

Lab Report

Your Performance



Your Score: 0 of 9 (0%)

Elapsed Time: 6 minutes 38 seconds

Pass Status: Not Passed

Required Score: 100%

Task Summary**✖ Enable Audit Policies** [Hide Details](#)

-  Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings:--Enabled
-  Audit: Shut down system immediately if unable to log security audits--Enabled





✖ Enable Event Log Policy [Hide Details](#)

-  Retention method for security log: Enabled--do not overwrite events (clear log manually)

✖ Enable Account Logon Audit Policy [Hide Details](#)

-  Audit Credential Validation: Success and Failure



✖ Enable Account Management Audit Policies [Hide Details](#)

-  Audit User Account Management: Success and Failure
-  Audit Security Group Management: Success and Failure
-  Audit Other Account Management Events: Success and Failure
-  Audit Computer Account Management: Success



✖ Enable Detailed Tracking Audit Policy [Hide Details](#)

-  Audit Process Creation: Success

✖ Enable Logon-Logoff Audit Policies [Hide Details](#)

-  Audit Logon: Success and Failure
-  Audit Logoff: Success





✖ Enable Policy Change Audit Policies [Hide Details](#)

-  Audit Authentication Policy Change: Success
-  Audit Audit Policy Change: Success and Failure

✖ Enable Privilege Use Audit Policy [Hide Details](#)

-  Audit Sensitive Privilege Use: Success and Failure

✖ Enable System Audit Policies [Hide Details](#)

-  Audit System Integrity: Success and Failure
-  Audit Security System Extension: Success and Failure
-  Audit Security State Change: Success and Failure
-  Audit IPsec Driver: Success and Failure

Explanation

In this lab, you configure the following audit policy settings in WorkstationGPO as follows:

Local Policies	Setting
Audit: Force audit policy subcategory settings (Windows Vista or later) to override audit policy category settings	Enabled
Audit: Shut down system immediately if unable to log security audits	Enabled

Event Log	Setting
Retention method for security log	Enabled: Do not overwrite events (clear log manually)

Advanced Audit Policy Configuration	Setting
Account Logon: Audit Credential Validation	Success and Failure
Account Management: Audit User Account Management	Success and Failure
Account Management: Audit Security Group Management	Success and Failure
Account Management: Audit Other Account Management Events	Success and Failure
Account Management: Audit Computer Account Management	Success
Detailed Tracking: Audit Process Creation	Success
Logon/Logoff: Audit Logon	Success and Failure
Logon/Logoff: Audit Logoff	Success
Policy Change: Audit Authentication Policy Change	Success
Policy Change: Audit Audit Policy Change	Success and Failure
Privilege Use: Audit Sensitive Privilege Use	Success and Failure
System: Audit System Integrity	Success and Failure
System: Audit Security System Extension	Success and Failure
System: Audit Security State Change	Success and Failure
System: Audit IPsec Driver	Success and Failure

Edit audit policies as follows:

1. From Server Manager, select **Tools > Group Policy Management**.
2. Expand Forest: **CorpNet.com > Domains > CorpNet.com > Group Policy Objects**.
3. Right-click **WorkstationGPO** and select **Edit**.
4. Under Computer Configuration, expand **Policies > Windows Settings > Security Settings**.
5. Modify Local Policies as follows:
 - a. Expand **Local Policies**.
 - b. Select **Security Options**.
 - c. In the right pane, double-click the **policy** you want to edit.
 - d. Select **Define this policy setting**.
 - e. Select the **policy settings** as required.
 - f. Click **OK**.
 - g. Click **Yes** to confirm changes as necessary.
 - h. Repeat steps 5c–5g for additional policy settings.

6. Modify the event log as follows:
 - a. In the left pane, select **Event Log**.
 - b. In the right pane, double-click the *policy* you want to edit.
 - c. Select **Define this policy setting**.
 - d. Select the *policy settings* as required.
 - e. Click **OK**.
7. Modify Advanced Audit Policy Configuration as follows:
 - a. In the left pane, expand **Advanced Audit Policy Configuration > Audit Policies**.
 - b. Select the **audit policy** category.
 - c. In the right pane, double-click the *policy* you want to edit.
 - d. Select **Configure the following audit events**.
 - e. Select the *policy settings* as required.
 - f. Click **OK**.
 - g. Repeat steps 7b–7f for additional policy settings.