

# COMPANY RELOCATION PROJECT TASK

## BACKGROUND:

*A company is moving from its current location to a new office. As a system administrator your job is to ensure that the move to the new premises is as smooth and trouble free as possible. At the current location every staff logs onto their computers with a local username and password. They also use WI-FI to access the internet. However, at the new location, they must work in a formal manner. The requirements are as follows:*

---

## SCOPE/SPECIFICATION:

1. Each user must log on to their system using a centrally controlled password.
2. Each user must have access to a shared folder for their department.
3. Department heads must have a shared folder for reports.
4. Each user should have a private folder where they store their own work.
5. All activity in the folders must be logged, including file upload, file deletion, file modification, file transfers, folder creation, folder deletion, folder transfer.
6. Users should be able to see the modification history of every file and be able to revert a file back to its previous history.
7. Each computer belonging to a department must have a unique IP address, and the address should identify which department the machine belongs to.
8. The central servers must also have unique addresses that can be used to identify them as central servers.
9. There are also servers hosting a website and an application used by the clients of the company. These machines must also have unique addresses that identify them as client facing servers.
10. There are four departments in total: Marketing, Accounting, Technology and Operations. There are 5 computers and one printer in each department.

## DELIVERABLES:

Your design must state the following:

- **1<sup>ST</sup>:** The software product or software products (including version numbers) used to achieve the design.
- **2<sup>ND</sup>:** The actual steps required to setup and configure the software to bring it to a usable state.
- **3<sup>RD</sup>:** A diagram showing the complete computer network, including all the required network equipment and IP addresses.

Bonus points:

- **4<sup>TH</sup>:** Include in your design multi-factor authentication to the computer using the Microsoft Authenticator or the Google Authenticator Mobile Apps.
- **5<sup>TH</sup>:** Include a plan for migrating the current local users onto the new system in the shortest possible time

---

## IMPLEMENTATION PROCEDURE

### Current location scenario description

*NB: When staff use local username and password to login into their PCs, it implies that, no domain is in place at the current site, instead, they communicated using WORKGROUP. Per the new requirements, a DOMAIN creation will be appropriate.*

# **1<sup>ST</sup> DELIBERABLE ITEM: SOFTWARE REQUIREMENTS**

## **High level overview of New location implementation process**

1. For each USER to login into their systems from a centrally controlled department, an **ACTIVE DIRECTORY DOMAIN CONTROLLER (AD DC)** role from (Windows server 2008/2012/2016) is suitable. For the purpose of this work, windows **server 2012R2** will be in focus.
2. Access to a shared folder, departmental heads shared folders and activities monitoring requires **FILE & STORAGE SERVICE** role to be configured in the central server (windows server 2012R2)
3. The identification of department based on IP can be achieved by assigning dedicated VLANS and a subnet to each department. Having been told that, there are currently 5 users and a printer in each department part from the servers, the designed implemented resorted to 14-usable hosts subnetting which leaves enough room for departmental up-scaling and at the same time conserve Ips as necessary. The servers are also given a dedicated subnet.
4. The servers (**Central, Application and WEB**) having unique addresses can be achieved by issuing STATIC IP configuration for them.
5. For the multi-factor authentication requirements, we shall make use of “**ManageEngine’s AD Self Service Plus product**”.

## **VLAN & IP Subnet/Space creation**

| S/No | DEPT        | VLAN/SUBNET      | DEFAULT<br>GATEWAY | DHCP HOST IP ALLOCATION<br>RANGE | PRINTER IP<br>(LAST USABLE IP)<br>STATICALLY ASSIGNED |
|------|-------------|------------------|--------------------|----------------------------------|---|
| 1.   | SERVER FARM | 192.168.10.0/28  | 192.168.10.1       | STATICALLY ASSIGNED              | -   |
| 2.   | TECHNOLOGY  | 192.168.10.16/28 | 192.168.10.17      | 192.168.10.18 - 192.168.10.29    | 192.168.10.30   |
| 3.   | ACCOUNTING  | 192.168.10.32/28 | 192.168.10.33      | 192.168.10.34 - 192.168.10.45    | 192.168.10.46   |
| 4.   | MARKETING   | 192.168.10.48/28 | 192.168.10.49      | 192.168.10.50 - 192.168.10.61    | 192.168.10.62   |
| 5.   | OPERATIONS  | 192.168.10.64/28 | 192.168.10.65      | 192.168.10.66 - 192.168.10.77    | 192.168.10.78   |

### 3<sup>rd</sup> DELIVERABLE ITEM: COMPUTER NETWORK TOPOLOGY

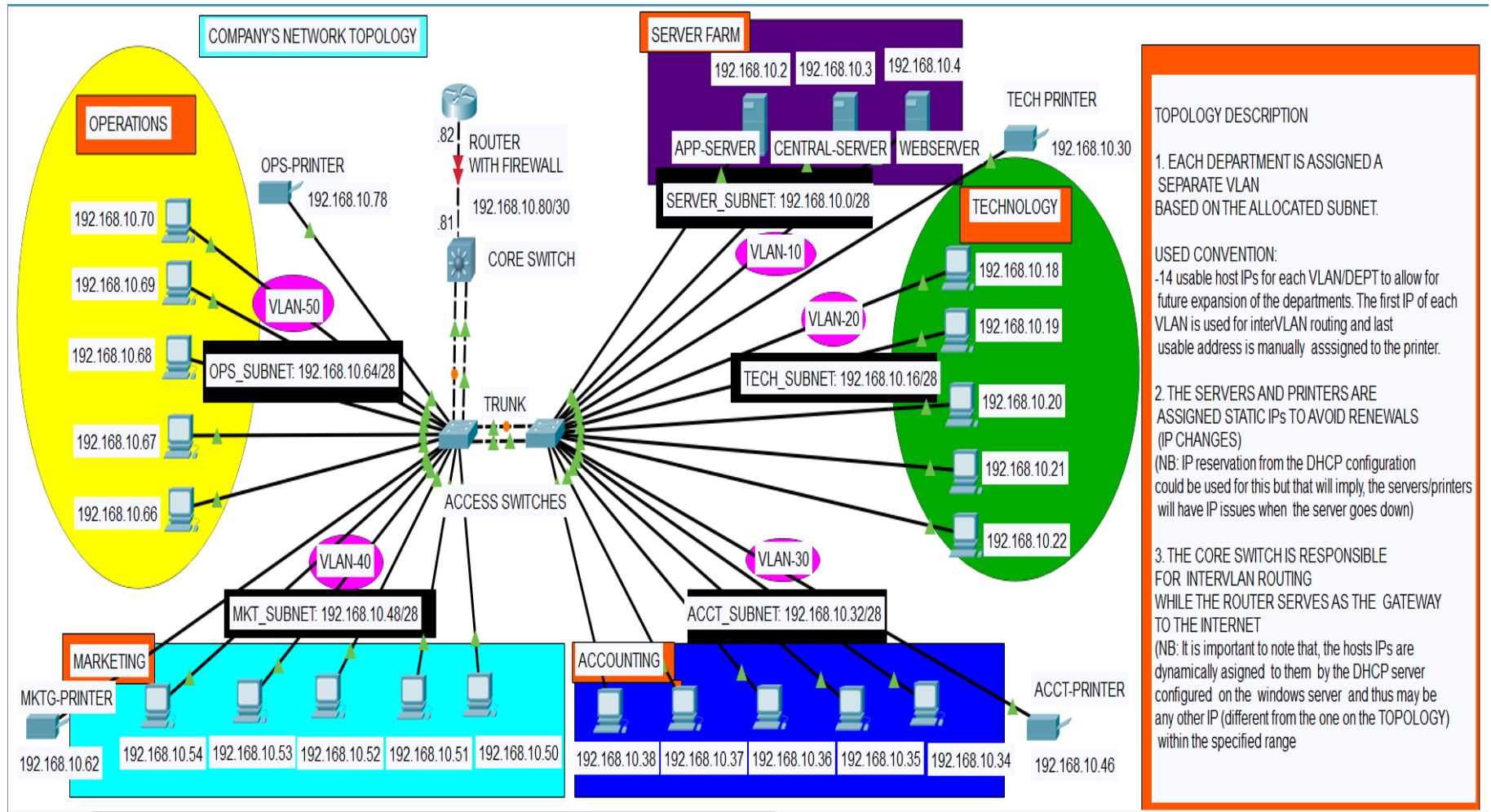


Figure 1.0 NETWORK TOPOLOGY

## **2<sup>ND</sup> DELIVERABLE ITEM: STEPS FOR REQUIREMENTS**

### **ACTUALIZATION**

#### **(1) Windows Server 2012R2 installation and configuration**

With regards to the central server, any of the windows server version (2008/2008R2, 2012/2012R2 and 2016) will be fine but for this task, focus is on server **2012R2**. After installing the windows Server OS, the computer will request to reboot and thereafter present the Initial Configuration Tasks Wizard. This wizard guides one through the most important initial tasks for configuring the new server.

#### **IMPORTANT NOTES DURING SERVER INSTALLATION**

- **Set the Administrator Password:** The very first thing one should do after installing Windows is set a secure administrator password.
- **Set the Time Zone:** This is necessary only if the indicated time zone is incorrect.
- **Configure Networking:** The default network settings are usually appropriate.
- **Provide Computer Name and Domain:** This option lets one change the server's computer name and join a domain.
- **Enable Automatic Updating:** Use this option if you want to let the server automatically check for operating system updates.
- **Download and Install Updates:** Use this option to check for critical operating system updates.
- **Add Roles:** This option launches the Add Roles Wizard, which lets ONE configure important roles for your server.
- **Add Features:** This option lets one add more operating system features.

- **Enable Remote Desktop:** We use this option to enable the Remote Desktop feature, which lets one administer this server from another computer.
- **Configure Windows Firewall:** Used to configure the built-in Windows firewall

## **(2) Active directory setup procedures to be used for this task**

### **PHASE I: Role & Feature installation**

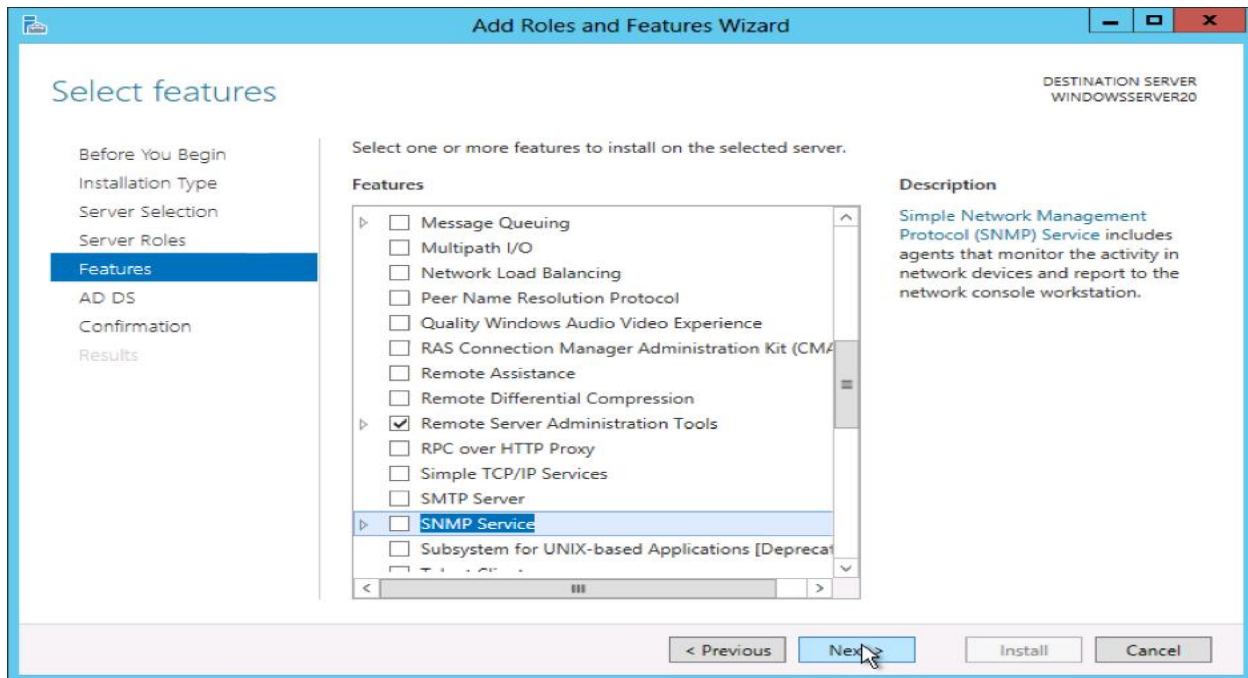
1. Open the **Server Manager** from the START menu on task bar OR search with the search pane.
2. From the **Server Manager** dashboard, select **Add roles and features**.  
The Roles and Features Wizard launches. This wizard enables one to make modifications to the Windows Server 2012R2 instance.

On the **Installation Type** screen, select **Role-based or features-based** and click **Next**.

3. By default, the current server is selected (server 2012R2). Click **Next**.
4. On the **Server Roles** screen, select the check box next to **Active Directory Domain Services**.  
A notice displays that explains that one must also install additional roles, services, or features in order to install Domain Services. These additional capabilities include certificate services, federation services, lightweight directory services, and rights management.

To select additional capabilities, click **Add Features**): *(the default selections are good to go with in our case)*.

5. On the Select features screen, select the check boxes next to the features that you want to install during the AD DS installation process and click Next.



6. Review the information on the **AD DS** tab, then click **Next**.
7. Review the information on the **Confirm installation selections** screen, then click **Install**.

## PHASE II: Start the remote registry service

Before one can promote the server to domain controller, one must start the remote registry service by using the following steps:

1. Click **Start > Control Panel**.
2. Under **Services**, right-click **Remote Registry** and open the **Properties** menu.
3. From the **Startup type:** drop-down menu, select **Automatic**.
4. Under **Service Status**, select **Start**.

The remote registry service starts.

## PHASE III: Configure Active Directory & promote server as a domain controller

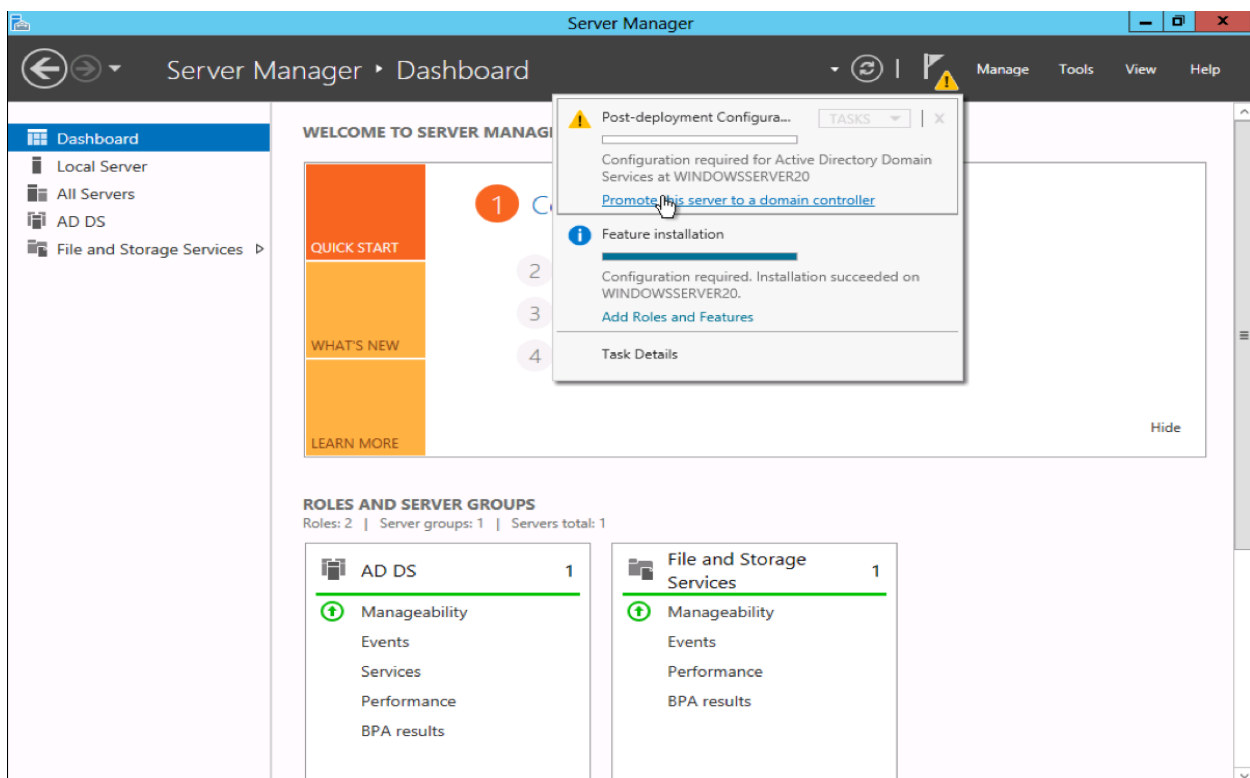
Promoting the server to a domain controller will allow all workstation/users to join the new centralized file server and user credentials environment. The user information (Full name, department, and designation etc) are collected to develop a user naming convention (In this task, we will use **First initial.last name**). Users will then be added to the Active Directory of the server



and assign them to security groups based on data obtained and placed on a documentation sheet. Shares will be created for specific groups of users and their workstations will be configured with login scripts for mapping drive letters to their workstations.

After installing the AD DS role, the server is configured for our created domain by using the following steps:

1. From the task bar, click **Open the Server Manager**.
2. Select the yellow notifications icon in the top navigation bar of the Server Manager window. The Notifications Pane opens and displays a **Post-deployment Configuration** notification. Click the **Promote this server to a domain controller** link that appears in the notification.



3. From the **Deployment Configuration** tab, select **Radial options > Add a new forest**. Enter root domain name in the **Root domain name** (in our case: **abccompany.com**) field and click **Next**.
4. Select a **Domain** and a **Forest functional level (2008)**.

Enter a password for Directory Services Restore Mode (DSRM) in the **Password** field.

1. Review the warning on the **DNS Options** tab and select **Next**.
2. Confirm or enter a **NetBIOS name** (in our case: **abc**) and click **Next**.
3. Specify the locations of the **Database**, **Log files**, and **SYSVOL folders**, then click **Next**.
4. Review the configuration options and click **Next**.
5. The system checks if all necessary prerequisites are installed on the system. If the system passes these checks, click **Install**.
6. After the server reboots, reconnect to it by using Microsoft Remote Desktop Protocol (RDP).

### **PHASE III: Promoting the new server to a domain controller**

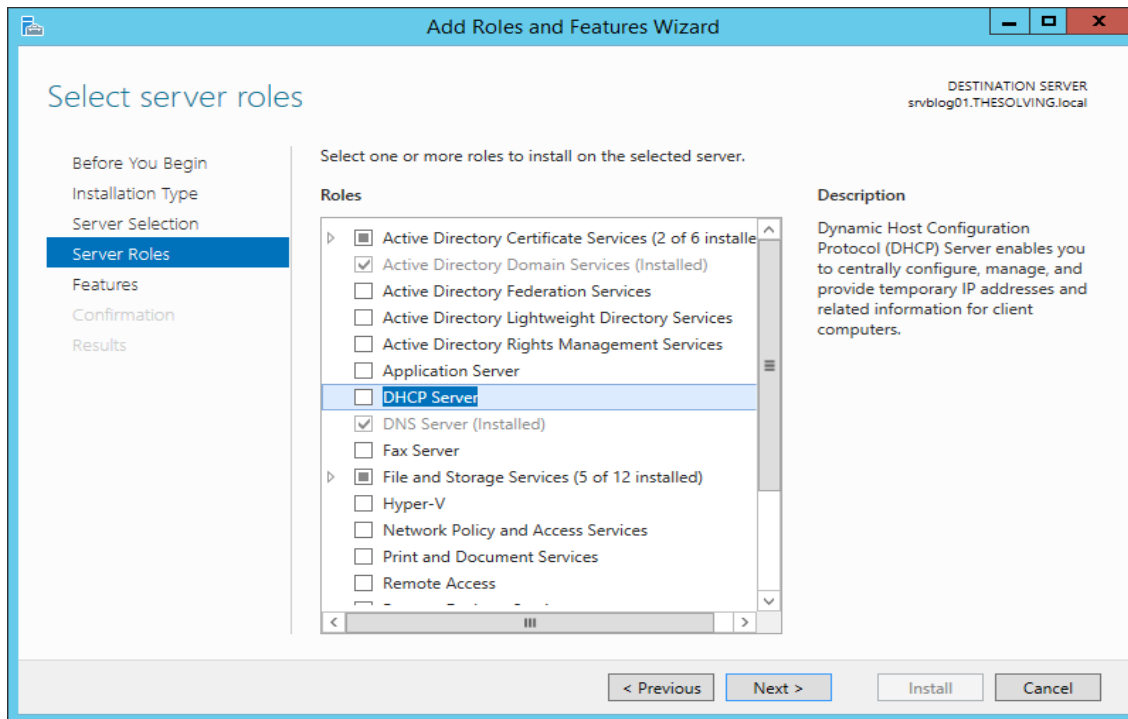
#### **(3) Configuring a Multi-scope DHCP server to work with VLANs on Windows Server**

To take advantage of the full capabilities of **LAN segmentation (VLAN)**, one needs to properly configure a **DHCP server** with different scopes (multi-scope setup). **Windows Server** offers a simple solution to the problem. Before this configuration, as shown in the NETWORK TOPOLOGY, a configured *layer-3 switch* with *multiple VLANs* is SETUP. The below steps guide the automatic assignment of *VLAN-aware* IP addresses to the devices connected at the physical ports of the switch. The switch will also need to forward *DHCP* requests to the *Windows Server*.

#### **STEP-I:**

The first step is to install the DHCP server role:

- Log in to Windows Server by Admin account
- Click **Add roles and features** -> DHCP Server
- Click **Add Features** -> Click **Next** to continue
- Add features dialog-BOX pops up, Click **Next** to continue
-



Click **Install**

Click **Complete DHCP configuration**

**Search for post deployment configuration from notification in server manager**

**Select complete DHCP configuration**

Click **Next** to continue

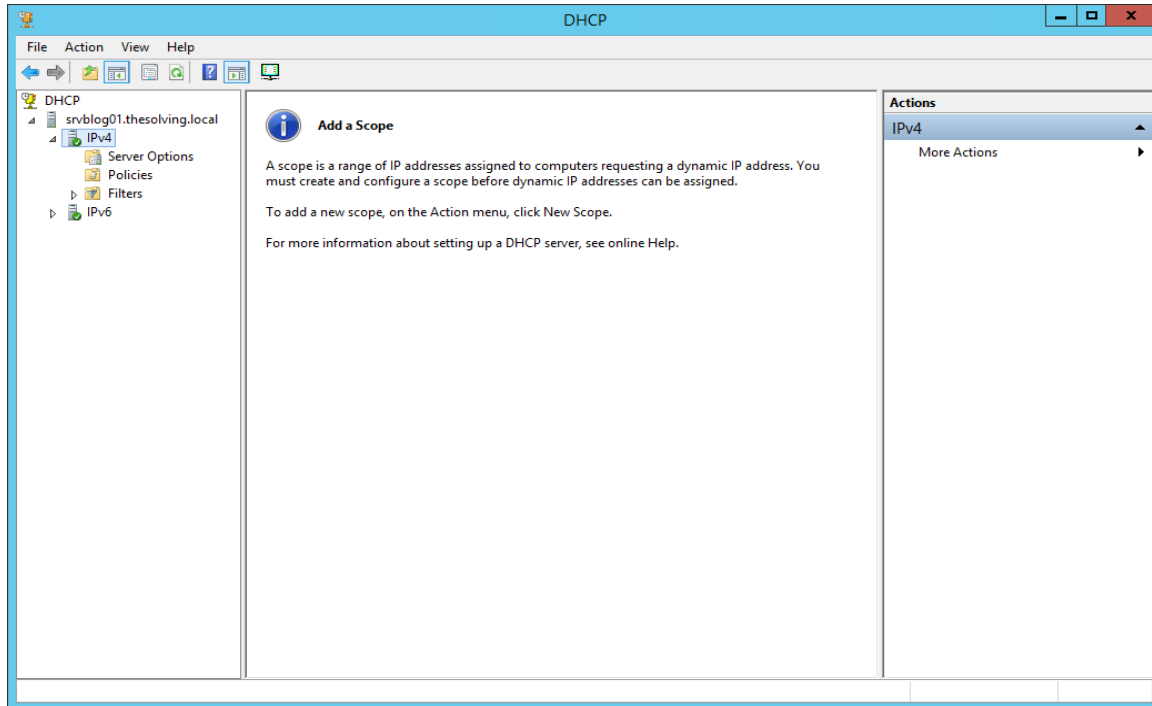
Choose **Skip AD authorization** -> Click **Commit**

Click **Close**

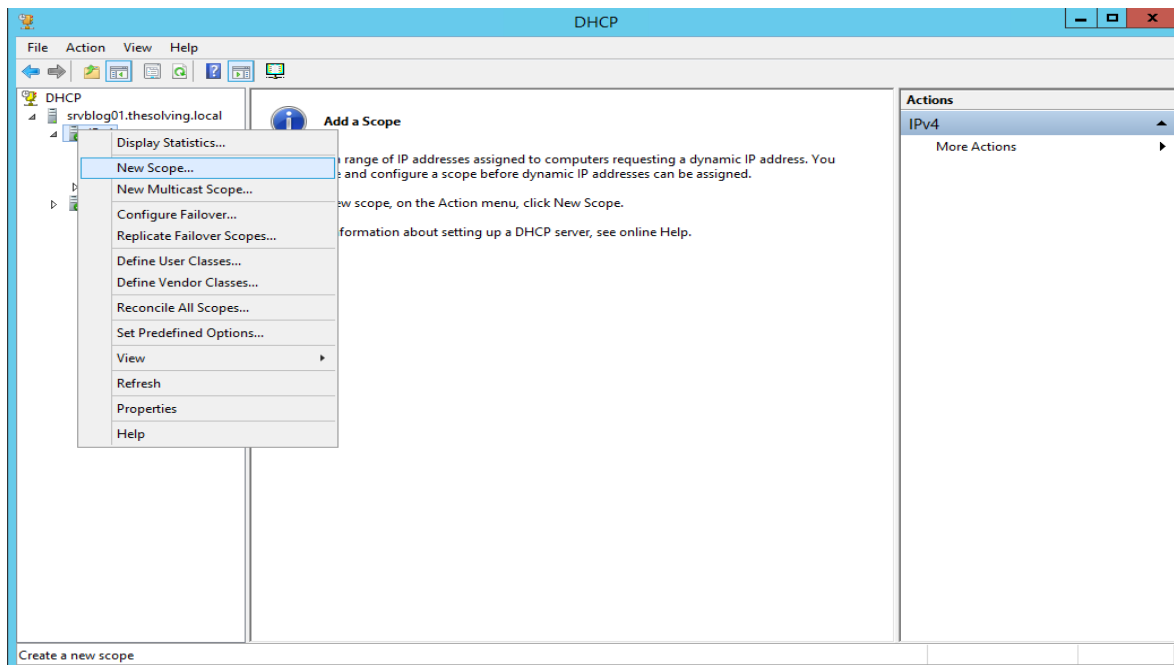
**STEP-II:**

**Configuring multi-scope DHCP**

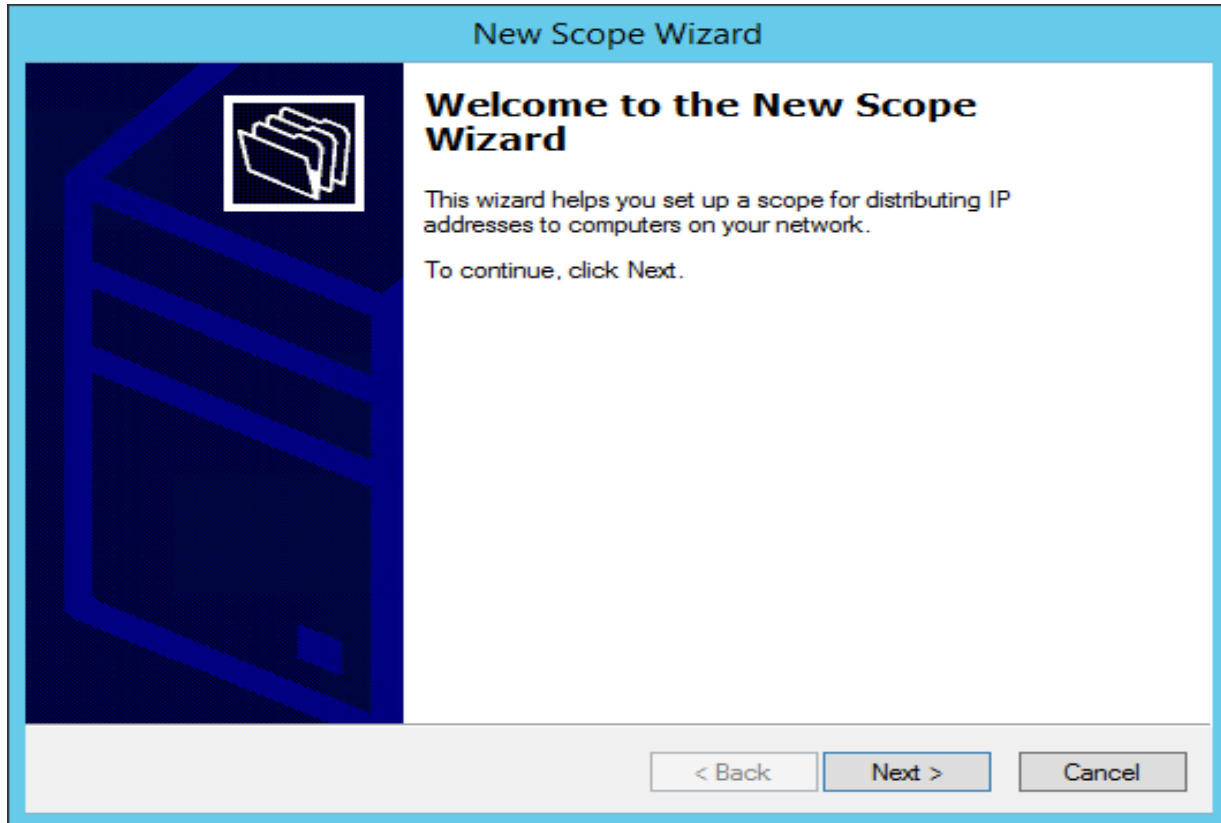
Open the *DHCP* management panel:



Right-click on *IPv4* and select *New Scope*, a *Wizard* will start:



Click *Next*:



The image shows the 'New Scope Wizard' window. On the left is a large blue graphic of a server rack. In the top right corner of the main area is a small icon of a folder with a document. The text reads: 'Welcome to the New Scope Wizard', 'This wizard helps you set up a scope for distributing IP addresses to computers on your network.', and 'To continue, click Next.' At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

New Scope Wizard

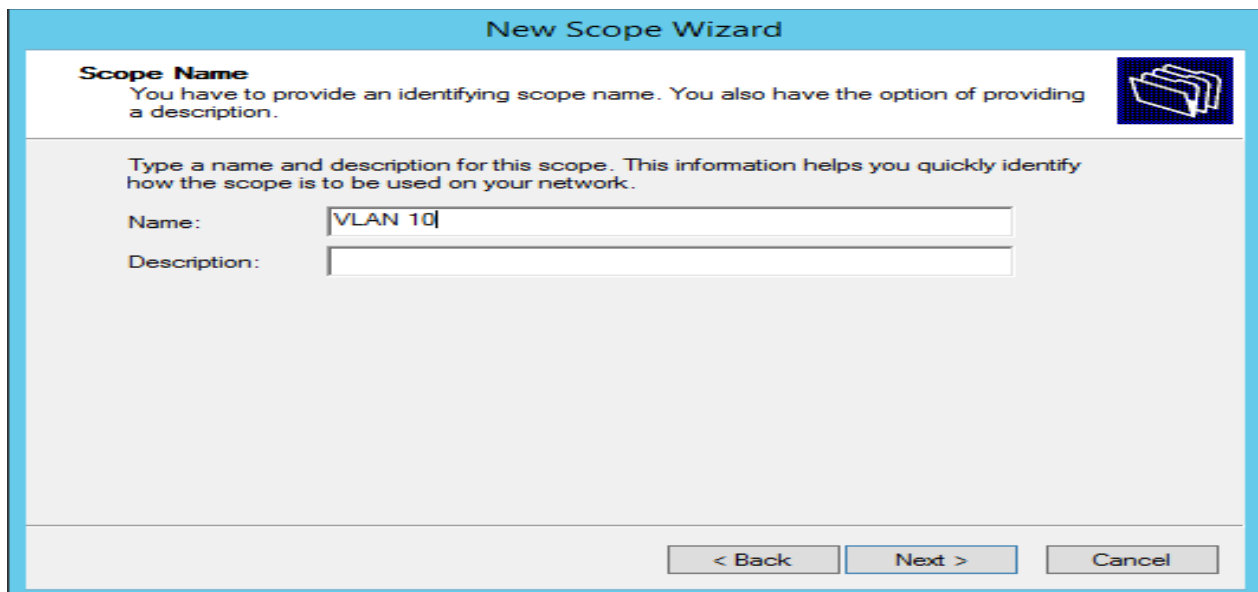
**Welcome to the New Scope Wizard**

This wizard helps you set up a scope for distributing IP addresses to computers on your network.

To continue, click Next.

< Back   Next >   Cancel

Give a name to the *scope* and Click *NEXT*:



The image shows the 'New Scope Wizard' window at the 'Scope Name' step. On the right is a small icon of a folder with a document. The text reads: 'Scope Name', 'You have to provide an identifying scope name. You also have the option of providing a description.', and 'Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.' There are two input fields: 'Name:' with the text 'VLAN 10' and 'Description:'. At the bottom right are three buttons: '< Back', 'Next >', and 'Cancel'.

New Scope Wizard

**Scope Name**

You have to provide an identifying scope name. You also have the option of providing a description.

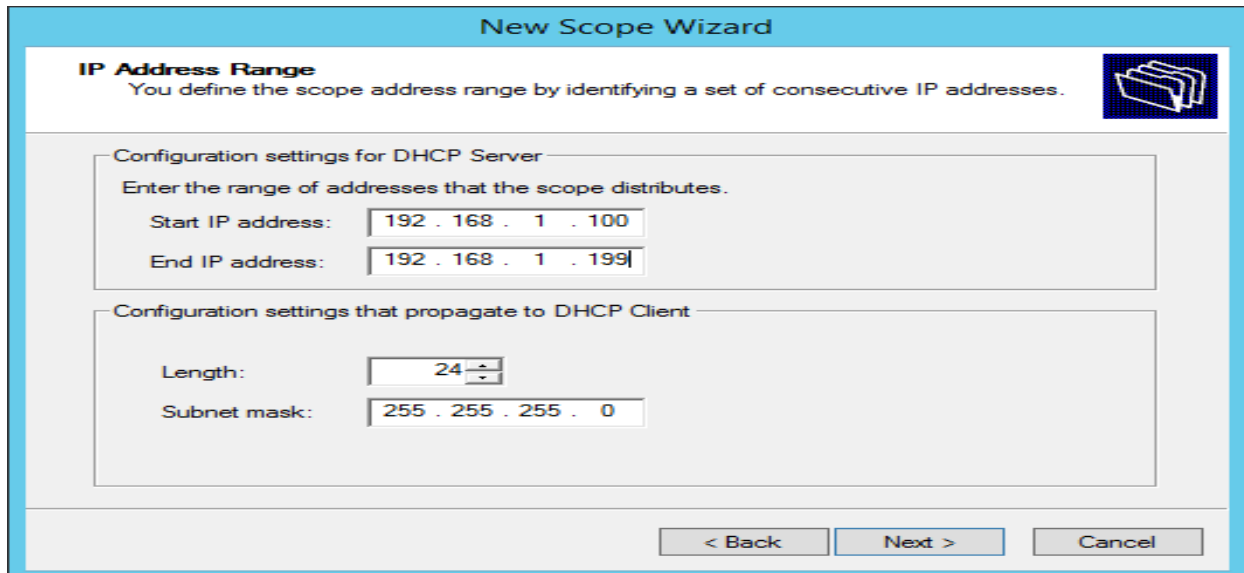
Type a name and description for this scope. This information helps you quickly identify how the scope is to be used on your network.

Name:

Description:

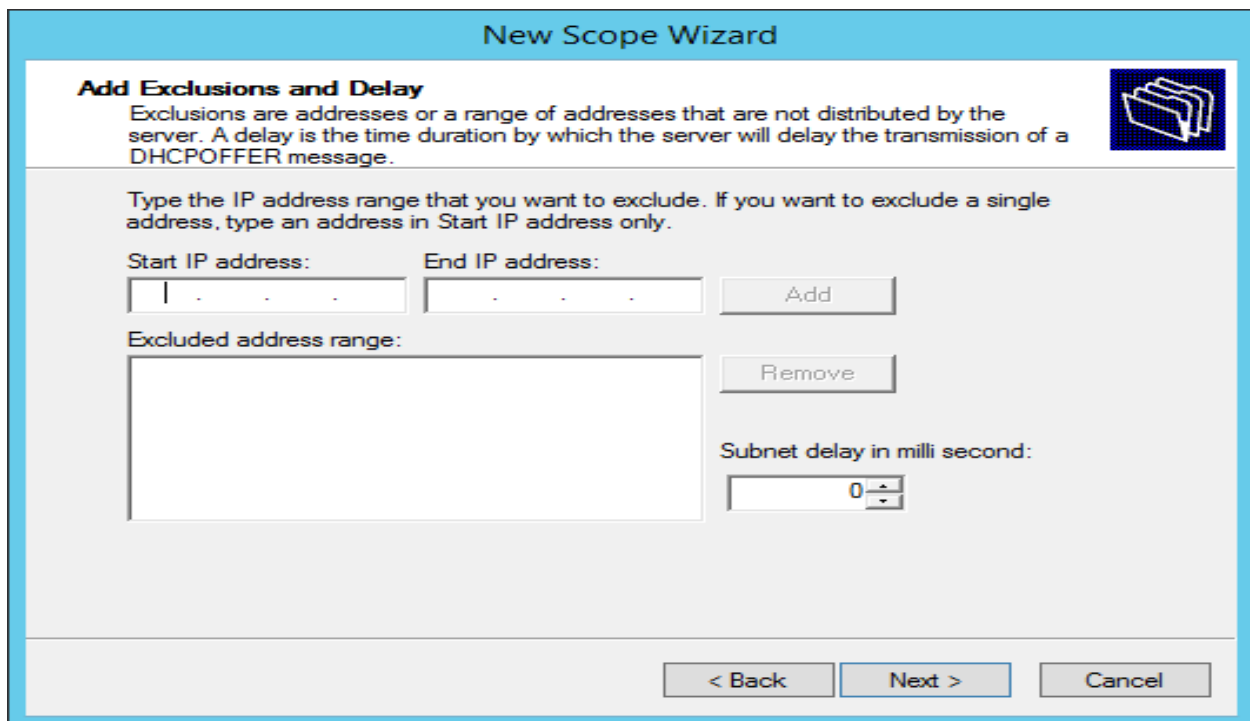
< Back   Next >   Cancel

Specify the range of *IP addresses* that will be assigned by the scope and Click NEXT. In our case for instance, **VLAN 10 in this task, the range will be (IP range 192.168.2 – 192.168.10.13) with class C subnet mask:**



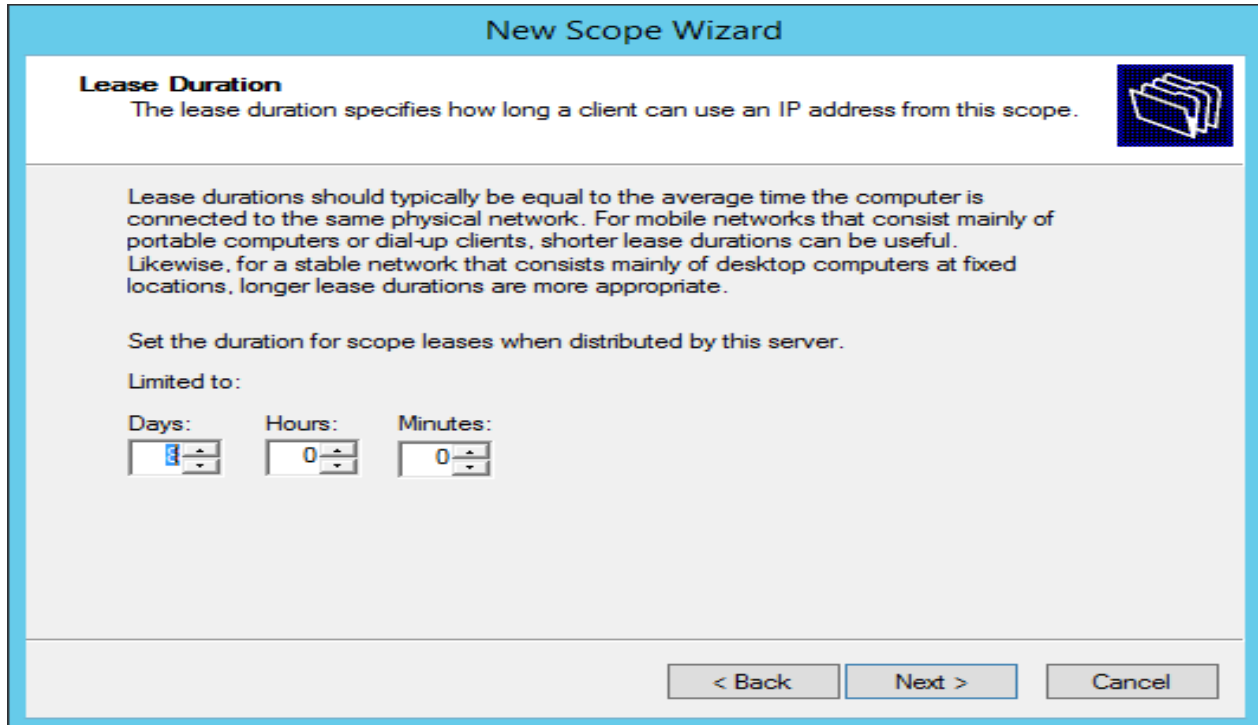
The screenshot shows the 'New Scope Wizard' window with the 'IP Address Range' tab selected. The window title is 'New Scope Wizard'. Below the title bar, there is a sub-header 'IP Address Range' and a description: 'You define the scope address range by identifying a set of consecutive IP addresses.' To the right of the description is a folder icon. The main content area is divided into two sections. The first section, 'Configuration settings for DHCP Server', contains the instruction 'Enter the range of addresses that the scope distributes.' and two input fields: 'Start IP address:' with the value '192 . 168 . 1 . 100' and 'End IP address:' with the value '192 . 168 . 1 . 199'. The second section, 'Configuration settings that propagate to DHCP Client', contains two input fields: 'Length:' with the value '24' and 'Subnet mask:' with the value '255 . 255 . 255 . 0'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

One can add exclusions to the range of *Ips if so desired*



The screenshot shows the 'New Scope Wizard' window with the 'Add Exclusions and Delay' tab selected. The window title is 'New Scope Wizard'. Below the title bar, there is a sub-header 'Add Exclusions and Delay' and a description: 'Exclusions are addresses or a range of addresses that are not distributed by the server. A delay is the time duration by which the server will delay the transmission of a DHCP OFFER message.' To the right of the description is a folder icon. The main content area contains instructions: 'Type the IP address range that you want to exclude. If you want to exclude a single address, type an address in Start IP address only.' Below this are two input fields: 'Start IP address:' and 'End IP address:'. To the right of these fields is an 'Add' button. Below the 'Start IP address:' field is an 'Excluded address range:' label and a large empty text box. To the right of this text box is a 'Remove' button. Below the 'Excluded address range:' text box is a 'Subnet delay in milli second:' label and a spin box with the value '0'. At the bottom of the window are three buttons: '< Back', 'Next >', and 'Cancel'.

Default lease duration settings OF 8 DAYS is fine (Click NEXT):



**New Scope Wizard**

**Lease Duration**  
The lease duration specifies how long a client can use an IP address from this scope.

Lease durations should typically be equal to the average time the computer is connected to the same physical network. For mobile networks that consist mainly of portable computers or dial-up clients, shorter lease durations can be useful. Likewise, for a stable network that consists mainly of desktop computers at fixed locations, longer lease durations are more appropriate.

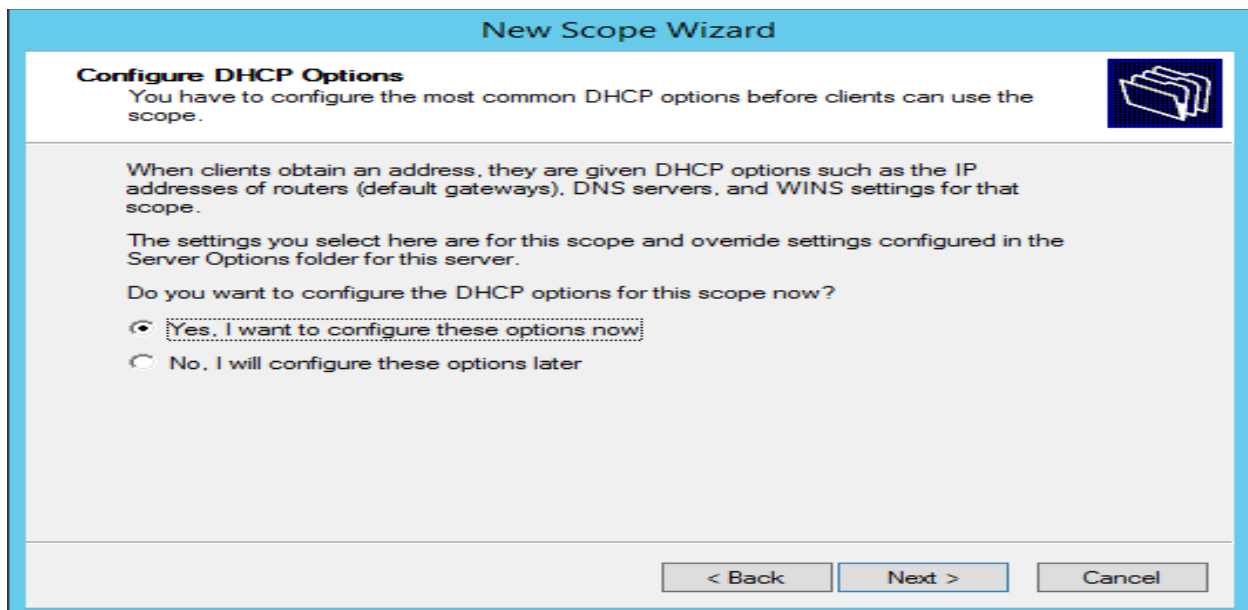
Set the duration for scope leases when distributed by this server.

Limited to:

Days:  Hours:  Minutes:

< Back   Next >   Cancel

Choose to Yes & click NEXT:



**New Scope Wizard**

**Configure DHCP Options**  
You have to configure the most common DHCP options before clients can use the scope.

When clients obtain an address, they are given DHCP options such as the IP addresses of routers (default gateways), DNS servers, and WINS settings for that scope.

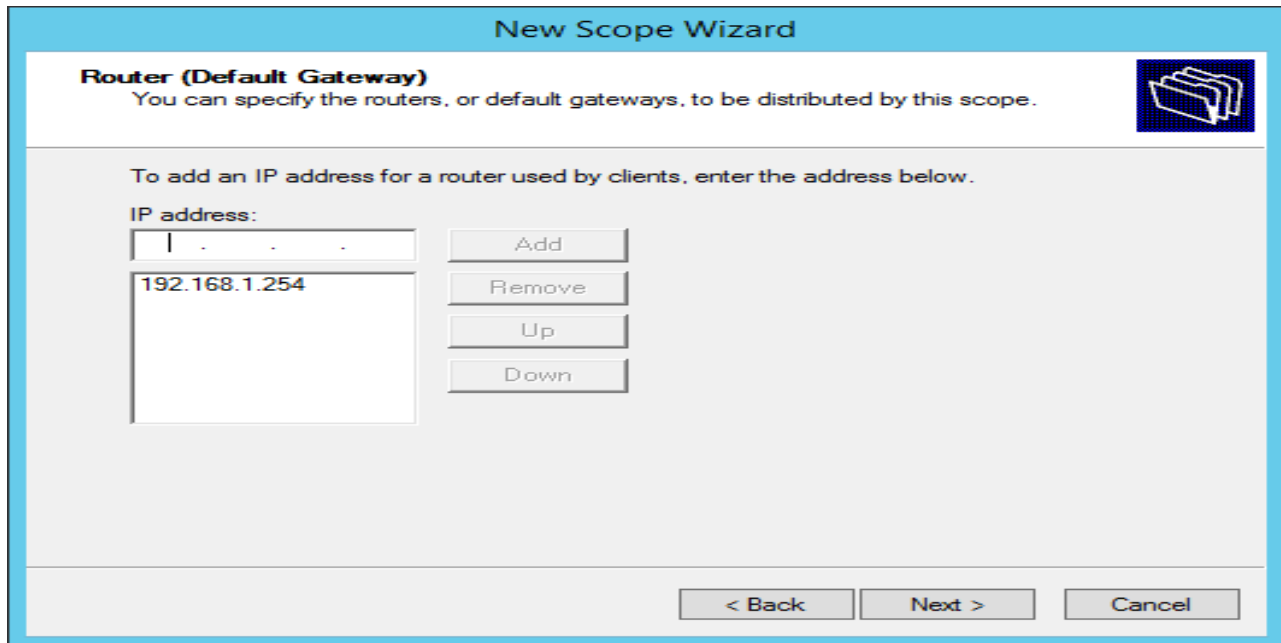
The settings you select here are for this scope and override settings configured in the Server Options folder for this server.

Do you want to configure the DHCP options for this scope now?

☒ Yes, I want to configure these options now  
☐ No, I will configure these options later

< Back   Next >   Cancel

Add the *gateway IP address* of the *VLAN* ( eg: VLAN 10 will have 192.168.10.1 as the default-gateway) and click NEXT:



**New Scope Wizard**

**Router (Default Gateway)**  
You can specify the routers, or default gateways, to be distributed by this scope.

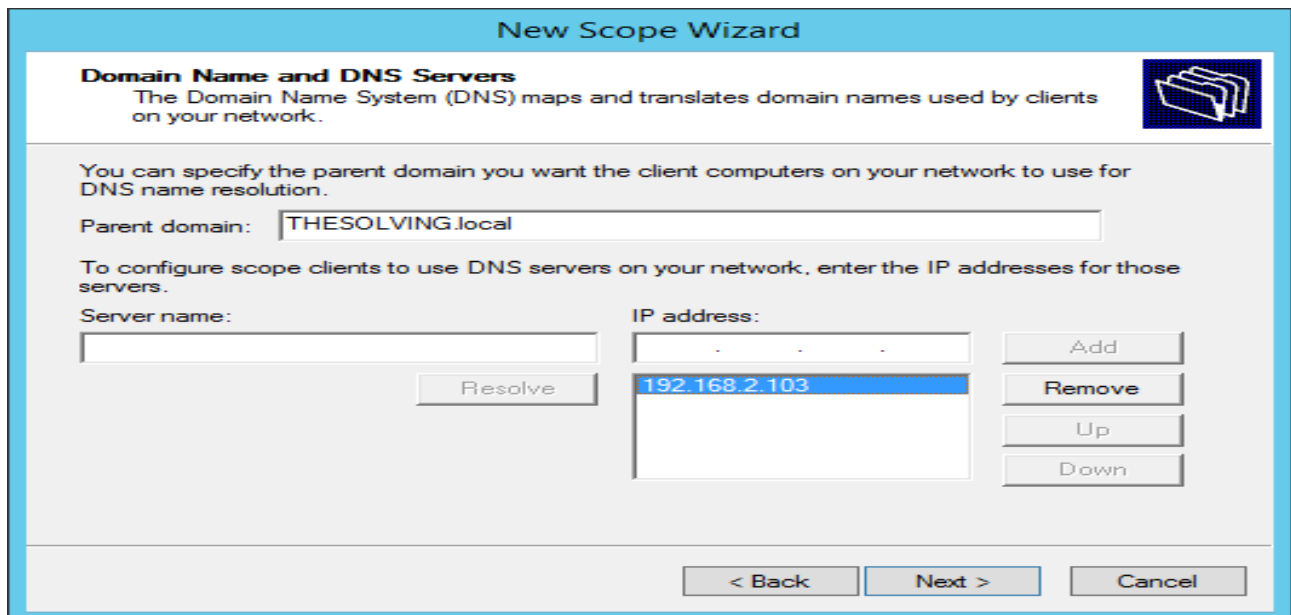
To add an IP address for a router used by clients, enter the address below.

IP address:

|               |        |
|---------------|--------|
|               | Add    |
| 192.168.1.254 | Remove |
|               | Up     |
|               | Down   |

< Back   Next >   Cancel

Specify the *DNS servers* (127.0.0.1):



**New Scope Wizard**

**Domain Name and DNS Servers**  
The Domain Name System (DNS) maps and translates domain names used by clients on your network.

You can specify the parent domain you want the client computers on your network to use for DNS name resolution.

Parent domain:

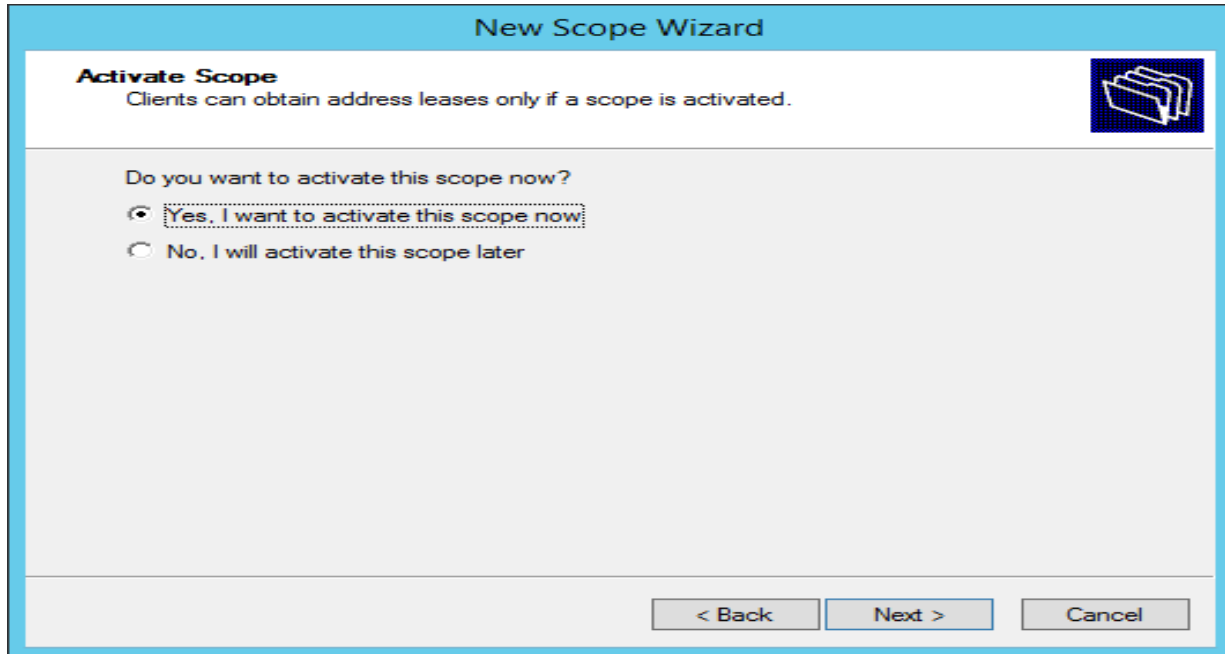
To configure scope clients to use DNS servers on your network, enter the IP addresses for those servers.

|              |                      |             |                      |        |
|--------------|----------------------|-------------|----------------------|--------|
| Server name: | <input type="text"/> | IP address: | <input type="text"/> | Add    |
|              | Resolve              |             | 192.168.2.103        | Remove |
|              |                      |             |                      | Up     |
|              |                      |             |                      | Down   |

< Back   Next >   Cancel



Click NEXT:



The image shows the 'New Scope Wizard' window, specifically the 'Activate Scope' step. The window has a light blue title bar with the text 'New Scope Wizard'. Below the title bar, the section is titled 'Activate Scope' with a subtext: 'Clients can obtain address leases only if a scope is activated.' To the right of this text is a small icon of a folder. The main area of the window contains the question 'Do you want to activate this scope now?' followed by two radio button options: 'Yes, I want to activate this scope now' (which is selected) and 'No, I will activate this scope later'. At the bottom of the window, there are three buttons: '< Back', 'Next >', and 'Cancel'.

**New Scope Wizard**

**Activate Scope**  
Clients can obtain address leases only if a scope is activated.

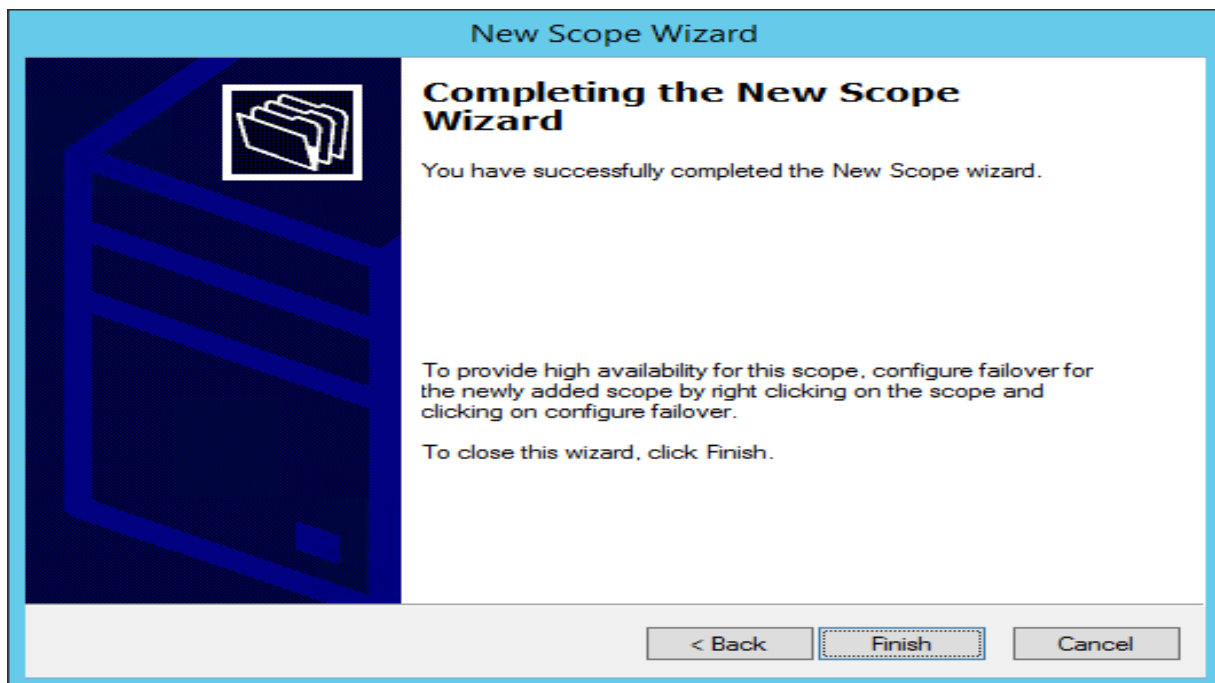
Do you want to activate this scope now?

☒ Yes, I want to activate this scope now

☐ No, I will activate this scope later

< Back   Next >   Cancel

Click FINISH



The image shows the 'New Scope Wizard' window, specifically the 'Completing the New Scope Wizard' step. The window has a light blue title bar with the text 'New Scope Wizard'. On the left side, there is a large blue graphic of a server rack. To the right of the graphic, the section is titled 'Completing the New Scope Wizard' with a subtext: 'You have successfully completed the New Scope wizard.' Below this, there is a paragraph of text: 'To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.' Another paragraph follows: 'To close this wizard, click Finish.' At the bottom of the window, there are three buttons: '< Back', 'Finish' (which is highlighted with a dashed border), and 'Cancel'.

**New Scope Wizard**

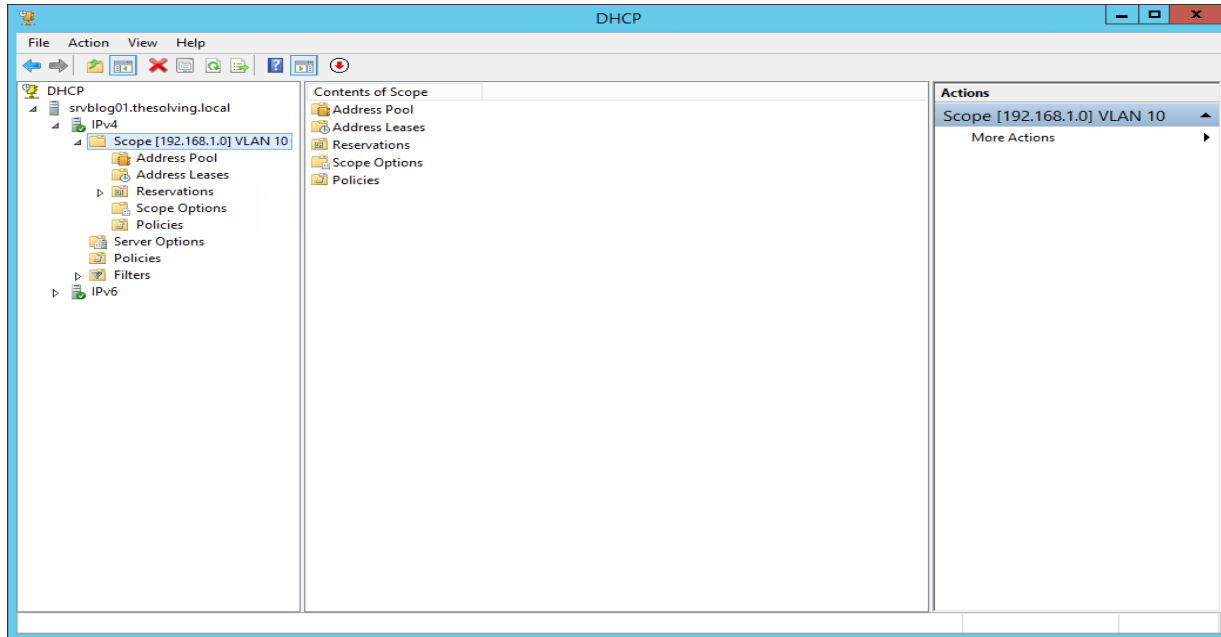
**Completing the New Scope Wizard**  
You have successfully completed the New Scope wizard.

To provide high availability for this scope, configure failover for the newly added scope by right clicking on the scope and clicking on configure failover.

To close this wizard, click Finish.

< Back   Finish   Cancel

The scope will appear in the panel.



*NB: Similar STEPS approach will be used to create the scope for the other VLANs/departments*

#### **(4) Adding users to domain to allow login**

##### New User Creation

Every user who accesses the network must have a user account. To create a new domain user account in Windows Server 2012, we use the follow steps:

##### STEP I

Choose **Start** → **Administrative Tools** → **Active Directory Users and Computers**.

This brings up the Active Directory Users and Computers management console.

##### STEP II

Right-click the domain that you want to add the user to and then choose New →User.

#### STEP III

Type the user's first name, middle initial, and last name.

#### STEP IV

Type the user logon name.

This name must be unique within the domain.

#### STEP V

Type the password twice.

You're asked to type the password twice, so type it correctly.

#### STEP VI

Click Next.

You're taken to the final page of the New Object — User Wizard.

#### STEP VII

Verify that the information is correct and then click Finish to create the account. If the account information is not correct, click the Back button and correct the error. You're done! Now you can customize the user's account settings. At a minimum, you'll probably want to add the user to one or more groups. You may also want to add contact information for the user or set up other account options.

### **(5) User file sharing and management system**

#### STEP I

Installation of the file server role can be done with the following powershell command:

**Install-WindowsFeature -Name FS-FileServer -IncludeAllSubFeature -IncludeManagementTools**

## **STEP II**

After installing the file and services role. In order to allow users to have access to files in the domain, we have to create a share. We do that with the following steps:

- We can directly click on the **FILE AND STORAGE SERVICES** menu from the server manager page.
- We can then create shared files with the menu that pop out which shows the disks available.
- We right click in the share space and **SELECT NEW SHARE** to create one.
- We then select the profile for the share which can be **SMB (windows)** or **NFS (LINUX, MAC OS)** share.
- We then select the volume we want the share to be located and thereafter give it a name.
- We select the local path on the server, remote file on the user machine.
- We select permissions as suited (so we allow full control in our case).
- We confirm and create.
- We create another with the quick profile and restrict the use to the user alone.
- We do this by changing permissions and give only a certain group or users permission by adding permission

## **ALTERNATIVE DETAILED PROCESS**

### **STEP II**

After installation in **STEP I**, we launch server manager and select the **File and Storage Services** node, and then **Shares** in the submenu.

### **STEP III**

Create Shared Folders in Windows Server 2012 - Computer Management

- First step in this process would be opening **Server Manager Dashboard** —> **go to Tools** —> **click Computer Management**.
- Once you click Computer Management, it will open up Computer Management Window, where you can see different types of tools and utilities. Now, expand **System Tools** —> **expand Shared Folders** —> **Right-click on Shares** —> **Select New Share**.
- As soon as you click New Share, it will open Create A **Shared Folder Wizard** —> **Click Next**.
- Click Browse or type the path to the folder, where you want to share.
- Click Make New Folder to create a new folder in the “C” drive, name it and subsequently click **OK** [Note- You can pick an existing folder].
- On clicking **Next** in the step given above, you will get some options to add a name and description to the shared folder. You can give a description in this step.
- In this step, we specify Permissions to the shared folder. We select All users have read-only Access, so that it can be accessed by all the users in my network.
- Click **Finish** to complete this process.

#### STEP IV

#### **Creating a Home Folder for Active Directory Users:**

Setup Folder Security:

- 1) We create a folder on the server - name it
- 2) Share the folder and change the default permissions
  - Right-click folder
  - Click “Properties”
  - Select the “Sharing” Tab
  - Check the “Advanced Sharing” button

- Check the box near “Share this folder”
- Click “Permissions”
- Check the “Allow” box near “Full Control”
- Click “OK” twice
- Select the “Security” Tab
- Click the “Advanced” button
- Click on the “Disable Inheritance” button
- A dialogue box will appear – select “Remove all inherited permission from this object”. You’ll either see nothing remaining on the list OR the Administrators group will be the only item listed. Follow the appropriate steps:

If the Administrators group remains,

- Click “Ok” and then click “Close” to exit the folder’s property pages.

If No entries remain, follow these steps:

- While still at the advanced security settings folder, click on Add
- Click on “select a principal”
- Type into the box: Administrators
- Click OK
- Check off the box near “full control”
- OK twice

- Close

The home folder share is now configured

## **(6) Tracking File and Folder Activities on Windows File Servers**

### **Step 1: Configure the “Audit Object Access” audit policy**

Perform the following steps to set up this audit policy:

1. On the primary domain controller, or on a workstation where “Administration Tools” are installed, open “Run” dialog box, type “gpmc.msc”, and click “OK” to open the “Group Policy Management” console.
2. In the “Group Policy Management” window, right-click on the default or a customized domain policy and select “Edit” from the context menu to open the Group Policy Management Editor window.

Note: It is recommended to create a new GPO, link it to the domain and edit it.

3. In “Group Policy Management Editor” window, navigate to “**Computer Configuration**” → “**Windows Settings**” → “**Security Settings**” → “**Local Policies**” → “**Audit Policy**”.
4. Double-click “Audit Object Access” to view its properties.
5. Click “Define these policy settings” checkbox. Click “Success” and “Failure” check boxes.

### **Step 2: Configure auditing on files and folders**

Follow the below steps to enable auditing for the files and folders to audit on Windows File Server.

1. Open “Windows Explorer” and navigate to the folder that you want to track.
2. Right-click the folder and select “Properties” from the context menu. The folder’s properties window appears on the screen.

3. Navigate to “Security” tab.
4. Click “Advanced” to access “Advanced Security Settings”. In “Advanced Security Settings” window, navigate to “Auditing” tab.
5. To create a new auditing entry, click “Add”. “Auditing Entry” window appears on the screen.
6. Click “Select a Principal” to choose users whose activities you want to track.
7. “Select User, Computer, Service Account, or Group” dialog box appears on the screen. If you want to audit all users’ activities, enter “Everyone” in the “Enter the object name to select” dialog box, and click “Checknames”. In our case, we enter “Everyone”.
8. Click “OK” to finalize your selection. It takes you back to “Auditing Entry” window.
9. Select “All” in “Type” drop-down menu to monitor both successful and failure events. You can select “Success” to monitor only successful events or you can select “Failure” to monitor only failure events.
10. In “Applies to” drop-down menu, select “This folder, subfolder, and files” option, if you want to audit all the subfolders and the files within this folder.
11. Click “Show advanced permission” option in the permissions section to view all the permissions. Select all the actions that you want to audit. If you want to audit all the actions, click “Full Control” checkbox. Here, we have selected “Full Control” checkbox.
12. Click “OK” to apply the auditing settings. It closes “Auditing Entry” window. Now on “Auditing” tab of “Advanced security settings” window, you can see the newly added audit entry.
13. Click “Apply” and “OK” in the “Advanced Security Setting” window to close it.
14. Click “Apply” and “OK” to close the folder properties window.



### Step 3: View Events in Windows Event Viewer

After configuring the above audit settings, one can track any change made to folders, subfolders, and files. For that, open “Windows Event Viewer” and go to “Windows Logs” → “Security”. In the right pane, use the “Filter Current Log” option to find the relevant events. For example, if anyone creates a new file, it will be logged.

#### ALTERNATIVELY

By Using **Lepide File Server Auditor** , one track all file and the folder activities of users. Unlike Native Auditing, one does not have to manually enable the auditing for different files and folders. One just need to install the solution, configure the audit settings once and you are good to go.

Clearly the easier option, Lepide’s File Server auditing software can help keep track of all the files and folders on Windows File Servers.

### **(7) Microsoft authenticator MFA to windows logon**

For this requirement, I have chosen the use of ‘**ManageEngine’s AD Self Service Plus product**’ in this task.

#### STEP I

##### Installing the software

We install my **AD SelfService Plus** software. The default port for the web service is 8888 – one can use a different port by entering it at this point. The installation will then proceed.

Once the installation is finished, we launch the console from the desktop shortcut, and you can also install it as a Windows service if you wish (from the Start menu shortcuts)

Installing the software as a service requires the server to be rebooted before it activates. Also, it is recommended to run the service as a domain account rather than LocalSystem, especially if it is going to be doing remote deployments of the client software from the console. As the console runs in a browser, you may need to turn off IE Enhanced Security Configuration if you are intending to access it from the server desktop.

## STEP II

### Setting up SSL

The AD SelfService Plus software uses a Tomcat instance so for it to work properly, one will need to install an SSL certificate. Log on to the console as admin (the default password is also admin)

Go to Admin | Product Settings | Connection

Check “Enable SSL port” and click Save

One can change the default port from 9251 if so wish. After doing this, restart the AD SelfService Plus service.

Log back into the console as admin again

Return to Admin | Product Settings | Connection.

Click SSL Certification Tool button.

Fill in the required fields for generating the Certificate Signing Request (CSR)

This will generate two files – a file called *SelfService.csr* at \webapps\adssp\Certificates and a file called *SelfService.keystore* at \jre\bin (both paths relative to the software install directory).

Log on to your Certificate Authority (<https://servername/certsrv>) and submit the CSR

Request a Certificate | Advanced Certificate request | Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

Copy the contents of the *SelfService.csr* file into the Saved Request box

Select Web Server from the options for Certificate Template

Click Submit and then click Yes

Click Download Certificate to download the certificate in .cer format

Click Download Certificate Chain to download the certificate in .p7b format

Place both the files at `\jre\bin`

Open an elevated command prompt

Change directory to `\jre\bin`

Run the following commands

**keytool -import -alias tomcat -trustcacerts -file certnew.p7b -keystore selfservice.keystore**

(password is the password you specified when generating the CSR)

Type 'y' or 'Yes' afterwards and press Enter

**.\keytool -importkeystore -srckeystore selfservice.keystore -destkeystore selfservice.keystore -deststoretype pkcs12**

(password is the password you specified when generating the CSR)

**keytool -import -alias tomcat -keystore ../lib/security/cacerts -file certnew.cer**

(password is *changeit*)

Type 'y' or 'Yes' afterwards and press Enter

Copy the *SelfService.Keystore* file from \jre\bin to \conf

Back up the server.xml file

Edit server.xml (you may need to run Notepad elevated to do this)

Replace both instances of *keystoreFile* value with *../conf/SelfService.keystore*

Replace both instances of *keystorePass* value with the password you specified when generating the CSR

Delete the property *keystoreType="PKCS12"*

Restart the AD SelfService Plus service

Log back on to the console. You should now see that your SSL certificate is trusted

### STEP III

#### Firewall configuration

Set up a Windows Firewall rule to allow inbound traffic on TCP port 9251

### STEP IV

#### Configuring the policy

Next, we need to configure a policy for our endpoint MFA

Log on to the console

Click on Configuration | Policy Configuration

You can either create a new policy or edit the default one (which will be named after the domain)

Select the OUs or Groups that the policy will apply to by clicking the Select OUs/Groups button.

I have chosen to apply the policy to an AD group

Click on Save Policy

Switch to the Multi-factor Authentication submenu on the left

Select the policy from the drop-down list and configure your authentication method (we are choosing Microsoft Authenticator)

Click on Enable Microsoft Authenticator

Switch to the Authenticator Settings tab

Choose the policy you are working on

Enable Endpoint MFA and select the second authentication type. Also, select whether you want users to be enabled to log in without 2FA if the AD SelfService Plus system is down

Next, click on Access URL and make sure you have switched to HTTPS with the right port number (9251 by default). It is imperative that this change is made before software is deployed to any target endpoints otherwise it will continue to try and connect on the old port.

Click on Save and then Save Settings

Deploy the client software to endpoints

Next we need to install the client software on the target endpoints where we wish to enable MFA. Whilst this software has an MSI download available which you can use to push the software via SCCM or a similar tool, with the free version, you must do the deployment via the console itself.

The endpoint requires two pre-requisites before deployment: -

1. Enable the Remote Registry service (either locally or via GPO)
2. Ensure that the target machine can be contacted via Windows File and Print Sharing exception in Windows Firewall (this can be done either locally or via a GPO), as the deployment process connects via the admin\$ share

Open the console

Click on Configuration | Administrative Tools | GINA/Mac/Linux (Ctrl-Alt-Del)

Click on GINA/Mac/Linux installation

In New Installation, locate the target machines you wish to deploy the software to

## Click Install

Once the install is successful, the console will report success. Checking the target endpoint's logon screen will now show an additional option as below

Clicking on the new option should successfully show the AD SelfService Plus options as configured in your password policy. If it fails, then remediate the error and try again (certificate issues should present themselves at this point, along with any other communications problems). The below image is similar to what you should see if it is successful (dependent on how the policy is configured)

## STEP V

Clicking on the new option should successfully show the AD SelfService Plus options as configured in the password policy. Once the user enters the PIN after they have scanned the QR code, they will be successfully enrolled.

## Verifying

Now it's simply a case of logging on as the enrolled user and using the Microsoft Authenticator app for a second level of verification.

When the user logs on, they should be presented with this screen. They then have to provide the PIN code from Microsoft Authenticator before they can successfully log on. Now we have 2FA configured for the Windows network logons (and free for up to 50 users which covers our current user size).

## **(8) Relocation plan measures**

In order to ensure smooth and hassle-free relocation of IT infrastructure and minimized downtime for the users, the following approach will be of a great help:

Prior to the actual relocation, inventory of IT equipment needs to be created in a form of spreadsheet with a listing of the equipment, and categorize it three ways:

- 1) existing to be discarded
- 2) existing to be reused, and
- 3) new.

The last two items are of interest as a system administrator. For those items, we shall include the quantity, item description, power draw, and receptacle requirements. Additional information such as requirements for temperature and humidity for each item will also have to be considered.

The scope of equipment to be relocated and the new site readiness to accommodate them are to be ascertained aforetime. After this is ensured, A deliberation talk with logistic team is held to understand the technical approach requirements. This is to ensure minimized damage probability. On arriving at the new site, it is expected that adequate care is taken to offload and install the equipment to ensure it performs as expected.

If something goes wrong when moving servers to a new location, delays or damage could affect the company. It is important to make sure the team involved with the relocation logistics understand the ramification of moving such sensitive equipment. Proper transportation, knowledge, and skill are key. Certain precautions should be taken to transport electronic devices like special packing and a controlled transit to keep the equipment safe.

Planning information technology components movement is pivotal to successfully getting the company up and running quickly. Leases, construction delays, permits, inspections, wiring internet activation determines move in schedule. Getting the IT team involved from the start will greatly improve the likelihood of a smooth transition.

The electrical system must have sufficient capacity for your equipment's load and have the right voltage and amperage and adequate surge protection. The data and electrical wiring must be well-



suited for the number of workstations, printers, and other devices attached to the network. A detailed examination of the data wiring is required to verify the integrity of all the connections. The flooring in the server room should be antistatic and grounded. The security system must ensure the safety of the server room equipment. Fire suppression systems should be evaluated to ensure it will suppress a fire without damaging electrical components and is safe for employees.