10.2 Solutions and Guided Walkthrough

Walkthrough

In order to complete the challenges in this laboratory exercise, see the steps in this walkthrough.

1. Navigate to `Start Menu` → `Control Panel` → `System` → `Computer Name, Domain, and Workgroup Settings` → `Change Settings` and then click Change to rename the computer.

2. Navigate to `Start Menu` → `Control Panel` → `Network and Sharing Center` → `Change Adapter Settings` → `Right-Click on the Local Area Connection and select Properties` → `Select Internet Protocol Version 4` → `Select Properties`. From here, configure the desired IP address settings.

3. Follow the steps in Step 2 and configure the desired DNS settings.

4. Navigate to `Start Menu` → `Control Panel` → `Date and Time` → `Change Time Zone`. From here, select the desired time zone settings.

5. In the Server Manager, right click on `Roles` and select `Add Roles`. Follow the steps in the wizard and select `Active Directory Domain Services` as the role to install.

6. During the Active Directory installation process, you should be asked to `Create a New Domain`. Select `Domain in a New Forest` and then click Next. Enter the name of the new domain.

7. During the Active Directory installation process, you should configure the Forest functional level to the desired setting when prompted.

8. During the Active Directory installation process, you should configure the Domain functional level to the desired setting when prompted.

9. During the Active Directory installation process, you should configure the Windows Server as a Global Catalog Server by checking the box next to Global Catalog Server. It may already be checked by default.

10. During the Active Directory installation process, you should configure the Windows Server as a DNS Server by checking the box next to DNS Server. This box is typically not checked by default, ensure this is checked.

11. In the Server Manager, expand the `Roles` tab. Expand the `DNS Server` tab. Expand the `DNS` tab. Then right-click the name of your server and select properties. Select the `Forwarders` tab. Click `Edit` and add the desired Forwarder IP address.

12. In the `Forwarders` tab mentioned in Step 11, uncheck the box labeled `Use root hints if no forwarders are available`.

13. In the Server Manager, expand the `Roles` tab. Expand the `Active Directory Domain Services` tab. Expand the `Active Directory Users and Computers` tab. Then right-click the name of your domain and select New. Select Organizational Unit. Configure the names as desired.

14. Follow the directions in Step 13 to navigate to your domain. Next, expand your domain, you should see the Organizational Units which were created in Step 13. Right-click on the Organizational Unit and select New. Next, select User. Follow the specifications to create the users appropriately.

15. Follow the directions in Step 14 to navigate to your Organizational Units. Right-click on the Organizational Unit and select New. Next, select Group. Name the group according to the specification. Ensure that the `Group Scope` and `Group Type` are configured according to the specification as well.

16. Follow the directions in Step 14 to navigate to your Organizational Units. Next select all of the users which need to be added to the Security Group. When all are selected, right-click on one of them and select `Add to Group`. Type in the name of the group.

17. Follow the directions in Step 14 to navigate to your Organizational Units. Next, right-click the Organizational Unit and select New. Next, select Shared Folder. Configure the name and network path according to the specification.

18. In the Server Manager, expand the `Roles` tab. Expand the `Active Directory Domain Services` tab. Expand the `Active Directory Sites and Services` tab. Right-click the `Sites` tab. Select New and then select `Site`. To add the server to the site, right-click the site and select New. Next, select Server. Enter the name of your server.

19. In the Server Manager, expand the `Features` tab. Expand the `Forest` tab. Expand the `Domains` tab. Expand the tab with your domain name. Right-click the `Domain Controllers` tab. Select `Create a GPO in this domain, and Link it here`.

    - Name the GPO according to the specification when prompted. *If not immediately brought to the Group Policy Management Editor, go back to the Domain Controllers tab and right-click on the name of your new GPO and select Edit.*
    - In the Group Policy Management Editor, navigate to `User Configuration` → `Policies` → `Windows Settings` → `Folder Redirection` and configure according to the specification.
    - In the Group Policy Management Editor, navigate to `User Configuration` → `Policies` → `Administrative Templates` → `Start Menu and Taskbar` and then find the setting titled **Remove Run menu from Start Menu**. Enable that setting.
    - In the Group Policy Management Editor, navigate to `User Configuration` → `Policies` → `Administrative Templates` → `Control Panel` and find the setting titled **Always Open all Control Panel Items when Opening Control Panel**. Enable that setting.
    - In the Group Policy Management Editor, navigate to `User Configuration` → `Policies` → `Administrative Templates` → `System` and then find setting titled **Prevent Access to Registry Editing Tools**. Enable that setting.
    - In the Group Policy Management Editor, navigate to `User Configuration` →

`Policies` → `Administrative Templates` → `System` and then find setting titled **Prevent Access to the command prompt**. Enable that setting.

- In the Group Policy Management Editor, navigate to `User Configuration` → `Policies` → `Administrative Templates` → `System` → `Locale Services` and then find setting titled **Disallow User Override of Locale Settings**. Enable that setting.
- In the Group Policy Management Editor, navigate to `User Configuration` → `Policies` → `Administrative Templates` → `System` → `Ctrl + Alt + Del Options` and then find setting titled **Remove Task Manager**. Enable that setting.

20. From the Server Manager, follow these steps:

    - Right-click on the `Roles` tab. Select `Add Roles`. Navigate through the Wizard. Ensure that `File Services` is selected to be installed.
    - Navigate to `Roles` → `File Services` → `Share and Storage Management` → `File Server Resource Manager` → `Classification Management`. Right-click on `Classification Properties` and select `Create Property`. Give the property a name and set the type as Yes/No. Next, right-click `Classification Rules` and select `Create a New Rule`. Name the rule and select the scope to which it should apply (which folders it should be applied to) based on the specification. Then select the `Classification` tab. Set the `Classification Mechanism` to `Content Classifier`. Set the `Property Name` to the name of the property you created earlier in this step. Set the property value accordingly. Next, select Advanced. Click on the `Additional Classification Parameters` tab. Set the Name field to **String** and set the value according to the specification.
    - Run the rule by right-clicking the `Classification Rules` tab and selecting `Run Classification with all Rules Now`.

21. To create a File Screen, follow these steps:

    - Navigate to `Roles` → `Services` → `Share and Storage Management` →

`File Server Resource Manager` → `File Screening Management` and right-click on `File Screens`.

- Select `Create File Screen`.
- Specify the path to the directory on which the screen should apply.
- Either use an existing file screen or create a custom screen.

22. To remove a browser on Windows Server, open the **Control Panel**. From there, navigate to Programs → Programs and Features → Uninstall or Change a Program. From here uninstall any browsers installed on the machine.

23. Apply Principles of Least Privilege

    Check your users and user groups to determine if there are users with unnecessary privileges. You can check this in the Server Manager. Navigate to **Roles** → **Active Directory Domain Services** → **Active Directory Users and Computers** → *Domain Name* → **Users**. Here, click the **Type** button in the top bar to sort by type, this will make it easier to see users vs groups. Ensure that the Guest account is disabled, this account is usually unprotected and unnecessary but provides an attack vector. Next, look through the remaining users, determine if they are necessary, if not, disable the account. Next, check the various security group and see what members are in them. To do this, right click the desired group, select **Properties**, then click on the **Members** tab. Ensure that a user is only in the group if necessary. One concept of least privilege is to only grant access as needed. Some individuals within an organization may need to perform domain services on occasion. Rather than leave that user account in an administrators group, only add them when necessary, and remove after. This ensures that accounts are not being compromised and used to perform privileged actions.

24. Hardening the Administrator Accounts

    Task 1: Require that administrator accounts need a smart card for logon.

    Task 2: Mark the administrator account as sensitive and cannot be delegated.

    For each of these tasks, access a user's properties by navigating to **Roles** → **Active**

Directory Domain Services → **Active Directory Users and Computers** → *Domain Name* → **Users** within the Server Manager. From here, right click on the desired user and select **Properties**. In the **Account** tab, there will be a sections titled **Account Options**. Scroll through the options and select the desired security features. *Note: In order to require the smart card login, your organization will need to have a public key infrastructure in place.*