CONFIGURING TARGET ACTIVE DIRECTORY DOMAIN FOR AUDIT BY NETWRIX AUDITOR

TECHNICAL ARTICLE

Product Version: 5.0
July 2013
Legal Notice

The information in this publication is furnished for information use only, and does not constitute a commitment from Netwrix Corporation of any features or functions discussed. Netwrix Corporation assumes no responsibility or liability for the accuracy of the information presented, which is subject to change without notice.

Netwrix is a registered trademark of Netwrix Corporation. The Netwrix logo and all other Netwrix product or service names and slogans are registered trademarks or trademarks of Netwrix Corporation. Active Directory is a trademark of Microsoft Corporation. All other trademarks and registered trademarks are property of their respective owners.

Disclaimers

This document may contain information regarding the use and installation of non-Netwrix products. Please note that this information is provided as a courtesy to assist you. While Netwrix tries to ensure that this information accurately reflects the information provided by the supplier, please refer to the materials provided with any non-Netwrix product and contact the supplier for confirmation. Netwrix Corporation assumes no responsibility or liability for incorrect or incomplete information provided about non-Netwrix products.

© 2013 Netwrix Corporation.

All rights reserved.
Table of Contents

1. INTRODUCTION ........................................................................................................ 4
2. CONFIGURING DOMAIN AUDIT POLICIES ......................................................... 6
3. CONFIGURING SECURITY EVENT LOG SIZE AND RETENTION SETTINGS .......... 7
4. CONFIGURING OBJECT-LEVEL AUDITING ......................................................... 11
5. CONFIGURING EXCHANGE SERVER AAL SETTINGS .......................................... 17
1. **INTRODUCTION**

Successful change auditing requires a certain configuration of the audit settings in the monitored Active Directory domain. Otherwise, your change reports may contain errors and incomplete audit data. For example, you can receive a report containing the “System” value instead of an account name in the “Who changed” column.

Netwrix Auditor can configure audit settings in the monitored AD domain automatically, by selecting the corresponding option on Managed Object creation, or through the Audit Configuration wizard. If you wish to do it manually, this article provides detailed step-by-step instructions on how to perform the necessary operations.

The table below lists the audit settings that must be configured to ensure collecting comprehensive and reliable audit data:

<table>
<thead>
<tr>
<th>Setting</th>
<th>Required Configuration</th>
<th>Explanation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain audit policies</td>
<td>• The “Audit account management” policy must be set to “Success”.</td>
<td>To track changes to user accounts and groups. This policy logs password resets, newly created accounts, changes to group membership, etc.</td>
</tr>
<tr>
<td></td>
<td>• The “Audit directory service access” policy must be set to “Success”.</td>
<td>To track the same activity as “Audit account management” but at a much lower level. For example, it can help identify which attributes of a user account (or another AD object) were accessed.</td>
</tr>
<tr>
<td></td>
<td>• The “Audit logon events” policy must be set to “Success”. Note: Only required if you select to detect the originating workstation when configuring the product to audit the target AD domain. With this option, you will be able to receive the IP address and the MAC address of the computer from which a change was made in Reports and Change Summaries. For more details on this option, refer to the following Netwrix KB article: Additional Audit Details: How It Works.</td>
<td>To identify the workstation from which a change was made.</td>
</tr>
<tr>
<td>Security event log size and retention method</td>
<td>• The Data Processing Account used to collect data from the monitored domain must be assigned the “Manage auditing and security log” right.</td>
<td>To be able to read the Security event log on the domain controllers.</td>
</tr>
<tr>
<td></td>
<td>• The Security event log size must be set to 300MB on pre-Windows Server 2008 Windows versions, or to 1GB on Windows Server 2008 and above.</td>
<td>To allow for more events to be written into the log.</td>
</tr>
<tr>
<td></td>
<td>• The retention method of the security event log must be set to “Do not overwrite when full” to ensure that data is retained for long periods of time.</td>
<td>To allow for events to be retained for long periods of time.</td>
</tr>
<tr>
<td>Security event log must be set to “Overwrite events as needed” (Unless it is set to “Archive the log when full”). Alternatively, auto archiving must be enabled for the Security event log to prevent audit data loss if log overwrites occur.</td>
<td>written into the log even if it reaches its maximum size (new events will overwrite the oldest events in the log).</td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
</tr>
<tr>
<td>Object-level audit settings</td>
<td>• Object-level audit settings must be configured for the Domain, Configuration and Schema containers.</td>
<td></td>
</tr>
<tr>
<td>To report the “Who” and “When” fields for all changes.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exchange Server Administrator Audit Logging</td>
<td>• Exchange Server Administrator Audit Logging (AAL) setting must be configured for Exchange Server 2010 and 2013.</td>
<td></td>
</tr>
<tr>
<td>To report the “Who” field correctly for changes to AD objects made through the Exchange Server 2010 or 2013 interface.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
2. CONFIGURING DOMAIN AUDIT POLICIES

To configure the domain audit policies, perform the following procedure:

Procedure 1. To configure domain audit policy settings

1. Open the Group Policy Management console on any domain controller in the target domain: navigate to Start → Group Policy Management.

2. In the left pane, navigate to Forest: <domain_name> → Domains → <domain_name> → Domain Controllers. Right-click the effective domain controllers policy (by default, it is the Default Domain Controllers Policy), and select Edit from the popup menu.


4. Double-click the Audit account management and Audit directory service access policies and set them to Success:

   Figure 1: Group Policy Management Editor Dialog

   ![Group Policy Management Editor Dialog]

   **Note:** If you are going to enable the Originating Workstation option to collect the information on the computer from which a change was made, also set the Audit logon event policy to Success (or Success and Failure).

5. Open the command line interface: navigate to Start and type “cmd”.

6. Type the “gpupdate” command and press Enter. The group policy will be updated.
3. Configuring Security Event Log Size and Retention Settings

Defining the Security event log size is essential for change auditing. If your Security log size is insufficient, overwrites may occur before data is written to the Audit Archive and the SQL database, and some audit data may be lost. To prevent overwrites, you must increase the maximum size of the Security event log.

On Windows Server 2003 systems, where the maximum size of the Security event log cannot exceed 300 MB (according to the following Microsoft Knowledge Base article: Event log may not grow to configured size), it is also recommended to enable automatic backup of the event log. With this option, the event log will be archived and log overwrites will not occur on domain controllers.

To adjust your Security event log size and retention settings, perform the following procedures:

- Increase the maximum size of the Security event log and set its retention method
- Enable event log Auto archiving
- Configure backup logs retention

Procedure 2. To increase the maximum size of the Security event log and set its retention method

1. Open the Group Policy Management console on any domain controller in the target domain: navigate to Start → Group Policy Management.
2. In the left pane, navigate to Forest: <domain_name> → Domains → <domain_name> → Domain Controllers. Right-click the effective domain controllers policy (by default, it is the Default Domain Controllers Policy), and select Edit from the popup menu.

   Figure 2: Group Policy Management Editor Dialog

4. Double-click the Maximum security log size policy. In the Maximum security log size Properties dialog, select the Define this policy setting option and set maximum security log size to 299968 kilobytes on pre-Windows 2008 Windows versions, or to 1048576 kilobytes (1GB) on Windows Server 2008 and above:
Figure 3: Maximum security log size Properties Dialog

5. Click OK to save the changes.

6. Double-click the Retention method for security log policy. In the Retention method for security log Properties dialog, select the Define this policy setting option and select Overwrite events as needed:

Figure 4: Retention method for security log Properties Dialog

7. Click OK to save the changes.

8. Open the command line interface: navigate to Start and type “cmd”.

9. Type the “gpupdate” command and press Enter. The group policy will be updated.
Procedure 3. To enable Auto archiving centrally on all domain controllers

1. Open the Group Policy Management console on any domain controller in the target domain: navigate to Start → Group Policy Management.
2. In the left pane, navigate to Forest: <domain_name> → Domains → <domain_name> → Domain Controllers. Right-click the effective domain controllers policy (by default, it is the Default Domain Controllers Policy), and select Edit from the popup menu.
4. In the Policy Templates dialog, navigate to the Netwrix Auditor installation directory, open the AD Change Reporter Full Version folder and select the Log Autobackup.adm file (if the product is installed on a different computer, copy this file to the domain controller), and click Open.
5. Click the Close button in the Add/Remove Templates dialog.
   
   Note: If you are running Windows Server 2003 or below, after step 4, click View in the Main menu, select Filtering and deselect the Only show policy settings that can be fully managed option.

7. Double-click the Automatically clear a full security event log and back up the log file setting. Select the Enabled option and click OK to save the changes.
8. Open the command line interface: navigate to Start and type "cmd".
9. Type the “gpupdate” command and press Enter. The group policy will be updated.
   
   Note: Depending on the activity in the monitored environment, the Security log auto backup files can fill the free space on your disk drive before the product removes them. To prevent disk drive overfilling, if needed, change the behavior of the backup logs by performing Procedure 4 To configure the retention period for the backup logs below.

Procedure 4. To configure the retention period for the backup logs

1. On the computer where Netwrix Auditor is installed, open the registry editor: navigate to Start, type "regedit" and press Enter.
2. Navigate to HKEY_LOCAL_MACHINE → SOFTWARE → Netwrix → AD Change Reporter (for 32-bit OS), or HKEY_LOCAL_MACHINE → SOFTWARE → Wow6432Node → Netwrix → AD Change Reporter (for 64-bit OS).
3. Double-click CleanAutoBackupLogs. The Edit DWORD Value dialog will open.
4. This value defines the time period (in hours) after which archives will be deleted automatically. By default, it is set to 50 (decimal). Modify this value, if necessary, and click OK to save the changes.
Figure 5:   Edit DWORD Value Dialog

Note: If the CleanAutoBackupLogs registry value is set to 0, you will have to remove the old automatic backups manually, or you may run out of space on your hard drive.
4. **CONFIGURING OBJECT-LEVEL AUDITING**

Object-level Active Directory auditing must be configured so that the “Who” and “When” information appears in audit reports. If, in addition to the Domain partition, you also want to monitor changes to AD configuration and schema, you must enable object-level auditing for these partitions.

**Note:** Monitoring of the Configuration partition is enabled by default. For instructions on how to enable monitoring of changes to the Schema partition in the target AD domain, refer to *Netwrix Auditor: Active Directory Administrator’s Guide*.

Perform the following procedures to configure object-level auditing for the Domain, Configuration and Schema partitions:

- **To configure object-level auditing for the Domain partition**
- **To enable object-level auditing for the Configuration and Schema partitions**

**Procedure 5. To configure object-level auditing for the Domain partition**

1. Open the Active Directory Users and Computers console on any domain controller in the target domain: Navigate to **Start** and select **Active Directory Users and Computers**.

2. In the **Active Directory Users and Computers** dialog, click **View** in the main menu and ensure that the **Advanced Features** option is selected:

   ![Active Directory Users and Computers Dialog](image)

   *Figure 6: Active Directory Users and Computers Dialog*

3. Right-click the `<domain_name>` node and select **Properties**. In the domain **Properties** dialog, open the **Security** tab and click the **Advanced** button. The **Advanced Security Settings** dialog will open. Select the **Auditing** tab:
4. Do the following depending on the OS version:

   - On pre-Windows Server 2012 Windows versions:
     a. Press the Add button. In the Select user, Computer, Service account, or Group dialog, type ‘Everyone’ in the Enter the object name to select entry field and click OK.
     b. In the Audit Entry dialog that opens, set the Successful parameter for all access entries except the following: Full Control, List Contents, Read All Properties and Read Permissions:

![Figure 8: Auditing Entry Dialog](image)
c. Make sure that the **Apply these auditing entries to objects and/or containers within this container only** check-box is **not** selected. Also, make sure that the **Apply onto** parameter is set to “This object and all descendant objects”.

d. Click **OK** to save the changes.

- **On Windows Server 2012:**
  
a. Press the **Add** button. In the **Auditing Entry** dialog, click on the **Select a principal** link.

b. In the Select user, Computer, Service account, or Group dialog, type ‘Everyone’ in the Enter the object name to select entry field and click OK.

c. Select “Success” from the **Type** drop-down list, and “This object and all descendant objects” in the **Applies to** drop-down list.

d. Under Permissions, select all check-boxes except the following: Full Control, List Contents, Read All Properties and Read Permissions:

![Auditing Entry Dialog](image)

Figure 9: **Auditing Entry Dialog**

- Select “Success” from the **Type** drop-down list, and “This object and all descendant objects” in the **Applies to** drop-down list.

d. Under Permissions, select all check-boxes except the following: Full Control, List Contents, Read All Properties and Read Permissions:

- Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container** check-box is **not** selected.

   - Click **OK** to save the changes.

### Procedure 6. To enable object-level auditing for the Configuration and Schema partitions

**Note:** To perform this procedure, you will need the [ADSI Edit](#) utility. In Windows 2003 systems, this utility is a component of Windows Server Support Tools. If it has not been installed, download Windows Server Support Tools from the official
website. On Windows 2008 systems and above, this component is installed together with the AD DS role.

1. Navigate to Start → Programs → Administrative Tools → ADSI Edit. The ADSI Edit dialog will open.

   **Figure 10: ADSI Edit dialog**

   ![ADSI Edit dialog](image)

   2. Right-click the ADSI Edit node and select the Connect To option. In the Connection Settings dialog, enable the Select a well-known Naming Context option and select Configuration from the drop-down list. Click OK.

   **Figure 11: Connection Settings Dialog**

   ![Connection Settings Dialog](image)

   3. Expand the Configuration <Your_Root_Domain_Name> node. Right-click the CN=Configuration, DC=... node and select Properties.

   4. In the CN=Configuration, DC=company, DC=local Properties dialog select the Security tab and press the Advanced button. In the Advanced Security Settings for Configuration dialog open the Auditing tab.

   5. Do the following depending on the OS version:

      - On pre-Windows Server 2012 Windows versions:

        a. Press the Add button.
b. In the Select User, Computer, Service Account, or Group dialog type ‘Everyone’ in the Enter the object name to select entry field and click OK. The Auditing Entry for Configuration dialog will open.

c. Set the Successful parameter for all access entries except the following: Full Control, List Contents, Read All Properties and Read Permissions:

**Figure 12: Auditing Entry for Configuration Dialog**

![Auditing Entry for Configuration Dialog]

d. Make sure that the Apply these auditing entries to objects and/or containers within his container only check-box is not selected. Also, make sure that the Apply onto parameter is set to This object and all descendant objects.

e. Click OK to save the changes.

- **On Windows Server 2012:**

  a. Press the Add button. In the Auditing Entry dialog, click on the Select a principal link.

  b. In the Select user, Computer, Service account, or Group dialog, type ‘Everyone’ in the Enter the object name to select entry field and click OK.

  c. Select “Success” from the Type drop-down list, and “This object and all descendant objects” in the Applies to drop-down list.

  d. Under Permissions, select all check-boxes except the following: Full Control, List Contents, Read All Properties and Read Permissions:
Figure 13: Auditing Entry Dialog

- Scroll to the bottom of the list and make sure that the **Only apply these auditing settings to objects and/or containers within this container check-box is not selected.**

- Click **OK** to save the changes.

6. **Repeat steps 2-5 for the Schema container if necessary.**
5. CONFIGURING EXCHANGE SERVER AAL SETTINGS

If the target AD domain has an Exchange organization running Microsoft Exchange Server 2010 or 2013, you must configure the Exchange server Administrator Audit Logging (AAL) settings. To do this, perform the following procedure on any of the monitored Exchange servers (these settings will then be replicated to all Exchange servers in the domain):

Procedure 7. To configure Exchange Server AAL settings

1. On the computer where the target Microsoft Exchange Server 2010 or 2013 is installed, navigate to Start → Programs → Exchange Management Shell.
2. Execute the following command depending on your Exchange Server version:
   - Exchange Server 2010:
     ```powershell
     [PS] C:\Windows\system32>Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets *
     ```
   - Exchange Server 2013:
     ```powershell
     [PS] C:\Windows\system32>Set-AdminAuditLogConfig -AdminAuditLogEnabled $true -AdminAuditLogAgeLimit 30 -AdminAuditLogCmdlets * -LogLevel Verbose
     ```
3. On the computer where Netwrix Auditor is installed, browse to the Netwrix Active Directory Change Reporter folder, locate the SetAALExcludedCmdlets.ps1 file and copy it to the Exchange server.
4. In Exchange Management Shell, in the command line, execute this file by specifying the path to it:
   ```powershell
   <Path_To_SetAALExcludedCmdlets_File>\SetAALExcludedCmdlets.ps1
   ```
   This file contains a list of cmdlets that must be excluded from Exchange Server logging to reduce server load.