Managing Admin Nodes

StorageGRID 11.5

NetApp
August 30, 2024

Table of Contents

Managing Admin Nodes

Each site in a StorageGRID deployment can have one or more Admin Nodes.

What an Admin Node is

Admin Nodes provide management services such as system configuration, monitoring, and logging. Each grid must have one primary Admin Node and might have any number of non-primary Admin Nodes for redundancy.

When you sign in to the Grid Manager or the Tenant Manager, you are connecting to an Admin Node. You can connect to any Admin Node, and each Admin Node displays a similar view of the StorageGRID system. However, maintenance procedures must be performed using the primary Admin Node.

Admin Nodes can also be used to load balance S3 and Swift client traffic.

Admin Nodes host the following services:

- AMS service
- CMN service
- NMS service
- Prometheus service
- Load Balancer and High Availability services (to support S3 and Swift client traffic)

Admin Nodes also support the Management Application Program Interface (mgmt-api) to process requests from the Grid Management API and the Tenant Management API.

What the AMS service is

The Audit Management System (AMS) service tracks system activity and events.

What the CMN service is

The Configuration Management Node (CMN) service manages system-wide configurations of connectivity and protocol features needed by all services. In addition, the CMN service is used to run and monitor grid tasks. There is only one CMN service per StorageGRID deployment. The Admin Node that hosts the CMN service is known as the primary Admin Node.

What the NMS service is

The Network Management System (NMS) service powers the monitoring, reporting, and configuration options that are displayed through the Grid Manager, the StorageGRID system's browser-based interface.

What the Prometheus service is

The Prometheus service collects time series metrics from the services on all nodes.

Related information

Using the Grid Management API

Use a tenant account

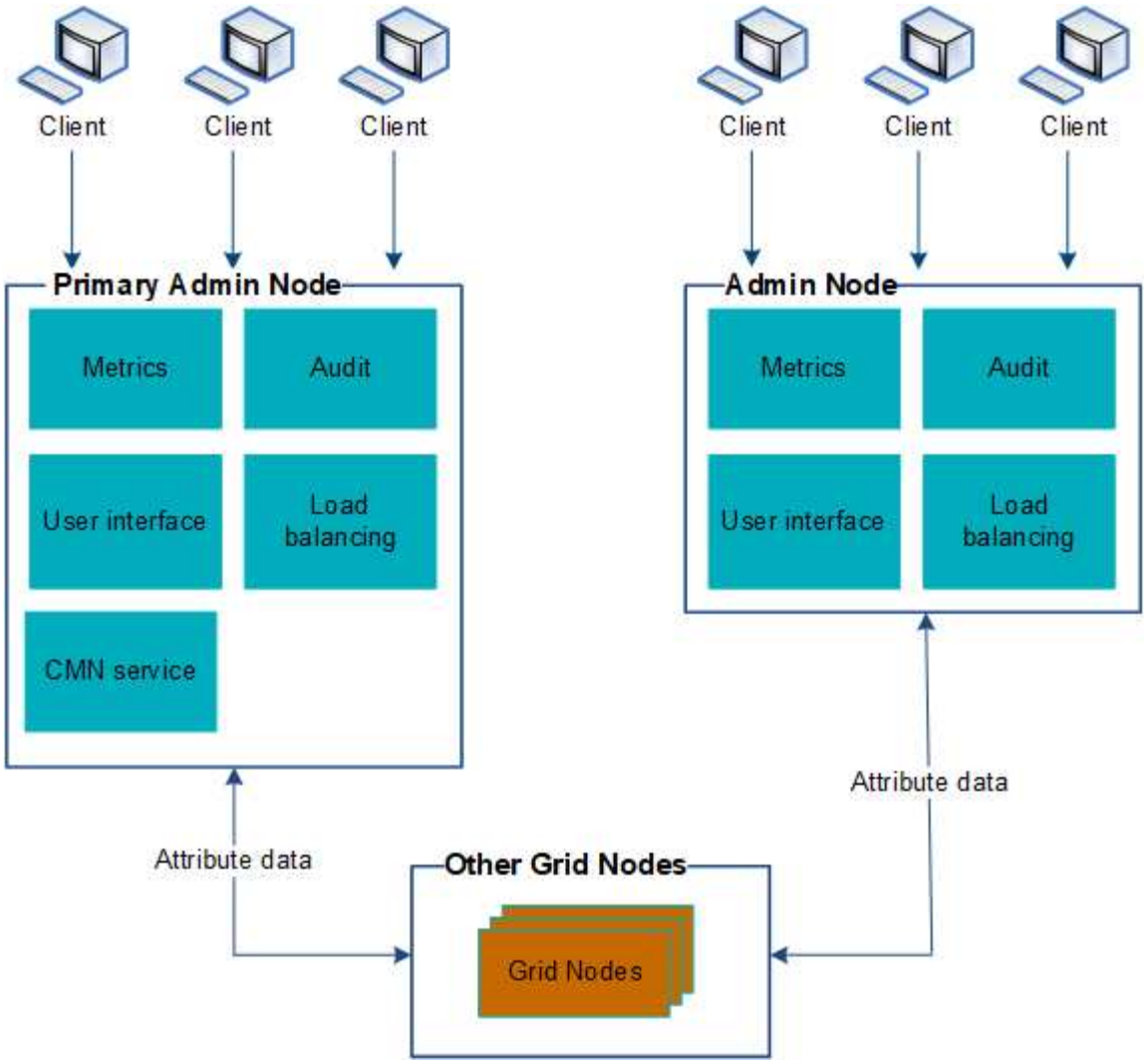
Managing load balancing

Managing high availability groups

Using multiple Admin Nodes

A StorageGRID system can include multiple Admin Nodes to enable you to continuously monitor and configure your StorageGRID system even if one Admin Node fails.

If an Admin Node becomes unavailable, attribute processing continues, alerts and alarms (legacy system) are still triggered, and email notifications and AutoSupport messages are still sent. However, having multiple Admin Nodes does not provide failover protection except for notifications and AutoSupport messages. In particular, alarm acknowledgments made from one Admin Node are not copied to other Admin Nodes.



There are two options for continuing to view and configure the StorageGRID system if an Admin Node fails:

- Web clients can reconnect to any other available Admin Node.
- If a system administrator has configured a high availability group of Admin Nodes, web clients can continue to access the Grid Manager or the Tenant Manager using the virtual IP address of the HA group.

> When using an HA group, access is interrupted if the Master Admin Node fails. Users must sign in again after the virtual IP address of the HA group fails over to another Admin Node in the group.

Some maintenance tasks can only be performed using the primary Admin Node. If the primary Admin Node fails, it must be recovered before the StorageGRID system is fully functional again.

Related information

Managing high availability groups

Identifying the primary Admin Node

The primary Admin Node hosts the CMN service. Some maintenance procedures can only be performed using the primary Admin Node.

What you'll need

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

Steps

1. Select **Support** > **Tools** > **Grid Topology**.
2. Select ***site*** > **Admin Node**, and then click ➕ to expand the topology tree and show the services hosted on this Admin Node.

   The primary Admin Node hosts the CMN service.

3. If this Admin Node does not host the CMN service, check the other Admin Nodes.

Selecting a preferred sender

If your StorageGRID deployment includes multiple Admin Nodes, you can select which Admin Node should be the preferred sender of notifications. By default, the primary Admin Node is selected, but any Admin Node can be the preferred sender.

What you'll need

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

About this task

The **Configuration** > **System Settings** > **Display Options** page shows which Admin Node is currently selected to be the preferred sender. The primary Admin Node is selected by default.

Under normal system operations, only the preferred sender sends the following notifications:

- AutoSupport messages
- SNMP notifications
- Alert emails
- Alarm emails (legacy system)

However, all other Admin Nodes (standby senders) monitor the preferred sender. If a problem is detected, a standby sender can also send these notifications.

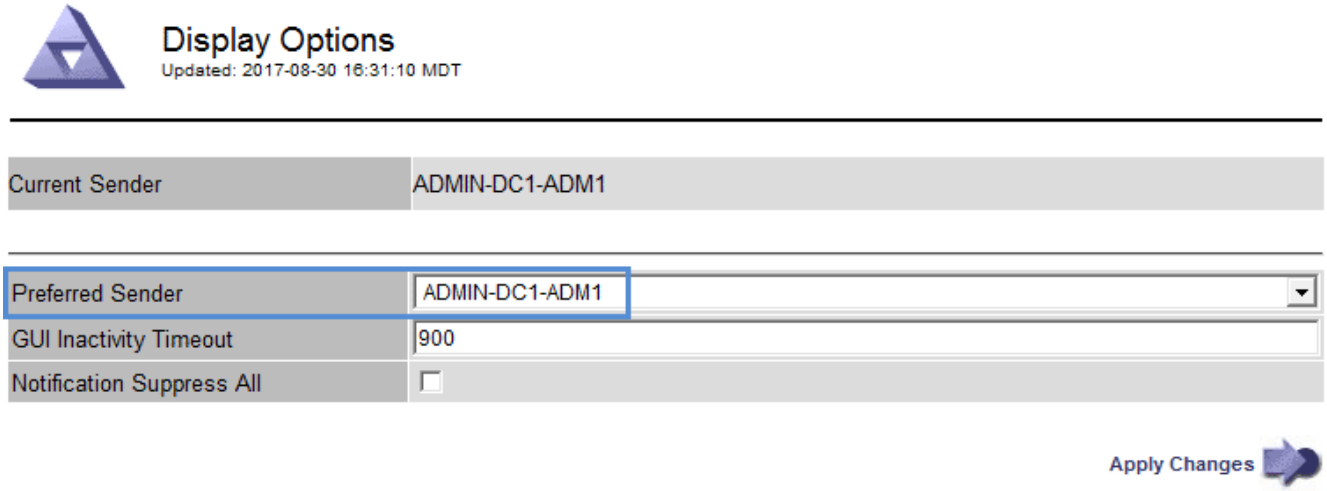
Both the preferred sender and a standby sender might send notifications in these cases:

- If Admin Nodes become "islanded" from each other, both the preferred sender and the standby senders will attempt to send notifications, and multiple copies of notifications might be received.
- After a standby sender detects problems with the preferred sender and starts sending notifications, the preferred sender might regain its ability to send notifications. If this occurs, duplicate notifications might be sent. The standby sender will stop sending notifications when it no longer detects errors on the preferred sender.

> ⓘ When you test alarm notifications and AutoSupport messages, all Admin Nodes send the test email. When you test alert notifications, you must sign in to every Admin Node to verify connectivity.

Steps

1. Select **Configuration** > **System Settings** > **Display Options**.
2. From the Display Options menu, select **Options**.
3. Select the Admin Node you want to set as the preferred sender from the drop-down list.



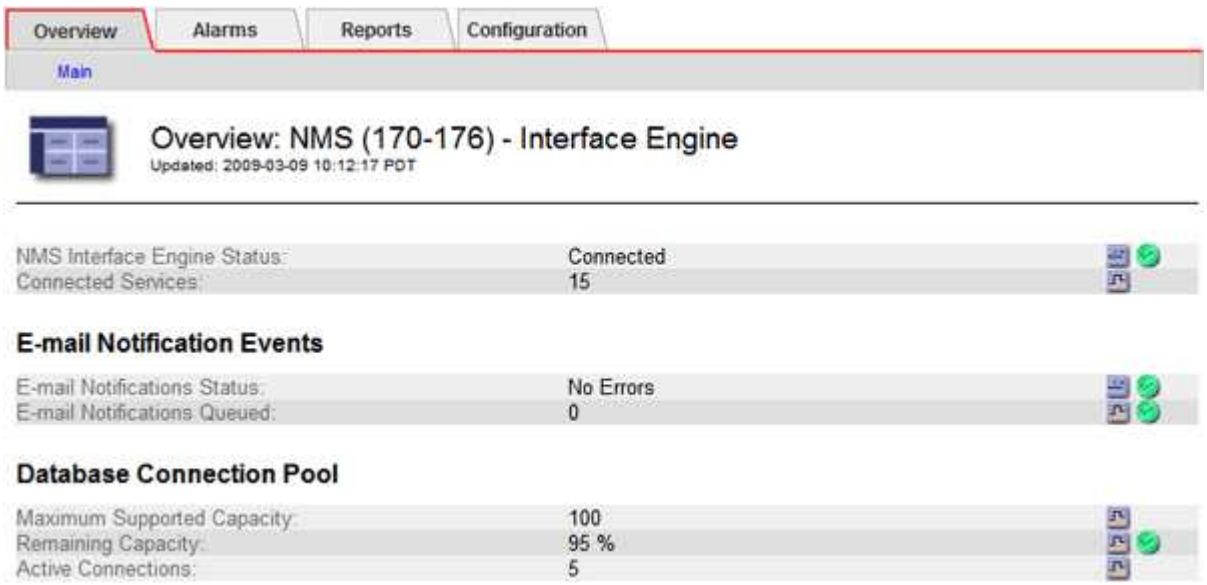
4. Click **Apply Changes**.

   The Admin Node is set as the preferred sender of notifications.

Viewing notification status and queues

The NMS service on Admin Nodes sends notifications to the mail server. You can view the current status of the NMS service and the size of its notifications queue on the Interface Engine page.

To access the Interface Engine page, select **Support** > **Tools** > **Grid Topology**. Finally, select ***site*** > ***Admin Node*** > **NMS** > **Interface Engine**.



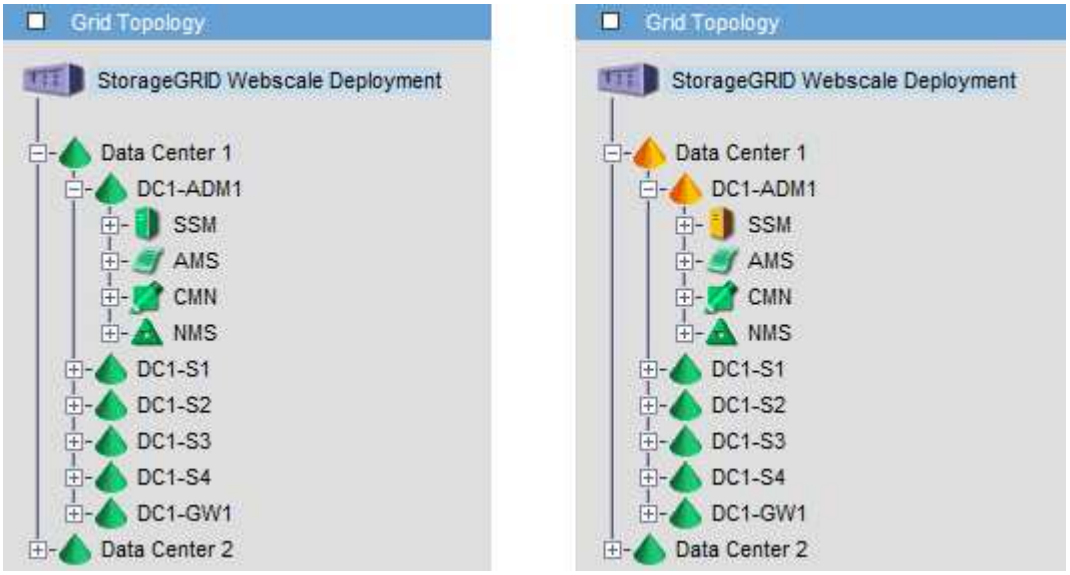
Notifications are processed through the email notifications queue and are sent to the mail server one after

another in the order they are triggered. If there is a problem (for example, a network connection error) and the mail server is unavailable when the attempt is made to send the notification, a best effort attempt to resend the notification to the mail server continues for a period of 60 seconds. If the notification is not sent to the mail server after 60 seconds, the notification is dropped from the notifications queue and an attempt to send the next notification in the queue is made. Because notifications can be dropped from the notifications queue without being sent, it is possible that an alarm can be triggered without a notification being sent. In the event that a notification is dropped from the queue without being sent, the MINS (E-mail Notification Status) Minor alarm is triggered.

How Admin Nodes show acknowledged alarms (legacy system)

When you acknowledge an alarm on one Admin Node, the acknowledged alarm is not copied to any other Admin Node. Because acknowledgments are not copied to other Admin Nodes, the Grid Topology tree might not look the same for each Admin Node.

This difference can be useful when connecting web clients. Web clients can have different views of the StorageGRID system based on the administrator needs.



Note that notifications are sent from the Admin Node where the acknowledgment occurs.

Configuring audit client access

The Admin Node, through the Audit Management System (AMS) service, logs all audited system events to a log file available through the audit share, which is added to each Admin Node at installation. For easy access to audit logs, you can configure client access to audit shares for both CIFS and NFS.

The StorageGRID system uses positive acknowledgment to prevent loss of audit messages before they are written to the log file. A message remains queued at a service until the AMS service or an intermediate audit relay service has acknowledged control of it.

For more information, see the instructions for understanding audit messages.

If you have the option to use CIFS or NFS, choose NFS.

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

Related information

What an Admin Node is

Review audit logs

Upgrade software

Configuring audit clients for CIFS

The procedure used to configure an audit client depends on the authentication method: Windows Workgroup or Windows Active Directory (AD). When added, the audit share is automatically enabled as a read-only share.

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

Related information

Upgrade software

Configuring audit clients for Workgroup

Perform this procedure for each Admin Node in a StorageGRID deployment from which you want to retrieve audit messages.

What you'll need

- You must have the `Passwords.txt` file with the root/admin account password (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

About this task

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

Steps

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_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.

      When you are logged in as root, the prompt changes from `$` to `#`.
2. Confirm that all services have a state of Running or Verified: `storagegrid-status`

If all services are not Running or Verified, resolve issues before continuing.

3. Return to the command line, press **Ctrl+C**.
4. Start the CIFS configuration utility: `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                 | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share        | set-authentication     | validate-config |
| enable-disable-share   | set-netbios-name       | help            |
| add-user-to-share      | join-domain            | exit            |
| remove-user-from-share | add-password-server    |                 |
| modify-group           | remove-password-server |                 |
|                        | add-wins-server        |                 |
|                        | remove-wins-server     |                 |
------------------------------------------------------------------------
```

5. Set the authentication for the Windows Workgroup:

   If authentication has already been set, an advisory message appears. If authentication has already been set, go to the next step.

   a. Enter: `set-authentication`
   b. When prompted for Windows Workgroup or Active Directory installation, enter: `workgroup`
   c. When prompted, enter a name of the Workgroup: *`workgroup_name`*
   d. When prompted, create a meaningful NetBIOS name: *`netbios_name`*

      or

      Press **Enter** to use the Admin Node's hostname as the NetBIOS name.

      The script restarts the Samba server and changes are applied. This should take less than one minute. After setting authentication, add an audit client.

   e. When prompted, press **Enter**.

      The CIFS configuration utility is displayed.

6. Add an audit client:

   a. Enter: `add-audit-share`

      The share is automatically added as read-only.

   b. When prompted, add a user or group: *`user`*
   c. When prompted, enter the audit user name: *`audit_user_name`*
   d. When prompted, enter a password for the audit user: *`password`*

e. When prompted, re-enter the same password to confirm it: *password*

f. When prompted, press **Enter**.

The CIFS configuration utility is displayed.

There is no need to enter a directory. The audit directory name is predefined.

7. If more than one user or group is permitted to access the audit share, add the additional users:

a. Enter: `add-user-to-share`

A numbered list of enabled shares is displayed.

b. When prompted, enter the number of the audit-export share: *share_number*

c. When prompted, add a user or group: `user`

or `group`

d. When prompted, enter the name of the audit user or group: *audit_user or audit_group*

e. When prompted, press **Enter**.

The CIFS configuration utility is displayed.

f. Repeat these substeps for each additional user or group that has access to the audit share.

8. Optionally, verify your configuration: `validate-config`

The services are checked and displayed. You can safely ignore the following messages:

```
Can't find include file /etc/samba/includes/cifs-interfaces.inc
Can't find include file /etc/samba/includes/cifs-filesystem.inc
Can't find include file /etc/samba/includes/cifs-custom-config.inc
Can't find include file /etc/samba/includes/cifs-shares.inc
rlimit_max: increasing rlimit_max (1024) to minimum Windows limit
(16384)
```

a. When prompted, press **Enter**.

The audit client configuration is displayed.

b. When prompted, press **Enter**.

The CIFS configuration utility is displayed.

9. Close the CIFS configuration utility: `exit`
10. Start the Samba service: `service smbd start`
11. If the StorageGRID deployment is a single site, go to the next step.

or

Optionally, if the StorageGRID deployment includes Admin Nodes at other sites, enable these audit share as required:

a. Remotely log in to a site's Admin 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.
b. Repeat the steps to configure the audit share for each additional Admin Node.
c. Close the remote secure shell login to the remote Admin Node: `exit`

12. Log out of the command shell: `exit`

Related information

Upgrade software

Configuring audit clients for Active Directory

Perform this procedure for each Admin Node in a StorageGRID deployment from which you want to retrieve audit messages.

What you'll need

- You must have the `Passwords.txt` file with the root/admin account password (available in the SAID package).
- You must have the CIFS Active Directory username and password.
- You must have the `Configuration.txt` file (available in the SAID package).

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

Steps

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_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.

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

2. Confirm that all services have a state of Running or Verified: `storagegrid-status`

   If all services are not Running or Verified, resolve issues before continuing.

3. Return to the command line, press **Ctrl+C**.
4. Start the CIFS configuration utility: `config_cifs.rb`

```
-------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
-------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
-------------------------------------------------------------------
```

5. Set the authentication for Active Directory: `set-authentication`

   In most deployments, you must set the authentication before adding the audit client. If authentication has already been set, an advisory message appears. If authentication has already been set, go to the next step.

   a. When prompted for Workgroup or Active Directory installation: `ad`
   b. When prompted, enter the name of the AD domain (short domain name).
   c. When prompted, enter the domain controller's IP address or DNS hostname.
   d. When prompted, enter the full domain realm name.

      Use uppercase letters.

   e. When prompted to enable winbind support, type **y**.

      Winbind is used to resolve user and group information from AD servers.

   f. When prompted, enter the NetBIOS name.
   g. When prompted, press **Enter**.

      The CIFS configuration utility is displayed.

6. Join the domain:

   a. If not already started, start the CIFS configuration utility: `config_cifs.rb`
   b. Join the domain: `join-domain`
   c. You are prompted to test if the Admin Node is currently a valid member of the domain. If this Admin Node has not previously joined the domain, enter: `no`
   d. When prompted, provide the Administrator's username: *`administrator_username`*

      where *`administrator_username`* is the CIFS Active Directory username, not the StorageGRID username.

   e. When prompted, provide the Administrator's password: *`administrator_password`*

      were *`administrator_password`* is the CIFS Active Directory username, not the StorageGRID

password.

f. When prompted, press **Enter**.

The CIFS configuration utility is displayed.

7. Verify that you have correctly joined the domain:
   a. Join the domain: `join-domain`
   b. When prompted to test if the server is currently a valid member of the domain, enter: `y`

      If you receive the message “Join is OK,” you have successfully joined the domain. If you do not get this response, try setting authentication and joining the domain again.

   c. When prompted, press **Enter**.

      The CIFS configuration utility is displayed.

8. Add an audit client: `add-audit-share`
   a. When prompted to add a user or group, enter: `user`
   b. When prompted to enter the audit user name, enter the audit user name.
   c. When prompted, press **Enter**.

      The CIFS configuration utility is displayed.

9. If more than one user or group is permitted to access the audit share, add additional users: `add-user-to-share`

   A numbered list of enabled shares is displayed.

   a. Enter the number of the audit-export share.
   b. When prompted to add a user or group, enter: `group`

      You are prompted for the audit group name.

   c. When prompted for the audit group name, enter the name of the audit user group.
   d. When prompted, press **Enter**.

      The CIFS configuration utility is displayed.

   e. Repeat this step for each additional user or group that has access to the audit share.

10. Optionally, verify your configuration: `validate-config`

    The services are checked and displayed. You can safely ignore the following messages:

    - Can’t find include file `/etc/samba/includes/cifs-interfaces.inc`
    - Can’t find include file `/etc/samba/includes/cifs-filesystem.inc`
    - Can’t find include file `/etc/samba/includes/cifs-interfaces.inc`
    - Can’t find include file `/etc/samba/includes/cifs-custom-config.inc`

- Can't find include file `/etc/samba/includes/cifs-shares.inc`
- rlimit_max: increasing rlimit_max (1024) to minimum Windows limit (16384)

> Do not combine the setting 'security=ads' with the 'password server' parameter. (by default Samba will discover the correct DC to contact automatically).

a. When prompted, press **Enter** to display the audit client configuration.

b. When prompted, press **Enter**.

The CIFS configuration utility is displayed.

11. Close the CIFS configuration utility: `exit`
12. If the StorageGRID deployment is a single site, go to the next step.

or

Optionally, if the StorageGRID deployment includes Admin Nodes at other sites, enable these audit shares as required:

a. Remotely log in to a site's Admin 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.

b. Repeat these steps to configure the audit shares for each Admin Node.

c. Close the remote secure shell login to the Admin Node: `exit`

13. Log out of the command shell: `exit`

Related information

Upgrade software

Adding a user or group to a CIFS audit share

You can add a user or group to a CIFS audit share that is integrated with AD authentication.

What you'll need

- You must have the `Passwords.txt` file with the root/admin account password (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

About this task

The following procedure is for an audit share integrated with AD authentication.

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

Steps

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_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.

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

2. Confirm that all services have a state of Running or Verified. Enter: `storagegrid-status`

   If all services are not Running or Verified, resolve issues before continuing.

3. Return to the command line, press **Ctrl**+**C**.
4. Start the CIFS configuration utility: `config_cifs.rb`

```
------------------------------------------------------------------------
| Shares                  | Authentication         | Config          |
------------------------------------------------------------------------
| add-audit-share         | set-authentication     | validate-config |
| enable-disable-share    | set-netbios-name       | help            |
| add-user-to-share       | join-domain            | exit            |
| remove-user-from-share  | add-password-server    |                 |
| modify-group            | remove-password-server |                 |
|                         | add-wins-server        |                 |
|                         | remove-wins-server     |                 |
------------------------------------------------------------------------
```

5. Start adding a user or group: `add-user-to-share`

   A numbered list of audit shares that have been configured is displayed.

6. When prompted, enter the number for the audit share (audit-export): *`audit_share_number`*

   You are asked if you would like to give a user or a group access to this audit share.

7. When prompted, add a user or group: `user` or `group`
8. When prompted for the user or group name for this AD audit share, enter the name.

   The user or group is added as read-only for the audit share both in the server's operating system and in the CIFS service. The Samba configuration is reloaded to enable the user or group to access the audit client share.

9. When prompted, press **Enter**.

   The CIFS configuration utility is displayed.

10. Repeat these steps for each user or group that has access to the audit share.
11. Optionally, verify your configuration: `validate-config`

    The services are checked and displayed. You can safely ignore the following messages:

    - Can't find include file /etc/samba/includes/cifs-interfaces.inc
    - Can't find include file /etc/samba/includes/cifs-filesystem.inc
    - Can't find include file /etc/samba/includes/cifs-custom-config.inc
    - Can't find include file /etc/samba/includes/cifs-shares.inc
        a. When prompted, press **Enter** to display the audit client configuration.
        b. When prompted, press **Enter**.
12. Close the CIFS configuration utility: `exit`
13. Determine if you need to enable additional audit shares, as follows:
    - If the StorageGRID deployment is a single site, go to the next step.
    - If the StorageGRID deployment includes Admin Nodes at other sites, enable these audit shares as required:
        a. Remotely log in to a site's Admin 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.
        b. Repeat these steps to configure the audit shares for each Admin Node.
        c. Close the remote secure shell login to the remote Admin Node: `exit`
14. Log out of the command shell: `exit`

Removing a user or group from a CIFS audit share

You cannot remove the last user or group permitted to access the audit share.

What you'll need

- You must have the `Passwords.txt` file with the root account passwords (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

About this task

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

Steps

1. Log in to the primary Admin Node:
    a. Enter the following command: `ssh admin@primary_Admin_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.

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

2. Start the CIFS configuration utility: `config_cifs.rb`

```
------------------------------------------------------------------
| Shares                | Authentication         | Config          |
------------------------------------------------------------------
| add-audit-share       | set-authentication     | validate-config |
| enable-disable-share  | set-netbios-name       | help            |
| add-user-to-share     | join-domain            | exit            |
| remove-user-from-share| add-password-server    |                 |
| modify-group          | remove-password-server |                 |
|                       | add-wins-server        |                 |
|                       | remove-wins-server     |                 |
------------------------------------------------------------------
```

3. Start removing a user or group: `remove-user-from-share`

   A numbered list of available audit shares for the Admin Node is displayed. The audit share is labeled audit-export.

4. Enter the number of the audit share: *`audit_share_number`*
5. When prompted to remove a user or a group: `user` or `group`

   A numbered list of users or groups for the audit share is displayed.

6. Enter the number corresponding to the user or group you want to remove: *`number`*

   The audit share is updated, and the user or group is no longer permitted access to the audit share. For example:

```
Enabled shares
 1. audit-export
Select the share to change: 1
Remove user or group? [User/group]: User
Valid users for this share
1. audituser
2. newaudituser
Select the user to remove: 1

Removed user "audituser" from share "audit-export".

Press return to continue.
```

7. Close the CIFS configuration utility: `exit`
8. If the StorageGRID deployment includes Admin Nodes at other sites, disable the audit share at each site as required.
9. Log out of each command shell when configuration is complete: `exit`

Related information

Upgrade software

Changing a CIFS audit share user or group name

You can change the name of a user or a group for a CIFS audit share by adding a new user or group and then deleting the old one.

About this task

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

Steps

1. Add a new user or group with the updated name to the audit share.
2. Delete the old user or group name.

Related information

Upgrade software

Adding a user or group to a CIFS audit share

Removing a user or group from a CIFS audit share

Verifying CIFS audit integration

The audit share is read-only. Log files are intended to be read by computer applications and verification does not include opening a file. It is considered sufficient verification that the audit log files appear in a Windows Explorer window. Following connection verification, close all windows.

Configuring the audit client for NFS

The audit share is automatically enabled as a read-only share.

What you'll need

- You must have the `Passwords.txt` file with the root/admin password (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).
- The audit client must be using NFS Version 3 (NFSv3).

About this task

Perform this procedure for each Admin Node in a StorageGRID deployment from which you want to retrieve audit messages.

Steps

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_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.

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

2. Confirm that all services have a state of Running or Verified. Enter: `storagegrid-status`

   If any services are not listed as Running or Verified, resolve issues before continuing.

3. Return to the command line. Press **Ctrl**+**C**.
4. Start the NFS configuration utility. Enter: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients               | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share       | validate-config |
| enable-disable-share  | remove-ip-from-share  | refresh-config  |
|                       |                       | help            |
|                       |                       | exit            |
------------------------------------------------------------------
```

5. Add the audit client: `add-audit-share`
   a. When prompted, enter the audit client's IP address or IP address range for the audit share: `client_IP_address`
   b. When prompted, press **Enter**.
6. If more than one audit client is permitted to access the audit share, add the IP address of the additional user: `add-ip-to-share`
   a. Enter the number of the audit share: *`audit_share_number`*
   b. When prompted, enter the audit client's IP address or IP address range for the audit share: *`client_IP_address`*
   c. When prompted, press **Enter**.

      The NFS configuration utility is displayed.

   d. Repeat these substeps for each additional audit client that has access to the audit share.
7. Optionally, verify your configuration.
   a. Enter the following: `validate-config`

      The services are checked and displayed.

   b. When prompted, press **Enter**.

The NFS configuration utility is displayed.

c. Close the NFS configuration utility: `exit`

8. Determine if you must enable audit shares at other sites.
   - If the StorageGRID deployment is a single site, go to the next step.
   - If the StorageGRID deployment includes Admin Nodes at other sites, enable these audit shares as required:
     a. Remotely log in to the site's Admin 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.
     b. Repeat these steps to configure the audit shares for each additional Admin Node.
     c. Close the remote secure shell login to the remote Admin Node. Enter: `exit`
9. Log out of the command shell: `exit`

NFS audit clients are granted access to an audit share based on their IP address. Grant access to the audit share to a new NFS audit client by adding its IP address to the share, or remove an existing audit client by removing its IP address.

Adding an NFS audit client to an audit share

NFS audit clients are granted access to an audit share based on their IP address. Grant access to the audit share to a new NFS audit client by adding its IP address to the audit share.

What you'll need

- You must have the `Passwords.txt` file with the root/admin account password (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).
- The audit client must be using NFS Version 3 (NFSv3).

Steps

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@primary_Admin_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.

   When you are logged in as root, the prompt changes from `$` to `#`.
2. Start the NFS configuration utility: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Enter: `add-ip-to-share`

   A list of NFS audit shares enabled on the Admin Node is displayed. The audit share is listed as: `/var/local/audit/export`

4. Enter the number of the audit share: *`audit_share_number`*
5. When prompted, enter the audit client's IP address or IP address range for the audit share: *`client_IP_address`*

   The audit client is added to the audit share.

6. When prompted, press **Enter**.

   The NFS configuration utility is displayed.

7. Repeat the steps for each audit client that should be added to the audit share.
8. Optionally, verify your configuration: `validate-config`

   The services are checked and displayed.

   a. When prompted, press **Enter**.

      The NFS configuration utility is displayed.

9. Close the NFS configuration utility: `exit`
10. If the StorageGRID deployment is a single site, go to the next step.

    Otherwise, if the StorageGRID deployment includes Admin Nodes at other sites, optionally enable these audit shares as required:

    a. Remotely log in to a site's Admin 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.
    b. Repeat these steps to configure the audit shares for each Admin Node.
    c. Close the remote secure shell login to the remote Admin Node: `exit`

11. Log out of the command shell: `exit`

Verifying NFS audit integration

After you configure an audit share and add an NFS audit client, you can mount the audit client share and verify that the files are available from the audit share.

Steps

1. Verify connectivity (or variant for the client system) using the client-side IP address of the Admin Node hosting the AMS service. Enter: `ping IP_address`

   Verify that the server responds, indicating connectivity.

2. Mount the audit read-only share using a command appropriate to the client operating system. A sample Linux command is (enter on one line):

   `mount -t nfs -o hard,intr` *`Admin_Node_IP_address`*`:/var/local/audit/export` *`myAudit`*

   Use the IP address of the Admin Node hosting the AMS service and the predefined share name for the audit system. The mount point can be any name selected by the client (for example, *`myAudit`* in the previous command).

3. Verify that the files are available from the audit share. Enter: `ls` *`myAudit`* `/*`

   where *`myAudit`* is the mount point of the audit share. There should be at least one log file listed.

Removing an NFS audit client from the audit share

NFS audit clients are granted access to an audit share based on their IP address. You can remove an existing audit client by removing its IP address.

What you'll need

- You must have the `Passwords.txt` file with the root/admin account password (available in the SAID package).
- You must have the `Configuration.txt` file (available in the SAID package).

About this task

You cannot remove the last IP address permitted to access the audit share.

Steps

1. Log in to the primary Admin Node:
   a. Enter the following command: `ssh admin@`*`primary_Admin_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.

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

2. Start the NFS configuration utility: `config_nfs.rb`

```
------------------------------------------------------------------
| Shares                | Clients              | Config          |
------------------------------------------------------------------
| add-audit-share       | add-ip-to-share      | validate-config |
| enable-disable-share  | remove-ip-from-share | refresh-config  |
|                       |                      | help            |
|                       |                      | exit            |
------------------------------------------------------------------
```

3. Remove the IP address from the audit share: `remove-ip-from-share`

   A numbered list of audit shares configured on the server is displayed. The audit share is listed as: `/var/local/audit/export`

4. Enter the number corresponding to the audit share: *`audit_share_number`*

   A numbered list of IP addresses permitted to access the audit share is displayed.

5. Enter the number corresponding to the IP address you want to remove.

   The audit share is updated, and access is no longer permitted from any audit client with this IP address.

6. When prompted, press **Enter**.

   The NFS configuration utility is displayed.

7. Close the NFS configuration utility: `exit`
8. If your StorageGRID deployment is a multiple data center site deployment with additional Admin Nodes at the other sites, disable these audit shares as required:
   a. Remotely log in to each site's Admin 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.
   b. Repeat these steps to configure the audit shares for each additional Admin Node.
   c. Close the remote secure shell login to the remote Admin Node: `exit`
9. Log out of the command shell: `exit`

Changing the IP address of an NFS audit client

1. Add a new IP address to an existing NFS audit share.
2. Remove the original IP address.

Related information

Copyright information

Trademark information