ManageEngine
ADAudit Plus

Hitachi NAS
Auditing Guide

Table of contents

Overview of Hitachi NAS auditing

Hitachi network-attached storage (NAS) devices are special-purpose storage devices or file servers that are connected directly to a network. Each Hitachi NAS file server can consist of several Enterprise Virtual Servers (EVSs).

ManageEngine ADAudit Plus is a change auditing solution that provides visibility into your Hitachi NAS servers. ADAudit Plus monitors the configured EVSs and the shares residing on these virtual servers. Driven by user behavior analytics, it delivers detailed reports on user activity in Hitachi NAS files and shares, analyzes permission changes, and automates instant responses to security incidents. ADAudit Plus also streamlines compliance with numerous regulations, such as HIPAA, FISMA, the GDPR, and SOX.

Supported versions

Hitachi NAS 13.2 and above

Audited events

ADAudit Plus audits every attempt to perform the following file activities on Hitachi NAS servers:

- Create
- Read
- Modify
- Write
- Delete
- Change file permissions
- Rename
- Move

This guide provides the steps to configure auditing for your Hitachi NAS servers using ADAudit Plus.

Privileges required

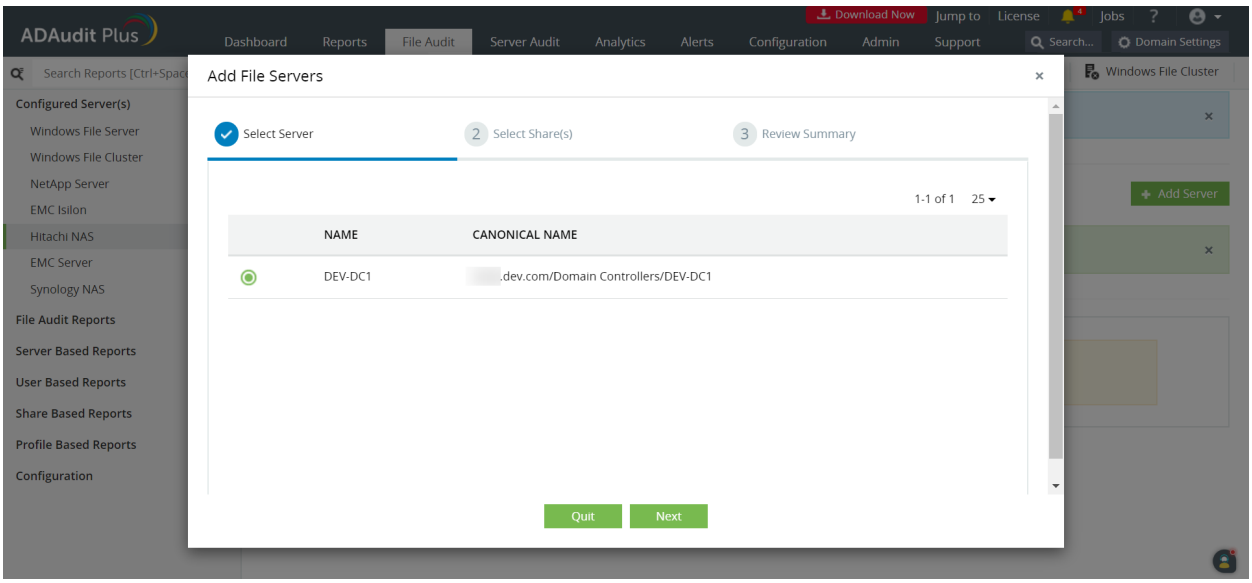
Certain minimum privileges are required to ensure the effective functioning of ADAudit Plus while auditing your Hitachi NAS servers. You can provide the following privileges to the user configured under Domain Settings in ADAudit Plus (in the top-right corner of the console):

- Discover shares.
- Scan the shares for metadata.
- Read audit files (EVT files) from the shared folder.
- Automatically enable the SACLs on each share.

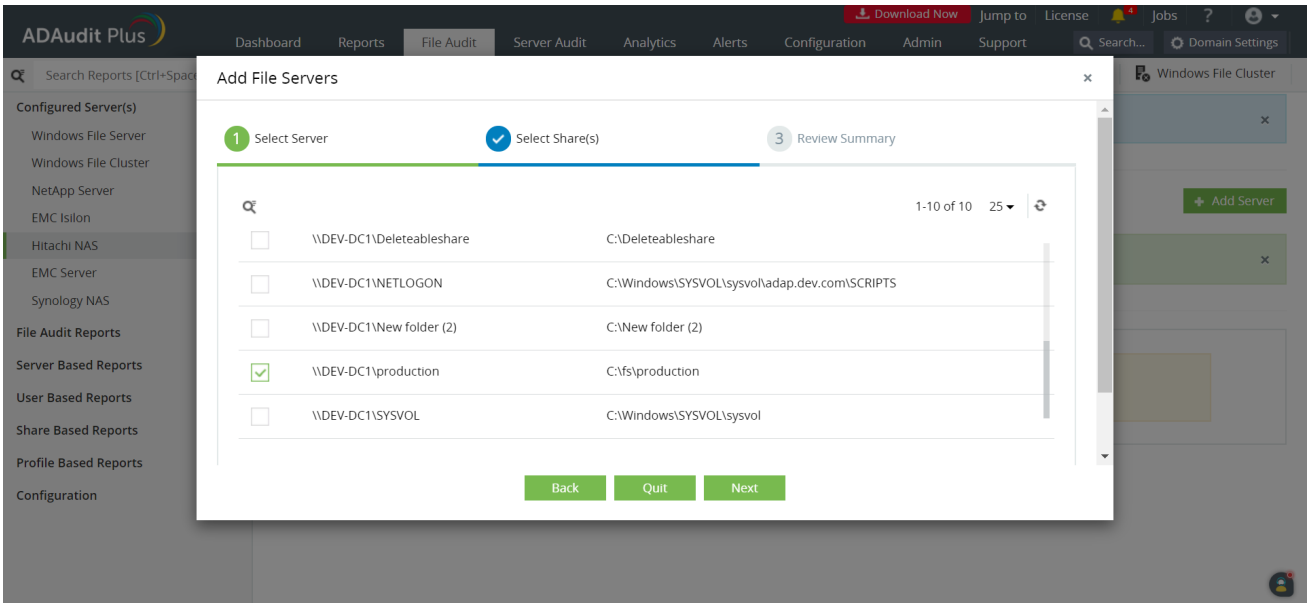
Adding Hitachi NAS servers

To add your target Hitachi NAS server to your ADAudit Plus console, follow these steps:

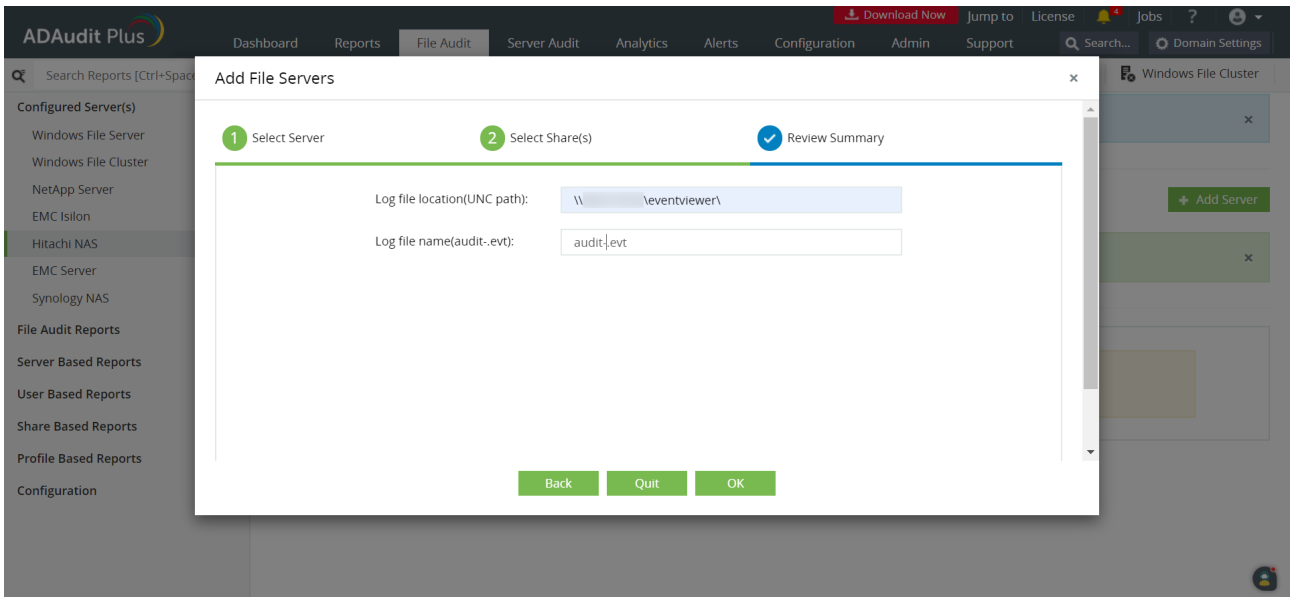
1. Log in to the ADAudit Plus web console.
2. Navigate to the **File Audit** tab > **Configured Server(s)** > **Hitachi NAS**. From the **Domain** drop-down, select the domain with the target server.
3. Click **+ Add Server** in the top-right corner. This will open the Add File Servers pop-up, listing all the servers available in the selected domain.



4. Select the target server and click **Next.**
5. From the listed shares, select the ones you wish to audit, then click **Next.**



6. Review your **Log file location (UNC path)** and the **Log file name (audit .evt),** then click **OK.**



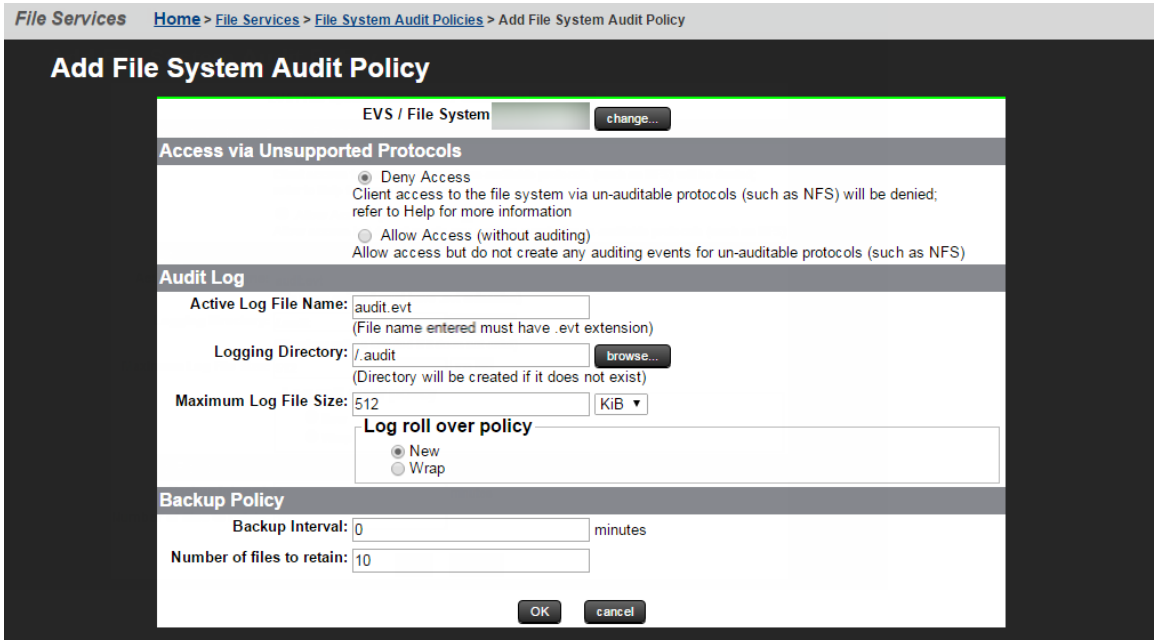
Configuring audit policies

This section outlines the steps to configure the Hitachi NAS file server for file system auditing.

a. Configure a file system audit policy on a Hitachi NAS EVS

To configure a file system audit policy on each EVS file system that you want to audit, follow the steps below:

1. Log in to the Hitachi NAS console using administrator credentials.
2. Navigate to **Home > File Services > File System Audit Policies.**
3. Select each **EVS / File System** that you want to enable auditing for, then click **add.**
4. On the Add File System Audit Policy page, retain the default settings specified, and click **OK** to save the policy.

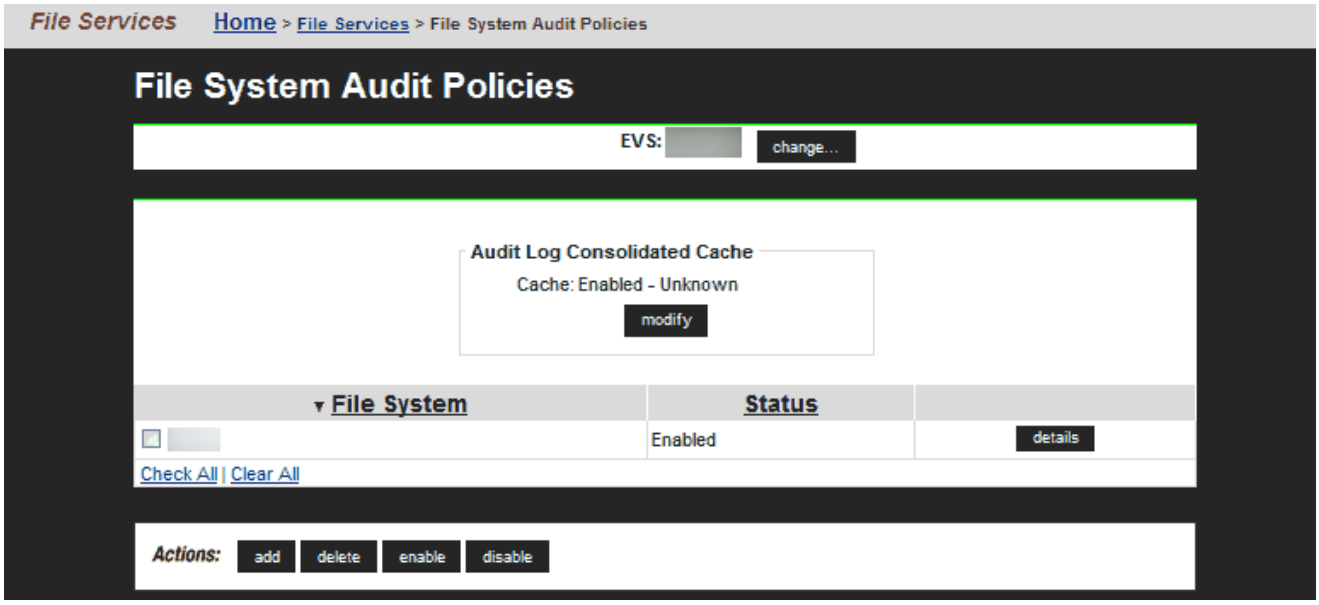


b. Enable auditing for a file system

File system auditing can be enabled on a per-file-system basis. To add a file system to the file system audit list and enable auditing, follow the steps below:

1. Log in to the Hitachi NAS console using administrator credentials.
2. Navigate to **Home > File Services > File System Audit Policies.**
3. If the file system you want to enable auditing on is listed, an audit policy has already been defined for that file system.

- If the Audit Policy Status is enabled, logging is already enabled for the file system, and no further actions are required.
- If the Audit Policy Status is disabled, select the check box next to the file system name, and click **enable.**



Note:

If the file system you want to enable auditing on is not displayed, a file system audit policy may not have been defined for that file system, or the file system might not be in the currently selected EVS.

If the file system you want to enable auditing on is not displayed, click **change** to go to the **Select an EVS page,** and select a different EVS.

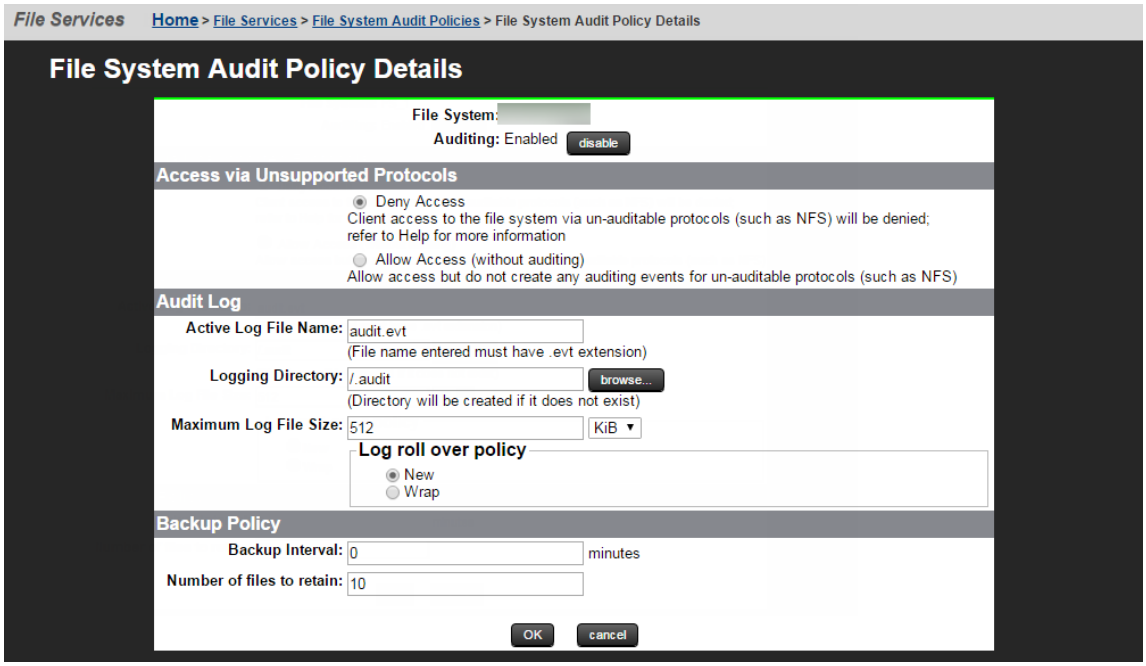
- After selecting a different EVS, if the file system you want to enable auditing on is now listed on the **File System Audit Policies** page, select the check box next to the file system name and click **enable.**

- After selecting a different EVS, if the file system you want to enable auditing on is still not displayed, you must define a file system audit policy for that file system. Click **add** to go to the **Add File System Audit Policy** page, and configure an audit policy for the file system.

c. Modify a file system audit policy

To modify a file system audit policy, follow the steps below:

1. Log in to the Hitachi NAS console using administrator credentials.
2. Navigate to **Home > Files Services > File System Audit Policies.**
3. Click **change** to go to the **Select an EVS** page, and select the EVS hosting the file system with the audit policy you want to change.
4. Click the **details** button on the file system with the audit policy you want to modify.
5. On the **File System Audit Policy** Details page, modify the policy as required.
6. Click **OK** to save the policy as specified.



d. Disable auditing for a file system

To disable auditing for a file system, follow the steps below:

1. Log in to the Hitachi NAS console using administrator credentials.
2. Navigate to **Home > Files Services > File System Audit Policies.**
3. Click **change** to go to the Select an EVS page, and select the EVS hosting the file system with the audit policy you want to disable.
4. Select the check box next to the name of the file system with the audit policy you want to disable.
5. Click **disable** to stop the policy from functioning.

Note:

When an audit policy is disabled, file system access operations are not logged and protocol restrictions are not enforced. Also, disabling a policy does not delete it.

e. Check if auditing is enabled on the EVS

To verify if auditing is enabled on the EVS for the required file system, generate some activity on the shares created on the file system. Execute the following command on the Hitachi NAS console to see if the events are generated:

```
audit-log-show <Name of file system>
```

Configuring object-level auditing

Configure auditing on the Windows client

To configure which events get audited from the Windows client, follow the steps below:

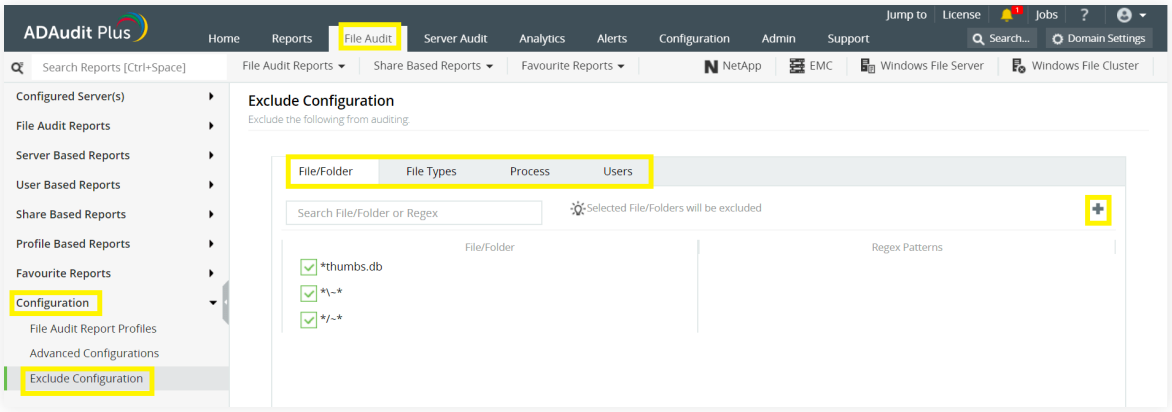
1. Right-click a folder that resides on a server file system that is configured for auditing, and select **Properties**. Select the **Security** tab.
2. Click **Advanced** and select the **Auditing** tab.
3. Select **Add** and choose which users get audited.
4. In the pop-up, select which events are to be audited for the specified user.

You can choose to audit events that are **Successful, Failed**, or **both** for each access type.

Exclude configuration

Files/folders can be excluded based on File/folder local path, file type, process name, and user name by using the Exclude Configuration setting.

Log in to ADAudit Plus' web console ⟶ Go to the File Audit tab, navigate to the left pane, click on Configuration and then on Exclude Configuration ⟶ Choose to exclude by File/Folder local path, File Type, Process Name, or Users ⟶ Click on '+', and configure the necessary settings.



Example scenarios, to exclude by File/Folder local path:

Objective	To exclude a folder and all of its subfolders and files	
Share configured	**Share path**	**Local path**
	\\SERVER_NAME\share_name	C:\sharefolder
Path of folder that is to be excluded	C:\sharefolder\excludefolder	
File/Folder or Regex Patterns	File/Folder Patterns	
Syntax	• C:\sharefolder\excludefolder • C:\sharefolder\excludefolder*	
What will get excluded	• C:\sharefolder\excludefolder • C:\sharefolder\excludefolder\folder • C:\sharefolder\excludefolder\files.txt • C:\sharefolder\excludefolder\folder\files.txt	
What won't get excluded		

Objective	To exclude "AppData" folder for every user profile
Share and folder path	\\SERVER_NAME\Users C:\Users
Path of folder that is to be excluded	C:\Users\user1\AppData
File/Folder or Regex Patterns	Regex Patterns
Syntax	C:\\Users\\[^\\]*\\AppData
What will get excluded	• C:\Users\user1\AppData • C:\Users\user2\AppData • C:\Users\user1\AppData\subfolder • C:\Users\user2\AppData\subfolder
What won't get excluded	• C:\Users\user1\subfolder\AppData • C:\Users\user2\subfolder\AppData

Objective	**To exclude files from a specific folder but audit all subfolders and its contents**
Share and folder path	\\SERVER_NAME\share_name C:\sharefolder
Path of folder that is to be excluded	C:\sharefolder\excludefolder
File/Folder or Regex Patterns	Regex Patterns
Syntax	^C:\\sharefolder\\excludefolder\\[^\\]*\.[^\\]*$
What will get excluded	• C:\sharefolder\excludefolder\file.txt • C:\sharefolder\excludefolder\folder.withDot
What won't get excluded	• C:\sharefolder\excludefolder • C:\sharefolder\excludefolder\folderWithoutDot • C:\sharefolder\excludefolder\folderWithoutDot\subfolder • C:\sharefolder\excludefolder\folderWithoutDot\testfile.txt • C:\sharefolder\excludefolder\folder.withDot\subfolder • C:\sharefolder\excludefolder\folder.withDot\testfile.txt

Troubleshooting

To learn about the common issues faced in Hitachi NAS auditing using ADAudit Plus, review these steps.

1. The network name cannot be found

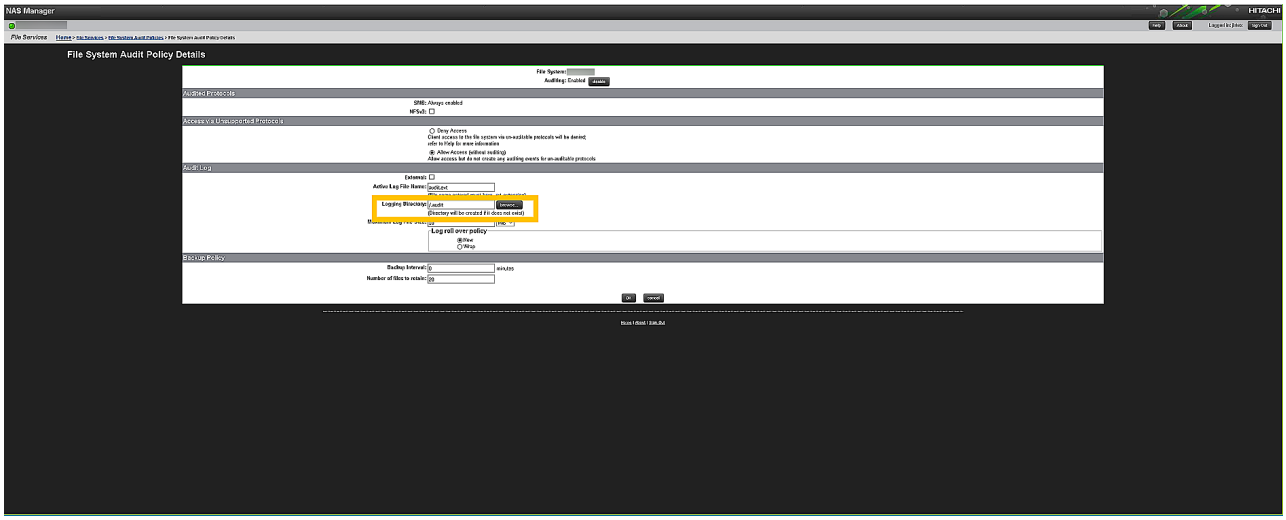
Cause:

This error occurs when the DNS server is not reachable or if the Hitachi server's name is not registered in the DNS.

Troubleshooting:

i. Check whether the audit files (evt file shares) located in the logging directory are accessible from the ADAudit Plus server.

1. Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
2. In the Network window, double click on the target Hitachi server.
3. Navigate to the audit file share path **(Logging Directory)** as specified in the Hitachi web console and try to access the audit file shares. Alternatively, you can run the UNC path to the audit file logging directory and try to access the shares.
4. If you are able to access the shares on the target Hitachi server, ping the Hitachi server.



ii. Ping the Hitachi server by name from the ADAudit Plus server.

1. Login to your ADAudit Plus web console.
2. Navigate to **File Audit > Configured Servers > Hitachi NAS.**
3. Select your domain and note the name of the Hitachi server as found in ADAudit Plus console.

4. Open **Command Prompt** in the ADAudit Plus server and ping the Hitachi server by its name as noted from the ADAudit Plus console to verify that the name resolves to the correct IP address.
5. If the ping to the Hitachi server is successful, name resolution is not likely to be the cause of the issue.
6. If the ping to the Hitachi server fails, append the DNS suffix in the **Advanced TCP/IP settings** or add a host record in the DNS server, mapping this name to the Hitachi server's IP address.

2. There are no more files - Error code - 12

Cause:

This error occurs when all the events from the audit file share have been processed and no more audit files (evt file shares) are available for processing.

3. The network path was not found

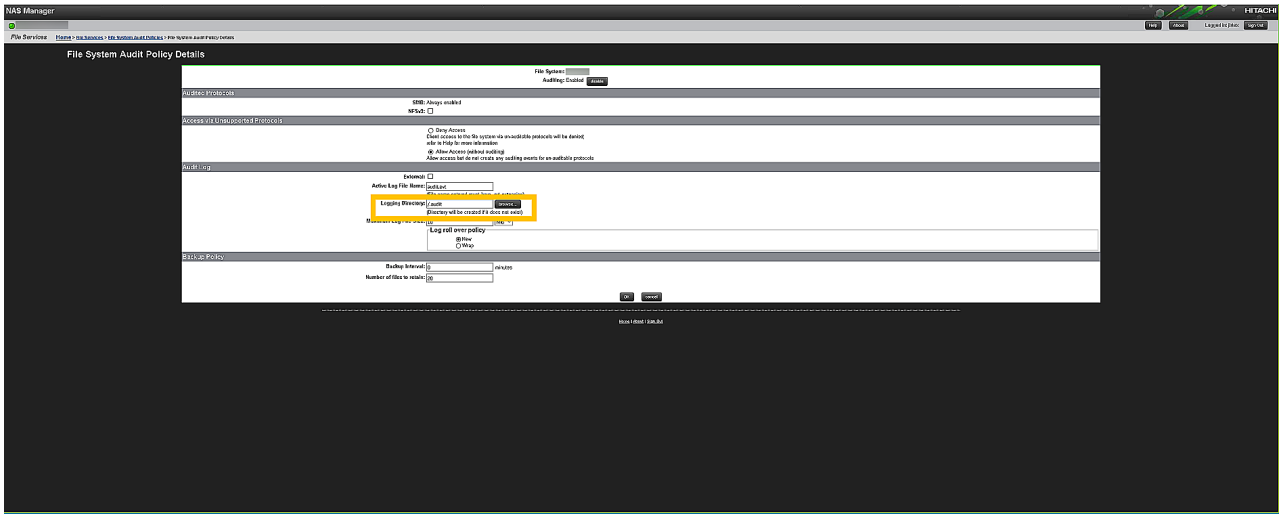
Cause:

This error occurs when the ADAudit Plus server is unable to contact the target Hitachi server.

Troubleshooting:

i. Try to connect to the audit files (evt files shares) from the ADAudit Plus server.

1. Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
2. In the Network window, double click on the target Hitachi server which contains the shared folder.
3. Navigate to the audit file share path **(Logging directory)** as specified in the Hitachi web console and double click on the share you want to access.
4. If you are able to access the shares on the target Hitachi server, ping the Hitachi server.



ii. Ping the Hitachi server by name from the ADAudit Plus server.

1. Login to your ADAudit Plus web console.
2. Navigate to **File Audit > Configured Servers > Hitachi NAS** and select your domain.
3. Identify and note the name of the Hitachi server showing the error.
4. Open **Command Prompt** in the ADAudit Plus server and ping the Hitachi server by its name as noted from ADAudit Plus console to verify that the name resolves to the correct IP address.
5. If the ping to the Hitachi server is successful, name resolution is not likely to be the cause of the issue.
6. If the ping to the Hitachi server fails, append the DNS suffix in the **Advanced TCP/IP settings** or add a host record in the DNS server, mapping this name to the Hitachi server's IP address.

4. The system cannot find the path specified

Cause:

This error occurs when the the Hitachi audit file path configured in ADAudit Plus is incorrect.

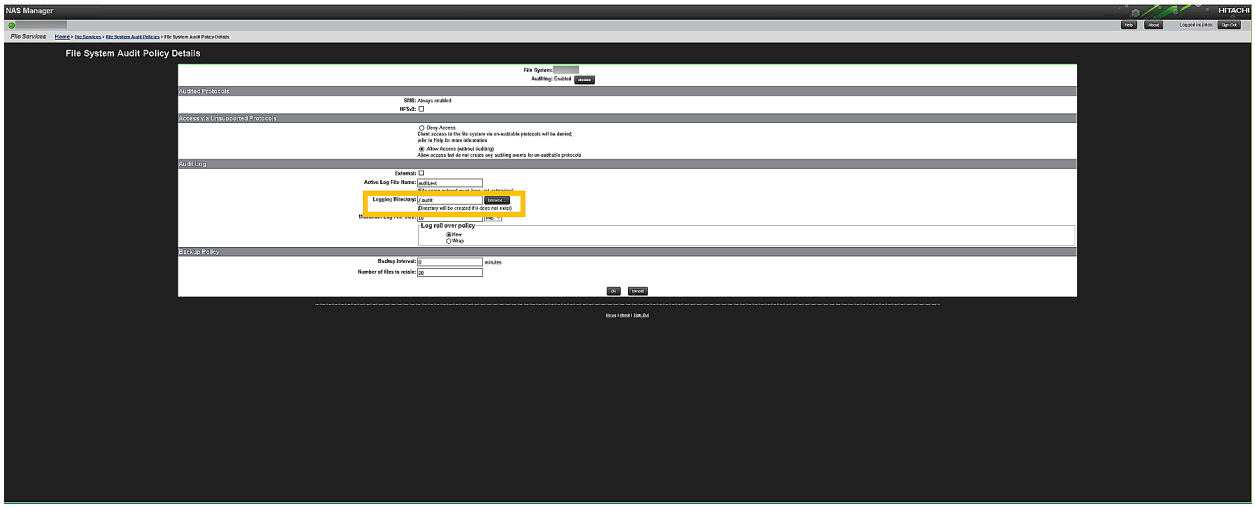
Solutions:

i. Verify if the service account used to run ADAudit Plus has access to the audit files (evt files) in logging directory from the ADAudit Plus server.

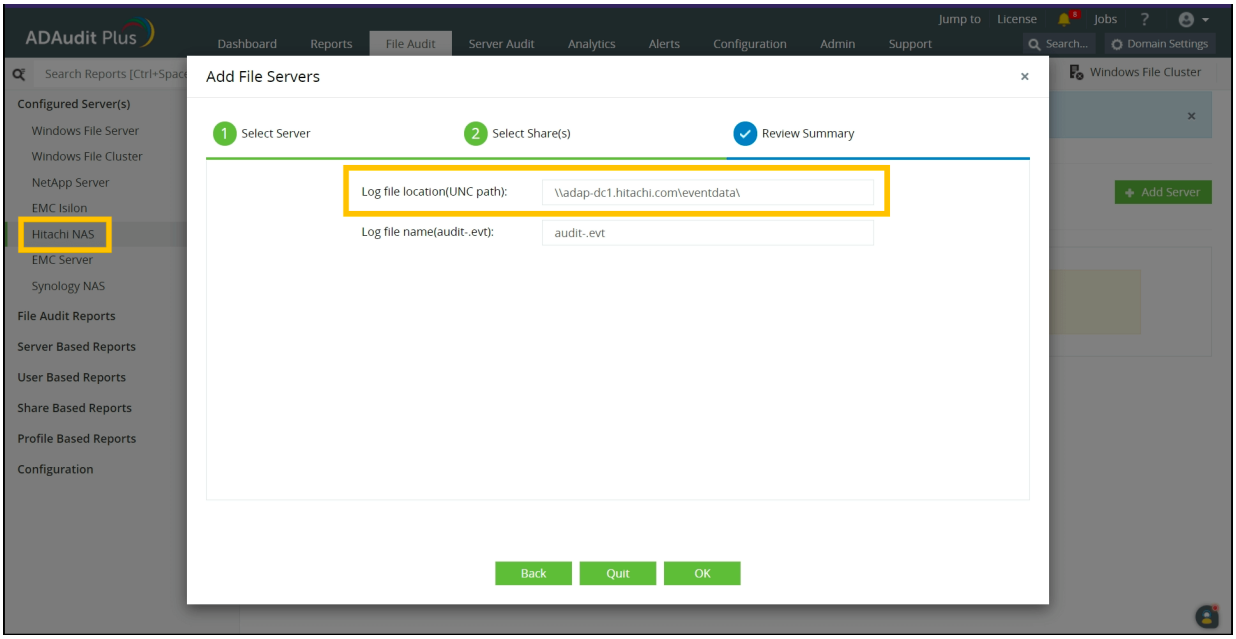
1. Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
2. In the Network window, double click on the target Hitachi server which contains the shared folder.
3. Navigate to the audit file share path **(Logging directory)** as specified in the ADAudit Plus web console **(File Audit > Configured Servers > Hitachi NAS)** during Hitachi file server configuration and double click on the share you want to access.
4. Alternatively, you can run the UNC path to the audit file logging directory and try to access the shares.
5. If you are unable to access the shares on the Hitachi server, the service account used to run ADAudit Plus does not have access to the audit files.

ii. Check the audit file path specified in the Hitachi web console.

1. Open the Hitachi web console.
2. Navigate to **Home > File Services > File System Audit Policies > File System Audit Policy Details.**
3. Note the audit file share path specified in the **Logging Directory** field.



4. Login to your ADAudit Plus web console.
5. Navigate to **File Audit > Configured Servers > Hitachi NAS.**
6. Check if the path to the **audit file share** found in ADAudit Plus web console is the same as the one found in Hitachi web console.



5. The system cannot find the file specified

Cause:

This error occurs when the Hitachi audit files do not exist in the specified location.

Solutions:

Check whether the audit files (evt file shares) exist in the specified location.

1. Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
2. In the Network window, double click on the target Hitachi server which contains the shared folder.
3. Navigate to the audit file logging directory as specified in the Hitachi web console and check whether the audit files exist.
4. Alternatively, you can run the UNC path to the audit file logging directory and check whether the audit files exist.

6. Access denied

Cause:

This error occurs when the service account used to run ADAudit Plus does not have sufficient privileges to read the audit files (evt file shares).

Solutions:

Check whether the Hitachi audit file share location is accessible from ADAudit Plus server.

1. Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
2. In the Network window, double click on the target Hitachi server which contains the shared folder.
3. Navigate to the audit file share path **(Logging directory)** as specified in the Hitachi web console and double click on the share you want to access.
4. Alternatively, you can run the UNC path to the audit file logging directory and try to access the shares.