ManageEngine
ADAudit Plus

Event collection
Troubleshooting

www.adauditplus.com

Table of contents

Overview

ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps secure Active Directory. To resolve the common issues faced during event collection in ADAudit Plus, review these steps. If the issue persists, contact our support team at support@adauditplus.com.

List of errors that occur during event collection:

Domain error codes:

1. No Domain Configuration available
2. The Servers are not operational
3. Unable to get domain DNS / FLAT name
4. What does "Last Event Read Time" in ADAudit Plus mean?

Reports based error codes:

1. No data available
2. Please install GPMC in the computer where ADAudit Plus is installed. After you install GPMC please Click here
3. User does not have admin privilege

General error codes:

1. RPC server unavailable
2. Access Denied
3. Remote Procedure Call Failed
4. Network Access Denied
5. A network adapter hardware error occurred
6. The parameter is incorrect
7. The handle is invalid
8. Not enough memory resources are available to process this command

Netapp filer error codes:

1. Network path not found
2. The system cannot find the file specified

EMC error codes:

1. The system cannot find the path specified

Synology error codes:

1. The system cannot find the path specified/Synology server not found
2. Share not found/Error in getting shares/Access is denied
3. Network port already in use/Problem in adding Syslog Port. Address already in use: Cannot bind
4. Username/Password is Wrong - Error Code:8007052e
5. No event received or timestamp is not updated

Hitachi error codes:

1. The network name cannot be found
2. There are no more files - Error code - 12
3. The network path was not found
4. The system cannot find the path specified
5. The system cannot find the file specified
6. Access denied

Errors while discovering shares:

1. The network path was not found

EMC Isilon error codes:

Refer the EMC Isilon troubleshooting guide.

Errors and solutions

2.1 Domain error codes

1. No Domain Configuration available

Cause:

Post installation, ADAudit Plus automatically discovers the local domain from the DNS server configured on the machine running ADAudit Plus. This error occurs when no domain details are found on the DNS server.

Solution:

Ensure that your domain is listed under **Domain Settings** in ADAudit Plus.

- Login to your ADAudit Plus web console.
- Click **Domain Settings** on the top right corner and check if your domain is added under **Configured Domain(s).**
- If your domain is not added, follow this Active Directory domain configuration guide to add your domain manually.

2. The Servers are not operational

Cause:

Post installation, ADAudit Plus automatically discovers the domain controllers (DC) in the local domain. This error occurs when the domain controllers in the domain are unreachable.

Solution:

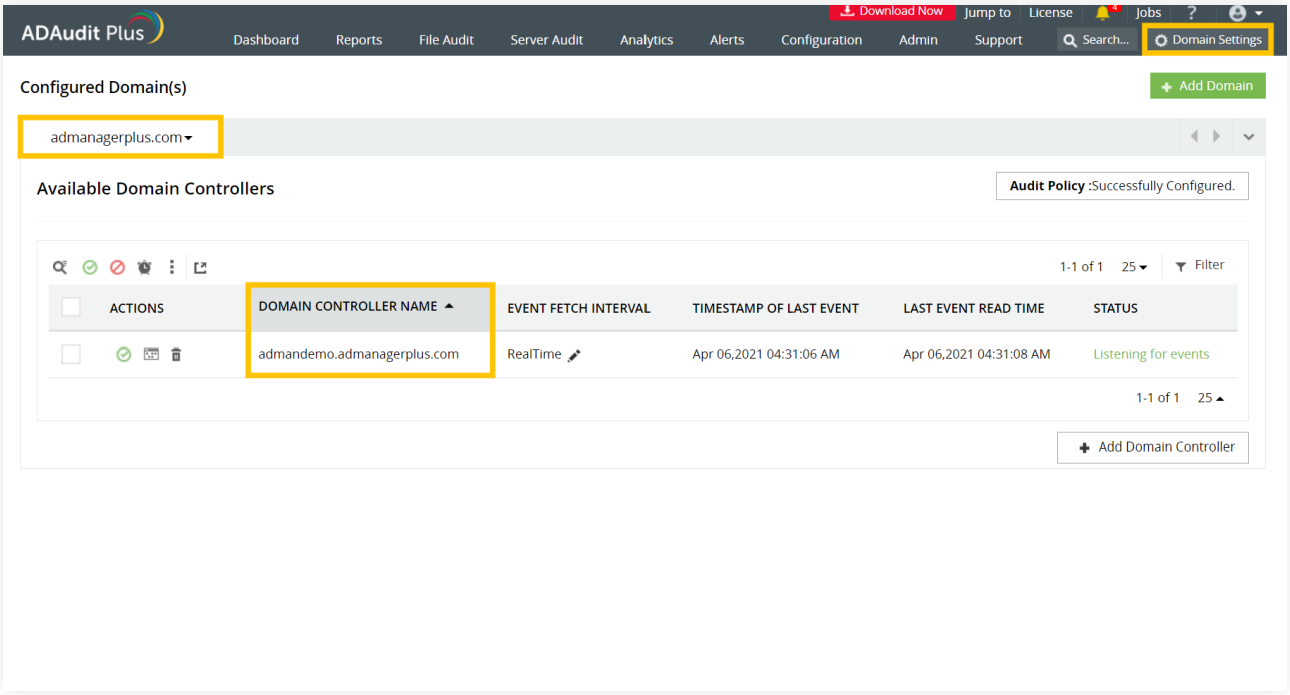
Check if the LDAP port (port no. 389) and RPC ports (static port no.135 and dynamic port no. 49152- 65535) are open to ensure that ADAudit Plus is able to contact the domain controllers in the domain.

- Follow this port guide to open the LDAP and RPC ports required to sync Active Directory objects with ADAudit Plus.

Troubleshooting:

Ping all the DCs added in ADAudit Plus.

- Login to you ADAudit Plus web console.
- Click **Domain Settings** on the top right corner and select your domain under **Configured Domain(s)** to find the available domain controllers.
- Open **Command Prompt** on the ADAudit Plus server and ping the domain controllers listed under **Domain Settings** in ADAudit Plus console by name to check if they are accessible.



3. Unable to get domain DNS / FLAT name

Cause:

While adding a domain, this error occurs when ADAudit Plus in unable to reach the domain.

Solution:

Ping the discovered domain controllers by name from the ADAudit Plus server and try to connect to the Syslog folder to ensure that domain controllers in the domain are accessible.

4. What does "Last Event Read Time" in ADAudit Plus mean?

The "Last Event Read Time" in ADAudit Plus is the last time that ADAudit Plus has contacted the security log of the event viewer and fetched newly logged audit data. The Last Event Read Time changes only if there is fresh and relevant data complying to the audit policy available in the security logs of corresponding computers.

5. How to configure remote servers in ADAudit Plus

Domains that do not have trust with domains configured in ADAudit Plus are considered as remote domains and the servers in those domains are remote servers. You can audit remote servers by following the steps below:

1. Check if you're able to ping the remote server from the ADAudit Plus server. If the ping is successful, you can audit the remote server without any issues.

2. If the ping is unsuccessful, add a DNS entry by following the steps below:

i. Go to the **Ethernet or Wi-Fi** settings in the ADAudit Plus server **(Windows Start > Control Panel > Network and Internet > Network Connections).**

ii. Right-click and select **Properties.**

iii. Click **Internet Protocol Version 4 (TCP/IPv4)** to enable the **Properties** option, and select and continue to the **Advanced...** option.

iv. In the **DNS** tab, add the remote domain's DNS server IP address. Then, select the **Append these DNS suffixes (in order)** option. Click **Add** to enter the **Domain Suffix** of the remote server. Click **OK** to save the setting.

For further queries, reach out to us via support@adauditplus.com.

2.2 Reports based error codes

1. No data available

Cause:

This error occurs when audit policy, or object level auditing, or event log size and retention settings are not configured correctly.

Solution:

1. Verify whether the audit policies are configured on the corresponding servers/domain controllers to ensure that events are logged whenever any activity occurs.

- Follow this active directory auditing guide and check if the audit policy is configured properly for:
- Domain controllers
- Windows servers
- Windows file servers
- Workstations

2. Check whether object level auditing is configured to ensure that events are logged whenever any Active Directory object-related activity occurs.

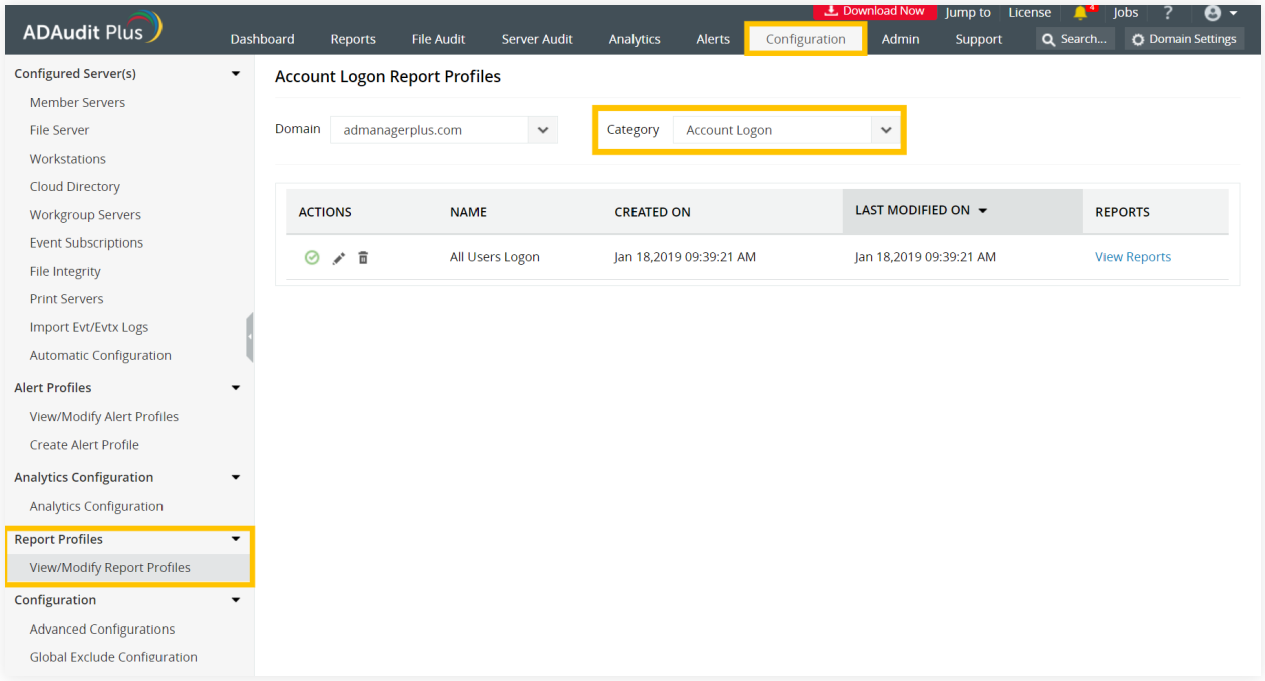
- Follow this object level auditing configuration guide and check if object level auditing is properly configured.

3. Verify whether event log size and retention settings are defined to prevent audit data loss due to events getting overwritten.

- Follow this event log size and retention settings guide to check if they are configured.

Troubleshooting:

1. Check if the report profiles are configured correctly.
   - Login to **ADAudit Plus > Configuration > Report Profiles.**
   - Click **View/Modify Report Profiles** and under each category, verify whether the report profiles are configured correctly.



1. Check whether the target server is configured in ADAudit Plus console.
   - Login to your ADAudit Plus web console.
   - Click **Domain Settings** on the top right corner, and check if the target server is found under **Available Domain Controllers.**
   - If the target server is not listed under Available Domain Controllers, go to the **Server Audit** tab and check if the target server is listed under **Configured Servers.**

2. Try to connect to the target server's Event Viewer from the ADAudit Plus server.
   - Open **Start** on the ADAudit Plus server and search for **Event Viewer.**
   - Right click on **Event Viewer** and click **Run as Administrator.** Enter your admin credentials and click **OK.**
   - In the Event Viewer window, right click on **Event Viewer (Local)** on the top left and select **Connect to Another Computer.**
   - Enter the target server name or IP address in the **Another Computer** field and click **OK.**
   - Once the target server's event viewer is connected, check if events are recorded.

2. Please install GPMC in the computer where ADAudit Plus is installed. After you install GPMC please Click here

Cause:

ADAudit Plus requires Group Policy Management Console (GPMC) to be installed on the machine in which it is running to generate reports on GPO setting changes.

Solution:

Follow this GPMC installation guide to install GPMC on the server running ADAudit Plus.

3. User does not have admin privilege

Cause:

This error occurs when the user account that runs ADAudit Plus does not have sufficient privileges to access the event logs.

Solution:

Follow this service account configuration guide to set-up a service account with minimum privileges required to audit your AD environment.

2.3 General error codes

1. RPC server unavailable

Cause:

This error occurs when the RPC ports (static port no.135 and dynamic port no. 49152- 65535) are not opened in the firewall.

Solution:

Ensure that the RPC ports (static port no.135 and dynamic port no. 49152- 65535*) are open so that ADAudit Plus can collect Windows logs from the monitored computers.
Follow this port guide to open the RPC ports required for Windows log collection.

Note:

If you are using Windows Firewall you can open dynamic ports (49152-65535) on the monitored computers by enabling the inbound rules listed below.

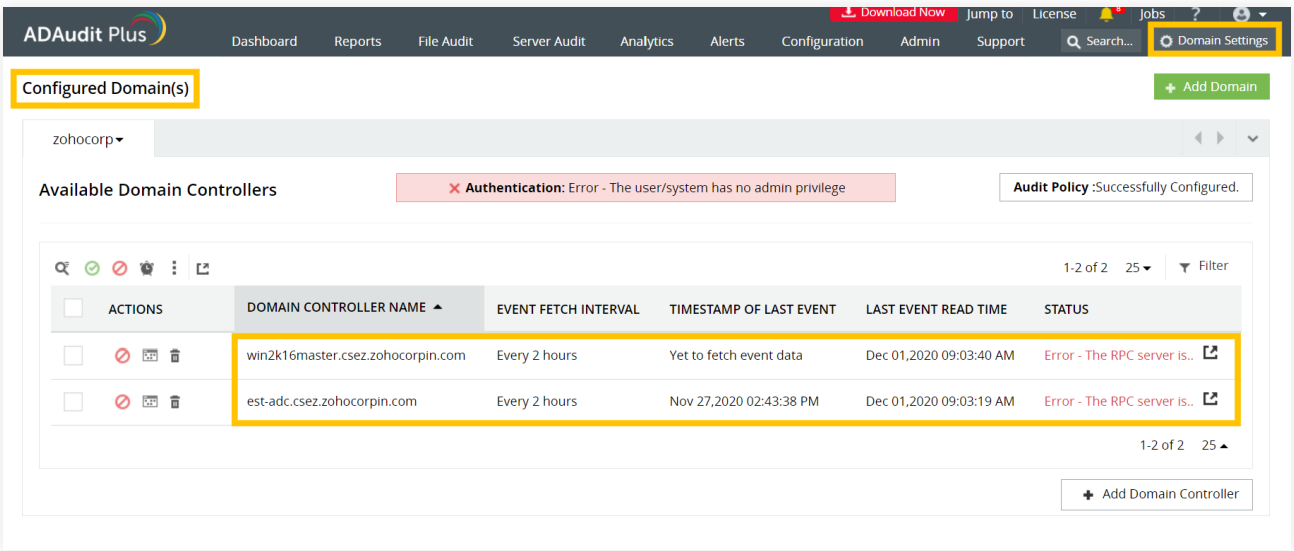
- Remote Event Log Management (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

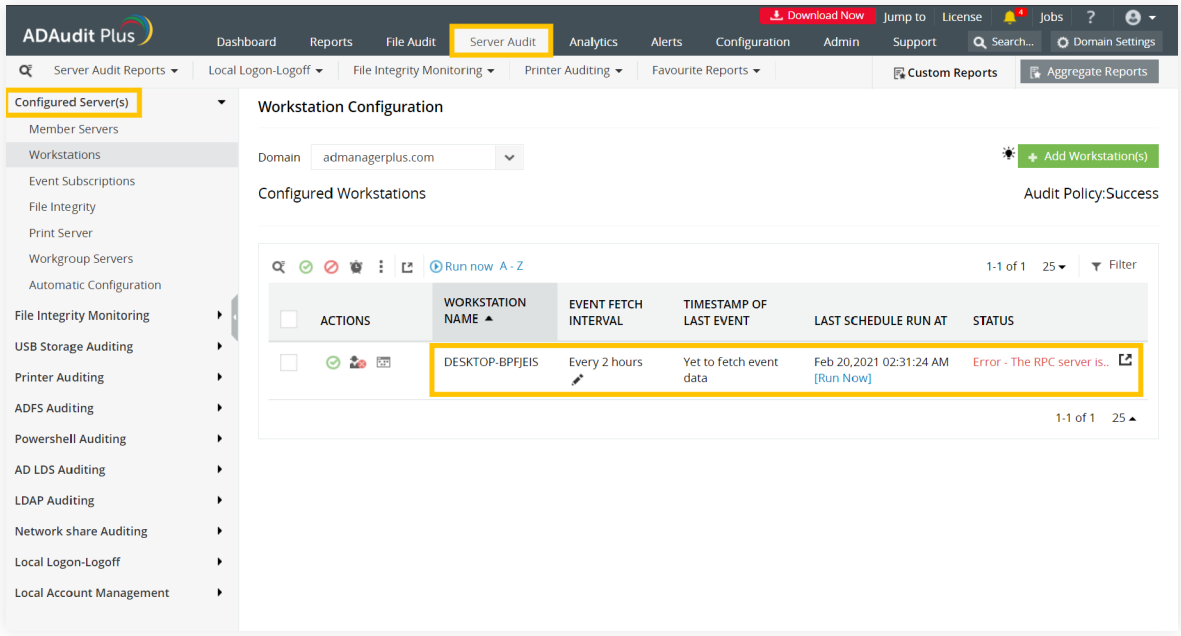
To enable the above rules: Open **Windows Firewall > Advanced settings > Inbound Rules > Right click on respective rule > Enable Rule.**

Troubleshooting:

1. Ping the target server by name from the ADAudit Plus server.

- Login to your ADAudit Plus web console.
- Identify the server showing the RPC error from the **Available Domain Controllers** under **Domain Settings** or under **Configured Server(s)** in the **File Audit** tab or under Configured server(s) in the Server Audit tab.
- Note the flat name of the server as found in ADAudit Plus console as well as its DNS name.
- Open **Command Prompt** in the ADAudit Plus server and ping the target server by its name as noted from ADAudit Plus console to verify that the name resolves to the correct IP address.
- If the ping to the server is successful, name resolution is not likely to be the cause of the issue.
- If the ping to the server fails, try pinging the server by its DNS name; if successful, append the DNS suffix in the **Advanced TCP/IP settings,** or add a host record in the DNS server, mapping this name to the server's IP address.





2. Try to connect to the target server's Event Viewer from the ADAudit Plus server.

- Open **Start** on the ADAudit Plus server and search for **Event Viewer.**
- Right click on **Event Viewer** and click **Run as Administrator.** Enter your admin credentials and click **OK.**
- In the Event Viewer window, right click on **Event Viewer (Local)** on the top left and select **Connect to Another Computer.**
- Enter the target server name or IP address in the **Another Computer** field and click **OK.**
- If you can connect to the target server, check if you are able to access the shares on the target server, next.

3. Try to connect to shares on the target server from the ADAudit Plus server.

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target computer which contains the shared folder.
- Open the shared folder and double click on the share you want to access.
- Alternatively, you can run the UNC path to the shared folder and access the shares.

2. Access Denied

Cause:

This error occurs when the user account that runs ADAudit Plus does not have sufficient privileges to access the event logs.

Solutions:

1. Provide Domain Admin privilege:

ADAudit Plus requires Domain Admin credentials to instantly audit activities in your Active Directory (AD). Ensure that you login to ADAudit Plus with Domain Admin credentials.

2. Set up a service account with minimum privileges:

If you do not want to provide Domain Admin credentials, you need to set up a service account with the least privileges required to audit your AD environment.

- Follow this service account configuration guide to set-up the service account with minimum privileges required for:
- Event log collection
- Automatic auditing and object level auditing configuration
- File server auditing

3. Grant the ADAudit Plus user special privileges to read security logs:

If you have given non-administrators the permission to read event logs, grant the same permissions to the user account that runs ADAudit Plus to access the security logs.

Troubleshooting:

Try to connect to the target server's Event Viewer from the ADAudit Plus server.

- Open **Start** in the ADAudit Plus server and search for **Event Viewer.**
- Right click on **Event Viewer** and click **Run as Administrator**. Enter credentials of the **user account** that runs ADAudit Plus.
- In the Event Viewer window, right click on **Event Viewer (Local)** on the top left and select **Connect to Another Computer.**
- Enter the target computer name or IP address in the **Another Computer** field and click **OK.**
- If you are unable to connect to the target computer, the user account that runs ADAudit Plus does not have sufficient privileges.

3. Remote Procedure Call Failed

Cause:

This error occurs when the RPC ports (static port no.135 and dynamic port no. 49152- 65535*) are not opened in the firewall or when packets are lost due to unstable Wide Area Network (WAN) link.

Solutions:

Ensure that the RPC ports (static port no.135 and dynamic port no. 49152- 65535*) are open so that ADAudit Plus can collect Windows logs from the monitored computers.

- Follow this port guide to open the RPC ports required for Windows log collection.

Note:

If you are using Windows Firewall you can open dynamic ports (49152-65535) on the monitored computers by enabling the inbound rules listed below.

- Remote Event Log Management (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

To enable the above rules: Open **Windows Firewall > Advanced settings > Inbound Rules > Right click on respective rule > Enable Rule.**

Troubleshooting:

1. Ping the target server by name from the ADAudit Plus server.

- Login to your ADAudit Plus web console.
- Identify the server showing the RPC error from the **Available Domain Controllers** under **Domain Settings** or under **Configured Server(s)** in the **File Audit** tab or under **Configured server(s)** in the **Server Audit** tab.
- Note the flat name of the target server as found in ADAudit Plus console as well as its DNS name.
- Open **Command Prompt** in the ADAudit Plus server and ping the target server by its flat name as noted from ADAudit Plus console to verify that the name resolves to the correct IP address.
- If the ping to the server is successful, name resolution is not likely to be the cause of the issue.
- If the ping to the server fails, try pinging the server by its DNS name; if successful, append the DNS suffix in the **Advanced TCP/IP settings** or add a host record in the DNS server, mapping this name to the server's IP address.

2. Try to connect to the target server's Event Viewer from the ADAudit Plus server.

- Open **Start** in the ADAudit Plus server and search for **Event Viewer.**
- Right click on **Event Viewer** and click **Run as Administrator.** Enter credentials with local admin rights on the remote computer you want to access.

3. Try to connect to shares on the target server from the ADAudit Plus server.

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target server which contains the shared folder.
- Open the shared folder and double click on the share you want to access.
- Alternatively, you can run the UNC path to the shared folder and access the shares.

Note:

If the target server and the ADAP server are connected across a WAN connection, we suggest that you install an agent for smoother data collection.

4. Network Access Denied

Cause:

This error occurs when the user account that runs ADAudit Plus does not have sufficient privileges to access the event logs.

Solution:

1. Provide Domain Admin privilege:

ADAudit Plus requires Domain Admin credentials to instantly audit activities in your Active Directory (AD). So, ensure that you login to ADAudit Plus with Domain Admin credentials or set up a service account with minimum privileges.

2. Set up a service account with minimum privileges:

If you do not want to provide Domain Admin credentials, you need to set up a service account with only the least privileges required to audit your AD environment.

- Follow this service account configuration guide to set-up the service account with minimum privileges required for:
- Event log collection
- Automatic auditing and object level auditing configuration
- File server auditing

3. Try to connect to shares on the target server from the ADAudit Plus server.

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target server which contains the shared folder.
- Open the shared folder and double click on the share you want to access.
- Alternatively, you can run the UNC path to the shared folder and access the shares.

Note:

If the target server and the ADAP server are connected across a WAN connection, we suggest that you install an agent for smoother data collection.

5. A network adapter hardware error occurred

Cause:

This error occurs when there are any connectivity issues between the ADAudit Plus server and the target computer.

Troubleshooting:

1. Try to connect to the target computer's Event Viewer from the ADAudit Plus server.
   - Open **Start** in the ADAudit Plus server and search for **Event Viewer.**
   - Right click on **Event Viewer** and click **Run as Administrator.** Enter credentials with local admin rights on the remote computer you want to access.
   - In the Event Viewer window, right click on **Event Viewer (Local)** on the top left and select **Connect to Another Computer.**
   - Enter the target computer name or IP address in the **Another Computer** field and click **OK.**
   - If you can connect to the target server, check if you are able to access the shares on the target server, next.

2. Try to connect to shares on the target computer from the ADAudit Plus server.
   - Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
   - In the Network window, double click on the target computer which contains the shared folder.
   - Open the shared folder and double click on the share you want to access.
   - Alternatively, you can run the UNC path to the shared folder and access the shares.

6. The parameter is incorrect

Cause:

This error occurs as a result of events getting overwritten before ADAudit Plus could read them due to insufficient log size. Reading the event logs across Wide Area Network (WAN) connections can also lead to this error.

Solution:

1. Verify whether event log size and retention settings are defined to prevent audit data loss due to events getting overwritten.

- Follow this event log size and retention settings guide to check if they are configured.

2. In case you have a large network that operates across WAN connections, deploy a client-side agent for smoother data collection and lower bandwidth utilization.

- Follow this agent configuration guide to:
- Install agent via ADAudit Plus UI
- Install agent manually

7. The handle is invalid

Cause:

This error occurs as a result of events getting overwritten before ADAudit Plus could read them due to insufficient log size. Reading the event logs across Wide Area Network (WAN) connections can also lead to this error.

Solution:

1. Verify whether event log size and retention settings are defined to prevent audit data loss due to events getting overwritten.

- Follow this event log size and retention settings guide to check if they are configured.

2. In case you have a large network that operates across WAN connections, deploy a client-side agent for smoother data collection and lower bandwidth utilization.

- Follow this agent configuration guide to:
- Install agent via ADAudit Plus UI
- Install agent manually

8. Not enough memory resources are available to process this command

Cause:

This error occurs if the RAM size is low on the target computer.

2.4 Netapp filer error codes

1. Network path not found

Cause:

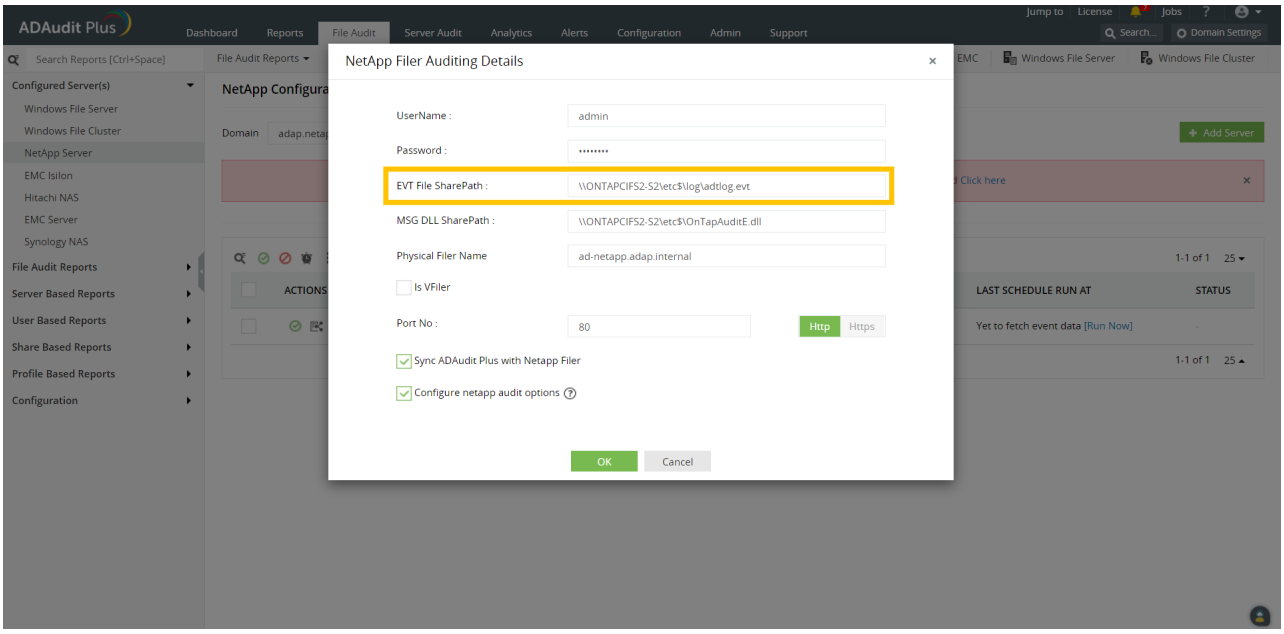
This error occurs when ADAudit Plus is unable to contact the Netapp server.

Solution:

Ensure that there are no connectivity issues between the ADAudit Plus server and the target Netapp server.

Troubleshooting:

1. Try to connect to the audit files (evt file shares) on the Netapp server:
   - Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
   - In the Network window, double click on the target Netapp server which contains the shared folder.
   - Navigate to the **Netapp audit location** and try to access the audit files (evt file shares). Alternatively, you can run the UNC path to the Netapp audit location and try to access the shares.
   - If you are able to access the shares, check if you can ping the Netapp server.



2. Ping the Netapp server by name from the ADAudit Plus server.

- Login to your ADAudit Plus web console.
- Navigate to **File Audit > Configured Servers > Netapp Server** and select your domain.
- Identify and note the name of the Netapp server showing the error.
- Open **Command Prompt** in the ADAudit Plus server and ping the Netapp server by its name as notedfrom ADAudit Plus console to verify that the name resolves to the correct IP address.
- If the ping to the Netapp server is successful, name resolution is not likely to be the cause of the issue.
- If the ping to the Netapp 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 Netapp server's IP address.

2. The system cannot find the file specified

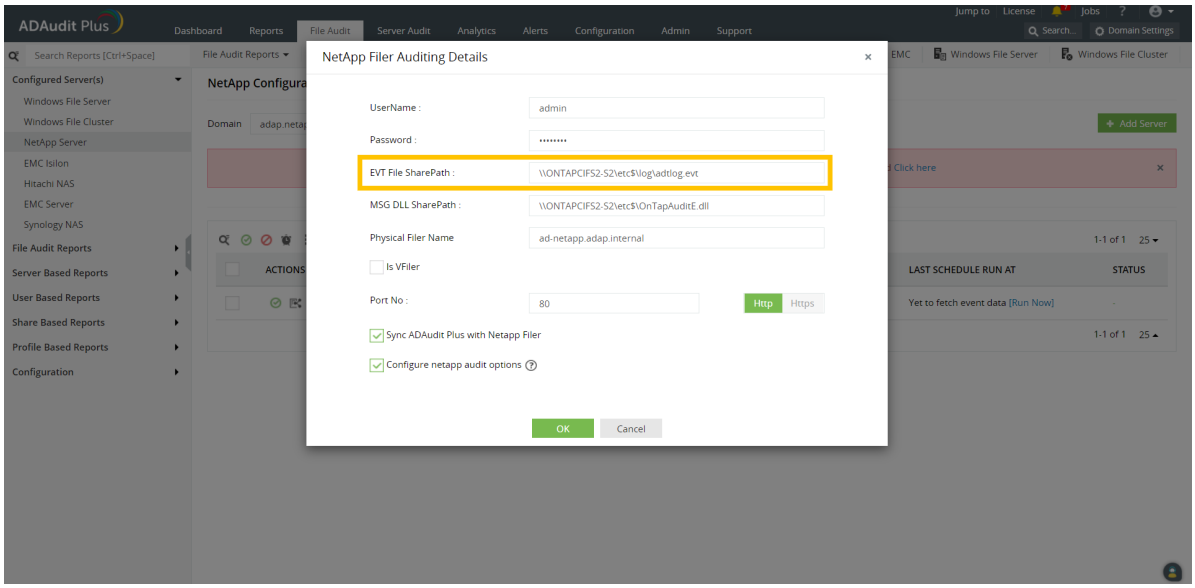
Cause:

This error occurs when ADAudit Plus is unable to locate the audit files on the Netapp server.

Troubleshooting:

1. Check if the audit files (evt files) exist in the Netapp audit location.

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target Netapp server.
- Navigate to the **Netapp audit location** and check if the audit files exist. Alternatively, you can run the UNC path to the Netapp audit location and check if the audit files exist.



2. Verify if the audit policies are configured on the Netapp server to ensure that events are logged whenever any activity occurs.

- Follow this audit policy configuration guide and check if the audit policy is configured properly.

2.5 EMC error codes

1. The system cannot find the path specified

Cause:

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

Solution:

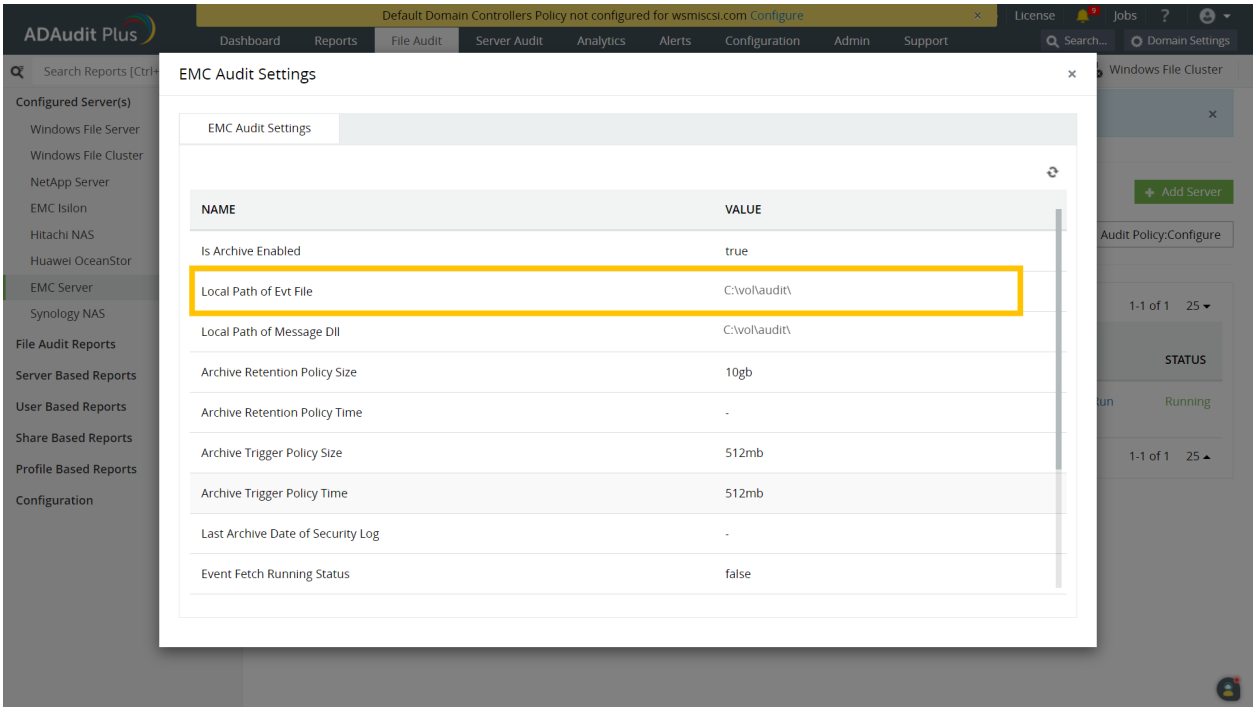
Check whether audit policies are configured on the EMC server to ensure that events are logged whenever any activity occurs.

- Follow this audit policy configuration guide and check if the audit policy is configured properly.

Troubleshooting:

Check if the audit files (evt files) exist in the EMC audit location.

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target EMC server which contains the shared folder.
- Navigate to the **EMC audit location** as specified in ADAudit Plus console and check if the files exist. Alternatively, you can run the UNC path to the EMC audit location and check if the files exist.
- If the audit location does not contain the audit files, locate the audit files on the EMC server and update the EMC audit location in ADAudit Plus.



Note:

EMC audit location is the UNC path of the audit folder shown in the image.

2.6 Synology error codes

1. The system cannot find the path specified/Synology server not found

Cause:

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

Solution:

Verify that the server is part of the selected domain and is accessible.

Troubleshooting:

Ping the Synology server by name from the ADAudit Plus server.

- Login to your ADAudit Plus web console.
- Navigate to **File Audit > Configured Servers > Synology NAS** and select your domain.
- Identify and note the name of the Synology server showing the error.

2. Share not found/Error in getting shares/Access is denied

Cause:

This error occurs when ADAudit Plus in unable to contact the Synology server or when the user account that runs ADAudit Plus does not have sufficient privileges to access the audit files (evt file shares) on the Synology server.

Solution:

Verify that the Synology server is accessible and ensure that the user account used to run ADAudit Plus has sufficient privileges to access the audit files.

Troubleshooting:

Ping the Synology server by name from the ADAudit Plus server.

- Login to your ADAudit Plus web console.
- Navigate to **File Audit > Configured Servers > Synology NAS** and select your domain.
- Identify and note the name of the Synology server showing the error.
- Open **Command Prompt** in the ADAudit Plus server and ping the Synology server by its name as noted from ADAudit Plus console to verify that the name resolves to the correct IP address.
- If the ping to the Synology server is successful, name resolution is not likely to be the cause of the issue. Ensure that the user account has sufficient privileges to access the audit files.
- If the ping to the Synology 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 Synology server's IP address.

3. Network port already in use/Problem in adding Syslog Port. Address already in use: Cannot bind

Cause:

This error occurs when the syslog port which is configured in ADAudit Plus is being used by another process.

Solution:

Verify that the syslog port which is configured in ADAudit Plus is not being used by another process.

4. Username/Password is Wrong - Error Code:8007052e

Cause:

This error occurs when the username or password entered is wrong.

Solution:

Check the server name, username and password.

5. No event received or timestamp is not updated

Cause:

This error occurs when no events are received by ADAudit Plus from the Synology server.

Solution:

Verify whether the forwarded syslog data is received by the ADAudit Plus server by installing ManageEngine Free Syslog Forwarder.

- Login to your ADAudit Plus web console.
- Navigate to **Admin > General Settings > Connection,** and set **Current Syslog Status** to **Off.** Alternatively, you can stop the ADAudit Plus Service.
- In the free syslog forwarder tool, click **Start** to receive syslog data.
- If no data is shown, check the syslog configuration settings by following this Synology configuration guide.

2.7 Hitachi error codes

1. The network name cannot be found

Cause:

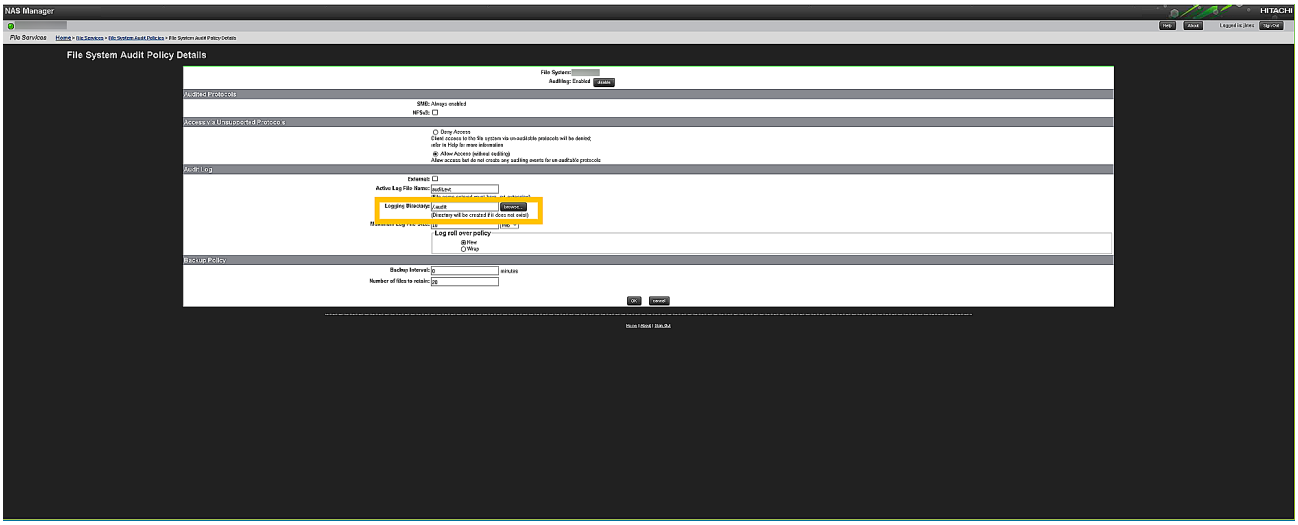
This error occurs when the DNS server is not reachable or if the Hitachi server's name is not registered in the DNS.

Troubleshooting:

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

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target Hitachi server.

- 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.
- If you are able to access the shares on the target Hitachi server, ping the Hitachi server.



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

- Login to your ADAudit Plus web console.
- Navigate to **File Audit > Configured Servers > Hitachi NAS.**
- Select your domain and note the name of the Hitachi server as found in ADAudit Plus console.
- 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.
- If the ping to the Hitachi server is successful, name resolution is not likely to be the cause of the issue.
- 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

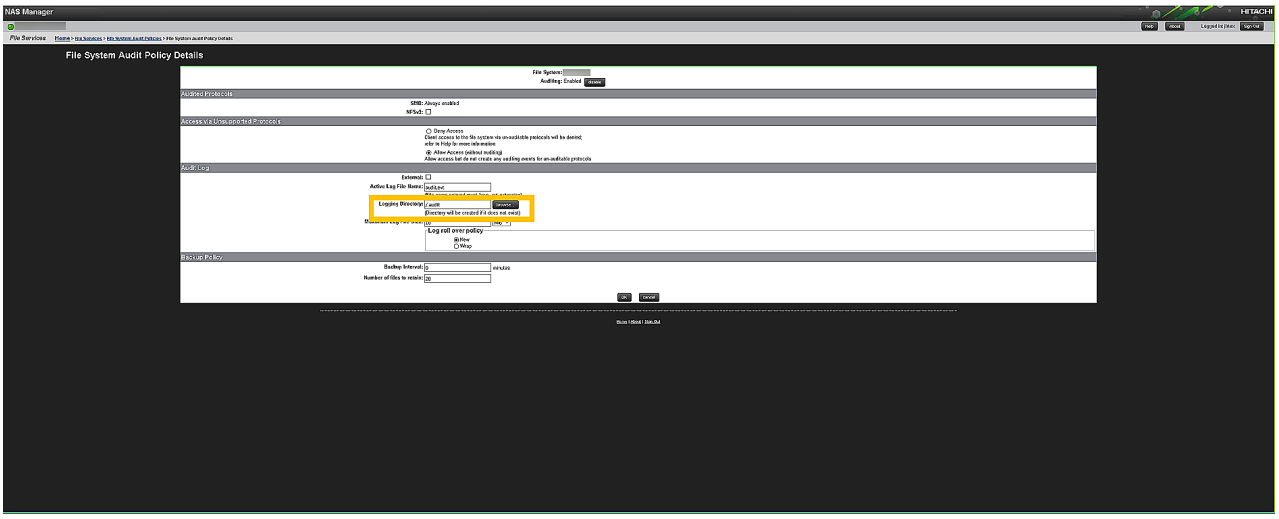
Cause:

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

Troubleshooting:

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

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target Hitachi server which contains the shared folder.
- 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.
- If you are able to access the shares on the target Hitachi server, ping the Hitachi server.



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

- Login to your ADAudit Plus web console.
- Navigate to **File Audit > Configured Servers > Hitachi NAS** and select your domain.
- Identify and note the name of the Hitachi server showing the error.
- 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.
- If the ping to the Hitachi server is successful, name resolution is not likely to be the cause of the issue.
- 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.

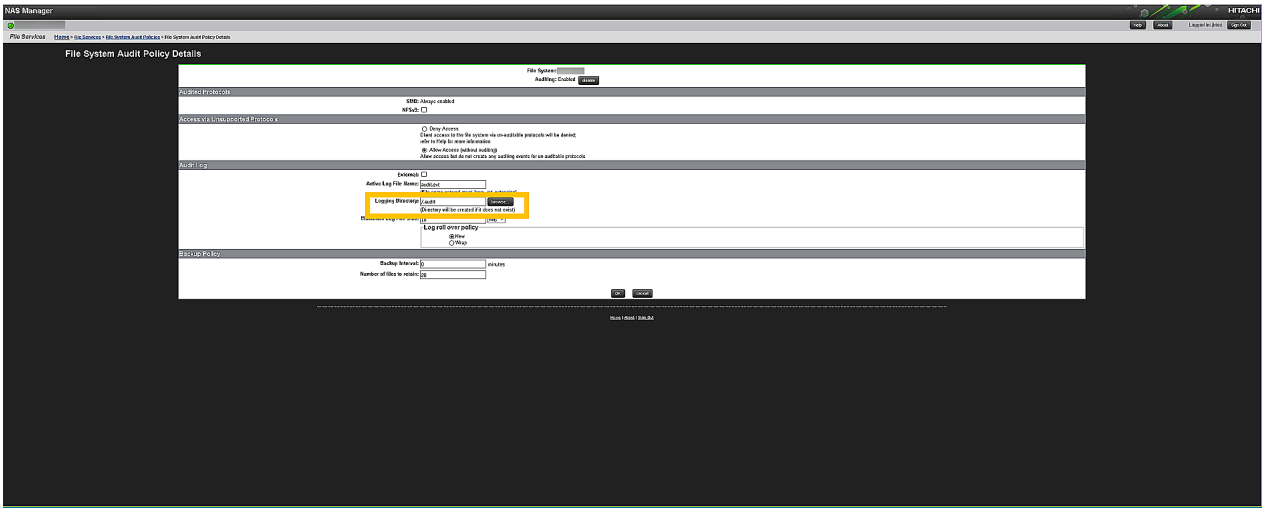
Solution:

1. 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.

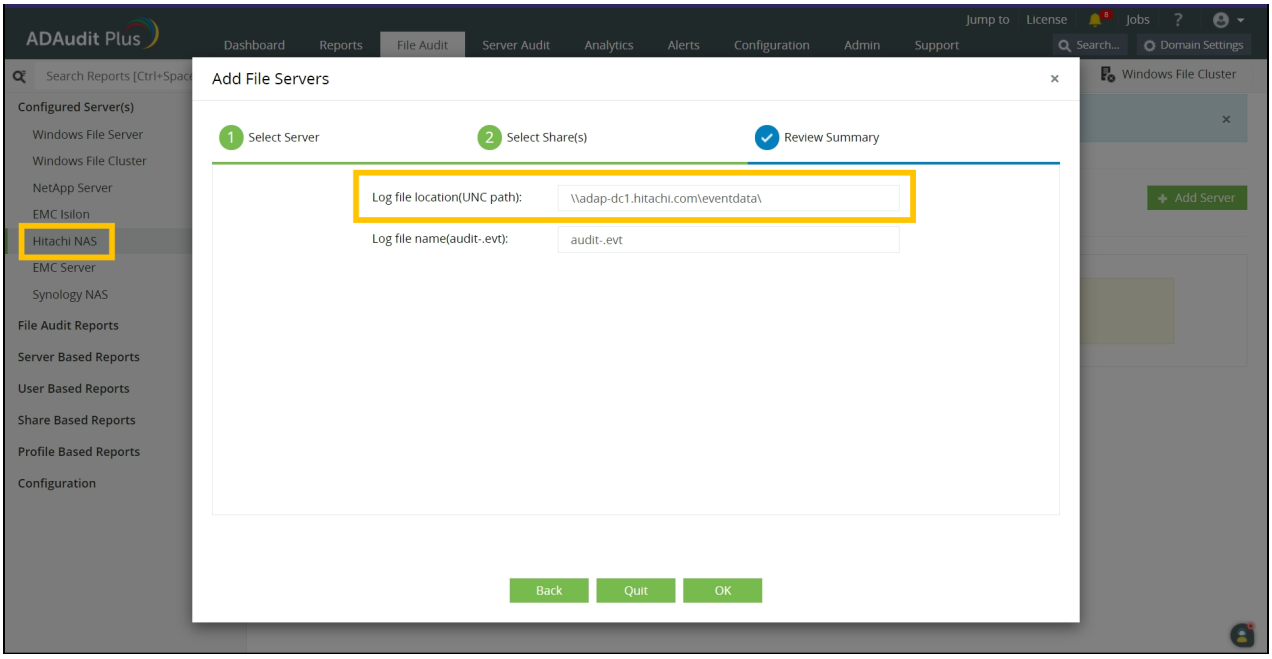
- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target Hitachi server which contains the shared folder.
- Navigate to the audit file share path **(Logging directory)** as specified in the ADAudit Plus web console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

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

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



- Login to your ADAudit Plus web console.
- Navigate to **File Audit > Configured Servers > Hitachi NAS.**
- 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.

Solution:

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

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target Hitachi server which contains the shared folder.
- Navigate to the audit file logging directory as specified in the Hitachi web console and check whether the audit files exist.
- 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).

Solution:

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

- Open **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
- In the Network window, double click on the target Hitachi server which contains the shared folder.
- 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.
- Alternatively, you can run the UNC path to the audit file logging directory and try to access the shares.

2.8 Errors while discovering file shares

1. The network path was not found

Cause:

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

Solution:

Ensure that there are no connectivity issues between the ADAudit Plus server and the target computer.

Troubleshooting:

1. Connect to the target computer's Event Viewer from the ADAudit Plus server.
   - Open **Start** in the ADAudit Plus server and search for **Event Viewer.**
   - Right click on **Event Viewer** and click **Run as Administrator.** Enter admin credentials and click **OK.**
   - In the Event Viewer window, right click on **Event Viewer (Local)** on the top left and select **Connect to Another Computer.**
   - Enter the remote computer name or IP address in the **Another Computer** field and click **OK.**
   - If you are able to connect to the target computer, try connecting to the shares.

2. Connect to shares on the target computer by following the steps below:
   - Click the **File Explorer** in the ADAudit Plus server and select **Network** from the left tree.
   - In the Network window, double click on the target computer which contains the shared folder.
   - Open the shared folder and double click on the share you want to access. Alternatively, you can run the UNC path to the shared folder and try to access the shares.