Lab 4
Web server and File Services

EXERCISE 1: INSTALL WEB SERVER

In this lab, you are requested to accomplish the following tasks:

1. Installing the Web Server
2. Verifying that Web server is working
3. Launching your first website
4. Configure Web server to run on HTTPS
5. Configure Web server to host multi-sites (at least 3 sites):
    a. Using different ports
    b. Using different IP addresses
    c. Using Host Headers

EXERCISE 2: INSTALL FTP SERVER

1. Install the FTP Server
2. Testing that we can upload and download file from FTP Server (using Mozilla or FTP client)
3. Configuring FTP server to use SSL
4. Verifying that we can upload and download file from FTP Server with SSL

EXERCISE 3: SHARING A FOLDER

In this exercise, you create a folder share using the File Explorer interface.

1. Logon to the FILE 1 computer using the domain administrator account
2. Open File Explorer and create a folder; Creating some files in this folder
3. Right-click on created folder and from context menu, select Properties
4. Click Sharing tab and then click Advanced Sharing
5. Select the Share This Folder check box
6. Click Permission. Clear all check boxes in the Allow column.
7. Click Add to select Domain users group and assign it the Allow Read permission only
8. Close all dialog boxes

9. Access to the shared folder from other computers with a domain user accounts. Try to copy file between this folder and folder of local computer => taking the screen shoots
10. Edit shared permissions for this folder, e.g., allowing Domain users group has Full Control permission
11. Repeat the step 9

EXERCISE 4: CREATING SHARES WITH SERVER MANAGER

In this exercise, you create shares directly within the Server Manager console.

1. Add the File Server role
2. Share a folder:
    a. Server Manager -> File and Storage Services -> Shares
    b. In the Shares tile, click Tasks > New Share
    c. Select SMB Share – Quick
    d. Select Folder and specify permission
3. Test the new share

EXERCISE 5: ENABLING DISTRIBUTED FILE SYSTEM AND CREATING A NAMESPACE

In this exercise, you are required to create a basic DFS environment with a single Namespace to allow access to different file server without having to specify the name of file servers

Configure the file server (e.g., SVR-MBR-B) for DFS:

1. Add DFS Namespaces and **DFS Replication** roles
2. Launch DFS Management (Server Manager -> Tools -> DFS Management)
3. Create a Namespace:
    a) Right-click on Namespaces and choose New Namespace….
    b) Enter the name of the server that is going to be your Namespace server: e.g., FILE1.
    c) Next, input a name for this new Namespace: e.g., IT-K44
    d) Select the local path for the shared folder and choose the appropriate permission
4. Create a folder inside this Namespace:

a) Right-click on the new Namespace and choose **New Folder…**:
b) Input a name for new folder in the Name field; this is the name that will be displayed inside the DFS Namespace when users access it.
c) Then click the Add… button to specify a share that this new folder is going to link to. E.g, \\FILE1\TestShareFolder

Test the namespace

Log in to a client computer and try browsing to \\Domain\namespace\shared folder, e.g., \\clc.com\IT-K44\TestShareFolder

EXERCISE 6: CONFIGURING DISTRIBUTED FILE SYSTEM REPLICATION

DFS enables automatic file replication between multiple servers. In exercise 5, we created a DFS Namespace with a folder inside to allow accessing to the files and folders all sitting on a single file server. In this exercise, you will set up DFSR between the two file servers in our environment to make sure that data is being synchronized between the two.

1. Launch DFS Management Console (Server Manager -> Tools -> DFS Management).
2. Right-click on Replication and choose New Replication Group…
3. For the following step:
    a. Choose **Multipurpose** replication group;
    b. Enter a name for your new replication group.
    c. Add file servers for the Replication Group members
    d. Choose the **Primary member**
    e. Add all folders that you want to replicate
    f. specify the local path for the folders to exist on the other member servers
4. Test DFS replication

- From a client computer, open up File Explorer and navigate to \\Domain\namespace\<DFS replication folder>, e.g., \\clc.com\IT-K44\TestRep
- Create a few test files in this folder
- Give it a little bit of time for replication to happen, then check inside the local replication folder on each file server. You should see that there are copies of your new files now located on both servers' hard drives!

EXERCISE 7: CREATING AN ISCSI TARGET ON YOUR SERVER

We utilized iSCSI to create an **iSCSI target** on the main storage server, and then connected to that block of storage with an **iSCSI initiator** on the application server where we were installing the software.

1. Add **iSCSI Target Server** role to FILE1 server
2. Add a New Virtual Disk:
    a. Server Manager -> File and Storage Services -> iSCSI.
    b. Tasks New iSCSI Virtual Disk….
    c. Choose a location for this iSCSI target to reside, e.g., D:
    d. Specify a name for iSCSI virtual disk (it is going to create and utilize a VHDX file for this storage).
    e. Specify the iSCSI Virtual Disk Size
    f. Create a name for the iSCSI target. This is the name that will use on the iSCSI initiator server later in order to connect to the storage, e.g., Database1.
    g. Now on the **Access Servers** screen, click the Add… button in order to specify which initiators will later connect to this target.

EXERCISE 8: CONFIGURING AN ISCSI INITIATOR CONNECTION

The device connecting to an iSCSI target is called an iSCSI initiator. In this exercise, we are going to take a file server in our environment and configure it to connect over the network using iSCSI to our iSCSI target server. When finished, we will have a new hard disk attached to our file server, even though it is really just block storage from the iSCSI target that is being accessed via the network.

1. Server Manager -> Tools -> iSCSI Initiator.
2. On Discovery tab and click on the Discover Portal… button
3. Type in the name of the server where you have an iSCSI target running and click OK.
4. Move back over to the Targets tab of the iSCSI Initiator Properties
5. iSCSI connection is now shown on the Targets tab by its IQN number. Currently, the status is set to Inactive. Select this connection and click on the Connect button

EXERCISE 7: SETTING UP WINDOWS SERVER 2019 WORK FOLDERS

Work Folders is a way to publish access to files and folders to multiple device types that the users may be logging in to. These files are accessed via a web listener that is configured on the Work Folders file server, which enables this data to be

accessed from inside or outside the corporate network, from both domain-joined and non-domain-joined systems. To fully configure Work Folders, you will also need the ability to acquire a valid SSL certificate and access to your public DNS environment in order to create a record.

Create Work Folders server

1. Add **Work Folders** role
2. Server Manager -> File and Storage Services -> Work Folders.
3. TASKS -> New Sync Share…
4. Choose or enter a path where you want the new Work Folders to be stored. This is the location on our file server that will be populated by folders that are named after our users. If you have already set up a folder and shared it, you will see it in the list to choose from.
5. Define which users and groups have access to use this sync

Connect to Work Folder

Client devices will connect to Work Folders on this file server via HTTPS. In order to make that happen successfully, we need to configure a DNS record that points at this file server, and an SSL certificate to be bound to the web listener on the server. In this exercise, we configure client to connect to Work Folder server using HTTP (not recommand).

1. Open command prompt with Administrator Privileges and type the following command:
   Reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\
   WorkFolders /v AllowUnsecureConnection /t REG_DWORD /d 1
2. Go to **Control Panel** and click on **Work Folders** and then click **Setup Work Folders**
3. Click on Enter a Work Folders URL instead and input the URL of Work Folder server.
4. Select the location where you want the **Work Folder** to be located on client machine

Challenge:

- Configuring Work Folders to use HTTPS
- Configuring clients automatically using Group Policy.