netwrix

File Server Auditing

WINDOWS **FILE SERVER AUDITING** CONFIGURATION CHECKLIST:

- [ ] Default Audit Settings on File Shares configured
- [ ] Audit Object Access Policy configured/ Granular Audit Policy Configured
- [ ] Event Log Settings configured
- [ ] For fully automated File Server auditing try Netwrix Auditor: netwrix.com/auditor

Before configuring the audit settings, consider that if you have multiple file shares frequently accessed by a significant number of users, it is reasonable to audit objects modification only. Tracking all access events may result in too much data written to the audit logs, whereas only some part of it may be of any interest.

HOW TO #1: CONFIGURE DEFAULT AUDIT SETTINGS ON FILE SHARES

1. Navigate to the required file share, right-click it and select **Properties.**

2. Select the **Security** tab and click the **Advanced** button. The Advanced Security Settings for <Share_Name> form will open.

3. Go to the Auditing tab, select the Everyone group (or another user-defined group of the selected users granted special permissions) and click **Edit.** The Advanced Security Settings for <Share_Name> form will open as a separate dialog.

4. Select the **Everyone** group and click the **Edit** button. The Auditing Entry for <Share_Name> dialog will appear.

5. Select the **Success** and **Failed** check-boxes for the following Access options: List Folder / Read Data; Create Files / Write Data; Create Folders / Append Data; Write Attributes; Write Extended Attributes; Delete Subfolders and File; Delete; Change Permissions; Take Ownership.

6. Make sure that the **Apply** onto parameter is set to **This folder, subfolders and files,** and the **Apply these auditing entries to objects and/or containers within this container only** check box is cleared.

7. Click **OK** to save the changes and close the dialog.

To collect data from the monitored file servers, you must configure the Audit object access policy on the file servers. You must be logged on as a member of the Administrators group or you must be granted the Manage auditing and security log permission in Group Policy to perform this procedure.

HOW TO #2: CONFIGURE AUDIT OBJECT ACCESS POLICY

1. Navigate to **Start > Programs > Administrative** Tools > Group Policy **Management.** The dialog will appear.

2. Expand the **Domains** node, right-click the **<Company_Domain_Name>** node and select **Create a GPO in this domain and Link it here** option. The New GPO dialog will appear.

3. Type in the name of your new GPO into the **Name** field and click **OK.**

4. Right-click the newly created GPO in the left pane of the **Group Policy Management** form and select the **Edit** option. **Group Policy Management Editor** will open

5. Expand the Computer Configuration node on the left and then go to Policies > Windows Settings > Security Settings > Local Policies > Audit Policy.

6. Double-click **Audit object access** on the right and select all check boxes in the **Audit** object access **Properties** dialog.

7. Click **OK** to save the changes and close the form.

To collect data from the monitored file servers, you must configure the Audit object access policy on the file servers. You must be logged on as a member of the Administrators group or you must be granted the Manage auditing and security log permission in Group Policy to perform this procedure.

HOW TO #3: CONFIGURE GRANULAR AUDIT POLICY (FOR WINDOWS SERVER 2008 R2/WINDOWS 7)

1. On a monitored file server, open the Local Security Policy snap-in (navigate to Start > Run and type 'secpol.msc').

2. Navigate to Security Settings > Local Policies > Security Options and locate the Audit: Force audit policy subcategory settings (Windows Vista or later) policy:

3. Double-click this policy and select the Enabled option in the dialog that opens.

4. RNavigate to Security Settings > Advanced Audit Policy Configuration > System Audit Policies > Object Access and enable the following subcategories: Audit File System and Audit Handle Manipulation. To do this, double click a subcategory, select the Configure the following audit events: option and select the Success and/or Failure checkboxes depending on the type of events you want to track.

5. Update your Group Policies by executing the gpupdate /force command in the command line interface.

6. Double-click **Audit object access** on the right and select all check boxes in the **Audit** object access **Properties** dialog.

***Note: You can check your current effective settings by executing the following command: auditpol /get /category:"Object Access"

Defining the event logs size is essential for configuration auditing. If your event log size is insufficient, overwrites may occur before data is written to the SQL database, and some audit data may be lost.

HOW TO #4: 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)

560/4656 – Object Open

567/4663 – Object Access Attempt