

Lab Report

Your Performance

Your Score: 0 of 9 (0%)
Elapsed Time: 5 minutes 7 seconds

Pass Status: Not Passed
Required Score: 100%

Task Summary

Required Actions

✖ Enable Audit PoliciesHide 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 PoliciesHide 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 PoliciesHide Details

Audit Logon: Success and Failure

Audit Logoff: Success

✖ Enable Policy Change Audit PoliciesHide Details

Audit Authentication Policy Change: Success

Audit Audit Policy Change: Success and Failure

- ✖ Enable Privelege Use Audit Policy
- ✖ Enable System Audit PoliciesHide 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 WorkstationGPO 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 | <i>Define: Do not overwrite events (clear log manually)</i> |

| 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:

- Using Group Policy Management, access CorpNet.local's **Group Policy Objects > WorkgroupGPO**.
 - From Server Manager's menu bar, select **Tools > Group Policy Management**.
 - Expand **Forest: CorpNet.local > Domains > CorpNet.local > Group Policy Objects**.
 - Maximize the windows for better viewing.
- Access the WorkstationGPO's Security Settings Local Policies.
 - Right-click **WorkstationGPO** and select **Edit**.
 - Maximize the windows for better viewing.
 - Under Computer Configuration, expand **Policies > Windows Settings > Security Settings > Local Policies**.
- Modify Local Policies.
 - Select **Security Options**.
 - From the right pane, double-click the *policy* you want to edit.
 - Select **Define this policy setting**.
 - Select the *policy settings* as required.
 - Select **OK**.
 - Select **Yes** to confirm changes as necessary.
 - Repeat steps 3b - 3f for additional policy settings.
- Modify the Event Log.
 - From the left pane, select **Event Log**.
 - From the right pane, double-click the *policy* you want to edit.
 - 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.