ManageEngine
ADAudit Plus

NetApp Cluster
Auditing Guide

www.adauditplus.com

Table of Contents

1. Overview

Overview of NetApp CMode/cluster/Vserver CIFS server auditing

A NetApp cluster is a storage system that consists of one or more nodes grouped together (as HA pairs) and runs on NetApp's proprietary operating system, ONTAP. Clusters allow resource pooling and enhance scalability. As a single management entity, they enable easier administration of enterprise storage.

ManageEngine ADAudit Plus is a real-time, UBA-driven change auditor that can monitor the CIFS file-based protocols over a network by scheduling reports and triggering email or SMS alerts for critical events. This helps ensure data security and streamlines compliance with regulations like HIPAA, FISMA, the GDPR, and SOX.

Supported versions

ADAudit Plus can audit the ONTAP versions below:
NetApp ONTAP 8.2.1 and above

Audited events

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

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

This guide provides steps to configure change auditing in your NetApp CMode/cluster/Vserver using ADAudit Plus.

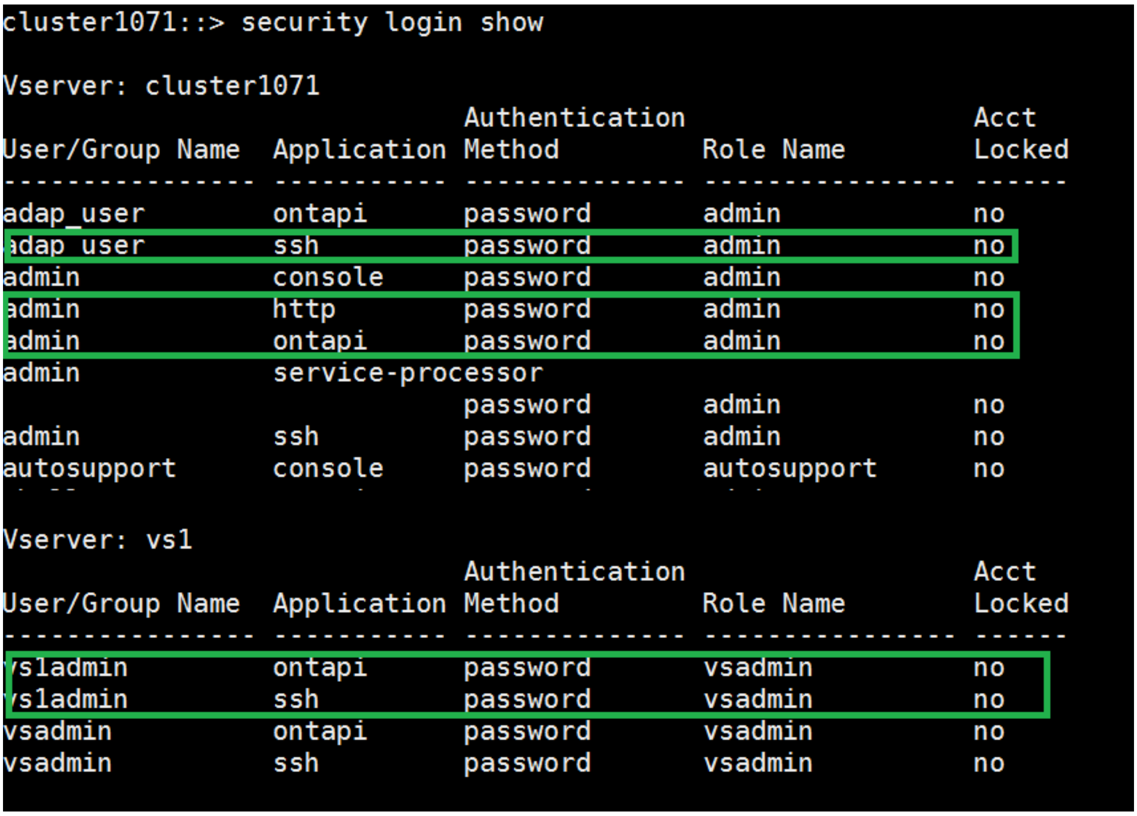
2. Configuration prerequisites

Prerequisites for NetApp cluster auditing

Keep the details below on hand before beginning your configuration of NetApp CMode/cluster /Vserver auditing in ADAudit Plus.

- **Target server name:** The NetApp CIFS server name.
- **Target shares:** The list of shares that you wish to audit.
- **Management IP:** The management IP of the target cluster or the Vserver.
- **Username and password:** The credentials required to connect to the management IP.

  This user can be the default admin, vsadmin, or any other user with the roles highlighted below:



```
cluster1071::> security login show

Vserver: cluster1071
                                 Authentication                  Acct
User/Group Name  Application Method          Role Name           Locked
---------------- ----------- -------------- ----------------  ------
adap_user        ontapi      password        admin               no
adap_user        ssh         password        admin               no
admin            console     password        admin               no
admin            http        password        admin               no
admin            ontapi      password        admin               no
admin            service-processor
                             password        admin               no
admin            ssh         password        admin               no
autosupport      console     password        autosupport         no

Vserver: vs1
                                 Authentication                  Acct
User/Group Name  Application Method          Role Name           Locked
---------------- ----------- -------------- ----------------  ------
vs1admin         ontapi      password        vsadmin             no
vs1admin         ssh         password        vsadmin             no
vsadmin          ontapi      password        vsadmin             no
vsadmin          ssh         password        vsadmin             no
```

- **Port number:** The port that will be used for HTTP or HTTPS communication between the NetApp cluster and the ADAudit Plus server.
- **Log storage location:** Either of the below locations for storing audit logs:

  i. A new aggregate with 3GB of available space: ADAudit Plus will create a volume named cifs_audit_log, mount it in the /cifs_audit_log path, and use it for storing logs.

  ii. An existing junction or local path, such as /logs/fs1/, with a minimum of 3GB of available space.

3. Configuring NetApp cluster auditing

3.1 Adding the target cluster

Choosing the NetApp server

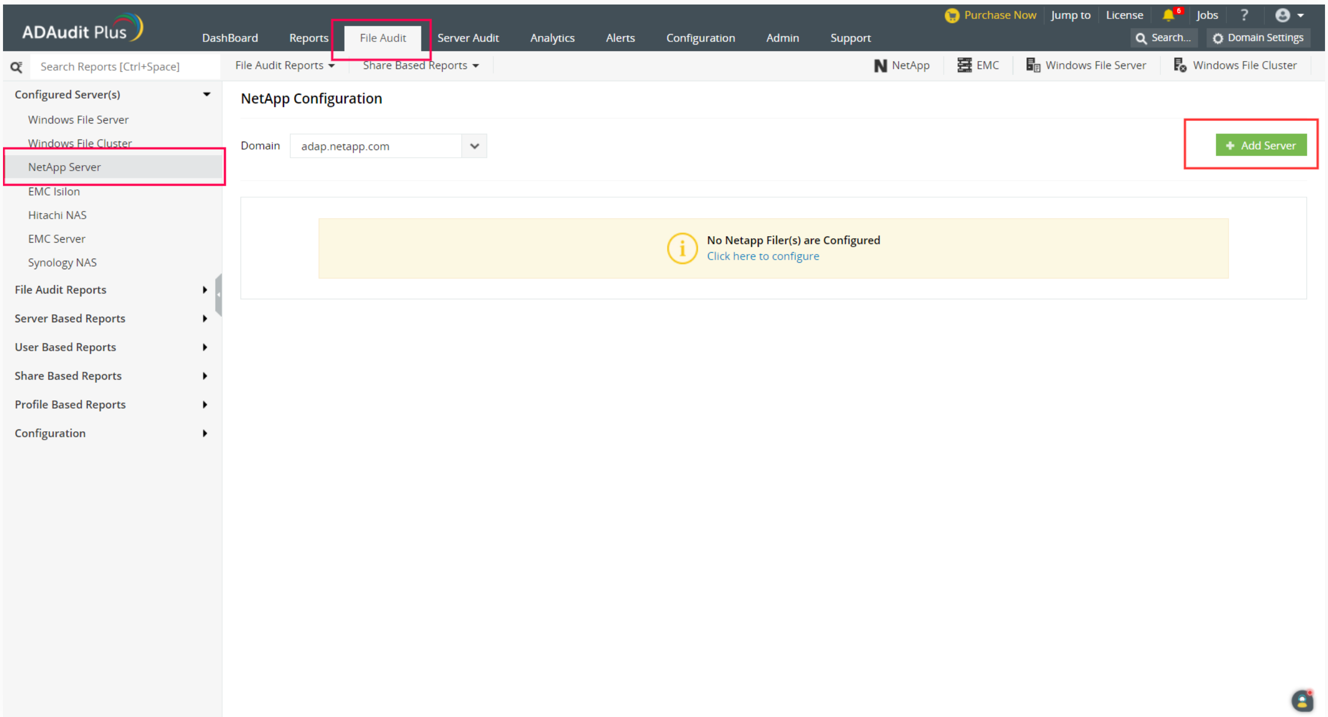
To add your target NetApp clusters:

i. Log in to the ADAudit Plus web console.

ii. Navigate to the **File Audit** tab > **Configured Server(s)** > **NetApp Server**. From the **Domain** drop-down, elect the domain with the target server.

iii. 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.

iv. Select the target server(s) and click **Next.**



NetApp Configuration

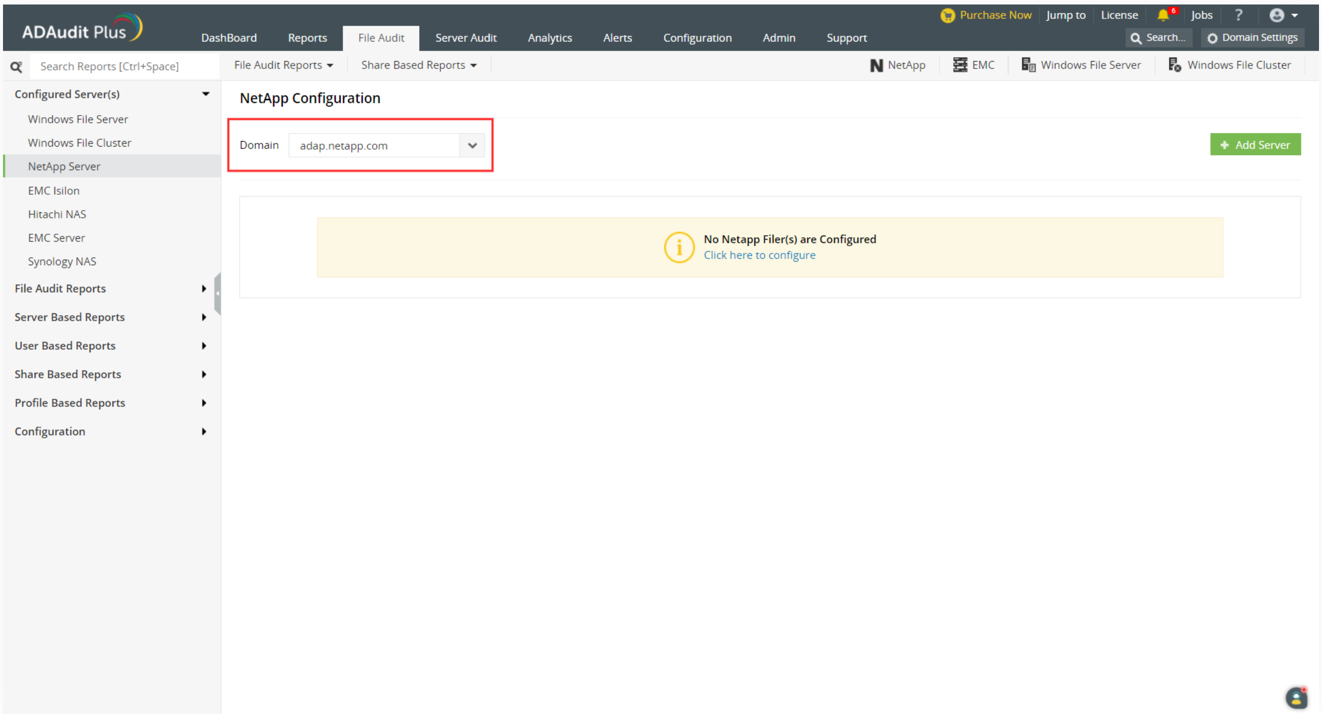
Domain: adap.netapp.com

No Netapp Filer(s) are Configured
Click here to configure

Troubleshooting

a. NetApp CIFS server name is not listed

Check whether the NetApp server is added to the Active Directory domain that is configured in the ADAudit Plus server.



NetApp Configuration

Domain: adap.netapp.com

No Netapp Filer(s) are Configured
Click here to configure

3.2 Adding the target shares

Selecting the target shares

To add the shares you wish to audit:

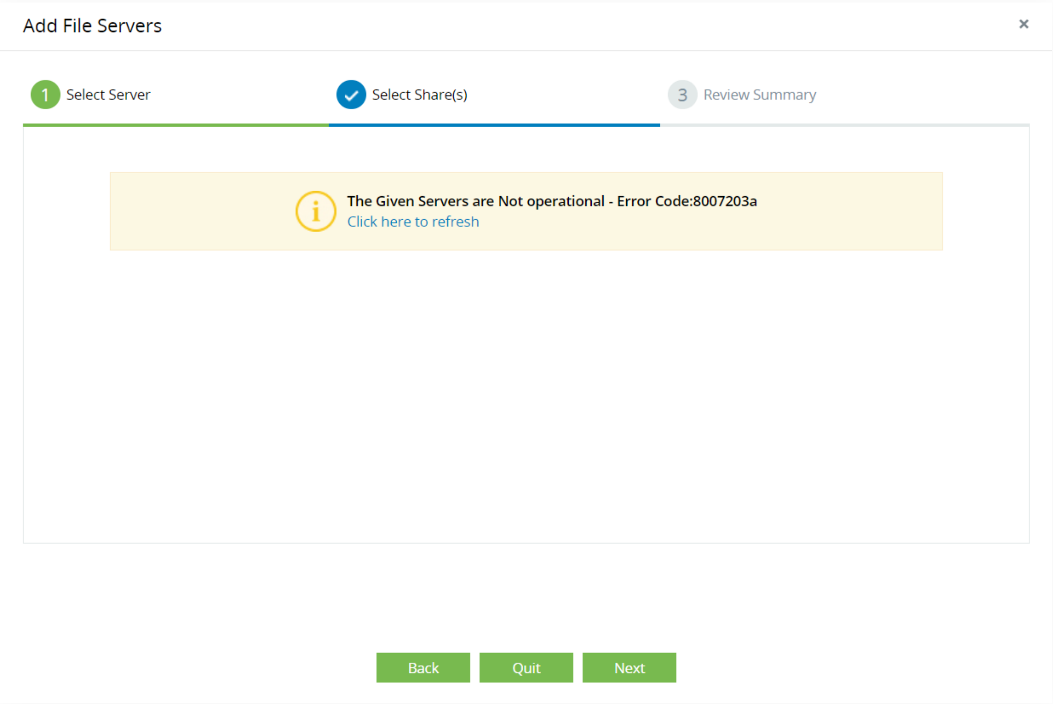
i. The next page on the pop-up lists all the shares in that server. You can also click the **Refresh** icon to update the list if needed.

ii. Select the target shares from the list and click **Next.**

Troubleshooting

a. The given servers are not operational - Error code 8007203a

Check whether the target NetApp server is accessible from the ADAudit Plus server.



Add File Servers

The Given Servers are Not operational - Error Code:8007203a
Click here to refresh

b. Access Denied

Log in to the ADAudit Plus server with the username configured in ADAudit Plus. Check whether the NetApp server's shares are accessible and whether the user has sufficient permission to access the shares.

3.3 Configuring audit options

Configuring audit options

On the Review Summary page of the Add Servers pop-up, you can configure your preferred audit options. Start by choosing your CIFS server type—in this case, **Cluster Mode/Vserver.**

Configure the settings below.

1. Configuring the management IP and the account

Provide the details below as discussed in the Prerequisites section:

- Management IP
- Username and password
- Port number

2. Configuring audit policies

The audit policies required for effective NetApp cluster auditing can be configured either automatically or manually.

2.1 Automatic audit policy configuration

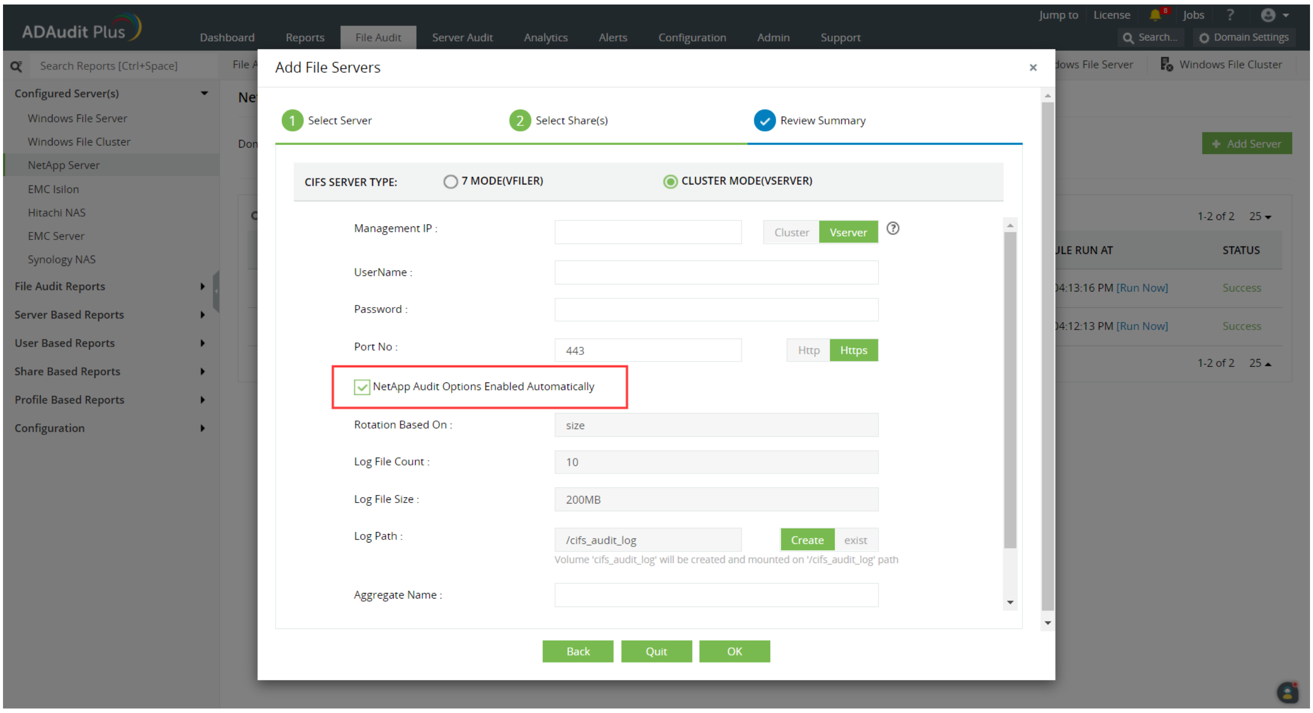
If you want to allow ADAudit Plus to configure the required audit settings automatically, select the **NetApp Audit Options Enabled Automatically** check box while adding the target NetApp server.

When this option is enabled, ADAudit Plus will configure a default audit policy and the below parameters in the NetApp CIFS server:

- **Rotation Based On:** Size
- **Maximum Log File Count:** 10
- **Log File Size:** 200MB
- **Log Path:** Select either **Create** or **Exist** based on whether you want to provide a new aggregate name or an existing path with 3GB space as explained in the Prerequisites page. If you choose **Create**, a new volume named cifs_audit_log will be created and mounted on the /cifs_audit_log path. If you choose **Exist**, provide an existing path with a minimum of 3GB for log storage.

Note:

For the **Exist** option, ensure that you provide the junction path and not the share path. For example, /root/logs/cifs is a valid path.



Add File Servers

1 Select Server　2 Select Share(s)　✓ Review Summary

CIFS SERVER TYPE: ○ 7 MODE(VFILER) ● CLUSTER MODE(VSERVER)

Management IP : Cluster [✓ Vserver]

UserName :

Password :

Port No : 443 Http [✓ Https]

☑ NetApp Audit Options Enabled Automatically

Rotation Based On : size

Log File Count : 10

Log File Size : 200MB

Log Path : /cifs_audit_log Create exist

Volume 'cifs_audit_log' will be created and mounted on '/cifs_audit_log' path

Aggregate Name :

Back Quit OK

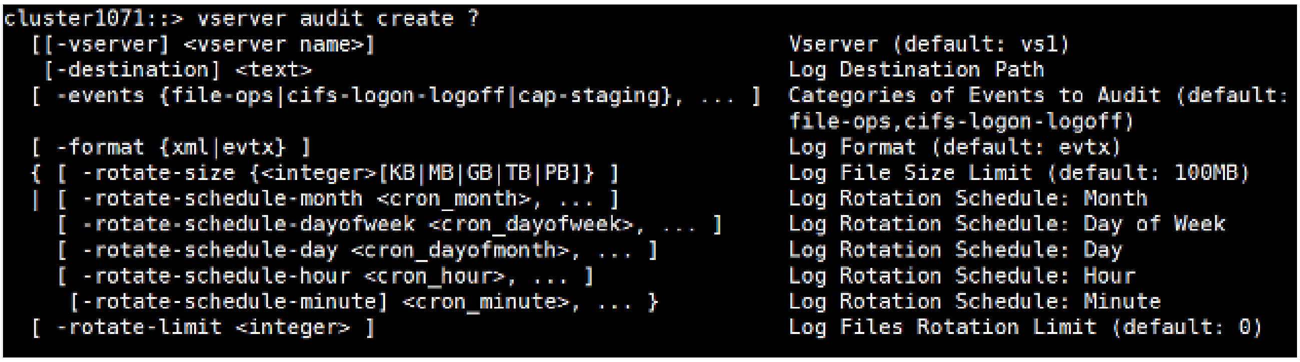
If you wish to configure the audit policies manually, follow the directions in the next section.

2.2 Manual audit policy configuration

The target NetApp cluster devices can be accessed through an SSH or Telnet connection using the required cluster or Vserver administrative credentials.

Use the command below to configure the audit settings for the respective CIFS servers:

Vserver **audit create -<Vserver_Name> -destination <Log_Destination_Path> -format <Log_Format_in_XML /evtx> -rotate-size <Log_File_Size_Limit_in_KB/MB/GB/TB/PB> -rotate-limit <Log_Files_Rotation_Limit>**



```
cluster1071::> vserver audit create ?
  [[-vserver] <vserver name>]                               Vserver (default: vs1)
   [-destination] <text>                                    Log Destination Path
  [ -events {file-ops|cifs-logon-logoff|cap-staging}, ... ] Categories of Events to Audit (default:
                                                            file-ops,cifs-logon-logoff)
  [ -format {xml|evtx} ]                                    Log Format (default: evtx)
  { [ -rotate-size {<integer>[KB|MB|GB|TB|PB]} ]            Log File Size Limit (default: 100MB)
  | [ -rotate-schedule-month <cron_month>, ... ]            Log Rotation Schedule: Month
    [ -rotate-schedule-dayofweek <cron_dayofweek>, ... ]    Log Rotation Schedule: Day of Week
    [ -rotate-schedule-day <cron_dayofmonth>, ... ]         Log Rotation Schedule: Day
    [ -rotate-schedule-hour <cron_hour>, ... ]              Log Rotation Schedule: Hour
     [-rotate-schedule-minute] <cron_minute>, ... }         Log Rotation Schedule: Minute
  [ -rotate-limit <integer> ]                               Log Files Rotation Limit (default: 0)
```

Here, the parameters to be defined are:

- **<Vserver_Name>:** The name of the Vserver that the audit configuration will be created on.
- **<Log_Destination_Path>:** The audit log destination path where consolidated audit logs are stored. The command will fail if the path is not valid. The path can be up to 864 characters in length and must have read-write permissions.
- **<Log_Format_in_XML/evtx>:** The output format of the audit logs. ADAudit Plus only supports Microsoft Windows EVTX log format.
- **<Log_File_Size_Limit_in_KB/MB/GB/TB/PB>:** The audit log file size limit, represented as an integer, along with the unit (e.g., 200MB).
- **<Log_Files_Rotation_Limit>:** The audit log files rotation limit. A value of "0" indicates that all the log files are retained, and a value of "5" indicates that the last five audit logs are retained.

Example: Vserver **audit create -Vserver vs1 -destination /cifs_audit_log -format evtx -rotate-size 200MB -rotate-limit 10**

Notes:

i. When you enable an audit policy in the NetApp CIFS server through the product console or manually, the **Audit-Guarantee** setting in the NetApp server is set to **True**. This setting prevents users from performing NetApp file operations when events aren't being logged, which can happen due to insufficient disk space (learn more here). To continue to perform file operations, you can set **Audit-Guarantee=False** in the NetApp server. However, if you do this, file operations will not get logged.

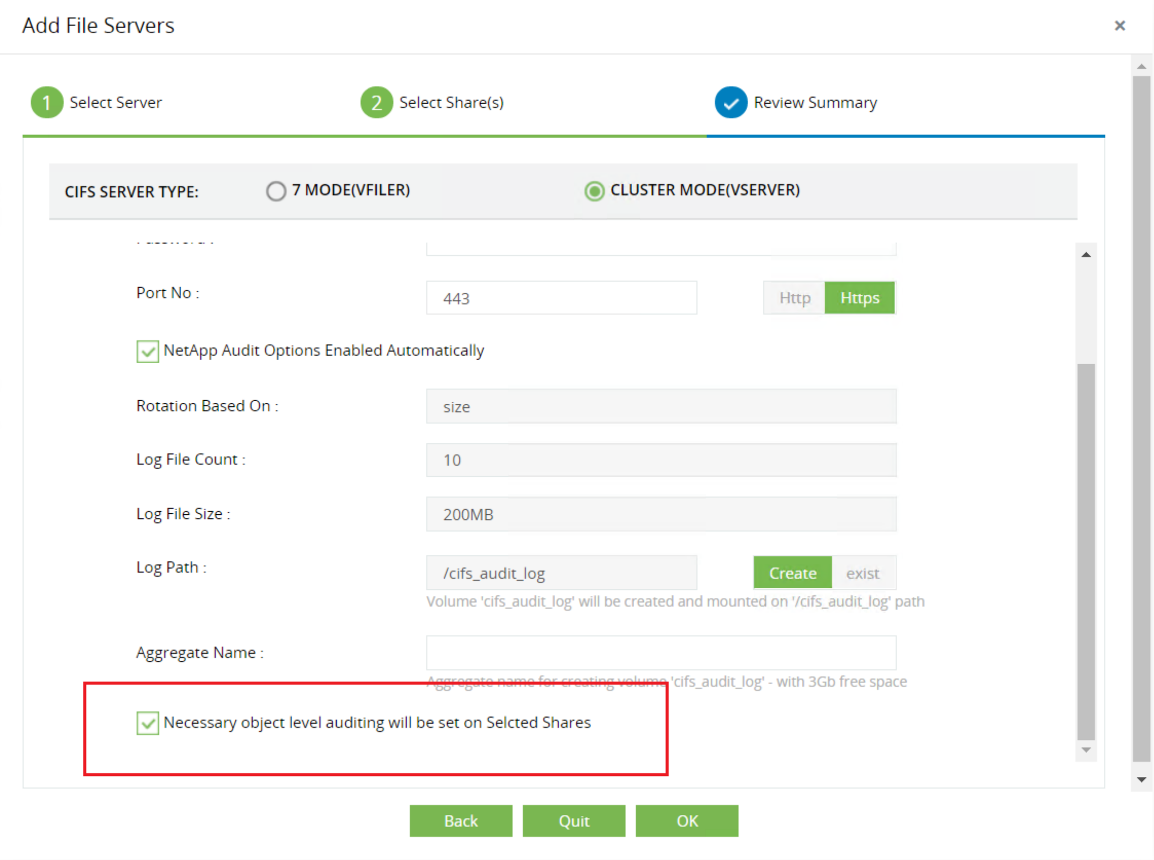
ii. We recommend disabling the snapshot policy in the volume where audit logs will be stored.>

3. Configuring SACLs in the shares

System access-control lists (SACLs) decide which files and folders will be audited and ensure that the system generates audit events when files are accessed. The required SACLs for NetApp CMode CIFS auditing can be configured either automatically or manually.

3.1 Automatic SACL configuration

If you want ADAudit Plus to auto-configure the required SACLs in the target cluster shares, ensure that the **Necessary object level auditing will be set on selected shares** check box is selected. Click **OK.**



Add File Servers ×

1 Select Server — 2 Select Share(s) — ✓ Review Summary

CIFS SERVER TYPE: ○ 7 MODE(VFILER) ● CLUSTER MODE(VSERVER)

Port No : 443 Http **Https**

☑ NetApp Audit Options Enabled Automatically

Rotation Based On : size

Log File Count : 10

Log File Size : 200MB

Log Path : /cifs_audit_log **Create** exist

Volume 'cifs_audit_log' will be created and mounted on '/cifs_audit_log' path

Aggregate Name :

Aggregate name for creating volume 'cifs_audit_log' - with 3Gb free space

☑ Necessary object level auditing will be set on Selcted Shares

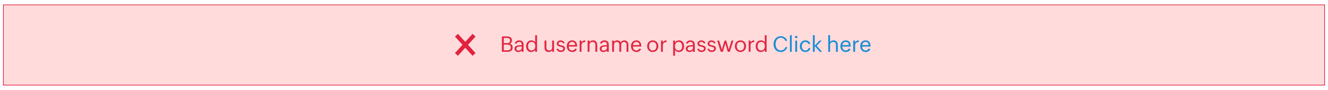
If you wish to configure SACLs manually, deselect the **Necessary object level auditing will be set on elected shares** check box and proceed to the next step.

3.2 Manual SACL configuration

For steps to manually configure object-level auditing in your NetApp cluster servers, refer to this page.

Troubleshooting

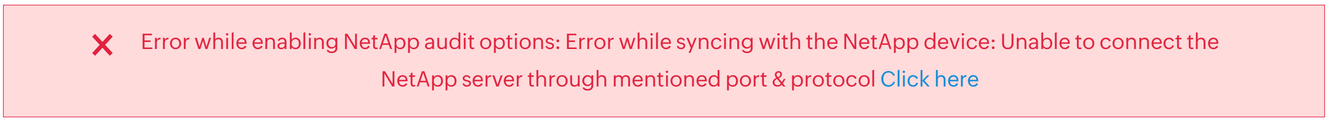
a. Bad username or password



✗ Bad username or password Click here

Check whether the provided username and password are correct.

b. Unable to connect to the NetApp Server through mentioned port and protocol



✗ Error while enabling NetApp audit options: Error while syncing with the NetApp device: Unable to connect the NetApp server through mentioned port & protocol Click here

Perform these checks:

i. Check if the management IP is correct and that you have selected the correct management IP type (i.e., either cluster or Vserver management IP).

ii. Ensure that the credentials entered belong to the provided management IP and are correct.

Note:

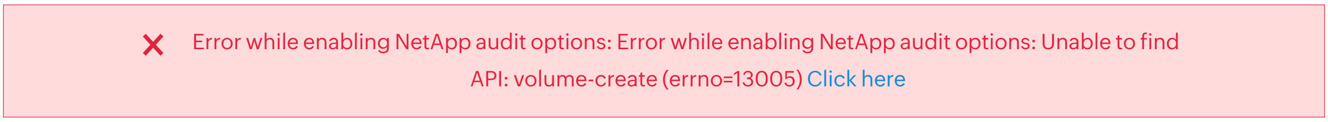
To check the items above, use a PuTTy or SSH client and connect to the provided NetApp management IP with the credentials. You should be able to log in without any errors.

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

Try connecting to the NetApp OnCommand center with the provided port and protocol.

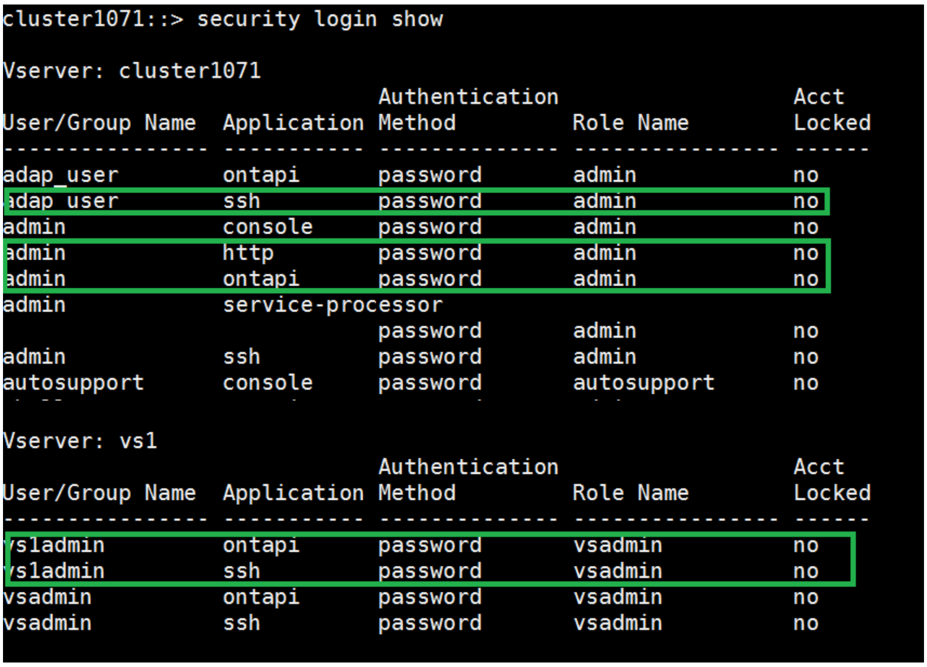
You should be able to access the web console.

c. Unable to find API: volume create (errno-13005)



✕ Error while enabling NetApp audit options: Error while enabling NetApp audit options: Unable to find API: volume-create (errno=13005) Click here

This error occurs when the configured user does not have sufficient permission to execute certain perations on the NetApp server. Refer to the image below for the required roles and permissions.



```
cluster1071::> security login show

Vserver: cluster1071
                                 Authentication                  Acct
User/Group Name  Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
adap_user        ontapi      password       admin            no
adap user        ssh         password       admin            no
admin            console     password       admin            no
admin            http        password       admin            no
admin            ontapi      password       admin            no
admin            service-processor
                             password       admin            no
admin            ssh         password       admin            no
autosupport      console     password       autosupport      no

Vserver: vs1
                                 Authentication                  Acct
User/Group Name  Application Method         Role Name        Locked
---------------- ----------- -------------- ---------------- ------
vsladmin         ontapi      password       vsadmin          no
vsladmin         ssh         password       vsadmin          no
vsadmin          ontapi      password       vsadmin          no
vsadmin          ssh         password       vsadmin          no
```

d. Aggregate does not exist (errno-14420)

✕ Error while enabling NetApp audit options: Error while enabling NetApp audit options: Aggregate adsdas does not exist (errno=14420) Click here

Check whether the aggregate name (provided for storing audit logs) is valid and has storage provisions for the configured CIFS Vserver.

e. The specified path does not exist in the namespace (errno-13001)

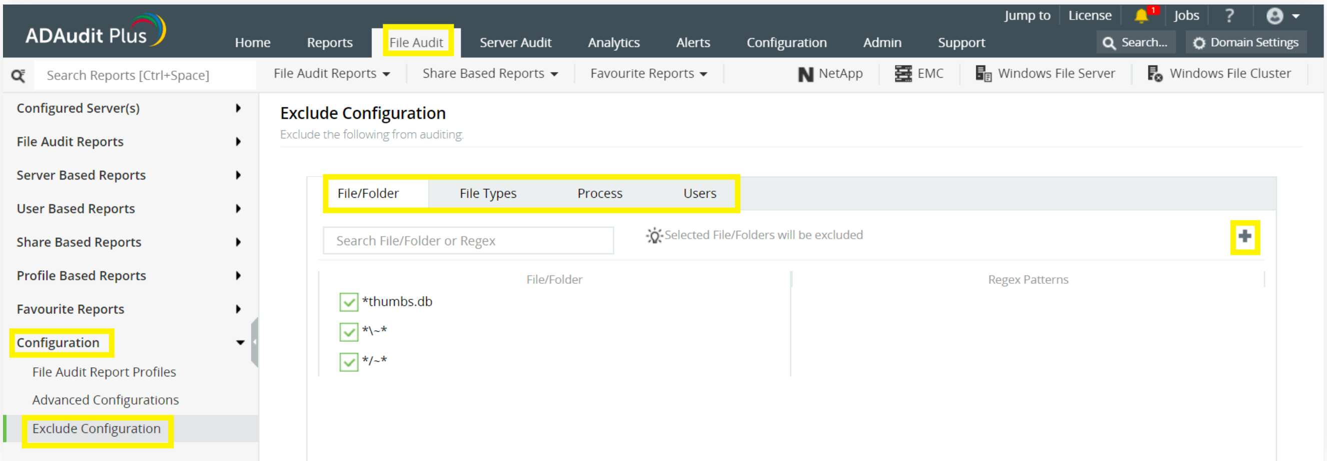
✕ Error while enabling NetApp audit options: Error while enabling NetApp audit options: The specified path "/ffsdsdsds/" does not exist in the namespace belonging to Vserver "Vs2". (errno=13001) Click here

Check whether the junction path provided for the log path is valid and mounted and that it belongs to the configured CIFS Vserver.

4. 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.



Exclude Configuration

Exclude the following from auditing

Selected File/Folders will be excluded

☑ *thumbs.db

☑ *\~*

☑ */~*

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

ManageEngine
ADAudit Plus

ManageEngine ADAudit Plus is an IT security and compliance solution. With over 200 event-specific reports and real-time email alerts, it provides in-depth knowledge about changes effected to both the content and configuration of Active Directory, Azure AD and Windows servers. Additionally it also provides thorough access intelligence for workstations and file servers (including NetApp and EMC).

To learn more about how ADAudit Plus can help you with all your Active Directory auditing needs, please visit:
https://www.manageengine.com/products/active-directory-audit/

$ Get Quote

⤓ Download