Lab Report

Your Performance

Your Score: 0 of 2 (0%) Pass Status: Not Passed

Elapsed Time: 5 minutes 20 seconds Required Score: 100%

Task Summary

✖ Enable auditing for logon events in the GPO Hide Details

⊖ Audit for successful events
⊖ Audit for failed events

✖ Configure additional GPO settings Hide Details

⊖ Shut down the system if the Event Log is full
⊖ Do not overwrite events in the Security log

Explanation

In this lab, you complete the following:

- In the audit policy of the GPO, enable the **Audit logon events** policy. This records logon to the local computer and an event in the workstation's security log.

  > Auditing for account logon tracks logon to a user account and records the event on the domain controller used for authentication.

- In the Audit logon events policy, enable both **Success** and **Failure**. In this scenario, you want to know when someone is able to log on and when logon is denied.
- In Security Options, enable the **Audit: Shut down system immediately if unable to log security audits** policy, which causes the computer to shut down if it can't log audit entries.
- In Event Log, enable the **Retention method for security log** policy and configure it to **Do not overwrite events (clear log manually)**.

Following are steps that an expert might take to perform the tasks in this lab:

1. From Hyper-V Manager, select **CORPSERVER**.
2. Right-click **CorpDC** and select **Connect**.
3. From Server Manager, select **Tools > Group Policy Management**.
4. Expand **Forest: CorpNet.com > Domains > CorpNet.com > Group Policy Objects**.
5. Right-click **AccountingGPO** and select **Edit**.
6. Under Computer Configuration, expand **Policies > Windows Settings > Security Settings > Local Policies**.
7. Select **Audit Policy**.
8. Right-click the **policy** you want to edit and select **Properties**.
9. Select **Define this policy setting**.
10. Make sure **Success** is selected.
11. Select **Failure**.
12. Click **OK**.
13. Edit Security Option policies as follows:
    1. Select **Security Options**.
    2. Right-click the ***policy*** and select **Properties**.
    3. Select **Define this policy setting**.
    4. Select **Enable**.
    5. Click **OK**.

6. Click **Yes** to confirm the setting change.

14. Edit Event Log policies as follows:
    1. Select **Event Log**.
    2. Right-click the ***policy*** and select **Properties**.
    3. Select **Define this policy setting**.
    4. Select **Do not overwrite events (clear log manually)**.
    5. Click **OK**.