

Huawei OceanStor Auditing Guide

www.adauditplus.com

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.
- \bigcirc Provide a user-friendly interface and detailed reports for analyzing file access attempts.
- O Detect abnormal user activities, such as an atypical volume of file changes or file modifications at unusual times.
- Strigger instant alerts when anomalous file activities are detected and execute automated scripts to protect data stores.
- O 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.

l OceanStor DeviceManager		Properties		۰. ۲	ms: 🚺 Critica	ll 0 (Major 9 🌖 War	ning 49 【简体中文】	₽ @.	eService
5610V5_CERT > Settings > Permission \$	Settings	You can add a maximum of	f 4 mutual backup IP addresses.		-			?	
Iser Management	🌾 After a domain authentication server is confi	IP Address		*	ns of domain a	uthentication server 0 to lo	g in.		
ecurity Policies	Domain Authenticati			^^		User Directory	Group Directory	*	命
tole Management	0				ninistrator,C	CN=Users,DC=WIN		<u> </u>	Home
Iomain Authentication Server Settings	2			<u>_</u>					E
uthorized IP Addresses	3	1 Entries, 0 Selected							System
AS Server Settings		Add Remove	200	(44-05505)					(A)
		Server Type:	Windows AD domain server	(110 05535)					Provisionir
		Protocol:	LDAP					~	00
	4 Entries, 1 Selected		A Security risks arise if the protoco advised to select the LDAPS pro	ol is set to LDAP. You are tocol.					vStore
	(Topeneo) (Teneon)	* Base DN:	DC=WIN2012R2AD,DC=com						
	You can add a maximum of 4 mutual backup IP	* Bind DN:	CN=Administrator,CN=Users,DC=	WIN2012R2AD	_			×	Data Protec
	100.115.9.104	* Bind Password:	•••••					^	
		* Confirm Bind Password:	•••••						-^-
		* User Directory:	CN=Users,DC=WIN2012R2AD,DC	=com					Monitor
		Group Directory:							6
		Advanced							Settings

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

5610V5_CERT > Settings > 5	Storage Settings	
Block Storage Service	AD Domain Settings	
File Storage Service	Active Directory (AD) is a directory use the information. How do I cont	/ service for Windows Standard Server, Windows Enterprise Server, and Windows Da figure an AD domain?
NFS Service	* Domain Administrator Usernan	ne:
CIFS Service	* Password:	
FTP Service	Full Domain Name:	Test
HTTP Service	Organization Unit:	CN=Computers,DC=WIN:
DNS Service	System Name:	5610V5
DNS-based Load Balancing		Alphanumeric characters are recommended.
Domain Authentication	Overwrite System Name:	🗌 Enable 😮
NDMP Settings	Domain Status:	Joined domain
Value added Service Settings	Join Domain Exit Domain	

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

OceanStor DeviceManager				•	 Alarms: () Critical 0 () Major 9 	Warning 49 【简体中爻
5610V5_CERT > Settings > Permission	Settings					
User Management	🔆 For optimal service sy	stem reliability and service data security, o	create users and allocate proper	permissions to them to control their op	erations.	
Security Policies	Current user: admin(Sup	er administrator)			Usernam	e Enter a keyword
Pole Management	Username	Level	Туре	Online/Offline	Password Status	Role
Tote Management		Super administrator	Local user	Online	Normal	Super administrator
Domain Authentication Server Settings		Administrator	LDAP user	Offline	Normal	Administrator
Authorized IP Addresses		Administrator	LDAP user	Offline	Normal	Administrator
		Administrator	LDAP user	Online	Normal	Administrator
CAS Server Settings		Administrator	I DAR user	Opline	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 Group User Mapping							
Create Delete Properties Refresh		Name	Enter a keyword	Searc			
Name	Description						
default_group	Members have no privileges.						
Administrators	Members have administrative privileges.	Members have administrative privileges.					
AntivirusGroup	Members have administrative privileges only when t	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	Members can back up files and directories, bypass traverse checking, and restore files and directories.					
Users	Members have no privileges. When vStore joins a de	omain, the Domain Users group is adde	d to this group. When leaves	the Do			
1/1 The selected 5 Entries, 1 Selected							
	•						
Local Authentication User Domain User Domain User Group							
Add Remove Refresh		Name	Enter a keyword	Searc			
Name	ID						

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

Strivis_CERT > Provisioning > Share	_	
NFS (Linux/UNIX/MAC) CIFS (Windows/MAC)	FTP CIFS Homedir	
Currently, the CIFS share service is Enabled. You can cl	ck Parameter Settings to modify the settings.	
Create Delete Properties Refresh		
Share Name	Share Path	Description
c\$	1	
test5610v5	/test5610v5/	
auditlog5610v5	/auditlog5610v5/	
test1	/FileSystem0047771/	
0406test	/nfs5610v5/	
5610v5-vst0	/FileSystem0047771/	
6 Entries 1 Selected		
	•	
Users/User Groups Accessible IP Address/A	ddress Segment File Name Extension Filtering Rule	
Add Remove Properties		

• For OceanStor V5 series vStores

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

🗏 OceanStor DeviceMa	inager				🔩 🔻 Alarms: 🚺 Critical 0	🚱 Major 9 🕛 Wa	rning 49 [
5610V5_CERT > vStore > vSto	pre004						
Provisioning	🔆 For optimal service syst	tem reliability and service data security, o	create users and allocate proper p	ermissions to them to control their op	erations.		
Data Protection						Username	Enter a key
File Storage Service	Username	Role	Level	Туре	Online/Offline	Pa	ssword Sta
, i i i i i i i i i i i i i i i i i i i		vStore administrator	Administrator	LDAP user	Offline	No	rmal
Antivirus							
Permission Settings							
User Management							
Domain Authentication Mode							

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

n CceanStor DeviceMana	ger	
• 5610V5_CERT > vStore > vStore0	04	
Provisioning	🔆 Select a domain authentication mode.	
Data Protection	Authentication Mode: vStore System	
File Storage Service		
Antivirus		
Permission Settings		
User Management		
Domain Authentication Mode		
		N

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

Data Protection		
	Active Directory (AD) is a directory set and use the information. How do I cor	rvice for Windows Standard Server, Windows Enterprise Server, and Win nfigure an AD domain?
File Storage Service	* Domain Administrator Username:	administrator
NFS Service	* Password:	••••••
CIFS Service	* Full Domain Name:	WIN2012R2AD.com Test
DNS Service	Organization Unit:	
DNS-based Load Balancing	* System Name:	5610v5_vstore4
Domain Authentication		() Alphanumeric characters are recommended.
NDMP Settings	Overwrite System Name:	🗌 Enable 😯
NDMI Settings	Domain Status:	Exited domain

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

the target shares.

🜺 OceanStor Devic	eManager	Narms: 🚺 Critical (
5610V5_CERT > vStore	> vStore004	
Provisioning	Local Authentication User Local Authentication User Group User Mapping	
LUN	Create Delete Properties Refresh	
File System	Name	Description
Share	default_group	Members have no privileges.
onare	Administrators	Members have administrative privileges.
User Authentication	AntivirusGroup	Members have administrative privileges only when the antiv
Port	Backup Operators	Members can back up files and directories, bypass traverse
Application	Users	Members have no privileges. When vStore joins a domain, t
Mapping View	S Entries, 1 Selected	
Host	Local Authentication User Domain User Domain User Group	8
SmartMigration		
Data Protection	Add Remove Reliesh	
File Storage Service	Name	
Antivirus		

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.

🙎 i OceanStor i	DeviceManager					崎 🔻 Alan	ns: 🔘 Critical 0 🚫 l/	ajor 4 🕕 Warning 48	(微体中文) D @	🖕 🙆 eSen
5610V5_CERT > P	Provisioning > Port									?
hemet Ports FC	Ports Port Groups	Bond Ports VLAN	Logical Ports Failover Gr	ague						
		Charles (June 14)	(Berdinan) (Berdinan				-	ama w Kanan	1 (Peared	5
T blama	L Dussies Status	L Chebre	Deachate Robie Malla	is a day		1 - 2 - serie Oble	L Data Pastanal	Line o pregnore	Luctara blama	
	Link un	Activated	IP V4 Address IP	Logical Port Properties:	129.115.56.1	×	NES+CIES	WER+REST API	vstore warne	Mome
	Unkup	Activated				18	NES+CIES	WEB+REST API	5610V5 vStore001	l e
,				* Name:		-				
				* IP Address Type:	IPv4 Address () IPv6 Address					Syster
				* IPv4 Address:						Gà
				* Subnet Mask:						Brouce
				IPv4 Gateway:						171011310
				Status:	Activated					00
				* Home Port	CTE0.AIOM2.P0 Browse					uStor
				Fallover Group;	System-defined Browse					
				IP Address Failover	Enable					
				Failback Mode:	Automatic					Data Prot
				Role	Management+Service					
				Dynamic DNS:	Enable 🕢					
				Listen DNS Query Reques	it: 🗌 Enable 🚱					Monit
				DNS Zone:	(Clear				
				Data Protocol:	NES+CIES					63
				Manage Access Mode:	WEB+REST API					Settin
				vStore Name:	-					
										(?)
				ОК	Apply Cancel	Help				Suppo
										<u>~</u>

Enabling auditing

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

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

Construction Construction Construction			
2 Outert100 > Statup > Statup > Statup ? File Statup > Statup > Statup \$ Statup Statup >	🌿 OceanStor DeviceMana	ager 🕹 - Alarms: 🧿 Critical 0 🕐 Major 8 🕠 Warning 1 🕕 Informational 1 [@8	冲文] 🗗 🕻
Fis Stands CFS Stands TP Stands <t< td=""><td>Cluster10GE > Settings > Storag</td><td>e Settings</td><td>•</td></t<>	Cluster10GE > Settings > Storag	e Settings	•
Save Cancel	 Unser rout: > Settings > Storg File Storage Senice CIFS Bervice FTP Senice Domain Authentication Directory Log Settings NDMP Settings Value-added Service Settings 	<pre>setungs</pre>	Home E System Provisionin Provisionin Data Protec Data Protec Aarms Settings Settings Support
		Save Cancel	

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

5610V5 CERT > Settings	> Monter Settings	
Parameter Settings	**************************************	
diameter octaingo		
Dump Settings	NAS protocol	命
Audit Log Settings	Service Name: NAS	Home
	Single Log Size (MB): 100 - (10 to 100)	_
	Storage File System: auditlog5510./5 ···	
	Automatically Delete: 🔀 Enable	System
	Configure the Threshold of the audit log automatic detelon function based on the capacity of the audit log tile system. If the capacity specified by this parameter is greater than the capacity of the audit log tile system. The capacity specified by this parameter is greater than the capacity of the audit log tile system. The capacity specified by this parameter is greater than the capacity of the audit log tile system. The capacity specified by this parameter is greater than the capacity of the audit log tile system. The capacity specified by this parameter is greater than the capacity of the audit log tile system.	GA
	⊙ Available Capacity (GB) 5 ⇒ (5 to 100)	G
	C Retenion Period (day)	riovision
		പ്പ
	Vumber of save Logs (Unit 1000)	vStore
	Automatically interrupt NAS Service: Enable	
	XULVersion: 0 12 0 20	\bigtriangledown
	Development and the second sec	Data Prote
	Record Loy. Endored Usame Parse	
	Manually Delete Audit Log	-1
	Start and Ford Time: 2021-03-01 🚔 In 2021-03-01 🚔 Delete XMI long only Cheste	Monitor
		~
		(Q)
		Setting
		0
		Suppor
	Save Cancel	



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.

File Storage Service	AD Domain Settings		
CIFS Service	Active Directory (AD) is a director and use the information. How do	ry service for Windows Standar I configure an AD domain?	d Server, Windows Enterprise Server, and Windows Datacenter S
FTP Service	* Domain Administrator Userna	ime:	
HTTP Service	- Domain Administrator Osema		
Domain Authentication	* Password:		
Directory Log Settings	Full Domain Name:		Test
NDMP Settings	Organization Unit:		
/alua addad Sanica Sattinga	System Name:	9000V5	
value-audeu Service Settings	Overwrite System Name:	🗌 Enable 😮	
	Domain Status:	Joined domain	

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

🜺 OceanStor DeviceManager		🔩 🔻 Alarms: 🚫 Crit	lical 0 (Major 8 🌔	🕒 Warning 0	iational 1 [
Cluster10GE > Provisioning > User Authentication					
Local Authentication User Local Authentication User Group User Mapping					
Create Delete Properties Refresh			Name	Enter a keyword	Se
Name	Description				
222222					
Administrators					
1/1 v > 9 Entries, 1 Selected	the articles are up				
	•				
Local Authentication User Domain User					
Add Remove Refresh			Name	Enter a keyword	Se
Name	LID.				

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 📀	Aajor 8 🌔	Warning 0 🍈 Informal	ional 1 [简
Cluster10GE > Provisioning > Share					
NFS (LInux/UNIX/MAC) CIFS (Windows/MAC)	FTP				
⁶ Currently, the CIFS share service is Enabled. You can click Pa	rameter Settings to modify the settings.				
Create Delete Properties Modify QoS Configu	ration Refresh	Share N	ame 👻	audit	Searc
Share Name	Share Path	Description			
ADAuditTest	/AuditTest				
AuditLog9000V5	/AuditLog9000V5				
Ald - 2 Entrino 1 Palacted					
2 Inn 2 Zennes, i Selected					
Users/User Groups					
Add Remove Properties		Ν	ame	Enter a keyword	Sear

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.

5610V5_CERT > Provisioning > Port						1	?
nemet Ports FC Ports Port Groups Band Ports	VLAN Logical Ports Failover Groups						
Create) (Delete) (Properties) (Failback) (Act	tivale) (Deactivale) (Roule Management	Refresh		N	lame 👻 Keyword	Search	
Name Running Status Status Link up Adwated	IPv4 Address IPv6 Addr	Logical Port Properties: 129.115.56.1	x le	Data Protocol NFS+CIFS	Manage Access WEB+REST API	VStore Name	Home
		A Nalin: I Pl Address: I Pl Address: Subnet Maak: Ph4 Gateway: Subnet Maak: Ph4 Gateway: Subnet Maak: Ph4 Gateway: Ph4 Factor Ph4 Gateway: Ph4 Factor Ph4 Gateway: Ph4 Factor Ph4 Gateway: Ph4 Factor Ph4 Factor	m)				Syster Syster Provision Usta Provision Vistore Data Prote Monto Setting Suppo

Enabling auditing

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

 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.

Cluster10GE > Settings > Storag	s Settings ?	
File Storage Service	🔯 Sat the operation log parameters of clients accessing shared directories.	
CIFS Service	File Directory Operation Log	命
FTP Service	Record Type: Create Cleate Read Write Rename	Home
HTTP Service	Log save year: (Browse,) To answer hells are not according to a strange with the file of a strange with an file to the set. Yes are not action to another up the set to act.	
Domain Authentication	re ensore that the topic street can observe the press, to incrimination into one one, priministron on the press, to one into asserve to consigner the doubt ministration. An empty interdor is recommended for saving logs. To not reader, defend on effectively.	System
NDMR Settings >	* Log Space Capacity: 500 GB 👻 (250GB-319)	GA
/alue-added Service Settings	When the used log space exceeds the specified value, log files are deleted cyclically.	Provision
		\bigcirc
		Data Prote
		-4-
		Alarms
		ŝ
		Setting
		0
		Suppo

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

Me OceanStor Dev	iceManager 🕘 * Alarms: 🕐 Critical 0 🚱 Major 4 🕕 Warning 48 [榆体中文] 🕒 💮 .	eService
• 5610V5_CERT > Settin	gs > Monitor Settings ?	•
Parameter Settings Dump Settings Audit Log Settings	y write a warding op is, the source and is contained in the quantity and storage labe system. To save storage space, you can manually delete awdit logs that are ponerated within a specific period of time. MAS protocol Bender Log Size (UB): Image: Contained and the quantity of the source in the capacity of the awdit log is has are ponerated within a specific period of time. Addomatically Delete: Image: Contained and the capacity of the awdit log is system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. If the capacity specified by this parameter is greater than the capacity of the awdit log life system. Automatically Interrupt to MS Service: Image: Imag	Anne Bystem Come Provisioning Vistore Vistore Data Protection Monitor Settings (?)

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.

 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.

,				TESTAuditLog @	TESTAuditLo	og @			
Crea	te C	reate From	Prote	Summary Shares	Basic Information	on			
	Ni Q 4F	Ownin	Capa		Share Name	TESTAuditLog		Owning vStore	test_Vs
	yydat	Syste	500	NFS Shares C	Share Path	/TESTAuditLog/		Homedir	No
		-	500.	To view CIFS Homedir shar	Notify	Enabled		Continuously Avail	able Enable
	psm	Syste	500.	Create Delete	SMB3 Encryption	Disabled		Unencrypted Clien	t Access Disable
	SHAR	Share			ABE	Disabled		Show Snapshot	Enabled
			200.0	Share Name Q 1	Description				
	ICAP0	ICAP	200.	TESTAuditLog	Permissions	File Name Exten	sion Filtering Rule	5	
	ICAP-Q	ICAP	2001		CIFS shares are acc	cessible only to use	ers or user groups in t	he permission list.	
			200.		Add R	emove			
	MEtest	ME	100.		User or Use	er Group Q	Туре	Permissio	on 🍸
	Test_fi	test_V	5.		Everyone		Local Windows aut	henti Read-or	nly
	TESTA	test_V	4 5,	Total: 1. Selected: 1	win2012r	2ad0\testvstore	AD domain user	Read-or	nly
	ikrtost	ME		Only show shares of th					

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 v	
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.

Select the file system	operations to be recorded:	
< Create	🛃 Read	Obtain security properties
✓ Delete	Rename	Set security properties
✓ Write	List folders	Obtain extension properties
🗹 Open	Obtain properties	Set extension properties
 Close 	Set 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 vStoreO for all the vStores.
- 5. Click Next.

🕰 🔹 Search Reports [Ctrl+Space	File Audit Reports 👻	Add File Servers		× EMC 🔓 V	findows File Server 🛛 🔒 Windows File Cluster
Configured Server(s) Windows File Server Windows File Cluster	• Huawei OceanS	Select Server 2 Select User	3 Select VStore(5) (4 Select Share(s) (5 Select Audit Log Path		×
NetApp Server EMC Isilon	Domain WIN201	NAME	1-6 of 6	25-	+ Add Server
Hitachi NAS Huawei OceanStor EMC Server	< ⊘ Ø ¥	S300V5	WIN2012R2AD.com/Computers/5300V5		1-1 of 1 25 v
Synology NAS	ACTIO	5300V5_VSTORE	WIN2012R2AD.com/Computers/5300V5_VSTORE		STATUS
File Audit Reports	``□ ⊙⊀	O 5610V5	WIN2012R2AD.com/Computers/5610V5	un Now)	Error - A user selects a 🗈
User Based Reports	•	O 5610V5_VSTORE1	WIN2012R2AD.com/Computers/5610V5_VSTORE1		1-1 of 1 25 *
Share Based Reports	•	9000/5	WIN201282AD.com/Computers/9000V5		
Profile Based Reports	•	0 1/57085001	Water 1201201	_	
Configuration	•	VSTOREDUT	WINZUT2RZAD.com/Computers/VSTOREDUT	_	
				I	

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**.

ADAudit Plus									🖶 Purcha	ise Now License 🤌 Jobs ?
Dashboard Rep	orts Azure AD	File Audit	Server Audit	Analytics	Alerts	Configuration	Admin	Support		Q Search O Domain Sett
Configured Domair	i(s)									+ Add Domain
adaudit.com -	adapdevelope	rs.com •								
 Modify credential Update Domain C 	s lers Dbjects	Managed Domai	n Computers							Audit Policy :Successfully Configured.
Delete domain Attach AzureADD	S Domain									1-2 of 2 25 - ▼ Filter
ACTION	S	DOMA	IN CONTROLLER NA	ME 🔺	EVENT	FETCH INTERVAL	TIME	STAMP OF LAST EVENT	LAST EVENT READ TIME	STATUS
□ ⊘ ●) 🖅 🖻, 💼	adaud	it-dc2.adaudit.com		RealTin	ne 🖌	Dec 0	5,2022 12:44:28 PM	Dec 05,2022 12:44:29 PM	Listening for events
_ ⊘ ●) 🖾 🖻, 💼	adaud	it-dc1.adaudit.com		RealTin	me 🖌	Dec 0	05,2022 12:39:33 PM	Dec 05,2022 12:39:38 PM	Listening for events
										1-2 of 2 25 🔺
										+ Add Domain Controller

- 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.

				🕞 Purchase Now 🛛 Jui	mp to License 🔎 Jobs ? 🙆 🕶
ADAudit Plus	Dashboard Reports	File Audit Server Audit Analytics Al	lerts Configuration Admin Support		Q Search O Domain Settings
Q Search Reports [Ctrl+Space]	File Audit Reports 👻	Add File Servers		× EMC 🔡 Wir	idows File Server 🛛 🗜 🛛 Windows File Cluster
Configured Server(s)	-				
Windows File Server		🕦 Select Server 🛛 🔗 Select User	3 Select VStore(S) 4 Select Share(s) 5 Select Audit Log Path		
Windows File Cluster	Huawei OceanSt				
NetApp Server	Domain WIN2012	Version :	V5 Series 🗸		+ Add Server
Hirachi NAS		UserName :			
Huawei OceanStor					
EMC Server	<	Password :			1-1 of 1 25.∞
Synology NAS	ACTION	Scope :	Domain User 🗸		STATUS
File Audit Reports	۶ O P	*This can be left blank, if user configured for the	e domain has to be used	un Now)	Error - A user selects a 🗳
Server Based Reports	•				
User Based Reports	•				1-1 07 1 25 *
Share Based Reports	•				
Profile Based Reports	•				
Configuration	•				
			Back Ouit Next		
					E

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.

ADAudit Plus	Dashboard Reports	File Audit Server /	Audit Analytics Ali	erts Configuration .	Admin Support		Purchase No	w Jump to License م	斗 Search O Domain Settin
Contemports (Ctrl+Space)	File Audit Reports 👻	Add File Servers					× EMC	🔓 Windows File Server	F 🕹 Windows File Cluste
Configured Server(s)	~								×
Windows File Server		Select Server	2 Select User	3 Select VStore(S)	Select Share(s)	5 Select Audit Log Path			
Windows File Cluster	Huawei OceanSto					-			
NetApp Server	Domain WIN2012F	q				1-3 of 3 25 ▾ 😌			+ Add Serve
Hirachi NAS			NAME		LOCAL PATH				
Huawei OceanStor									
EMC Server	Q Q Q	\checkmark	\\5610V5\auditlog5610v5		C:\auditlog5610v5\				1-1 of 1 25 -
Synology NAS	ACTIONS		\\5610V5\test1		C:\FileSystem0047771\			STATUS	
ile Audit Reports	<u>۶</u> 📀 ک		115610V51tort5610v5		Cutort6610x6		un Now]	Error - A us	er selects a 💷 🗳
erver Based Reports	•		(Jorovo (lestorrovo		CatestS010454				
ser Based Reports	•								1-1011 25*
hare Based Reports	•								
rofile Based Reports	•								
onfiguration	•								
					1000				
				Back Quit	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**.

ADAudit Plus	Renords BriteAndrin Server Audit: Analytics Alerts Configuration Admin Support	Purchase Now Jump to License ² Jobs ? O -
C Search Reports [Ctrl+Space] File Audit Re	Add File Servers	🗙 EMC 🛛 🖥 Windows File Server 🛛 🔂 Windows File Cluster
Configured Server(s) File Audit Re Vindows File Server Huawei Windows File Cluster Huawei NetApp Server Domain Hitach NAS Image: Server Huawei DroanStor Image: Server Synology MS Image: Server Share Based Reports Image: Server Configuration Image: Server Share Based Reports Image: Server Configuration Image: Server	Select Server Select User Select VStore(5) Select Share(a) Select Audi VVIN2012F Log file location(UNC path): US610/51 US610/51 C TONE P P P P	x ENC Big Windows File Server R: Windows File Cluster it Lag Path x it Lag Path it Lag
	Back Quit OK	
		6

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 \rightarrow Go to the **File Audit** tab, navigate to the left pane, click on **Configuration** and then on **Exclude Configuration** \rightarrow Choose to exclude by **File/Folder** local path, **File Type, Process Name**, or Users \rightarrow 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	C:\sharefolder\excludefolderC:\sharefolder\excludefolder*			
What will get excluded	 C:\sharefolder\excludefolder C:\sharefolder\excludefolder\folder C:\sharefolder\excludefolder\files.txt C:\sharefolder\excludefolder\folder\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\AppDataC:\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.txtC:\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
- 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:

- 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.
- 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.

Our Products

AD360 | Log360 | ADManager Plus | ADSelfService Plus | DataSecurity Plus | M365 Manager Plus

About ADAudit Plus

ADAudit Plus is a UBA-driven auditor that helps keep your AD, Entra ID, file systems (including Windows, NetApp, EMC, Synology, Hitachi, Huawei, Amazon FSx for Windows, Azure and QNAP), Windows Server, and workstations secure and compliant. ADAudit Plus transforms raw and noisy event log data into real-time reports and alerts, enabling you to get full visibility into activities happening across your Windows Server ecosystem in just a few clicks. For more information about ADAudit Plus, visit manageengine.com/active-directory-audit.