Active Directory Auditing Configuration Checklist:

- Audit Policy settings configured in GPO.
- Object-Level AD auditing settings configured.
- Event log settings set.
- For fully automated AD auditing try Netwrix Auditor: netwrix.com/trial

How To #1: Audit Policy Settings

Using the Group Policy Management Console, edit "Default Domain Controllers Policy":


How To #2: Object-level AD Auditing

Launch ADSIEdit from Administrator Tools > Right-click Domain > Properties > Security (Tab) > Advanced (Button) > Auditing (Tab) > Select "Everyone" > Edit (Button) > Make sure the following are OFF:

- Full Control, List Contents, Read all properties, Read permissions
- "Apply these auditing entries to objects and/or containers within this container only" (Check Box) > Click "OK" x3

How To #3: Security Event Log Settings

Perform the following using GPMC, edit "Default Domain Controllers Policy":

> Computer Configuration > Policies > Security Settings > Local Policies > Event Log > Maximum security log size > Define > 130048 > OK

> Retain security log > Define >14* > OK

> Retention method for security log > Define > Overwrite events as needed

*Check available disk space

517/1102 – Security Log Cleared
528/4624 – Login Succeeded
529/4625* – Failed Login
530/4625* – Failed Login (Time Restr.)
531/4625* – Disabled User Acct.
532/4625* – Account Expired
533/4625* – Failed Login (Wrkst. Restr.)
534/4625* (5461) – Failed Login (Does not have rights to use login method)
535/4625* – Password Expired
539/4625* – Failed Login, Acct. Locked
540/4624 – Login Succeeded (2k, k3, xp)
624/4720 – User Acct. Created
626/4722 – User Acct. Enabled
628/4724 – User Acct. Password Set
629/4725 – User Acct. Disabled
630/4726 – User Acct. Deleted
631(1), (5), 648, 653(3), (8), 663/4727), (31), (44), (49), (54), (59)
Group Created
632, 636, 650, 655, 660, 665/4728, 4732, 4746, 4751, 4756, 4761
Group Member Added
633, 638, 652, 657, 662, 667/4730, 4734, 4748, 4753, 4758, 4763
Group Deleted
639, 641, 649, 654, 659, 664/4735, 4737, 4745, 4750, 4755, 4760
Group Changed
644/4740 – User Acct. Locked Out (Due to Failed Login Attempts)
647/4743 – Computer Deleted
668/4764 – Group Type Changed
671/4767 – User Acct. Unlocked
675/4771 – Auth. Fail-Workstation

Click to share this document with others:  

Visit netwrix.com/trial to learn more.