ManageEngine
ADAudit Plus

Huawei OceanStor Auditing Guide

www.adauditplus.com

Table of contents

Overview of Huawei OceanStor auditing

ManageEngine ADAudit Plus is a UBA-driven change auditor that reports on and analyzes user activity across Active Directory, Windows servers, file storage systems, and workstations. For Huawei OceanStor storage systems, it can:

- ✓ Audit file activities with details on who did what, in which file, when, and where.
- ✓ Provide a user-friendly interface and detailed reports for analyzing file access attempts.
- ✓ Detect abnormal user activities, such as an atypical volume of file changes or file modifications at unusual times.
- ✓ Trigger instant alerts when anomalous file activities are detected and execute automated scripts to protect data stores.
- ✓ Deliver out-of-the-box compliance audit reports for regulations such as HIPAA, SOX, the GDPR, the PCI DSS, ISO/IEC 27001, FISMA, and the GLBA.

Supported platforms	Supported log format	Audited events
Huawei OceanStor V5 series	XML	Success events: Create, read, write, delete, rename, move, permission change, and owner change Failure event: Read deny
Huawei OceanStor 9000 V5	LOG	Success events: Create, read, write, delete, rename, and move
Huawei OceanStor Dorado All-Flash Storage and OceanStor Hybrid Flash Storage	XML	Success events: Create, read, write, delete, rename, move, permission change, and owner change

This guide provides the steps to configure change auditing for your Huawei OceanStor storage systems using ADAudit Plus.

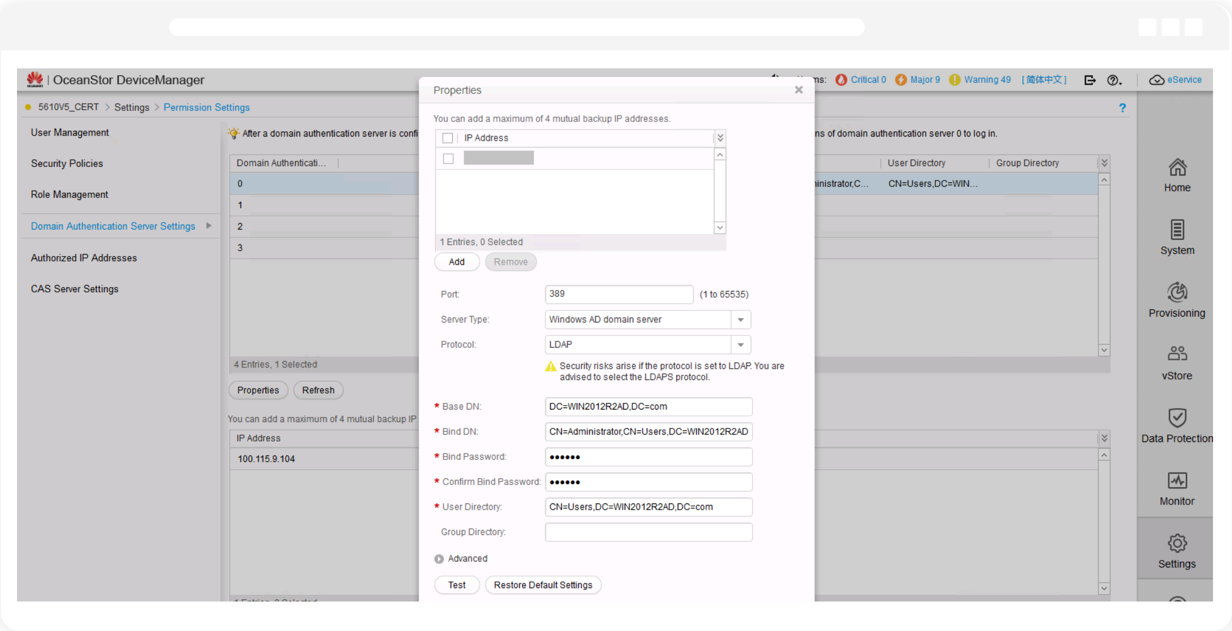
Huawei OceanStor V5 series

Minimum privileges required

For OceanStor V5 series (system vStore 0 or default vStore), provide the necessary privileges to the user configured in the **Domain Settings** of **ADAudit Plus** (in the top-right corner of the console and referred to below as the Domain Settings user), or create a dedicated ADAudit Plus Huawei user account and provide it with the privileges below.

- **For OceanStor V5 series (system vStore 0 or default vStore)**

1. In **OceanStor DeviceManager,** configure the domain authentication server to provide the domain users with management permission.



After a domain authentication server is confi ... ns of domain authentication server 0 to log in.

Domain Authenticati...	...	User Directory	Group Directory
0	inistrator,C...	CN=Users,DC=WIN...	
1			
2			
3			

4 Entries, 1 Selected

You can add a maximum of 4 mutual backup IP

IP Address
100.115.9.104

Properties

You can add a maximum of 4 mutual backup IP addresses.

□ IP Address
□ [redacted]

1 Entries, 0 Selected

Port: 389 (1 to 65535)

Server Type: Windows AD domain server

Protocol: LDAP

Security risks arise if the protocol is set to LDAP. You are advised to select the LDAPS protocol.

* Base DN: DC=WIN2012R2AD,DC=com

* Bind DN: CN=Administrator,CN=Users,DC=WIN2012R2AD

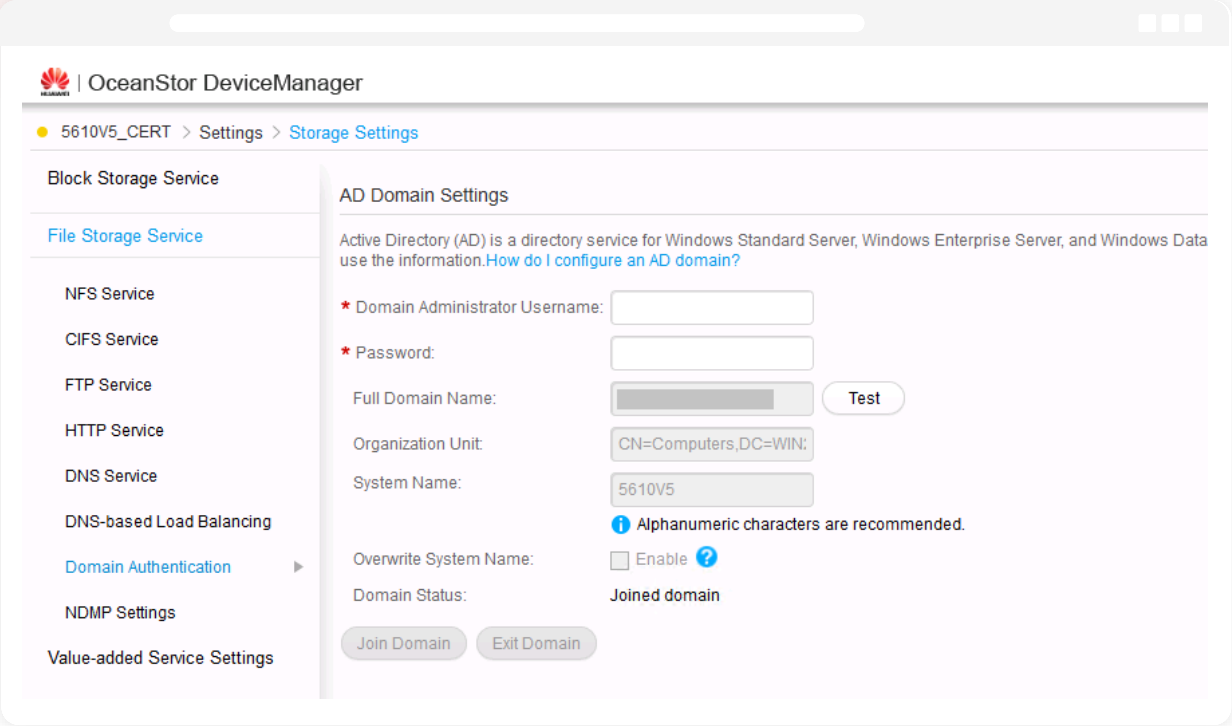
* Bind Password: ••••••

* Confirm Bind Password: ••••••

* User Directory: CN=Users,DC=WIN2012R2AD,DC=com

Group Directory:

2. Join the **File Storage Service** to the AD domain by providing the necessary details under **Domain Authentication.**



OceanStor DeviceManager

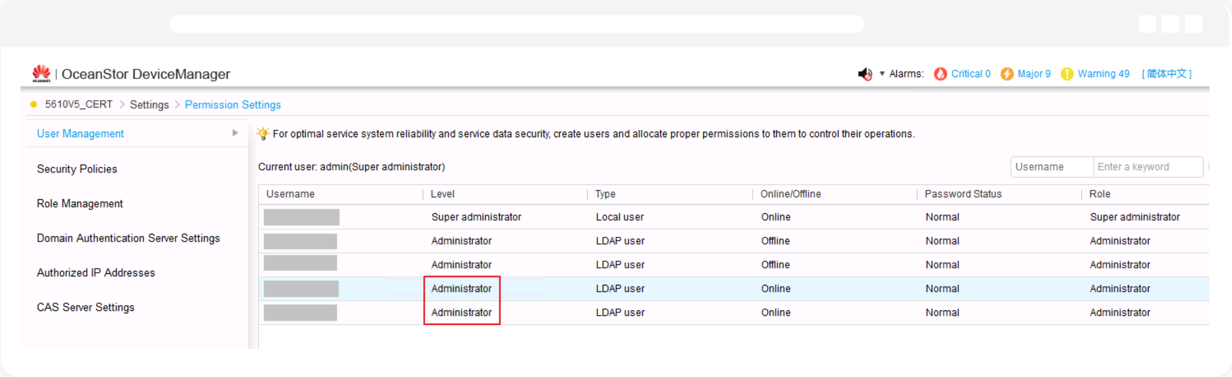
5610V5_CERT > Settings > Storage Settings

AD Domain Settings

Active Directory (AD) is a directory service for Windows Standard Server, Windows Enterprise Server, and Windows Data use the information.How do I configure an AD domain?

* Domain Administrator Username:	
* Password:	
Full Domain Name:	[redacted] Test
Organization Unit:	CN=Computers,DC=WIN:
System Name:	5610V5
	Alphanumeric characters are recommended.
Overwrite System Name:	□ Enable
Domain Status:	Joined domain

3. Provide the ADAudit Plus user account with administrator-level privileges.



OceanStor DeviceManager

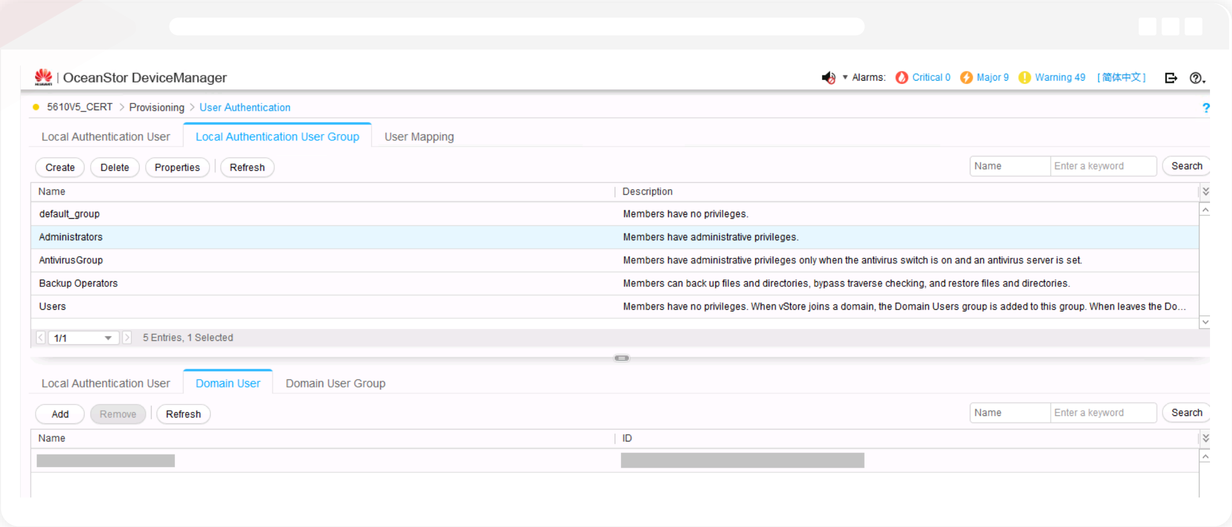
5610V5_CERT > Settings > Permission Settings

For optimal service system reliability and service data security, create users and allocate proper permissions to them to control their operations.

Current user: admin(Super administrator)

Username	Level	Type	Online/Offline	Password Status	Role
[redacted]	Super administrator	Local user	Online	Normal	Super administrator
[redacted]	Administrator	LDAP user	Offline	Normal	Administrator
[redacted]	Administrator	LDAP user	Offline	Normal	Administrator
[redacted]	Administrator	LDAP user	Online	Normal	Administrator
[redacted]	Administrator	LDAP user	Online	Normal	Administrator

4. Provide the user with permission to access shares.



OceanStor DeviceManager
Alarms: Critical 0 Major 9 Warning 49 [简体中文]

5610V5_CERT > Provisioning > User Authentication

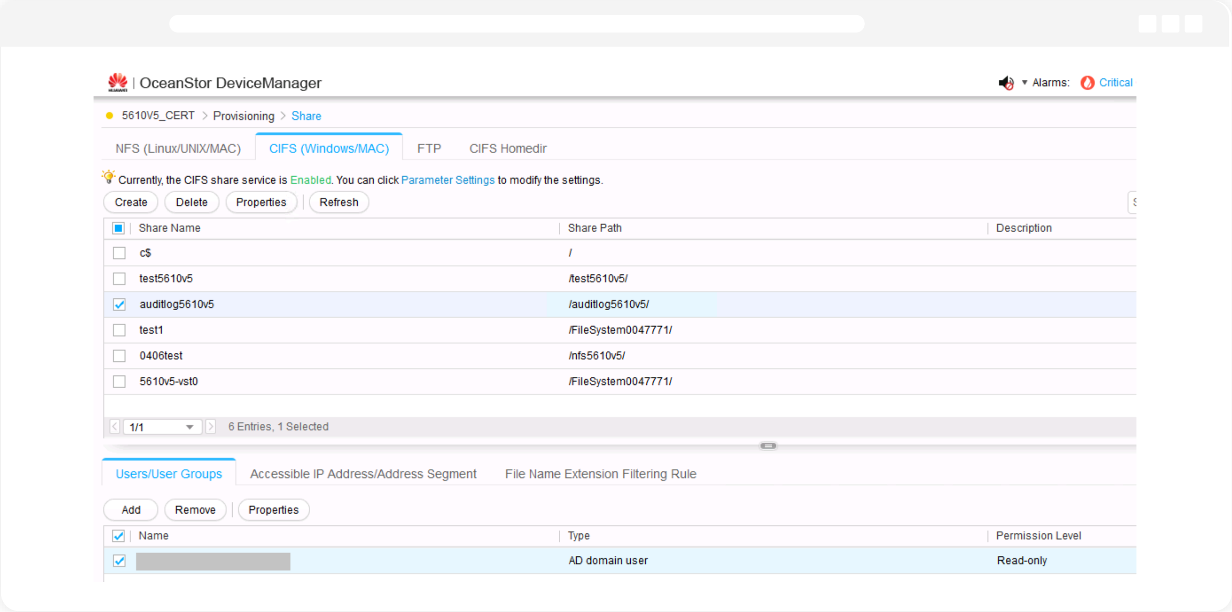
Local Authentication User
Local Authentication User Group
User Mapping
Create
Delete
Properties
Refresh
Name
Enter a keyword
Search

Name	Description
default_group	Members have no privileges.
Administrators	Members have administrative privileges.
AntivirusGroup	Members have administrative privileges only when the antivirus switch is on and an antivirus server is set.
Backup Operators	Members can back up files and directories, bypass traverse checking, and restore files and directories.
Users	Members have no privileges. When vStore joins a domain, the Domain Users group is added to this group. When leaves the Do...

1/1 5 Entries, 1 Selected

Name	ID
[redacted]	[redacted]

5. Provide the user with permission to read the share paths of the target shares and the audit log.



5610V5_CERT > Provisioning > Share

Currently, the CIFS share service is Enabled. You can click Parameter Settings to modify the settings.

☑	Share Name	Share Path	Description
□	c$	/	
□	test5610v5	/test5610v5/	
☑	auditlog5610v5	/auditlog5610v5/	
□	test1	/FileSystem0047771/	
□	0406test	/nfs5610v5/	
□	5610v5-vst0	/FileSystem0047771/	

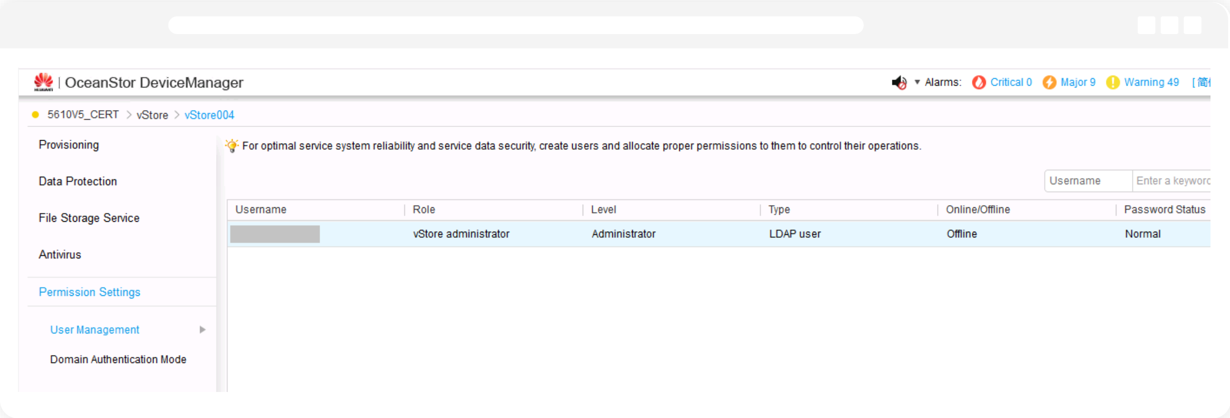
1/1 6 Entries, 1 Selected

Users/User Groups
Accessible IP Address/Address Segment
File Name Extension Filtering Rule
Add
Remove
Properties

☑	Name	Type	Permission Level
☑	[redacted]	AD domain user	Read-only

- **For OceanStor V5 series vStores**

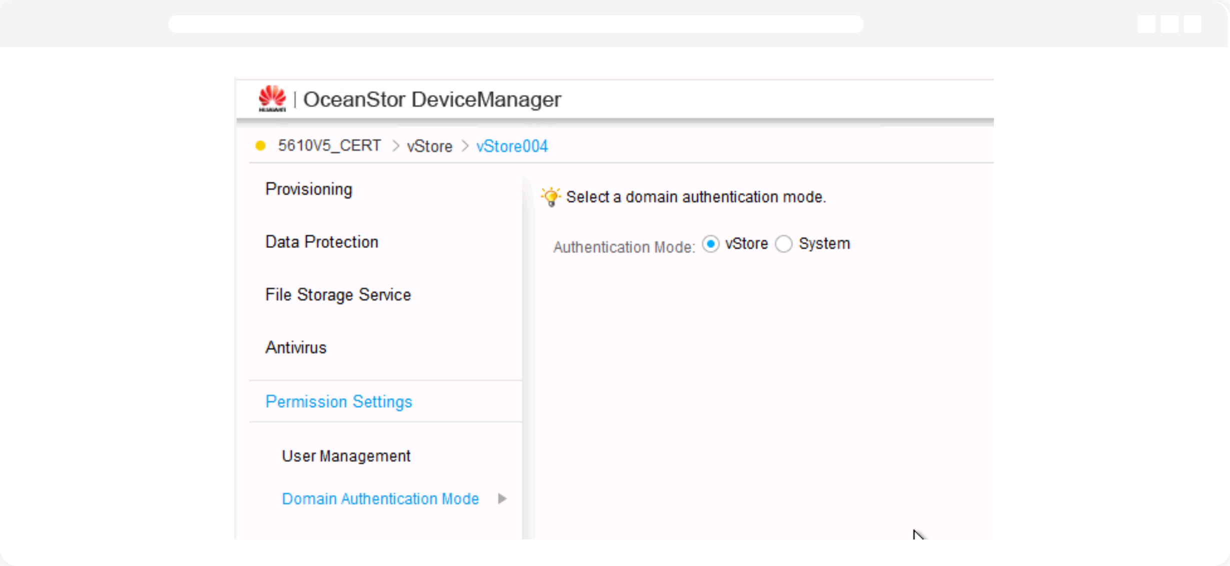
1. In **OceanStor DeviceManager**, give the ADAudit Plus user account administrator-level privileges and provide management permission.



For optimal service system reliability and service data security, create users and allocate proper permissions to them to control their operations.

Username	Role	Level	Type	Online/Offline	Password Status
[redacted]	vStore administrator	Administrator	LDAP user	Offline	Normal

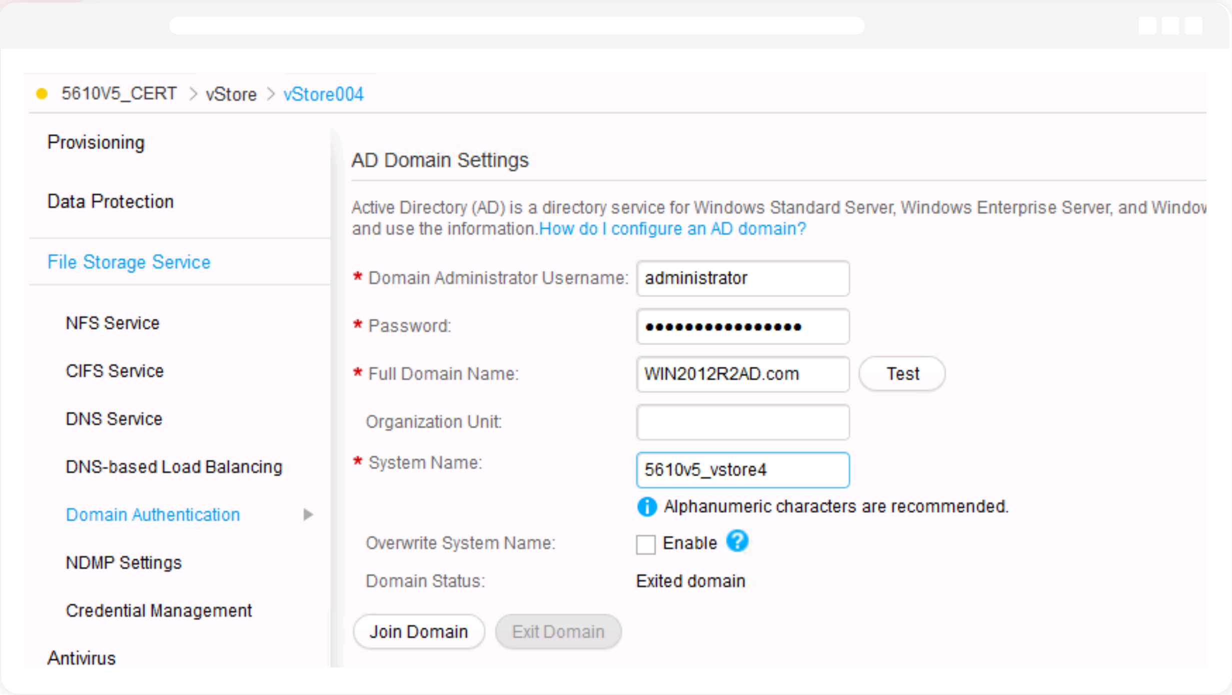
2. Ensure that the **Domain Authentication Mode** is set to **vStore.**



Select a domain authentication mode.

Authentication Mode: ● vStore ○ System

3. Join the **File Storage Service** to the AD domain by providing the necessary details under **Domain Authentication.**



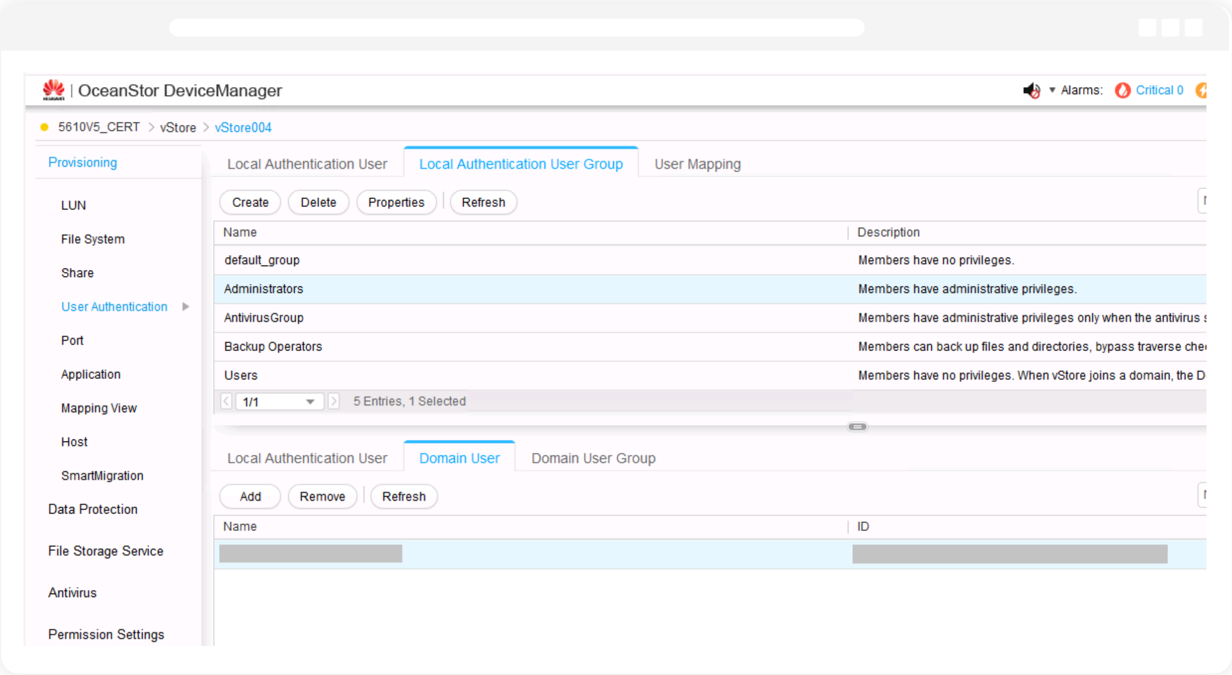
AD Domain Settings

Active Directory (AD) is a directory service for Windows Standard Server, Windows Enterprise Server, and Windov
and use the information.How do I configure an AD domain?

* Domain Administrator Username:	administrator
* Password:	●●●●●●●●●●●●●●●●
* Full Domain Name:	WIN2012R2AD.com Test
Organization Unit:	
* System Name:	5610v5_vstore4
	Alphanumeric characters are recommended.
Overwrite System Name:	□ Enable
Domain Status:	Exited domain

Join Domain Exit Domain

4. Add the user to the **Administrators** group and provide the user with permission to access the target shares.



Name	Description
default_group	Members have no privileges.
Administrators	Members have administrative privileges.
AntivirusGroup	Members have administrative privileges only when the antivirus s
Backup Operators	Members can back up files and directories, bypass traverse che
Users	Members have no privileges. When vStore joins a domain, the D

1/1 5 Entries, 1 Selected

Name	ID
[redacted]	[redacted]

5. Provide the user with permission to read the share paths of the target shares and the audit log.

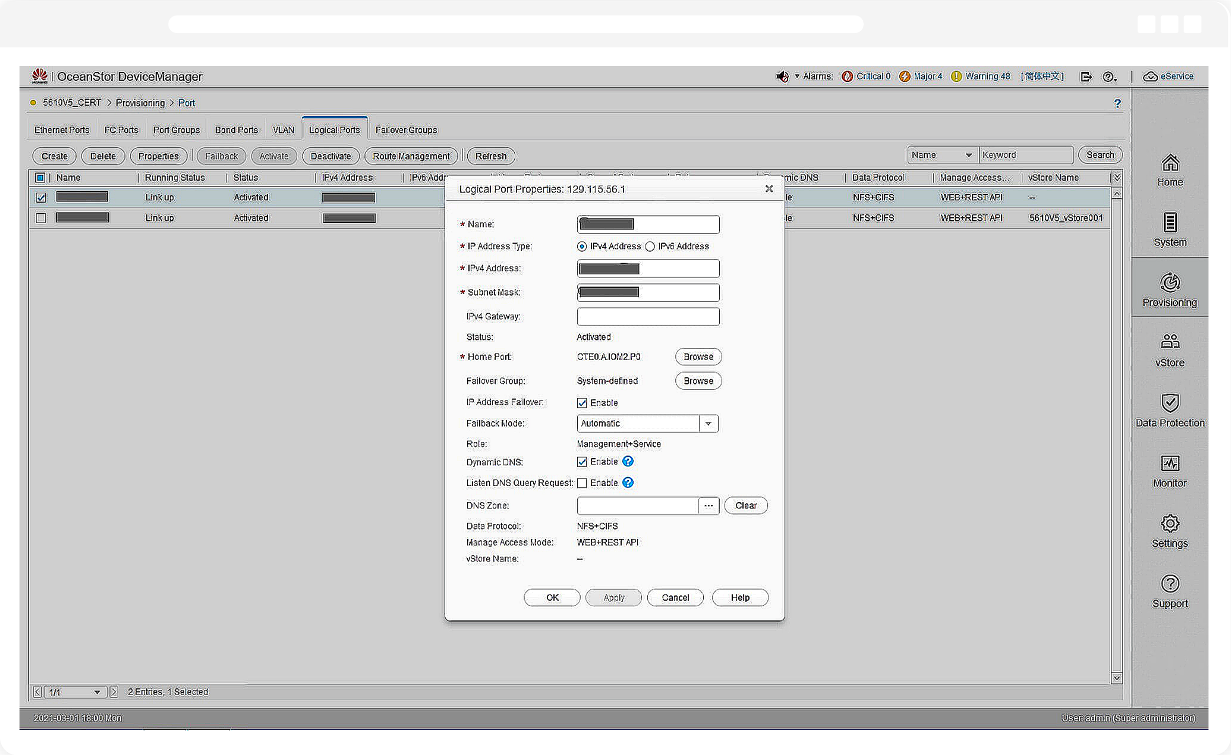
Configuration prerequisites

The settings below need to be configured prior to adding your OceanStor V5 series storage systems in ADAudit Plus.

1. In **OceanStor DeviceManager,** create a dedicated ADAudit Plus Huawei user account and provide it with the required minimum privileges according to the steps in this section.

2. Ensure that the OceanStor storage device's name resolves to an IP that serves as both the management and service IP.

3. Ensure that a logical port—that is not dedicated to a vStore—is set up for accessing the REST API.



☐	Name	Running Status	Status	IPv4 Address	IPv6 Addr...	...mic DNS	Data Protocol	Manage Access...	vStore Name
☑	[redacted]	Link up	Activated	[redacted]		...le	NFS+CIFS	WEB+REST API	--
☐	[redacted]	Link up	Activated	[redacted]		...le	NFS+CIFS	WEB+REST API	5610V5_vStore001

Logical Port Properties: 129.115.56.1

* Name: [redacted]
* IP Address Type: ● IPv4 Address ○ IPv6 Address
* IPv4 Address: [redacted]
* Subnet Mask: [redacted]
IPv4 Gateway:
Status: Activated
* Home Port: CTE0.A.IOM2.P0 Browse
Failover Group: System-defined Browse
IP Address Failover: ☑ Enable
Failback Mode: Automatic
Role: Management+Service
Dynamic DNS: ☑ Enable
Listen DNS Query Request: ☐ Enable
DNS Zone: Clear
Data Protocol: NFS+CIFS
Manage Access Mode: WEB+REST API
vStore Name: --

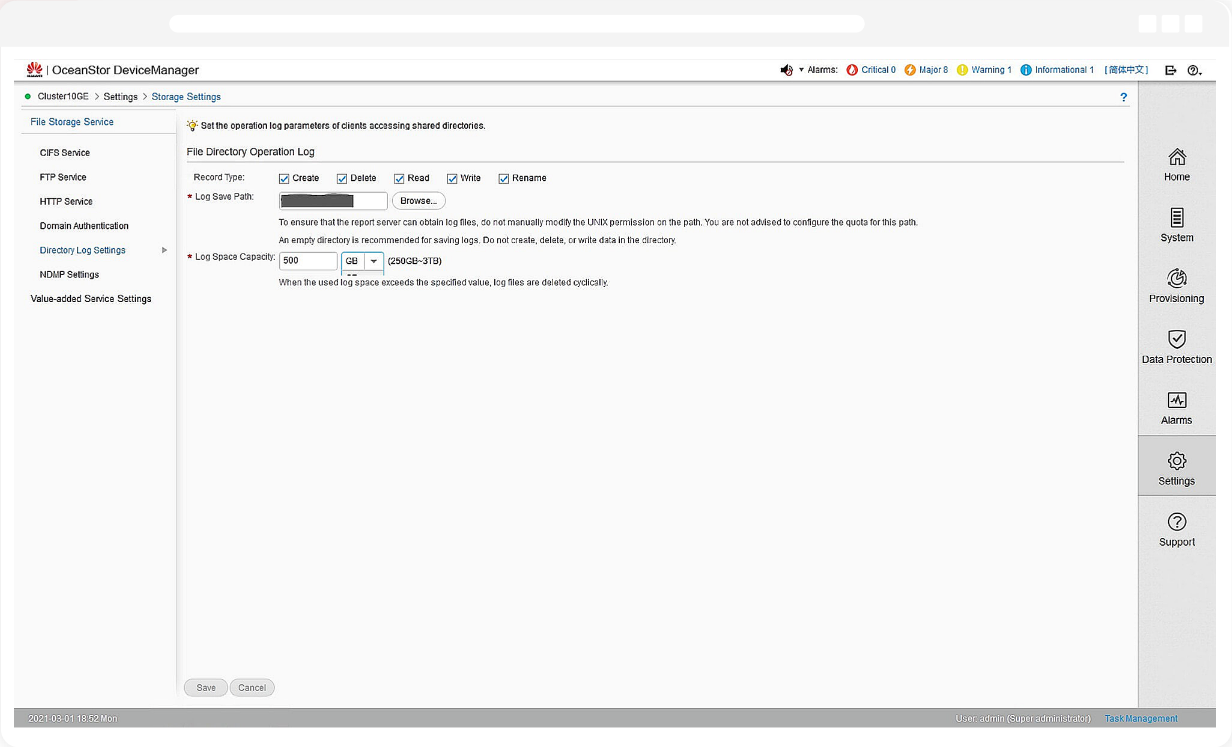
OK Apply Cancel Help

Enabling auditing

Follow the steps below to configure auditing in your target OceanStor V5 series vStores.

1. To view the ACL values before and after permission change and owner change events, log on to the **ADAudit Plus** web console, go to **Admin > Configuration > Alert/Report Settings**, and enable **Show detailed permission changes for NAS devices.**

2. Open **OceanStor DeviceManager** and enable auditing under **Settings > Storage Settings > Directory Log Settings > File Directory Operation Log**. Select the events you wish to audit.



Set the operation log parameters of clients accessing shared directories.

File Directory Operation Log

Record Type: ☑ Create ☑ Delete ☑ Read ☑ Write ☑ Rename

* Log Save Path: [redacted] Browse...

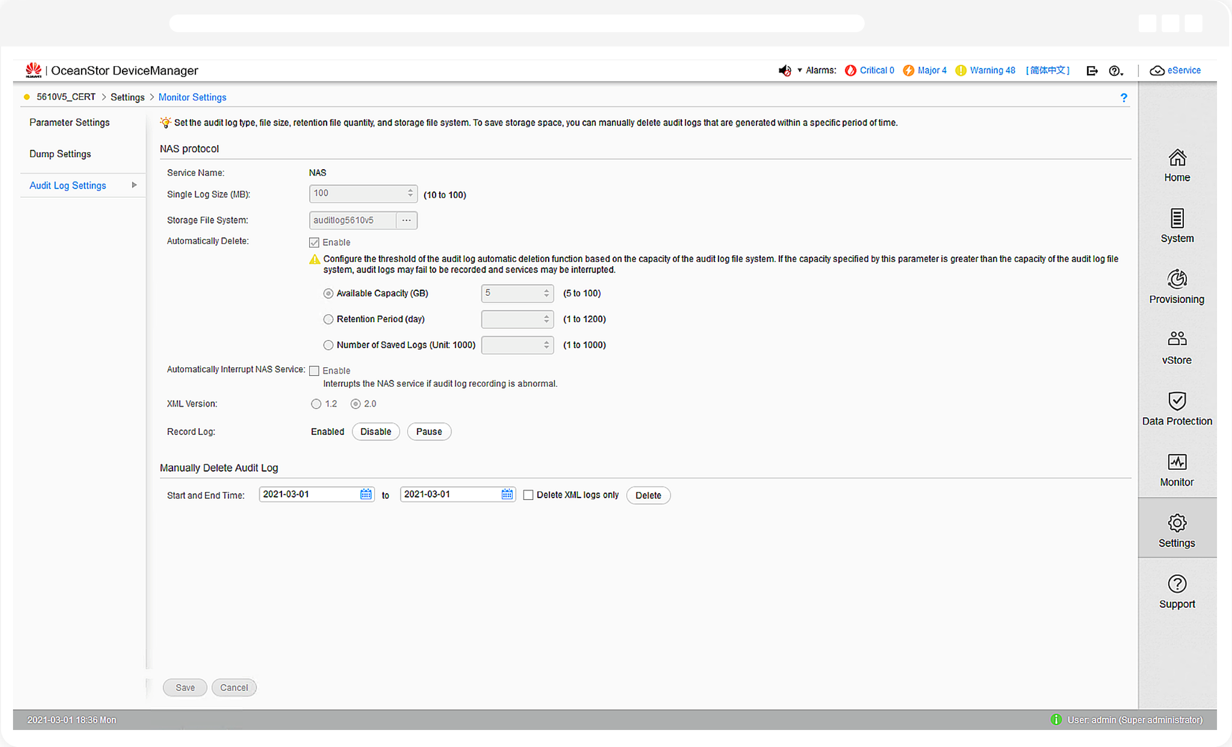
To ensure that the report server can obtain log files, do not manually modify the UNIX permission on the path. You are not advised to configure the quota for this path.

An empty directory is recommended for saving logs. Do not create, delete, or write data in the directory.

* Log Space Capacity: 500 GB (250GB~3TB)

When the used log space exceeds the specified value, log files are deleted cyclically.

3. Set the audit log location and purge settings. Set the logs to purge after seven days.



Set the audit log type, file size, retention file quantity, and storage file system. To save storage space, you can manually delete audit logs that are generated within a specific period of time.

NAS protocol

Service Name: NAS

Single Log Size (MB): 100 (10 to 100)

Storage File System: auditlog5610v5

Automatically Delete: ☑ Enable

Configure the threshold of the audit log automatic deletion function based on the capacity of the audit log file system. If the capacity specified by this parameter is greater than the capacity of the audit log file system, audit logs may fail to be recorded and services may be interrupted.

● Available Capacity (GB) 5 (5 to 100)

○ Retention Period (day) (1 to 1200)

○ Number of Saved Logs (Unit: 1000) (1 to 1000)

Automatically Interrupt NAS Service: □ Enable
Interrupts the NAS service if audit log recording is abnormal.

XML Version: ○ 1.2 ● 2.0

Record Log: Enabled Disable Pause

Manually Delete Audit Log

Start and End Time: 2021-03-01 to 2021-03-01 □ Delete XML logs only Delete

4. To filter out event noise and reduce the time it takes to generate logs, disable logon and logoff events in OceanStor V5 series by executing the commands below via SSH:

   (For vStores only)

   CLI command admin:/>change vstore view name=vStore004

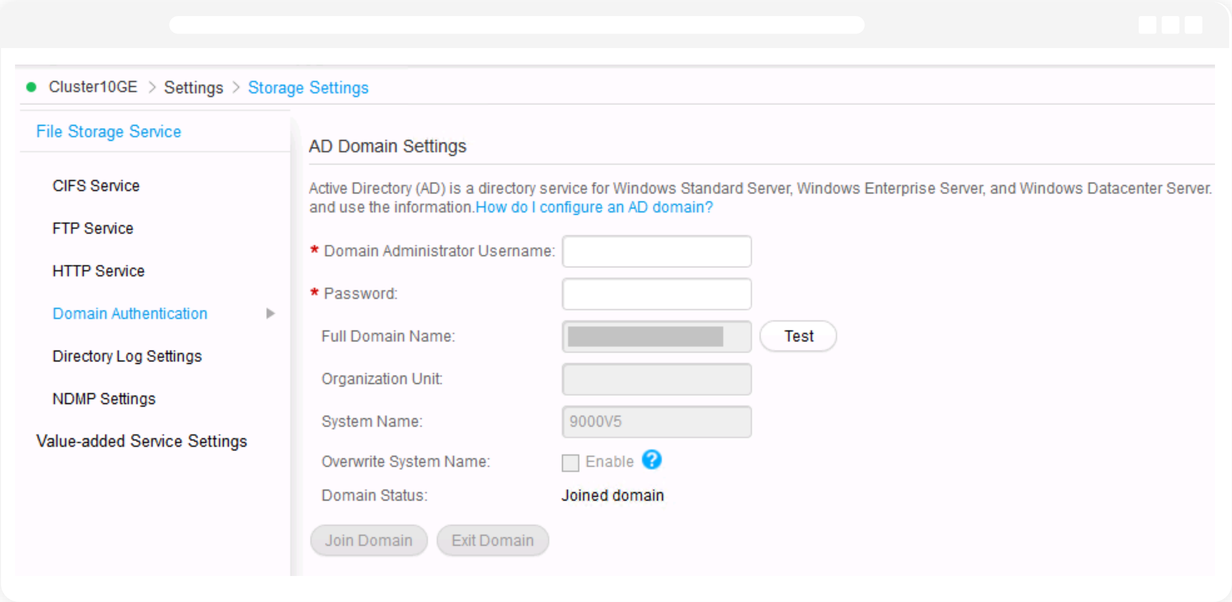
   CLI command admin:/>change service cifs logon_audit_disable=yes

Huawei OceanStor 9000 V5

Minimum privileges required

For OceanStor 9000 V5 storage systems, provide the necessary privileges to the user configured in the Domain Settings of ADAudit Plus (in the top-right corner of the console and referred to below as the Domain Settings user), or create a dedicated ADAudit Plus Huawei user account and provide it with the privileges below.

1. Join the **File Storage Service** to the AD domain by providing the necessary details under **Domain Authentication.**



AD Domain Settings

Active Directory (AD) is a directory service for Windows Standard Server, Windows Enterprise Server, and Windows Datacenter Server. and use the information.How do I configure an AD domain?

* Domain Administrator Username:

* Password:

Full Domain Name: [redacted]

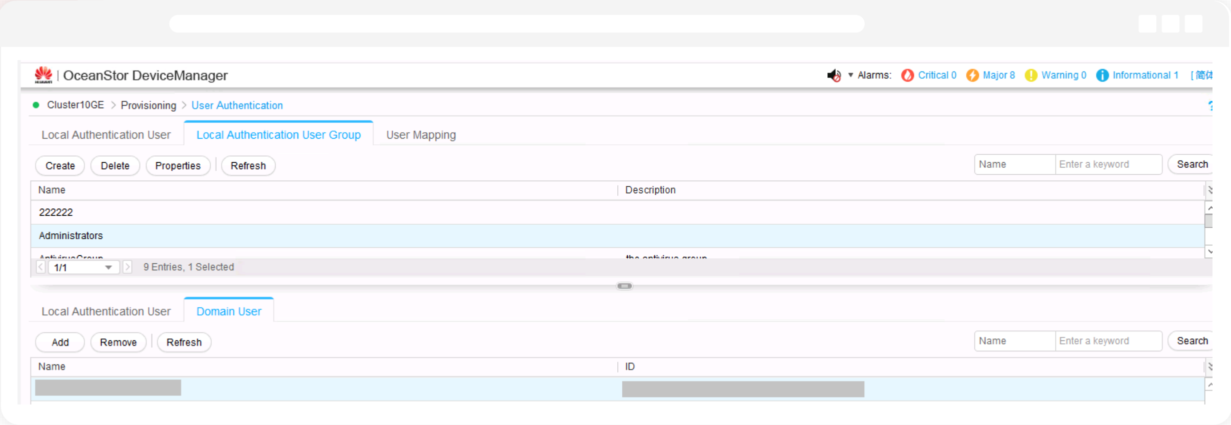
Organization Unit:

System Name: 9000V5

Overwrite System Name: □ Enable

Domain Status: Joined domain

2. Provide the Domain Settings user with permission to access the target shares.



OceanStor DeviceManager
Alarms: Critical 0 Major 8 Warning 0 Informational 1 [简体

● Cluster10GE > Provisioning > User Authentication

Local Authentication User
Local Authentication User Group
User Mapping
Create
Delete
Properties
Refresh
Search

Name: Enter a keyword

Name	Description
222222	
Administrators	
AntivirusGroup	the antivirus group

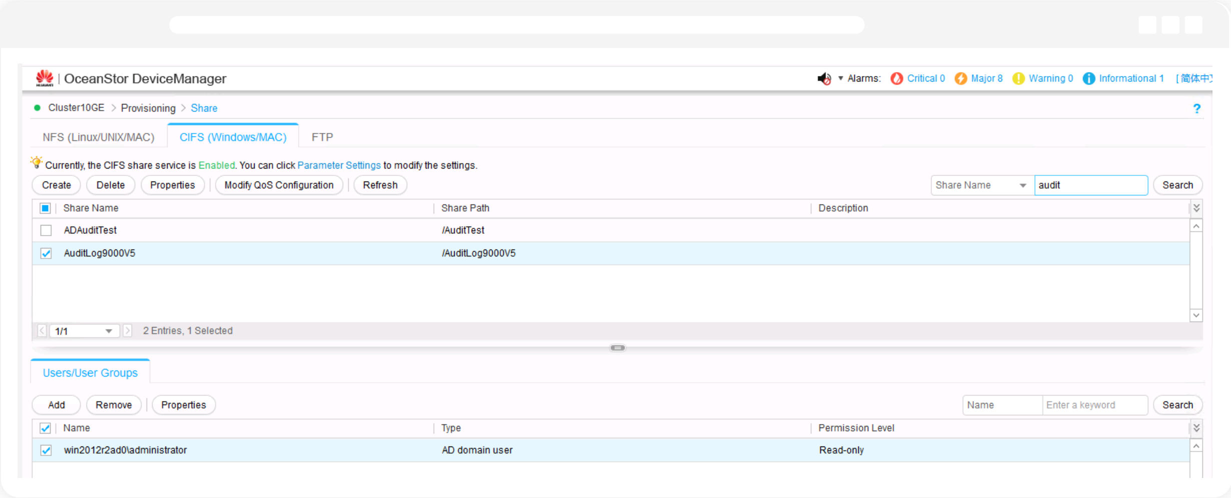
1/1 9 Entries, 1 Selected

Local Authentication User
Domain User
Add
Remove
Refresh
Search

Name: Enter a keyword

Name	ID
[redacted]	[redacted]

3. Provide the Domain Settings user with permission to read the share paths of the target shares and the audit log.



OceanStor DeviceManager
Alarms: Critical 0 Major 8 Warning 0 Informational 1 [简体中]
?

● Cluster10GE > Provisioning > Share

Currently, the CIFS share service is Enabled. You can click Parameter Settings to modify the settings.

Share Name: audit

■	Share Name	Share Path	Description
□	ADAuditTest	/AuditTest	
☑	AuditLog9000V5	/AuditLog9000V5	

1/1 2 Entries, 1 Selected

Name: Enter a keyword

☑	Name	Type	Permission Level
☑	win2012r2ad0\administrator	AD domain user	Read-only

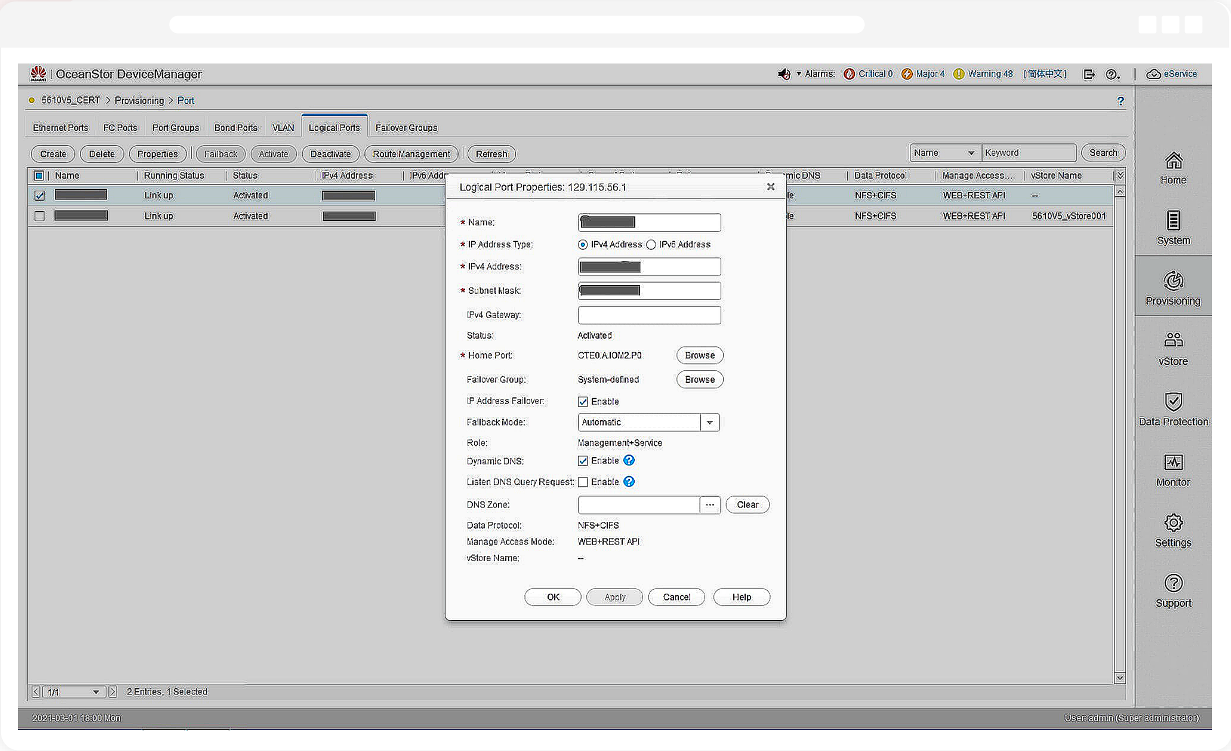
Configuration prerequisites

The settings below need to be configured prior to adding your OceanStor 9000 V5 storage systems in ADAudit Plus.

1. Create a dedicated ADAudit Plus Huawei user account and provide it with the required minimum privileges according to the steps in this section.

2. Ensure that the OceanStor storage device's name resolves to an IP that serves as the management IP.

3. Ensure that a logical port—that is not dedicated to a vStore—is set up for accessing the REST API.



	Name	Running Status	Status	IPv4 Address	IPv6 Addr	…	…mic DNS	Data Protocol	Manage Access…	vStore Name
☑	[redacted]	Link up	Activated	[redacted]			…le	NFS+CIFS	WEB+REST API	--
□	[redacted]	Link up	Activated	[redacted]			…le	NFS+CIFS	WEB+REST API	5610V5_vStore001

Logical Port Properties: 129.115.56.1

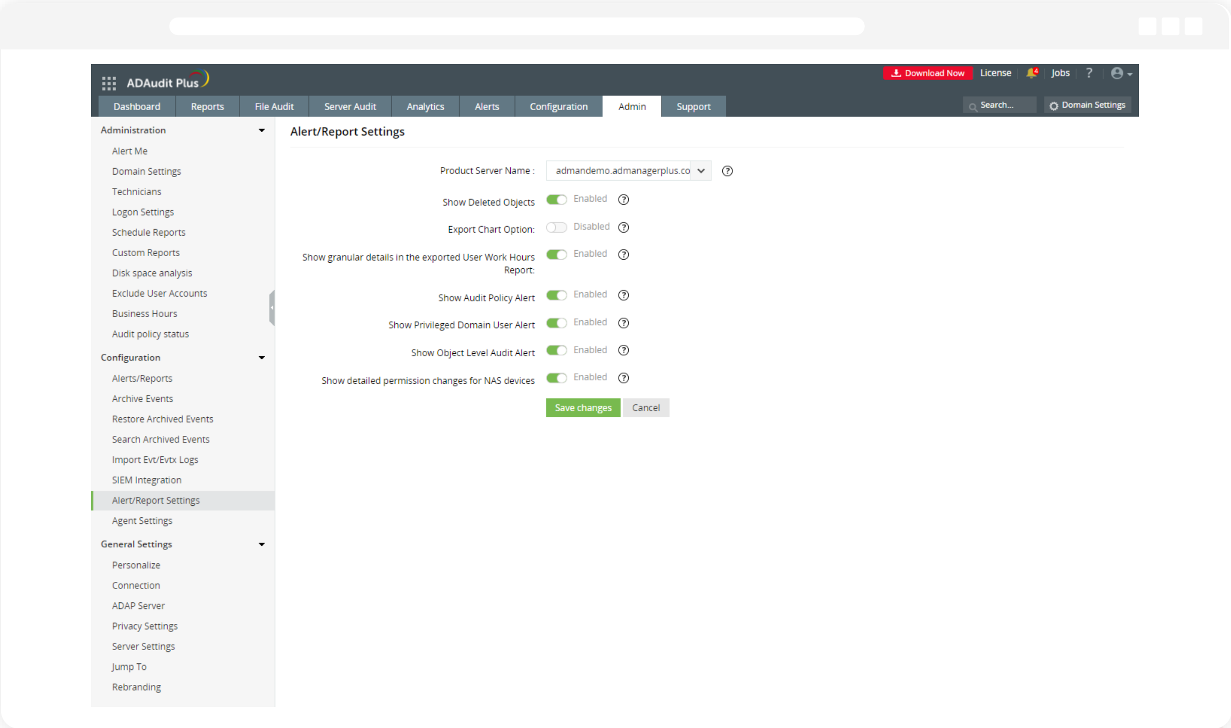
* Name: [redacted]
* IP Address Type: ● IPv4 Address ○ IPv6 Address
* IPv4 Address: [redacted]
* Subnet Mask: [redacted]
IPv4 Gateway:
Status: Activated
* Home Port: CTE0.A.IOM2.P0 Browse
Failover Group: System-defined Browse
IP Address Failover: ☑ Enable
Failback Mode: Automatic
Role: Management+Service
Dynamic DNS: ☑ Enable
Listen DNS Query Request: □ Enable
DNS Zone: Clear
Data Protocol: NFS+CIFS
Manage Access Mode: WEB+REST API
vStore Name: --

OK Apply Cancel Help

Enabling auditing

Follow the steps below to configure auditing in your target OceanStor 9000 V5 storage devices.

1. To view the ACL values before and after permission change and owner change events, log on to the **ADAudit Plus** web console, go to **Admin > Configuration > Alert/Report Settings,** and enable **Show detailed permission changes for NAS devices.**

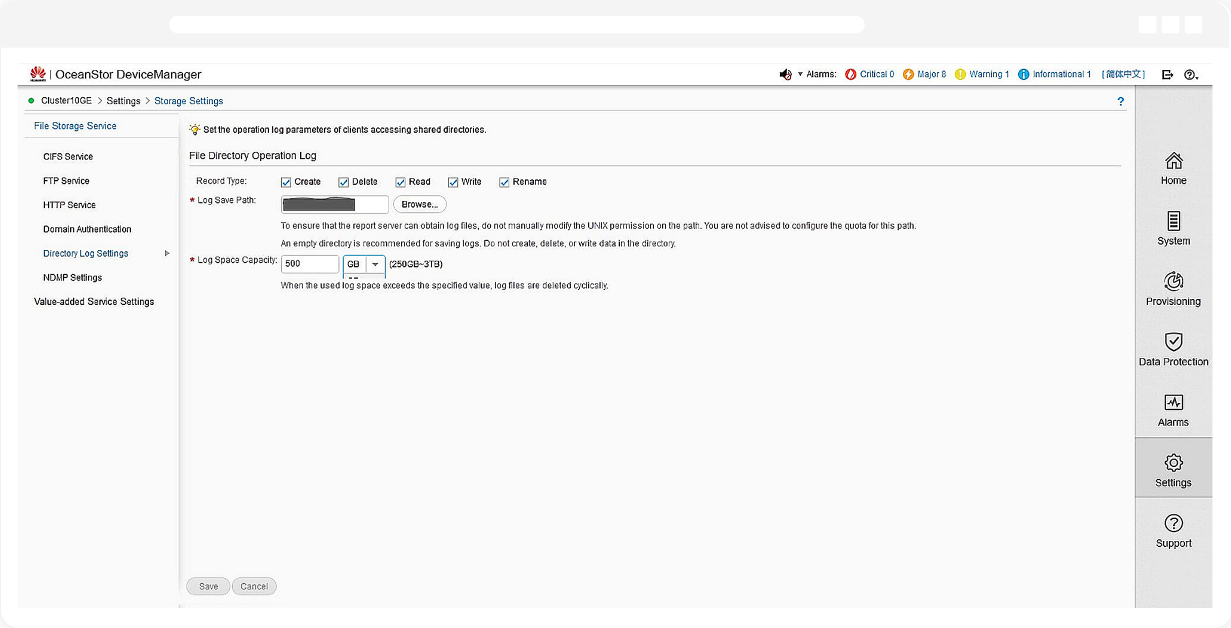


Alert/Report Settings

Product Server Name : admandemo.admanagerplus.co
Show Deleted Objects: Enabled
Export Chart Option: Disabled
Show granular details in the exported User Work Hours Report: Enabled
Show Audit Policy Alert: Enabled
Show Privileged Domain User Alert: Enabled
Show Object Level Audit Alert: Enabled
Show detailed permission changes for NAS devices: Enabled

Save changes Cancel

2. Open **OceanStor DeviceManager** and enable auditing under **Settings > Storage Settings > Directory Log Settings > File Directory Operation Log**. Select the events you wish to audit.



Set the operation log parameters of clients accessing shared directories.

File Directory Operation Log

Record Type: ☑ Create ☑ Delete ☑ Read ☑ Write ☑ Rename

* Log Save Path: [redacted]

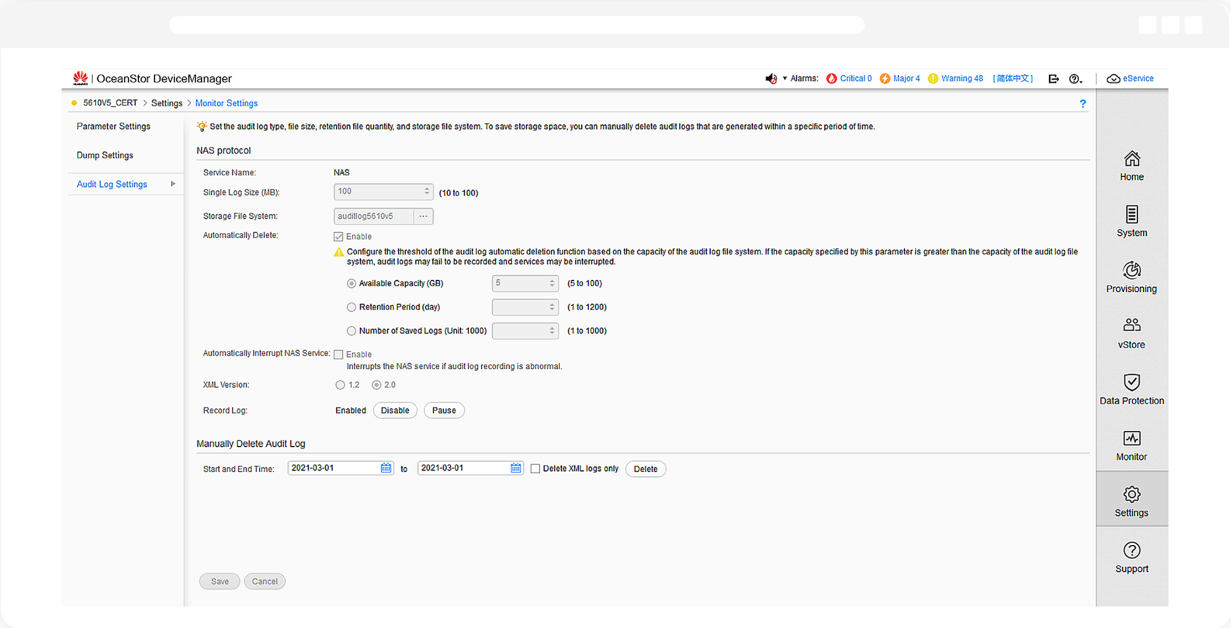
To ensure that the report server can obtain log files, do not manually modify the UNIX permission on the path. You are not advised to configure the quota for this path.

An empty directory is recommended for saving logs. Do not create, delete, or write data in the directory.

* Log Space Capacity: 500 GB (250GB~3TB)

When the used log space exceeds the specified value, log files are deleted cyclically.

3. Set the audit log location and purge settings. Set the logs to purge after reaching 20GB.



Set the audit log type, file size, retention file quantity, and storage file system. To save storage space, you can manually delete audit logs that are generated within a specific period of time.

NAS protocol

Service Name: NAS

Single Log Size (MB): 100 (10 to 100)

Storage File System: auditlog5610v5

Automatically Delete: ☑ Enable

Configure the threshold of the audit log automatic deletion function based on the capacity of the audit log file system. If the capacity specified by this parameter is greater than the capacity of the audit log file system, audit logs may fail to be recorded and services may be interrupted.

● Available Capacity (GB) 5 (5 to 100)

○ Retention Period (day) (1 to 1200)

○ Number of Saved Logs (Unit: 1000) (1 to 1000)

Automatically Interrupt NAS Service: □ Enable

Interrupts the NAS service if audit log recording is abnormal.

XML Version: ○ 1.2 ● 2.0

Record Log: Enabled

Manually Delete Audit Log

Start and End Time: 2021-03-01 to 2021-03-01 □ Delete XML logs only

4. To filter out event noise and reduce the time it takes to generate logs, disable logon and logoff events in OceanStor 9000 V5 by executing the commands below via SSH:

(For vStores only)

CLI command admin:/>change vstore view name=vStore004

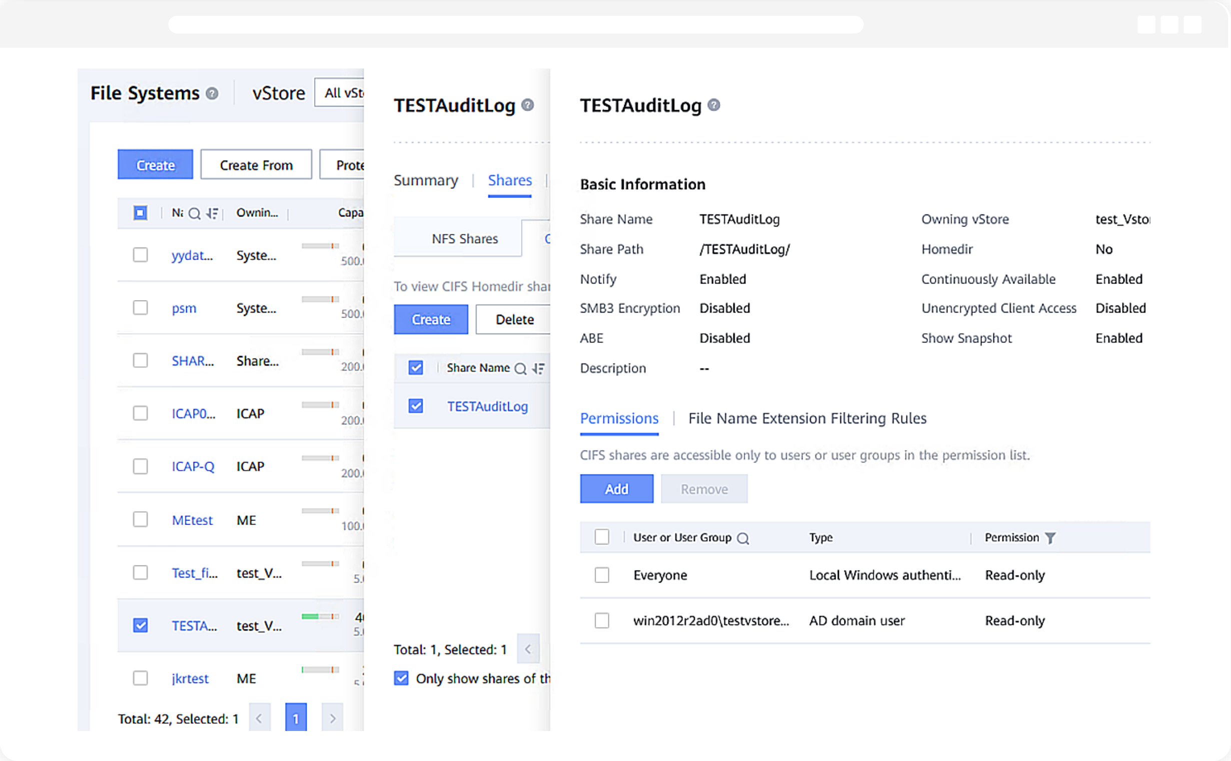
CLI command admin:/>change service cifs logon_audit_disable=yes

Huawei OceanStor Dorado All-Flash Storage and OceanStor Hybrid Flash Storage

Minimum privileges required

For OceanStor Dorado All-Flash Storage and OceanStor Hybrid Flash Storage, provide the necessary privileges to the user configured in the **Domain Settings** of **ADAudit Plus** (in the top-right corner of the console and referred to below as the Domain Settings user), or create a dedicated ADAudit Plus Huawei user account and provide it with the privileges below.

1. Provide the user with read-only access to the share where the audit logs are located. To check that the Domain Settings user has this access in **OceanStor DeviceManager**, go to **Services > File Service > File Systems**, select the share with the audit logs, and view the permissions to the audit log share path.



■	N:	Ownin...	Capa
□	yydat...	Syste...	500.
□	psm	Syste...	500.
□	SHAR...	Share...	200.
□	ICAP0...	ICAP	200.
□	ICAP-Q	ICAP	200.
□	MEtest	ME	100.
□	Test_fi...	test_V...	5.
☑	TESTA...	test_V...	4 5.
□	jkrtest	ME	5

Total: 42, Selected: 1

To view CIFS Homedir shar

☑	Share Name
☑	TESTAuditLog

Total: 1, Selected: 1

☑ Only show shares of th

TESTAuditLog

Basic Information

Share Name	TESTAuditLog	Owning vStore	test_Vsto
Share Path	/TESTAuditLog/	Homedir	No
Notify	Enabled	Continuously Available	Enabled
SMB3 Encryption	Disabled	Unencrypted Client Access	Disabled
ABE	Disabled	Show Snapshot	Enabled
Description	--		

CIFS shares are accessible only to users or user groups in the permission list.

□	User or User Group	Type	Permission
□	Everyone	Local Windows authenti...	Read-only
□	win2012r2ad0\testvstore...	AD domain user	Read-only

2. Ensure that the Domain Settings user has read-only access to the shares you want to audit with ADAudit Plus.

Configuration prerequisites

The settings below need to be configured prior to adding your OceanStor Dorado All-Flash Storage and OceanStor Hybrid Flash Storage systems in ADAudit Plus.

1. Create a dedicated ADAudit Plus Huawei user account and provide it with the required minimum privileges according to the steps in this section.

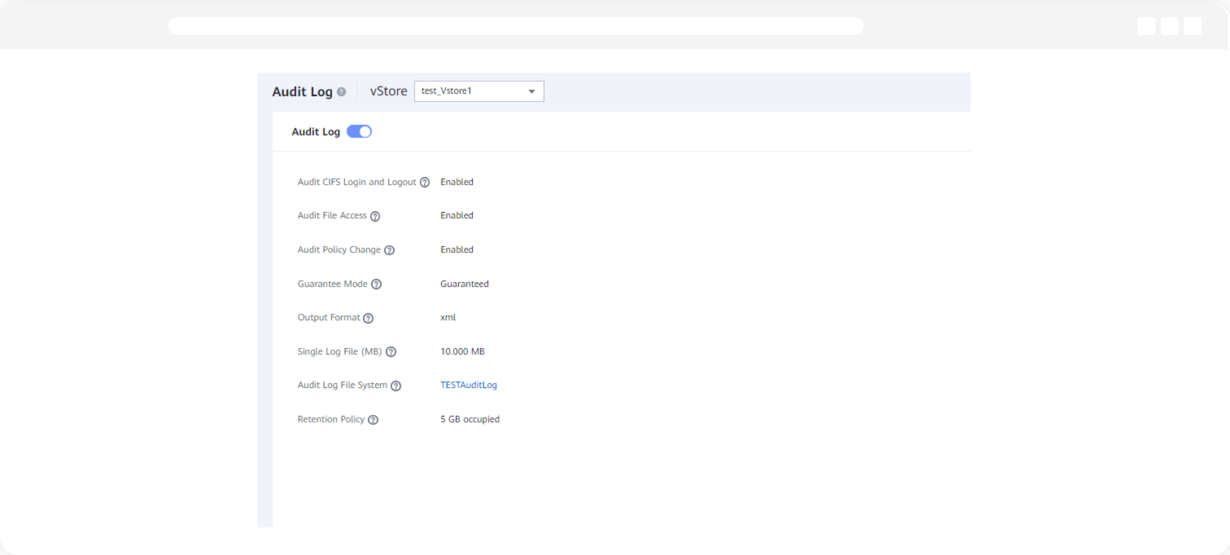
2. Ensure that the OceanStor storage device's name resolves to an IP that serves as both the management and service IP. However, if you already have an IP that serves only as the service IP, you can still proceed with it.

3. Ensure that a logical IP—that is dedicated to a vStore—is set up for accessing the REST API. If you have not created a management IP, you can skip this step and proceed.

Enabling auditing

Follow the steps below to configure auditing in your target OceanStor Dorado All-Flash Storage and OceanStor Hybrid Flash Storage devices.

1. If you have set up the management IP, configure an administrator account to access the REST API.
   i. **In OceanStor DeviceManager**, go to **Services > vStore Service > vStores** and select the vStore that you want to audit.
   Go to **User Management > Create** and add an LDAP user.
2. Configure audit log settings.
   Go to **Settings > File Service > Audit Log** and select the vStore from the drop-down.
   i. Select **xml** as the *Output Format.*
   ii. Input your desired log file size in megabytes in the *Single Log File (MB)* field. By default, this will be set to 100MB.



Audit Log | vStore test_Vstore1

Audit Log

Audit CIFS Login and Logout	Enabled
Audit File Access	Enabled
Audit Policy Change	Enabled
Guarantee Mode	Guaranteed
Output Format	xml
Single Log File (MB)	10.000 MB
Audit Log File System	TESTAuditLog
Retention Policy	5 GB occupied

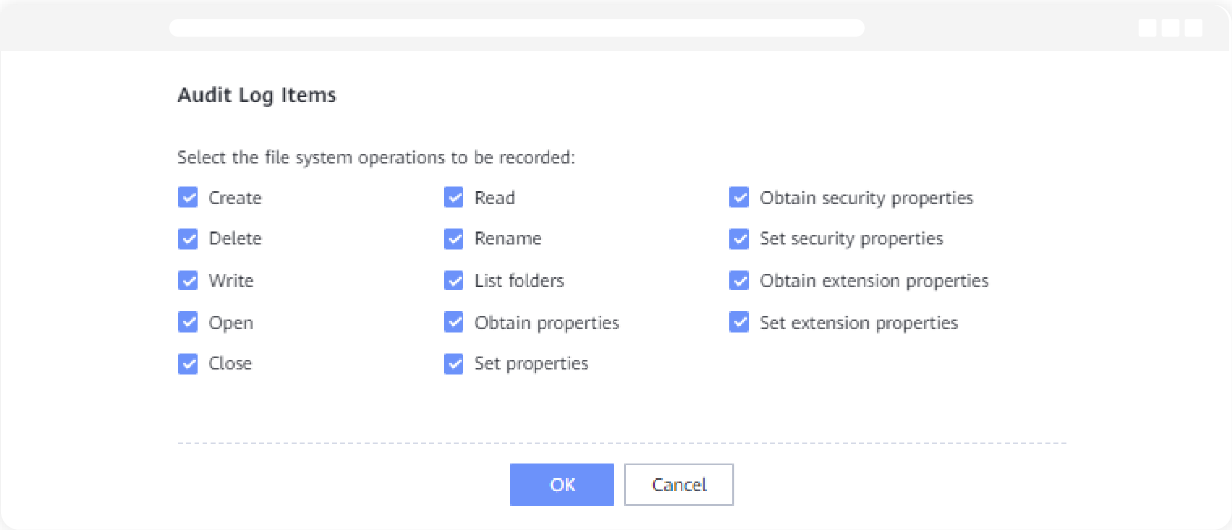
3. Configure auditing options for the domain.

   Go to **Services > File Service > File Systems.**

   i. Select the vStore and file system you want to audit.

   In the top-right corner, click **More** and select **Modify.**

   ii. Enable auditing and select the file system operations you want to audit.



Audit Log Items

Select the file system operations to be recorded:

☑ Create
☑ Delete
☑ Write
☑ Open
☑ Close

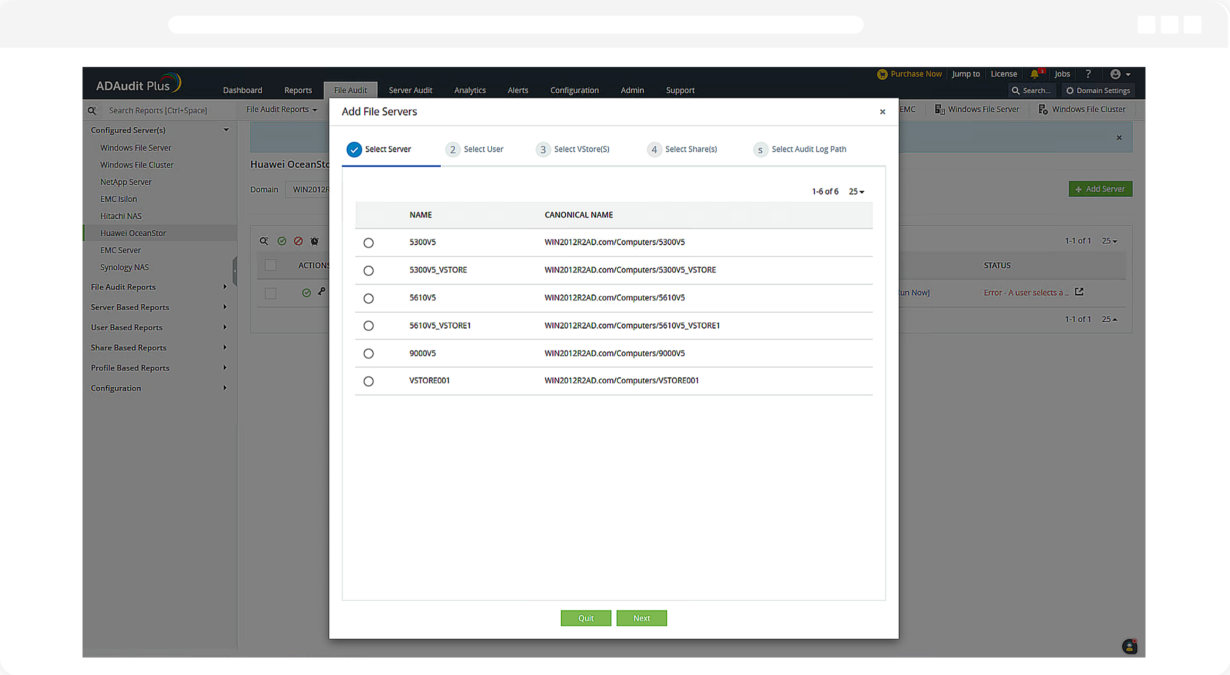
☑ Read
☑ Rename
☑ List folders
☑ Obtain properties
☑ Set properties

☑ Obtain security properties
☑ Set security properties
☑ Obtain extension properties
☑ Set extension properties

Adding Huawei OceanStor systems in ADAudit Plus

To add a Huawei OceanStor storage system to the ADAudit Plus console, follow the steps below.

1. Log on to the **ADAudit Plus** web console.
2. Go to **File Audit > Configured Server(s) > Huawei OceanStor.**
3. Click **+ Add Server** in the top-right corner. This will open the *Add File Servers* pop-up.
4. Select the storage system you wish to audit with ADAudit Plus. In case the server has a different AD join name and vStore name, the former will be displayed in the pop-up. Here, for an OceanStor V5 series system, always select the storage system **vStore0** for all the vStores.
5. Click **Next.**



Add File Servers

Select Server · 2 Select User · 3 Select VStore(S) · 4 Select Share(s) · 5 Select Audit Log Path

1-6 of 6 25

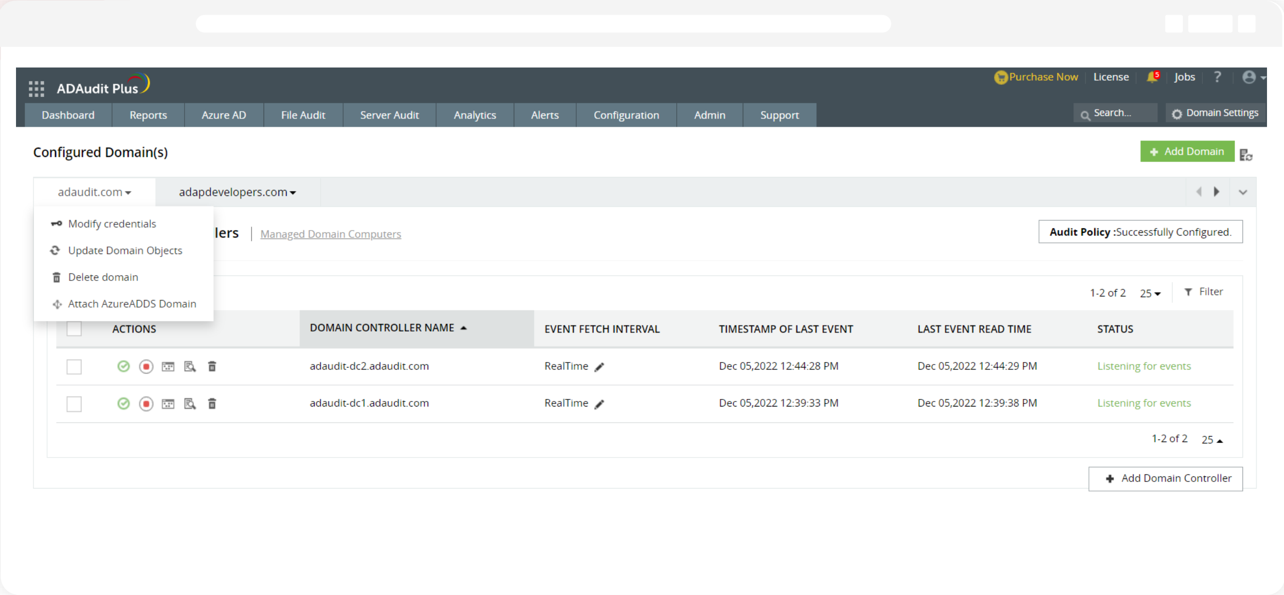
	NAME	CANONICAL NAME
○	5300V5	WIN2012R2AD.com/Computers/5300V5
○	5300V5_VSTORE	WIN2012R2AD.com/Computers/5300V5_VSTORE
○	5610V5	WIN2012R2AD.com/Computers/5610V5
○	5610V5_VSTORE1	WIN2012R2AD.com/Computers/5610V5_VSTORE1
○	9000V5	WIN2012R2AD.com/Computers/9000V5
○	VSTORE001	WIN2012R2AD.com/Computers/VSTORE001

Quit Next

Troubleshooting tip

If the storage system you wish to audit is not listed in the Add File Servers pop-up, check that it is connected to the target domain. If it is, refresh the computer objects for that domain by following the steps below.

- In the **ADAudit Plus** console, go to **Domain Settings** in the top-right corner.
- From the domain drop-down, select **Update Domain Objects** to open the corresponding pop-up.
- Select **Computers** from the list and click **Save.**



Configured Domain(s)

adaudit.com ▾ | adapdevelopers.com ▾

lers | Managed Domain Computers

Audit Policy :Successfully Configured.

1-2 of 2 25 ▾

□	ACTIONS	DOMAIN CONTROLLER NAME ▲	EVENT FETCH INTERVAL	TIMESTAMP OF LAST EVENT	LAST EVENT READ TIME	STATUS
□		adaudit-dc2.adaudit.com	RealTime	Dec 05,2022 12:44:28 PM	Dec 05,2022 12:44:29 PM	Listening for events
□		adaudit-dc1.adaudit.com	RealTime	Dec 05,2022 12:39:33 PM	Dec 05,2022 12:39:38 PM	Listening for events

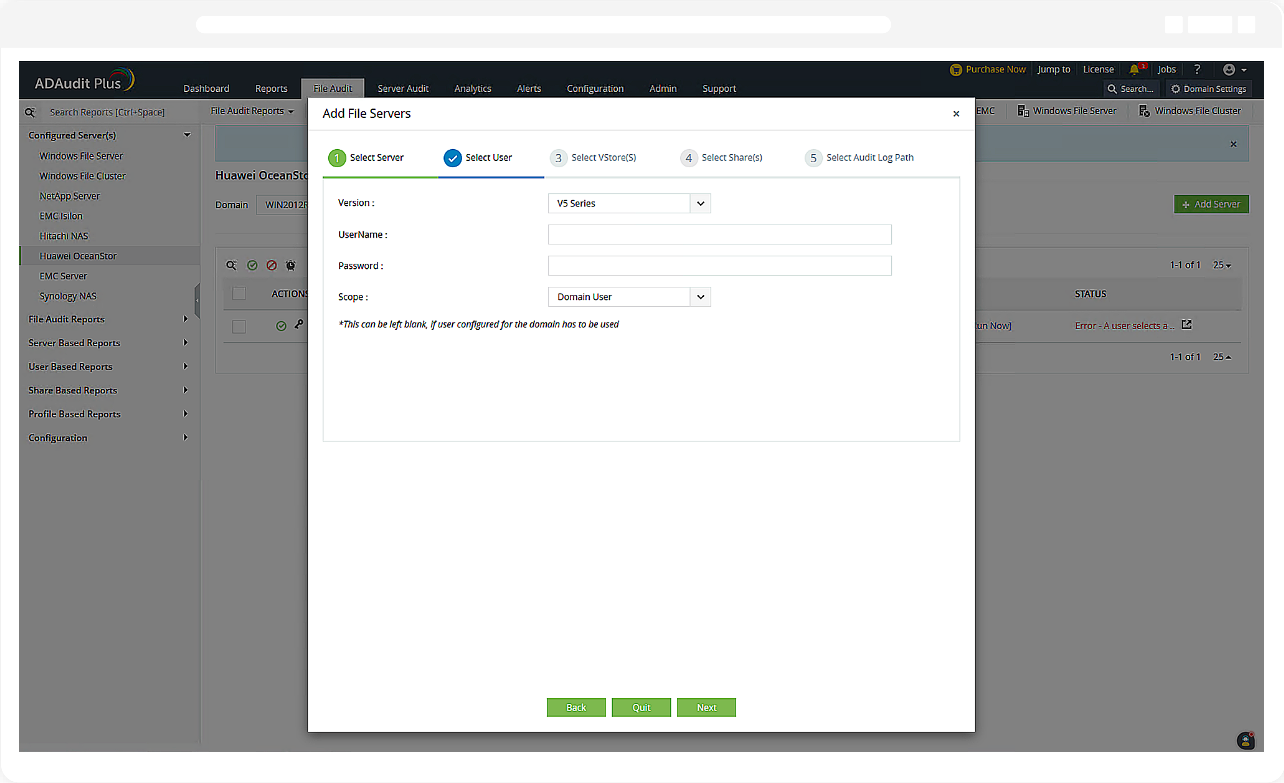
1-2 of 2 25 ▴

6. Now, provide the following details.

i. Provide the *Version* of the target OceanStor system: **V5 Series, 9000 V5**, or **V6.**

ii. If you are using a dedicated ADAudit Plus Huawei user account, provide the *UserName* and *Password.* If you are using a domain user account, ADAudit Plus will automatically use those credentials, and you can move to the next step.

iii. Provide the Scope of the provided user.



Add File Servers

1 Select Server | ✓ Select User | 3 Select VStore(S) | 4 Select Share(s) | 5 Select Audit Log Path

Version : V5 Series

UserName :

Password :

Scope : Domain User

**This can be left blank, if user configured for the domain has to be used*

Troubleshooting tip

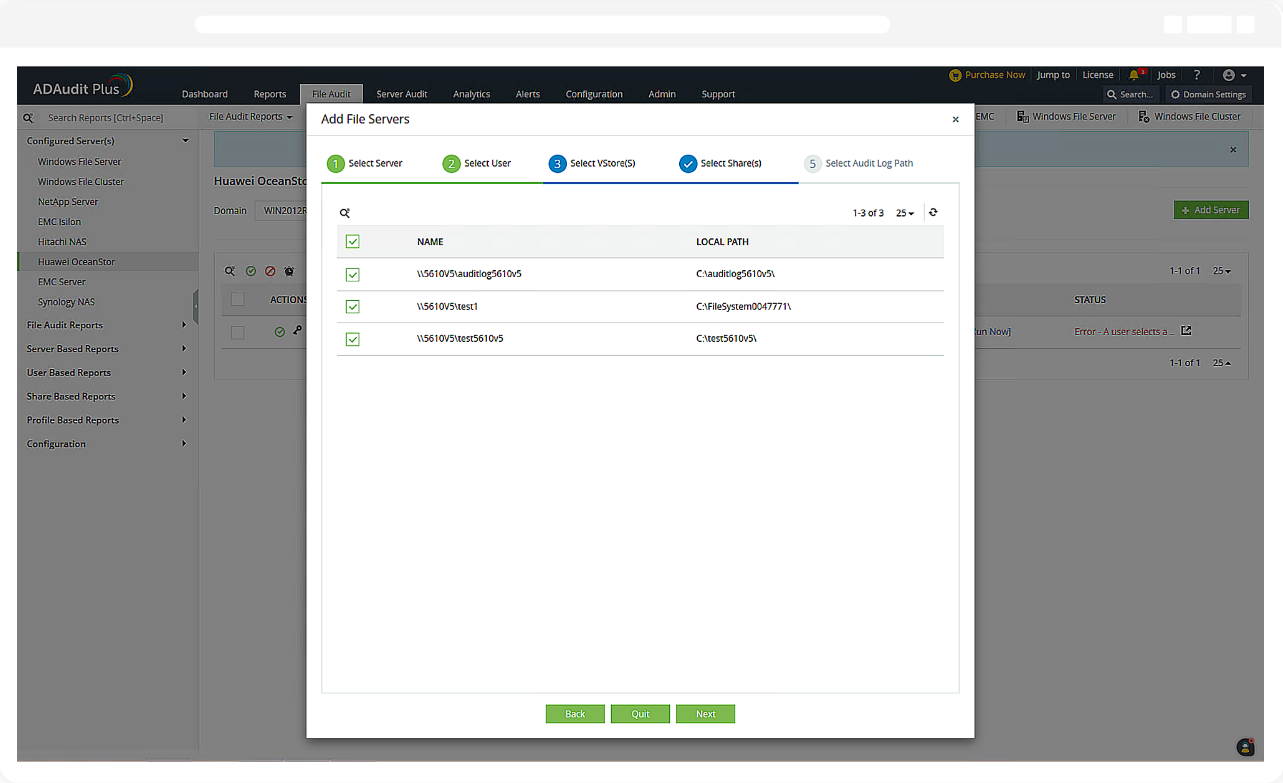
If you encounter an error while adding the ADAudit Plus Huawei user's credentials, check that the user has the required minimum privileges.

7. Select the target vStore and click **Next**. For OceanStor 9000 V5, this step is not required.

Troubleshooting tip

If no vStores are listed, or if only the system or default vStores are listed, check that the ADAudit Plus Huawei user has the required minimum privileges. If the issue persists after the privileges have been assigned correctly, contact the support team at support@adauditplus.com for further assistance.

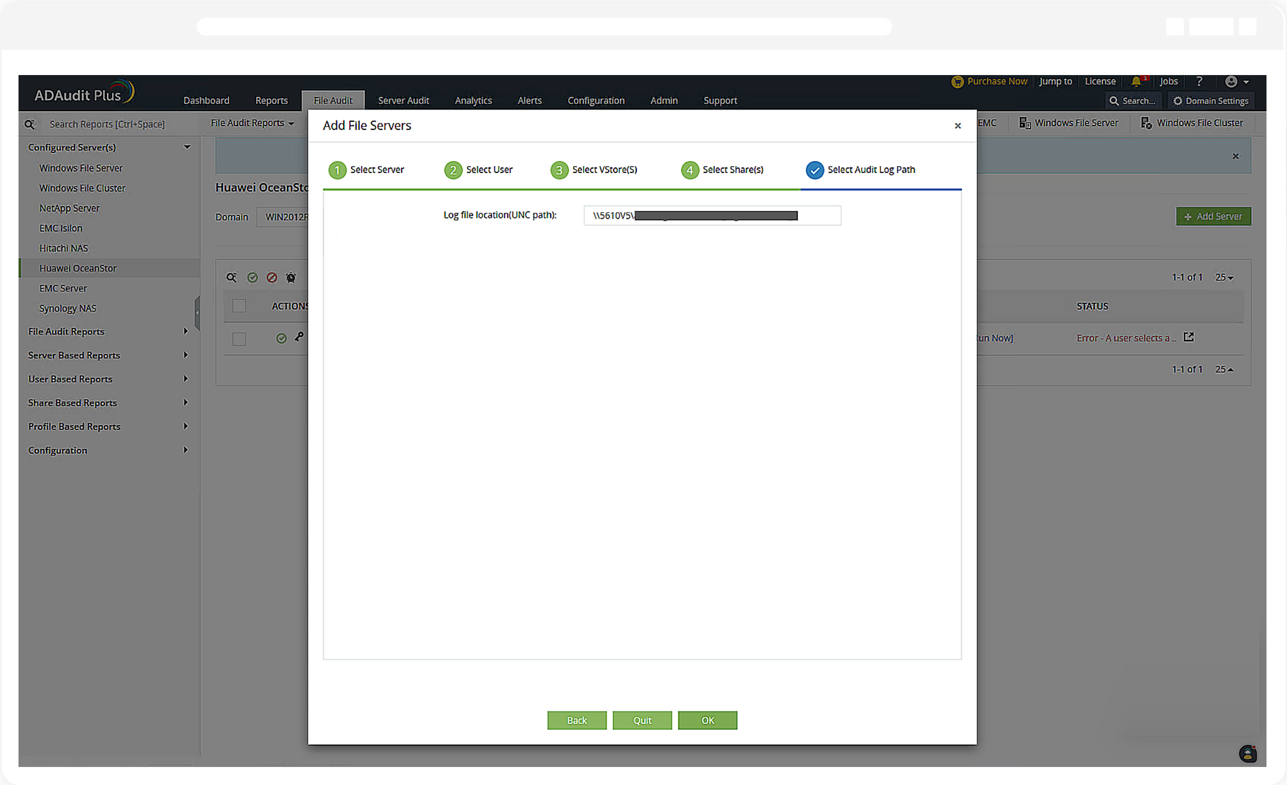
8. Select the shares you want to audit in the chosen vStore and click **Next.**



Add File Servers

☑	NAME	LOCAL PATH
☑	\\5610V5\auditlog5610v5	C:\auditlog5610v5\
☑	\\5610V5\test1	C:\FileSystem0047771\
☑	\\5610V5\test5610v5	C:\test5610v5\

9. Provide the Universal Naming Convention (UNC) path of the audit log's location. For OceanStor V5 series, the UNC path is discovered automatically. For OceanStor 9000 V5 and in cases where the path is not detected automatically, input the UNC path manually. Click **OK.**



Error - A user selects a ...

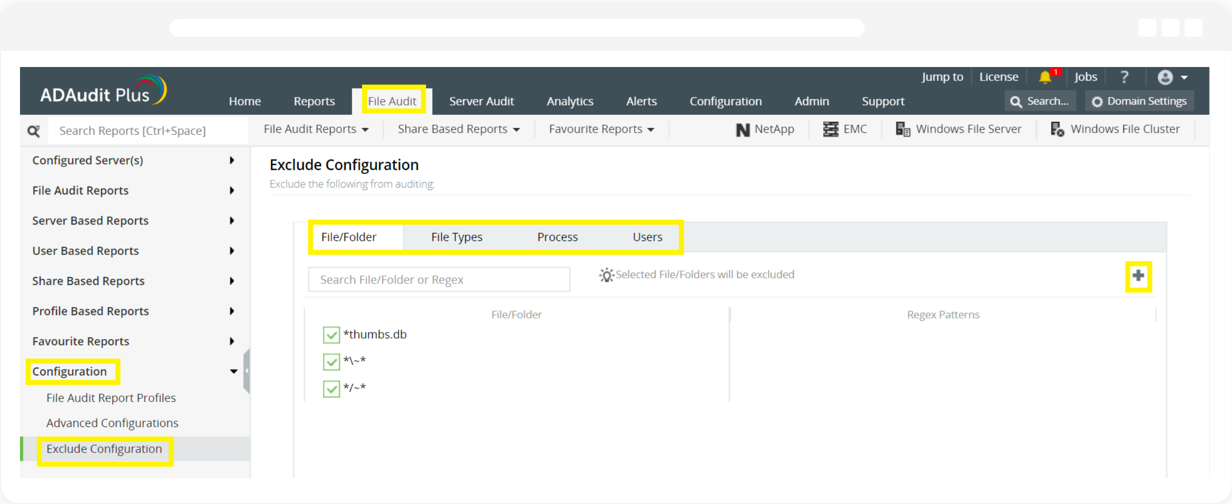
Log file location(UNC path): \\5610V5\[redacted]

10. Your target OceanStor storage system will be added to the web console, and ADAudit Plus will begin reporting on access to the target shares.

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

Troubleshooting

Below are some common issues faced in Huawei OceanStor storage system auditing using ADAudit Plus and the steps to resolve them.

- **The target storage system is not listed in the Add File Servers pop-up**
  Ensure that the target storage system is connected to the domain. If it is, refresh the computer objects for that domain by following the steps below.
  1. In the **ADAudit Plus** console, go to **Domain Settings** in the top-right corner.
  2. From the domain drop-down, select **Update Domain Objects** to open the corresponding pop-up.
  3. Select **Computers** from the list and click **Save.**

- **Shares are not discovered**
  1. Run the command below with the Domain Settings user's account:
     runas /user:domain/user /savecred mmc
  2. Add the target share as a snap-in by following the steps below.
     Run **mmc.exe.**
     Go to **File > Add/Remove Snap-in > Shared Folders.**
     Connect to your target server, select the target share, and save the snap-in.
  3. Check that the share is accessible. If not, check **OceanStor DeviceManager** to ensure that the Domain Settings user is added to **Authentication Users** and has access to the target share. Refer to this Huawei support guide for more information.

- **Any error message appears when the ADAudit Plus Huawei user's credentials are provided in the console**
  If you encounter an error while adding the ADAudit Plus Huawei user's credentials, check that the user has been provided with the required minimum privileges.

- **Issues occur in displaying the vStores**
  1. If no vStores are listed, or if only the system or default vStores are listed, check that the ADAudit Plus Huawei user has been provided the required minimum privileges.
  2. If the issue persists after the privileges have been assigned correctly, contact the support team at support@adauditplus.com for further assistance.

- **Issues occur in displaying the shares in the selected storage system**
  1. If the shares you wish to audit are not listed, check that the Domain Settings user has been provided with the required minimum privileges.
  2. If the issue persists after the privileges have been assigned correctly, contact the support team at support@adauditplus.com for further assistance.

- **Certificate exceptions occur**
  If a certificate exception error message is displayed, import the certificate file from OceanStor to the Java KeyStore using a keytool. The KeyStore can be found at *<installation_directory>\jre (e.g., C:\Program Files (x86)\ManageEngine\ADAudit Plus\jre).*

To export the certificate from Google Chrome:

1. Open Google Chrome on your computer, enter **<YOUR SERVER NAME>:8088** in the address bar, and press **Enter.**
2. Click the **View site information** option in the address bar to the left of the URL.
3. Click **Connection is secure**, then click **Certificate is valid,** which opens the *Certificate Viewer* window.
4. Click the **Details** tab, then click **Export**, which opens the *Save As* window.
5. Enter a suitable name for the certificate file, select **DER-encoded binary, single certificate** from the *Save as type* drop-down, then click **Save.**

To import the certificate:

1. Copy the exported CERT or PEM file to the <*Installation directory*>*\jre\bin* folder.
2. Open Command Prompt in that folder and run the following command:

   keytool -importcert -file <Certificate Name> -alias selfsigned -keystore "<Installation Path>\jre\lib\security\cacerts"

   For example:

   keytool -importcert -file dmcert-1.pem -alias selfsigned -keystore "C:\Program Files (x86)\ManageEngine\ADAudit Plus\jre\lib\security\cacerts"
3. When prompted for the password, enter **changeit.**
4. Type **yes** when you are asked to trust the certificate.
5. Restart ADAudit Plus.