Configure audit client access

StorageGRID 11.7

NetApp
April 12, 2024

Table of Contents

Configure audit client access

Configure audit client access for NFS

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

To access audit logs, you can configure client access to audit shares for NFS. Or, you can use an external syslog server.

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 Review audit logs.

Before you begin

- You have the `Passwords.txt` file with the root/admin password.
- You have the `Configuration.txt` file (available in the Recovery Package).
- The audit client is 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 aren't 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.

Add 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.

Before you begin

- You have the `Passwords.txt` file with the root/admin account password.
- You have the `Configuration.txt` file (available in the Recovery Package).
- The audit client is 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`

Verify 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.

Remove 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.

Before you begin

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

About this task

You can't 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`

Change the IP address of an NFS audit client

Complete these steps if you need to change the IP address of an NFS audit client.

Steps

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

Related information

- Add an NFS audit client to an audit share
- Remove an NFS audit client from the audit share