Lab 8: Installing, Configuring, and Troubleshooting the Network Policy Server Role Service

Objectives:

After completing this lab, you will be able to:

- Install the Network Policy Server role service and configure Network Policy Server settings

- Configure a RADIUS client

- Configure certificate auto-enrolment

Scenario

Adatum Bank is expanding its remote-access solution to all its branch office employees. This will require

multiple Routing and Remote Access servers located at different points to provide connectivity for its

employees. You will use RADIUS to centralize authentication and accounting for the remote-access

solution.

The Windows Infrastructure Services Technology Specialist has been tasked with installing and configuring

Network Policy Server into an existing infrastructure to be used for NAP, Wireless and Wired access,

RADIUS, and RADIUS Proxy.

Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must:

1. Add a Second Network Adapter (NIC) to LON-SVR1.

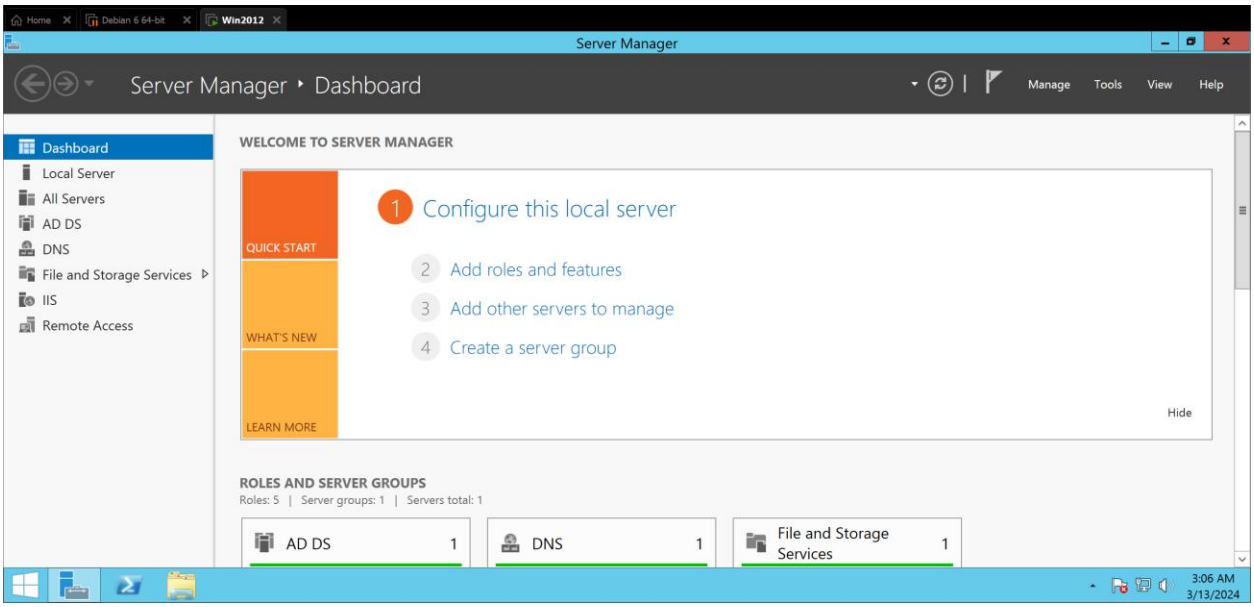
2. Start the LON-DC1 and LON-SVR1 virtual machines.

3. Log on to the LON-SVR1 and LON-DC1 virtual machines with the user name Administrator and the

password Pa$$w0rd.

4. Close the Initial Configuration Tasks window that appears after you log on.

5. Close the Server Manager window.



Exercise 1: Installing and Configuring the Network Policy Server Role Service

Exercise Overview

In this exercise, you will install and configure the Network Policy Server role.

The main tasks are as follows:

1. Ensure that you have completed the steps in the Lab Setup.

2. Open the Server Manager tool on LON-DC1.

3. Install the Network Policy and Access Services role.

Task 2: Open the Server Manager tool on LON-DC1

·On LON-DC1, open Server Manager from the Administrative Tools menu.

Task 3: Install the Network Policy and Access Services role

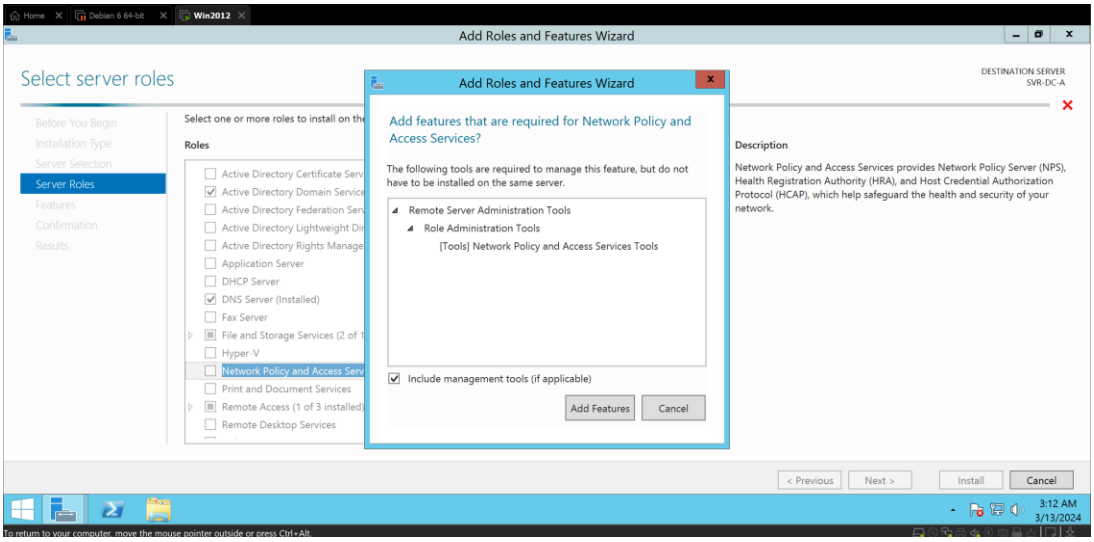
1. In the Server Manager list pane, right-click Roles and then click Add Roles.

2. Install the Network Policy Server role service from the Network Policy and Access Services role.

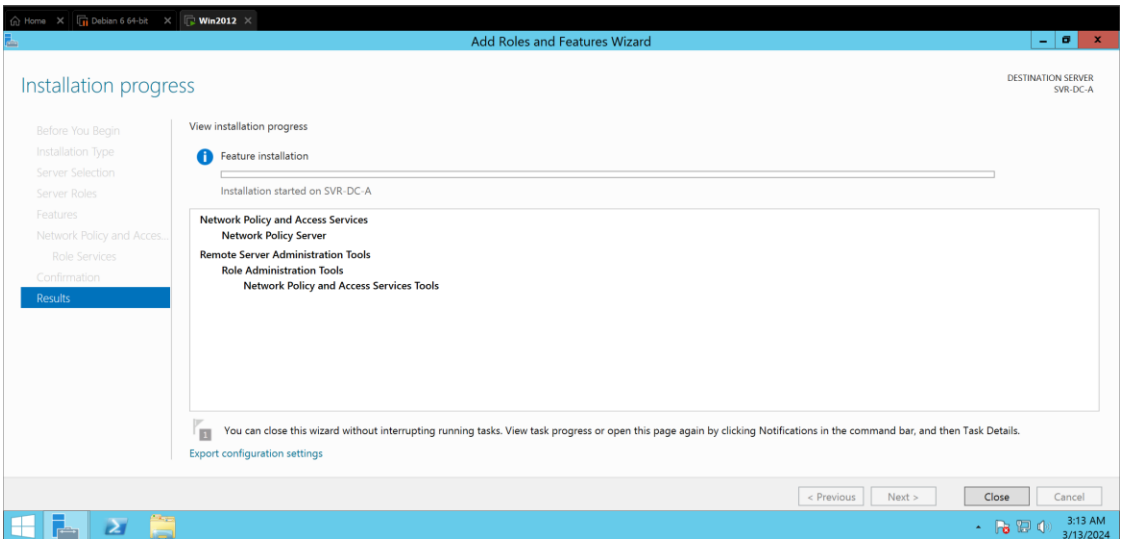
3. On the Installation Results page, verify Installation succeeded appears in the details pane and then click Close.

The Network Policy Server role is installed on LON-DC1.

4. Do not log off or shut down the virtual PCs at this point.



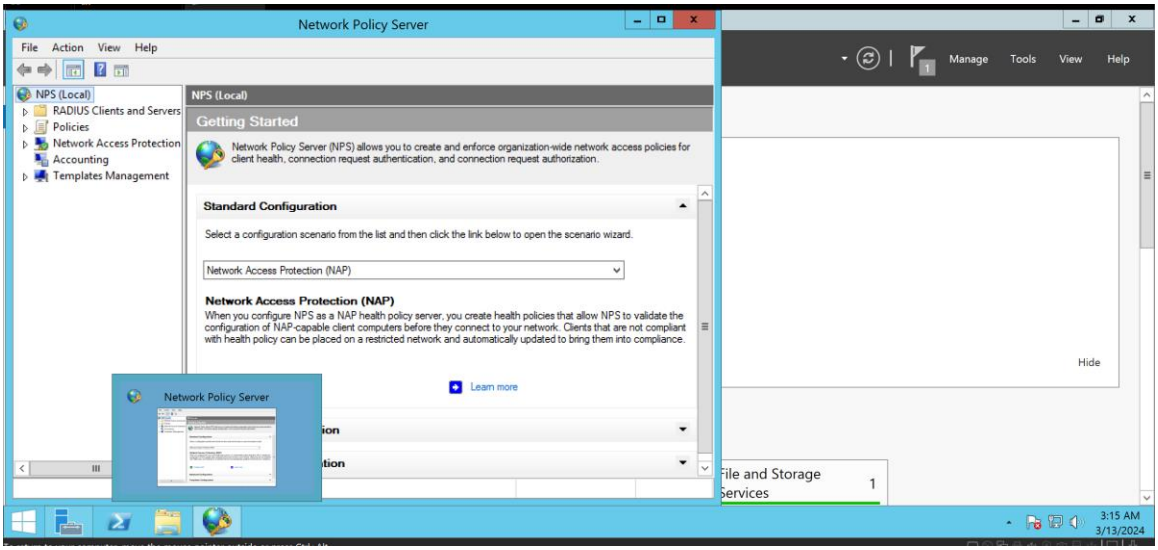
4. Register NPS in Active Directory.

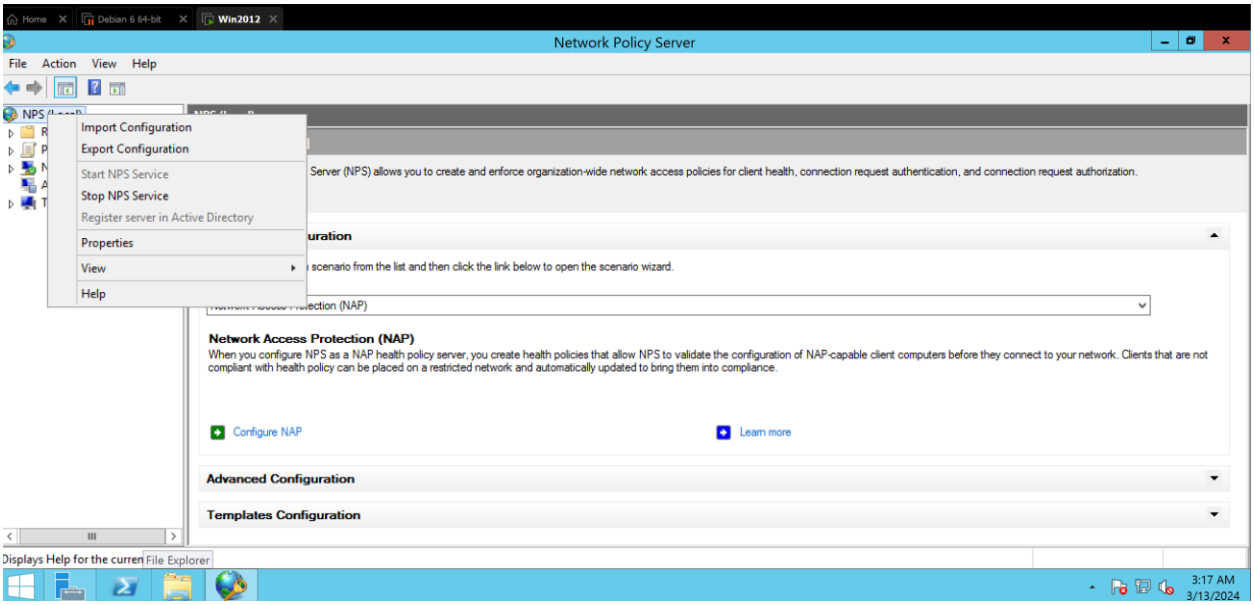


5. Configure LON-DC1 to be a RADIUS server for dial-up or VPN connections.
Step 1: Register NPS in Active Directory

Open the Network Policy Server console. You can find it in the Administrative Tools menu or search for "Network Policy Server" in the Start menu.

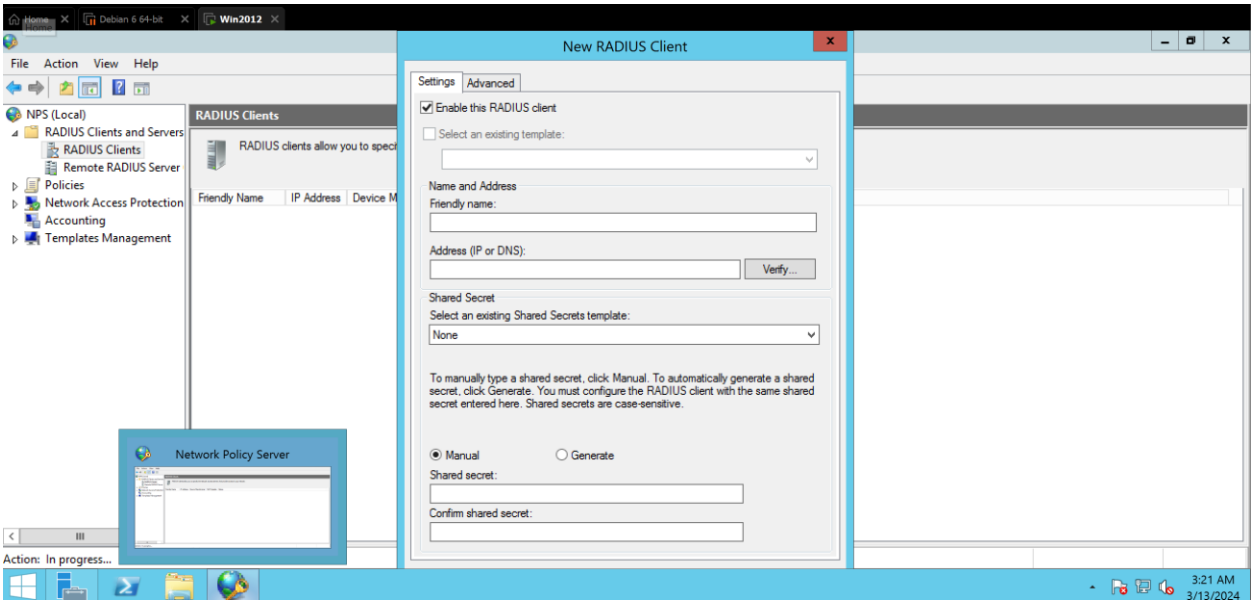
In the left pane of the Network Policy Server console, right-click on NPS (Local), and then click Register Server in Active Directory.



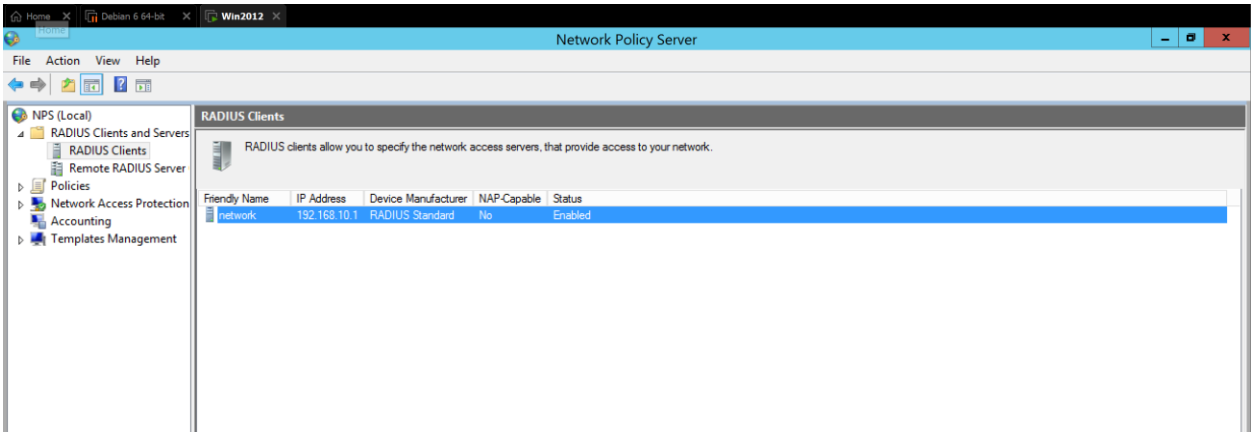


Step 2: Configure LON-DC1 as a RADIUS server

1. In the Network Policy Server console, expand RADIUS Clients and Servers.
2. Right-click on RADIUS Clients and select New.



3. In the New RADIUS Client dialog box, enter the friendly name and IP address of the RADIUS client (e.g., VPN server) that will be communicating with LON-DC1.
4. Enter a shared secret that will be used for authentication between the RADIUS client and LON-DC1. Note down this secret as you'll need it during configuration on the RADIUS client.
5. Click OK to save the RADIUS client configuration.



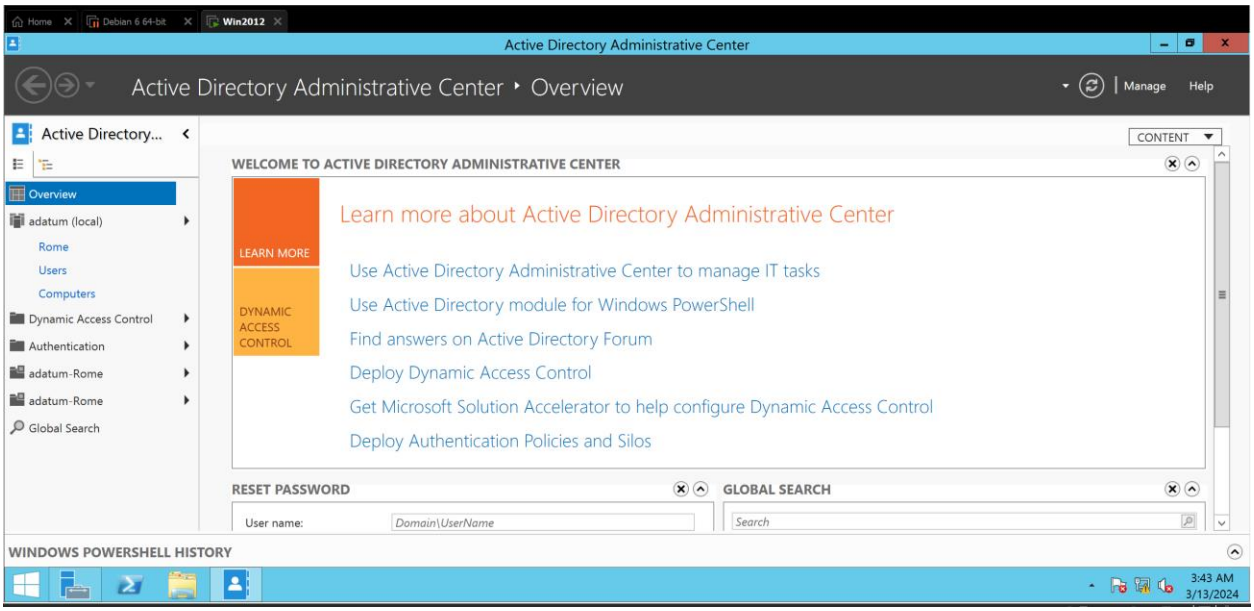
6. Next, you'll need to create network policies to define the conditions under which connections are allowed or denied. Right-click on Network Policies and select New.
7. Follow the wizard to create a new network policy. Define the conditions under which the policy applies (e.g., based on user groups, connection type, etc.) and specify the access permissions (e.g., grant or deny access).
8. Once the network policy is created, it will be applied based on the conditions specified.

Task 1: Ensure that you have completed the steps in the Lab Setup

Review the Lab Setup section and ensure you have completed the steps before you continue with this lab

Task 2: Open the Server Manager tool on LON-DC1

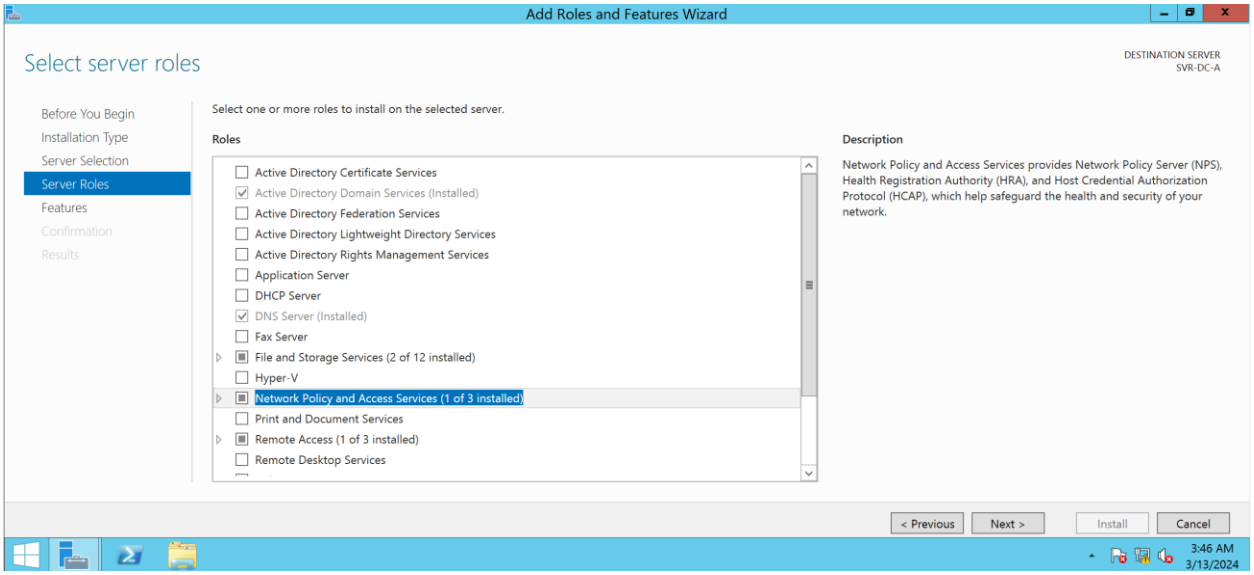
·On LON-DC1, open Server Manager from the Administrative Tools menu.



Task 3: Install the Network Policy and Access Services role

1. In the Server Manager list pane, right-click Roles and then click Add Roles.

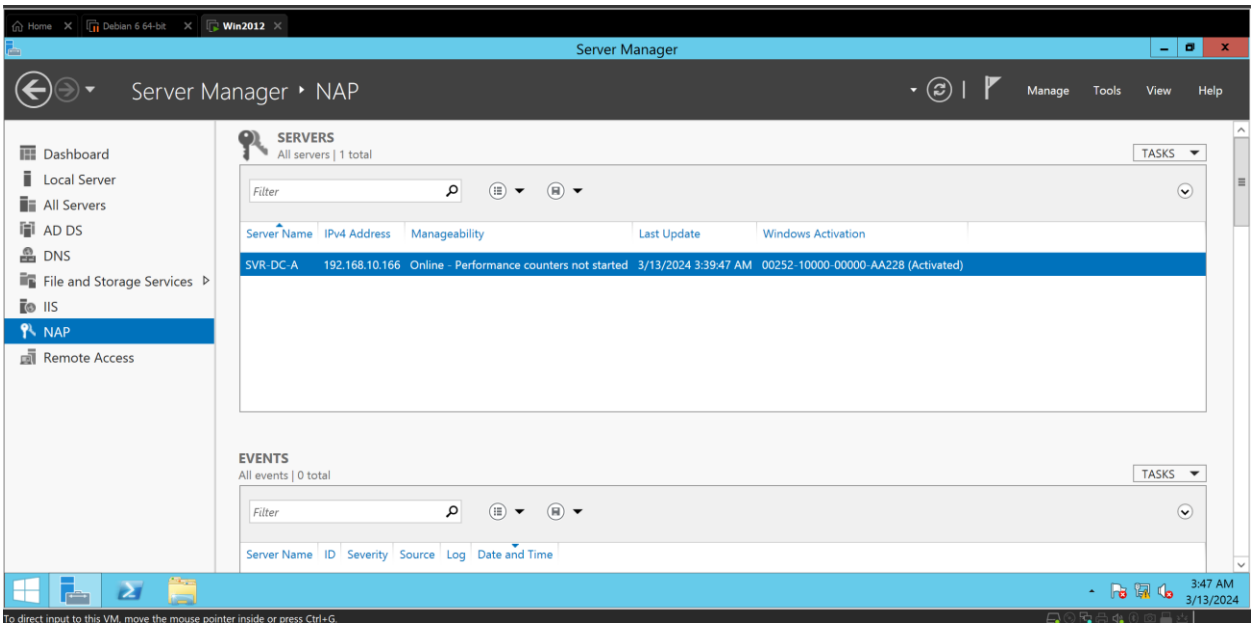
2. Install the Network Policy Server role service from the Network Policy and Access Services role.



3. On the Installation Results page, verify Installation succeeded appears in the details pane and then click Close.

The Network Policy Server role is installed on LON-DC1.

4. Do not log off or shut down the virtual PCs at this point.



Task 4: Register NPS in Active Directory

1. Open Network Policy Server from the Administrative Tools menu.

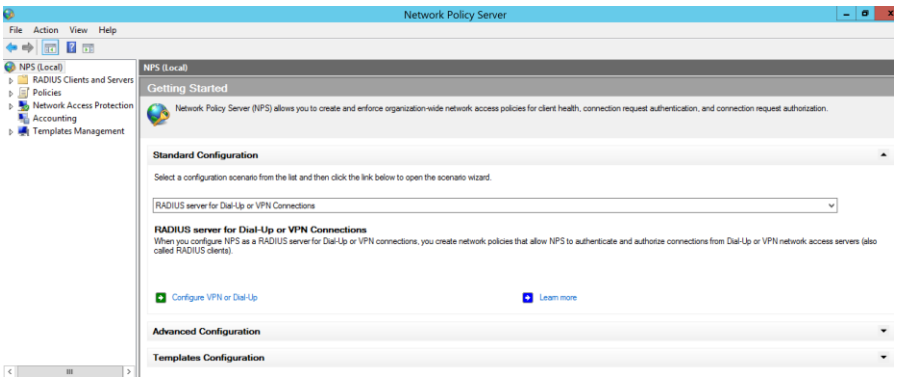
2. Using the NPS tool, register NPS in Active Directory.

The Network Policy server is registered in Active Directory.

Task 5: Configure LON-DC1 to be a RADIUS server for dial-up or VPN connections

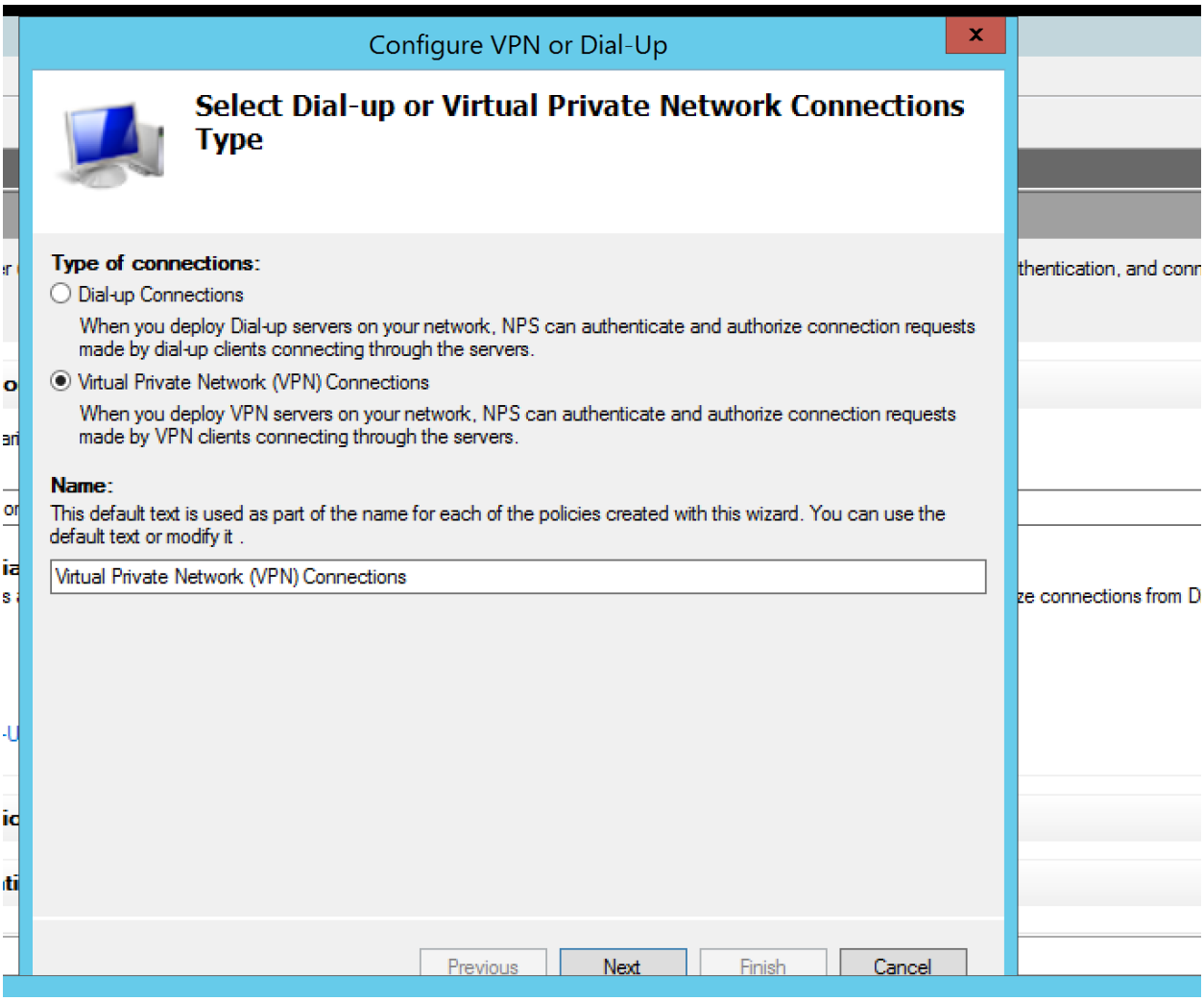
1. In the Network Policy Server management tool list pane, click NPS (Local).

2. In the details pane under Standard Configuration, click RADIUS server for Dial-Up or VPN Connections.



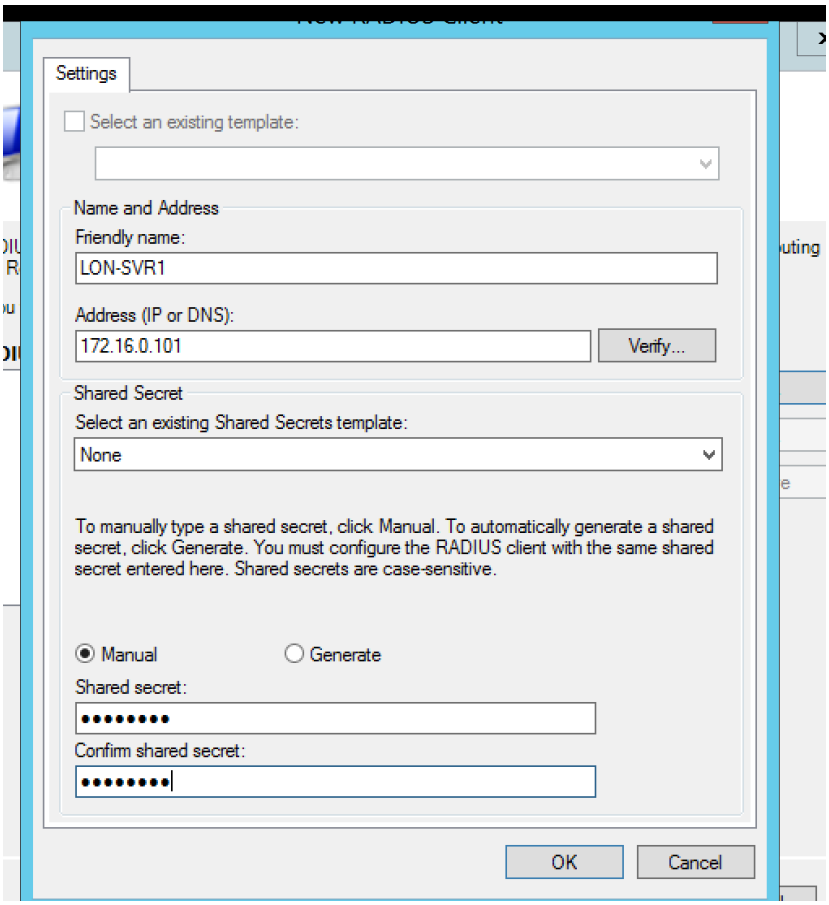
3. Under Radius server for Dial-Up or VPN Connections, click Configure VPN or Dial-Up and specify Virtual Private

Network (VPN) Connections, and accept the default name.

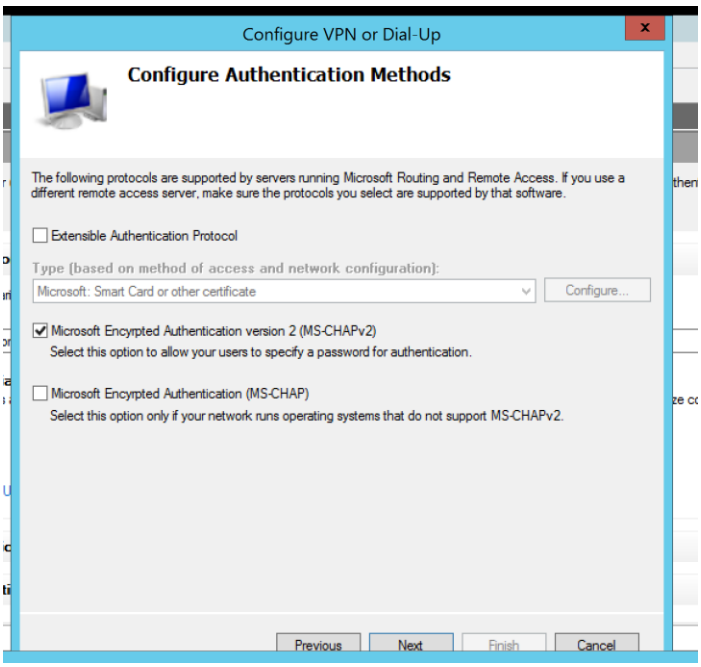


4. In the RADIUS clients dialog box, add LON-SVR1 as a RADIUS client with an address of 172.16.0.101

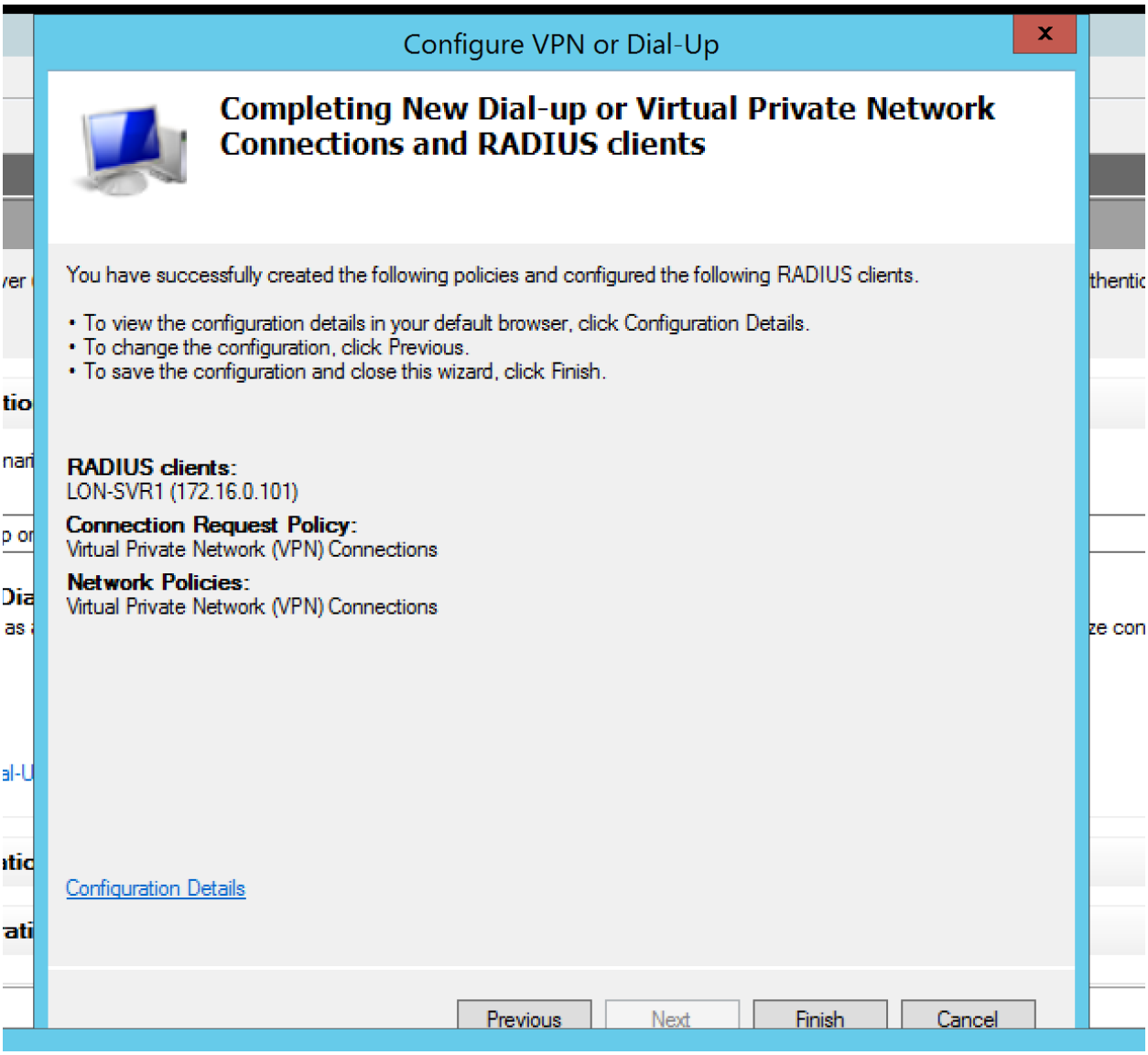
5. In the New RADIUS Client dialog box, specify and confirm the shared secret of Pa$$w0rd and then click OK.



6. In the Specify Dial-Up or VPN Server dialog box, accept the default setting.



7. In the Configure Authentication Methods dialog box, select Extensible Authentication Protocol and select (EAPMSCHAPv2).



Exercise 2: Configuring a RADIUS Client

Exercise Overview

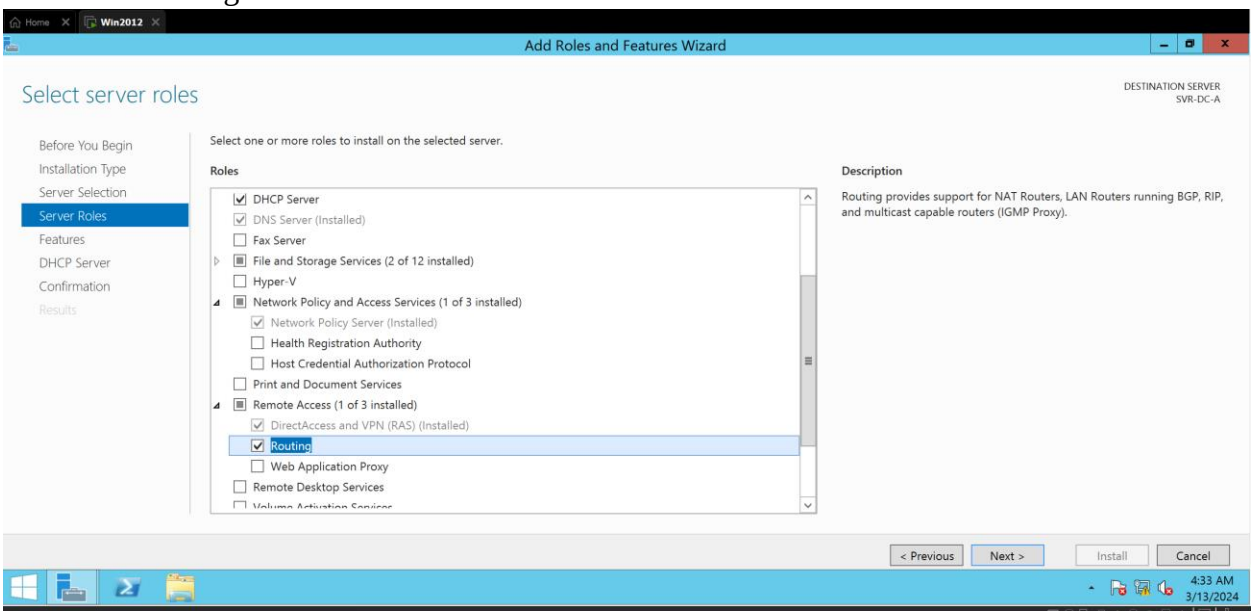
In this exercise, you will configure LON-SVR1 to host Routing and Remote Access Services and configure LONSVR1 as a RADIUS client.

The main tasks are as follows:

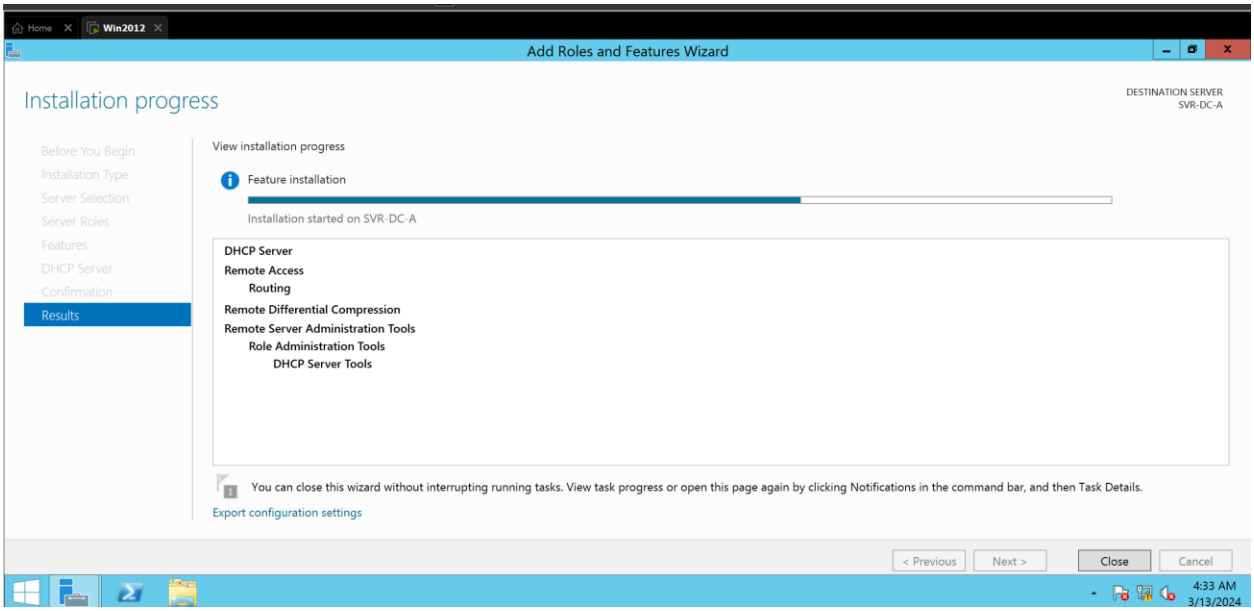
-On LON-SVR1, open Server Manager from the Administrative Tools menu.

Task 2: Install the Network Policy and Access Services and Remote Access role on LON-SVR1.

1. Using Server Manager, install the Network Policy and Access Services role with the role service of Routing and Remote Access.



2. On the Installation Results page, verify Installation succeeded appears in the details pane, and then click Close.



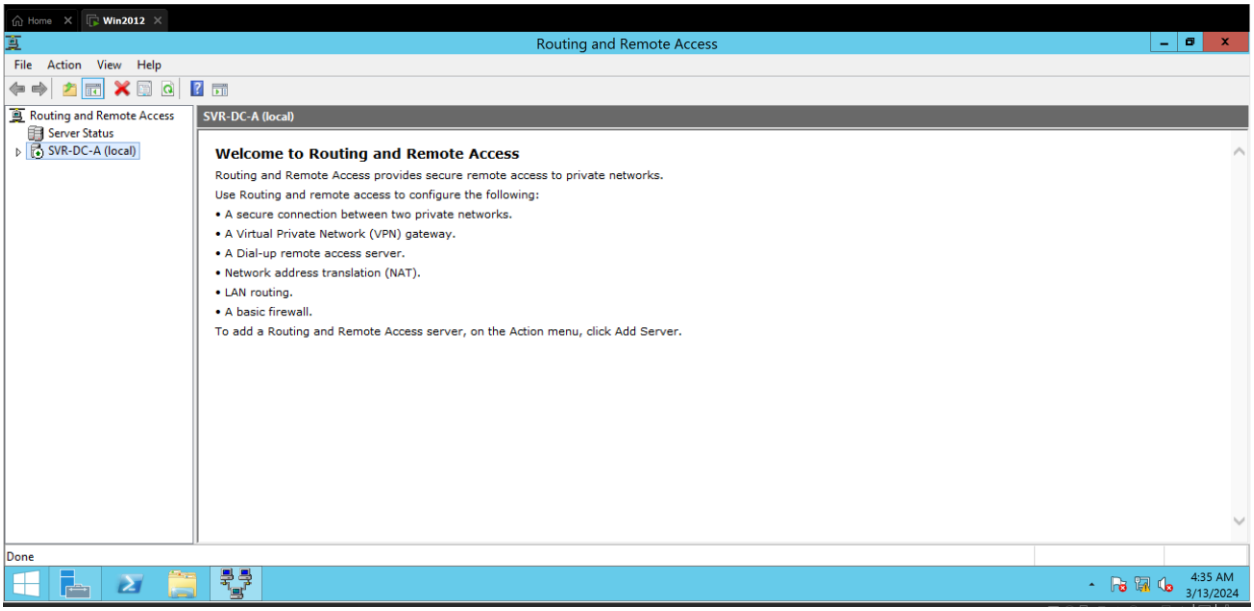
3. Do not log off or shut down the virtual PCs at this point.

The Routing and Remote Access Services role is installed on LON-SVR1.

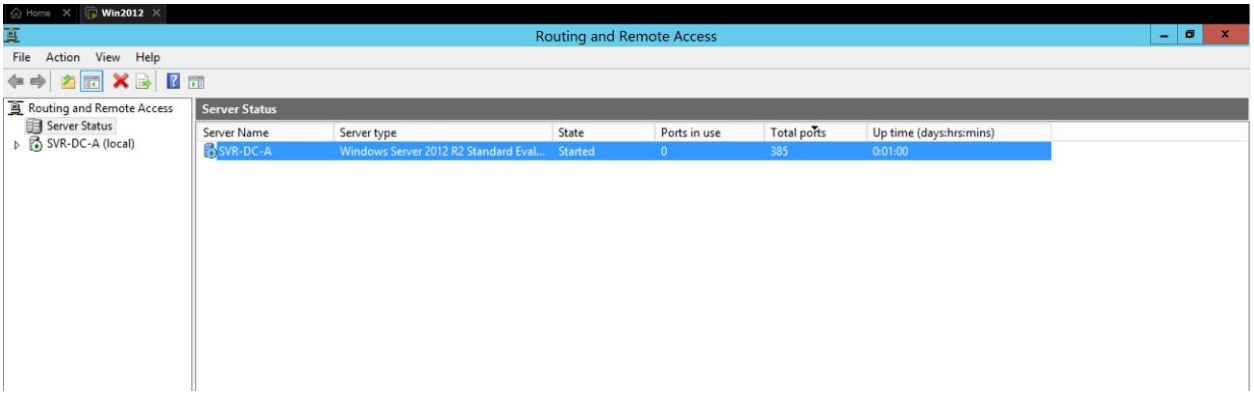
Task 3: Configure LON-SVR1 as a VPN server with a static address pool for Remote Access

clients and specify RADIUS authentication and accounting

1. Open the Routing and Remote Access Services administrative tool and click Configure and Enable Routing and Remote Access.



3. Configure the default Remote Access (dial-up or VPN), and on the Remote Access page, select the VPN option.



3. On the VPN Connection page, select the Local Area Connection 2 interface.

4. On the IP Address Assignment page, select From a specified range of addresses.

5. Use the range of 172.16.0.160 with 5 available addresses for the static pool.

6. On the Managing Multiple Remote Access Servers page, select Yes, set up this server to work with a RADIUS server, and then click Next.

7. Configure the following settings:

- Primary RADIUS server: LON-DC1

- Shared secret for the RADIUS server: Pa$$w0rd

- Accept the default settings for the remainder of the configuration process .

Close the Routing and Remote Access Services administrative tool.

Exercise 3: Configuring Certificate Auto-Enrollment

Exercise Overview

In this exercise, you will configure Certificate Auto-Enrollment for computers to use advanced authentication.

The main tasks are as follows:

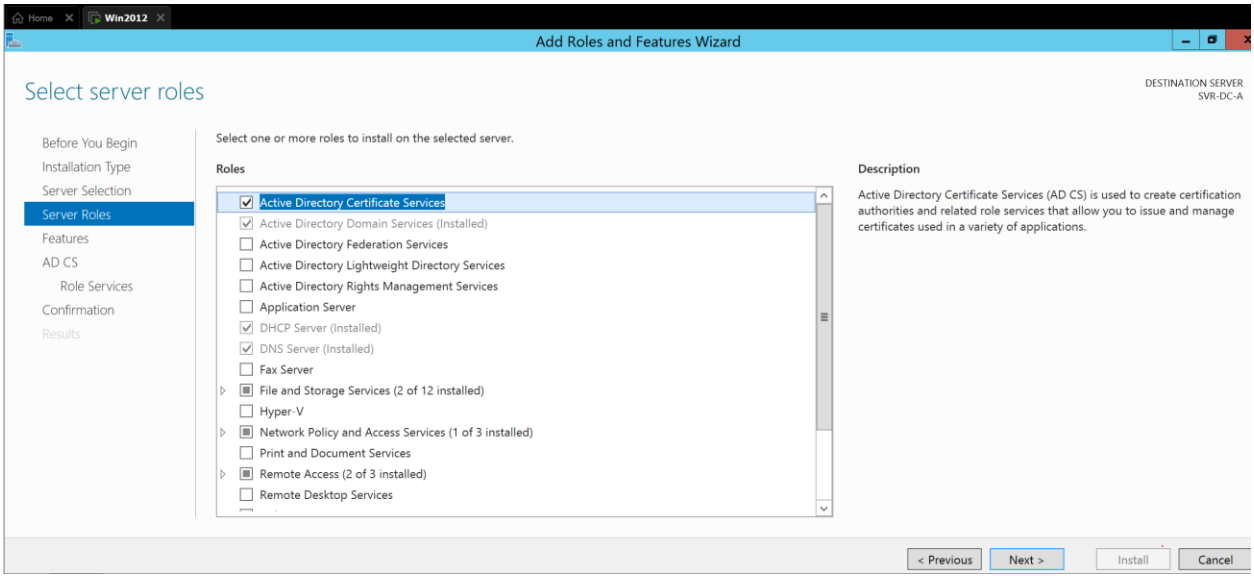
1. Install and configure Certificate Services on LON-DC1.

2. Open the Group Policy Management tool on LON-DC1 and configure automatic certificate enrollment.

3. Close all virtual machines and delete changes.

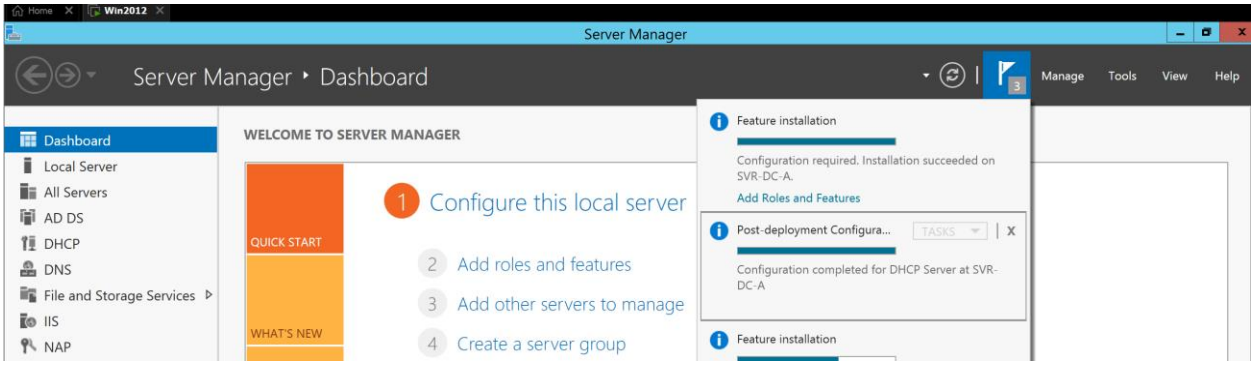
Install and configure Certificate Services on LON-DC1:

Select "Active Directory Certificate Services" from the list of roles to install.



Complete the installation process by following the wizard.

After installation, configure the Certificate Services by running the "Configure Active Directory Certificate Services" wizard.

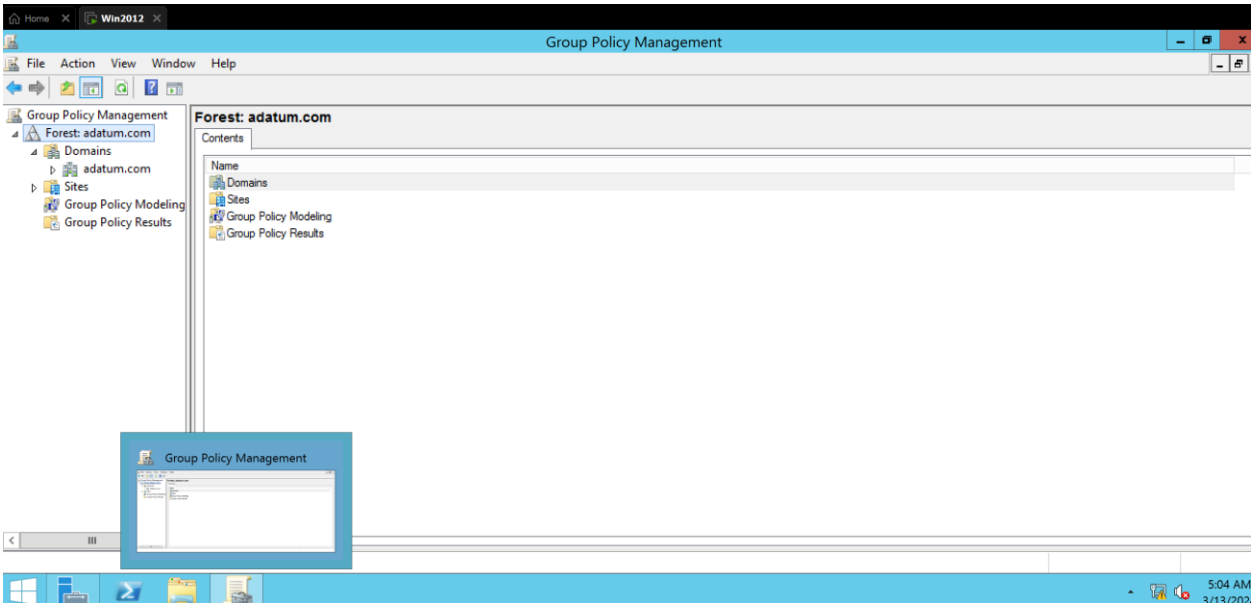


Follow the wizard to set up Certificate Authority and other necessary configurations. Ensure you choose the appropriate CA type (e.g., Enterprise CA) based on your network requirements.

Open the Group Policy Management tool on LON-DC1 and configure automatic certificate enrollment:

Open "Group Policy Management" from the administrative tools or search for it in the start menu.

Navigate to the appropriate Group Policy Object (GPO) that applies to the computers you want to configure for certificate auto-enrollment. You may need to create a new GPO if necessary.



Task 2: Open the Group Policy Management tool on LON-DC1 and configure automatic certificate

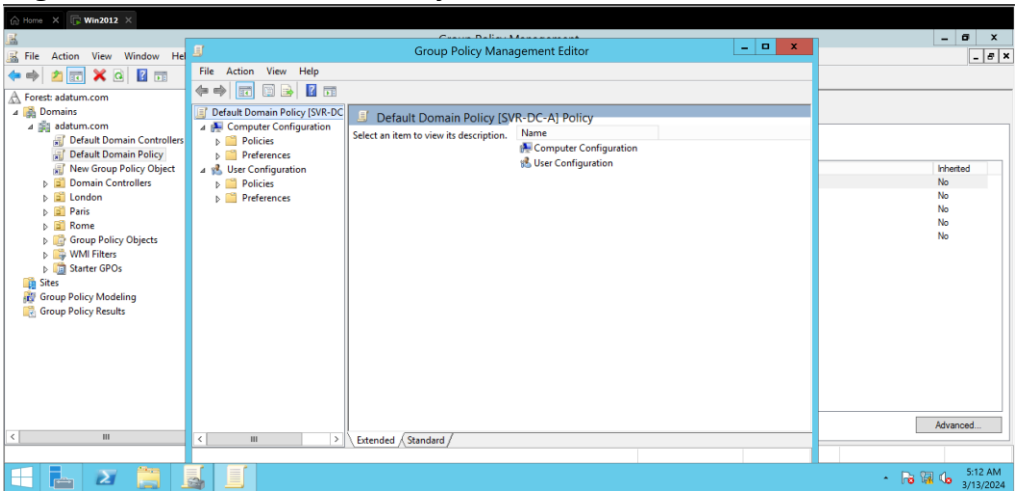
enrollment

1. On LON-DC1, open Group Policy Management from the Administrative Tools menu.

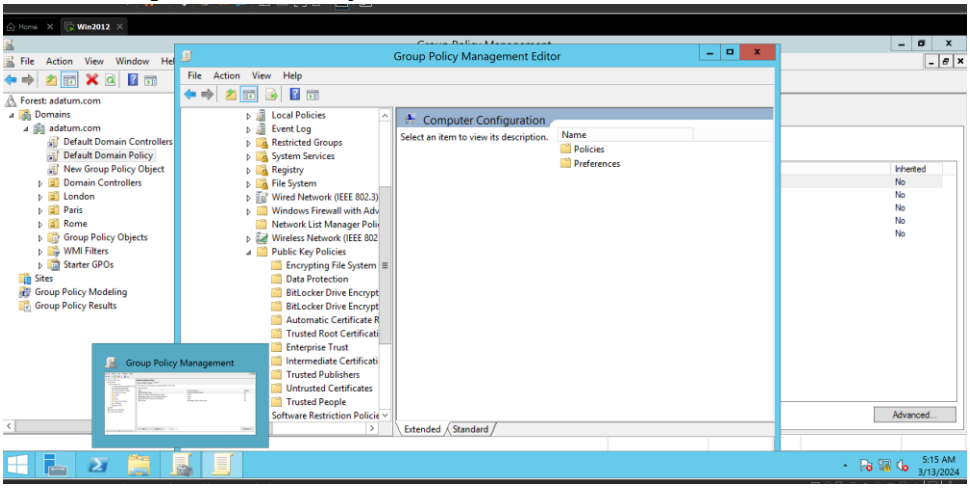
2. In the Group Policy Management tool, expand Forest: Adatum.com, expand Domains and expand

Adatum.com.

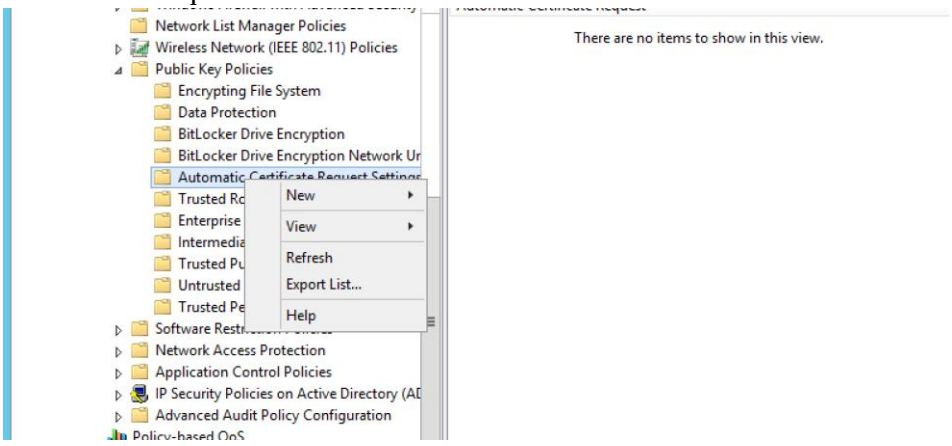
4. Right-click Default Domain Policy, and then click Edit.

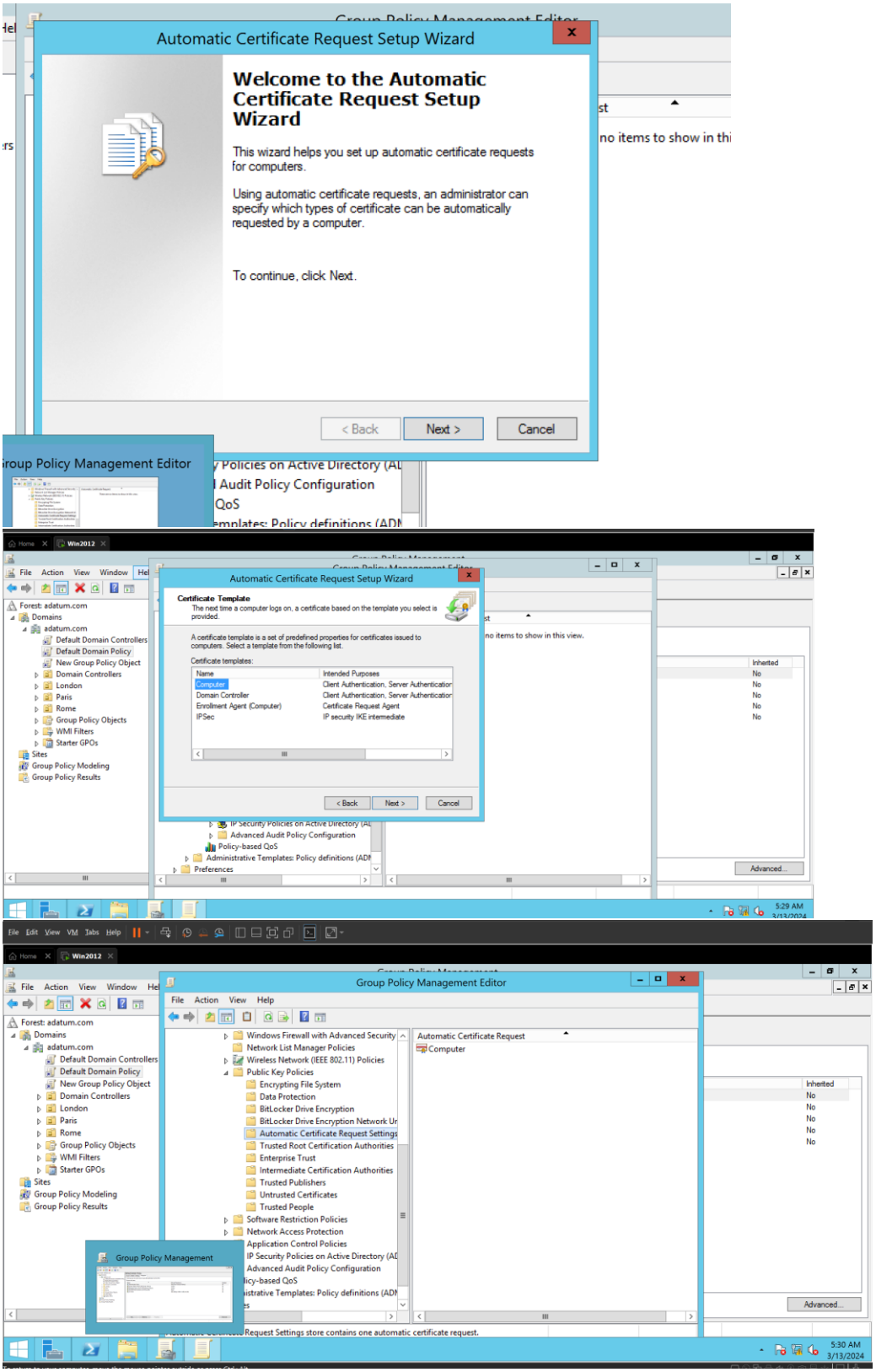


5. Expand Computer Configuration, expand Window Settings, expand Security Settings, and then expand Public Key Policies.



6. Right-click Automatic Certificate Request Settings, click New and then click Automatic Certificate Request.




Automatic Certificate Request Setup Wizard
Welcome to the Automatic Certificate Request Setup Wizard
This wizard helps you set up automatic certificate requests for computers.
Using automatic certificate requests, an administrator can specify which types of certificate can be automatically requested by a computer.
To continue, click Next.
< Back
Next >
Cancel
Group Policy Management Editor
Certificate Template
The next time a computer logs on, a certificate based on the template you select is provided.
A certificate template is a set of predefined properties for certificates issued to computers. Select a template from the following list.
Certificate templates:
Name
Intended Purposes
Computer
Client Authentication, Server Authentication
Domain Controller
Client Authentication, Server Authentication
Enrollment Agent (Computer)
Certificate Request Agent
IPSec
IP security IKE intermediate
Automatic Certificate Request
Computer
Group Policy Management
Advanced...

Conclusion:

In this lab, Network Policy Server (NPS) was successfully installed, configured, and integrated with Active Directory for centralized authentication and accounting, enabling secure remote access via RADIUS. Additionally, Certificate Services were deployed on LON-DC1 with automatic certificate enrollment configured via Group Policy Management, enhancing authentication with advanced certificate-based security measures.

References:

1- STONE, Gary N., LUNDY, Bert, et XIE, Geoffrey G. Network policy languages: a survey and a new approach. IEEE network, 2001, vol. 15, no 1, p. 10-21.
2- ENACEANU, Alexandru et GARAIS, Gabriel. Cost Effective RADIUS Authentication for Wireless Clients. Database Systems, 2010, vol. 27.
3- ERHARDT, Bill et CALVANO, Chuck. 2002 NPS Integrated Project-Expeditionary Warfare. Monterey, California: Naval Postgraduate School., 2014.
4- Sharma, S., Staessens, D., Colle, D., Pickavet, M., & Demeester, P. (2013). Automatic configuration of routing control platforms in OpenFlow networks. ACM SIGCOMM Computer Communication Review, 43(4), 491-492.