ManageEngine

Windows server auditing guide



www.adauditplus.com

Table of Contents

Document summary	3				
1. Configure Windows servers in ADAudit Plus	4				
1.1 Using product console					
1.2 Using command line arguments	4				
2. Configure audit policies in your domain	5				
2.1 Automatic configuration	5				
2.2 Manual configuration	6				
2.2.1 Configure list of Windows servers to be audited	6				
2.2.2 Configure advanced audit policies	7				
2.2.3 Force advanced audit policies	9				
2.2.4 Configure legacy audit policies	10				
3. Configure event log settings in your domain	12				
4. FAQ	13				

Document summary

A Windows member server is a computer that runs on Windows Server, belongs to a domain, and is not a domain controller. Windows member servers typically run different services and can act like a file server, print server, etc. For the sake of convenience, Windows member servers will be referred to as Windows servers in this guide.

ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps keep your Windows servers secure and compliant. With ADAudit Plus, you can:

- Monitor file integrity.
- Audit local logon and account management.
- Track printer, removable storage, AD FS, AD LDS, and LAPS activities.
- Keep tabs on scheduled tasks and processes.

ADAudit Plus enables you to audit the following versions of Windows Server:

- Windows Server 2008/2008 R2
- Windows Server 2012/2012 R2
- Windows Server 2016
- Windows Server 2019
- Windows Server 2022

This guide takes you through the process of setting up ADAudit Plus and your Windows servers for real-time change auditing and user behavior analytics.

1. Configure Windows servers in ADAudit Plus

1.1 Using product console

From the product console up to a 100 windows servers can be configured at a time, to do this: Log in to the ADAudit Plus web console. Go to the **Server Audit** tab \rightarrow **Configured Servers** \rightarrow **Member Servers** \rightarrow **Add Server.** Enter the details needed to complete the configuration.

Note: ADAudit Plus can automatically configure the required audit policies for Windows server auditing. In the final step, you can either choose **Yes** to let ADAudit Plus automatically configure the required audit policies, or choose **No** to manually configure the required audit policies.

Audit Plus	lome Reports File A	udit Server Audit Analytics Alerts Conf	iguration Admin Suppo	ort Q	Search 🔅 Domain Se
Server Audit Repo	Computers			>	Aggregate Repo
gured Server(s)					
ember Servers Men	hber Servers Active M	ember Servers			
orkstations ent Subscriptions				1-1 of 1 25 🗸 😌	+ Add Server
e Integrity	NAME	CANONICAL NAME			udit Policy:Configure
nt Server	ADAP-CLUSTER	adap.internal.com/Computers/ADAP-CL	USTER		
orkgroup Servers					25 🗸 📉 🔻 Filter
ntegrity Monitoring					
itorage Auditing					
er Auditing					ess is denied 🗳
OS Auditing					
Auditing					ess is denied 🗳 🛛
Auditing					
ork share Auditing					RPC server is 🗳
Logon-Logoff		OK Cancel			
					ass is denied

1.2 Using command line arguments

Using command line arguments all Windows servers in your environment can be configured at a time, to do this:

Create a CSV file by the name 'servers.csv' in the location <installation dir>\ManageEngine\
 ADAudit Plus\bin. From the Encoding tab, save the document in UTF-8 format. → Open the file, enter
 the names of all Windows servers (that you want to audit) in adjacent lines, and separate
 them using commas.

For example, to add the file servers Test-MS1, Test-MS2, and Test-MS3; open the servers.csv file and enter:

Test-MS1,

Test-MS2,

Test-MS3

Navigate to <installation dir>\ManageEngine\ADAudit Plus\bin. → Open command prompt and execute 'cmdUtil.bat'. → Enter ADAudit Plus' default admin credentials. →
 Note: ADAudit Plus' default username and password are both 'admin'.
 And execute the following command:
 config server add -machinetype ms -isauditpolicy true (or) false

After -isauditpolicy, enter **'true'** to automatically configure the required object access audit policy and **'false'** to manually configure the required object access audit policy.

For example, if you want to audit all Windows servers and configure the required audit policies automatically; execute the following command: config server add -machinetype ms -isauditpolicy **true**

2. Configure audit policies in your domain

Audit policies must be configured to ensure that events are logged whenever any activity occurs.

2.1 Automatic configuration

Log in to the ADAudit Plus web console. Go to the Server Audit tab \rightarrow Configured Servers \rightarrow Member Servers \rightarrow Audit Policy: Configure.

Note: ADAudit Plus can automatically configure the required audit policies for Windows server auditing. After clicking **Audit Policy: Configure** in the above step, you can either choose **Yes** to let ADAudit Plus automatically configure the required audit policies, or choose **No** to manually configure the required audit policies.

ADAudit Plus	Home	Report	s File Audit	Server Audit Ana	llytics Alerts	Configuration Admin	Jump to L Support	icense 斗 Jobs ? 😣 Q Search O Domain Setti
🗙 Server Audit Reports 👻	Local Lo	gon-Logoff 🔻	 File Integrity 	Monitoring 🗸 🔰 Printer	Auditing 👻		🛃 Custom	Reports 🛛 🖟 Aggregate Report
onfigured Server(s) Member Servers	-	Member	Server Configu	iration				
Workstations		Domain	adap.internal.com	~				+ Add Serve
Event Subscriptions		Configure	ad Member Ser	ver(c)				
File Integrity		configure	eu member ser	ver(5)				Audit Policy:Configur
Print Server								
Workgroup Servers		¢ ⊘	o 🐨 🗄 🖸	• Run now A - Z				1-19 of 19 25 🗸 🔻 Filter
le Integrity Monitoring	•			MEMBER SERVER	EVENT CETCH	TIMESTAMP OF LAST		
SB Storage Auditing	•		ACTIONS		INTERVAL	EVENT	LAST SCHEDULE RUN AT	STATUS
rinter Auditing	•			ADAP-CLUSTER1	Every 2 hours 💉	Jan 16,2019 10:53:58	Jun 19,2019 01:51:19 PM	Error - Access is denied 🗳
D LDS Auditing	•					AM	[Run Now]	
DFS Auditing	•			ADAP-CLUSTER2	Every 2 hours 💉	Jan 16,2019 11:01:06	Jun 19,2019 01:50:51 PM	Error - Access is denied 🗳
DAP Auditing	•					AM	[Run Now]	
etwork share Auditing	•		Ø ফ 🖾	ADAP-DCTEMP	Every 2 hours 💉	Yet to fetch event data	Jun 19,2019 01:33:04 PM [Run Now]	Error - The RPC server is 🗳
ocal Logon-Logoff	•			ADAP-MS1	Every 2 hours 🖌	Apr 08,2019 02:55:06	Jun 19,2019 01:21:00 PM	Error - Access is denied 🗳
					· · ·			

2.2 Manual configuration

2.2.1 Configure list of Windows servers to be audited

- 1. Open Active Directory Users and Computers.
- 2. Right-click the domain and select New > Group.
- In the New object Group window that opens, type in "ADAuditPlusMS" as the Group name, check Group scope: Domain Local and Group type: Security. Click OK.
- Right-click the newly created group and select Properties > Members > Add. Add all the Windows servers that you want to audit as a member of this group. Click OK.
- Using domain admin credentials, log in to any computer that has the Group Policy Management Console (GPMC) on it.

Note: The GPMC will not be installed on workstations and/or enabled on member servers by default, so we recommend configuring audit policies on Windows domain controllers. Otherwise follow the steps in this page to install GPMC on your desired member server or workstation.

- 6. Go to Start > Windows Administrative Tools > Group Policy Management.
- In the GPMC, right-click the domain in which you want to configure the Group Policy. Select Create a GPO and Link it here. In the New GPO window that opens, type in "ADAuditPlusMSPolicy" and click OK.
- Select the ADAuditPlusMSPolicy GPO. Under Security Filtering, select Authenticated Users.
 Click Remove. In the Group Policy Management window that opens, select OK.
- 9. Select the ADAuditPlusMSPolicy GPO. Under Security Filtering, click Add and choose the security group ADAuditPlusMS created previously. Click OK.

Koroup Policy Management		- 🗆 X
属 File Action View Window Help		_ & ×
 File Action View Window Help Action View Help Action View	ADAuditPlusMSPolicy Scope Details Settings Delegation Status Links Display links in this location: adapworkshop.com The following sites, domains, and OUs are linked to this GPO: Location Enforced Link Enforced Ink Enforced Ink Enforced Ink Enforced Ink Enforced Ink Enforced Ink Enforced	abled Path adapworkshop.com
GP012 GP02 GPOfororgtest11 GPOnetlogon han hanige hanitestOU haniy test HaniyGPO haniy-gpo hi New Group Policy Object New Group Policy Object1 New Group Policy Object1 New Group Policy Object1 newgpo100	Security Filtering The settings in this GPO can only apply to the following groups, users, and convertings Name ADAudtPlusMS ADAudtPlusMS ADAudtPlusMS Add Remove Properties WMI Filtering This GPO is linked to the following WMI filter: (none>	imputers:

2.2.2 Configure advanced audit policies

Advanced audit policies help administrators exercise granular control over which activities get recorded in the logs, helping cut down on event noise. We recommend configuring advanced audit policies on Windows Server 2008 and above.

- **1.** Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, then right-click **ADAuditPlusMSPolicy** and select **Edit.**
- 2. In the Group Policy Management Editor, go to Computer Configuration \rightarrow Policies \rightarrow Windows Settings
 - \rightarrow Security Settings \rightarrow Advanced Audit Policy Configuration \rightarrow Audit Policy. Double-click on the relevant policy setting.
- Navigate to the right pane and right-click on the relevant Subcategory. Select Properties, then choose Success, Failure, or both, as directed in the table below.

ManageEngine) ADAudit Plus

Category	Subcategory	Audit Events
Account Management	 Audit Computer Account Management Audit Distribution Group Management Audit Security Group Management 	✓ Success
	 Audit User Account Management 	✓ Success and Failure
Detailed Tracking	 Audit Process Creation Audit Process Termination 	✓ Success
DS Access	 Audit Directory Service Changes Audit Directory Service Access 	 ✓ Success
Logon/Logoff	Audit LogonAudit Network Policy Server	 Success and Failure
	 Audit Other Logon/Logoff Events Audit Logoff 	 ✓ Success
Object Access	 Audit File System Audit Handle Manipulation Audit File Share 	✓ Success and Failure
Policy Change	 Audit Authentication Policy Change Audit Authorization Policy Change 	 ✓ Success
System	 Audit Security State Change 	 ✓ Success

ManageEngine) ADAudit Plus



2.2.3 Force advanced audit policies

When using advanced audit policies, ensure that they are forced over legacy audit policies.

1. Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC,

right-click ADAuditPlusMSPolicy, then select Edit.

2. In the Group Policy Management Editor, go to Computer Configuration \rightarrow Policies \rightarrow Windows

Settings \rightarrow Security Settings \rightarrow Local Policies \rightarrow Security Options.

Navigate to the right pane, then right-click Audit: Force audit policy subcategory settings.
 Select Properties, then Enable.

<u>.</u>		Group Policy Management Editor			_	x
File Action View Help						
🗢 🔿 📶 🗙 🗊 🔂 🔟 🗊						
ADAuditPlusMSPolicy	~	Policy		Policy Setting		 ^
🖌 📻 computer configuration		Accounts: Administrator account status		Not Defined		
⊿ 🚆 Policies		🖏 Accounts: Block Microsoft accounts		Not Defined		
Software Settings		🕼 Accounts: Guest account status		Not Defined		
⊿ indows Settings		🕅 Accounts: Limit local account use of blank passwords to console logon onl	1	Not Defined		=
Name Resolution Policy		🕃 Accounts: Rename administrator account		Not Defined		
Scripts (Startup/Shutdown)		🕃 Accounts: Rename guest account		Not Defined		
Deployed Printers		🖏 Audit: Audit the access of global system objects		Not Defined		
A security Settings		🔯 Audit: Audit the use of Backup and Restore privilege		Not Defined		
Account Policies		🏽 Audit: Force audit policy subcategory settings (Windows Vista or later) to o	erride audit policy categ	Enabled		
	=	Audia Francisculta a line and anatomical and 2 X		Not Defined		
Licer Rights Assignment		Audit: Force audit policy subcategory settings wi	(SDDL) syntax	Not Defined		
Security Options		Security Policy Setting Explain	e (SDDL) syntax	Not Defined		
Event Log			1	Not Defined		
Restricted Groups		Audit: Force audit policy subcategory settings (Windows Vista or		Not Defined		
System Services		later) to override addit policy category settings		Not Defined		
Registry		Define this policy setting:		Not Defined		
File System		Enabled		Not Defined		
Wired Network (IEEE 802.3) Policies				Not Defined		
Windows Firewall with Advanced Security	-11	 Disabled 		Not Defined		
Network List Manager Policies				Not Defined		
Wireless Network (IEEE 802.11) Policies				Not Defined		
Public Key Policies				Not Defined		
Software Restriction Policies				Not Defined		
Intwork Access Protection				Not Defined		
Application Control Policies	~			Not Defined		
< III >				Not Defined		~
ntelle" – Stati taivie a – Statis						
www.mainet.com/angle.com/angl						
이 왜 있는 것 같은 것 같은 것 같은 것 같은 것 같이 않는 것 같이 않는 것						
이상에 다 집에서 이렇는 것 같아요. 것이 나 있는 것이 없는 것이 없다.						
		OK Cancel Apply		і (1-41) - 431 1 - 431 1 - 63 - 63 - 11 - 11 - 11		

2.2.4 Configure legacy audit policies

Due to the unavailability of advanced audit policies in Windows Server 2003 and earlier versions, legacy audit policies need to be configured for these types of servers.

- Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, right-click ADAuditPlusMSPolicy, then select Edit.
- In the Group Policy Management Editor, go to Computer Configuration → Policies → Windows
 Settings → Security Settings → Local Policies, and double-click Audit Policy.
- Navigate to the right pane and right-click on the relevant policy. Select Properties, then choose Success, Failure, or both, as directed in the table below:

Category	Audit Events
Account Logon	✓ Success and Failure
Audit Logon/Logoff	✓ Success and Failure
Account Management	✓ Success
Directory Service Access	✓ Success
Process Tracking	✓ Success
Object Access	✓ Success
• System Events	✓ Success

🗾 Group Policy Management Edite	_		\times					
File Action View Help								
🗢 🔿 🙍 📷 🗙 🗟 🛙 🛛								
 ✓ Computer Configuration ∧ ✓ Policies > Software Settings ✓ Windows Settings > Name Resolut Scripts (Startu > Deployed Prin ✓ Security Settir > Account P ✓ Local Polic ✓ Audit I > User Ri > System Se > Registry > Registry > Windows I Network L > Wireless N > Public Key > Software F 	Policy Policy Setting Image: Audit account logon events Success, Failure Image: Audit account management Success Image: Audit directory service access Success Image: Audit logon events Success, Failure Image: Audit logon events Success, Failure Image: Audit logon events Success, Failure Image: Audit object access Success Image: Audit policy change Not Defined Image: Audit process tracking Success Image: Audit system events Success							

3. Configure event log settings in your domain

Event log size needs to be defined to prevent loss of audit data due to overwriting of events. To configure event log size and retention settings, follow the steps outlined below:

- Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, right-click ADAuditPlusMSPolicy, then select Edit.
- In the Group Policy Management Editor, select Computer Configuration → Policies → Windows
 Settings → Security Settings → Event Log.
- Navigate to the right pane and right-click on Retention method for security log.
 Select Properties → Overwrite events as needed.
- **4.** Navigate to the right pane, then right-click **Maximum security log size** and define the size as directed in the table below.

Role	Operating System	Operating System
Windows file server	Windows Server 2003	512MB
Windows file server	Windows Server 2008 and above	4,096MB



4. FAQs

1. To verify if the desired audit policies and security log settings are configured:

Log in to any computer that has the GPMC with Domain Admin credentials. Open the GPMC, right-click **Group Policy Results**, and open the Group Policy Results Wizard. Select the computer and user (current user), then verify if the desired settings as defined in step 2.2 are configured.

2. To verify if the desired events are getting logged:

Log in to any computer with Domain Admin credentials. Open **Run**, then type "eventvwr.msc". Right-click on Event Viewer. Connect to the target computer, then verify if events corresponding to the configured audit policies are getting logged.

For example, event ID 4768 should get logged when Success audit events is configured under the Audit Kerberos Authentication Service Subcategory, under the Account Logon Category (refer to step 2.2.1).

ManageEngine) ADAudit 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.

