

Group Policy

- [Windows Server Audit Policy](#)
- [GPO WMI Filters](#)
- [Reset GPO](#)

Windows Server Audit Policy

Backup

To backup existing auditing settings:

```
auditpol /backup /file:C:\Temp\Audit.txt
```

Restore

To restore the auditing settings:

```
auditpol /restore /file:C:\Temp\Audit.txt
```

Display Settings

To check the auditing settings:

```
auditpol /get /category:*
```

Clear Settings

Option 1 - Copy and paste from good server

1. 'auditpol /backup /file:c:\temp\audit.txt' on a good DC in the lab
2. 'auditpol /backup /file:c:\temp\audit.txt' on the borked DC
3. Open c:\temp\audit.txt on the borked DC
4. Copy/paste the contents from the good DC into audit.txt on borked DC in notepad
5. Replace good DC name with borked DC name and save file
6. 'auditpol /restore /file:c:\temp\audit.txt'

Option 2 - Reset everything

To clear or rollback to defaults settings:

1. Reset all of your local advanced audit settings. If you did this via GPO, reset the settings in this GPO.

```
auditpol /clear
```

For local policies delete the **Audit.csv** from all of these locations. Some may be hidden, but they are there!!

- C:\Windows\security\audit

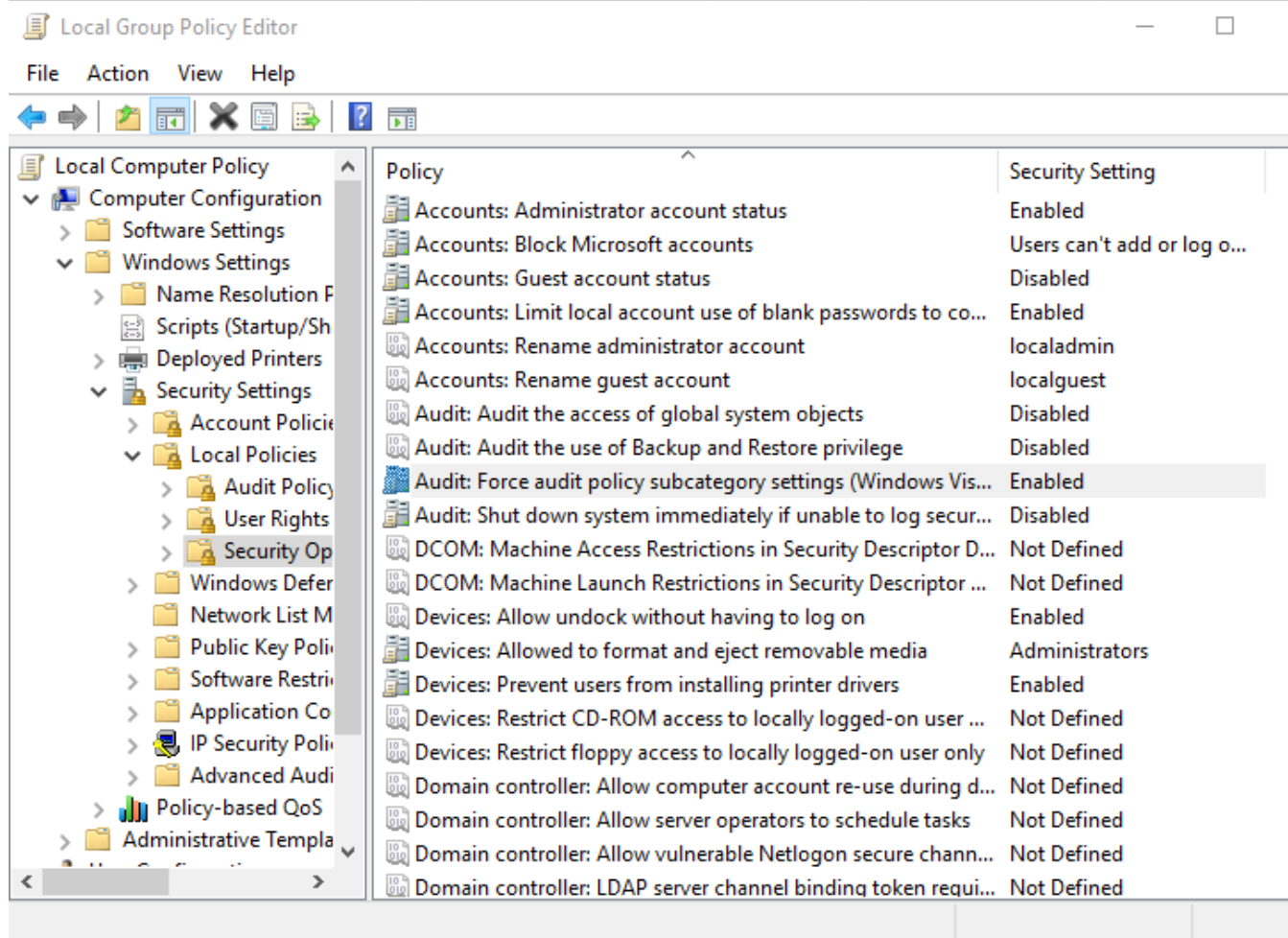
- C:\Windows\System32\GroupPolicy\Machine\Microsoft\Windows NT\Audit

For domain based policy this will be in SYSVOL

- \[Domain]\sysvol\[Domain]\Policies\{GUID}\Machine\Microsoft\Windows NT\Audit

2. You must set the local policy "Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings" to **DISABLED**.

In GPO, "Security Settings->Local Policies->Security Options", setting "Audit: Force audit policy subcategory settings".



When you do this and it is applied you will see the registry key
HKLM\SYSTEM\CurrentControlSet\Control\Lsa - SCENoApplyLegacyAuditPolicy = 0
(DWORD)

3. Now reboot or "gpupdate /force" and you should be back to the start again.

GPO WMI Filters

Hostname Filter

```
Select * From Win32_ComputerSystem Where Name = "ComputerName"
```

Target Hostname

General

Delegation

WMI Filter

Description:

Edit Filter...

Queries:

| Namespace | Query |
|------------|----------------------------------------------------------------|
| root\CIMv2 | Select * From Win32_ComputerSystem Where Name = "ComputerName" |

Windows 2019 Domain Controller Filter

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.17763" AND ProductType LIKE "2"
```

Windows Server 2019 Domain Controller Filter

General

Delegation

WMI Filter

Description: WMI Filter for Windows Server 2019 Domain Controller

Edit Filter...

Queries:

| Namespace | Query |
|------------|----------------------------------------------------------------------------------------------|
| root\CIMv2 | SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.17763" AND ProductType LIKE "2" |

Windows 2019 Member Server Filter

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.17763" AND ProductType LIKE "3"
```

Windows Server 2019 Server Member Filter

General Delegation

WMI Filter

Description: WMI Filter for Windows Server 2019 Server Member

Edit Filter...

Queries:

| Namespace | Query |
|------------|----------------------------------------------------------------------------------------------|
| root\CIMv2 | SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.17763" AND ProductType LIKE "3" |

Windows Server 2016 Domain Controller Filter

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.14393" AND ProductType LIKE "2"
```

Windows Server 2016 Domain Controller Filter

General Delegation

WMI Filter

Description: WMI Filter for Windows Server 2016 Domain Controller

Edit Filter...

Queries:

| Namespace | Query |
|------------|----------------------------------------------------------------------------------------------|
| root\CIMv2 | SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.14393" AND ProductType LIKE "2" |

Windows Server 2016 Server Member Filter

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.14393" AND ProductType LIKE "3"
```

Windows Server 2016 Server Member Filter

General Delegation

WMI Filter

Description: WMI Filter for Windows Server 2016 Server Member

Edit Filter...

Queries:

| Namespace | Query |
|------------|----------------------------------------------------------------------------------------------|
| root\CIMv2 | SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "10.0.14393" AND ProductType LIKE "3" |

Windows Server 2012 R2 Server Member Filter

```
SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "6.3%" AND ProductType="3"
```

Windows Server 2012 R2 Server Member Filter

General Delegation

WMI Filter

Description: WMI Filter for Windows Server 2012 R2 Server Member

Edit Filter...

Queries:

| Namespace | Query |
|------------|-----------------------------------------------------------------------------------|
| root\CIMv2 | SELECT * FROM Win32_OperatingSystem WHERE Version LIKE "6.3%" AND ProductType="3" |

Windows Server Member (Hyper-V) Filter

```
SELECT * FROM Win32_ServerFeature WHERE ID=20
```

Windows Server Member (Hyper-V) Filter

General Delegation

WMI Filter

Description: WMI Filter for Windows Server Member with Hyper-V Role

Edit Filter...

Queries:

| Namespace | Query |
|------------|-----------------------------------------------|
| root\CIMv2 | SELECT * FROM Win32_ServerFeature WHERE ID=20 |
| | |

Windows Web Service (IIS) Role Filter

```
SELECT Name FROM Win32_ServerFeature WHERE Name = "Web Server (IIS)"
```

Windows Web Service (IIS) Role Filter

General Delegation

WMI Filter

Description: WMI Filter for Windows Web Service (IIS) Role

Edit Filter...

Queries:

| Namespace | Query |
|------------|----------------------------------------------------------------------|
| root\CIMv2 | SELECT Name FROM Win32_ServerFeature WHERE Name = "Web Server (IIS)" |
| | |

Reset GPO

To clear Local GPO

Delete everything inside the GPO folder

```
RD /S /Q "%WinDir%\System32\GroupPolicyUsers" && RD /S /Q "%WinDir%\System32\GroupPolicy"
```

To clear Domain GPO

Make a backup of the GPO in the domain first.

To reset the Default Domain Controller Policy:

```
dcgpofix /ignoreschema /target:DC
```

To reset the Default Domain Policy:

```
dcgpofix /ignoreschema /target:Domain
```