SMARTER DATA. BETTER SIEM.

SGBox Windows Auditing

Guida alla Configurazione

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

Informazioni sul documento

Le informazioni trasmesse in questo documento sono destinate esclusivamente al destinatario e possono contenere materiale riservato.

Indice

1 Introduzione

Per poter raccogliere tutti i log necessari per fare auditing su Server e Workstation Windows è necessario configurare opportunamente le Group Policy abilitando l'auditing di quanto ci interessa monitorare e, nel caso sia necessario fare File Auditing, le ACL relativamente alle cartelle che si vogliono controllare.

È possibile controllare sia cartelle condivise che cartelle locali non condivise.

La prima fase consiste nel configurare le Group Policy, o le Policy locali nel caso in cui il Server o la Workstation da controllare non facciano parte di un dominio Active Directory.

È poi necessario configurare l'Object Level Auditing ACL relativamente alle cartelle e/o ai dischi che si desidera controllare tenendo presente che, per ottenere gli eventi di audit, entrambe le configurazioni devono essere attive sulla cartella o sul disco da controllare. Se le ACL non vengono applicate, o se le Group Policy non vengono configurate non verranno generati gli eventi necessari all'auditing.

Nel caso in cui si vogliano controllare gli eventi relativi ad un Dominio di Active Directory sarà necessario configurare l'Object Level Auditing anche a livello di Dominio.

2 Configurazione Advanced Audit Policy

Per poter avere un maggior dettaglio ed un maggior controllo sui livelli di auditing attivati è preferibile configurare ed utilizzare le Advanced Auditing Policies.

2.1 Attività preliminari

Prima di passare alla configurazione delle Group Policy è necessario configurare due elementi indispensabili per il corretto funzionamento della soluzione:

- Le Security Options
- La dimensione del Security Event Log e relativa metodologia di ritenzione

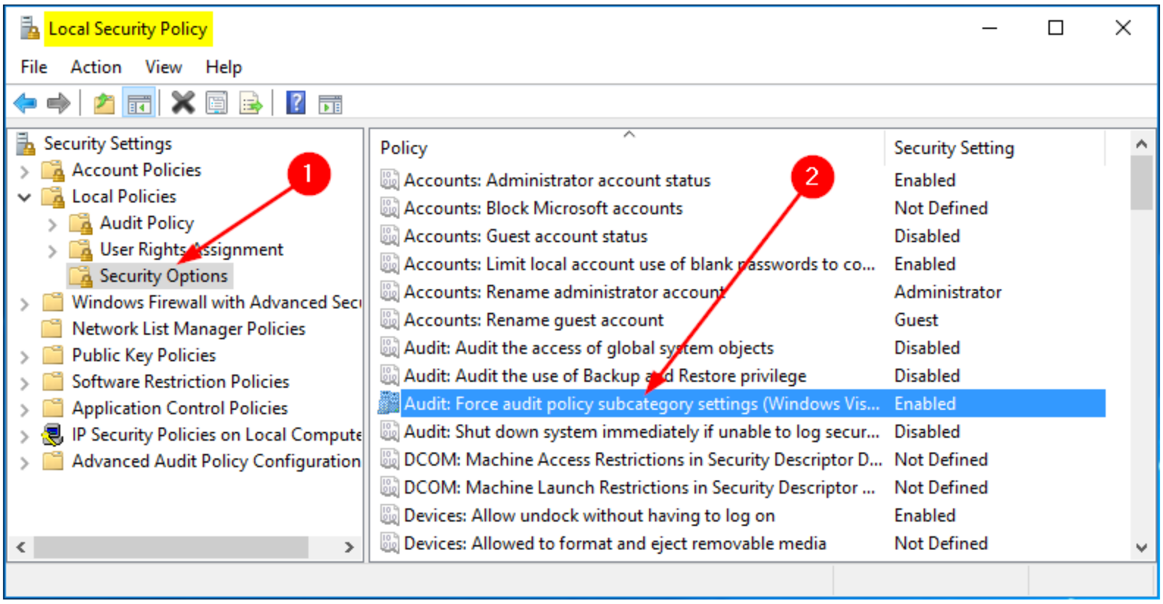
Se per caso dovessero essere definite entrambe le Audit Policy (base e avanzate) otterremmo valori di audit errati, per ovviare a questo problema è necessario impostare opportunamente la Security Policy.

2.2 Configurazione Security Options

Verificare che localmente, su ogni Server/Workstation che desideriamo monitorare, la Security Policy **Audit: Force audit policy subcategory settings to override audit policy category settings** (2) sia configurata su **Enabled** (impostazione predefinita di sistema) in modo che vengano ignorate le Basic Audit Policy in favore delle Advanced Audit Policy.

Sulle macchine da verificare, aprire il pannello delle Local Security Policy che si trova in

Start -> Windows Administrative Tools -> Local Security Policy


Local Security Policy
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Audit Policy
User Rights Assignment
Security Options
Windows Firewall with Advanced Secu
Network List Manager Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Local Compute
Advanced Audit Policy Configuration
1
2

Policy	Security Setting
Accounts: Administrator account status	Enabled
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Disabled
Accounts: Limit local account use of blank passwords to co...	Enabled
Accounts: Rename administrator account	Administrator
Accounts: Rename guest account	Guest
Audit: Audit the access of global system objects	Disabled
Audit: Audit the use of Backup and Restore privilege	Disabled
Audit: Force audit policy subcategory settings (Windows Vis...	Enabled
Audit: Shut down system immediately if unable to log secur...	Disabled
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Enabled
Devices: Allowed to format and eject removable media	Not Defined

3 Configurazione Event Log

La configurazione delle caratteristiche del Security Event Log può essere eseguita sia localmente, per ogni macchina, che centralmente tramite Group Policy.

È molto importante configurare opportunamente anche la dimensione e la modalità operativa del Security Log affinché non vengano persi eventi in caso di temporanee mancanze di connessione con Il Server o il Collettore SGBox.

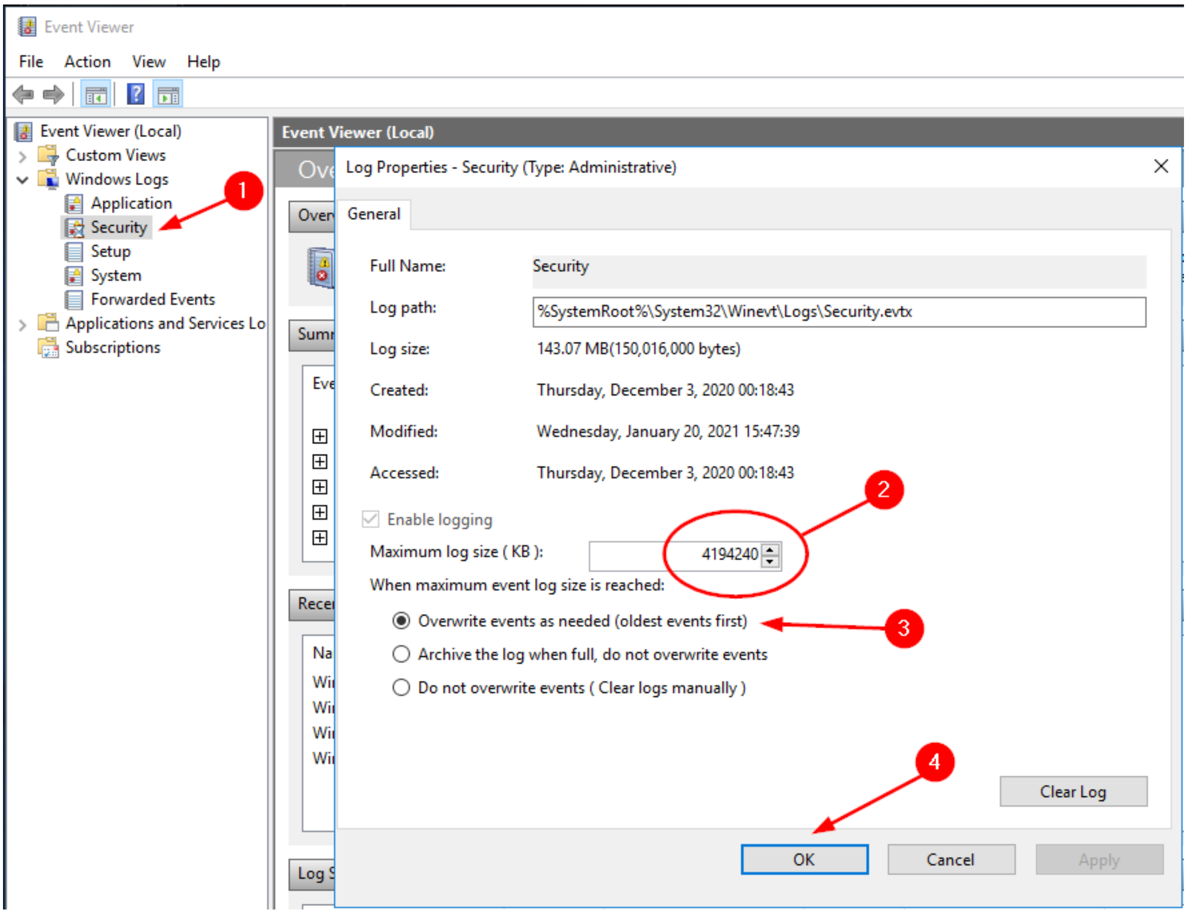
3.1 Configurazione locale

Aprire il pannello Event Viewer che si trova in *Start -> Windows Administrative Tools -> Local Security Policy*, espandere la voce *Windows Logs*, fare click destro su **Security** (1) e scegliere **Properties** dal menu pop-up.

Posizionarsi su **Security** (1) e impostare i valori come segue:

- *Maximum log size (KB)*: **4194240** (2)
- selezionare **Overwrite events as needed** (3)

e premere **OK** (4) per salvare la configurazione.



Log Properties - Security (Type: Administrative)

General

Full Name: Security

Log path: %SystemRoot%\System32\Winevt\Logs\Security.evtx

Log size: 143.07 MB(150,016,000 bytes)

Created: Thursday, December 3, 2020 00:18:43

Modified: Wednesday, January 20, 2021 15:47:39

Accessed: Thursday, December 3, 2020 00:18:43

☑ Enable logging

Maximum log size (KB): 4194240

When maximum event log size is reached:

● Overwrite events as needed (oldest events first)

○ Archive the log when full, do not overwrite events

○ Do not overwrite events (Clear logs manually)

Clear Log

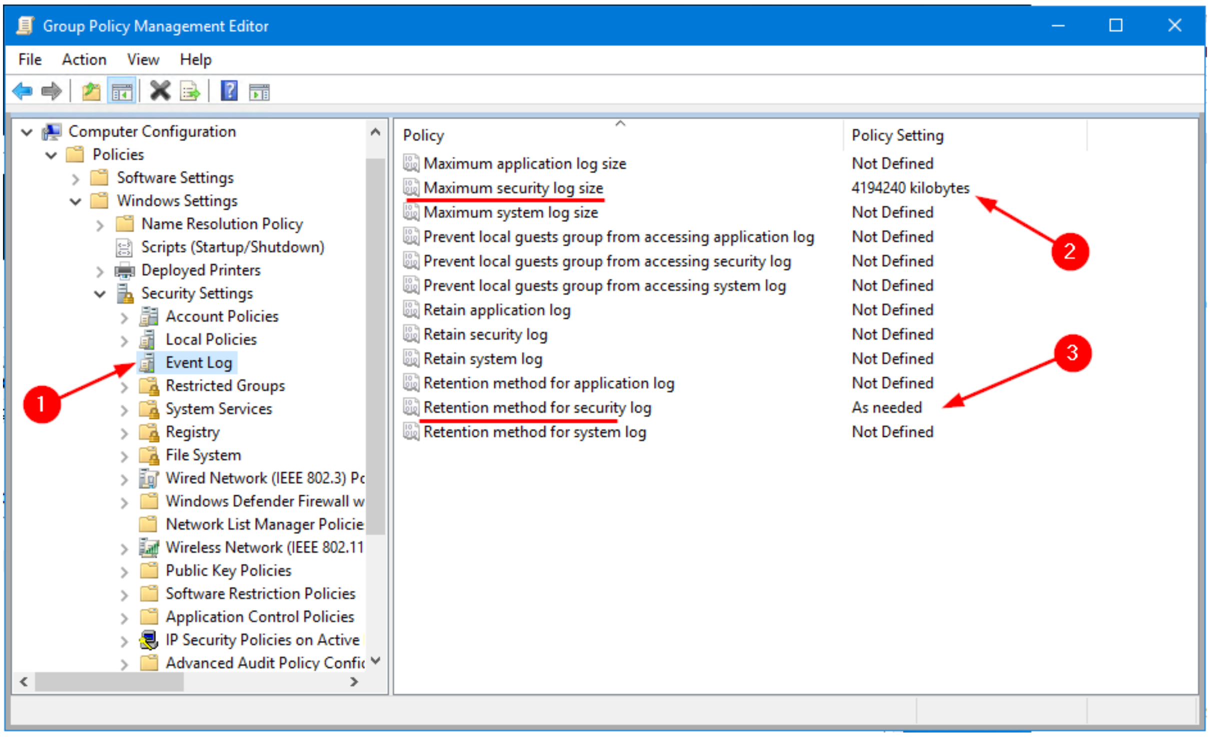
OK Cancel Apply

3.2 Configurazione tramite GPO

Sul Domain Controller aprire lo snap-in Group Policy Management che si trova in *Start* → *Windows Administrative Tools* o in *Start* -> *Administrative Tools*, a seconda della versione di Windows.

Posizionarsi su Event Log (1) e impostare i valori delle policy come segue:

- *Maximum security log size*: 4194240 kilobytes (2)
- *Retention method for security log*: As Needed (3)



- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802.3) Pc
        - Windows Defender Firewall w
        - Network List Manager Policie
        - Wireless Network (IEEE 802.11
        - Public Key Policies
        - Software Restriction Policies
        - Application Control Policies
        - IP Security Policies on Active
        - Advanced Audit Policy Confic

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	4194240 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

Chiudere lo Snap-in ed accertarsi che la policy venga correttamente distribuita.

4 Configurazione GPO Advanced Audit Policy

È possibile sia racchiudere tutte le impostazioni in un'unica GPO che creare GPO specializzate per ognuna delle quattro categorie illustrate di seguito.

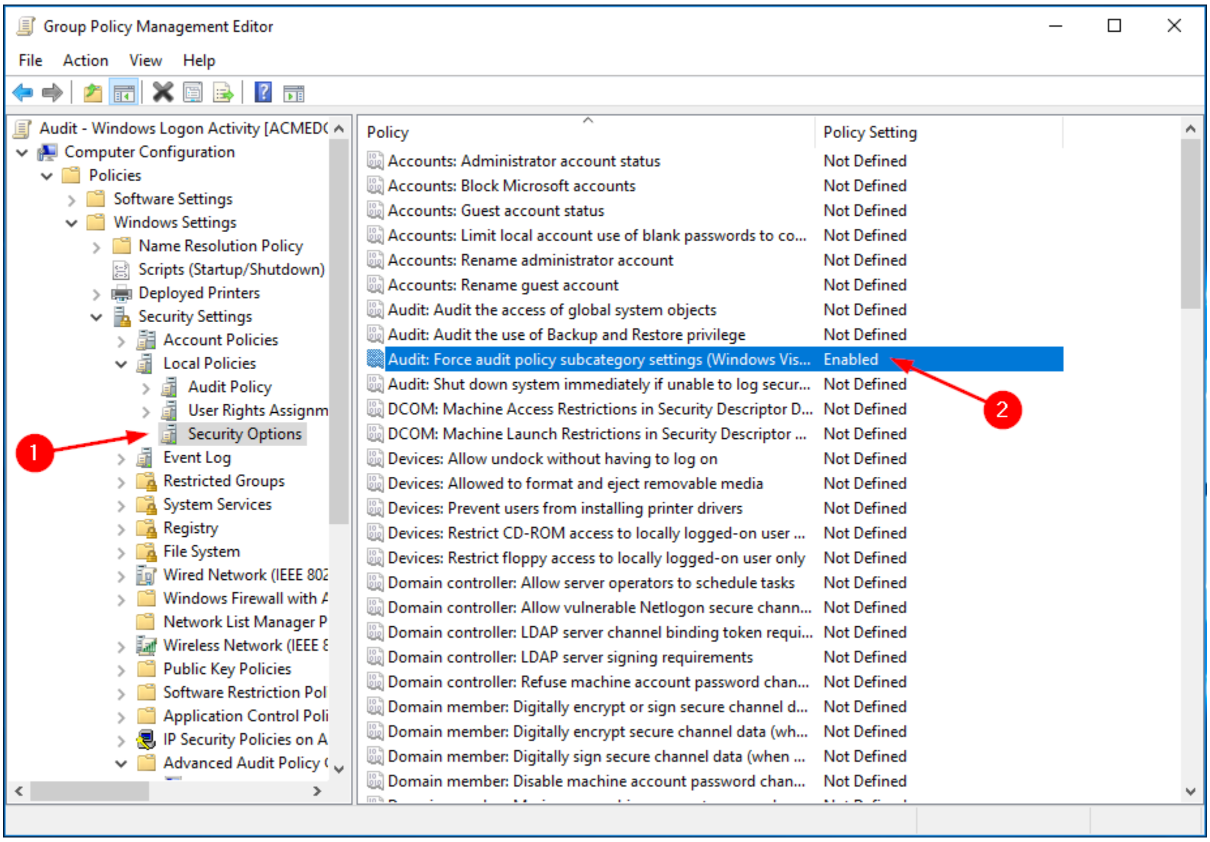
4.1 Audit Logon Activities

Sul Domain Controller aprire lo snap-in Group Policy Management che si trova in *Start* → *Windows Administrative Tools* o in *Start* -> *Administrative Tools*, a seconda della versione di Windows.

Creare una GPO specifica per la categoria, oppure utilizzarne una generalizzata, e configurare le varie opzioni come illustrato di seguito.

4.1.1 Security Options

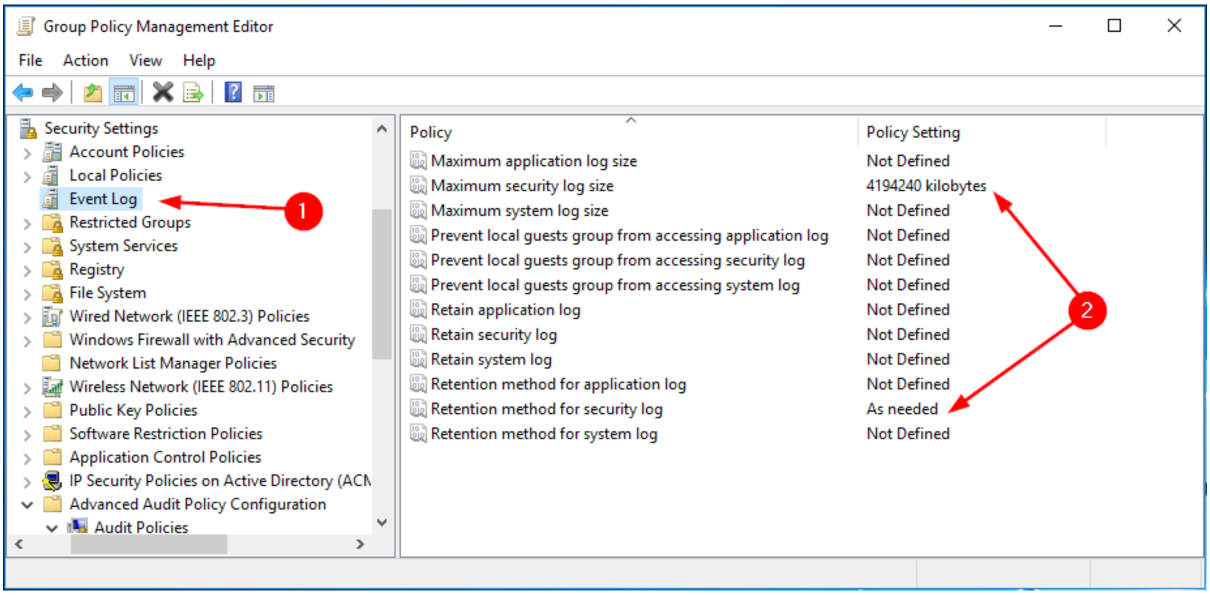
Da *Computer Configuration* -> *Policies* -> *Windows Settings* -> *Security Settings* -> *Local Policy* posizionarsi su **Security Options** (1) e configurare i parametri (2) come indicato in figura.



Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Enabled
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined

4.1.2 Event Log

Da Computer Configuration -> Policies -> Windows Settings -> Security Settings posizionarsi su **Event Log** (1) e configurare i parametri (2) come indicato in figura.

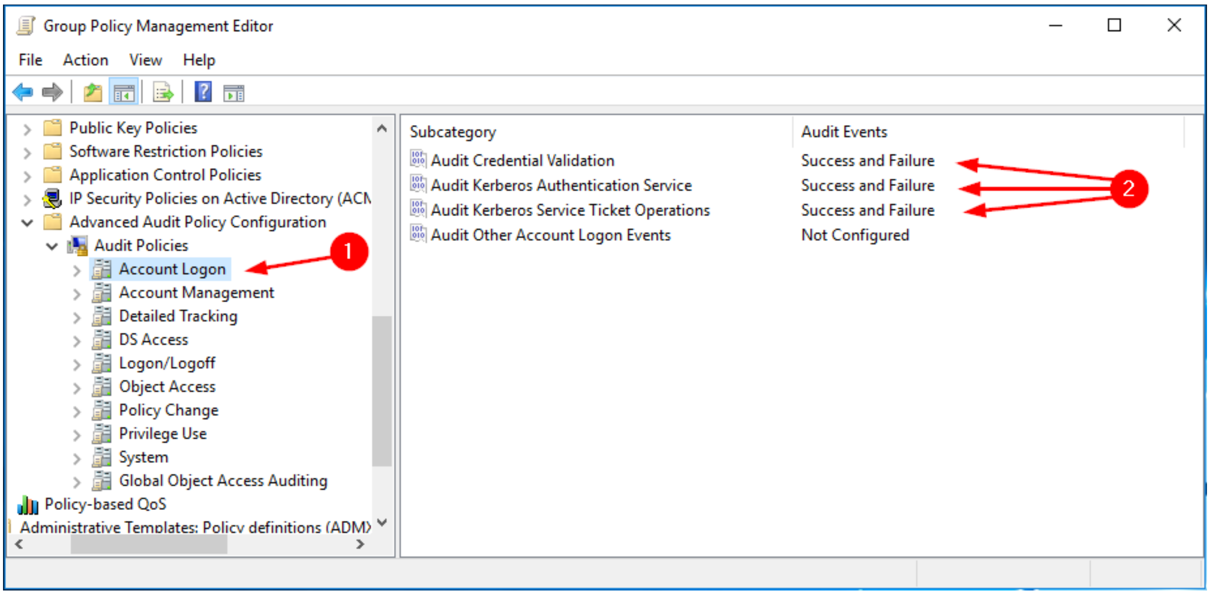


- Security Settings
  - Account Policies
  - Local Policies
  - Event Log
  - Restricted Groups
  - System Services
  - Registry
  - File System
  - Wired Network (IEEE 802.3) Policies
  - Windows Firewall with Advanced Security
  - Network List Manager Policies
  - Wireless Network (IEEE 802.11) Policies
  - Public Key Policies
  - Software Restriction Policies
  - Application Control Policies
  - IP Security Policies on Active Directory (ACN
  - Advanced Audit Policy Configuration
    - Audit Policies

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	4194240 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

4.1.3 Account Logon

Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **Account Logon** (1) e configurare i parametri (2) come indicato in figura.

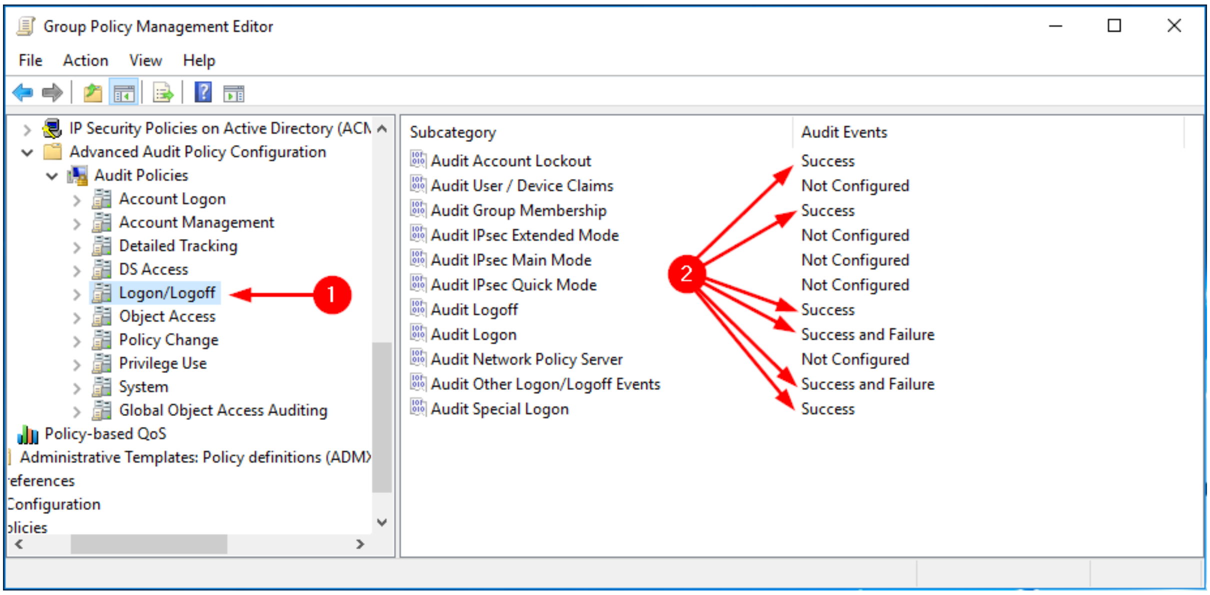


- Public Key Policies
- Software Restriction Policies
- Application Control Policies
- IP Security Policies on Active Directory (ACN
- Advanced Audit Policy Configuration
  - Audit Policies
    - Account Logon
    - Account Management
    - Detailed Tracking
    - DS Access
    - Logon/Logoff
    - Object Access
    - Policy Change
    - Privilege Use
    - System
    - Global Object Access Auditing
- Policy-based QoS
- Administrative Templates: Policy definitions (ADM)

Subcategory	Audit Events
Audit Credential Validation	Success and Failure
Audit Kerberos Authentication Service	Success and Failure
Audit Kerberos Service Ticket Operations	Success and Failure
Audit Other Account Logon Events	Not Configured

4.1.4 Logon/Logoff

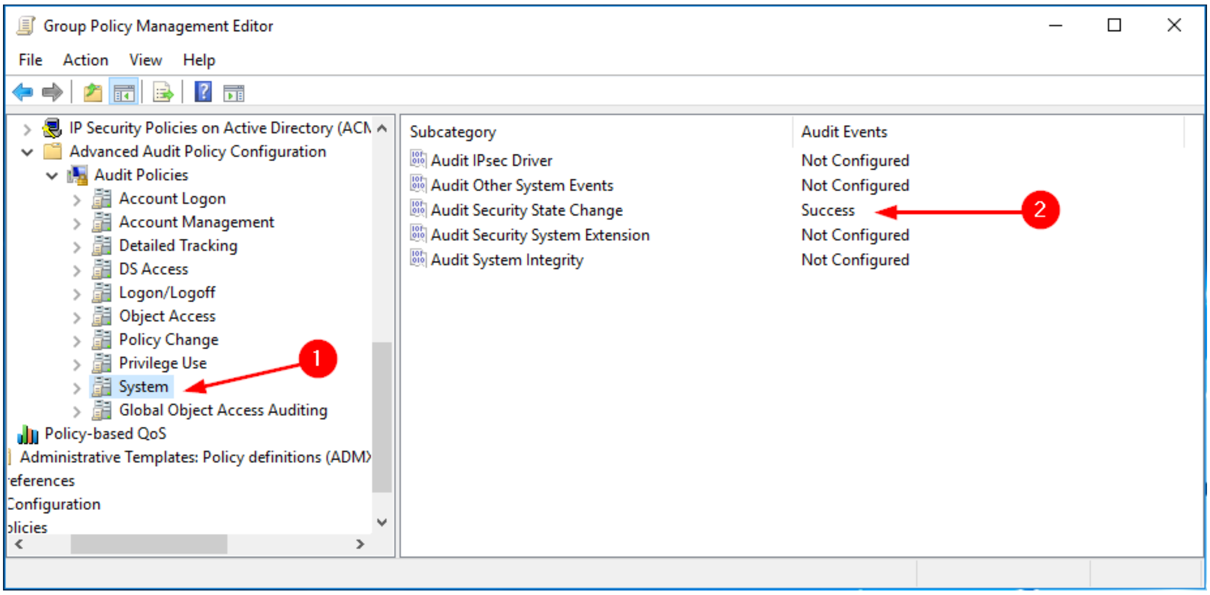
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **Logon/Logoff** (1) e configurare i parametri (2) come indicato in figura.



Subcategory	Audit Events
Audit Account Lockout	Success
Audit User / Device Claims	Not Configured
Audit Group Membership	Success
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Success and Failure
Audit Special Logon	Success

4.1.5 System

Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **System** (1) e configurare i parametri (2) come indicato in figura.



Subcategory	Audit Events
Audit IPsec Driver	Not Configured
Audit Other System Events	Not Configured
Audit Security State Change	Success
Audit Security System Extension	Not Configured
Audit System Integrity	Not Configured

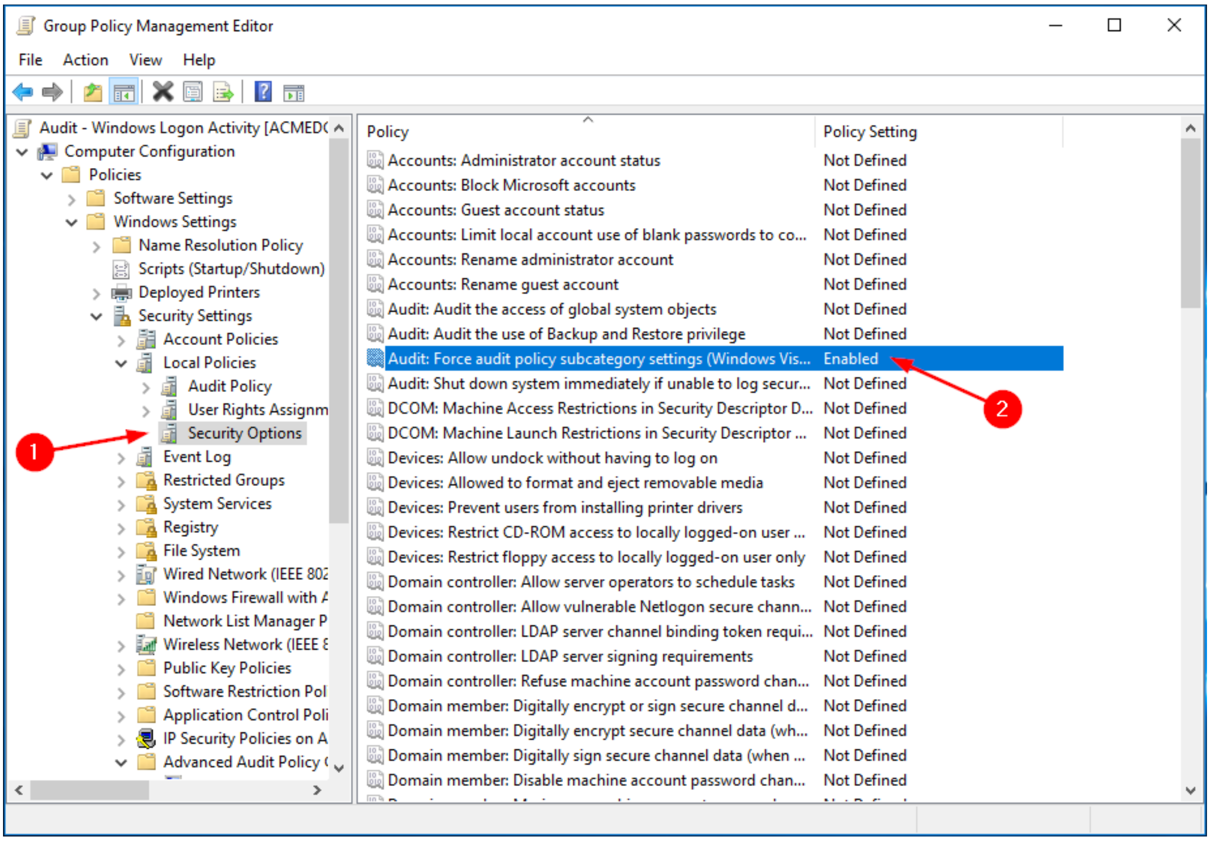
4.2 Audit Domain Controllers

Sul Domain Controller aprire lo snap-in Group Policy Management che si trova in *Start* → *Windows Administrative Tools* o in *Start* -> *Administrative Tools*, a seconda della versione di Windows.

Creare una GPO specifica per la categoria, oppure utilizzarne una generalizzata, e configurare le varie opzioni come illustrato di seguito.

4.2.1 Security Options

Da *Computer Configuration* -> *Policies* -> *Windows Settings* -> *Security Settings* -> *Local Policy*, posizionarsi su **Security Options** (1) e configurare i parametri (2) come indicato in figura.

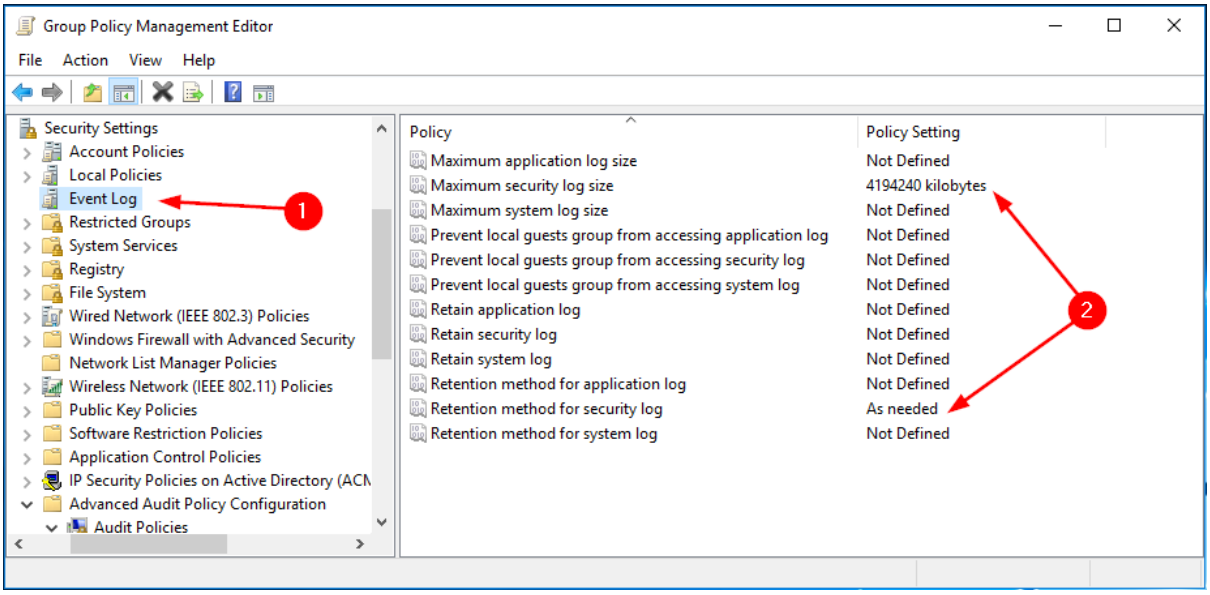


```
Audit - Windows Logon Activity [ACMEDC
  Computer Configuration
    Policies
      Software Settings
      Windows Settings
        Name Resolution Policy
        Scripts (Startup/Shutdown)
        Deployed Printers
        Security Settings
          Account Policies
          Local Policies
            Audit Policy
            User Rights Assignm
            Security Options
          Event Log
          Restricted Groups
          System Services
          Registry
          File System
          Wired Network (IEEE 802
          Windows Firewall with A
          Network List Manager P
          Wireless Network (IEEE 8
          Public Key Policies
          Software Restriction Pol
          Application Control Poli
          IP Security Policies on A
          Advanced Audit Policy C
```

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Enabled
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined

4.2.2 Event Log

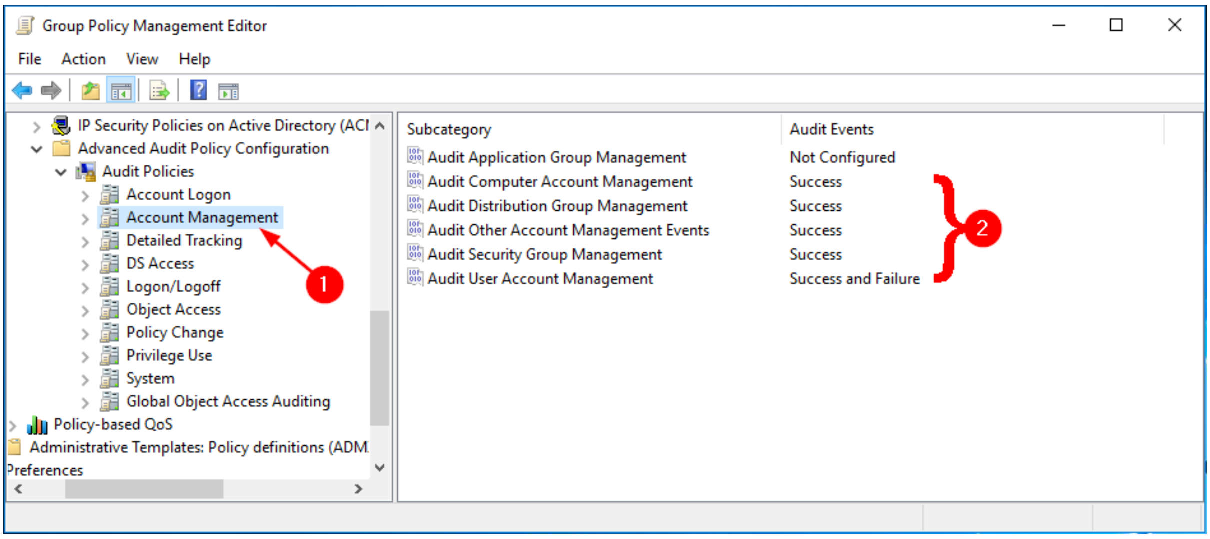
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings,* posizionarsi su **Event Log** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (ACN
Advanced Audit Policy Configuration
Audit Policies
1
2

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	4194240 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

4.2.3 Account Management

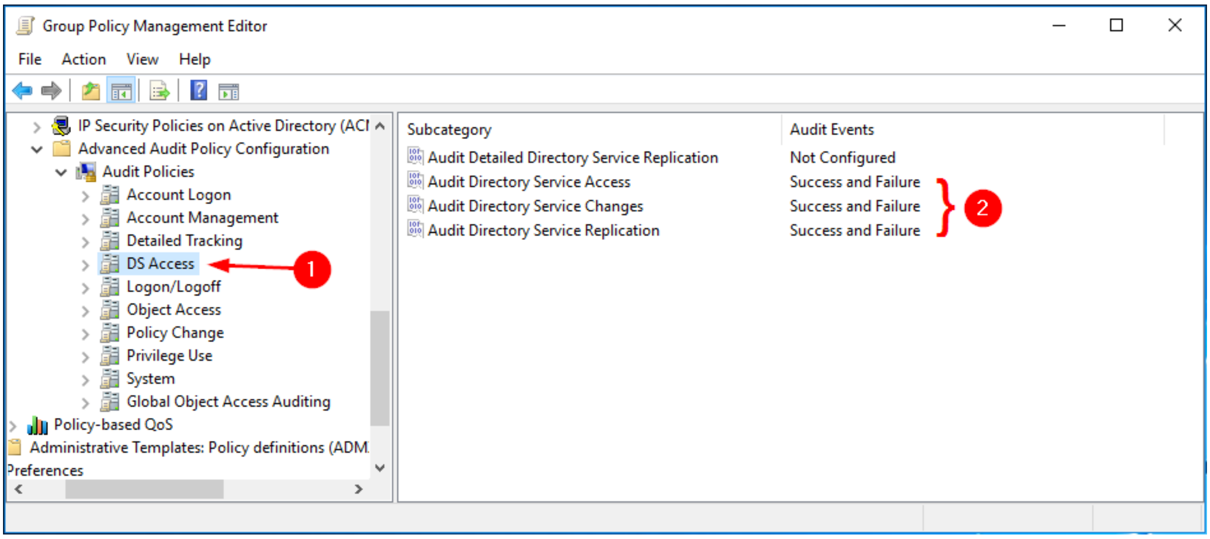
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy,* posizionarsi su **Account Management** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
IP Security Policies on Active Directory (ACI
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
1
2

Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Success
Audit Distribution Group Management	Success
Audit Other Account Management Events	Success
Audit Security Group Management	Success
Audit User Account Management	Success and Failure

4.2.4 DS Access

Da *Computer Configuration* -> *Policies* -> *Windows Settings* -> *Security Settings* -> *Advanced Audit Policy Configuration* -> *Audit Policy*, posizionarsi su DS Access (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
IP Security Policies on Active Directory (ACI
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (ADM
Preferences
1
2

Subcategory	Audit Events
Audit Detailed Directory Service Replication	Not Configured
Audit Directory Service Access	Success and Failure
Audit Directory Service Changes	Success and Failure
Audit Directory Service Replication	Success and Failure

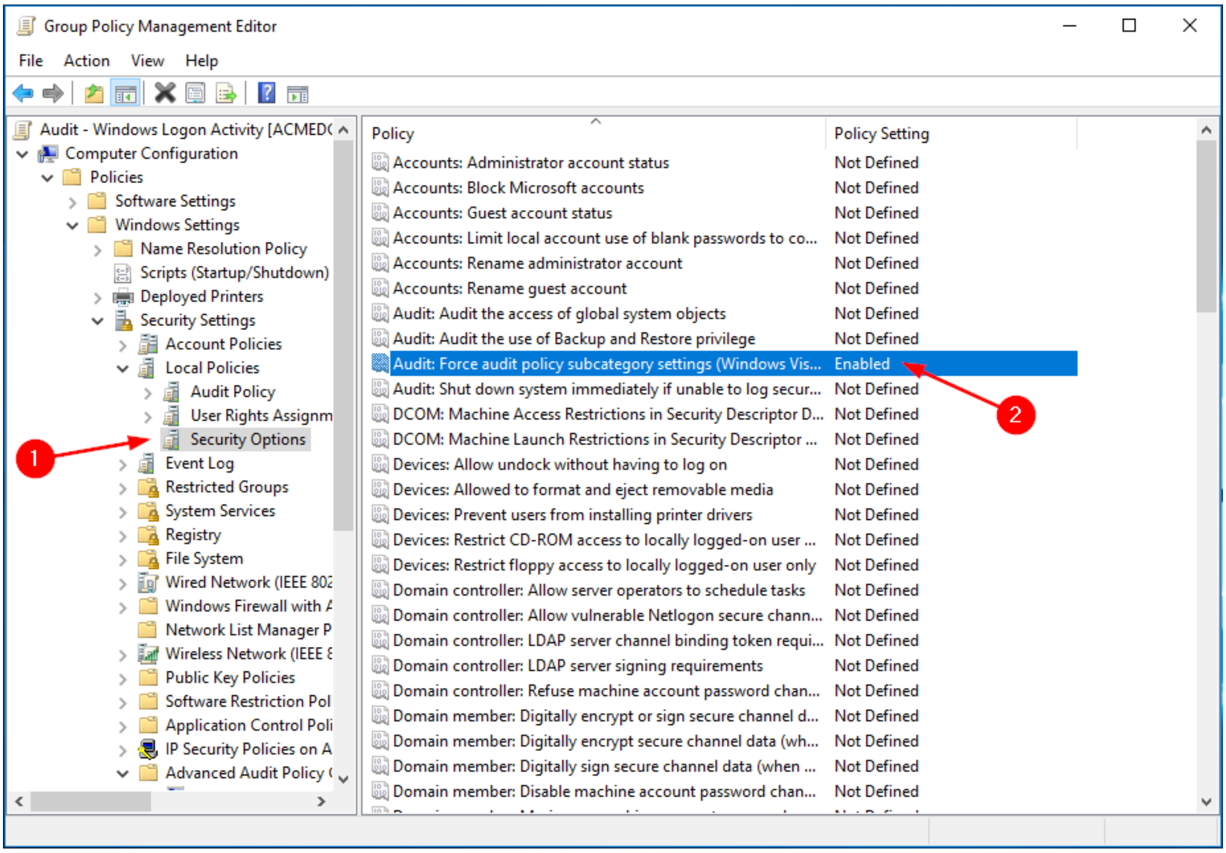
4.3 Audit File Servers

Sul Domain Controller aprire lo snap-in Group Policy Management che si trova in *Start* → *Windows Administrative Tools* o in *Start* -> *Administrative Tools*, a seconda della versione di Windows.

Creare una GPO specifica per la categoria, oppure utilizzarne una generalizzata, e configurare le varie opzioni come illustrato di seguito.

4.3.1 Security Options

Da *Computer Configuration* -> *Policies* -> *Windows Settings* -> *Security Settings* -> *Local Policy*, posizionarsi su **Security Options** (1) e configurare i parametri (2) come indicato in figura.

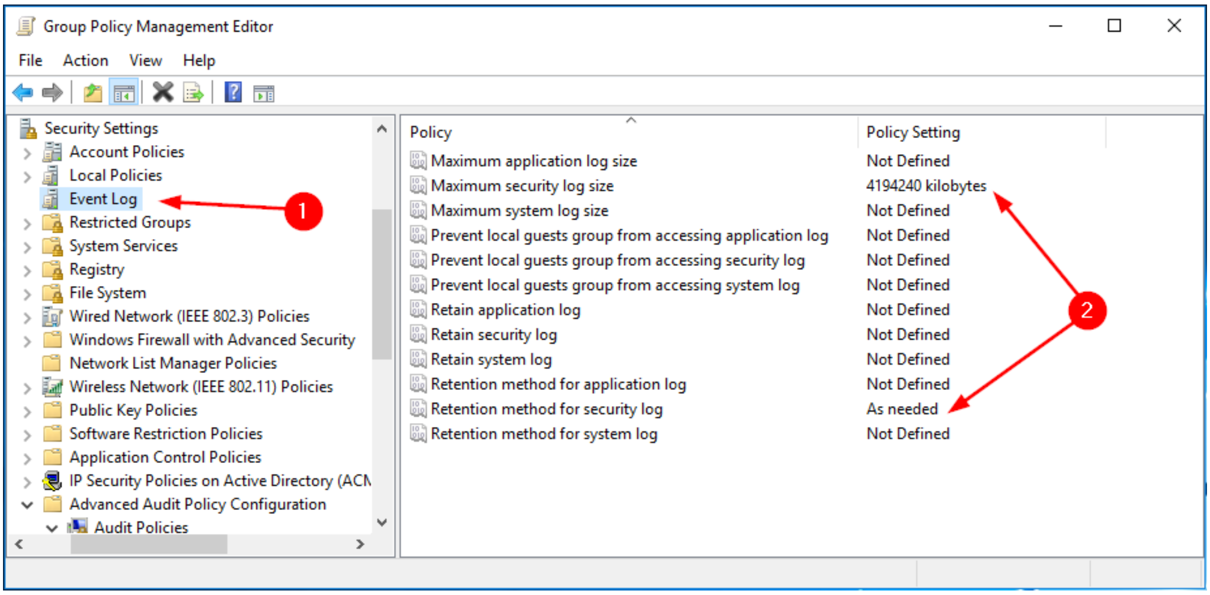


```
Audit - Windows Logon Activity [ACMED(
  Computer Configuration
    Policies
      Software Settings
      Windows Settings
        Name Resolution Policy
        Scripts (Startup/Shutdown)
        Deployed Printers
        Security Settings
          Account Policies
          Local Policies
            Audit Policy
            User Rights Assignm
            Security Options
          Event Log
          Restricted Groups
          System Services
          Registry
          File System
          Wired Network (IEEE 802
          Windows Firewall with A
          Network List Manager P
          Wireless Network (IEEE 8
          Public Key Policies
          Software Restriction Pol
          Application Control Poli
          IP Security Policies on A
          Advanced Audit Policy (
```

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Enabled
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined

4.3.2 Event Log

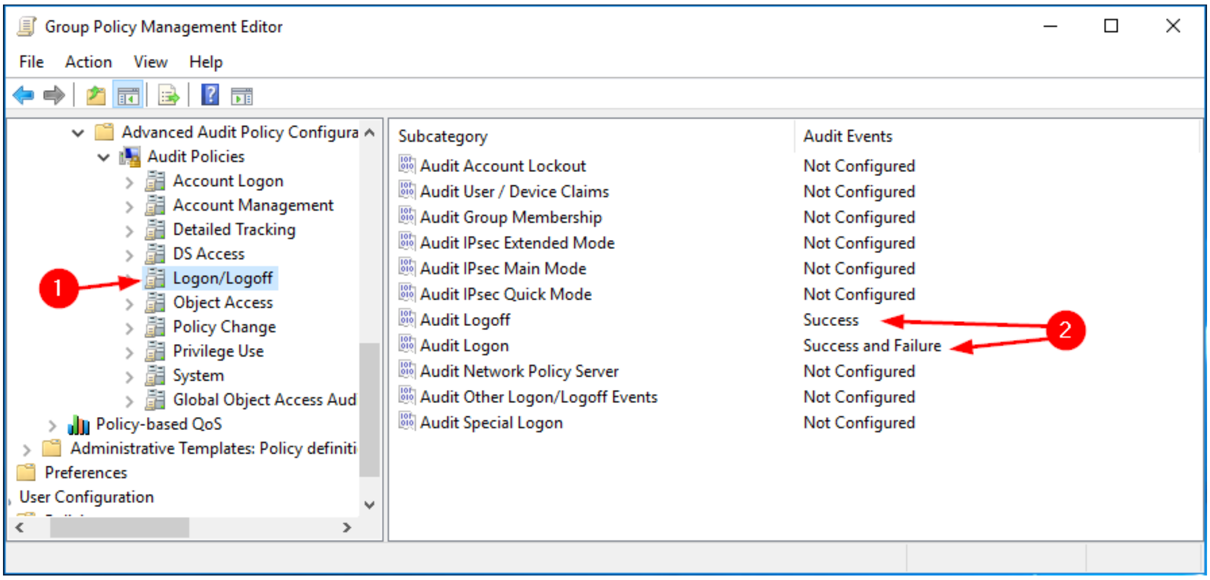
Da Computer Configuration -> Policies -> Windows Settings -> Security Settings posizionarsi su **Event Log** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (ACN
Advanced Audit Policy Configuration
Audit Policies
1
2

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	4194240 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

4.3.3 Logon/Logoff

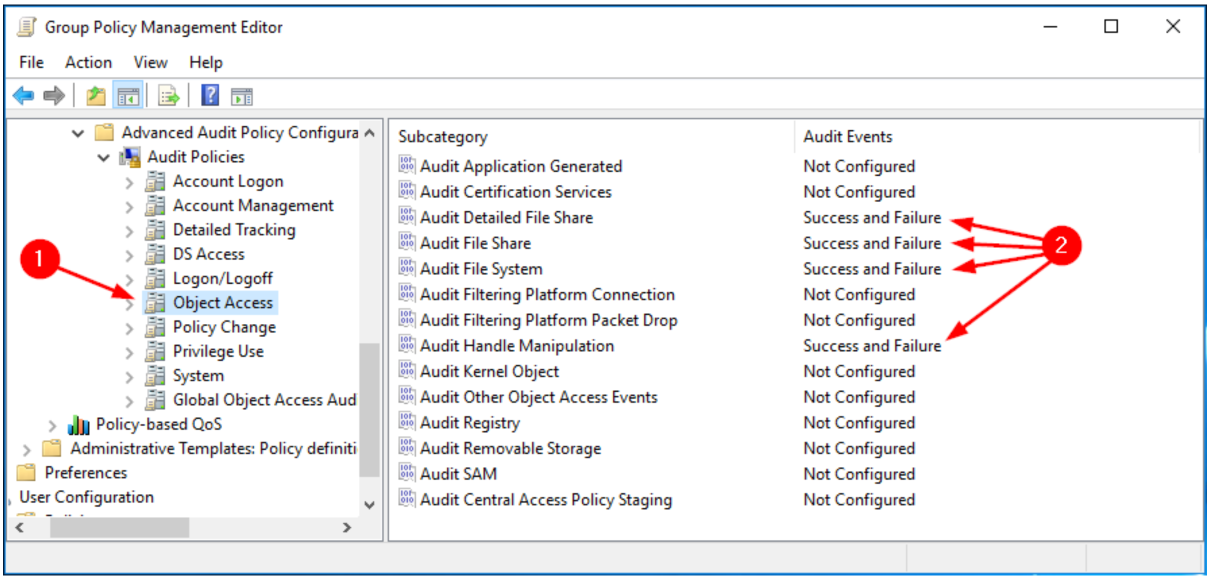
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **Logon/Logoff** (1) e configurare i parametri (2) come indicato in figura.



Subcategory	Audit Events
Audit Account Lockout	Not Configured
Audit User / Device Claims	Not Configured
Audit Group Membership	Not Configured
Audit IPsec Extended Mode	Not Configured
Audit IPsec Main Mode	Not Configured
Audit IPsec Quick Mode	Not Configured
Audit Logoff	Success
Audit Logon	Success and Failure
Audit Network Policy Server	Not Configured
Audit Other Logon/Logoff Events	Not Configured
Audit Special Logon	Not Configured

4.3.4 Object Access

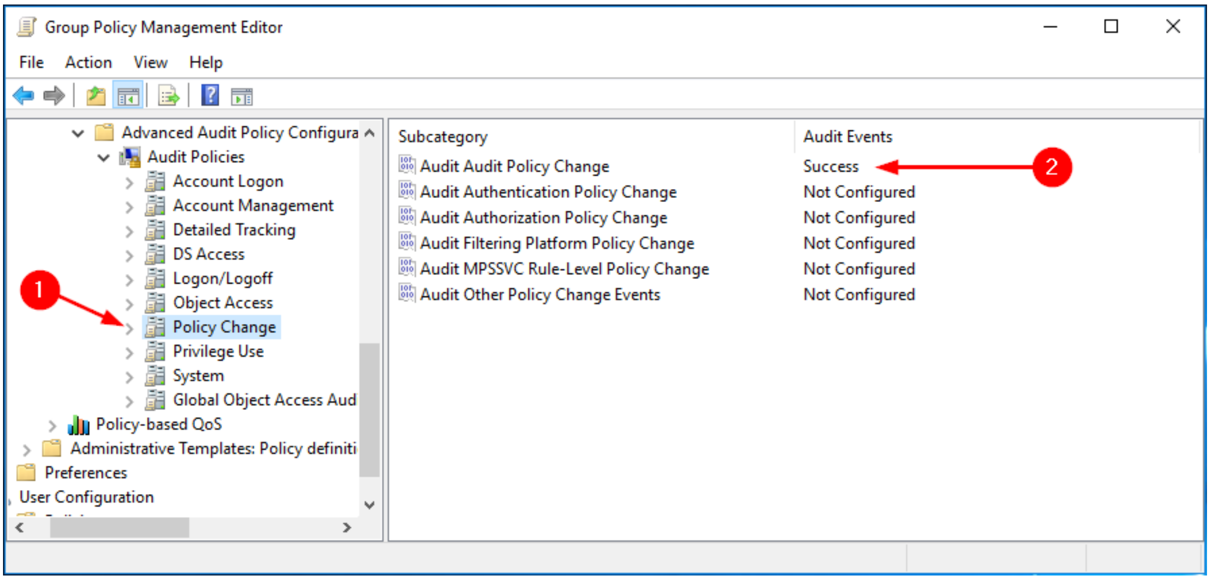
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy* posizionarsi su **Objec Access** (1) e configurare i parametri (2) come indicato in figura.



Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Not Configured
Audit Detailed File Share	Success and Failure
Audit File Share	Success and Failure
Audit File System	Success and Failure
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Success and Failure
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Not Configured
Audit Registry	Not Configured
Audit Removable Storage	Not Configured
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

4.3.5 Policy Change

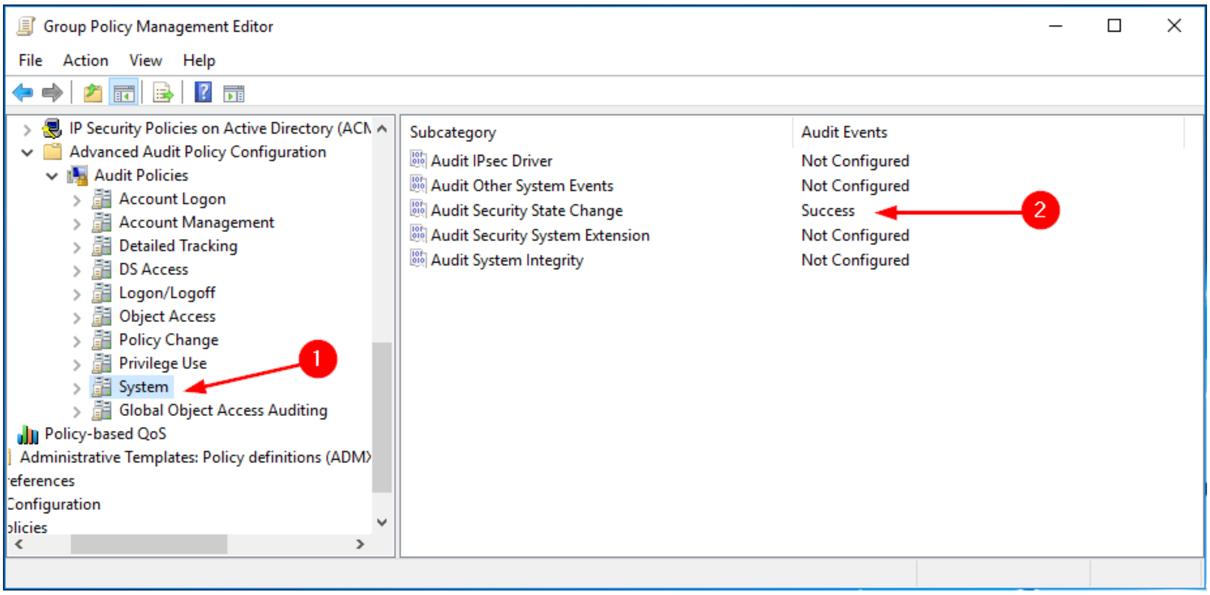
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **Policy Change** (1) e configurare i parametri (2) come indicato in figura.



Subcategory	Audit Events
Audit Audit Policy Change	Success
Audit Authentication Policy Change	Not Configured
Audit Authorization Policy Change	Not Configured
Audit Filtering Platform Policy Change	Not Configured
Audit MPSSVC Rule-Level Policy Change	Not Configured
Audit Other Policy Change Events	Not Configured

4.3.6 System

Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy* posizionarsi su **System** (1) e configurare i parametri (2) come indicato in figura.



Subcategory	Audit Events
Audit IPsec Driver	Not Configured
Audit Other System Events	Not Configured
Audit Security State Change	Success
Audit Security System Extension	Not Configured
Audit System Integrity	Not Configured

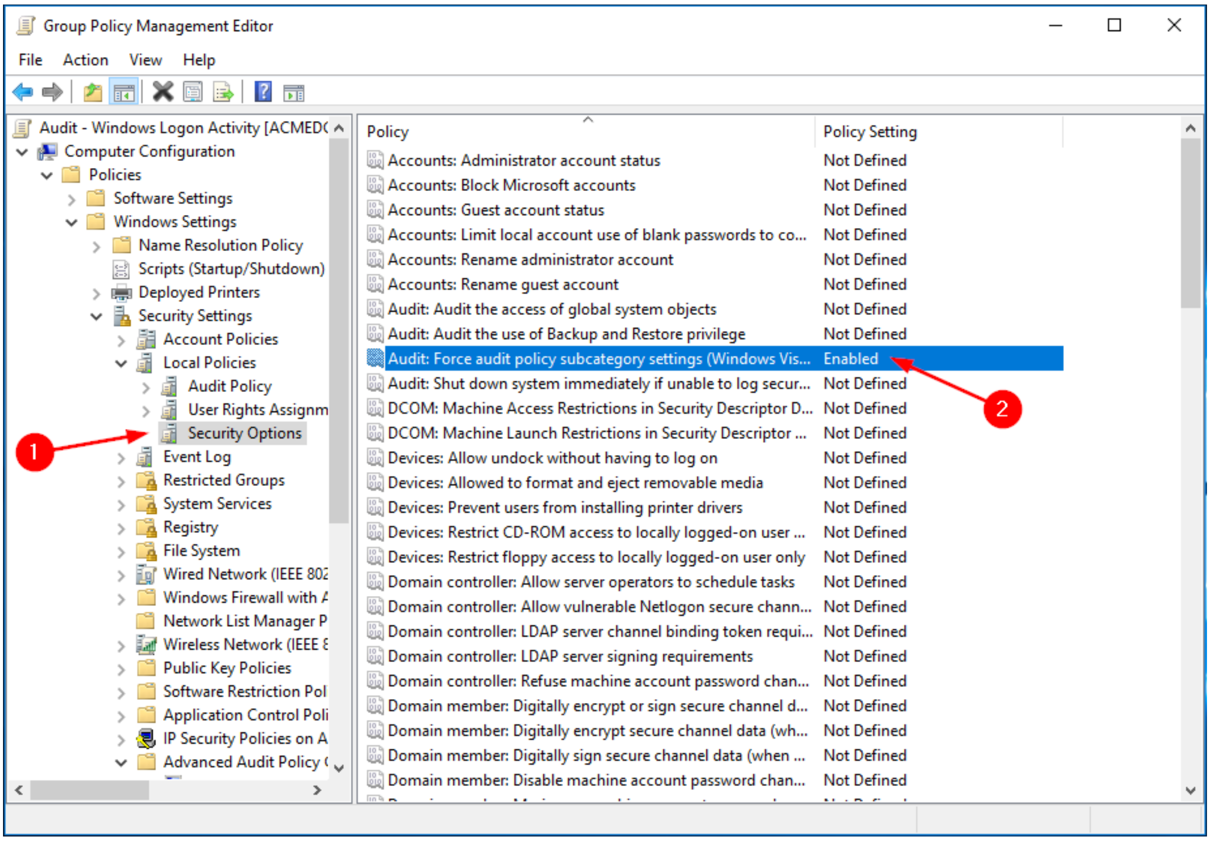
4.4 Audit Windows Servers e Workstation

Sul Domain Controller aprire lo snap-in Group Policy Management che si trova in *Start* → *Windows Administrative Tools* o in *Start* -> *Administrative Tools*, a seconda della versione di Windows.

Creare una GPO specifica per la categoria, oppure utilizzarne una generalizzata, e configurare le varie opzioni come illustrato di seguito.

4.4.1 Security Options

Da *Computer Configuration* -> *Policies* -> *Windows Settings* -> *Security Settings* -> *Local Policy*, posizionarsi su **Security Options** (1) e configurare i parametri (2) come indicato in figura.

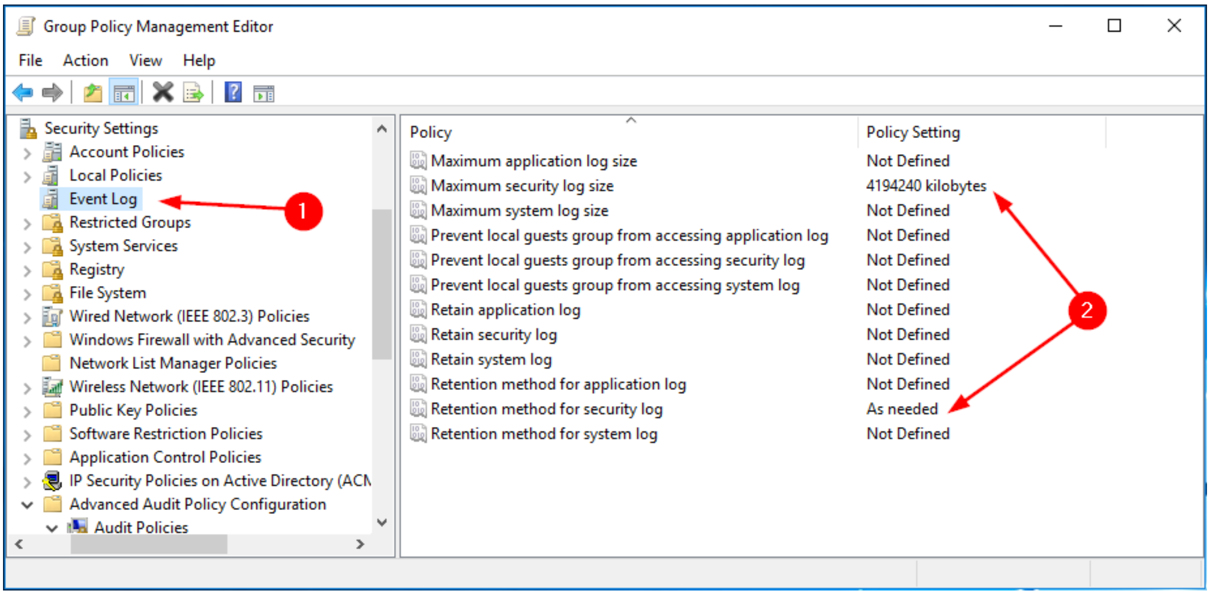


Audit - Windows Logon Activity [ACMED(
- Computer Configuration
  - Policies
    - Software Settings
    - Windows Settings
      - Name Resolution Policy
      - Scripts (Startup/Shutdown)
      - Deployed Printers
      - Security Settings
        - Account Policies
        - Local Policies
          - Audit Policy
          - User Rights Assignm
          - Security Options
        - Event Log
        - Restricted Groups
        - System Services
        - Registry
        - File System
        - Wired Network (IEEE 802
        - Windows Firewall with A
        - Network List Manager P
        - Wireless Network (IEEE 8
        - Public Key Policies
        - Software Restriction Pol
        - Application Control Poli
        - IP Security Policies on A
        - Advanced Audit Policy (

Policy	Policy Setting
Accounts: Administrator account status	Not Defined
Accounts: Block Microsoft accounts	Not Defined
Accounts: Guest account status	Not Defined
Accounts: Limit local account use of blank passwords to co...	Not Defined
Accounts: Rename administrator account	Not Defined
Accounts: Rename guest account	Not Defined
Audit: Audit the access of global system objects	Not Defined
Audit: Audit the use of Backup and Restore privilege	Not Defined
Audit: Force audit policy subcategory settings (Windows Vis...	Enabled
Audit: Shut down system immediately if unable to log secur...	Not Defined
DCOM: Machine Access Restrictions in Security Descriptor D...	Not Defined
DCOM: Machine Launch Restrictions in Security Descriptor ...	Not Defined
Devices: Allow undock without having to log on	Not Defined
Devices: Allowed to format and eject removable media	Not Defined
Devices: Prevent users from installing printer drivers	Not Defined
Devices: Restrict CD-ROM access to locally logged-on user ...	Not Defined
Devices: Restrict floppy access to locally logged-on user only	Not Defined
Domain controller: Allow server operators to schedule tasks	Not Defined
Domain controller: Allow vulnerable Netlogon secure chann...	Not Defined
Domain controller: LDAP server channel binding token requi...	Not Defined
Domain controller: LDAP server signing requirements	Not Defined
Domain controller: Refuse machine account password chan...	Not Defined
Domain member: Digitally encrypt or sign secure channel d...	Not Defined
Domain member: Digitally encrypt secure channel data (wh...	Not Defined
Domain member: Digitally sign secure channel data (when ...	Not Defined
Domain member: Disable machine account password chan...	Not Defined

4.4.2 Event Log

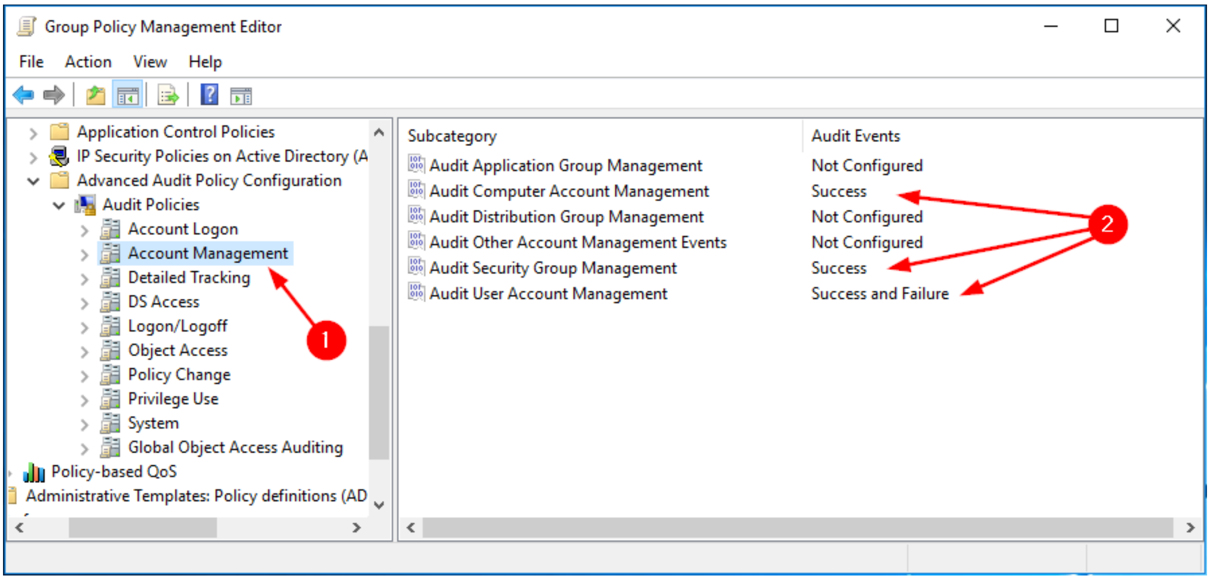
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings,* posizionarsi su **Event Log** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
Security Settings
Account Policies
Local Policies
Event Log
Restricted Groups
System Services
Registry
File System
Wired Network (IEEE 802.3) Policies
Windows Firewall with Advanced Security
Network List Manager Policies
Wireless Network (IEEE 802.11) Policies
Public Key Policies
Software Restriction Policies
Application Control Policies
IP Security Policies on Active Directory (ACN
Advanced Audit Policy Configuration
Audit Policies
1
2

Policy	Policy Setting
Maximum application log size	Not Defined
Maximum security log size	4194240 kilobytes
Maximum system log size	Not Defined
Prevent local guests group from accessing application log	Not Defined
Prevent local guests group from accessing security log	Not Defined
Prevent local guests group from accessing system log	Not Defined
Retain application log	Not Defined
Retain security log	Not Defined
Retain system log	Not Defined
Retention method for application log	Not Defined
Retention method for security log	As needed
Retention method for system log	Not Defined

4.4.3 Account Management

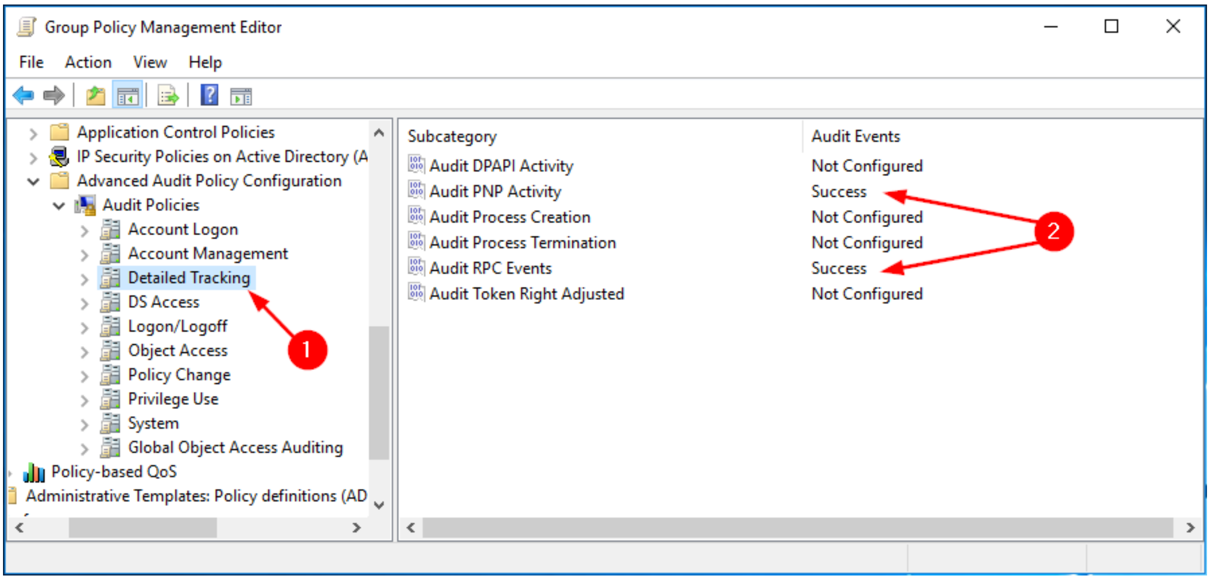
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy,* posizionarsi su **Account Management** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
Application Control Policies
IP Security Policies on Active Directory (A
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (AD
1
2

Subcategory	Audit Events
Audit Application Group Management	Not Configured
Audit Computer Account Management	Success
Audit Distribution Group Management	Not Configured
Audit Other Account Management Events	Not Configured
Audit Security Group Management	Success
Audit User Account Management	Success and Failure

4.4.4 Detailed Tracking

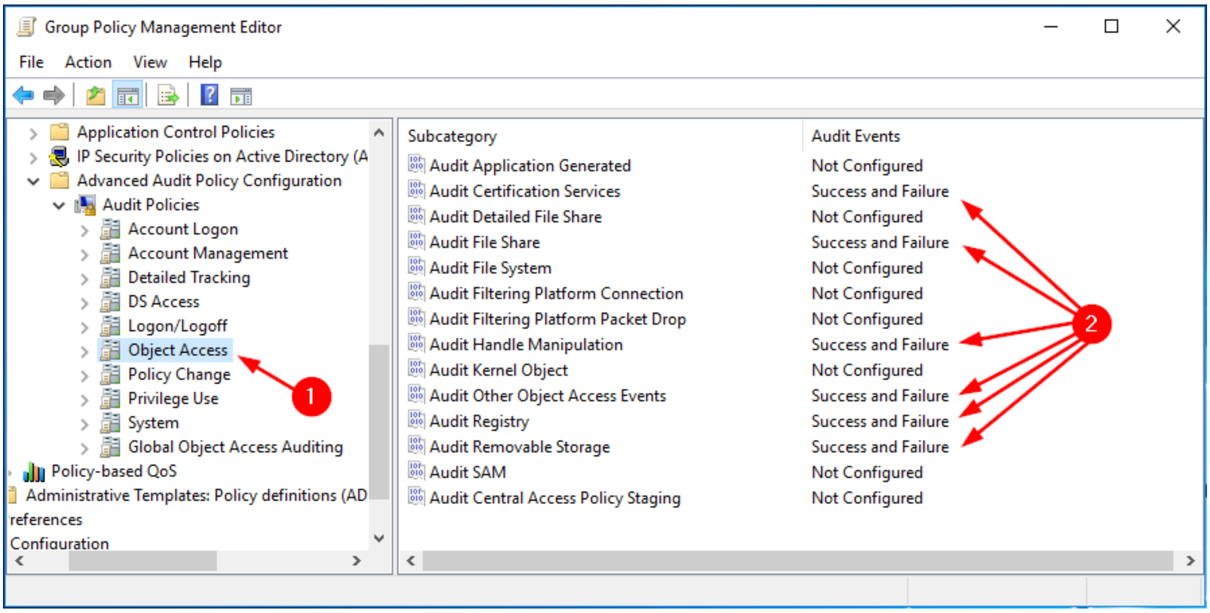
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **Detailed Tracking** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
Application Control Policies
IP Security Policies on Active Directory (A
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (AD
1
2

Subcategory	Audit Events
Audit DPAPI Activity	Not Configured
Audit PNP Activity	Success
Audit Process Creation	Not Configured
Audit Process Termination	Not Configured
Audit RPC Events	Success
Audit Token Right Adjusted	Not Configured

4.4.5 Object Access

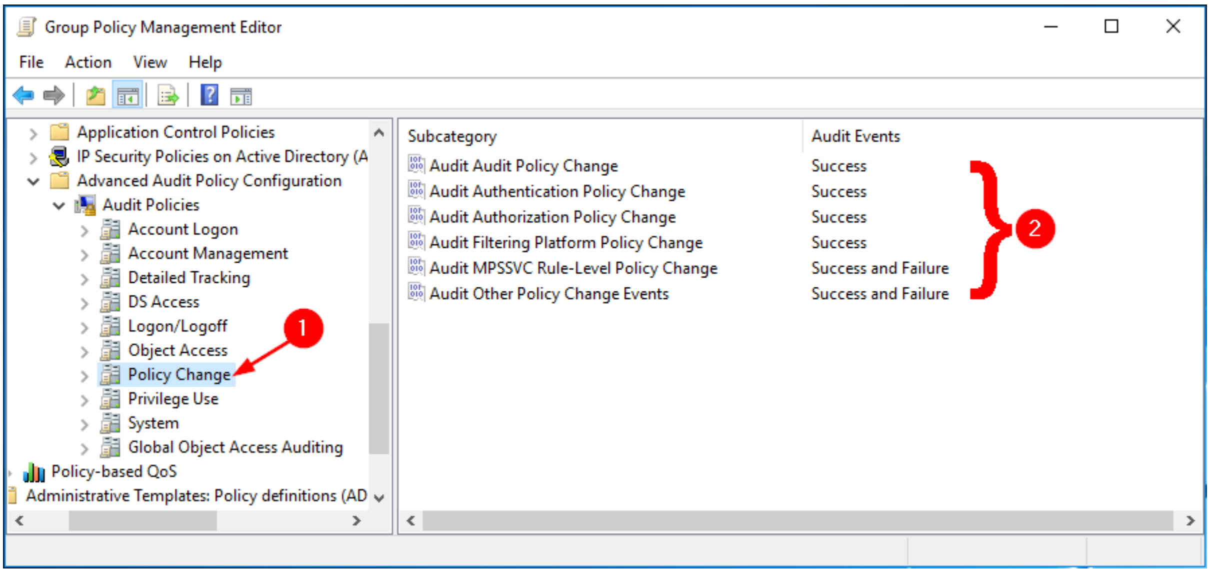
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **Objec Access** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
Application Control Policies
IP Security Policies on Active Directory (A
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (AD
references
Configuration
1
2

Subcategory	Audit Events
Audit Application Generated	Not Configured
Audit Certification Services	Success and Failure
Audit Detailed File Share	Not Configured
Audit File Share	Success and Failure
Audit File System	Not Configured
Audit Filtering Platform Connection	Not Configured
Audit Filtering Platform Packet Drop	Not Configured
Audit Handle Manipulation	Success and Failure
Audit Kernel Object	Not Configured
Audit Other Object Access Events	Success and Failure
Audit Registry	Success and Failure
Audit Removable Storage	Success and Failure
Audit SAM	Not Configured
Audit Central Access Policy Staging	Not Configured

4.4.6 Policy Change

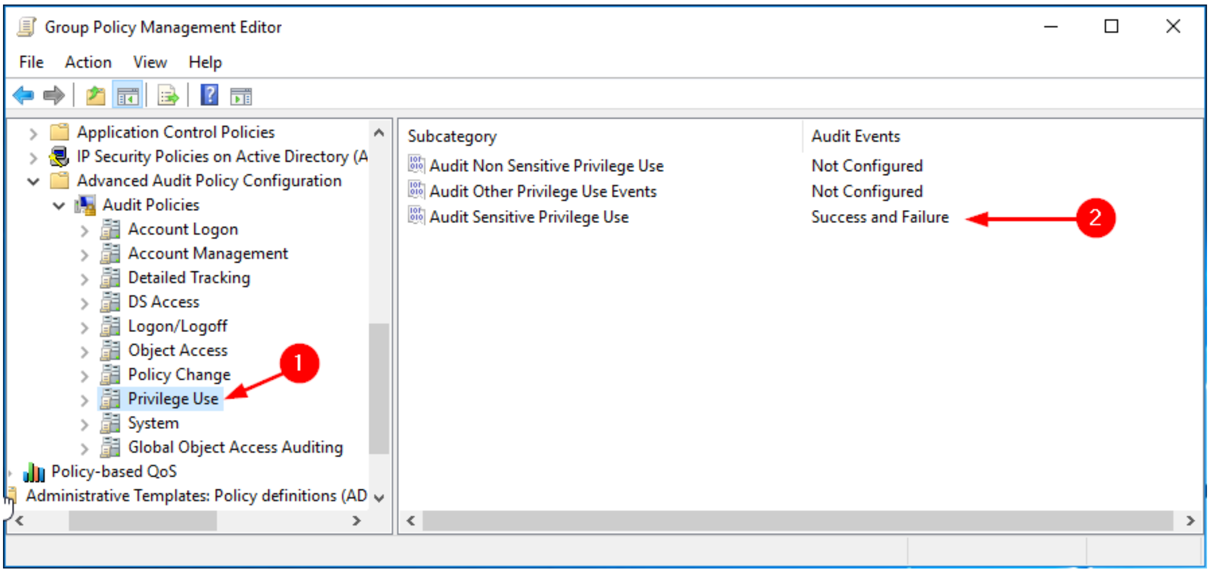
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **Policy Change** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
Application Control Policies
IP Security Policies on Active Directory (A
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (AD
1
2

Subcategory	Audit Events
Audit Audit Policy Change	Success
Audit Authentication Policy Change	Success
Audit Authorization Policy Change	Success
Audit Filtering Platform Policy Change	Success
Audit MPSSVC Rule-Level Policy Change	Success and Failure
Audit Other Policy Change Events	Success and Failure

4.4.7 Privileged Use

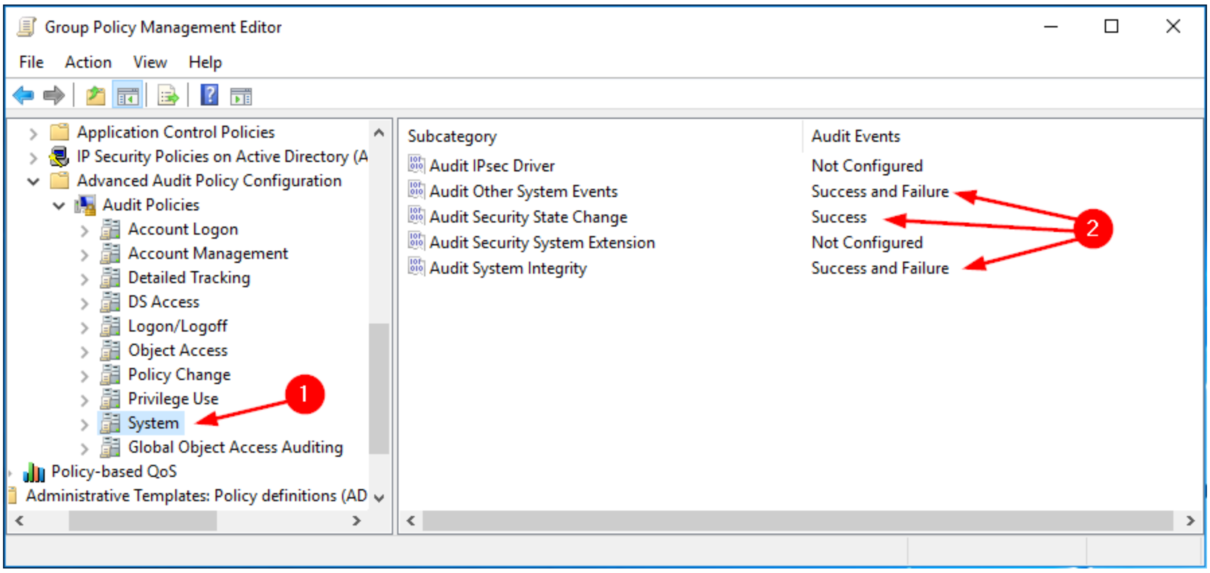
Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy*, posizionarsi su **Privileged Use** (1) e configurare i parametri (2) come indicato in figura.


Group Policy Management Editor
File
Action
View
Help
Application Control Policies
IP Security Policies on Active Directory (A
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (AD
1
2

Subcategory	Audit Events
Audit Non Sensitive Privilege Use	Not Configured
Audit Other Privilege Use Events	Not Configured
Audit Sensitive Privilege Use	Success and Failure

4.4.8 System

Da *Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Advanced Audit Policy Configuration -> Audit Policy,* posizionarsi su **System** (1) e configurare i parametri (2) come indicato in figura.



Group Policy Management Editor
File
Action
View
Help
Application Control Policies
IP Security Policies on Active Directory (A
Advanced Audit Policy Configuration
Audit Policies
Account Logon
Account Management
Detailed Tracking
DS Access
Logon/Logoff
Object Access
Policy Change
Privilege Use
System
Global Object Access Auditing
Policy-based QoS
Administrative Templates: Policy definitions (AD
1
2

Subcategory	Audit Events
Audit IPsec Driver	Not Configured
Audit Other System Events	Success and Failure
Audit Security State Change	Success
Audit Security System Extension	Not Configured
Audit System Integrity	Success and Failure

5 Configurazione Object-level access auditing

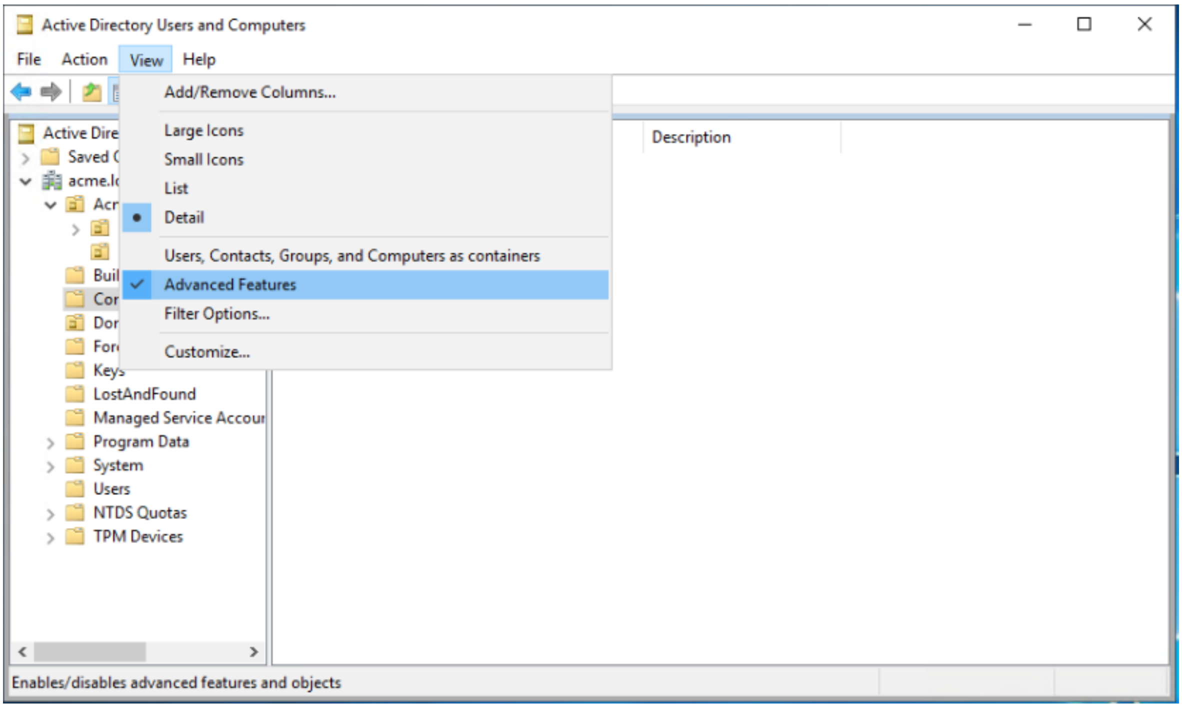
5.1 Active Directory Windows Server 2012 e superiori

È necessario configurare l’Object-level auditing per la Domain partition se si desidera raccogliere informazioni sull'attività utente nel dominio. Se si desidera anche controllare le modifiche alla configurazione e allo schema di AD, è necessario abilitare l’Object-level auditing anche per Configuration and Schema partitions.

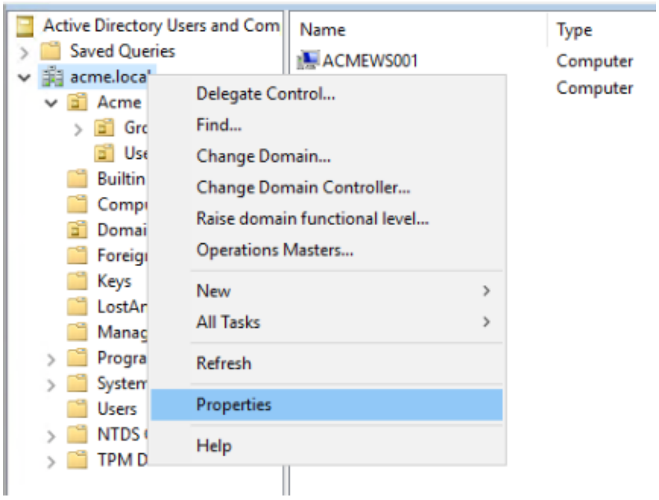
Seguire la procedura di seguito illustrata per ogni cartella o disco che si desidera controllare

1) Da un qualsiasi Domain Controller appartenente al dominio che si desidera controllare, aprire lo snap-in **Active Directory Users and Computers Group** che si trova in *Start* → *Windows Administrative Tools* o in *Start* -> *Administrative Tools*, a seconda della versione di Windows.

   Cliccare su View e verificare che “Advanced Features” sia selezionato.

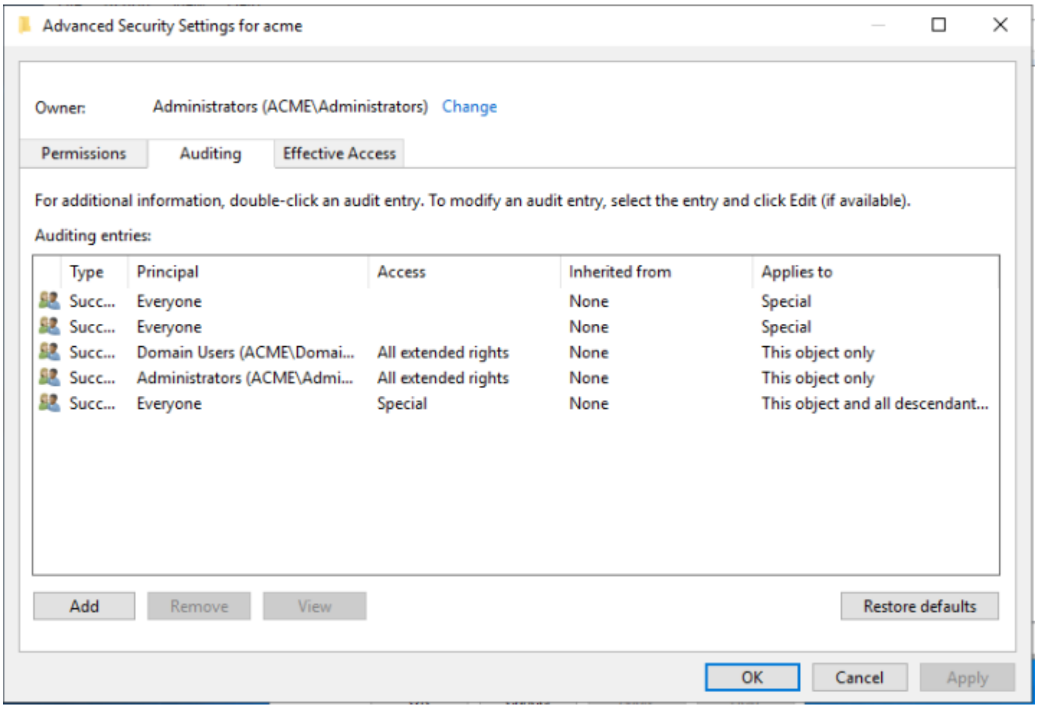


2) Cliccare con il tasto destro del mouse sul nodo del dominio da controllare, e selezionare la voce **Properties**.



3) All'interno del pannello delle proprietà selezionare il tab **Security** e poi cliccare il pulsante **Advanced** in basso a destra.

4) Nel pannello "Advanced Security Settings" selezionare il tab **Auditing**.



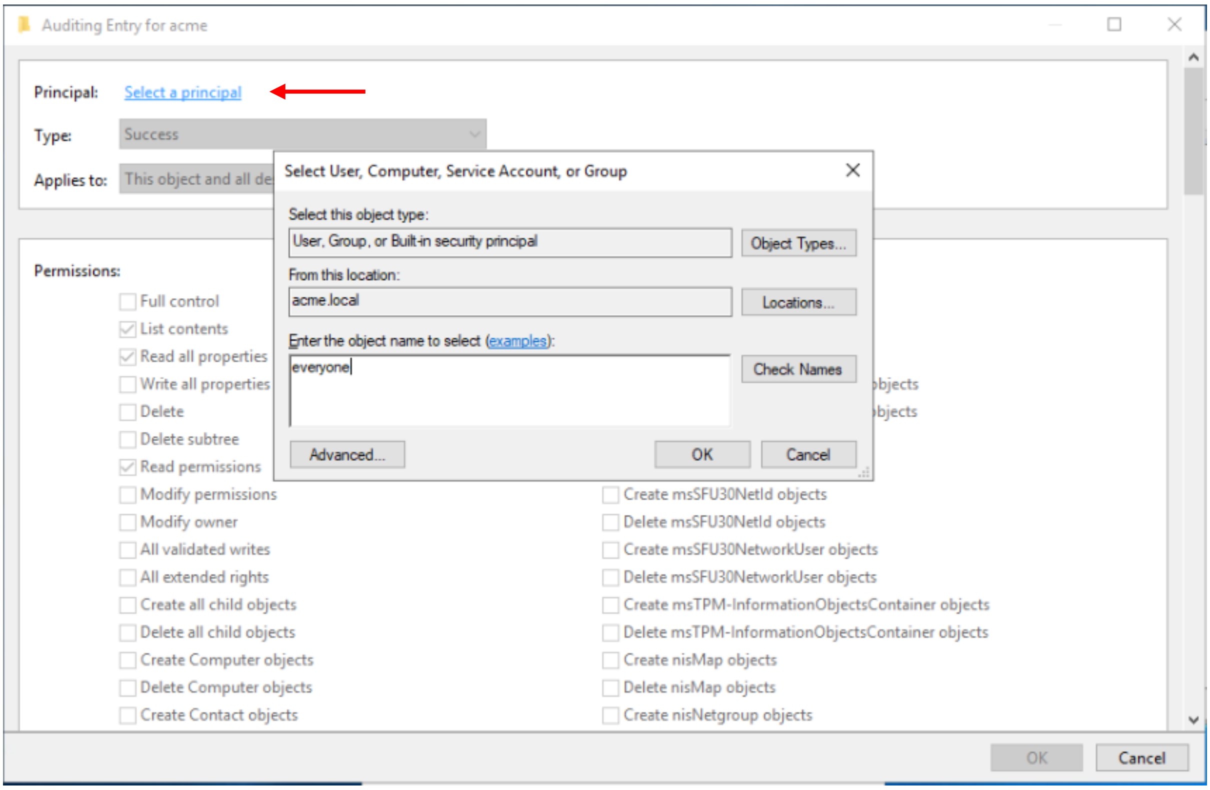
Owner: Administrators (ACME\Administrators) Change

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to
Succ...	Everyone		None	Special
Succ...	Everyone		None	Special
Succ...	Domain Users (ACME\Domai...	All extended rights	None	This object only
Succ...	Administrators (ACME\Admi...	All extended rights	None	This object only
Succ...	Everyone	Special	None	This object and all descendant...

Cliccare sul pulsante **Add** e poi nel pannello "Auditing Entry" selezionare il link **Select a principal**.



Auditing Entry for acme

Principal: Select a principal

Type: Success

Applies to: This object and all de

Select User, Computer, Service Account, or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
acme.local

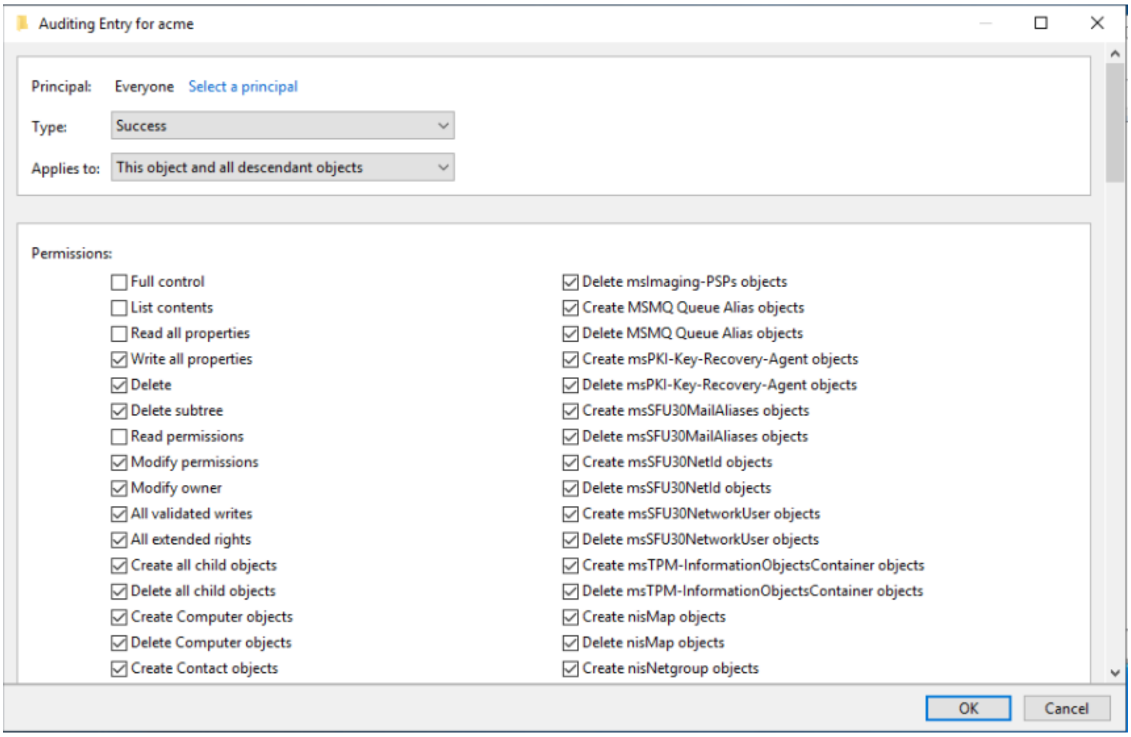
Enter the object name to select (examples):
everyone

Permissions:

- □ Full control
- ☑ List contents
- ☑ Read all properties
- □ Write all properties
- □ Delete
- □ Delete subtree
- ☑ Read permissions
- □ Modify permissions
- □ Modify owner
- □ All validated writes
- □ All extended rights
- □ Create all child objects
- □ Delete all child objects
- □ Create Computer objects
- □ Delete Computer objects
- □ Create Contact objects
- □ Create msSFU30NetId objects
- □ Delete msSFU30NetId objects
- □ Create msSFU30NetworkUser objects
- □ Delete msSFU30NetworkUser objects
- □ Create msTPM-InformationObjectsContainer objects
- □ Delete msTPM-InformationObjectsContainer objects
- □ Create nisMap objects
- □ Delete nisMap objects
- □ Create nisNetgroup objects

5) Nel pannello "Select User, Computer, Service Account, or Group" digitare "*everyone*" nel campo **Enter the object name to select** e confermare cliccando il pulsante OK.

Tornati nel pannello "Auditing Entry" impostare il campo **Type:** su "*Success*" ed il campo **Applies to:** su "*This object and all descendant objects*".



Auditing Entry for acme

Principal: Everyone Select a principal

Type: Success

Applies to: This object and all descendant objects

Permissions:

- □ Full control
- □ List contents
- □ Read all properties
- ☑ Write all properties
- ☑ Delete
- ☑ Delete subtree
- □ Read permissions
- ☑ Modify permissions
- ☑ Modify owner
- ☑ All validated writes
- ☑ All extended rights
- ☑ Create all child objects
- ☑ Delete all child objects
- ☑ Create Computer objects
- ☑ Delete Computer objects
- ☑ Create Contact objects
- ☑ Delete msImaging-PSPs objects
- ☑ Create MSMQ Queue Alias objects
- ☑ Delete MSMQ Queue Alias objects
- ☑ Create msPKI-Key-Recovery-Agent objects
- ☑ Delete msPKI-Key-Recovery-Agent objects
- ☑ Create msSFU30MailAliases objects
- ☑ Delete msSFU30MailAliases objects
- ☑ Create msSFU30NetId objects
- ☑ Delete msSFU30NetId objects
- ☑ Create msSFU30NetworkUser objects
- ☑ Delete msSFU30NetworkUser objects
- ☑ Create msTPM-InformationObjectsContainer objects
- ☑ Delete msTPM-InformationObjectsContainer objects
- ☑ Create nisMap objects
- ☑ Delete nisMap objects
- ☑ Create nisNetgroup objects

6) Nel box **Permissions** selezionare tutti i checkboxes, fatta eccezione per i seguenti permessi:
   - Full Control
   - List Contents
   - Read All Properties
   - Read Permissions

7) Verificare che, a fondo pagina, il checkbox **Only apply these auditing settings to objects and/or containers within this container** non sia selezionato, e cliccare il pulsante **OK** per confermare.

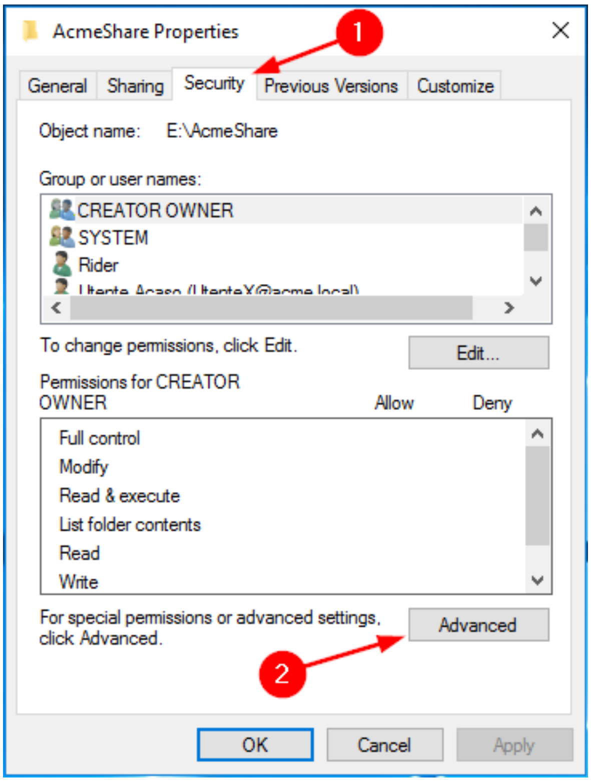
5.2 Windows File Server 2012 e superiori

La configurazione dell'Object-level access auditing è indispensabile per poter raccogliere gli eventi di audit generati grazie a quanto specificato nella Advanced Audit Policy.

Tramite la configurazione dell'Object-level access auditing andremo a specificare quali classi di eventi raccogliere e quali utenti controllare.

Seguire la procedura di seguito illustrata per ogni cartella o disco che si desidera controllare.

1) Fare click destro sulla cartella che si vuole controllare e selezionare **Properties** dal menu pop-up. Selezionare il tab **Security** (1) e poi fare click su **Advanced** (2).



Object name: E:\AcmeShare

Group or user names:

CREATOR OWNER
SYSTEM
Rider
Utente Acaso (UtenteX@acme.local)

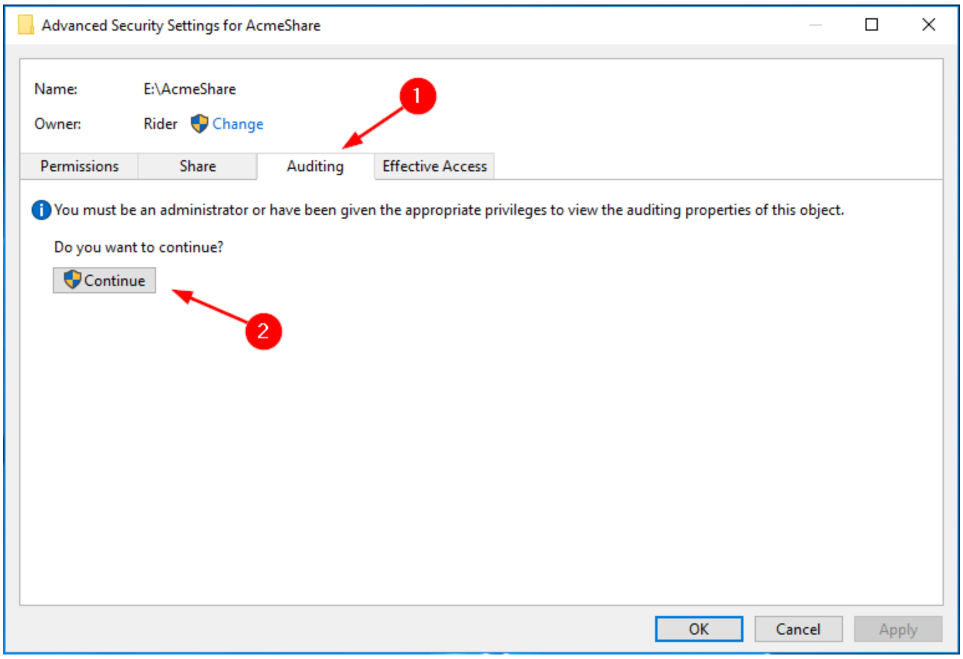
To change permissions, click Edit.

Permissions for CREATOR OWNER Allow Deny

Full control
Modify
Read & execute
List folder contents
Read
Write

For special permissions or advanced settings, click Advanced.

2) Selezionare il tab **Auditing** e fare click su **Continue** (2)



Advanced Security Settings for AcmeShare

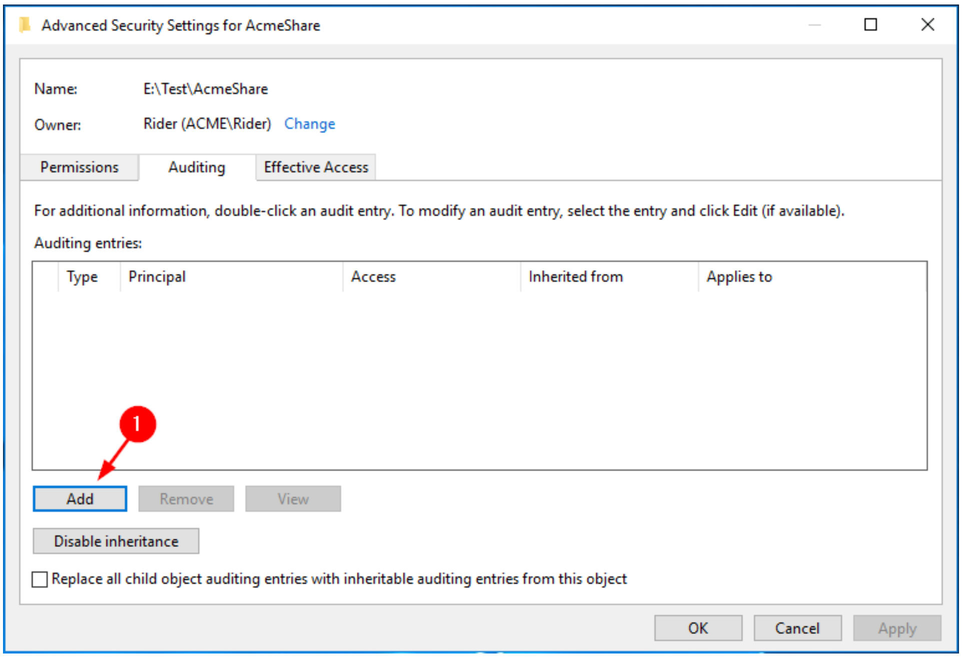
Name: E:\AcmeShare

Owner: Rider Change

You must be an administrator or have been given the appropriate privileges to view the auditing properties of this object.

Do you want to continue?

3) fare click sul pulsante **Add** (1) per aggiungere una nuova configurazione dei permessi di auditing.



Advanced Security Settings for AcmeShare

Name: E:\Test\AcmeShare

Owner: Rider (ACME\Rider) Change

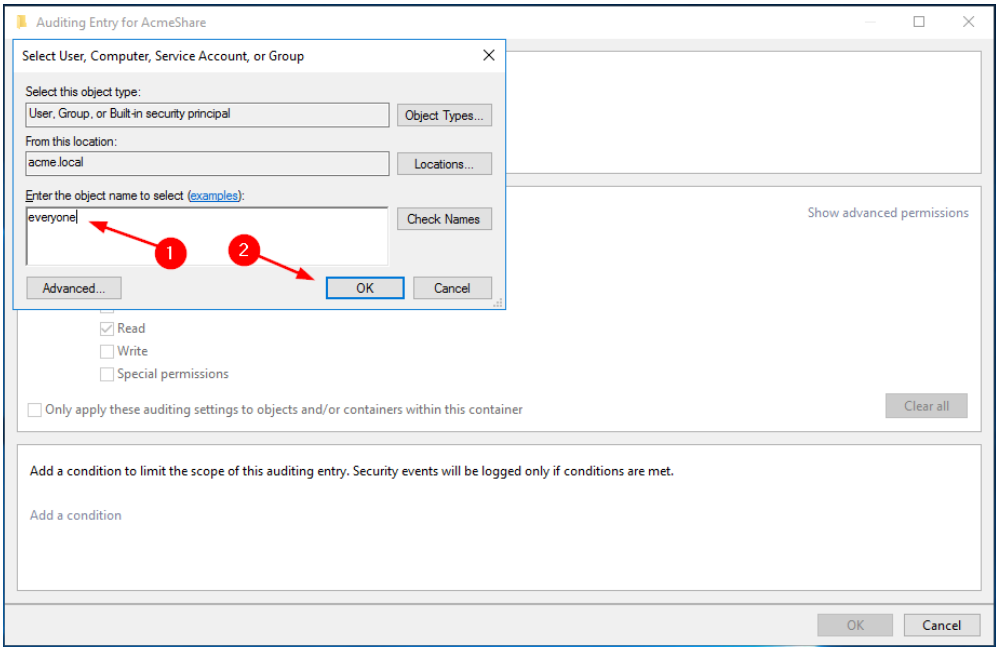
For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	Principal	Access	Inherited from	Applies to

□ Replace all child object auditing entries with inheritable auditing entries from this object

4) Fare click sul link **Select a principal** in alto a sinistra per aggiungere un nuovo principal, e selezionare **Everyone** (1), o qualsiasi gruppo personalizzato contenente gli utenti dei quali si vogliono monitorare gli accessi.



Auditing Entry for AcmeShare

Select User, Computer, Service Account, or Group

Select this object type:
User, Group, or Built-in security principal

From this location:
acme.local

Enter the object name to select (examples):
everyone

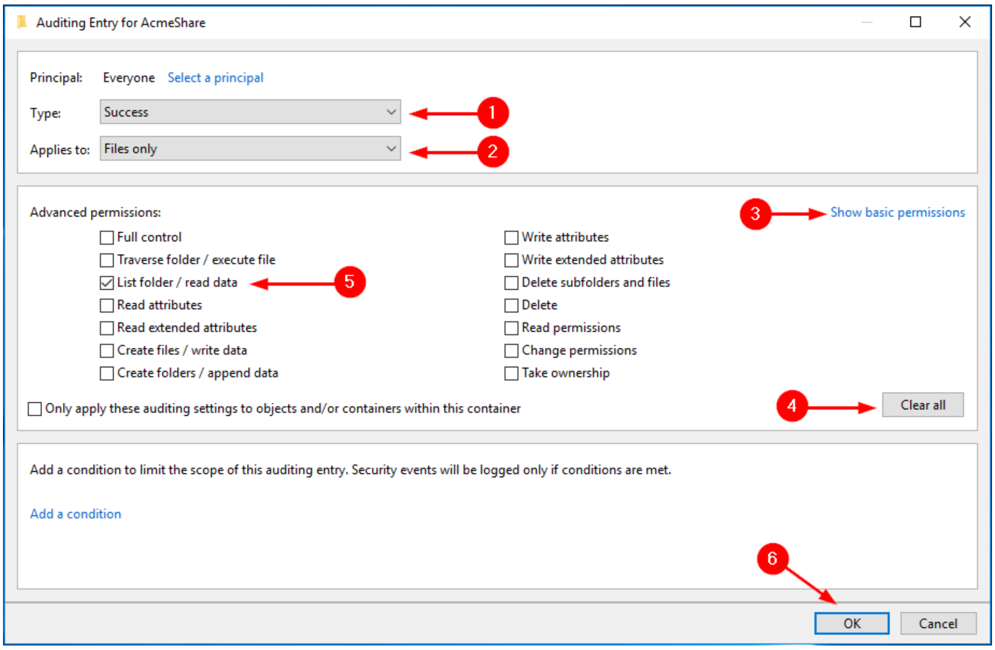
☑ Read
□ Write
□ Special permissions

□ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

A questo punto è possibile impostare le voci di controllo relative ai tipi di accesso che si vuole controllare. Di seguito vengono illustrate le configurazioni necessarie:

5) Controllo accessi in lettura riusciti



Auditing Entry for AcmeShare

Principal: Everyone Select a principal

Type: Success

Applies to: Files only

Advanced permissions:

□ Full control
□ Traverse folder / execute file
☑ List folder / read data
□ Read attributes
□ Read extended attributes
□ Create files / write data
□ Create folders / append data
□ Write attributes
□ Write extended attributes
□ Delete subfolders and files
□ Delete
□ Read permissions
□ Change permissions
□ Take ownership

□ Only apply these auditing settings to objects and/or containers within this container

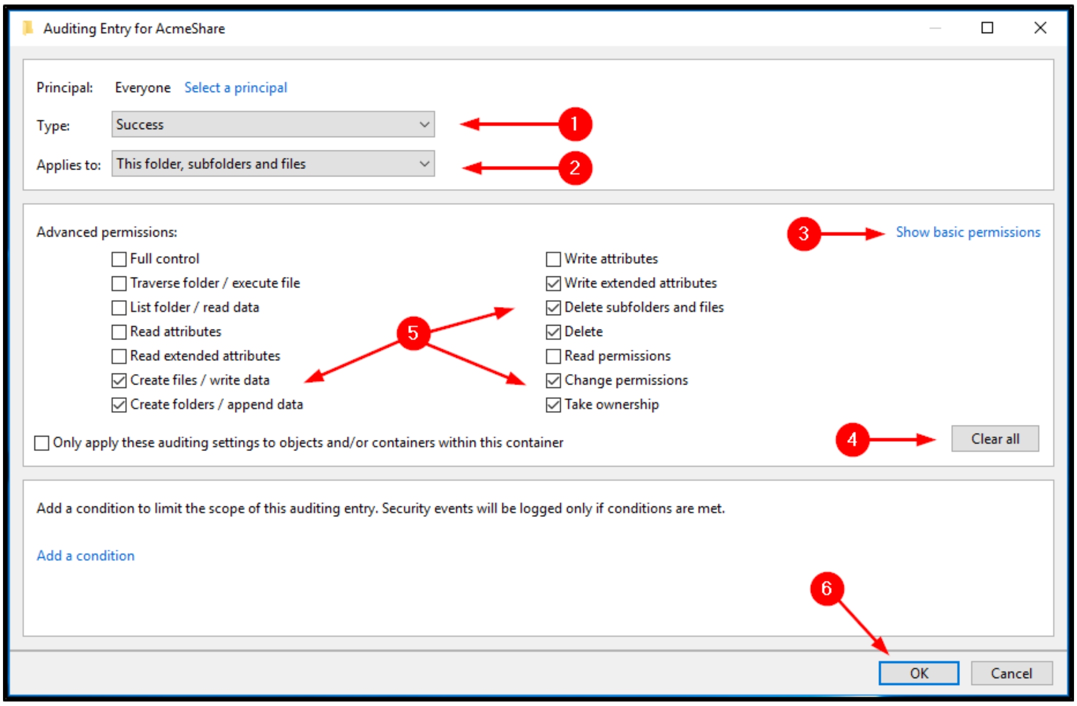
Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

- Impostare il campo **Type**: -> Success (1)
- Impostare il campo **Applies to:** -> File Only (2)

- Fare click sul link **Show Advanced Permissions** (3)
- Fare click sul pulsante **Clear All** (4) per deselezionare tutti i permessi preimpostati
- Selezionare i seguenti permessi (5)
    - List folder / read data
- Premere il pulsante **OK** (6) per salvare la configurazione

6) Controllo accessi in modifica riusciti

Ripetere i punti 3 e 4 per creare un nuovo set di permessi ed impostare come segue:



Auditing Entry for AcmeShare

Principal: Everyone Select a principal

Type: Success

Applies to: This folder, subfolders and files

Advanced permissions:

☐ Full control
☐ Traverse folder / execute file
☐ List folder / read data
☐ Read attributes
☐ Read extended attributes
☑ Create files / write data
☑ Create folders / append data

☐ Write attributes
☑ Write extended attributes
☑ Delete subfolders and files
☑ Delete
☐ Read permissions
☑ Change permissions
☑ Take ownership

☐ Only apply these auditing settings to objects and/or containers within this container

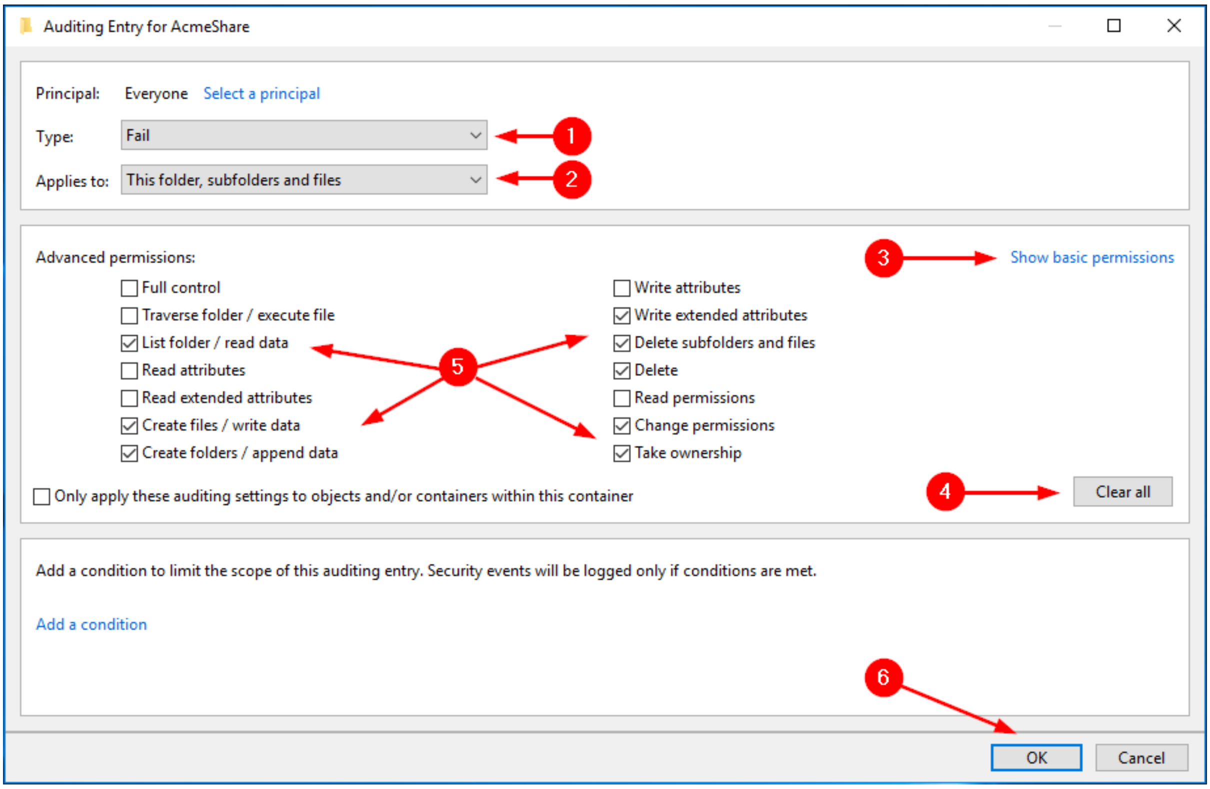
Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

Add a condition

- Impostare il campo **Type**: -> Success (1)
- Impostare il campo **Applies to:** -> This folder, subfolders, and files (2)
- Fare click sul link **Show Advanced Permissions** (3)
- Fare click sul pulsante **Clear All** (4) per deselezionare tutti i permessi preimpostati
- Selezionare i seguenti permessi (5)
    - Create files / write data
    - Create folders / append data
    - Write extended attributes
    - Delete subfolders and files
    - Delete
    - Change permissions
    - Take ownership
- Premere il pulsante **OK** (6) per salvare la configurazione

7) Controllo accessi in lettura o modifica falliti

Ripetere i punti 3 e 4 per creare un nuovo set di permessi ed impostare come segue:



Auditing Entry for AcmeShare

Principal: Everyone Select a principal

Type: Fail

Applies to: This folder, subfolders and files

Advanced permissions:

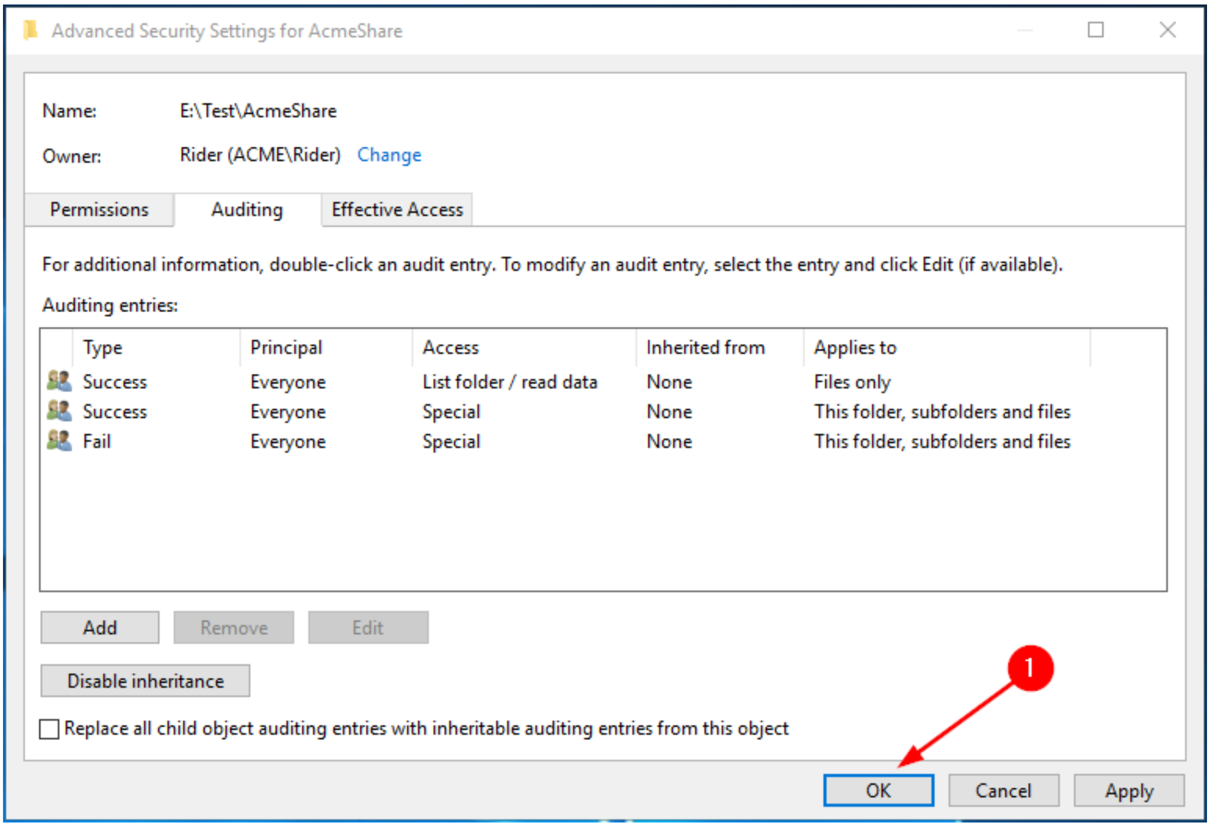
☐ Full control
☐ Traverse folder / execute file
☑ List folder / read data
☐ Read attributes
☐ Read extended attributes
☑ Create files / write data
☑ Create folders / append data
☐ Write attributes
☑ Write extended attributes
☑ Delete subfolders and files
☑ Delete
☐ Read permissions
☑ Change permissions
☑ Take ownership

☐ Only apply these auditing settings to objects and/or containers within this container

Add a condition to limit the scope of this auditing entry. Security events will be logged only if conditions are met.

- Impostare il campo **Type**: -> Fail (1)
- Impostare il campo **Applies to:** -> This folder, subfolders, and files (2)
- Fare click sul link **Show Advanced Permissions** (3)
- Fare click sul pulsante **Clear All** (4) per deselezionare tutti i permessi
- Selezionare i seguenti permessi (5)
  - List folder / read data
  - Create files / write data
  - Create folders / append data
  - Write extended attributes
  - Delete subfolders and files
  - Delete
  - Change permissions
  - Take ownership
- Premere il pulsante **OK** (6) per salvare la configurazione

8) Terminate le configurazioni fare click sul pulsante **OK** (1) per salvare ed applicare i permessi impostati.



Advanced Security Settings for AcmeShare

Name: E:\Test\AcmeShare

Owner: Rider (ACME\Rider) Change

Permissions | Auditing | Effective Access

For additional information, double-click an audit entry. To modify an audit entry, select the entry and click Edit (if available).

Auditing entries:

Type	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

□ Replace all child object auditing entries with inheritable auditing entries from this object