

# Huawei OceanStor Auditing Guide

# Table of contents

Overview of Huawei OceanStor auditing	1
Huawei OceanStor V5 series	2
Huawei OceanStor 9000 V5	9
Huawei OceanStor Dorado All-Flash Storage and OceanStor Hybrid Flash Storage	13
Adding Huawei OceanStor systems in ADAudit Plus	16
Exclude configuration	20
Troubleshooting	22

# 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.

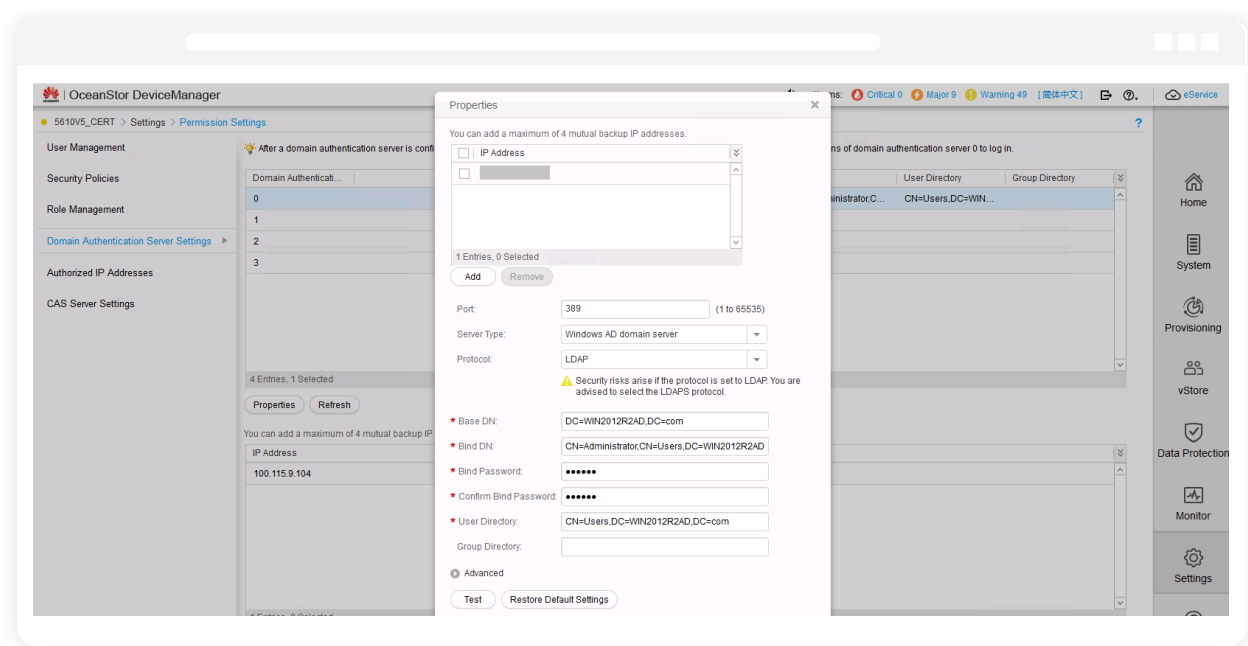
# Huawei OceanStor V5 series

## Minimum privileges required

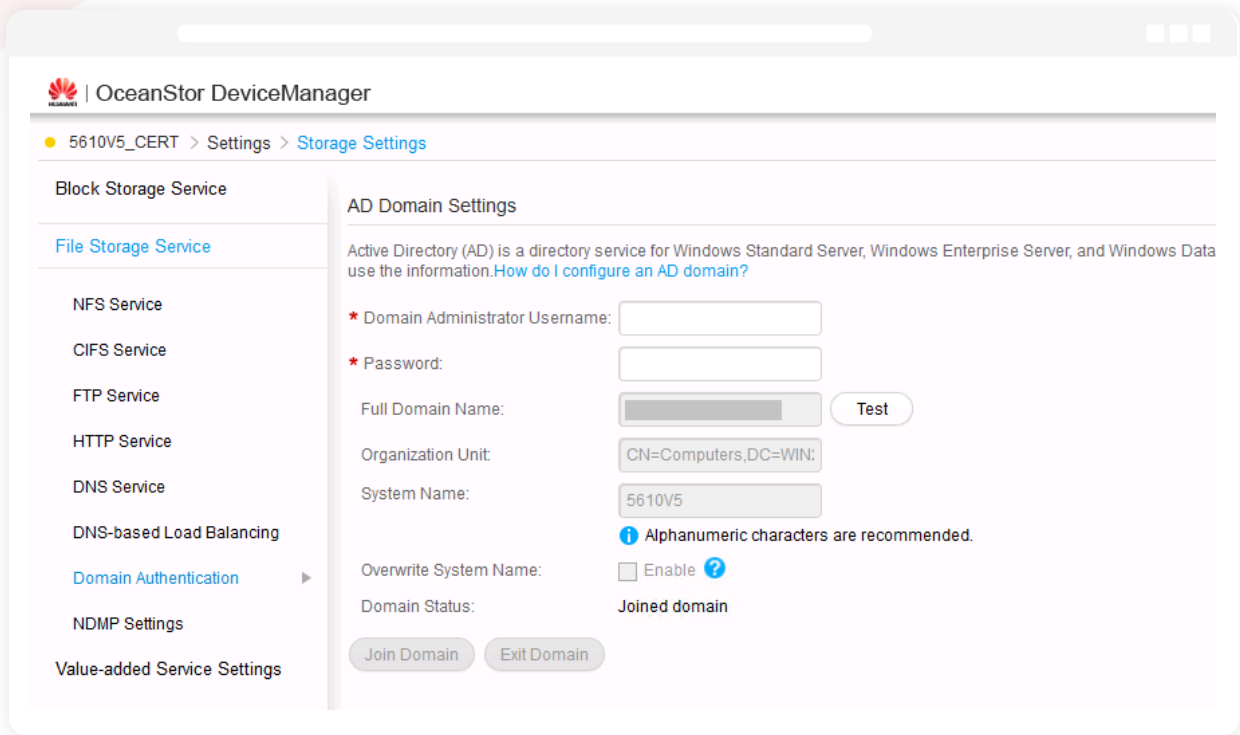
For OceanStor V5 series (system vStore 0 or default vStore), provide the necessary privileges to the user configured in the **Domain Settings** of **ADAudit Plus** (in the top-right corner of the console and referred to below as the Domain Settings user), or create a dedicated ADAudit Plus Huawei user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

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

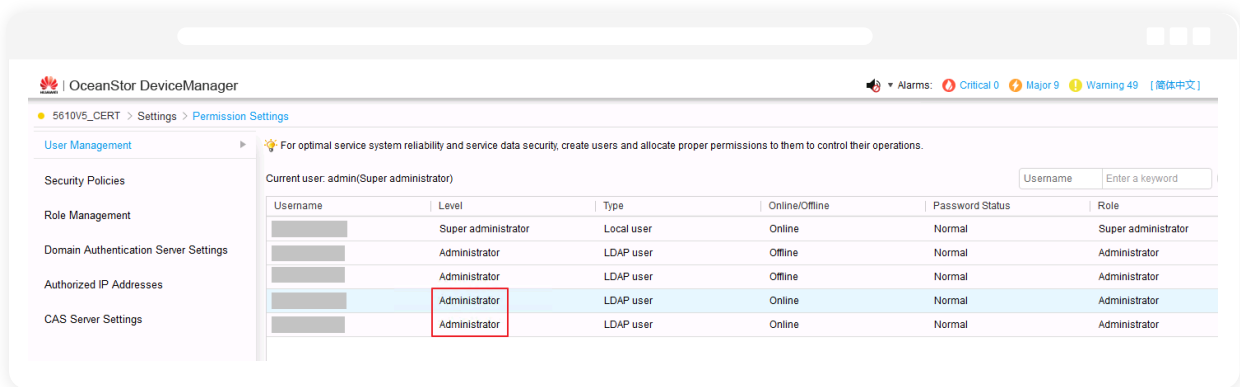
1. In **OceanStor DeviceManager**, configure the domain authentication server to provide the domain users with management permission.



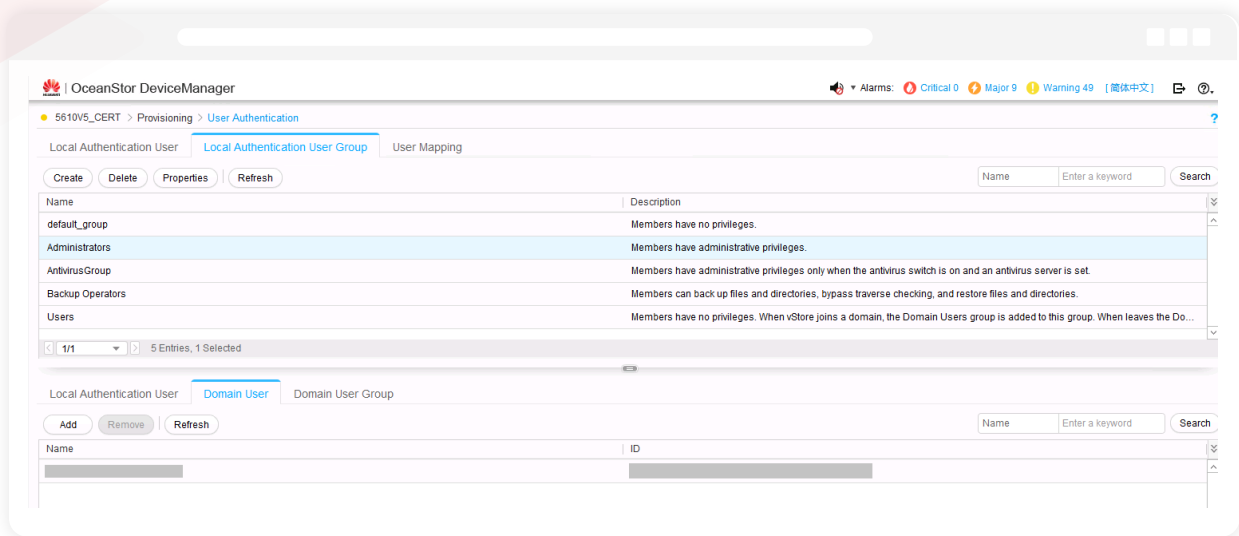
2. Join the **File Storage Service** to the AD domain by providing the necessary details under **Domain Authentication**.



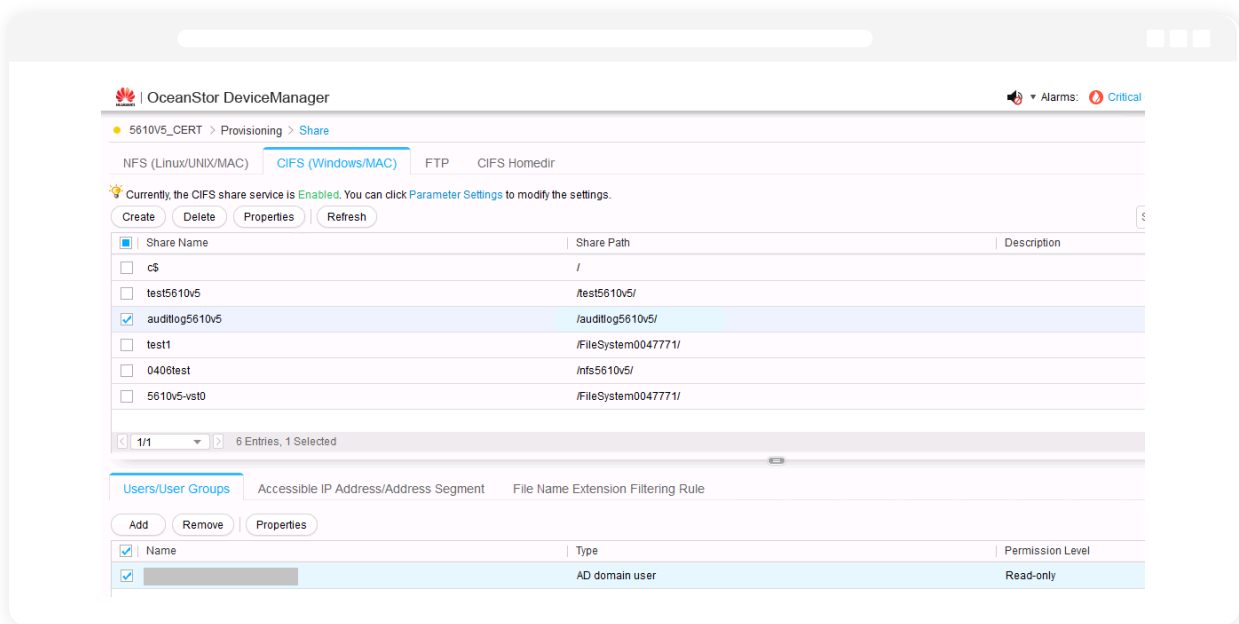
3. Provide the ADAudit Plus user account with administrator-level privileges.



4. Provide the user with permission to access shares.

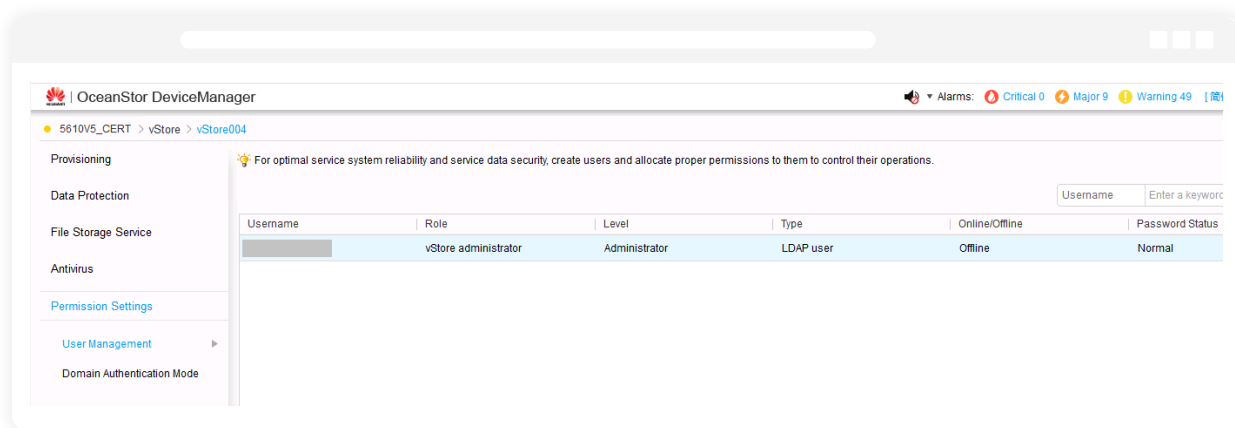


5. Provide the user with permission to read the share paths of the target shares and the audit log.

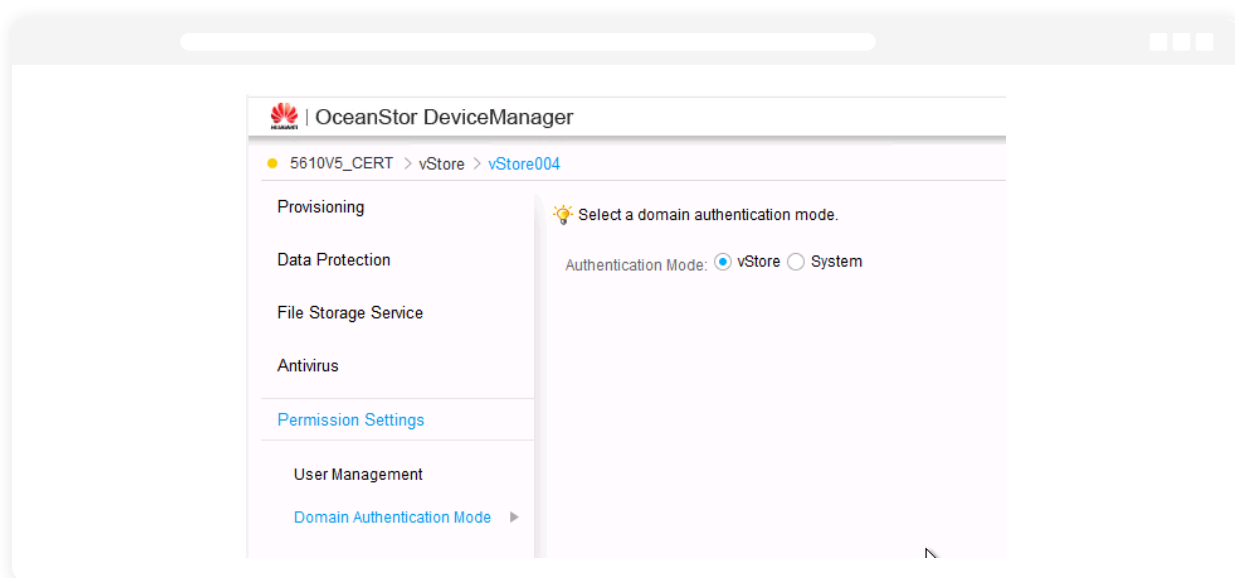


- For OceanStor V5 series vStores

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



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



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

The screenshot shows the 'AD Domain Settings' configuration window. On the left is a sidebar with navigation options: Provisioning, Data Protection, File Storage Service (highlighted), NFS Service, CIFS Service, DNS Service, DNS-based Load Balancing, Domain Authentication (highlighted), NDMP Settings, Credential Management, and Antivirus. The main area is titled 'AD Domain Settings' and contains the following fields and options:

- Active Directory (AD)** is a directory service for Windows Standard Server, Windows Enterprise Server, and Windows Server 2008 and use the information. [How do I configure an AD domain?](#)
- Domain Administrator Username:** administrator
- Password:** [Masked with dots]
- Full Domain Name:** WIN2012R2AD.com (with a **Test** button)
- Organization Unit:** [Empty field]
- System Name:** 5610v5\_vstore4 (with a note: **Alphanumeric characters are recommended.**)
- Overwrite System Name:** ☐ Enable ?
- Domain Status:** Exited domain
- Buttons:** Join Domain, Exit Domain

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

The screenshot shows the 'OceanStor DeviceManager' User Authentication configuration window. The left sidebar includes: Provisioning, LUN, File System, Share, User Authentication (highlighted), Port, Application, Mapping View, Host, SmartMigration, Data Protection, File Storage Service, Antivirus, and Permission Settings. The main area is titled 'Local Authentication User' and contains the following sections:

- Local Authentication User Group:**
  - Buttons: Create, Delete, Properties, Refresh
  - Table with columns: Name, Description
  - Table content:

default_group	Members have no privileges.
Administrators	Members have administrative privileges.
AntivirusGroup	Members have administrative privileges only when the antivirus is enabled.
Backup Operators	Members can back up files and directories, bypass traverse checks.
Users	Members have no privileges. When vStore joins a domain, the Domain Users group is added.
- Domain User:**
  - Buttons: Add, Remove, Refresh
  - Table with columns: Name, ID
  - Table content: [Empty table]

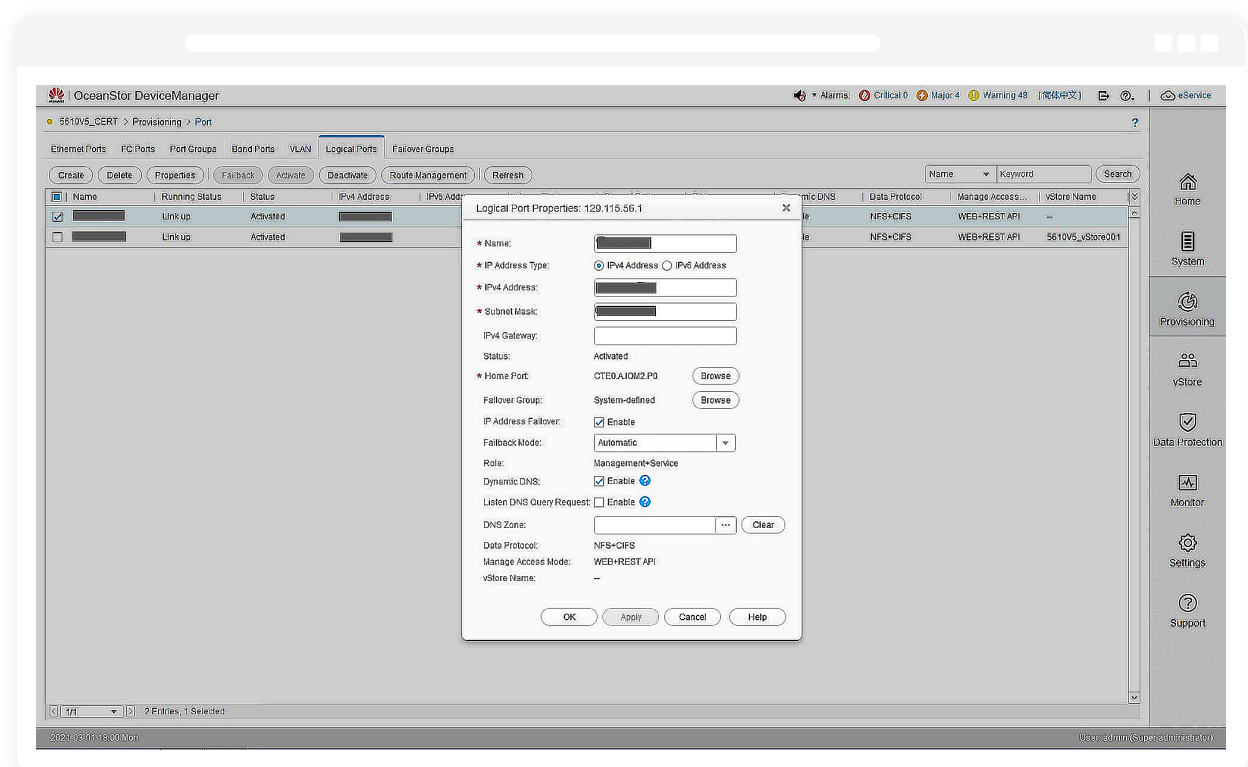
5. Provide the user with permission to read the share paths of the target shares and the audit log.



## Configuration prerequisites

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

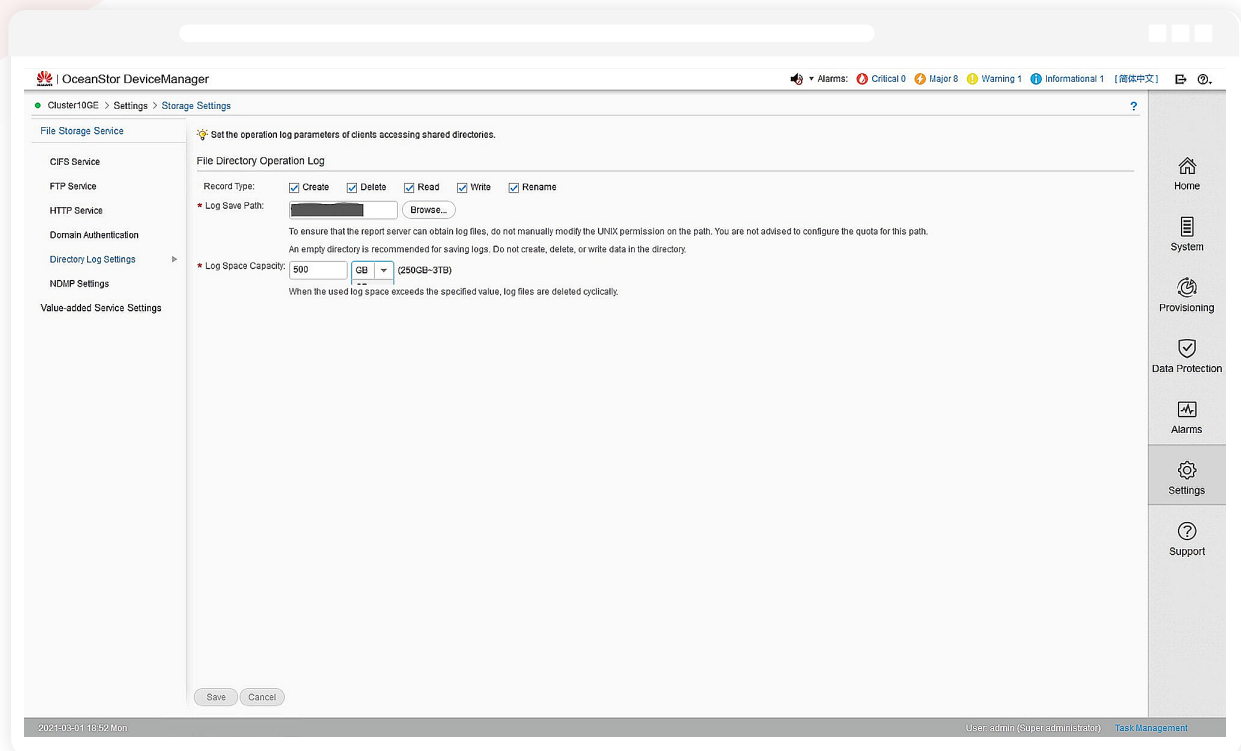
1. In **OceanStor DeviceManager**, create a dedicated ADAudit Plus Huawei user account and provide it with the required minimum privileges according to the steps in [this section](#).
2. Ensure that the OceanStor storage device's name resolves to an IP that serves as both the management and service IP.
3. Ensure that a logical port—that is not dedicated to a vStore—is set up for accessing the REST API.



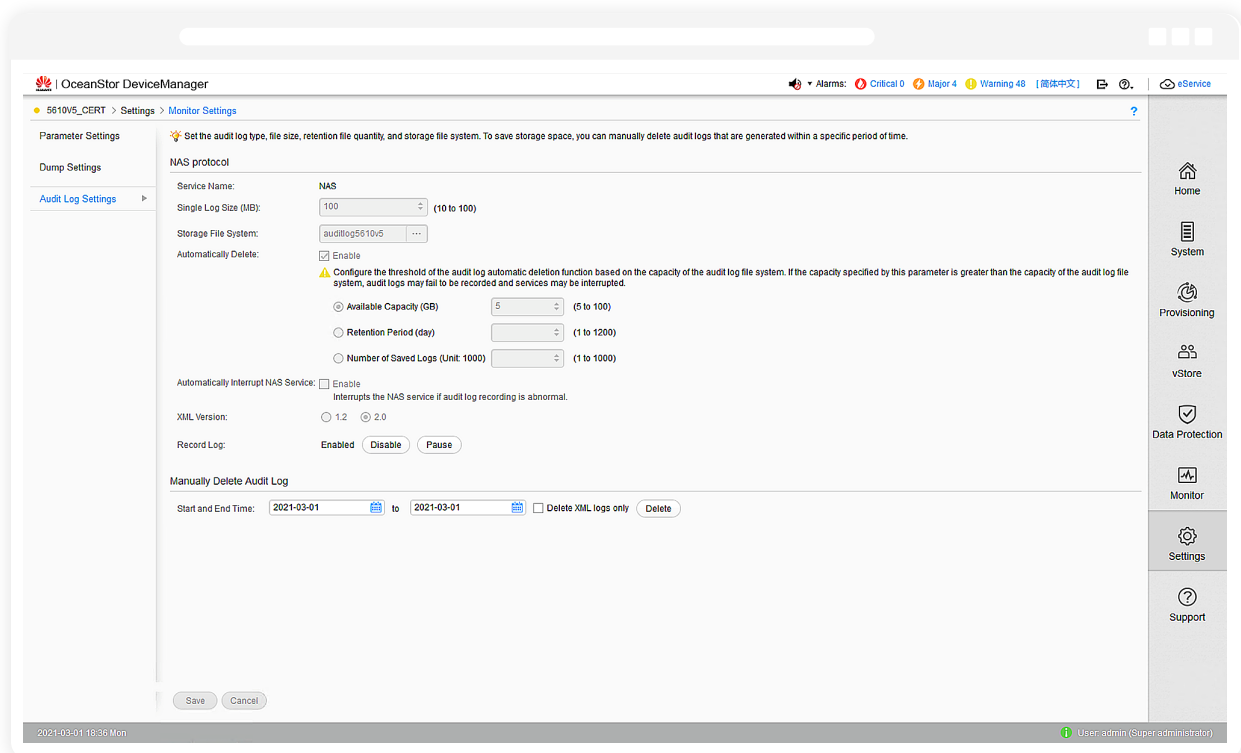
## Enabling auditing

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.



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



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

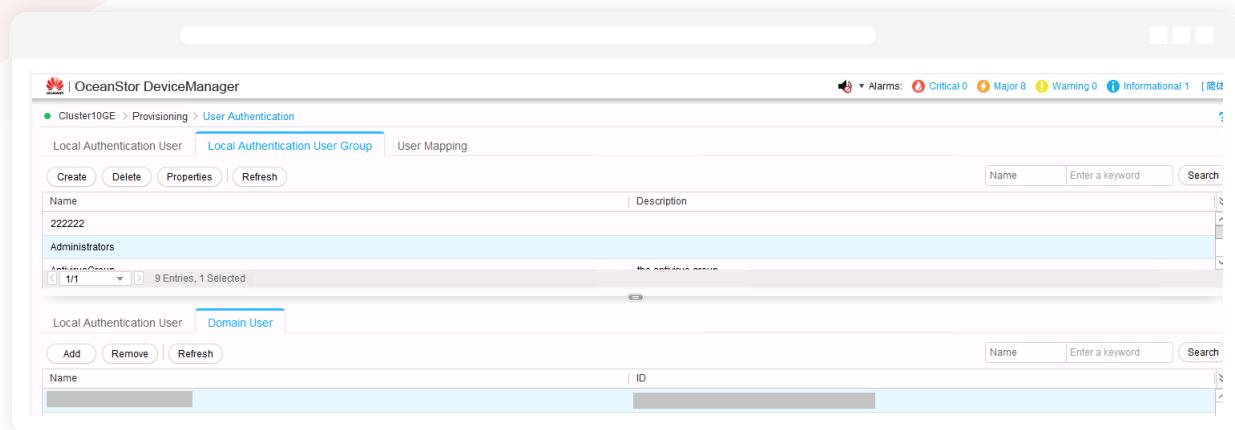
For OceanStor 9000 V5 storage systems, provide the necessary privileges to the user configured in the Domain Settings of ADAudit Plus (in the top-right corner of the console and referred to below as the Domain Settings user), or create a dedicated ADAudit Plus Huawei user account and provide it with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

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

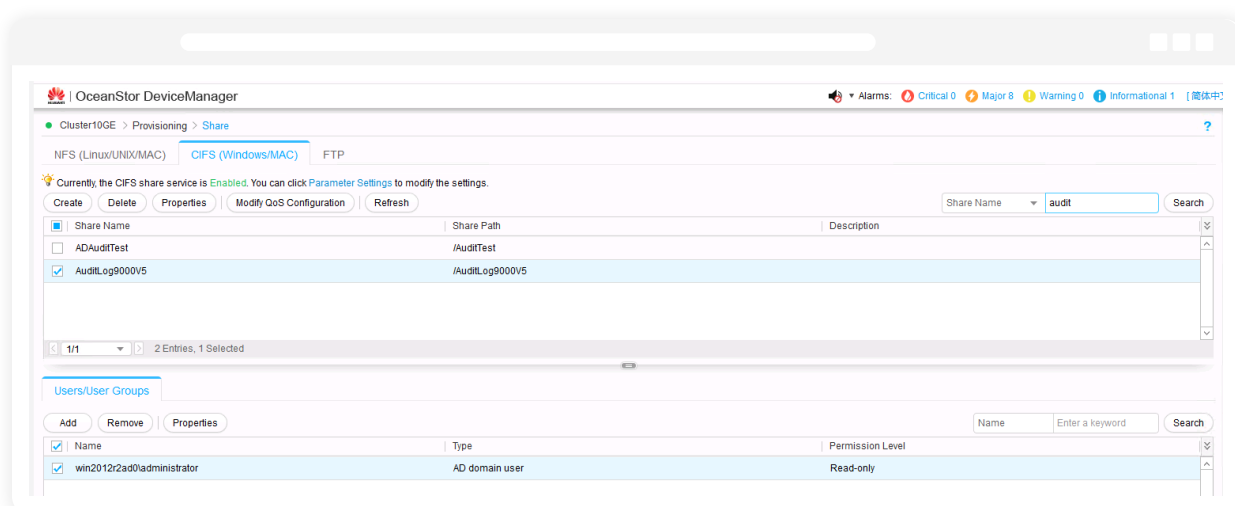
The screenshot displays the 'Cluster10GE > Settings > Storage Settings' page. On the left sidebar, 'File Storage Service' is selected, with 'Domain Authentication' highlighted. The main panel, titled 'AD Domain Settings', contains the following fields and controls:

- 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:
- Organization Unit:
- System Name:
- Overwrite System Name: ☐ Enable
- Domain Status: **Joined domain**
- 

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



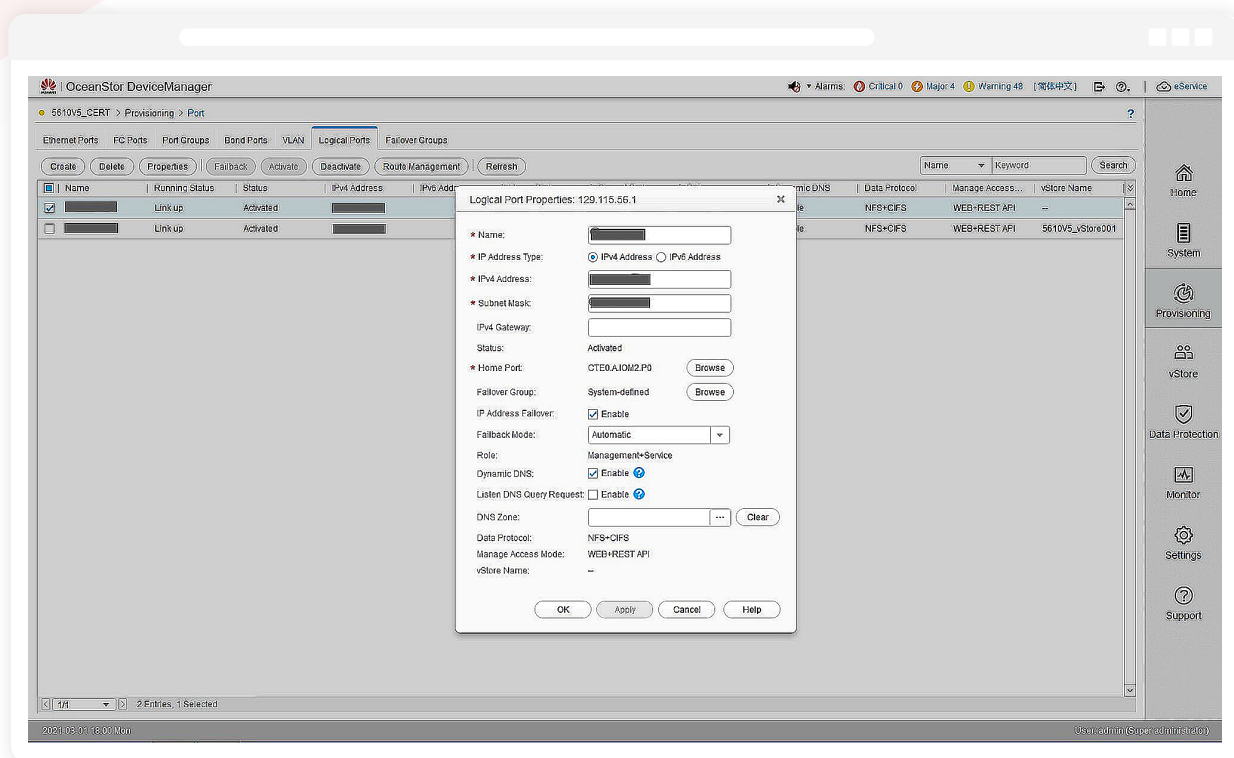
3. Provide the Domain Settings user with permission to read the share paths of the target shares and the audit log.



## Configuration prerequisites

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

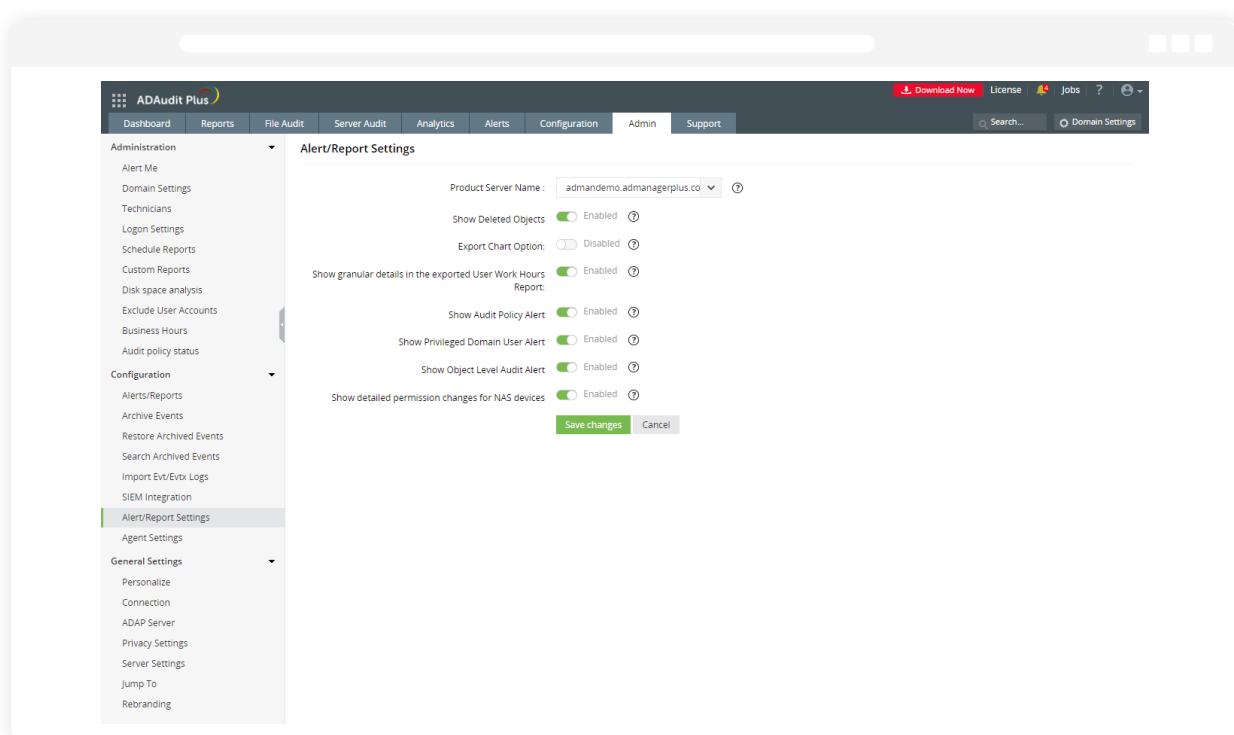
1. Create a dedicated ADAudit Plus Huawei user account and provide it with the required minimum privileges according to the steps in [this section](#).
2. Ensure that the OceanStor storage device's name resolves to an IP that serves as the management IP.
3. Ensure that a logical port—that is not dedicated to a vStore—is set up for accessing the REST API.



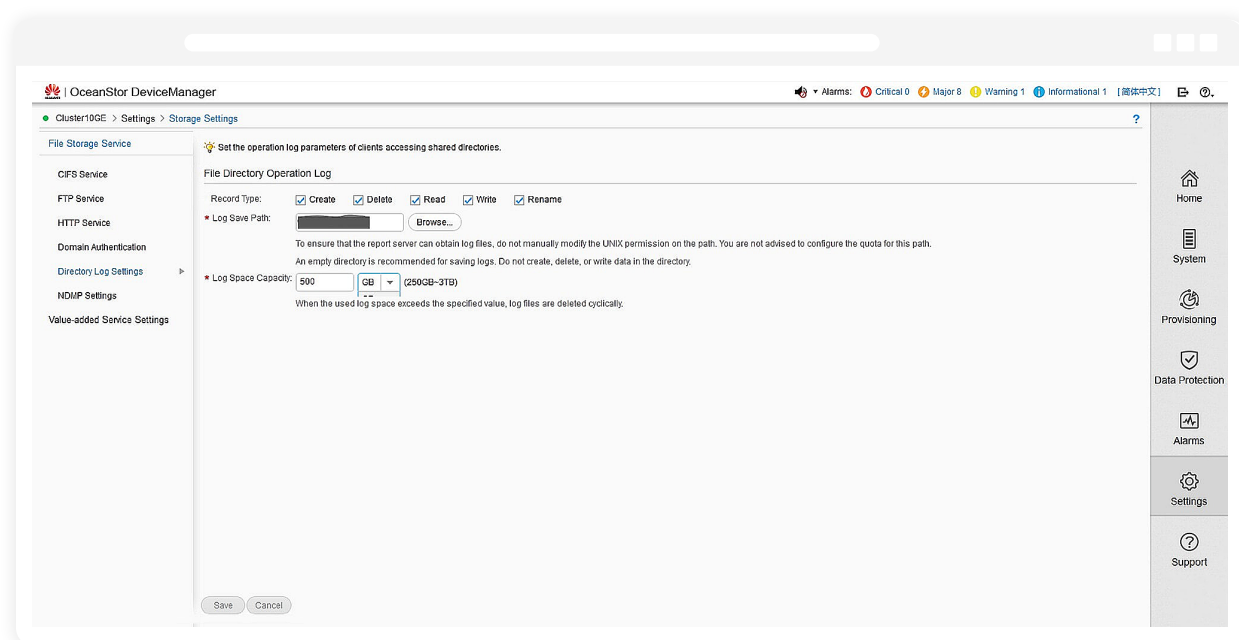
## Enabling auditing

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

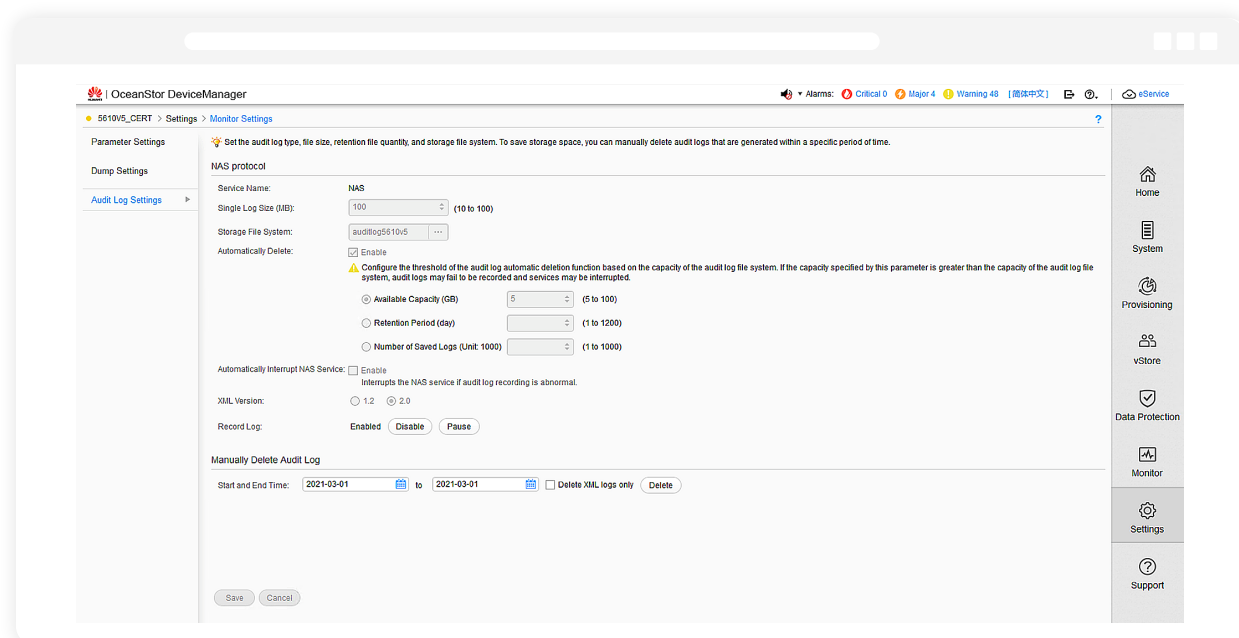
1. To view the ACL values before and after permission change and owner change events, log on to the **ADAudit Plus** web console, go to **Admin > Configuration > Alert/Report Settings**, and enable **Show detailed permission changes for NAS devices**.



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.



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



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**

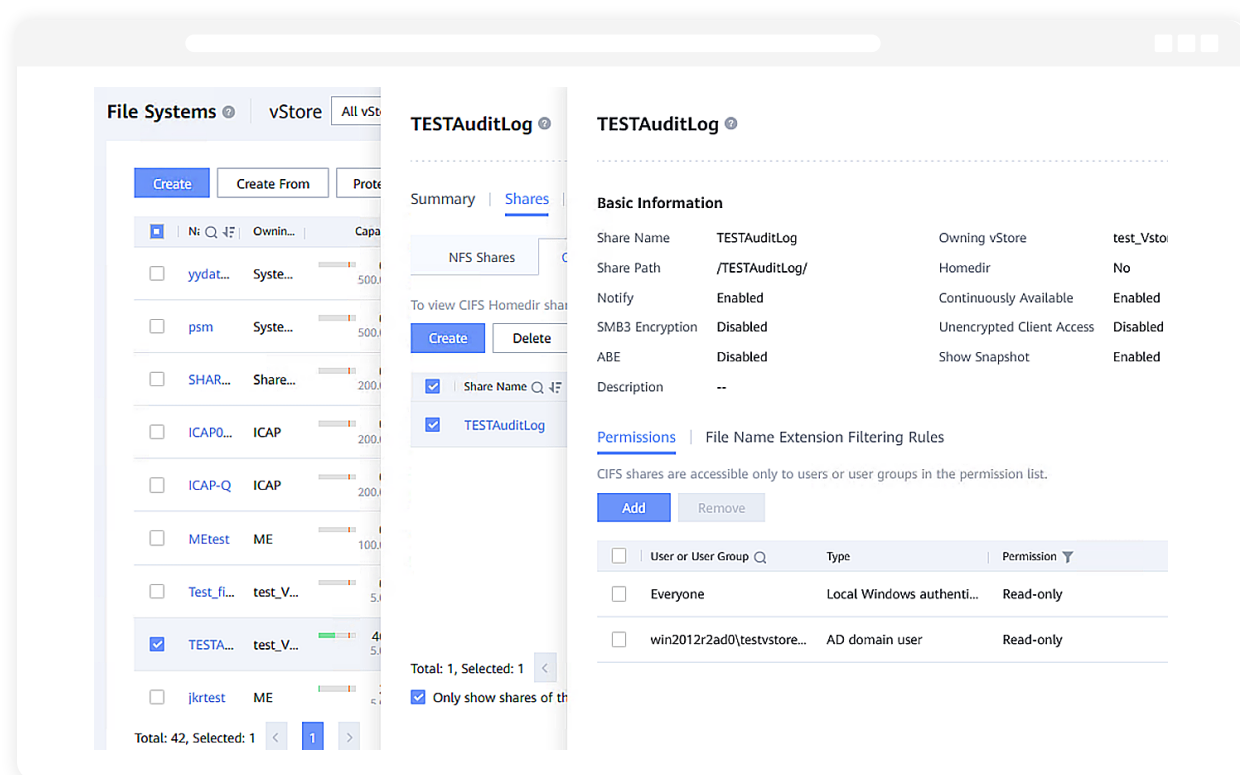
**CLI command admin:/>change service cifs logon\_audit\_disable=yes**

# 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.



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

## Configuration prerequisites

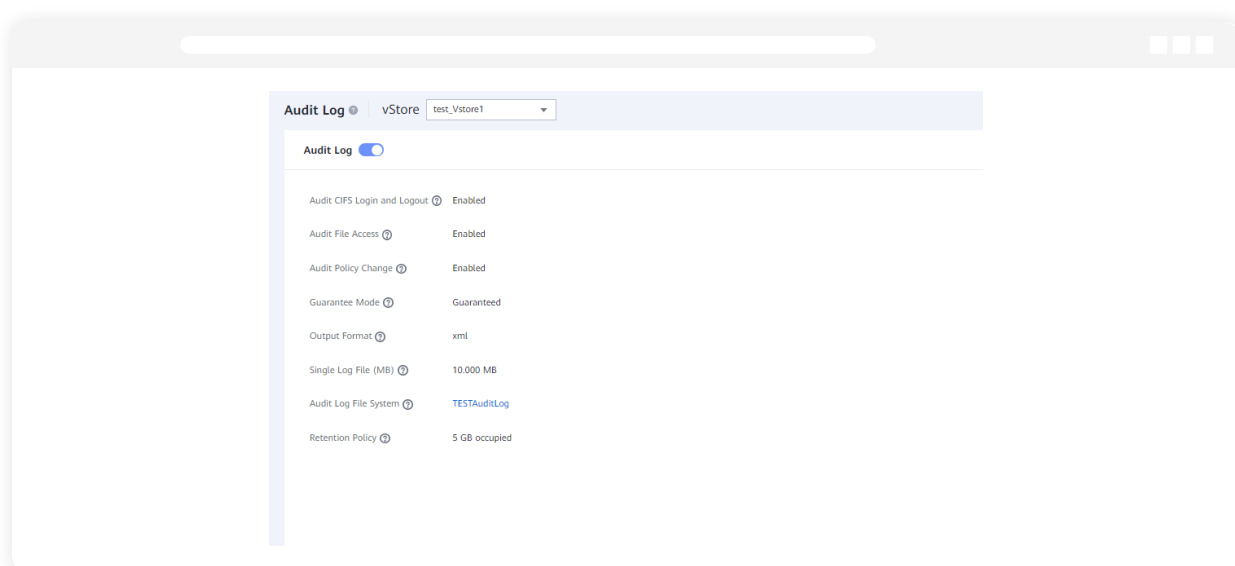
The settings below need to be configured prior to adding your OceanStor Dorado All-Flash Storage and OceanStor Hybrid Flash Storage systems in ADAudit Plus.

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.





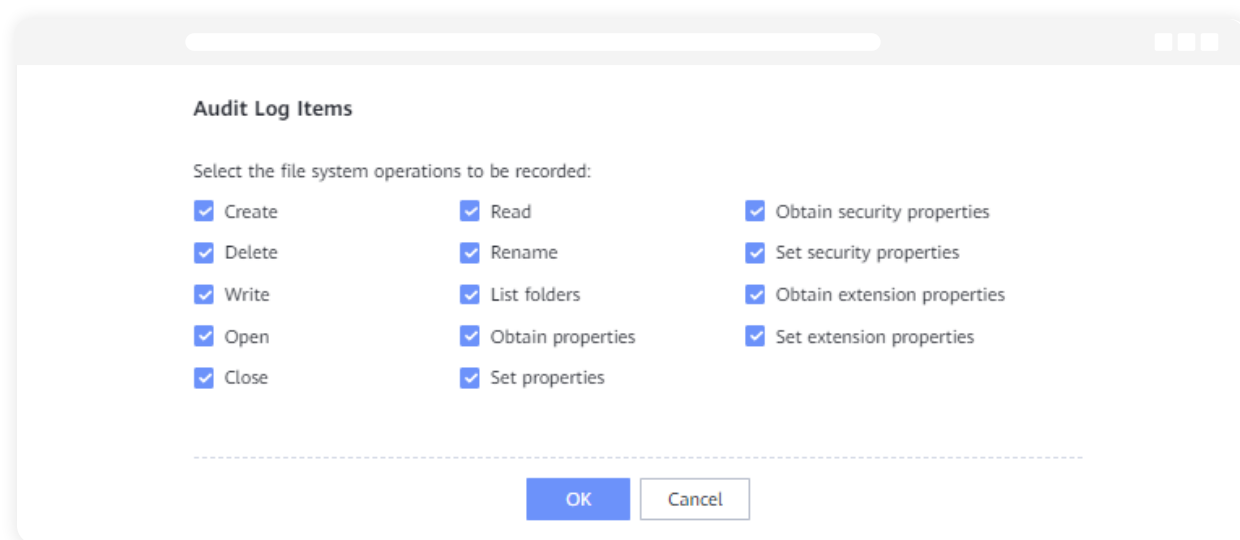
### 3. Configure auditing options for the domain.

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**.

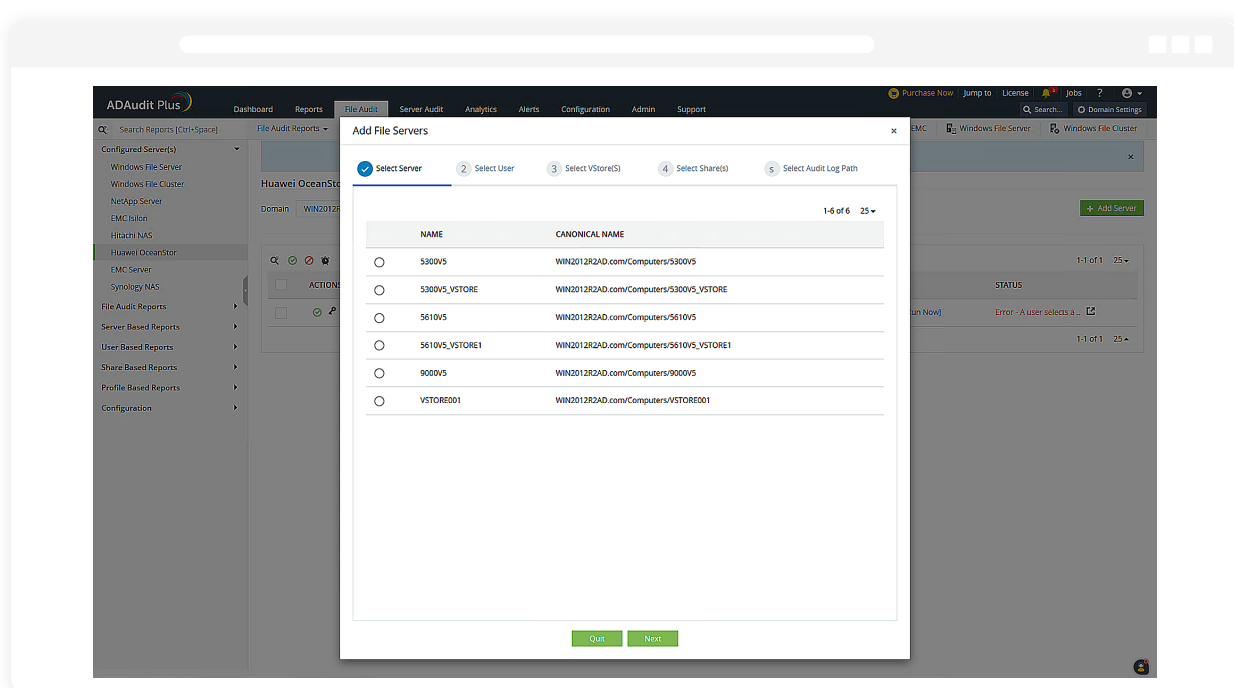
ii. Enable auditing and select the file system operations you want to audit.



# Adding Huawei OceanStor systems in ADAudit Plus

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

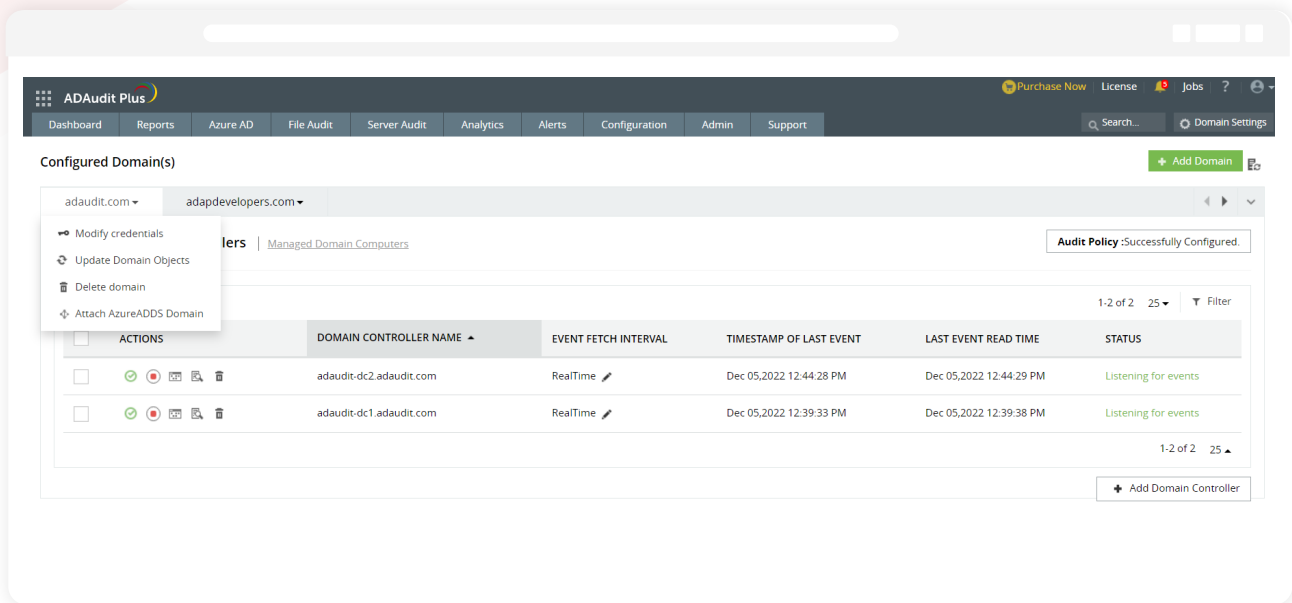
1. Log on to the **ADAudit Plus** web console.
2. Go to **File Audit > Configured Server(s) > Huawei OceanStor**.
3. Click **+ Add Server** in the top-right corner. This will open the *Add File Servers* pop-up.
4. Select the storage system you wish to audit with ADAudit Plus. In case the server has a 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**.



## Troubleshooting tip

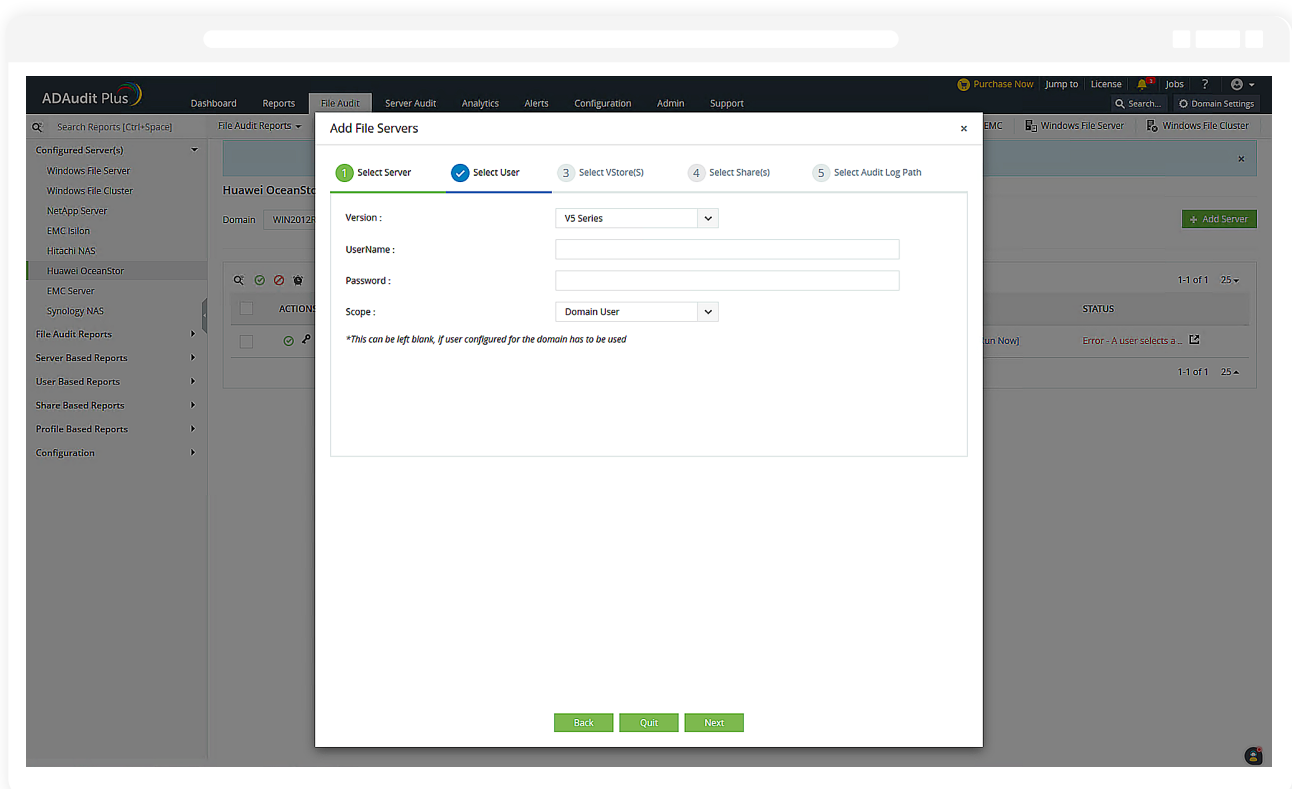
If the storage system you wish to audit is not listed in the Add File Servers pop-up, check that it is connected to the target domain. If it is, refresh the computer objects for that domain by following the steps below.

- 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**.



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.



### Troubleshooting tip

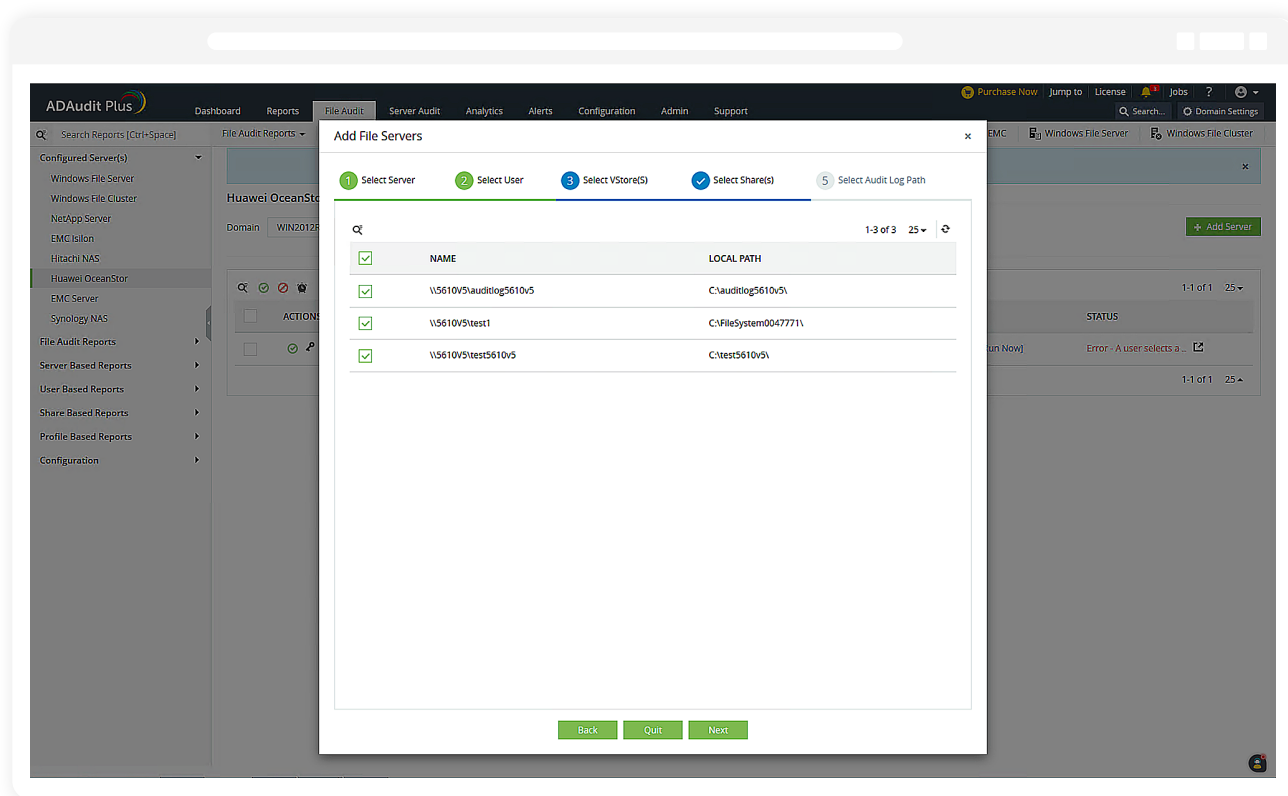
If you encounter an error while adding the ADAudit Plus Huawei user's credentials, check that the user has the required minimum privileges.

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

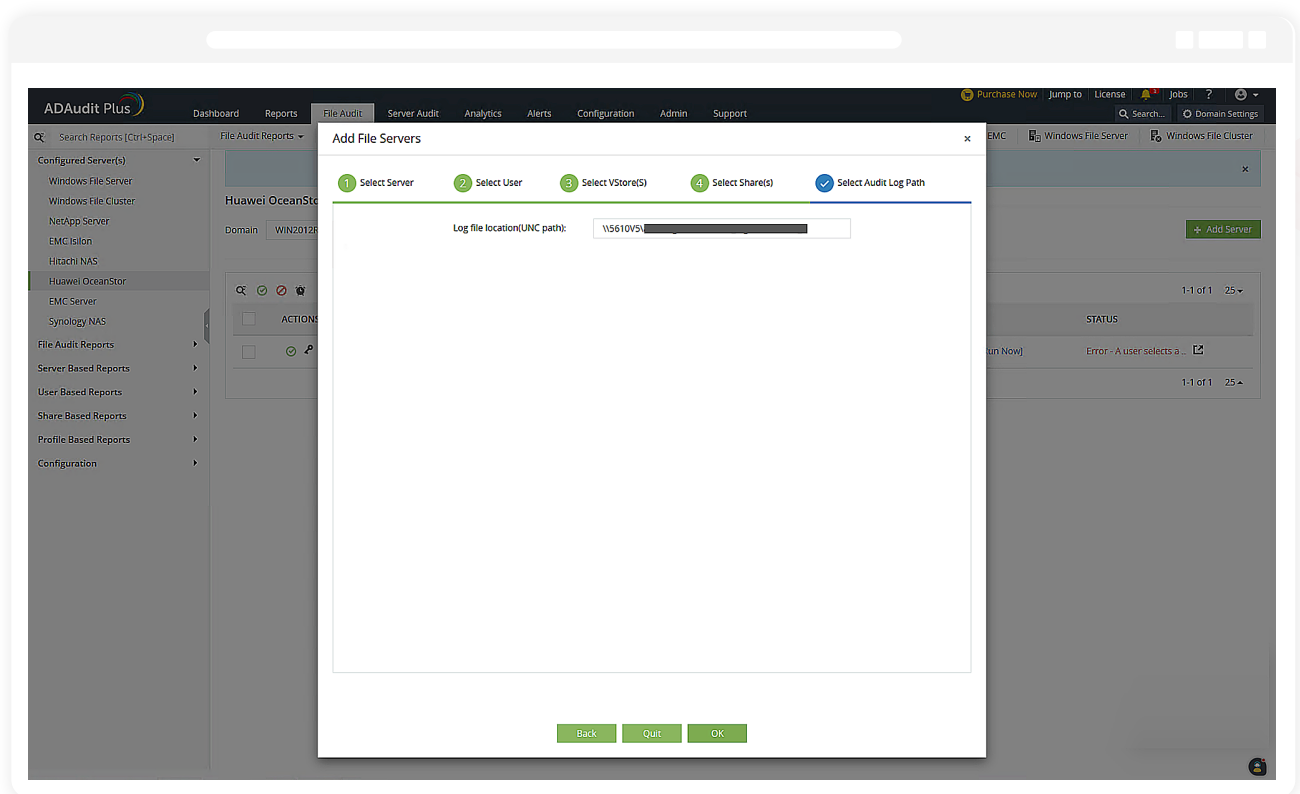
### Troubleshooting tip

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](mailto:support@adauditplus.com) for further assistance.

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



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**.

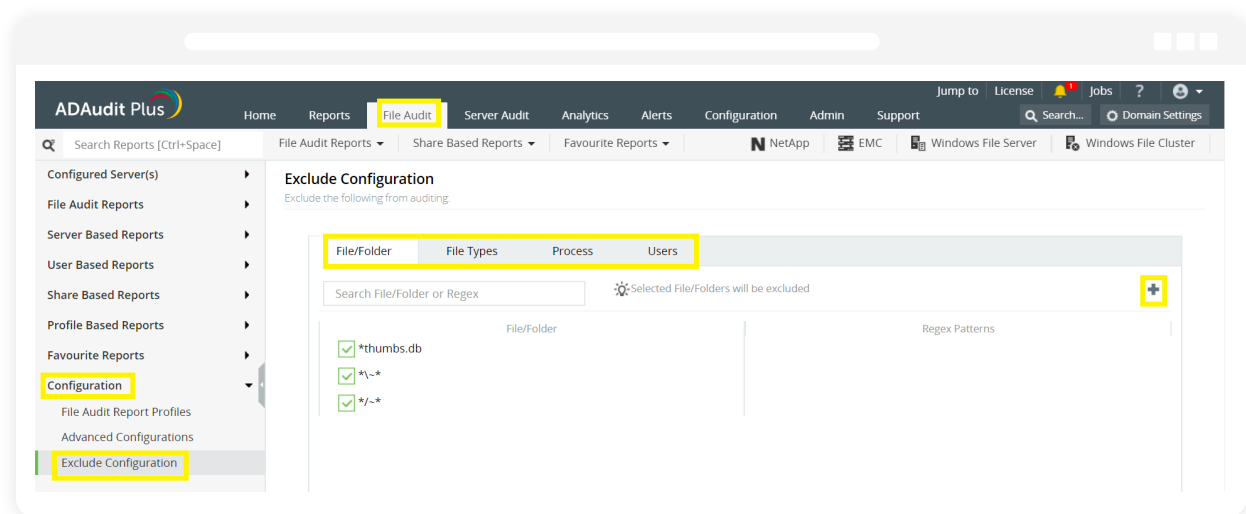


10. Your target OceanStor storage system will be added to the web console, and ADAudit Plus will begin reporting on access to the target shares.

# 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.



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"><li>C:\sharefolder\excludefolder</li><li>C:\sharefolder\excludefolder\*</li></ul>	
What will get excluded	<ul style="list-style-type: none"><li>C:\sharefolder\excludefolder</li><li>C:\sharefolder\excludefolder\folder</li><li>C:\sharefolder\excludefolder\files.txt</li><li>C:\sharefolder\excludefolder\folder\files.txt</li></ul>	
What won't get excluded	—	

<b>Objective</b>	To exclude "AppData" folder for every user profile
<b>Share and folder path</b>	\\SERVER_NAME\Users C:\Users
<b>Path of folder that is to be excluded</b>	C:\Users\user1\AppData
<b>File/Folder or Regex Patterns</b>	Regex Patterns
<b>Syntax</b>	C:\\Users\\[^\\]*\\AppData
<b>What will get excluded</b>	<ul style="list-style-type: none"> <li>C:\Users\user1\AppData</li> <li>C:\Users\user2\AppData</li> <li>C:\Users\user1\AppData\subfolder</li> <li>C:\Users\user2\AppData\subfolder</li> </ul>
<b>What won't get excluded</b>	<ul style="list-style-type: none"> <li>C:\Users\user1\subfolder\AppData</li> <li>C:\Users\user2\subfolder\AppData</li> </ul>

<b>Objective</b>	<b>To exclude files from a specific folder but audit all subfolders and its contents</b>
<b>Share and folder path</b>	\\SERVER_NAME\share_name C:\sharefolder
<b>Path of folder that is to be excluded</b>	C:\sharefolder\excludefolder
<b>File/Folder or Regex Patterns</b>	Regex Patterns
<b>Syntax</b>	^C:\\sharefolder\\excludefolder\\[^\\]*\\.\\[^\\]*\$
<b>What will get excluded</b>	<ul style="list-style-type: none"> <li>C:\sharefolder\excludefolder\file.txt</li> <li>C:\sharefolder\excludefolder\folder.withDot</li> </ul>
<b>What won't get excluded</b>	<ul style="list-style-type: none"> <li>C:\sharefolder\excludefolder</li> <li>C:\sharefolder\excludefolder\folderWithoutDot</li> <li>C:\sharefolder\excludefolder\folderWithoutDot\subfolder</li> <li>C:\sharefolder\excludefolder\folderWithoutDot\testfile.txt</li> <li>C:\sharefolder\excludefolder\folder.withDot\subfolder</li> <li>C:\sharefolder\excludefolder\folder.withDot\testfile.txt</li> </ul>

# 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](mailto: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](mailto: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`).





ManageEngine  
**AD Audit Plus**

ManageEngine ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps keep your Active Directory, Azure AD, Windows servers, and workstations secure and compliant.

[\\$ Get Quote](#)

[Download](#)