With the blue latch on the right, slide the replacement power supply into the chassis.

   Both installed power supplies must be the same model and wattage.

   Ensure that the blue latch is on the right side when you slide the replacement unit in.

   You will feel a click when the power supply is locked into place.



6. Push the handle back down against the body of the PSU.
7. If you are replacing both power supplies, repeat steps 2 though 6 to replace the second power supply.
8. Connect the power cords to the replaced units and apply power.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace fan in an SGF6112

The SGF6112 appliance has eight cooling fans. If one of the fans fails, you must replace it as soon as possible to ensure that the appliance has proper cooling.

Before you begin

- You have the correct replacement fan.
- You have determined the location of the fan to replace.
- You have physically located the SGF6112 appliance where you are replacing the fan in the data center.

  A controlled shutdown of the appliance is required before removing the appliance from the rack.

- You have disconnected all cables and removed the appliance cover.
- You have confirmed that the other fans are installed and running.

About this task

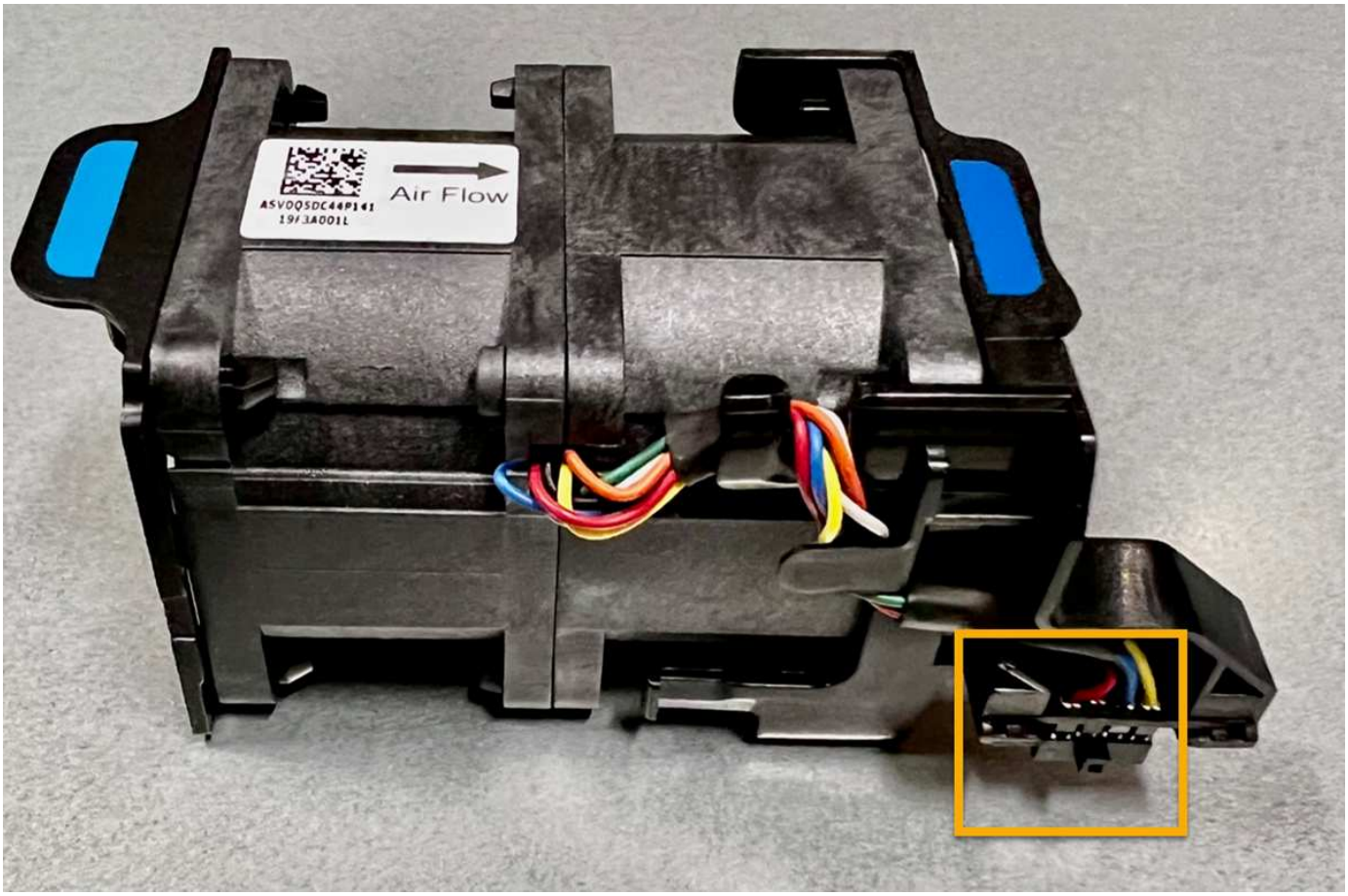
To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before starting the fan replacement or replace the fan during a scheduled maintenance window when periods of service disruption are acceptable. See the information about monitoring node connection states.

If you have ever used an ILM rule that creates only one copy of an object, you must replace the fan during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about why you should not use single-copy replication.

The appliance node will not be accessible while you replace the fan.

The photograph shows a fan for the appliance. The electrical connector is highlighted. The cooling fans are accessible after you take the top cover off of the appliance.

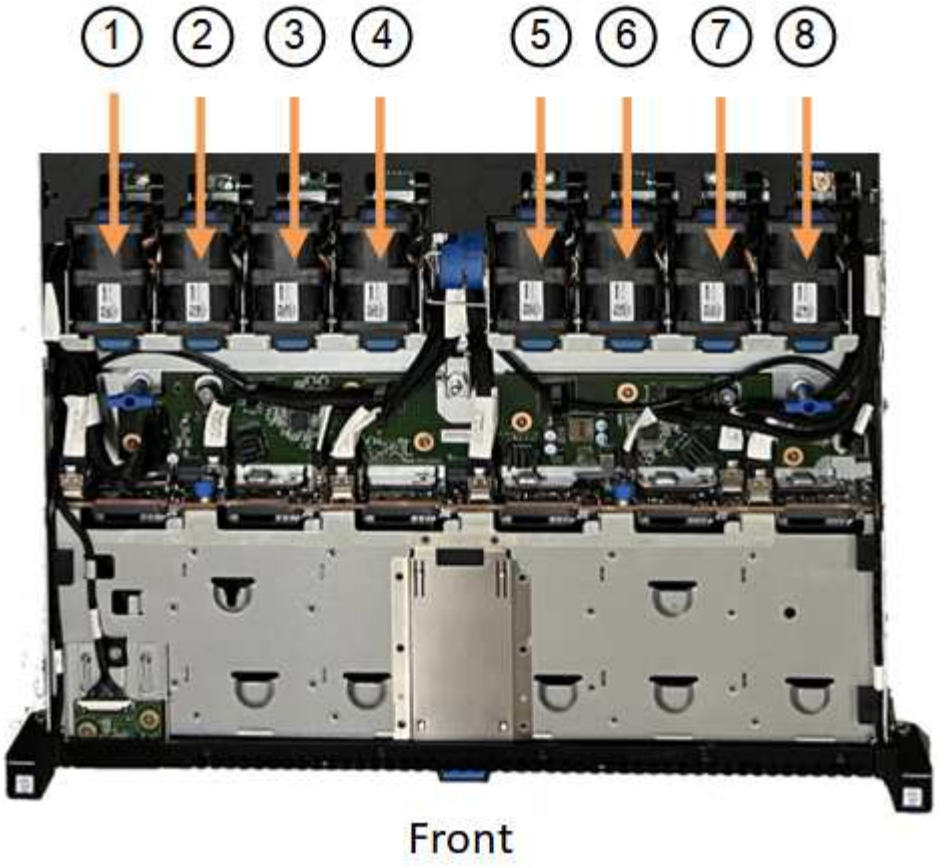
Each of the two power supply units also contain a fan. The power supply fans aren't included in this procedure.



Steps

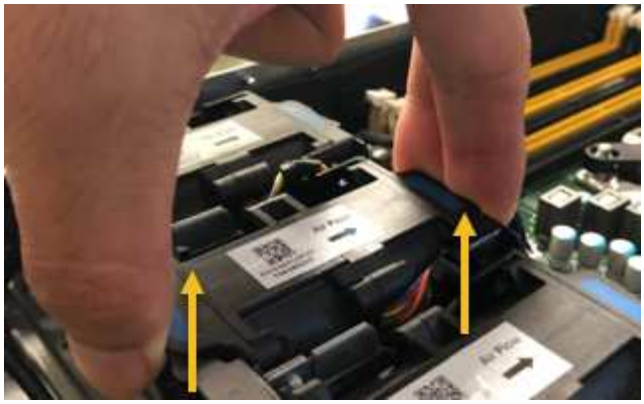
1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Locate the fan that you need to replace.

   The eight fans are in the following positions in the chassis (front half of SGF6112 with top cover removed shown):



	Fan unit
1	Fan_SYS0
2	Fan_SYS1
3	Fan_SYS2
4	Fan_SYS3
5	Fan_SYS4
6	Fan_SYS5
7	Fan_SYS6
8	Fan_SYS7

3. Using the blue tabs on the fan, lift the failed fan out of the chassis.



4. Slide the replacement fan into the open slot in the chassis.

   Be sure to align the connector on the fan with the socket in the circuit board.

5. Press the fan’s connector firmly into the circuit board (socket highlighted).

After you finish

1. Put the top cover back on the appliance, and press the latch down to secure the cover in place.
2. Power on the appliance and monitor the appliance LEDs and boot-up codes.

   Use the BMC interface to monitor boot-up status.

3. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace drives in the SGF6112

The SGF6112 storage appliance contains 12 SSD drives. Data on the drives is protected by a RAID scheme that enables the appliance to recover from any single drive failure without having to copy data from another node.

The failure of a second drive before an initial drive failure has been corrected might require data be copied from other nodes to restore redundancy. This restoration of redundancy can take longer, and might be impossible, if single-copy ILM rules are in use or were used in the past, or if data redundancy has been impacted by failures on other nodes. Therefore, if one of the SGF6112 drives fails, you must replace it as soon as possible to ensure redundancy.

Before you begin

- You have physically located the appliance.
- You have verified which drive has failed by noting that the drive's left LED is solid amber or using the Grid Manager to view the alert caused by the failed drive.

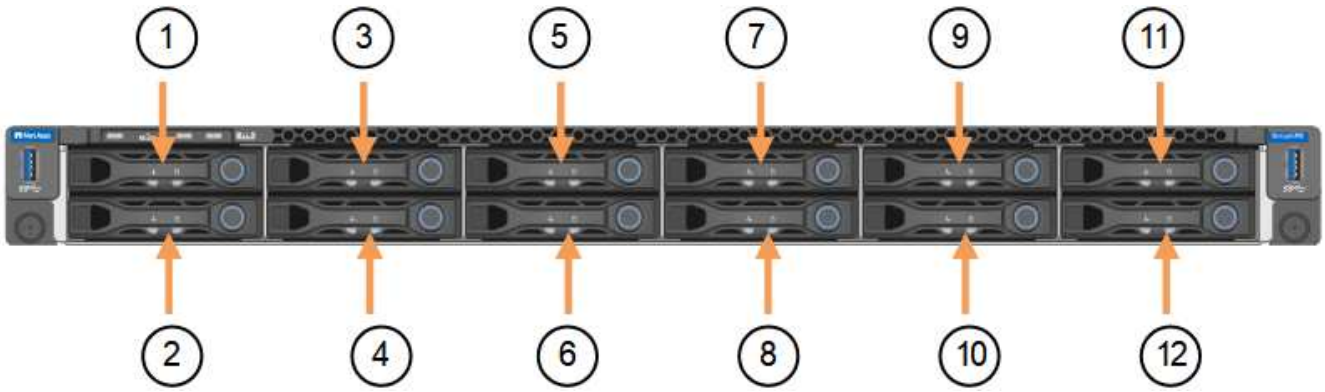
  See the information about viewing status indicators to verify the failure.

- You have obtained the replacement drive.
- You have obtained proper ESD protection.

Steps

1. Verify that the drive's left fault LED is amber or use the drive slot ID from the alert to locate the drive.

   The twelve drives are in the following positions in the chassis (front of chassis with bezel removed shown):



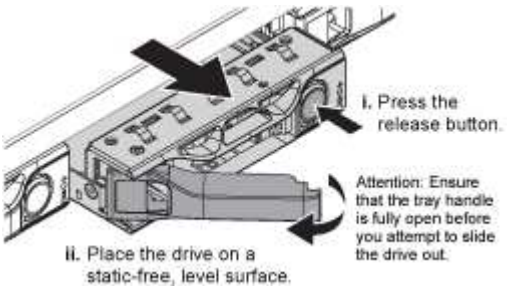
Position	Drive
1	HDD00
2	HDD01
3	HDD02
4	HDD03
5	HDD04
6	HDD05
7	HDD06
8	HDD07
9	HDD08
10	HDD09
11	HDD10
12	HDD11

You can also use the Grid Manager to monitor the status of the SSD drives. Select **NODES**. Then select `Storage Node` > **Hardware**. If a drive has failed, the Storage RAID Mode field contains a message about which drive has failed.

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. Unpack the replacement drive, and set it on a static-free, level surface near the appliance.

   Save all packing materials.

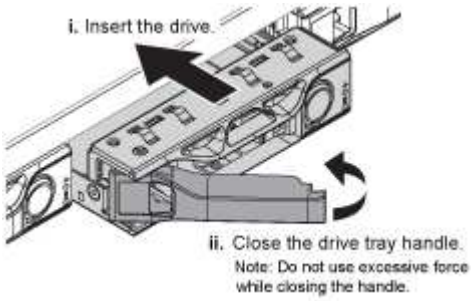
4. Press the release button on the failed drive.



   The handle on the drive springs open partially, and the drive releases from the slot.

5. Open the handle, slide the drive out, and place it on a static-free, level surface.
6. Press the release button on the replacement drive before you insert it into the drive slot.

   The latch springs open.



7. Insert the replacement drive in the slot, and then close the drive handle.

   Don't use excessive force while closing the handle.

   When the drive is fully inserted, you hear a click.

   The replaced drive is automatically rebuilt with mirrored data from the working drives. The drive LED should blink initially, but then stop blinking as soon as the system determines that the drive has enough capacity and is functional.

   You can check the status of the rebuild by using the Grid Manager.

8. If more than one drive failed and has been replaced, you might have alerts indicating that some volumes need to have data restored to them. If you receive an alert, before attempting volume recovery, select **NODES** > **`appliance Storage Node`** > **Hardware**. In the StorageGRID Appliance section of the page, verify that the Storage RAID mode is healthy or rebuilding. If the status lists one or more failed drives, correct this condition before attempting volume restoration.
9. In the Grid Manager, go to **NODES** > **`appliance Storage Node`** > **Hardware**. In the StorageGRID Appliance section of the page, verify that the Storage RAID mode is healthy.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace NIC in the SGF6112

You might need to replace a Network Interface Card (NIC) in the SGF6112 if it is not functioning optimally or if it has failed.

Use these procedures to:

- Remove the NIC
- Reinstall the NIC

Remove the NIC

Before you begin

- You have the correct replacement NIC.

- You have determined the location of the NIC to replace.
- You have physically located the SGF6112 appliance where you are replacing the NIC in the data center.

> A controlled shutdown of the appliance is required before removing the appliance from the rack.

- You have disconnected all cables and removed the appliance cover.

About this task

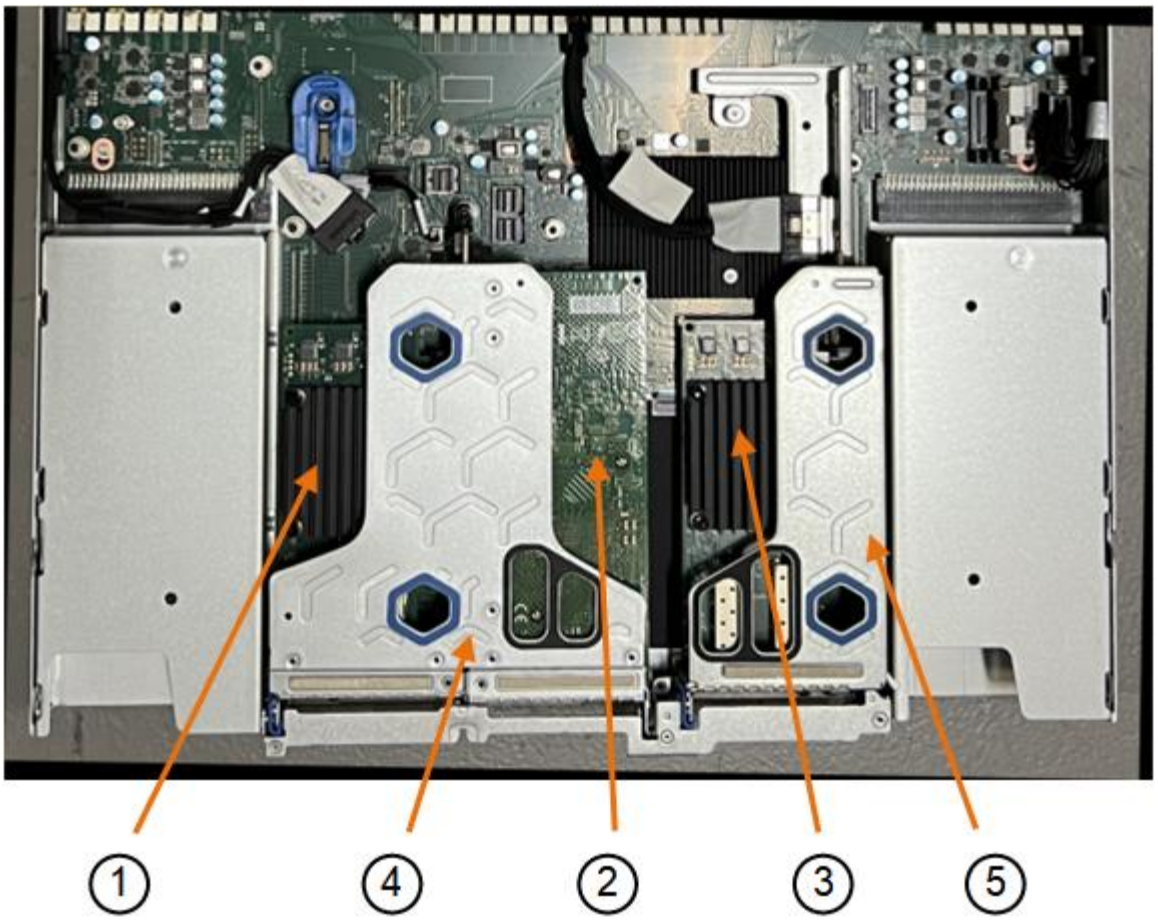
To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before starting the Network Interface Card (NIC) replacement or replace the NIC during a scheduled maintenance window when periods of service disruption are acceptable. See the information about monitoring node connection states.

> If you have ever used an ILM rule that creates only one copy of an object, you must replace the NIC during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about why you should not use single-copy replication.

Steps

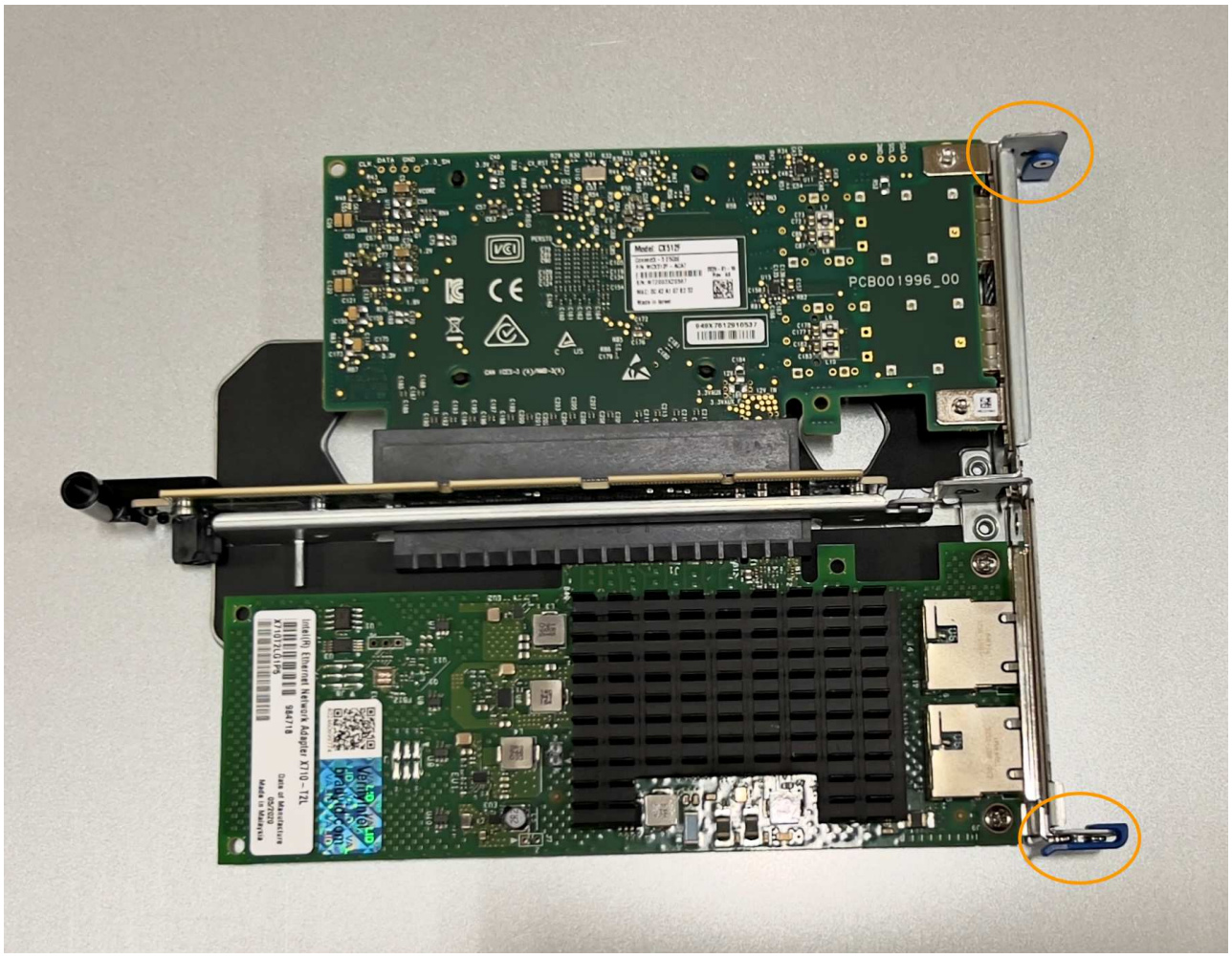
1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Locate the riser assembly that contains the NIC at the rear of the appliance.

   The three NICs in the appliance are in two riser assemblies in the positions in the chassis shown in the photograph (Rear of appliance with top cover removed shown):

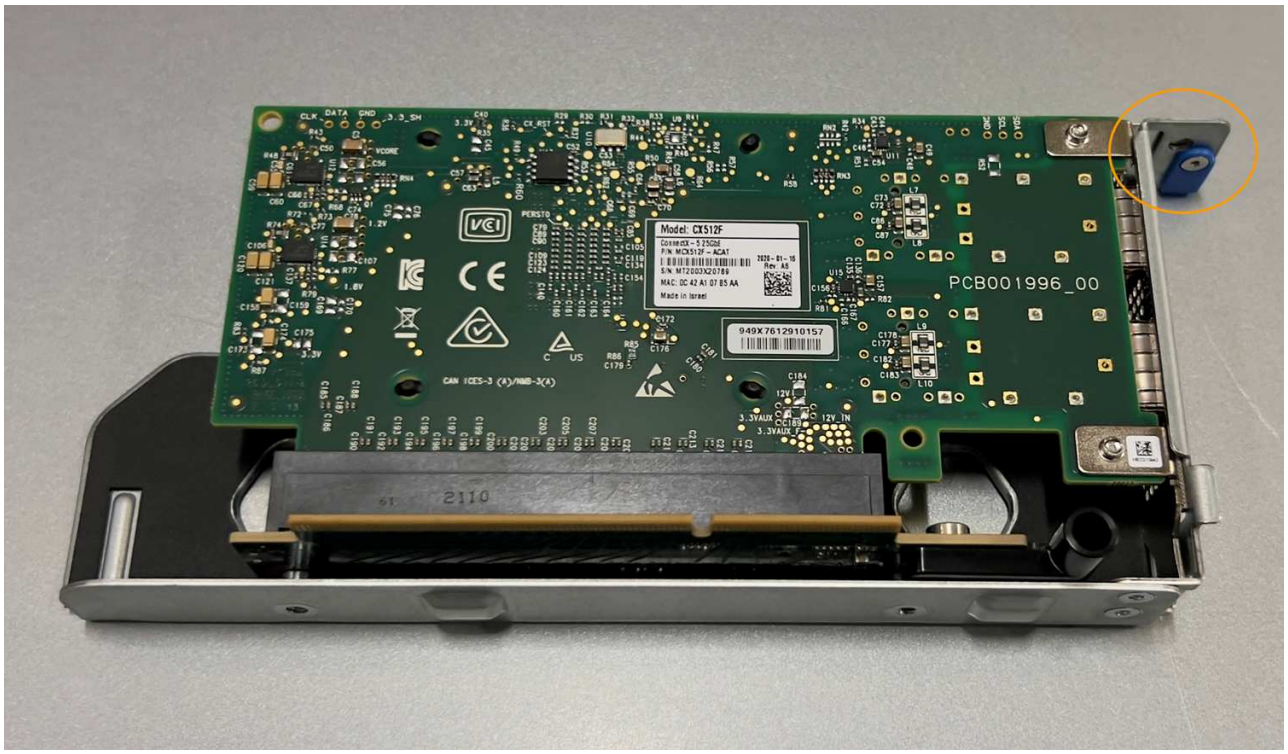


	Device or Part name	Description
1	hic1/hic2	10/25-GbE Ethernet network ports in the two-port riser assembly
2	mtc1/mtc2	1/10GBase-T management ports in the two-port riser assembly
3	hic3/hic4	10/25-GbE Ethernet network ports in the one-port riser assembly
4	Two-slot riser assembly	Support for one of the 10/25-GbE NICs and the 1/10GBase-T NIC
5	One-slot riser assembly	Support for one of the 10/25-GbE NICs

3. Grasp the riser assembly with the failed NIC 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 NICs to clear the chassis.
4. Place the riser on a flat anti-static surface with the metal frame side down to access the NICs.
    - **Two-slot riser assembly with two NICs**



- **One-slot riser assembly with one NIC**



5. Open the blue latch (circled) on the NIC to be replaced and carefully remove the NIC from the riser assembly. Rock the NIC slightly to help remove the NIC from its connector. Don't use excessive force.
6. Place the NIC on a flat anti-static surface.

Reinstall the NIC

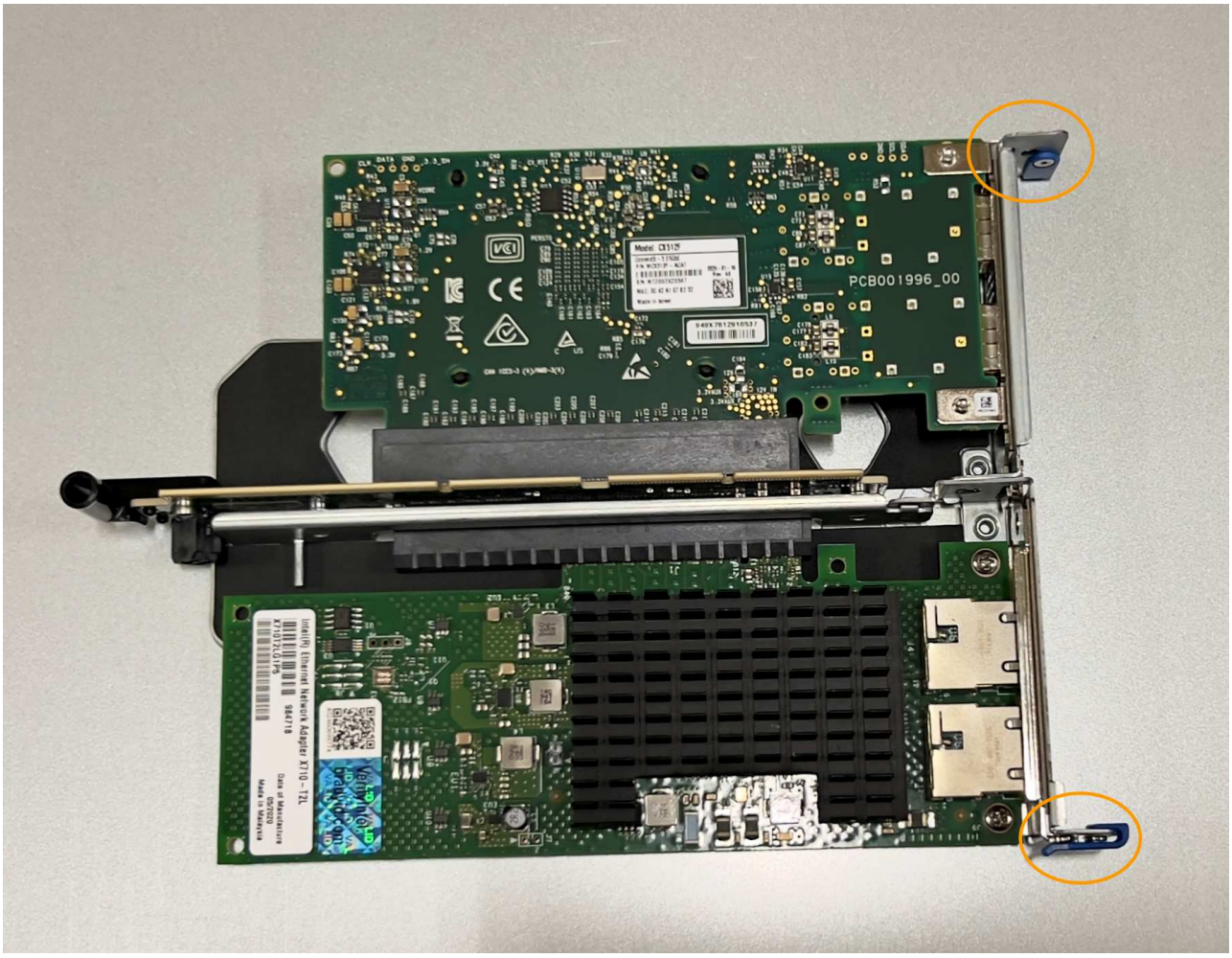
Install the replacement NIC into the same location as the one that was removed.

Before you begin

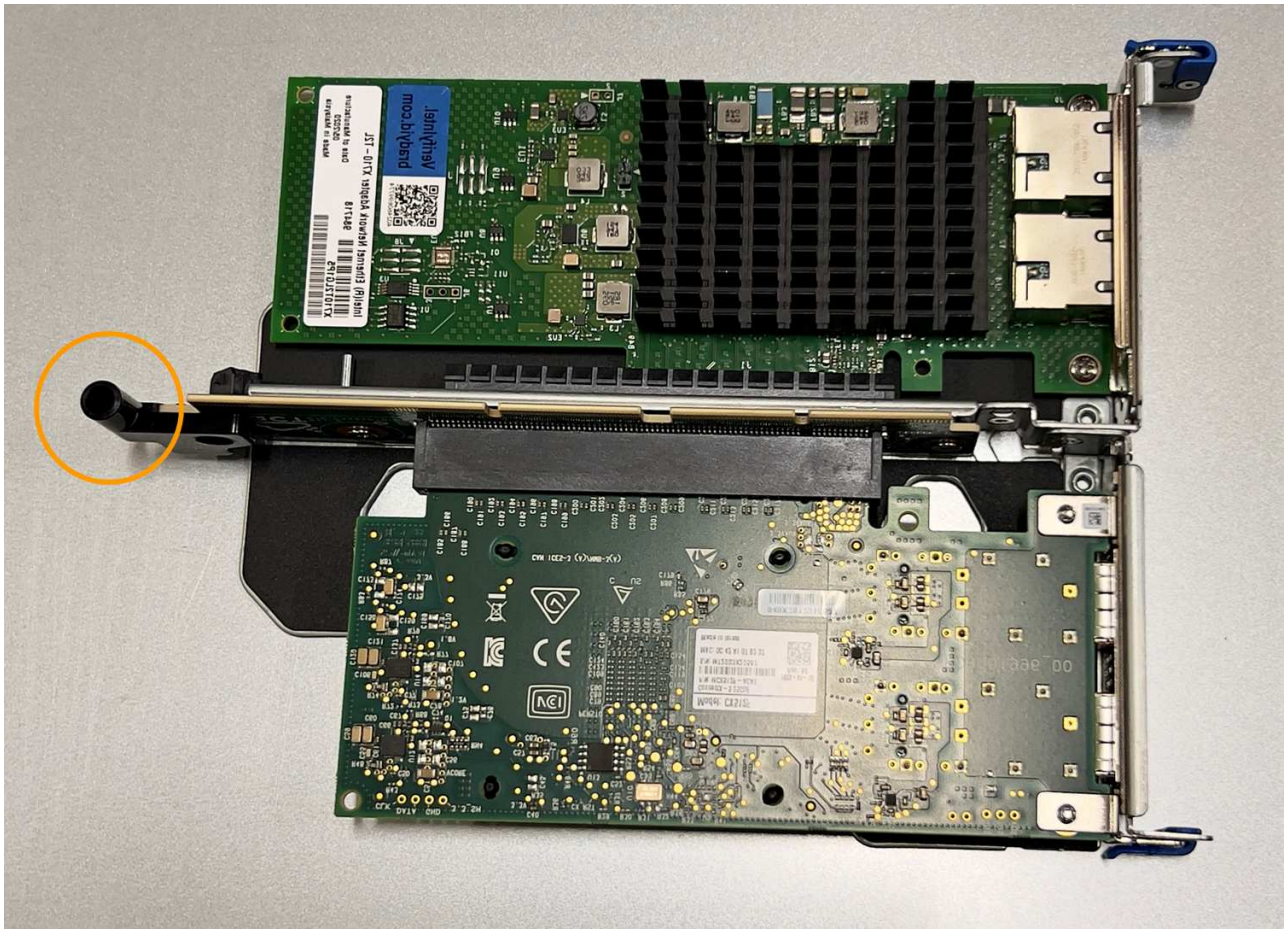
- You have the correct replacement NIC.
- You have removed the existing failed NIC.

Steps

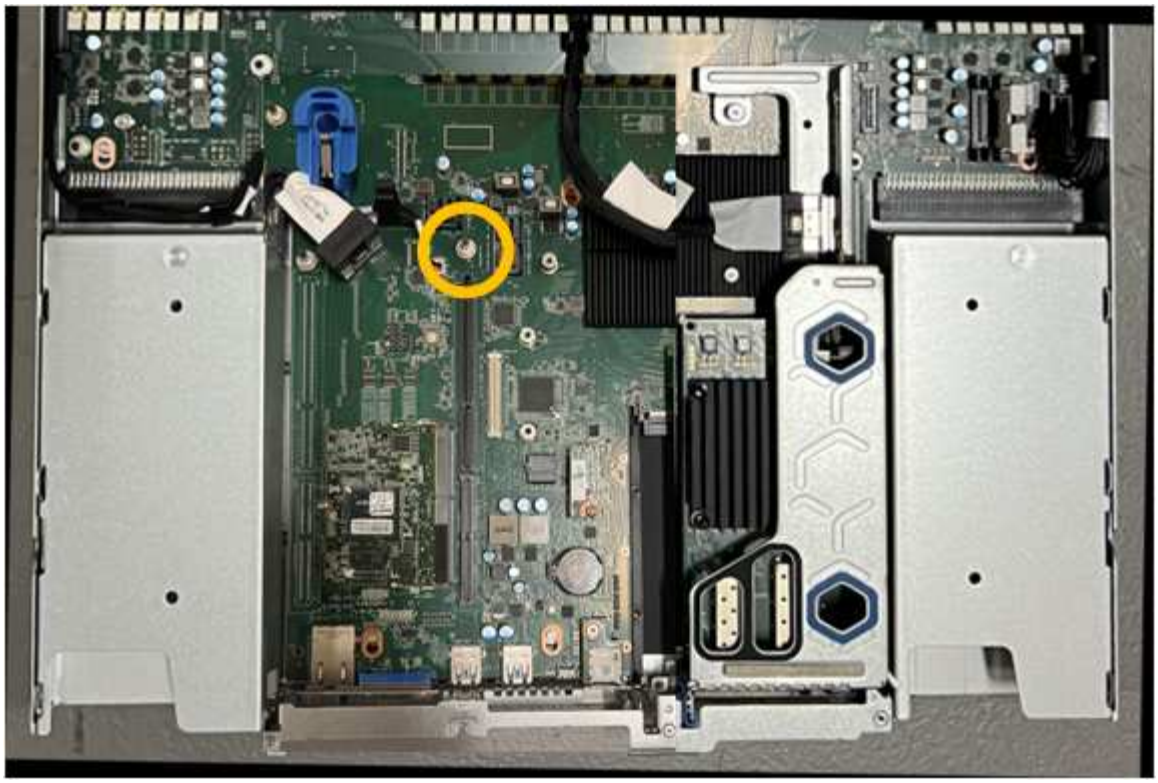
1. Wrap the strap end of the ESD wristband around your wrist, and secure the clip end to a metal ground to prevent static discharge.
2. Remove the replacement NIC from its packaging.
3. If you are replacing one of the NICs in the two-slot riser assembly, do the following:
   a. Ensure the blue latch is in the open position.
   b. Align the NIC with its connector on the riser assembly. Carefully press the NIC into the connector until it is fully seated, as shown in the photograph, and then close the blue latch.



c. Locate the alignment hole on the two-slot riser assembly (circled) that aligns with a guide pin on the system board to ensure correct riser assembly positioning.



d. Locate the guide pin on the system board



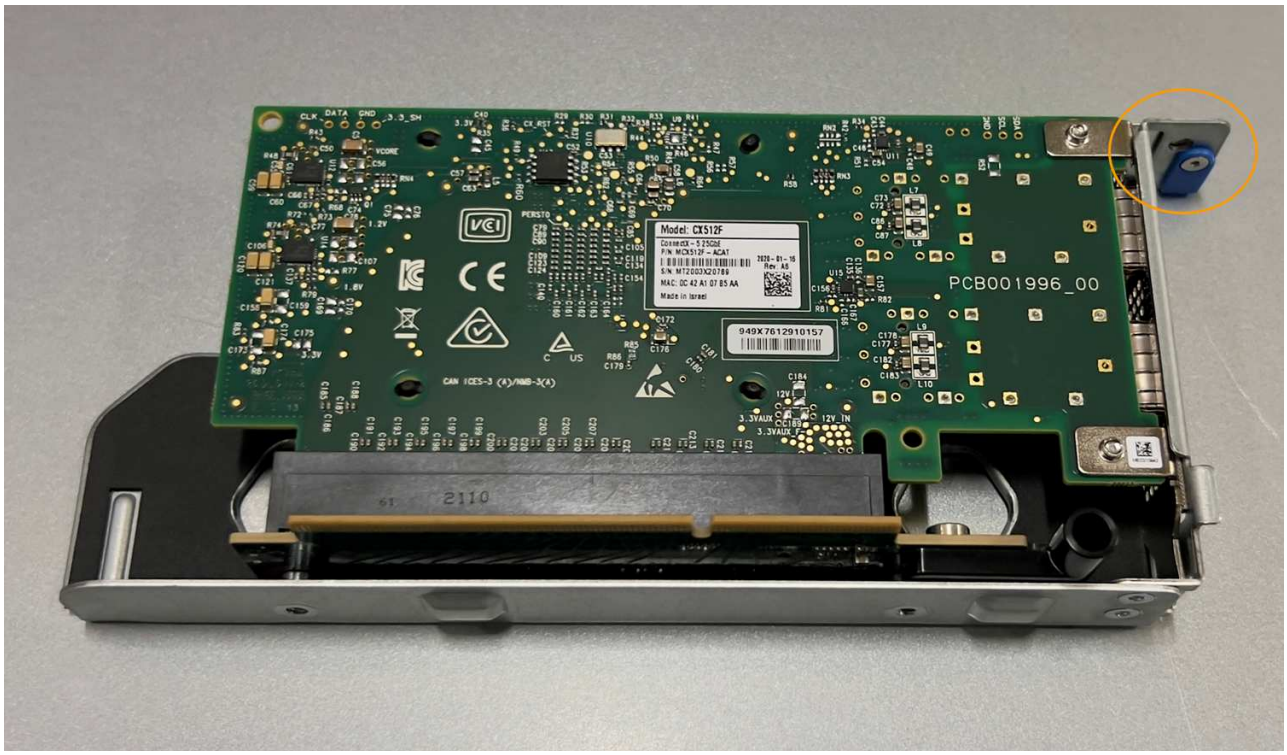
e. Position the riser assembly in the chassis, making sure that it aligns with the connector on the system board and guide pin.

f. Carefully press the two-slot riser assembly in place along its center line, next to the blue-marked holes, until it is fully seated.

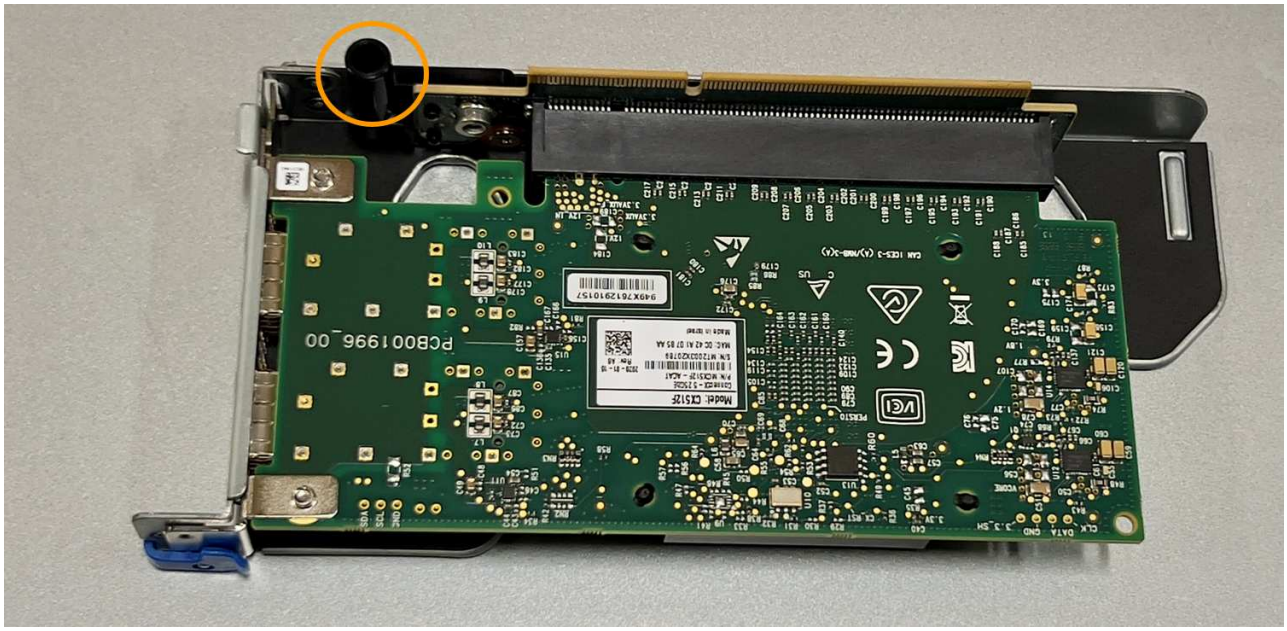
4. If you are replacing the NIC in the one-slot riser assembly, do the following:

a. Ensure the blue latch is in the open position.

b. Align the NIC with its connector on the riser assembly. Carefully press the NIC into the connector until it is fully seated as shown in the photograph and close the blue latch.



c. Locate the alignment hole on the one-slot riser assembly (circled) that aligns with a guide pin on the system board to ensure correct riser assembly positioning.



d. Locate the guide pin on the system board

e. Position the one-slot riser assembly in the chassis, making sure that it aligns with the connector on the system board and guide pin.

f. Carefully press the one-slot riser assembly in place along its center line, next to the blue-marked holes, until it is fully seated.

5. Remove the protective caps from the NIC ports where you will be reinstalling cables.

After you finish

If you have no other maintenance procedures to perform in the appliance, reinstall the appliance cover, return the appliance to the rack, attach cables, and apply power.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Replace SGF6112 CMOS battery

Use this procedure to replace the CMOS coin cell battery on the system board.

Use these procedures to:

- Remove the CMOS battery
- Reinstall the CMOS battery

Remove the CMOS battery

Before you begin

- You have verified the appliance where the CMOS battery needs to be replaced.
- You have physically located the SGF6112 appliance where you are replacing the CMOS battery in the data center.

> A controlled shutdown of the appliance is required before removing the appliance from the rack.

- You have disconnected all cables and removed the appliance cover.

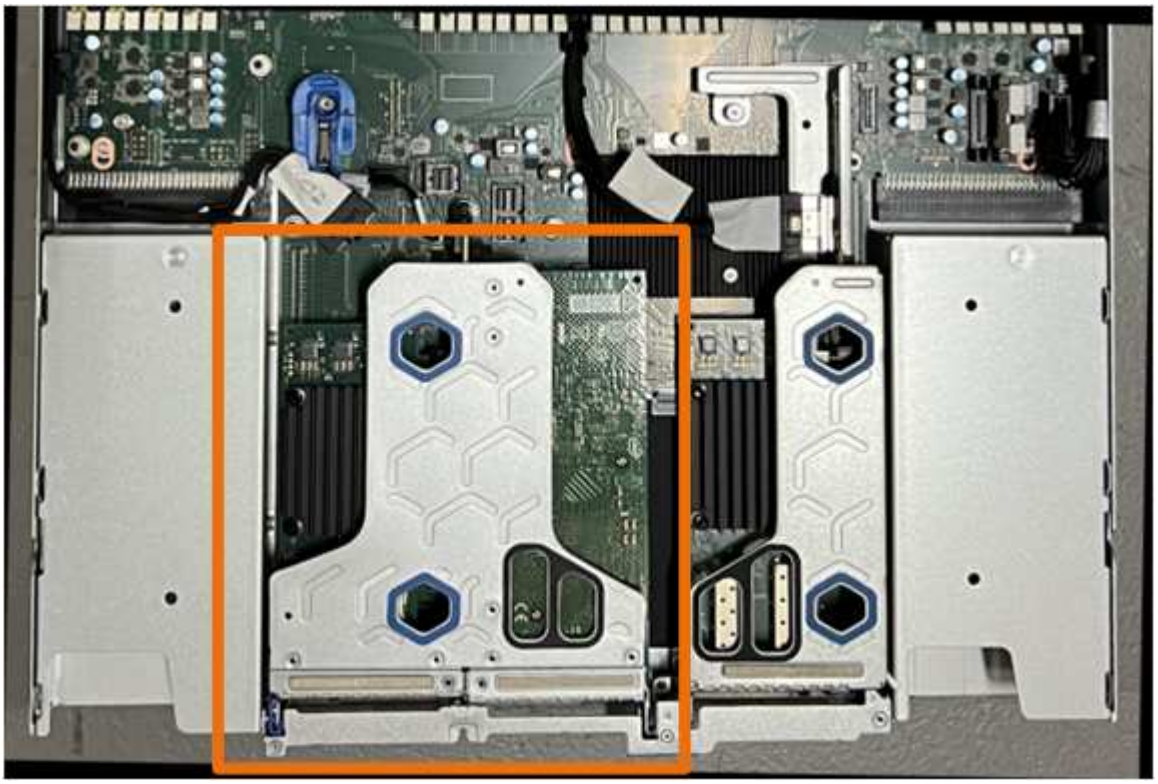
About this task

To prevent service interruptions, confirm that all other Storage Nodes are connected to the grid before starting the CMOS battery replacement or replace the battery during a scheduled maintenance window when periods of service disruption are acceptable. See the information about monitoring node connection states.

> If you have ever used an ILM rule that creates only one copy of an object, you must replace the battery during a scheduled maintenance window. Otherwise, you might temporarily lose access to those objects during this procedure. See information about why you should not use single-copy replication.

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 two-slot riser assembly at the rear of the appliance.



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 NICs to clear the chassis.
4. Place the riser on a flat anti-static surface with the metal frame side down.
5. Locate the CMOS battery on the system board in the position beneath the removed riser assembly.

6. Use your finger or a plastic pry tool to press the retaining clip (highlighted) away from the battery to spring it from the socket.

7. Remove the battery and dispose of it properly.

Reinstall the CMOS battery

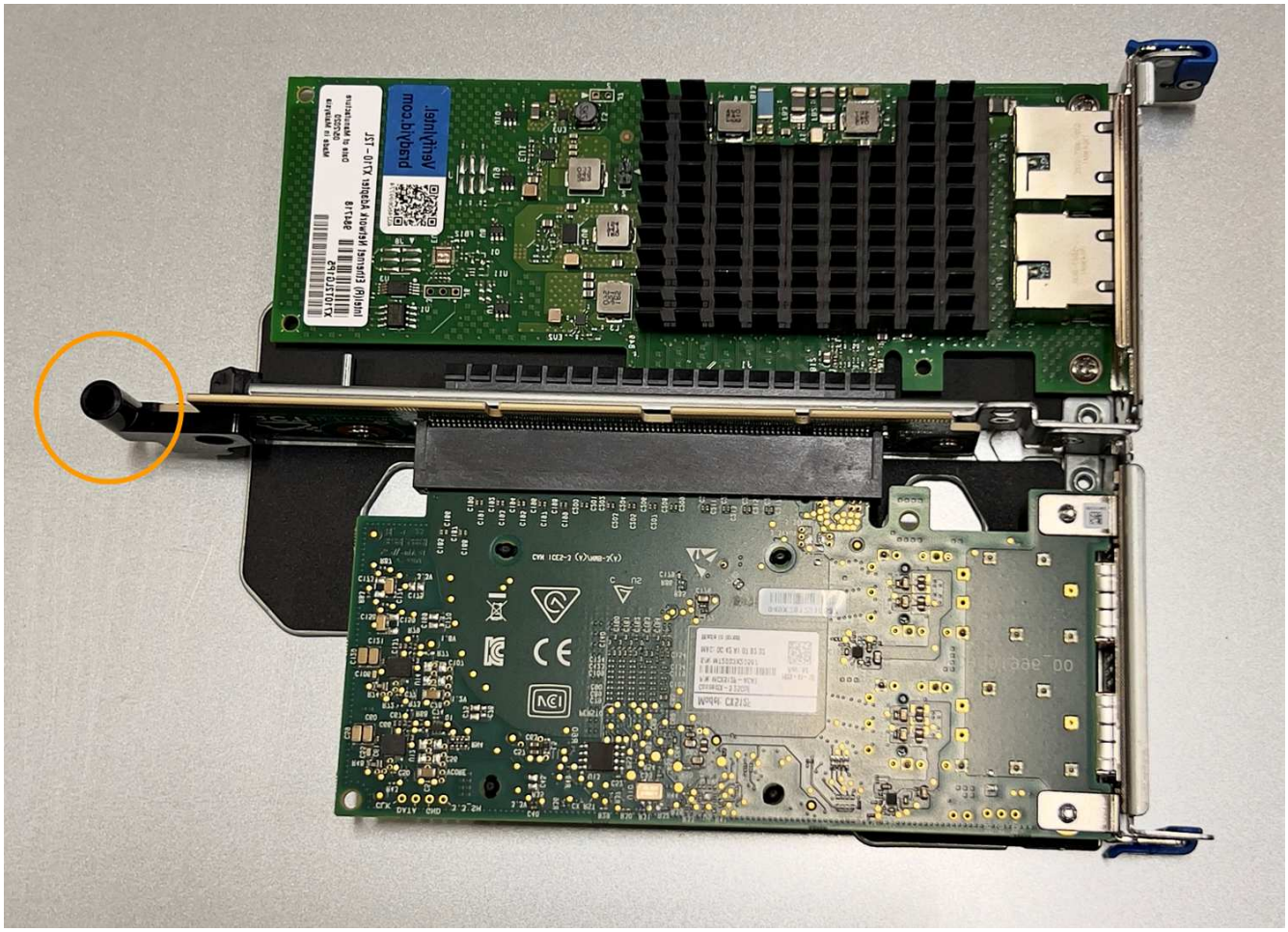
Install the replacement CMOS battery into the socket on the system board.

Before you begin

- You have the correct replacement CMOS battery (CR2032).
- You have removed the failed CMOS battery.

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 CMOS battery from its packaging.
3. Press the replacement battery into the empty socket on the system board with the positive (+) side up until the battery snaps in place.
4. Locate the alignment hole on the two-slot riser assembly (circled) that aligns with the guide pin on the system board to ensure correct riser assembly positioning.



5. Locate the guide pin on the system board.

6. Position the riser assembly in the chassis, making sure that it aligns with the connector on the system board and guide pin.
7. Carefully press the two-slot riser assembly in place along its center line, next to the blue-marked holes, until it is fully seated.
8. If you have no other maintenance procedures to perform in the appliance, reinstall the appliance cover, return the appliance to the rack, attach cables, and apply power.
9. If the appliance you replaced had drive encryption enabled for the SED drives, you must enter the drive encryption passphrase to access the encrypted drives when the replacement appliance starts for the first time.
10. If the appliance you replaced used a key management server (KMS) to manage encryption keys for node encryption, additional configuration might be required before the node can join the grid. If the node does not automatically join the grid, make sure that these configuration settings have transferred to the new appliance and manually configure any settings that don't have the expected configuration:
    - Configure StorageGRID connections
    - Configure node encryption for the appliance
11. Log in to the appliance:
    a. Enter the following command: `ssh admin@grid_node_IP`
    b. Enter the password listed in the `Passwords.txt` file.
    c. Enter the following command to switch to root: `su -`
    d. Enter the password listed in the `Passwords.txt` file.
12. Restore BMC network connectivity for the appliance using one of these options:
    - Use static IP, netmask, and gateway
    - Use DHCP to obtain an IP, netmask, and gateway

a. To restore the BMC configuration to use a static IP, netmask, and gateway, enter the following commands:

```
run-host-command ipmitool lan set 1 ipsrc static

run-host-command ipmitool lan set 1 ipaddr Appliance_IP

run-host-command ipmitool lan set 1 netmask Netmask_IP

run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

b. To restore the BMC configuration to use DHCP to obtain an IP, netmask, and gateway, enter the following command:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

13. After restoring BMC network connectivity, connect to the BMC interface to audit and restore any additional custom BMC configuration you might have applied. For example, you should confirm the settings for SNMP trap destinations and email notifications. See Configure BMC interface.
14. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

Replace SGF6112 cover

Remove the appliance cover to access internal components for maintenance, and replace the cover when you are finished.

Remove cover

Before you begin

Remove the appliance from the cabinet or rack to access the top cover.

Steps

1. Make sure that the appliance 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 appliance 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 appliance.

Reinstall cover

Before you begin

You have completed all maintenance procedures inside the appliance.

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 appliance 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 appliance in the cabinet or rack.

Replace SGF6112 appliance

You might need to replace the appliance if it is not functioning optimally or if it has failed.

Before you begin

- You have a replacement appliance with the same part number as the appliance you are replacing.
- You have labels to identify each cable that is connected to the appliance.
- You have physically located the appliance.

About this task

The StorageGRID node will not be accessible while you replace the appliance. If the appliance is functioning sufficiently, you can perform a controlled shutdown at the start of this procedure.

> If you are replacing the appliance 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 can't access it from hosts on other subnets. This condition should resolve itself within 15 minutes (when any ARP cache entries for the original appliance 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. Display the current configurations of the appliance and record them.
   a. Log in to the appliance to be replaced:
      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: **`run-host-command ipmitool lan print`** to display the current BMC configurations for the appliance.
2. Shut down the appliance.
3. If any of the network interfaces on this StorageGRID appliance are configured for DHCP, you need to update the permanent DHCP lease assignments on the DHCP servers to reference the MAC addresses of the replacement appliance. This ensures that the appliance is assigned the expected IP addresses.

   Contact your network or DHCP-server administrator to update the permanent DHCP lease assignments. The administrator can determine the MAC addresses of the replacement appliance from the DHCP server logs or by inspecting the MAC address tables in the switches to which the appliance Ethernet ports are connected.

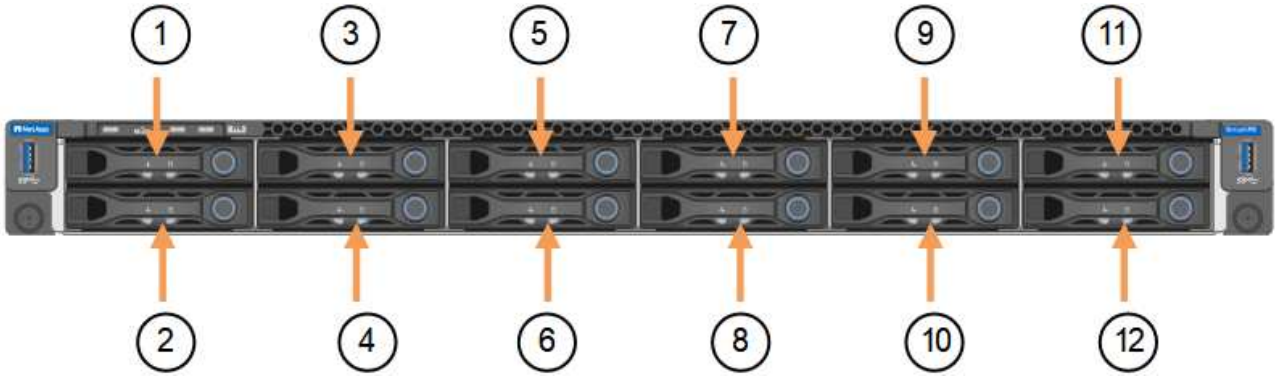
4. Remove and replace the appliance:
   a. Label the cables and then disconnect the cables and any network transceivers.

To prevent degraded performance, don't twist, fold, pinch, or step on the cables.

b. Remove the failed appliance from the cabinet or rack.

c. Note the position of the replaceable components (two power supplies, three NICs, and twelve SSDs) in the failed appliance.

The twelve drives are in the following positions in the chassis (front of chassis with bezel removed shown):



	Drive
1	HDD00
2	HDD01
3	HDD02
4	HDD03
5	HDD04
6	HDD05
7	HDD06
8	HDD07
9	HDD08
10	HDD09
11	HDD10
12	HDD11

d. Transfer the replaceable components to the replacement appliance.

Follow the maintenance instructions provided for reinstalling the replaceable components.

> If you wish to retain the data on the drives, be sure to insert the SSD drives into the same drive slots they occupied in the failed appliance. If you don't, the Appliance Installer will display a warning message and you will have to put the drives into the correct slots and reboot the appliance before the appliance can rejoin the grid.

e. Install the replacement appliance into the cabinet or rack.

f. Replace the cables and any optical transceivers.

5. Power on the appliance.
6. If the appliance you replaced had hardware drive encryption enabled for the SED drives, you must enter the drive encryption passphrase to access the encrypted drives when the replacement appliance starts for the first time.
7. Wait for the appliance to rejoin the grid. If the appliance does not rejoin the grid, follow the guidance on the StorageGRID Appliance Installer home page to address any issues.

> To prevent data loss if the Appliance Installer indicates that physical hardware changes are required, such as moving disk drives to different slots, power down the appliance before making hardware changes.

8. If the appliance you replaced used a key management server (KMS) to manage encryption keys for node encryption, additional configuration might be required before the node can join the grid. If the node does not automatically join the grid, make sure that these configuration settings have transferred to the new appliance and manually configure any settings that don't have the expected configuration:
   - Configure StorageGRID connections
   - Configure node encryption for the appliance
9. Log in to the replaced appliance:
   a. Enter the following command: `ssh admin@grid_node_IP`
   b. Enter the password listed in the `Passwords.txt` file.
   c. Enter the following command to switch to root: `su -`
   d. Enter the password listed in the `Passwords.txt` file.
10. Restore BMC network connectivity for the replaced appliance. There are two options:
    - Use static IP, netmask, and gateway
    - Use DHCP to obtain an IP, netmask, and gateway
      a. To restore the BMC configuration to use a static IP, netmask, and gateway, enter the following commands:

```
run-host-command ipmitool lan set 1 ipsrc static

run-host-command ipmitool lan set 1 ipaddr Appliance_IP

run-host-command ipmitool lan set 1 netmask Netmask_IP

run-host-command ipmitool lan set 1 defgw ipaddr Default_gateway
```

b. To restore the BMC configuration to use DHCP to obtain an IP, netmask, and gateway, enter the following command:

```
run-host-command ipmitool lan set 1 ipsrc dhcp
```

11. After restoring BMC network connectivity, connect to the BMC interface to audit and restore any additional custom BMC configuration you might have applied. For example, you should confirm the settings for SNMP trap destinations and email notifications. See Configure BMC interface.
12. Confirm that the appliance node appears in the Grid Manager and that no alerts appear.

After you finish

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Related information

View status indicators

View boot-up codes for appliance

Relocate SGF6112 in cabinet or rack

Remove the SGF6112 from a cabinet or rack to access the top cover or to move the appliance to a different location, then reinstall the appliance into a cabinet or rack when hardware maintenance is complete.

Remove SGF6112 from cabinet or rack

Before you begin

- You have labels to identify each cable that is connected to the SGF6112.
- You have physically located the SGF6112 where you are performing maintenance in the data center.
- You have shut down the SGF6112.

> Don’t shut down the appliance using the power switch.

Steps

1. Label and then disconnect the appliance 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 appliance data cables and any SFP+ or SFP28 transceivers.

> To prevent degraded performance, don’t twist, fold, pinch, or step on the cables.

4. Loosen the two captive screws on the appliance front panel.

5. Slide the SGF6112 forward out of the rack until the mounting rails are fully extended and you hear the latches on both sides click.

   The appliance top cover is accessible.

6. Optional: If you are fully removing the appliance from the cabinet or rack, follow the instructions for the rail kit to remove the appliance from the rails.

After replacing the part, return the failed part to NetApp, as described in the RMA instructions shipped with the kit. See the Part Return & Replacements page for further information.

Reinstall SGF6112 into cabinet or rack

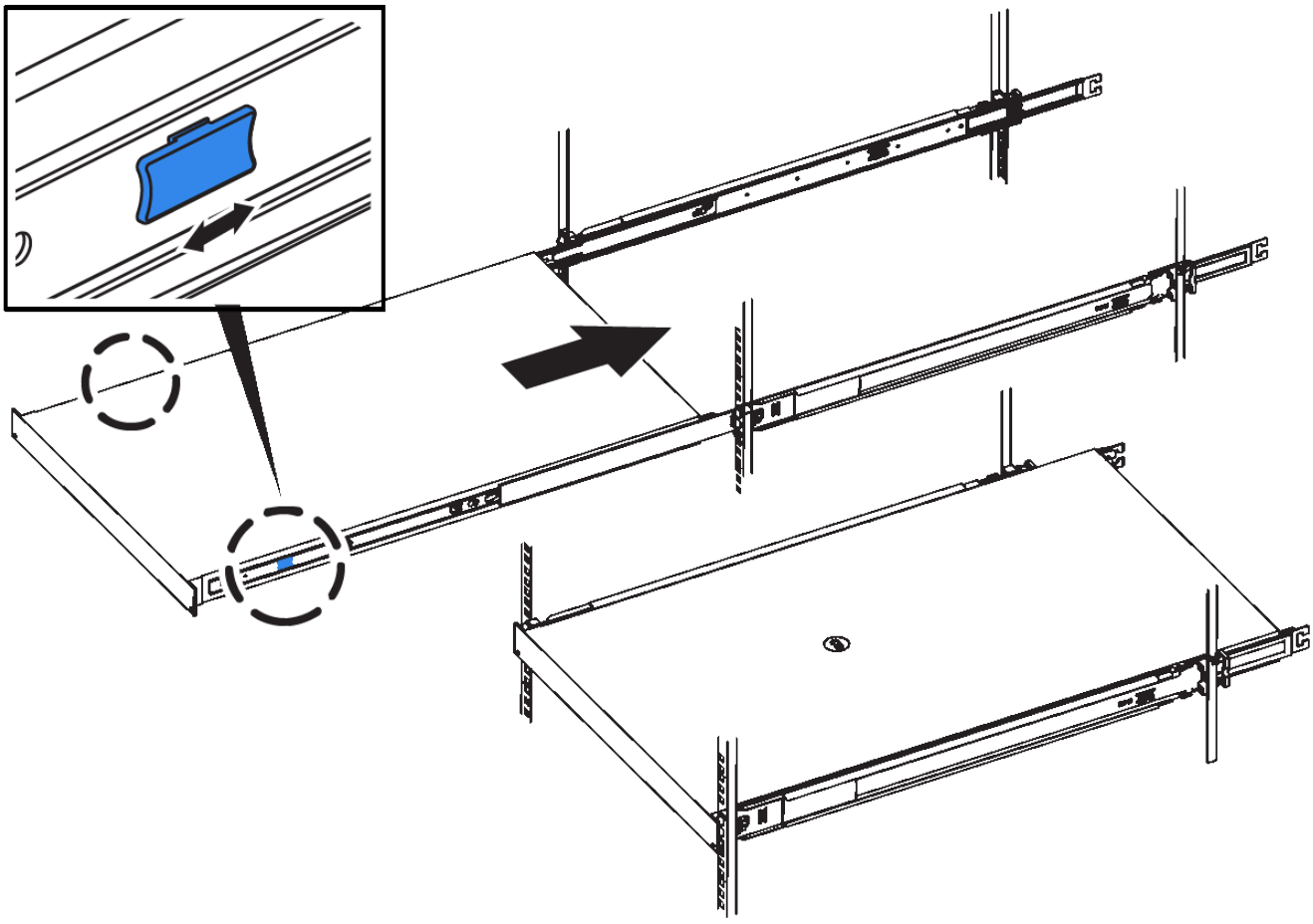
Before you begin

You have reinstalled the appliance cover.

Steps

1. Press the blue rail releases both rack rails at the same time and slide the SGF6112 into the rack until it is fully seated.

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



Don't 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, don't twist, fold, pinch, or step on the cables.

5. Reconnect the controller power cables.

After you finish

Restart the appliance.