Configure audit clients for CIFS

StorageGRID

NetApp
March 01, 2022

Table of Contents

Configure 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.

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

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

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

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

Change 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

- Add a user or group to a CIFS audit share
- Remove a user or group from a CIFS audit share

Verify 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.

Copyright Information

Trademark Information