

NetApp Filer Auditing Guide



Table of Contents

1. Overview	1
2. Adding NetApp 7Mode/vFiler CIFS server	1
3. Configure audit policies	7
Automatic configuration	7
Manual configuration	8
4. Configure object-level auditing	9
Automatic configuration	9
Manual configuration	11
5. Exclude configuration	13
6. Troubleshooting	15

1. Overview of NetApp filer auditing

NetApp filer network-attached storage (NAS) devices, also known as NetApp fabric-attached storage (FAS), are storage systems that use NetApp's proprietary operating system, ONTAP. A vFiler unit is a partition of a storage system and the associated network resources. Each vFiler partition appears to the user as a separate storage system on the network, and functions as a storage system.

ManageEngine ADAudit Plus, a user behavior analytics (UBA)-driven change auditor, provides real-time visibility into your NetApp 7Mode/vFiler CIFS servers. It delivers detailed reports on user activity in NetApp files and shares, analyzes permission changes, and automates instant responses to security incidents. It also streamlines compliance with numerous regulations such as HIPAA, FISMA, GDPR, SOX, CCPA, and more.

Supported versions

ADAudit Plus can monitor these ONTAP versions:

NetApp ONTAP 7.2 and above

Audited events

ADAudit Plus audits every attempt to perform these file activities in NetApp filers:

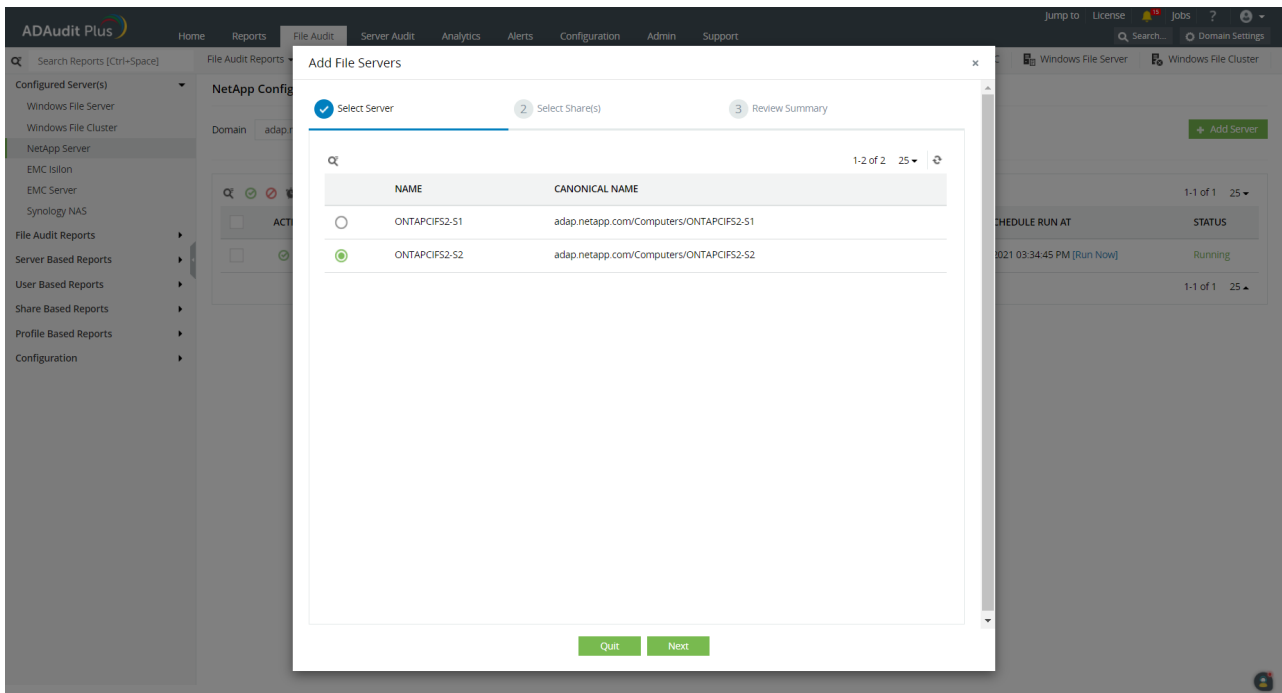
- Create
- Read
- Modify
- Write
- Delete
- Change file permissions
- Rename
- Move

This guide provides steps to configure change auditing in your NetApp 7Mode/vFiler CIFS servers using ADAudit Plus.

2. Adding NetApp 7Mode/vFilers in ADAudit Plus

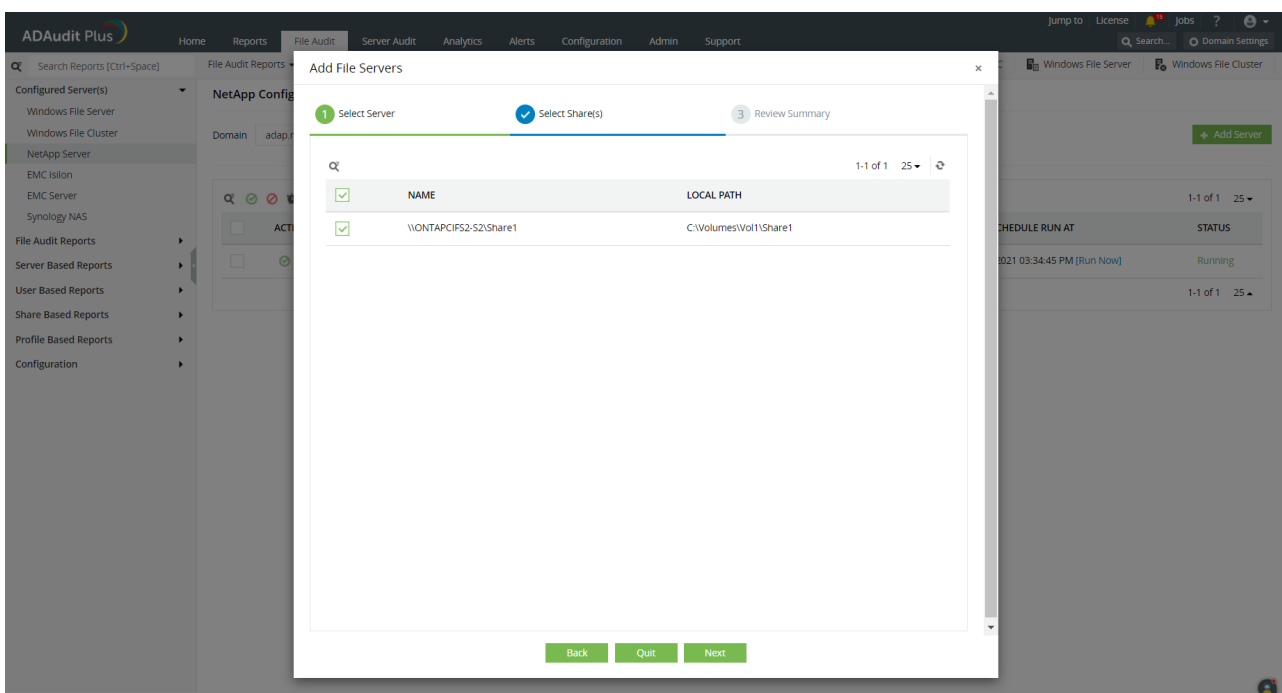
To add your target NetApp filers to your ADAudit Plus console, follow these steps:

1. Log in to the ADAudit Plus web console.
2. Navigate to the **File Audit** tab > **Configured Server(s)** > **NetApp Server**. 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.

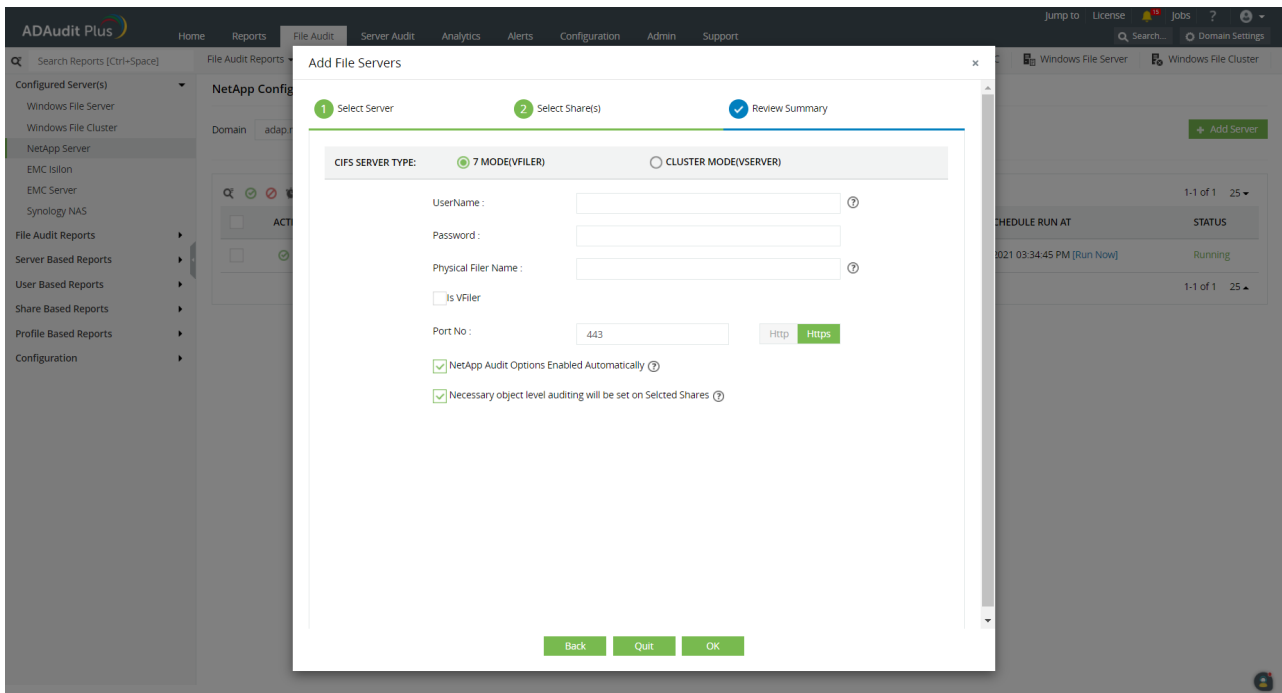


4. Select the target server and click **Next**.

5. From the listed shares, select the ones you wish to audit and click **Next**.



6. Choose your CIFS server type, in this case, **7Mode (vFiler)**.



7. Provide these details:

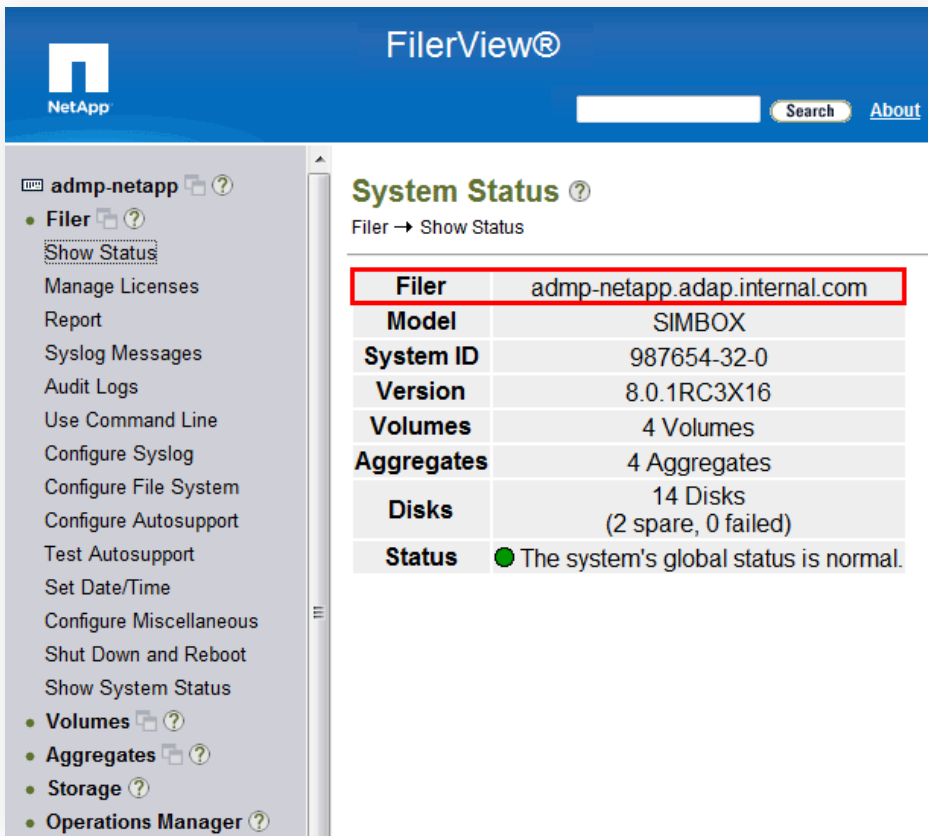
- **Username:** A NetApp account with administrative permissions, such as **login-http-admin**, **api-system-cli**, **api-options-get**, or **cli-cifs**, will set the NetApp audit options and also help in the manual generation of audit log (EVT) files.

```

admp-netapp> useradmin user list root
Name: root
Info: Default system administrator.
Rid: 0
Groups:
Full Name:
Allowed Capabilities: login-http-admin, api-system-cli, api-options-get, cli-cifs
Password min/max age in days: 0/never
Status: enabled
admp-netapp>

```

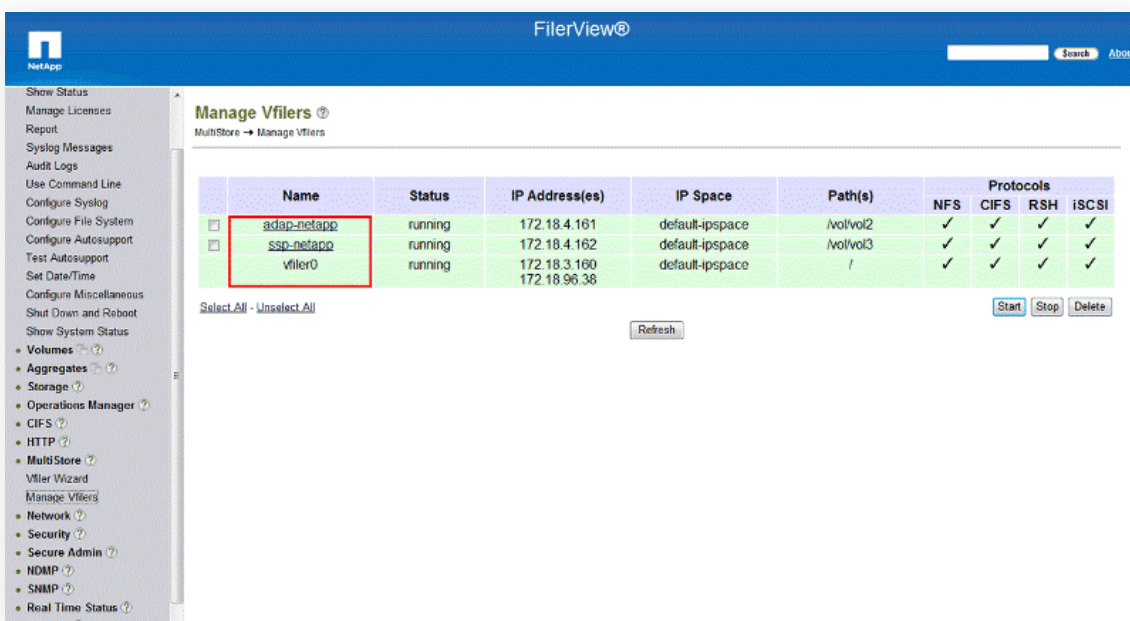
- **Password:** The password of the chosen NetApp user account.
- **Physical Filer Name:** The name of the target storage systems running Data ONTAP or the storage system on which vFiler units are created.



System Status ?
Filer → Show Status

Filer	admp-netapp.adap.internal.com
Model	SIMBOX
System ID	987654-32-0
Version	8.0.1RC3X16
Volumes	4 Volumes
Aggregates	4 Aggregates
Disks	14 Disks (2 spare, 0 failed)
Status	● The system's global status is normal.

- **Is vFiler:** If the selected CIFS Server is on a vFiler, check the **Is vFiler** box.
- **vFiler Name:** Provide the name of the vFiler unit, a storage partition. The partition can be created using the [NetApp MultiStore](#) feature.



Manage Vfilers ?
MultiStore → Manage Vfilers

	Name	Status	IP Address(es)	IP Space	Path(s)	NFS	CIFS	RSH	iSCSI
<input type="checkbox"/>	adap-netapp	running	172.18.4.161	default-ipspace	/vol/vol2	✓	✓	✓	✓
<input type="checkbox"/>	ssp-netapp	running	172.18.4.162	default-ipspace	/vol/vol3	✓	✓	✓	✓
	vfiler0	running	172.18.3.160 172.18.96.38	default-ipspace	/	✓	✓	✓	✓

Select All - Unselect All Start Stop Delete
Refresh

- **Port number and protocol:** Provide the number of the port that will be used for HTTP or HTTPS communication between the vFiler and the ADAudit Plus server. By default, this will be 80 for HTTP connections and 443 for HTTPS connections. Either HTTP or SSL must be enabled for ADAudit Plus to connect to the NetApp Filer, and to set the audit options automatically.

```
login as: root
root@admp-netapp's password:

admp-netapp> options httpd
httpd.access                legacy
httpd.admin.access         legacy
httpd.admin.enable         on
httpd.admin.hostsequiv.enable off
httpd.admin.max connections 512
httpd.admin.ssl.enable     on
httpd.admin.top-page.authentication on
httpd.autoindex.enable     off
httpd.bypass_traverse_checking off
httpd.enable               on
httpd.log.format           common
httpd.method.trace.enable  off
httpd.rootdir              XXX
httpd.timeout              300
httpd.timewait.enable      off
admp-netapp>
```

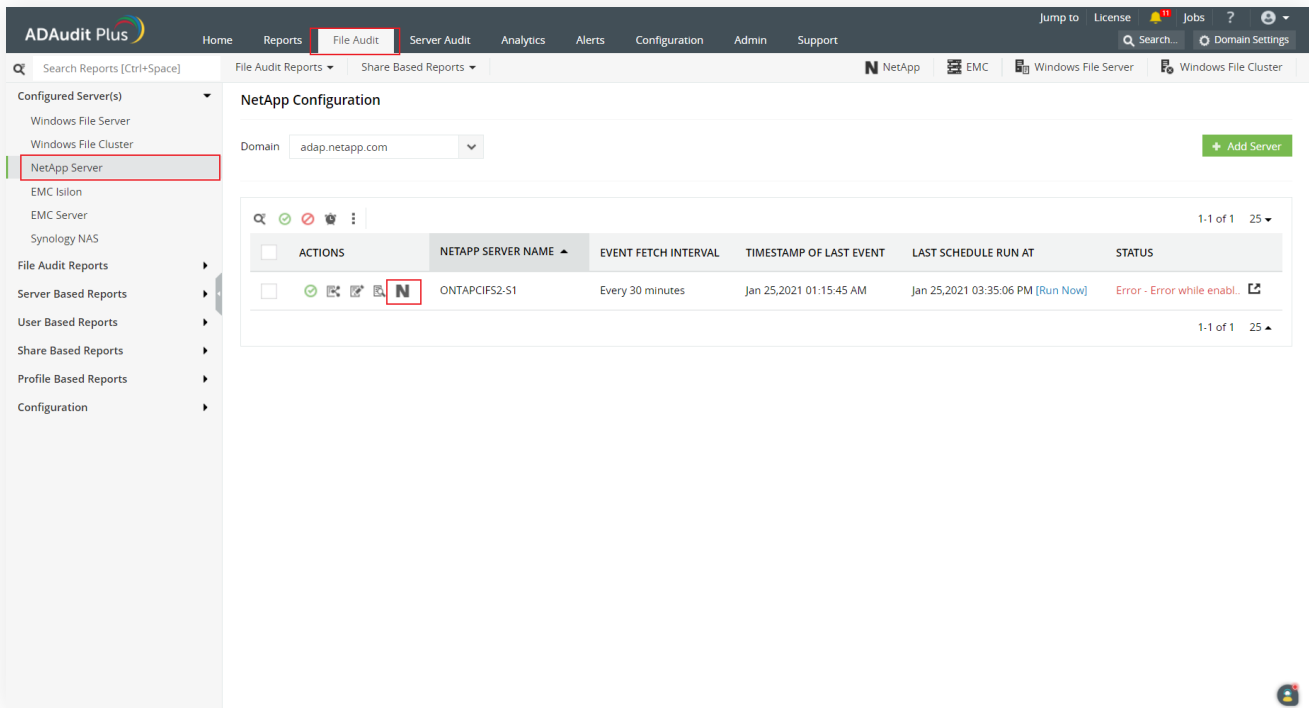
Note: If you want ADAudit Plus to auto-configure the required audit policies and object-level auditing (SACL) in the target shares, ensure that the **NetApp Audit Options Enabled Automatically** and **Necessary object level auditing will be set on Selected Shares** checkboxes are selected. Otherwise, deselect the checkboxes and proceed with the next step. You will need to manually configure the audit policies and SACLs on the target shares to ensure that the system generates audit events when files are accessed.

8. Click **OK**.

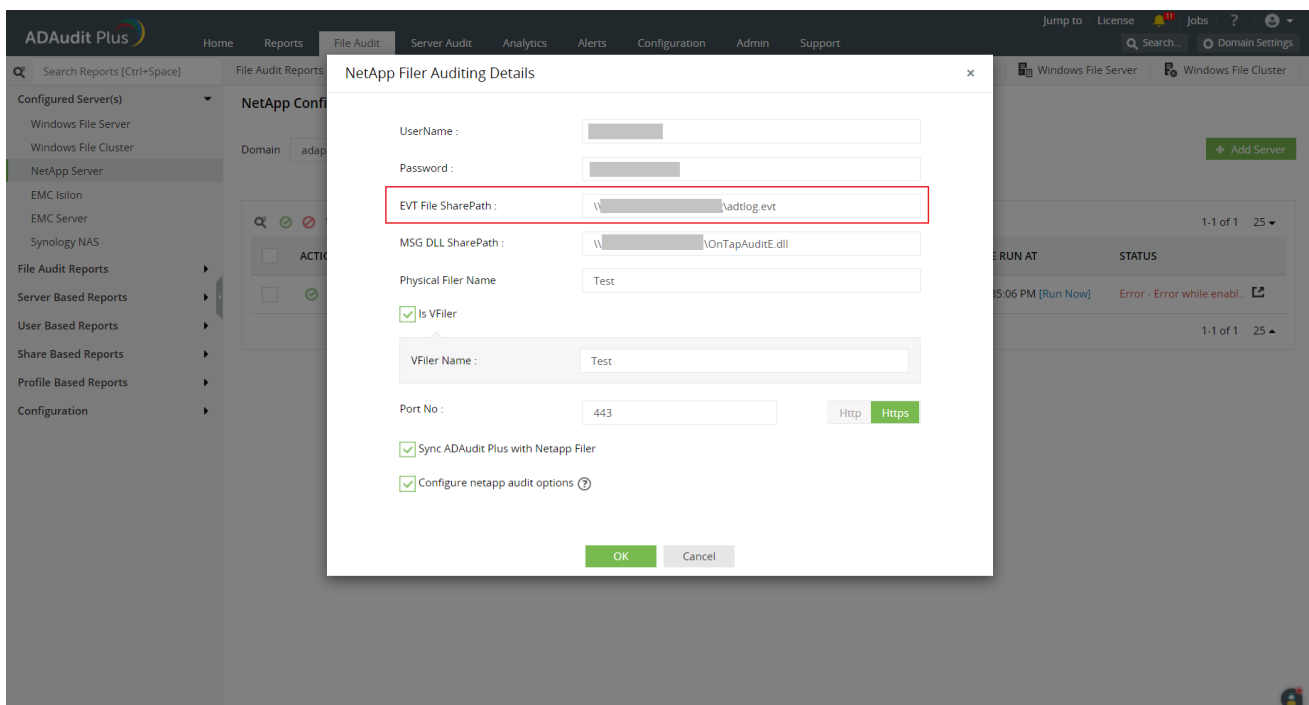
Your target NetApp server will be added to the ADAudit Plus console.

Then, to view or update the EVT file share path, follow these steps:

1. On the ADAudit Plus web console, navigate to the **File Audit** tab > **Configured Server(s)** > **NetApp Server**.
2. From the **Domain** drop-down, select the domain with the target server. All the servers configured in that domain will be displayed in the table.
3. Under Actions, click the icon for **NetApp Audit Options Configuration**.



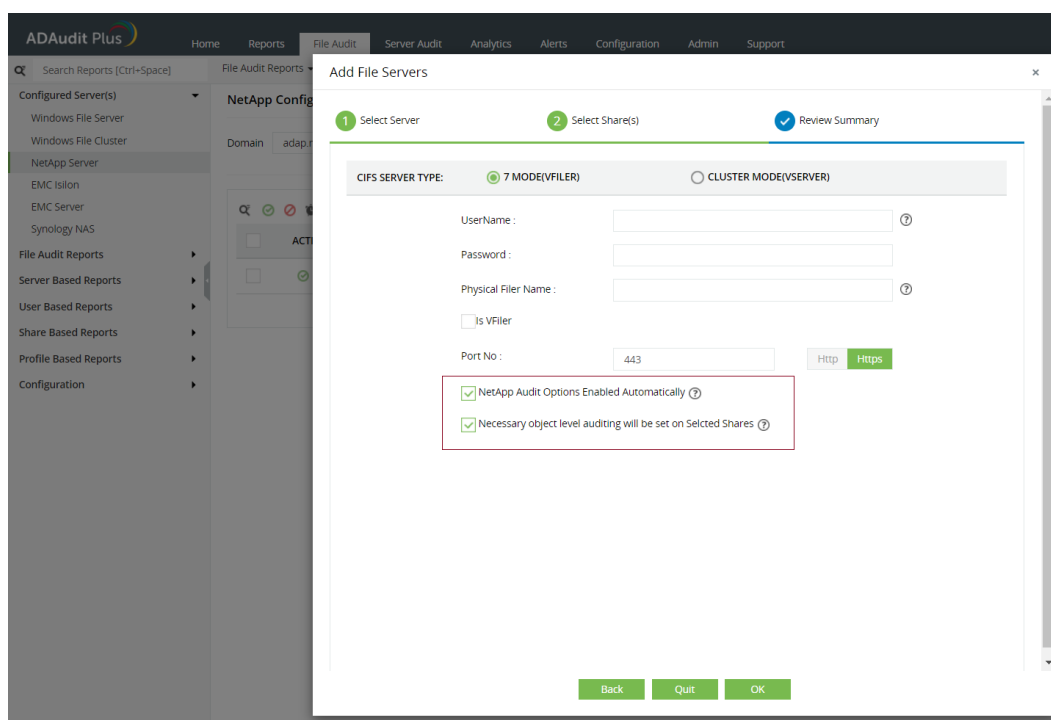
4. In the resulting **NetApp Filer Auditing Details** pop-up, you can view or edit the configure username and password, the default EVT file share path, the MSG DLL share path, the port number, protocol, and other details.



3. Configuring Audit Policies in NetApp 7-Mode CIFS server/vFilers

3.1 Automatic configuration

To allow ADAudit Plus to enable the required NetApp audit policies automatically, ensure that the box next to **NetApp Audit Options Enabled Automatically** is checked while adding your target NetApp filer. Then, click **OK**.



```
admp-netapp> options cifs.audit
cifs.audit.account_mgmt_events.enable off
cifs.audit.autosave.file.extension timestamp
cifs.audit.autosave.file.limit 10
cifs.audit.autosave.onsize.enable on
cifs.audit.autosave.onsize.threshold 100%
cifs.audit.autosave.ontime.enable off
cifs.audit.autosave.ontime.interval 5h
cifs.audit.enable on
cifs.audit.file_access_events.enable on
cifs.audit.liveview.allowed_users
cifs.audit.liveview.enable off
cifs.audit.logon_events.enable off
cifs.audit.logsize 268435456
cifs.audit.nfs.enable off
cifs.audit.nfs.filter.filename
cifs.audit.saveas /etc/log/adtlog.evt
admp-netapp>
```

To configure object-level auditing automatically, ensure that the box next to **Necessary object level auditing will be set on Selected Shares** is checked. Alternatively, you can follow the manual configuration steps in the next section.

3.2 Manual configuration

This section details the procedure to configure the required NetApp audit policies manually in your target vFilers.

Audit policies must be configured to ensure that events are logged whenever any activity occurs in your NetApp filers. They are set via the NetApp Filer command prompt, which is accessible through an SSH/Telnet connection.

To configure the audit policies, connect to the filer via SSH and execute these basic commands:

- To get an option value:
options < option_name >
- To set the option value:
options < option_name > < option_value >

For example, to enable the `cifs.audit.enable` option, execute the following command:

```
options cifs.audit.enable on
```

Note: For a full list of commands along with their descriptions, refer to this [NetApp document](#).

Execute the commands below to specify when automatic saves occur, the maximum number of automatically-saved files, and other prerequisites. These audit options have to be enabled in the NetApp filer via SSH to generate the required file audit events and automatically capture them as EVT files.

- `options cifs.audit.account_mgmt_events.enable off`
- `options cifs.audit.logon_events.enable off`
- `options cifs.audit.liveview.enable off`
- `options cifs.audit.enable on`
- `options cifs.audit.file_access_events.enable on`
- `options cifs.audit.autosave.file.extension timestamp`
- `options cifs.audit.autosave.file.limit 10`
- `options cifs.audit.autosave.onsize.enable on`
- `options cifs.audit.autosave.onsize.threshold 100%`
- `options cifs.audit.autosave.ontime.enable off`
- `options cifs.audit.logsize 268435456`

Further, you must disable the **`cifs.audit.liveview.enable`** option since it interferes with ADAudit Plus's processing of the collected audit data.

```
admp-netapp> options cifs.audit
cifs.audit.account_mgmt_events.enable off
cifs.audit.autosave.file.extension timestamp
cifs.audit.autosave.file.limit 10
cifs.audit.autosave.onsize.enable on
cifs.audit.autosave.onsize.threshold 100%
cifs.audit.autosave.ontime.enable off
cifs.audit.autosave.ontime.interval 5h
cifs.audit.enable on
cifs.audit.file_access_events.enable on
cifs.audit.liveview.allowed_users
cifs.audit.liveview.enable off
cifs.audit.logon_events.enable off
cifs.audit.logsize 268435456
cifs.audit.nfs.enable off
cifs.audit.nfs.filter.filename
cifs.audit.saveas /etc/log/adtlog.evt
admp-netapp>
```

Note: For more information on these commands and settings, refer to this [NetApp document](#).

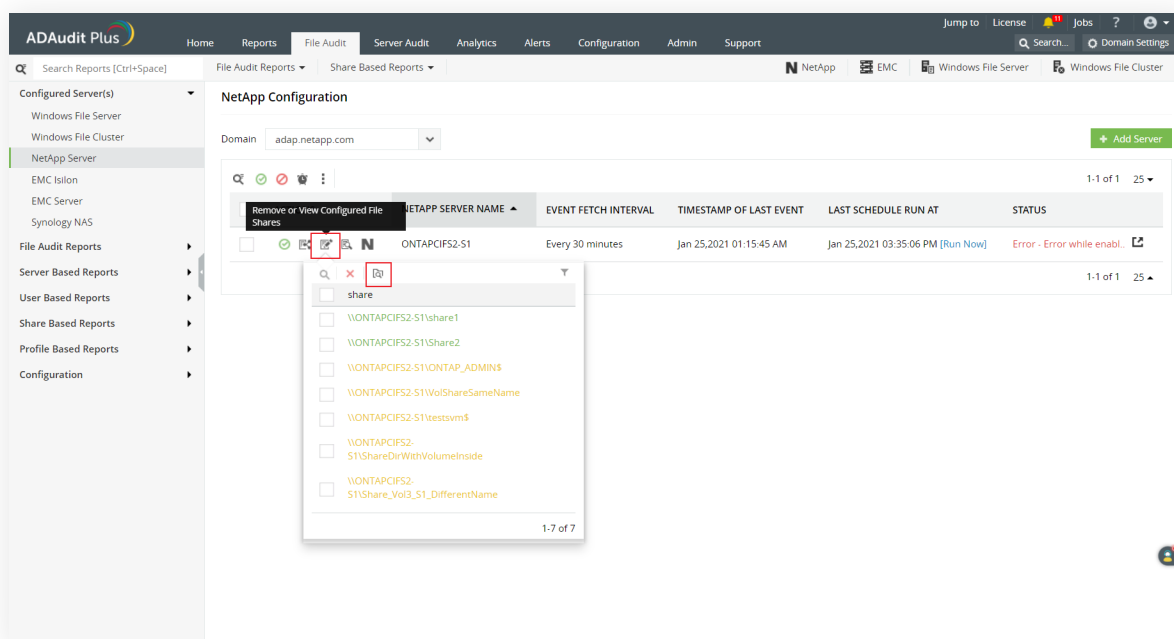
4. Configuring object-level auditing

4.1 Automatic configuration

To configure object-level auditing automatically for your target NetApp shares, follow these steps:

A) For shares that have already been added:

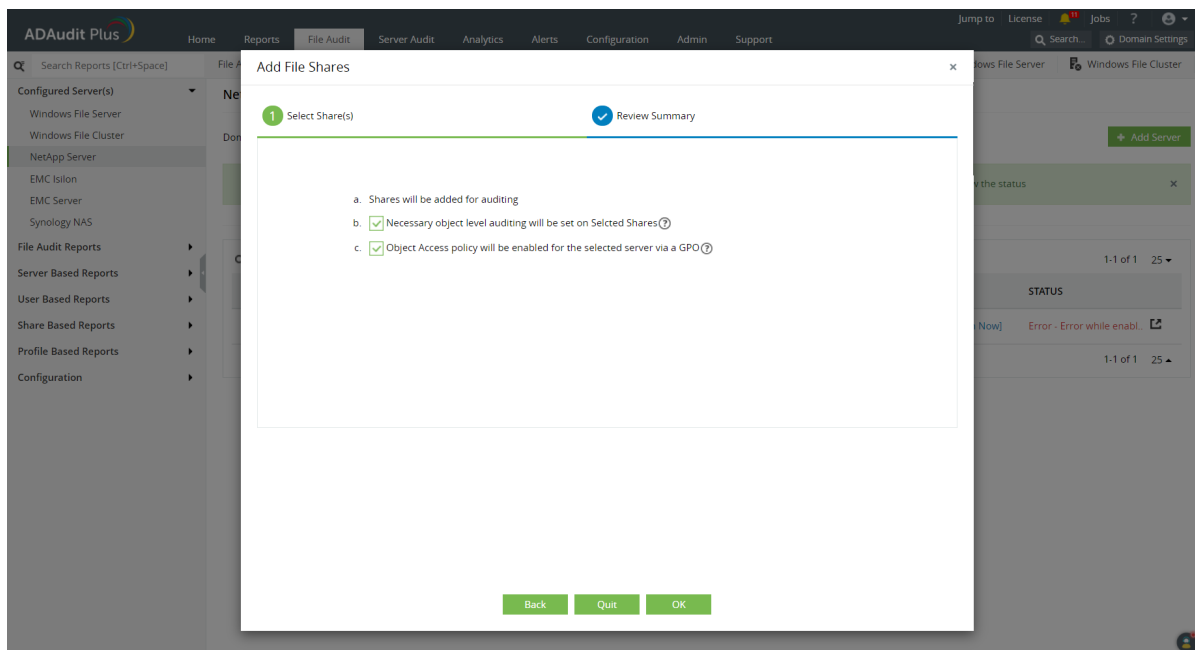
1. Log in to the ADAudit Plus web console and navigate to the **File Audit** tab > **Configured Server(s) > NetApp Server**.
2. From the **Domain** drop-down, select the domain with the target server. This will display all the available servers in that domain.
3. In the **Actions** column of the target server, click the icon labeled **Remove or View Configured File Shares** to list the shares that have been added.



4. Select the shares that you wish to enable object-level auditing in.
5. Click the icon labeled **Apply object level audit settings on shares**.
6. Click **Yes** to confirm the action.

B) For new shares:

1. Log in to the ADAudit Plus web console and navigate to the **File Audit** tab > **Configured Server(s) > NetApp Server**.
2. From the **Domain** drop-down, select the domain with the target server. This will display all the available servers in that domain.
3. In the **Actions** column of the target server, click the icon labeled **Add new file shares for auditing**. This will list all the available shares in that server.
4. Select the shares you wish to audit and click **Next**.
5. Ensure that both the checkboxes are selected to configure object-level auditing automatically.
6. Click **OK**.



Color codes:

When the **Remove or View Configured File Shares** pop-up is opened, the available shares will be highlighted in one of these colors based on the status of the object-level auditing configuration:

- Green—Object-level auditing is set correctly.
- Red—Object-level auditing is not set correctly, or an error occurred during the configuration.
- Orange—Object-level auditing configuration is in progress.

4.2 Manual configuration

Using Windows shares

Right-click on the **share folder** that you want to audit, select **Properties**, and then click on the **Security** tab → Select **Advanced**, and then click on the **Auditing** tab → For the **Everyone** group, add the following entries:

	Principal	Type	Access	Applies To
File/folder changes	Everyone	Success, Failure	<ul style="list-style-type: none"> • Create files / Write Data • Create folders / Append data • Write attributes • Write extended attributes • Delete sub folders and files • Delete 	This Folder, sub folders, and files
Folder permission and owner changes	Everyone	Success, Failure	<ul style="list-style-type: none"> • Take ownership • Change permissions 	This Folder and sub folders
File read	Everyone	Success, Failure	<ul style="list-style-type: none"> • List folder / Read data 	Files only
Folder read failure	Everyone	Failure	<ul style="list-style-type: none"> • List folder / Read data 	This Folder and sub folders

Using PowerShell cmdlets

Go to the `<installation directory>\bin` folder within the PowerShell command prompt → Type in **ADAP-Set-SACL.ps1** → Follow the steps to apply object-level auditing to shares on the file server.

- Create a CSV file containing the Universal Naming Convention (UNC) path or local path and the type of auditing (file server auditing [FA] or file integrity monitoring [FIM]) of all the folders that you need to enable auditing for.
- The CSV file should contain the list of folders in the following format: `<folder>,<type>`

Example:

```
\\SERVERNAME\folder,FA
```

```
C:\test folder,FA
```

```
E:\test folder,FIM
```

```
\\SERVERNAME\c$\folder,FIM
```

Once you have the CSV file that lists all the servers and the type of auditing required, go to the `<Installation Directory>\bin` folder within the PowerShell command prompt.

Type in:

`.\ADAP-Set-SACL.ps1 -file '.\file name' -mode add (or) remove -recurse true (or) false -username`

`DOMAIN_NAME\username`

Where

parameter	input variable	mandatory
-file	name of the CSV file containing the list of shared folders	yes
-mode	add - sets the object-level auditing settings (or) remove - removes the object-level auditing settings	yes
-recurse	true - Replace all sub-folder object-level auditing settings with inheritable auditing settings applied to the chosen folder. (or) false - Apply object-level auditing settings only to the chosen folder Note: By default, the -recurse parameter is set to false	no
-username	DOMAIN_NAME\username of the user with privilege over the file or folder to set the object-level auditing settings. (No cross-domain support)	no

Note: When removing object-level auditing for a set of folders, the **-type** parameter is not mandatory.

For example:

- To set object-level auditing for the list of folders in the shared_folders_list.CSV file, use:
`.\ADAP-Set-SACL.ps1 -file '.\shared_folders_list.CSV' -mode add`
- To replace all sub-folder object-level auditing settings with inheritable auditing settings applied to the shared_folders_list.CSV file, use:
`.\ADAP-Set-SACL.ps1 -file '.\shared_folders_list.CSV' -mode add -recurse true`
- To remove object-level auditing for the list of folders in the shared_folders_list.CSV file, use:
`.\ADAP-Set-SACL.ps1 -file '.\shared_folders_list.CSV' -mode remove`

```

Administrator: C:\Windows\System32\cmd.exe
Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.
C:\Program Files (x86)\ManageEngine\ADAudit Plus 6001\ADAudit Plus\bin\powershell.exe .\ADAP-Set-SACL.ps1

Directory: C:\Program Files (x86)\ManageEngine\ADAudit Plus 6001\ADAudit Plus\bin\ADAP-SET-SACL-Logs

Mode                LastWriteTime         Length Name
----                -
-a-----        6/27/2019   5:27 AM             0 ADAP-SET-SACL-(6-27-2019)-(05-27-02-424).txt
Transcript started, output file is C:\Program Files (x86)\ManageEngine\ADAudit Plus 6001\ADAudit Plus\bin\ADAP-SET-SACL-Logs\ADAP-SET-SACL-(6-27-2019)-(05-27-02-424).txt
Start Time : 6-27-2019 - 05:27:02:721AM
ERROR :: -file should not be empty
ERROR :: -mode should be empty

Usage:
ADAP-Set-SACL.ps1 -file [-mode [-recurse] [-username]]

-file          [Mandatory] CSU File
-mode         [Mandatory] add (Adding the SACL on all folder and subfolders) or remove (Removing the SACL on the folder and subfolders) : For remove - 'recurse' not applicable
-recurse     [Optional] Enable Inheritance and Remove all explicit SACL on all subfolders : 'true' or 'false' : By default false
-username    [Optional] Domain User having privilege over the folder or share

Examples:
1) .\ADAP-Set-SACL.ps1 -file '.\folders.csv' -mode add
2) .\ADAP-Set-SACL.ps1 -file '.\folders.csv' -mode add -username DOMAIN_NAME\username
3) .\ADAP-Set-SACL.ps1 -file '.\folders.csv' -mode add -recurse true
4) .\ADAP-Set-SACL.ps1 -file '.\folders.csv' -mode remove
5) .\ADAP-Set-SACL.ps1 -file '.\folders.csv' -mode remove -username DOMAIN_NAME\username

In Input csv file, Format should be as
<Folder>,<Type>
-Folder UNC Path (Ex: \\SERVERNAME\ShareName) or Local Path (Ex: C:\Test Folder)
-Type    FA (File Auditing) or FIM (File Integrity Monitoring)

For removing SACL -type is not required

Examples:
In file 'folders.csv'
\\SERVERNAME\Folder_FA
C:\Test Folder_FA
C:\Test Folder_FIM
\\SERVERNAME\Folder_FIM

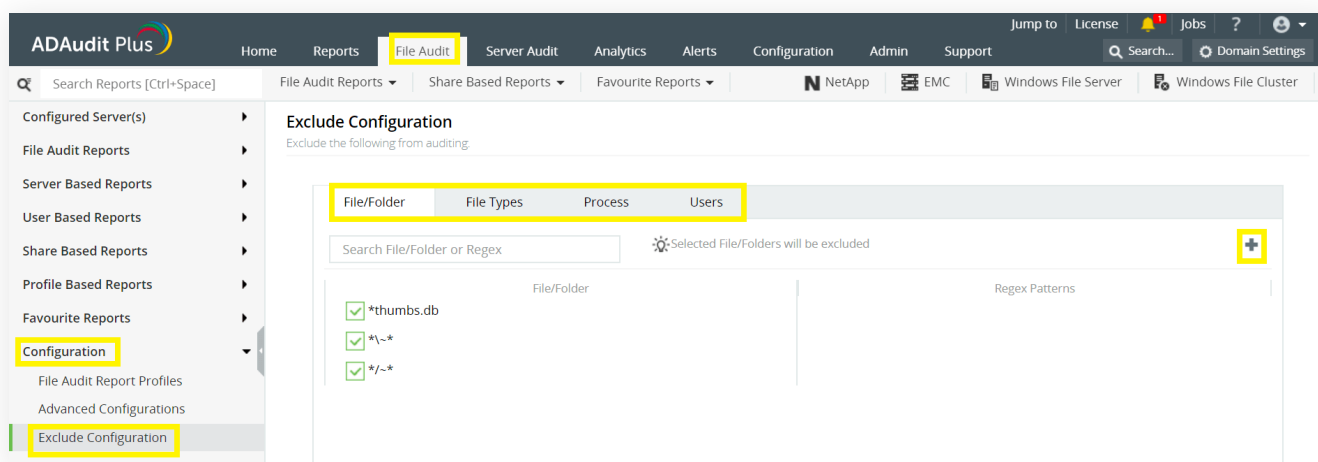
End Time : 6-27-2019 - 05:27:02:793AM
Transcript stopped, output file is C:\Program Files (x86)\ManageEngine\ADAudit Plus 6001\ADAudit Plus\bin\ADAP-SET-SACL-Logs\ADAP-SET-SACL-(6-27-2019)-(05-27-02-424).txt

C:\Program Files (x86)\ManageEngine\ADAudit Plus 6001\ADAudit Plus\bin>_
  
```

5. 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	<ul style="list-style-type: none"> C:\sharefolder\excludefolder C:\sharefolder\excludefolder* 	
What will get excluded	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> C:\Users\user1\AppData C:\Users\user2\AppData C:\Users\user1\AppData\subfolder C:\Users\user2\AppData\subfolder
What won't get excluded	<ul style="list-style-type: none"> 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\[^\w]*\.[^\w]*\$
What will get excluded	<ul style="list-style-type: none"> C:\sharefolder\excludefolder\file.txt C:\sharefolder\excludefolder\folder.withDot
What won't get excluded	<ul style="list-style-type: none"> 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

6. Troubleshooting

Understand and resolve the most common issues faced while auditing your NetApp filers using ADAudit Plus.

i No Data Available

1. Login to the ADAudit Plus server with the user account configured in ADAudit Plus. Then, check whether the NetApp server's shares are accessible and whether the account has sufficient privileges to access the target servers and collect audit data. The required privileges are listed in this image:

```
admp-netapp> useradmin user list root
Name: root
Info: Default system administrator.
Rid: 0
Groups:
Full Name:
Allowed Capabilities: login-http-admin, api-system-cli, api-options-get, cli-cifs
Password min/max age in days: 0/never
Status: enabled
admp-netapp> █
```

2. Verify whether the audit policies described in [Section 3](#) of this guide have been configured correctly.

ii Access Denied

Login to the ADAudit Plus server with the user account configured in ADAudit Plus. Then, check whether the NetApp server's shares are accessible and whether the user has sufficient permission to access the target shares.

The required privileges are listed in this image:

```
admp-netapp> useradmin user list root
Name: root
Info: Default system administrator.
Rid: 0
Groups:
Full Name:
Allowed Capabilities: login-http-admin, api-system-cli, api-options-get, cli-cifs
Password min/max age in days: 0/never
Status: enabled
admp-netapp> █
```

iii The network path was not found

This error occurs when the target computer cannot be contacted, or when the ADAudit Plus service account does not have sufficient privileges to access the share on the target computer.

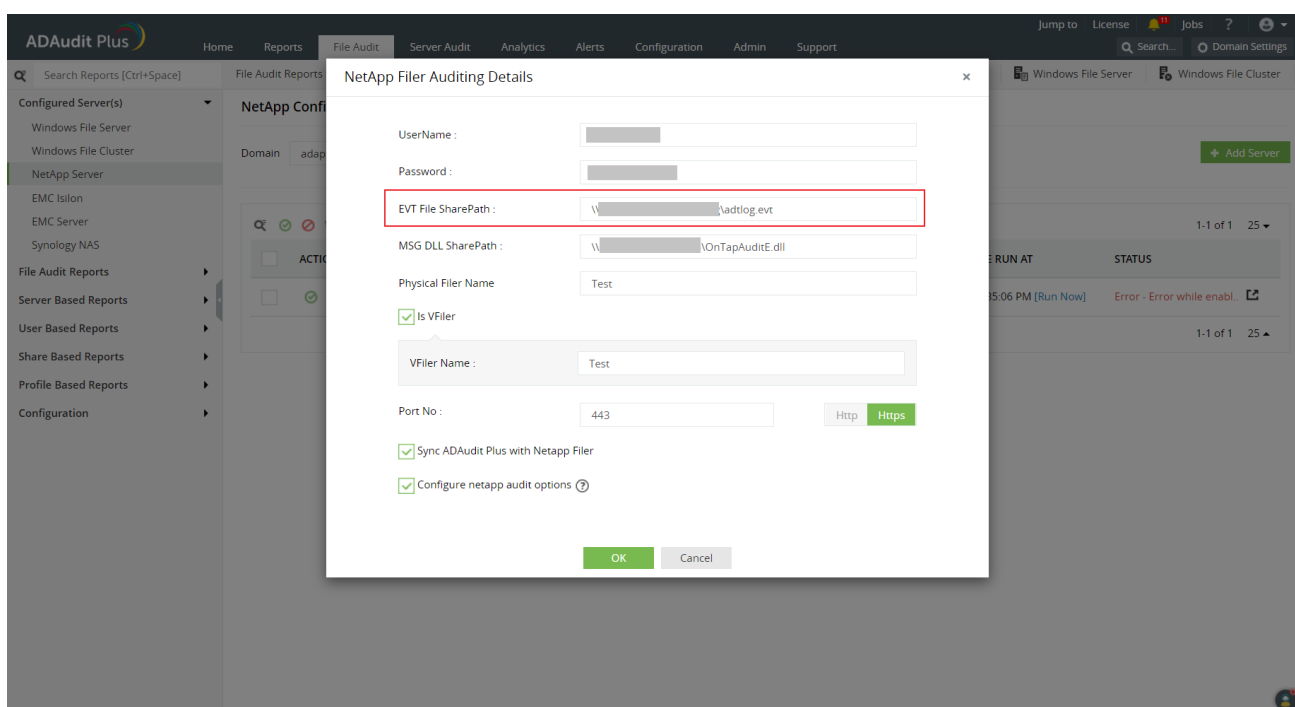
To troubleshoot:

1. Connect to the audit files (EVT file shares) on the target computer.
2. Open File Explorer from the taskbar and select Network from the left tree.
3. Double-click on the NetApp server which contains the target shared folder.
4. Open the shared folder and double-click on the share you want to access.
5. If you can access the share, try pinging the NetApp server by following these steps:
 - a. Login to your ADAudit Plus web console.
 - b. Navigate to File Audit > Configured Servers > NetApp Server and identify the NetApp server showing the error.
 - c. Note the name of the NetApp server as found in ADAudit Plus console.
 - d. Open Command Prompt and ping the NetApp server with its name as noted from the ADAudit Plus console. For example, if the server's name is servername1, type the command **ping servername1**.
 - e. 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.

iv The system cannot find the specified path

Check if the shares containing the audit logs are accessible from the ADAudit Plus server. This can also occur when the NetApp auditing EVT file share path configured in ADAudit Plus is incorrect.

To resolve this, check if the NetApp EVT file path is the default location \\NetApp Filer Name\etc\$\log. Also, check if the location \\NetApp Filer\C\$\etc\log is configured in ADAudit Plus. If it is incorrect, provide the correct path and try again.



v The system cannot find the specified file

This error occurs when the service account used to run ADAudit Plus is unable to locate the audit files.

To troubleshoot:

1. Check whether the audit files (EVT files) exist in the Netapp audit location by following these steps:
 - a. Open File Explorer from the task bar and select Network from the left tree.
 - b. Double-click on the NetApp server which contains the target shared folder.
 - c. Navigate to the NetApp audit location and double-click on the audit file share you want to access.
2. Verify if audit policies are configured on the NetApp server to ensure that events are logged whenever any activity occurs.

vi Unable to connect to the NetApp Server through mentioned port and protocol

Ensure that the port number and protocol (HTTP/HTTPS) used for the web console are correct.

Try connecting to the NetApp OnCommand center from the ADAudit Plus server with the provided port and protocol. You should be able to access the web console.

