

Lab Report

Your Performance

Your Score: 0 of 9 (0%)

Pass Status: Not Passed

Elapsed Time: 5 minutes 7 seconds

Required Score: 100%

Task Summary

Required Actions

- 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

- Enable Account Logon Audit Policy

- 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

- 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 Privelege Use Audit Policy

- 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

While completing this lab, use the following Workstation GPO settings:

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	Define: 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. Using Group Policy Management, access CorpNet.local's **Group Policy Objects > WorkgroupGPO**.
 - a. From Server Manager's menu bar, select **Tools > Group Policy Management**.
 - b. Expand **Forest: CorpNet.local > Domains > CorpNet.local > Group Policy Objects**.
 - c. Maximize the windows for better viewing.
2. Access the WorkstationGPO's Security Settings Local Policies.
 - a. Right-click **WorkstationGPO** and select **Edit**.
 - b. Maximize the windows for better viewing.
 - c. Under Computer Configuration, expand **Policies > Windows Settings > Security Settings > Local Policies**.
3. Modify Local Policies.
 - a. Select **Security Options**.
 - b. From 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. Select **OK**.
 - f. Select **Yes** to confirm changes as necessary.
 - g. Repeat steps 3b - 3f for additional policy settings.
4. Modify the Event Log.
 - a. From the left pane, select **Event Log**.
 - b. From 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. Select **OK**.
5. Modify Advanced Audit Policy Configuration.
- a. From the left pane, expand **Advanced Audit Policy Configuration > Audit Policies**.
 - b. Select the audit policy category.
 - c. From 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. Select **OK**.
 - g. Repeat steps 5b–5f for additional policy settings.