

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

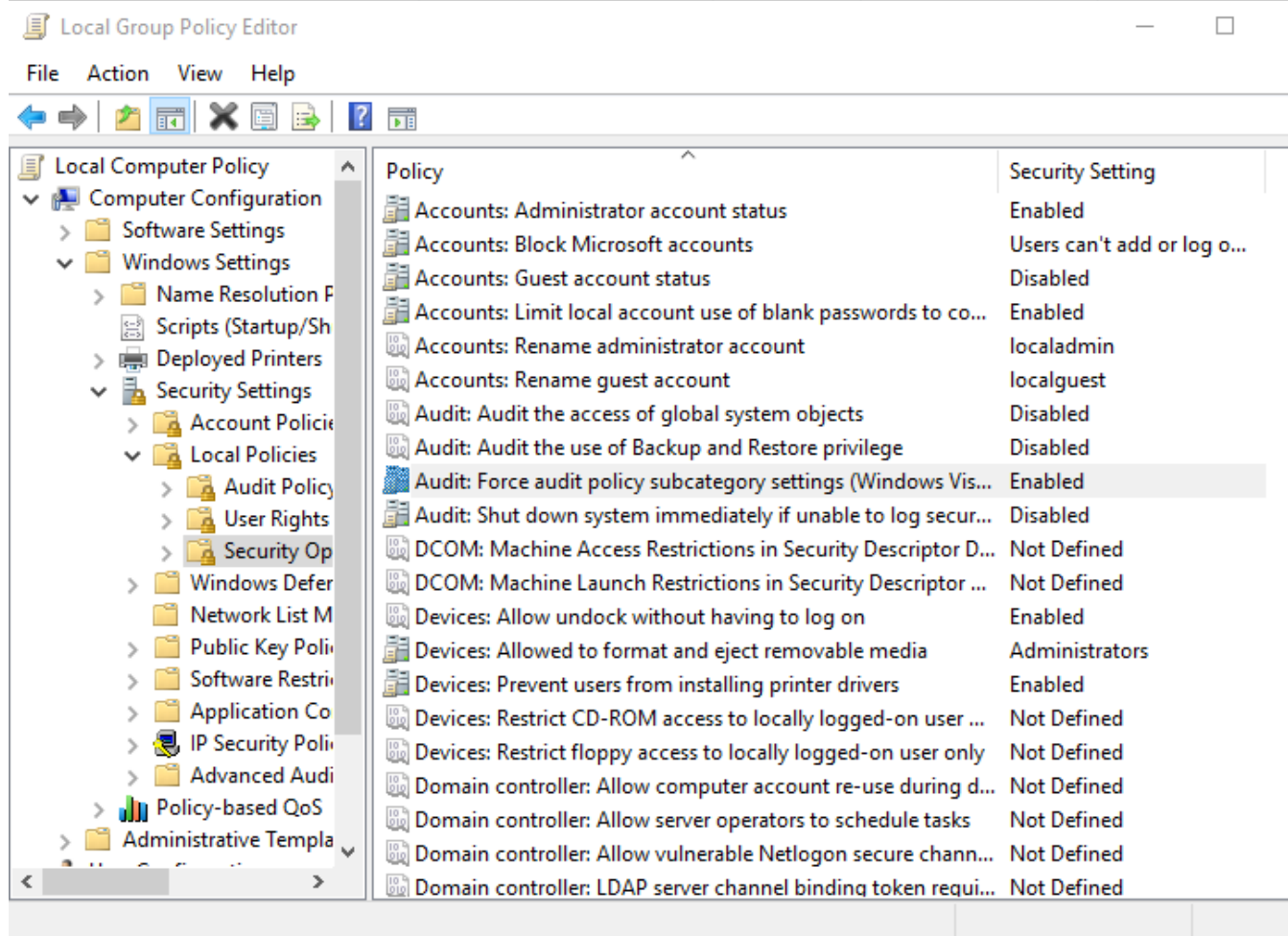
- C:\Windows\System32\GroupPolicy\Machine\Microsoft\Windows NT\Audit

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.

Revision #3

Created 1 January 2024 18:59:14 by aki

Updated 1 January 2024 20:03:16 by aki