Quick Reference Guide: WINDOWS SERVER AUDITING

Windows Server Auditing Configuration Checklist:

- [ ] Local Audit Policy settings configured in GPO.
- [ ] Windows Registry Audit Settings configured.
- [ ] Event Log Settings configured.
- [ ] Download Netwrix Auditor To Simplify Your Auditing netwrix.com/trial

How To #1: Configure Local Audit Policies

To configure Local Policy settings in GPO, Right-click GPO > Edit > Group Policy Mgmt. The Editor *opens.*

Expand the Computer Configuration *node on the left* > Policies > Windows Settings > Security Settings > Local Policies > Audit Policy > Account Mgmt. *Double-click* Audit account Mgmt. *on the right* > *Select* Success > OK.

Repeat this operation for the Audit object access policy

How To #2: Configure Windows Registry Audit Settings

Start > Run, *type* "regedit" > OK.
Expand HKEY_LOCAL_MACHINE > *Right-click* Software > Permissions > Advanced > *Select* Auditing tab > *Click* Add button > *Type* Everyone > OK.

In the Auditing Entry for SOFTWARE *dialog, select* Successful. *For* : Set Value, Create Subkey, Delete, Write DAC, Write Owner > OK.

Repeat steps for the HKEY_LOCAL_MACHINE\SYSTEM *and* HKEY_USERS\.DEFAULT *nodes.*

How To #3: Configure Event Log Settings

Start > Programs > Administrative Tools > Event Viewer > *Open* Windows Logs *node* > *Right-click* Applications > Properties.

Make sure the Enable logging *check box is selected.*

Specify values in the Maximum log size *field: for 2K3* – 300MB/ *for 2K8* – 1GB.

Set retention method to Overwrite events as needed *or* Archive the log when full.

Repeat this operation for the Security and System event logs located under the Windows Logs *node, and for the Microsoft-WindowsTaskScheduler/Operational event log by navigating to* Applications and Services Logs > Microsoft > Windows > TaskScheduler > Operational.

Event ID Reference (2k3/2k8)

636/4732 – Local Group Member Added
637/4733 – Local Group Member Removed
635/4731 – Local Group Created
638/4734 – Local Group Deleted
624/4720 – User Account Created
630/4276 – User Account Deleted
639/4735 – Local Group Changed
642/4738 – User Account Changed
627/4723 – Change Password Attempt
628/4724 – User Account Password Set
685/4781 – User Name Changed
567/4657, 4663 – Object Access Attempt
560/4656 – Object Open
562/4658 – Handle Closed
602/4699 – Scheduled Task Created
602/4699 – Scheduled Task Deleted
602/4700 – Scheduled Task Enabled
602/4701 – Scheduled Task Disabled