

SGBox Windows Auditing

Configuration Guide

SGBox

SecureGate S.r.l.

Via Melchiorre Gioia, 168 - 20125 Milano (Italy) Tel: +39 02 60830172 - Fax: +39 02 60736014 - Email: info@sgbox.it www.sgbox.it





Index

1	Intro	oduction	3
2	Adva	anced Audit Policy Configuration	4
	2.1 2.1.1 2.1.2		4
	2.2 2.2.1 2.2.2 2.2.3 2.2.4	2 Domain Controller Auditing	7 10 13
3	Obje	ect-level access auditing configuration	22
	3.1	Active Directory Windows Server 2012 and higher	22
	3.2	Windows File Server 2012 and higher	26



1 Introduction

To collect all the logs necessary to audit Windows Servers and Workstations, you need to configure the Group Policies enabling auditing for those objects you want to monitor and, if you want to Audit Files activity, the ACLs for the folders you want to check have to be configured as well.

You can control file activities on both shared folders and not shared local folders.

The first step is to configure group policies, or local policies if the Server or Workstation to be controlled is not part of an Active Directory domain.

You must also configure ACLs for the folders and/or disks that you want to monitor, bearing in mind that to obtain audit events, both configurations must be active on the folder or disk to be audited. If acLs are not applied, or if group policies are not configured, the events required for auditing will not be raised.

Be careful that if you want to check the events relating to an Active Directory Domain, you will need to configure the Object Level Auditing also at the Domain level.



2 Advanced Audit Policy Configuration

To have more detail and greater control over the auditing levels activated, it is preferable to configure and use advanced auditing policies.

2.1 Preliminary Activities

Before you switch to group policy configuration, you need to configure a couple of things that are essential for the solution to work properly:

- Security Options
- Security event log size and its retention methodology

2.1.1 Security Options Configuration

If both basic and advanced audit policies are defined by chance, we would obtain incorrect audit values, to overcome this problem it is necessary to set up the Security Policy appropriately.

Verify that locally, on each Server/Workstation we are going to monitor, the Security Policy (1) Audit: Force audit policy subcategory settings to override audit policy category settings (2) is configured on Enabled (system default) so that basic audit policies are ignored in favor of advanced audit policies.

On the machines to be verified, open the Local Security Policy panel located in

Start -> Windows Administrative Tools -> Local Security Policy





2.1.2 Event Log Configuration

The configuration of the security event log features can be performed both locally, for each machine, and centrally through Group Policy.

It is also very important to configure the size and operating mode of the Security Log appropriately so that no events are lost in case of temporary lack of connection with the Server or the SGBox Collector.

2.1.2.1 Local Configuration

On the machines to be monitored, open the Event Viewer csnap-in located in *Start* -> *Windows Administrative Tools* -> *Local Security Policy*, expand *Windows Logs* menu entry, right click on **Security** (1) and choose **Properties** from the pop-up menu.

Position yourself on **Security** (1) and set the values as follows:

- Maximum log size (KB): 4194240 (2)
- check the radio button Overwrite events as needed (3)

and press **OK** (4) to save the configuration.





2.1.2.2 GPO Configuration

On the Domain Controller, open the Group Policy Management snap-in located in Start \rightarrow Windows Administrative Tools or Start -> Administrative Tools, depending on the Windows version.

Click on Event Log (1) and set policy values as follows:

- Maximum security log size:

4194240 kilobytes (2) **As Needed** (3)

- Retention method for security log:



Close the Snap-in and ensure that the policy is properly deployed.



2.2 GPO Advanced Audit Policy Configuration

You can both enclose all settings in a single GPO or create specialized GPOs for each of the four categories shown below.

2.2.1 Logon Activity Auditing

On the Domain Controller, open the Group Policy Management snap-in located in Start \rightarrow Windows Administrative Tools or Start -> Administrative Tools, depending on the Windows version.

Create a category-specific GPO, or use a general GPO, and configure the various options as follows.

2.2.1.1 Security Options

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policy* click on **Security Options** (1) and set the parameters (2) as shown in the picture.





2.2.1.2 Event Log

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings*, click on **Event Log** (1) and configure parameters (2) as shown in the figure.



2.2.1.3 Account Logon

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy* click on **Account Logon** (1) and configure parameters (2) as shown in the figure.





2.2.1.4 Logon/Logoff

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy, click on Logon/Logoff (1) and configure parameters (2) as shown in the figure.



2.2.1.5 System

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy* click on **System** (1) and configure parameters (2) as shown in the figure.





2.2.2 Domain Controller Auditing

On the Domain Controller, open the Group Policy Management snap-in located in $Start \rightarrow$ Windows Administrative Tools or Start -> Administrative Tools, depending on the Windows version.

Create a category-specific GPO, or use a general GPO, and configure the various options as follows.

2.2.2.1 Security Options

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policy,* click on **Security Options** (1) and configure parameters (2) as shown in the figure.

🗊 Group Policy Management Editor		-	- 🗆	×
File Action View Help				
Þ 🔿 🙋 📆 🗙 🗐 🛃 🛐				
Audit - Windows Logon Activity [ACMEDC ~ Audit - Windows Logon Activity [ACMEDC ~ Policies Software Settings Software Settings Software Settings Software Settings Software Settings Software Resolution Policy Scripts (Startup/Shutdown) Socurity Settings Socurity Settings Socurity Settings Socurity Optices Software Registry Software Restriction Pol Wireless Network (IEEE 802 Software Restriction Pol Software Restriction Pol	 Policy Accounts: Administrator account status Accounts: Block Microsoft accounts Accounts: Guest account status Accounts: Guest account use of blank passwords to co Accounts: Rename administrator account Accounts: Rename guest account Audit: Audit the access of global system objects Audit: Audit the access of global system objects Audit: Force audit policy subcategory settings (Windows Vis DCOM: Machine Access Restrictions in Security Descriptor D DCOM: Machine Access Restrictions in Security Descriptor T DCOM: Machine Access Restrictions in Security Descriptor Devices: Allow undock without having to log on Devices: Nevent users from installing printer drivers Devices: Restrict CD-ROM access to locally logged-on user Devices: Restrict Daver operators to schedule tasks Domain controller: LDAP server signing requirements Domain controller: LDAP server signing requirements Domain controller: Refuse machine account password chan Domain member: Digitally sign secure channel data (when 	Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined		
🗸 🦳 Advanced Audit Policy (Domain member: Disable machine account password chan	Not Defined		



2.2.2.2 Event Log

From Computer Configuration -> Policies -> Windows Settings -> Security Settings, click on **Event** Log (1) and configure parameters (2) as shown in the figure.



2.2.2.3 Account Management

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy click on Account Management (1) and configure parameters (2) as shown in the figure.





2.2.2.4 DS Access

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy click on DS Access (1) and configure parameters (2) as shown in the figure.





2.2.3 File Server Auditing

On the Domain Controller, open the Group Policy Management snap-in located in $Start \rightarrow Windows$ Administrative Tools or Start -> Administrative Tools, depending on the Windows version.

Create a category-specific GPO, or use a general GPO, and configure the various options as follows.

2.2.3.1 Security Options

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policy,* click on **Security Options** (1) and configure parameters (2) as shown in the figure.

Group Policy Management Editor			- 0	×
File Action View Help				
Þ 🔿 🚈 📰 💥 🖾 🔒 👔 🖬				
Audit - Windows Logon Activity [ACMED(Audit - Windows Logon Activity [ACMED(Policies Software Settings Mame Resolution Policy Scripts (Startup/Shutdown) Deployed Printers Security Settings Account Policies Account Policies Account Policies Account Policies Account Policies Account Policies Security Options Event Log Registry System Services Registry Sig System Sig System Wirelos Network (IEEE 802 Windows Firewall with A Network List Manager P Wireless Network (IEEE 8 Public Key Policies Software Restriction Pol Sig System Control Poli Application Control Poli	Policy Accounts: Administrator account status Accounts: Block Microsoft accounts Accounts: Block Microsoft accounts Accounts: Guest account status Accounts: Limit local account use of blank passwords to co Accounts: Rename administrator account Accounts: Rename administrator account Accounts: Rename guest account Accounts: Rename guest account Audit: Audit the access of global system objects Audit: Audit the use of Backup and Restore privilege Audit: Shut down system immediately if unable to log secur COM: Machine Launch Restrictions in Security Descriptor D COM: Machine Launch Restrictions in Security Descriptor m Devices: Allow undock without having to log on Devices: Allow undock without having to log on Devices: Restrict CD-ROM access to locally logged-on user m Domain controller: Allow server operators to schedule tasks Domain controller: LDAP server signing requirements Domain controller: DAP server signing requirements Domain controller: DAP server sign secure channel d Domain member: Digitally encrypt or sign secure channel data (wh)	Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined Not Defined		
> 🜏 IP Security Policies on A 🗸 🦳 Advanced Audit Policy (🗸	Domain member: Digitally sign secure channel data (when	Not Defined		
	Domain member: Disable machine account password chan	Not Defined		



2.2.3.2 Event Log

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings*, click on **Event Log** (1) and configure parameters (2) as shown in the figure.



2.2.3.3 Logon/Logoff

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy, click on Logon/Logoff (1) and configure parameters (2) as shown in the figure.





2.2.3.4 Object Access

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy, click on **Object Access** (1) and configure parameters (2) as shown in the figure.



2.2.3.5 Policy Change

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy, click on Policy Change (1) and configure parameters (2) as shown in the figure.





2.2.3.6 System

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy, click on **System** (1) and configure parameters (2) as shown in the figure.

Group Policy Management Editor			_	Х
File Action View Help				
 IP Security Policies on Active Directory (ACN Advanced Audit Policy Configuration Advanced Audit Policy Configuration Account Logon Account Management Detailed Tracking DS Access Cogon/Logoff Object Access Policy Change Privilege Use System Global Object Access Auditing Policy-based QoS Administrative Templates: Policy definitions (ADM) efferences Configuration Sicies Sonface 	Subcategory Audit IPsec Driver Audit Other System Events Audit Security State Change Audit Security System Extension Audit System Integrity	Audit Events Not Configured Not Configured Success Not Configured Not Configured	2	



2.2.4 Windows Servers and Workstation Auditing

On the Domain Controller, open the Group Policy Management snap-in located in $Start \rightarrow Windows$ Administrative Tools or Start -> Administrative Tools, depending on the Windows version.

Create a category-specific GPO, or use a general gpo, and configure the various options as follows.

2.2.4.1 Security Options

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Local Policy,* click on **Security Options** (1) and configure parameters (2) as shown in the figure.



2.2.4.2 Event Log

From Computer Configuration -> Policies -> Windows Settings -> Security Settings, click on **Event** Log (1) and configure parameters (2) as shown in the figure.



2.2.4.3 Account Management

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy, click on Account Management (1) and configure parameters (2) as shown in the figure.





2.2.4.4 Detailed Tracking

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Detailed Tracking** (1) and configure parameters (2) as shown in the figure.



2.2.4.5 Object Access

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Object Access** (1) and configure parameters (2) as shown in the figure.





2.2.4.6 Policy Change

From *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, click on **Policy Change** (1) and configure parameters (2) as shown in the figure.



2.2.4.7 Privileged Use

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy, click on **Privileged Use** (1) and configure parameters (2) as shown in the figure.





2.2.4.8 System

From Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy, click on System (1) and configure parameters (2) as shown in the figure.





3 Object-level access auditing configuration

3.1 Active Directory Windows Server 2012 and higher

If you want to collect information on user activity in the domain, it is necessary to configure Object-level auditing for the Domain partition also.

If you also want to check for changes to the AD Configuration and Schema, you must also enable Object-level auditing for Configuration and Schema partitions.

Please follow the procedure below for each Domain or Organizational Unit you wish to control.

 From any Domain Controller belonging to the Domain you want to control, open the Active Directory Users and Computers snap-in located in Start → Windows Administrative Tools or in Start -> Administrative Tools, depending on the Windows version.

Click on the View tab and verify that Advanced Features is selected.

Active Directory Users and Computers		-	\times
File Action View Help			
< < 🔁 🚦 Add/Remove Columns			
Active Dire Large Icons	Description		
> 📫 Saved 🤇 Small Icons			
→ 🛱 acme.le List			
> C Detail			
Users, Contacts, Groups, and Computers as containers			
Cor Advanced Features			
Dor Filter Options			
For Customize			
Keys LostAndFound			
Managed Service Accour			
> Program Data			
> System			
Sers Users			
> 📫 NTDS Quotas			
> 📫 TPM Devices			
< >>			
Enables/disables advanced features and objects			



2) Right click on the Domain node you want to control and select Properties.

Active Directory Us	ers and Com	Name		Туре
> 📫 Saved Queries		ACMEWS001		Computer
✓ ∰ acme.loca' ✓ ☑ Acme	Delegate Co	ontrol		Computer
> 🖬 Grc 📓 Use 🎬 Builtin 🎬 Compi 🗃 Domai	Raise domai	main Controller in functional level		
Coreigi Keys LostAr Manac	Operations New All Tasks	Masters	>	
> Progra	Refresh			
📔 Users	Properties			
> 🚆 NTDS (> 🚆 TPM D	Help			

- 3) Within the Propertis panel select the **Security** tab then click on the button **Advanced** in the lower right corner.
- 4) In the "Advanced Security Settings" panel select the Auditing tab.

Adva	anced S	ecurity Settings for acme			- 0
Owne	er:	Administrators (ACME\Admin	istrators) Change		
Perm	nissions	Auditing Effective Ac	cess		
	dditiona ting entr	el information, double-click an au	dit entry. To modify an a	udit entry, select the entr	y and click Edit (if available).
1	Туре	Principal	Access	Inherited from	Applies to
<u>82</u> s	Succ	Everyone		None	Special
<u>88</u> S	Succ	Everyone		None	Special
<u>88</u> S	Succ	Domain Users (ACME\Domai	All extended rights	None	This object only
	Succ		All extended rights	None	This object only
<u>8</u>	Succ	Everyone	Special	None	This object and all descendant
4	Add	Remove View			Restore defaults
				[OK Cancel Apply

Click on the **Add** button and then, within the "Auditing Entry" panel, select the **Select a principal** link.



Principal:	Select a principal	—					
Туре:	Success	\sim					
Applies to:	This object and all de	Select User, Computer, Service Account, o	r Group	×	:		
		Select this object type:					
		User, Group, or Built-in security principal		Object Types			_
ermissions	s:	From this location:					
	Full control	acme.local		Locations			
	✓ List contents	Enter the object name to select (examples):		_ ·			
	Read all properties	everyone		Check Names			
	Write all properties	everyoner		Check Names	objects		
	Delete				bjects		
	Delete subtree	Advanced	ОК	Canaal			
	Read permissions	Advanced	UK	Cancel			
	Modify permissions		Create msSFU3	0NetId objects			
	Modify owner		Delete msSFU3	0NetId objects			
	All validated writes		Create msSFU3	0NetworkUser obje	cts		
	All extended rights		Delete msSFU3	0NetworkUser obje	cts		
	Create all child obje	cts	Create msTPM	-InformationObject	tsContainer objects		
	Delete all child obje	cts	Delete msTPM-	-InformationObject	tsContainer objects		
	Create Computer of	bjects	Create nisMap	objects			
	Delete Computer ob	ojects	Delete nisMap	objects			
	Create Contact obje	ects	Create nisNetg	roup objects			

5) In the "Select User, Computer, Service Account, or Group" panel type everyone in the Enter the object name to select field, then confirm clicking the OK button.

Back in the "Auditing Entry" panel, set the **Type:** field to "Success" and the **Applies to:** field on "This object and all descendant objects".

📕 Auditing E	intry for acme				×
Principal:	Everyone Select a principal				Î
Type:	Success	\sim			
Applies to:	This object and all descendant objects	\sim			
Permission	5:				
	Full control		Delete msImaging-PSPs objects		
	List contents		Create MSMQ Queue Alias objects		
	Read all properties		Delete MSMQ Queue Alias objects		
	Write all properties		Create msPKI-Key-Recovery-Agent objects		
	✓ Delete		Delete msPKI-Key-Recovery-Agent objects		
	Delete subtree		Create msSFU30MailAliases objects		
	Read permissions		Delete msSFU30MailAliases objects		
	Modify permissions		✓ Create msSFU30NetId objects		
	Modify owner		Delete msSFU30NetId objects		
	All validated writes		Create msSFU30NetworkUser objects		
	All extended rights		Delete msSFU30NetworkUser objects		
	Create all child objects		Create msTPM-InformationObjectsContainer objects		
	Delete all child objects		Delete msTPM-InformationObjectsContainer objects		
	Create Computer objects		✓ Create nisMap objects		
	Delete Computer objects		Delete nisMap objects		
	Create Contact objects		Create nisNetgroup objects		



- 6) In the **Permissions** box, select all the checkboxes but the following:
 - Full Control
 - List Contents
 - Read All Properties
 - Read Permissions
- 7) Check that at the end of the Permission box, the checkbox **Only apply these auditing settings to objects and/or containers within this container** <u>is not</u> selected and click the **OK** button to confirm changes.



3.2 Windows File Server 2012 and higher

Object-level access auditing configuration is essential to be able to collect audit events generated by the Advanced Audit Policy specified above.

By configuring Object-level access auditing we will specify which event classes to collect and which users to monitor.

Follow these steps for each folder or disk that you want to monitor.

1) Right-click the folder you want to monitor and select **Properties** from the pop-up menu. Select the **Security** tab (1) and then click **Advanced** (2).

AcmeShare Properties	×
General Sharing Security Previous Versions Customize	
Object name: E:\AcmeShare	
Group or user names:	
SECREATOR OWNER	^
SYSTEM	
Rider I Hente Ansen (I Hente X@some local)	¥
< >>	
To change permissions, click Edit. Edit	
Permissions for CREATOR	
OWNER Allow Deny	_
Full control	^
Modify	
Read & execute	
List folder contents	
Read	
Write	~
For special permissions or advanced settings, Advanced click Advanced.	
2	
OK Cancel Ap	oly



2) Select the Auditing tab and click Continue (2)

Advanced Sec	urity Settings for A	cmeShare				×
Name: Owner:	E:\AcmeShare Rider 💎 Chang	e	1			
Permissions	Share	Auditing	Effective Access			
Contin		2				

3) click the Add button (1) to add a new auditing permission configuration.

	ecurity Settings for	AcmeShare					×
Name:	E:\Test\AcmeSł	hare					
Owner:	Rider (ACME\R	ider) Change					
Permissions	Auditing	Effective Acce	255				
For additional Auditing entri		ble-click an audit	entry. To modi	fy an audit entry, select the entry	and click Edit (if availab	ole).	
Туре	Principal		Access	Inherited from	Applies to		
	•						
و	D						
Add	Remove	View					
Add Disable inh		View					
Disable inh	neritance		sheritable auditi	ing entries from this object			



4) Click the **Select a principal** link in the top-left corner to add a new principal. Then select **Everyone** (1), or any custom group that contains the users for whom you want to monitor access.

Auditing Entry for AcmeShare		>
elect User, Computer, Service Account, or Group	×	
Select this object type:		
User, Group, or Built-in security principal	Object Types	
rom this location:		
acme.local	Locations	
Inter the object name to select (examples):		
everyone	Check Names	Show advanced permissions
Advanced	OK Cancel	
Read		
Write		
Special permissions		
Only apply these auditing settings to objects and/	or containers within this container	Clear all
Add a condition to limit the scope of this auditing er	try. Security events will be logged only if conditions are	met.
Add a condition		
		OK Cancel

You can now set the audit entries for the access types you want to control. The configurations needed are shown below:

5) Read access succeeded

Auditing E	ntry for AcmeShare	>
Principal:	Everyone Select a principal	
Type:	Success	 ✓ ← 1
Applies to:	Files only	⊻ ← 2
Advanced p	permissions:	3 Show basic permissions
	Full control	Write attributes
	Traverse folder / execute file	Write extended attributes
	List folder / read data	Delete subfolders and files
	Read attributes	Delete
	Read extended attributes	Read permissions
	Create files / write data	Change permissions
	Create folders / append data	Take ownership
Only app	ly these auditing settings to objects and/or conta	ners within this container
Add a cond	ition to limit the scope of this auditing entry. Sec	ity events will be logged only if conditions are met.
Add a cond	lition	
		6
		OK Cancel

- Set Type: -> Success (1)
- Set Applies to: -> File Only (2)
- Click the link Show Advanced Permissions (3)



- Click the Clear All button (4) to clear all preset permissions
- Select the following permissions (5)
 - o List folder / read data
- Press the **OK** button (6) to save the configuration
- 6) Successful edit access

Repeat steps 3 and 4 to create a new permission set and set it as follows:

🖡 Auditing E	ntry for AcmeShare		– 🗆 X
Principal:	Everyone Select a principal		
Туре:	Success 🗸	←1	
Applies to:	This folder, subfolders and files $\qquad \lor$	← _2	
Advanced p	permissions:		3 Show basic permissions
	Full control	Write attributes	-
	Traverse folder / execute file	✓ Write extended attributes	
	List folder / read data	Delete subfolders and files	
	Read attributes	✓ Delete	
	Read extended attributes	Read permissions	
	🗹 Create files / write data	Change permissions	
	Create folders / append data	🗹 Take ownership	
Only app	ly these auditing settings to objects and/or containers	within this container	4 Clear all
Add a cond	ition to limit the scope of this auditing entry. Security e	events will be logged only if conditions are met.	
Add a cond	lition		
1.00 0 0010			
			<u>U</u>
			X
			OK Cancel

- Set **Type**: -> Success (1)
- Set **Applies to:** -> This folder, subfolders, and files (2)
- Click the link Show Advanced Permissions (3)
- Click the Clear All button (4) to clear all preset permissions
- Select the following permissions (5)
 - o Create files / write data
 - o Create folders / append data
 - Write extended attributes
 - o Delete subfolders and files
 - o Delete
 - Change permissions
 - o Take ownership
- Press the **OK** button (6) to save the configuration



7) Read or Edit access failed

Repeat steps 3 and 4 to create a new permission set and set as follows:

📕 Auditing E	ntry for AcmeShare				_		×
Principal:	Everyone Select a principal						
Туре:	Fail	~ -1					
Applies to:	This folder, subfolders and files	- ←2					
Advanced p	ermissions:			3	 Show basic 	: permiss	ions
	Full control		Write attributes	-			
	Traverse folder / execute file	2	Write extended attributes				
	🗸 List folder / read data		Delete subfolders and files				
			Delete				
	Read extended attributes	_	Read permissions				
	🗸 Create files / write data	_	Change permissions				
	Create folders / append data	2] Take ownership				
Only app	ly these auditing settings to objects and/or conta	iners within this contain	er	4-		Clear a	II
Add a cond	ition to limit the scope of this auditing entry. Sec	rity events will be logge	d only if conditions are met.				
Add a cond	ition						
				6			
					ОК	Can	icel

- Set **Type**: -> Fail (1)
- Set Applies to: -> This folder, subfolders, and files (2)
- Click the link Show Advanced Permissions (3)
- Click the Clear All button (4) to clear all preset permissions
- Select the following permissions (5)
 - o List folder / read data
 - o Create files / write data
 - Create folders / append data
 - Write extended attributes
 - o Delete subfolders and files
 - o Delete
 - o Change permissions
 - o Take ownership
- Press the **OK** button (6) to save the configuration



8) After the configurations, click the **OK** button (1) to save and apply the set permissions.

	E:\Test\AcmeShare			
wner:	Rider (ACME\Rider)	Change		
Permissions	Auditing Effective Access			
uditing entries	: Principal	Access	Inherited from	Applies to
Success	Everyone	List folder / read data	None	Files only
Success	Everyone	Special	None	This folder, subfolders and files
👢 Fail	Everyone	Special	None	This folder, subfolders and files
	Remove	Edit		
644	Remove	Edit		•
Add				
Add Disable inher	itance			