Lab: Configuring NAP and DHCP as an enforcement point

Objective

- Configure NAP for DHCP clients.

Logon Information

- Virtual Machines: LON-DC1, LON-SVR1, and LON-CL1
- User Name: Adatum\Administrator
- Password: Pa$$w0rd

Scenario

As the Adatum Bank Technology Specialist, you have been tasked with automatically bringing client computers into compliance by using Network Policy Server, creating client compliance policies and configuring a NAP server to check computers' current health.

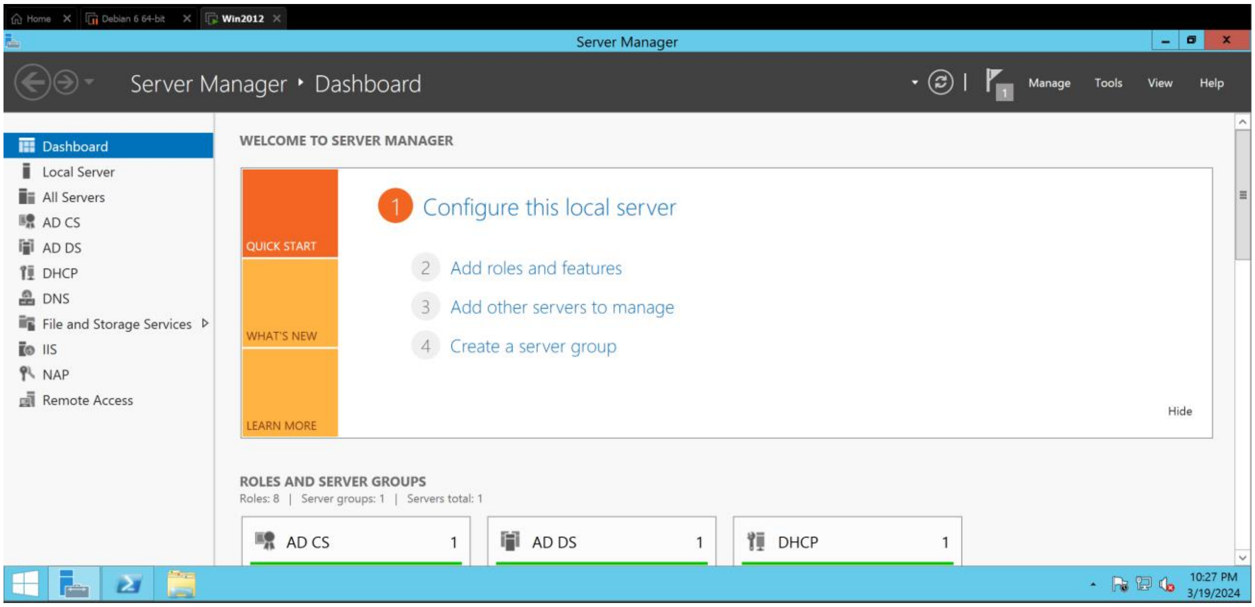
Exercise 1: Configuring NAP for DHCP Clients

In this exercise, you will configure and test NAP for DHCP clients.

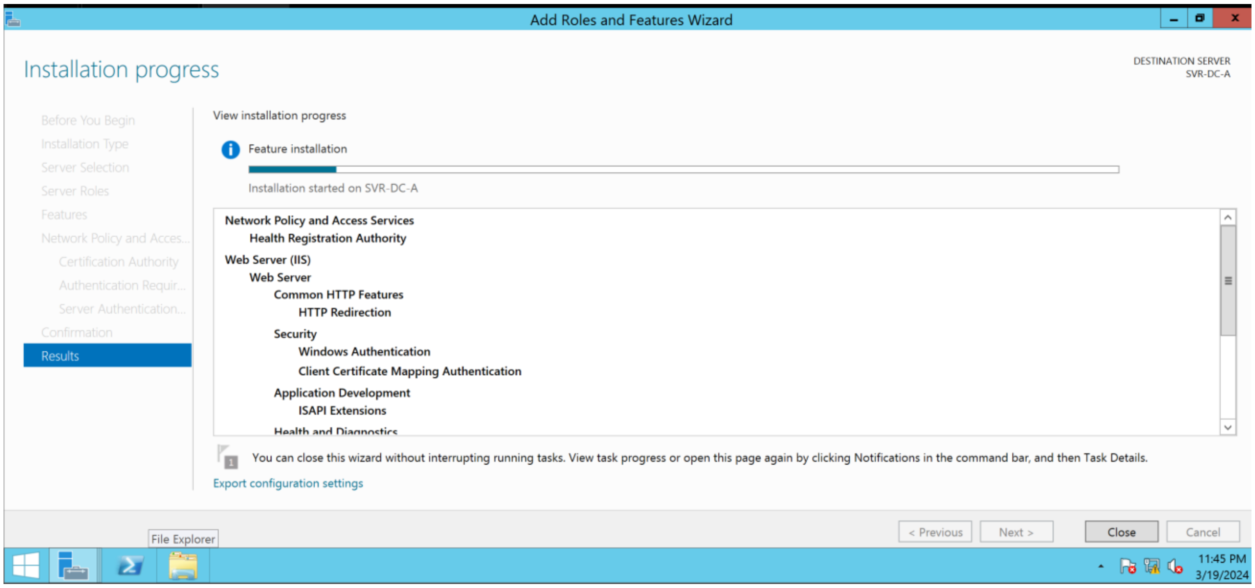
The main tasks are as follows:

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

2. Open the Server Manager tool on LON-SVR1.



3. Install the DHCP and NPS server roles.



Installation progress

View installation progress

Feature installation

Installation started on SVR-DC-A

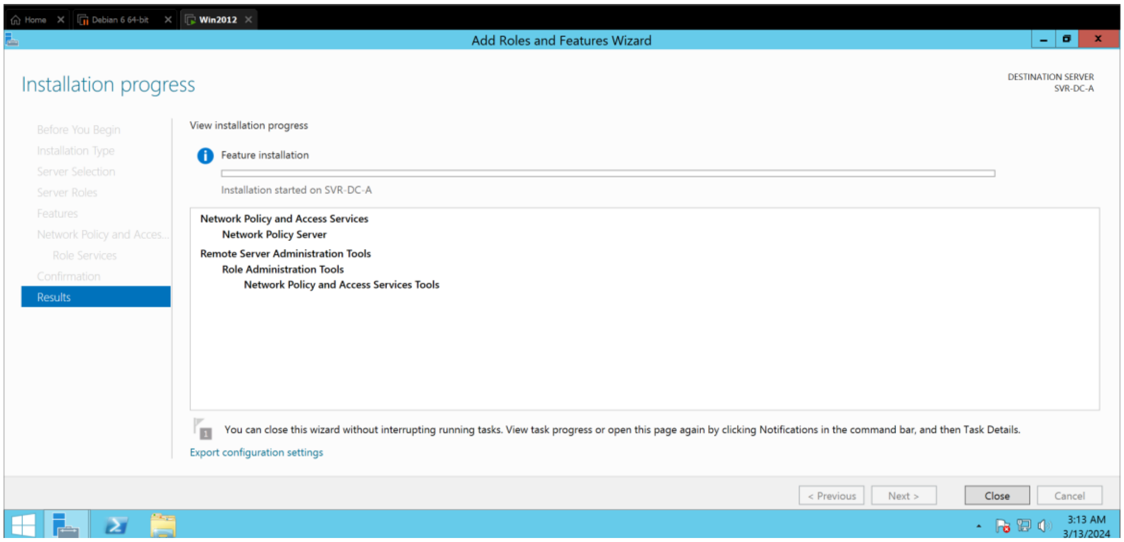
```
Network Policy and Access Services
    Health Registration Authority
Web Server (IIS)
    Web Server
        Common HTTP Features
            HTTP Redirection
        Security
            Windows Authentication
            Client Certificate Mapping Authentication
        Application Development
            ISAPI Extensions
        Health and Diagnostics
```

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

4. Configure LON-SVR1 as a NAP health policy server.

5. Configure DHCP service for NAP enforcement.



Installation progress

View installation progress

Feature installation

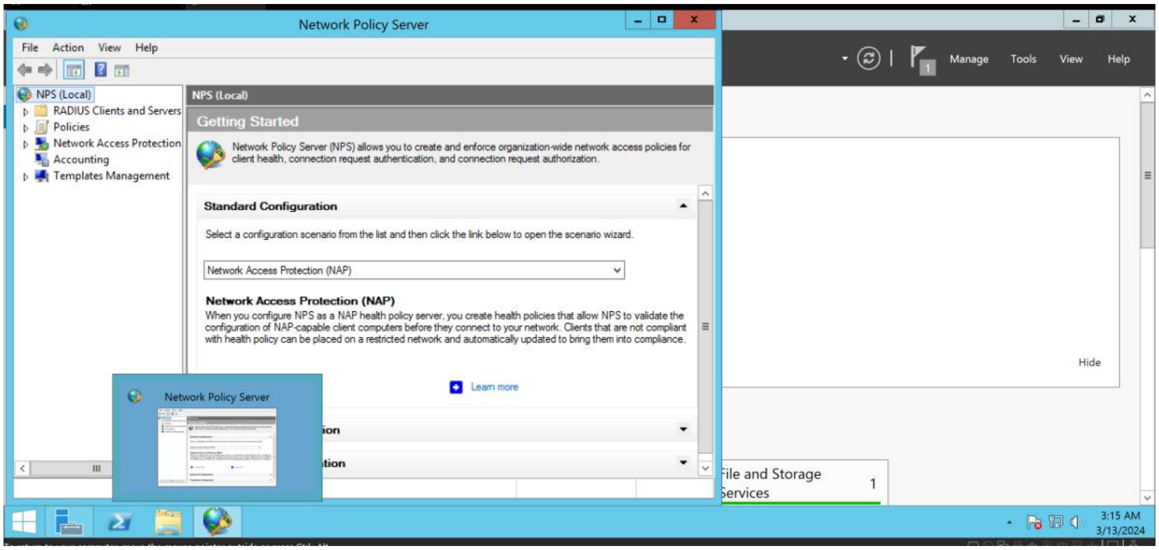
Installation started on SVR-DC-A

```
Network Policy and Access Services
    Network Policy Server
Remote Server Administration Tools
    Role Administration Tools
        Network Policy and Access Services Tools
```

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

6. Configure LON-CL1 as a DHCP and NAP client.



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

Network Access Protection (NAP)

Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

7. Test NAP enforcement.

8. Shut down the virtual machines and do not save changes.

Task 1: Ensure that you have read the installation steps

Task 2: Open the Server Manager tool on LON-SVR1

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

Task 3: Install the NPS and DHCP server roles

1. On LON-SVR1, open Server Manager.

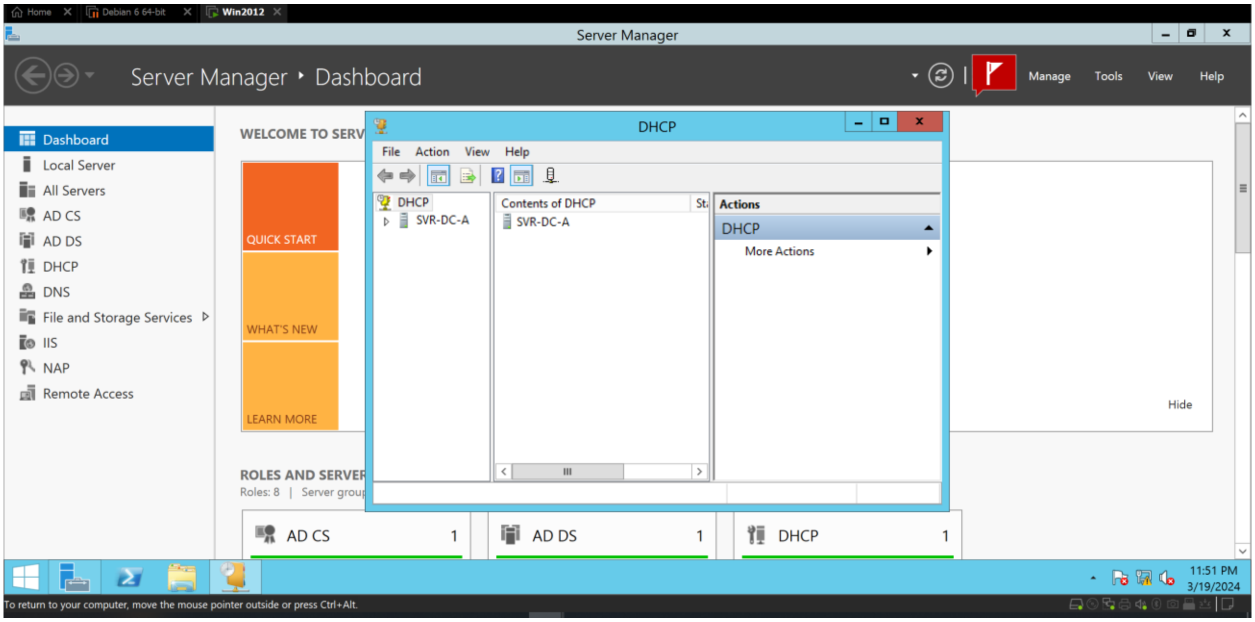
2. Right-click Roles, and then click Add Roles.

3. On the Select Server Roles page, select the DHCP Server and Network Policy and Access Services check boxes.

4. On the Select Role Services page, select the Network Policy Server.

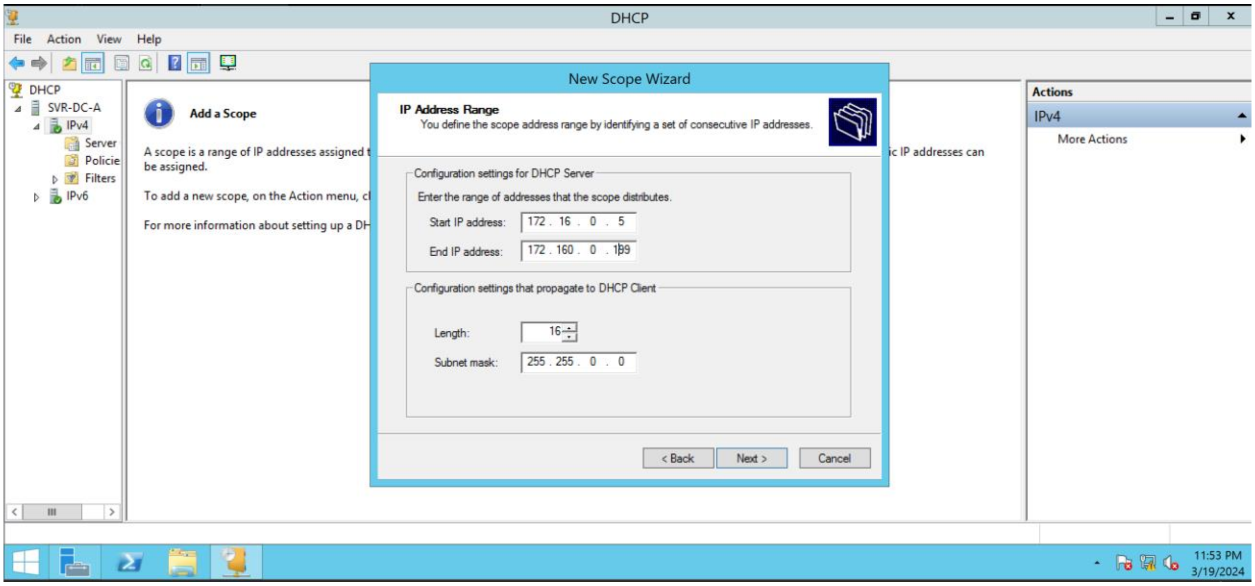
5. Authorize the DHCP Server

6. Configure DHCP Scope (go to tools> DHCP)



7. Right click On IPv4, and click on Add new Scope .

8. In the Add Scope dialog box, type NAP Scope next to Scope Name. Next to Starting IP Address, type 172.16.0.50, next to Ending IP Address type 172.16.0.199, and next to Subnet Mask type 255.255.0.0.



A scope is a range of IP addresses assigned t
be assigned.

To add a new scope, on the Action menu, cl

For more information about setting up a DH

ic IP addresses can

IP Address Range

You define the scope address range by identifying a set of consecutive IP addresses.

Configuration settings for DHCP Server

Enter the range of addresses that the scope distributes.

Start IP address: 172 . 16 . 0 . 5

End IP address: 172 . 160 . 0 . 199

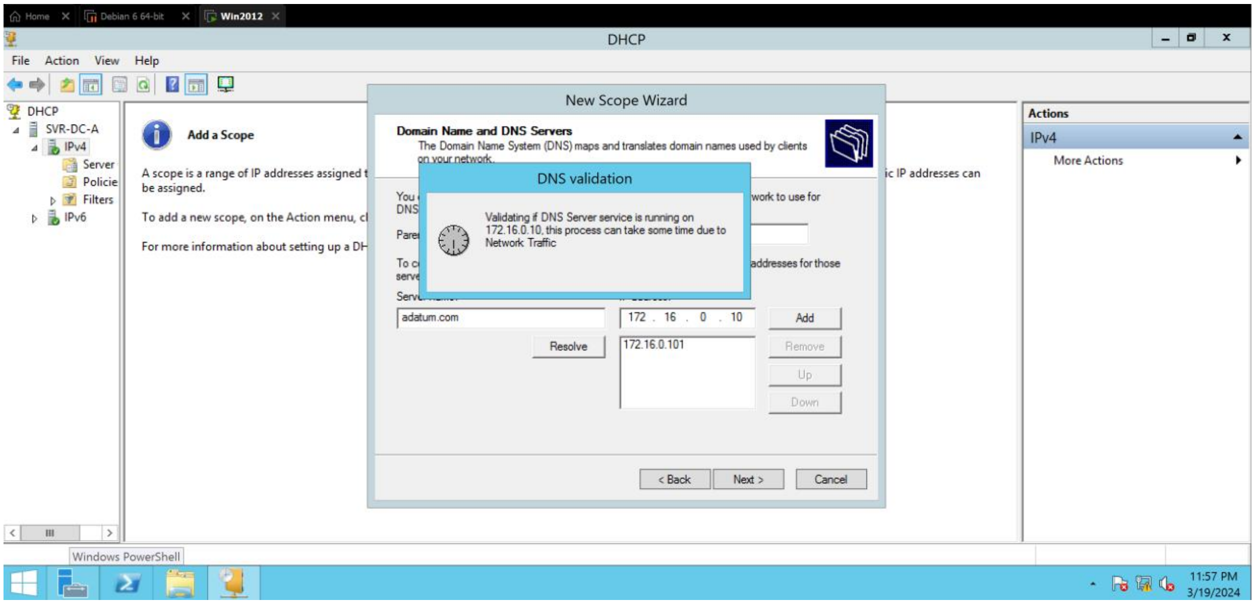
Configuration settings that propagate to DHCP Client

Length: 16

Subnet mask: 255 . 255 . 0 . 0

9. On the Specify DNS Server Settings page, verify that adatum.com is listed under Parent domain.

10. Type 172.16.0.10 under Preferred DNS server IP address, and click Next. Verify that the result returned is Valid.



Add a Scope

A scope is a range of IP addresses assigned t… be assigned.

To add a new scope, on the Action menu, cl…

For more information about setting up a DH…

New Scope Wizard

Domain Name and DNS Servers

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

DNS validation

Validating if DNS Server service is running on 172.16.0.10, this process can take some time due to Network Traffic

Server name: adatum.com

IP address: 172 . 16 . 0 . 10

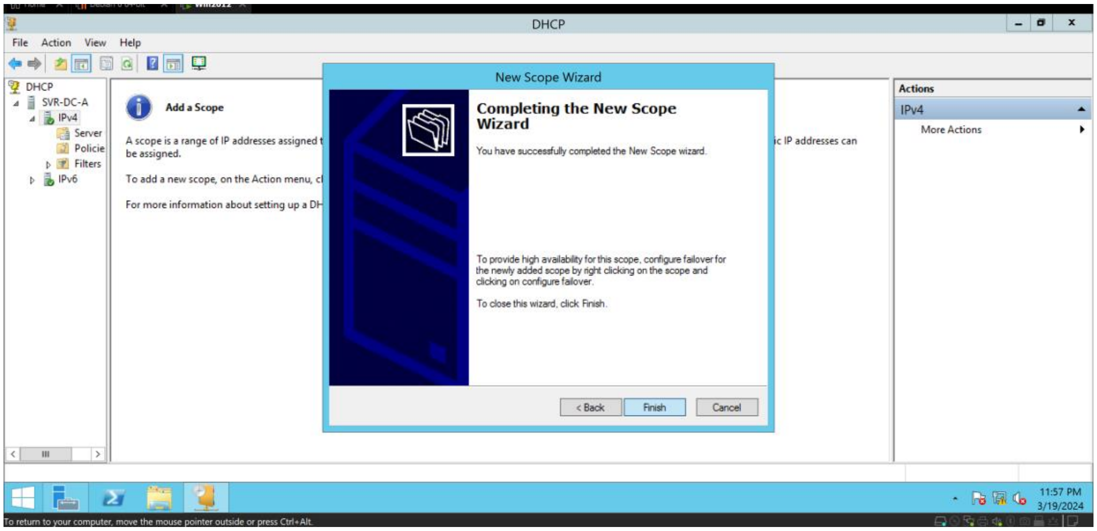
172.16.0.101

11. On the Specify WINS Server Settings page, accept the default setting.

12. Select the Activate this scope check box, and then click OK.

13. On the Confirm Installation Selections page, click Install.

14. Verify the installation was successful, and then click Close.



Add a Scope

A scope is a range of IP addresses assigned t… be assigned.

To add a new scope, on the Action menu, cl…

For more information about setting up a DH…

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.

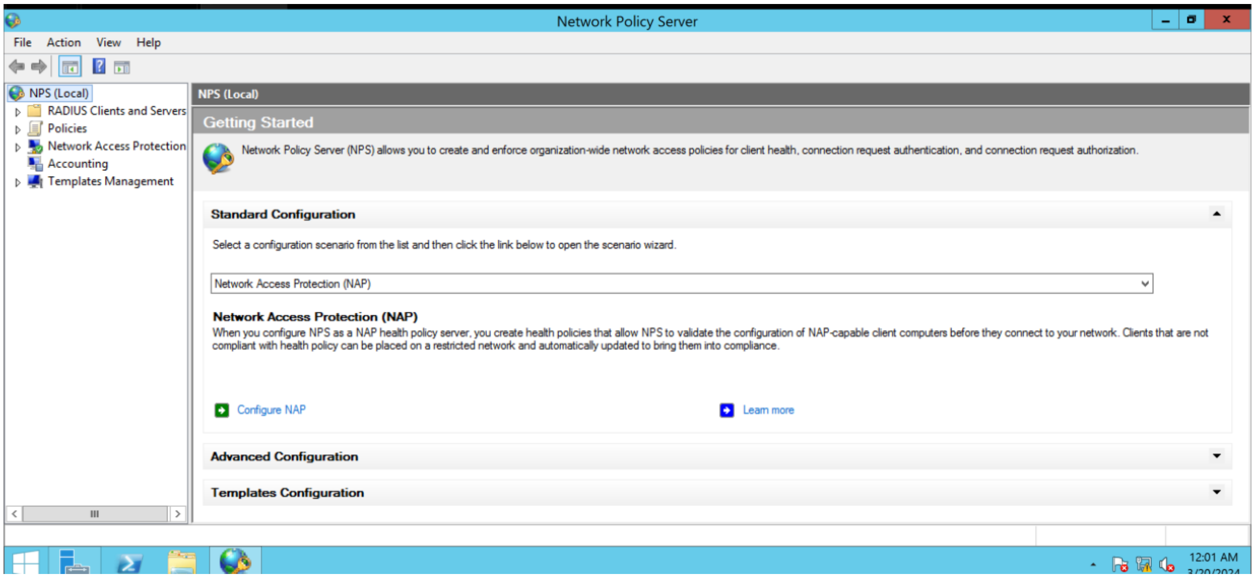
To close this wizard, click Finish.

To return to your computer, move the mouse pointer outside or press Ctrl+Alt.

15. Close the Server Manager window.

<u>Task 4: Configure LON-SVR1 as a NAP health policy server</u>

1. Open the Network Policy Server administrative tool from the Start Menu, Administrative Tools location.



Network Policy Server (NPS) allows you to create and enforce organization-wide network access policies for client health, connection request authentication, and connection request authorization.

Select a configuration scenario from the list and then click the link below to open the scenario wizard.

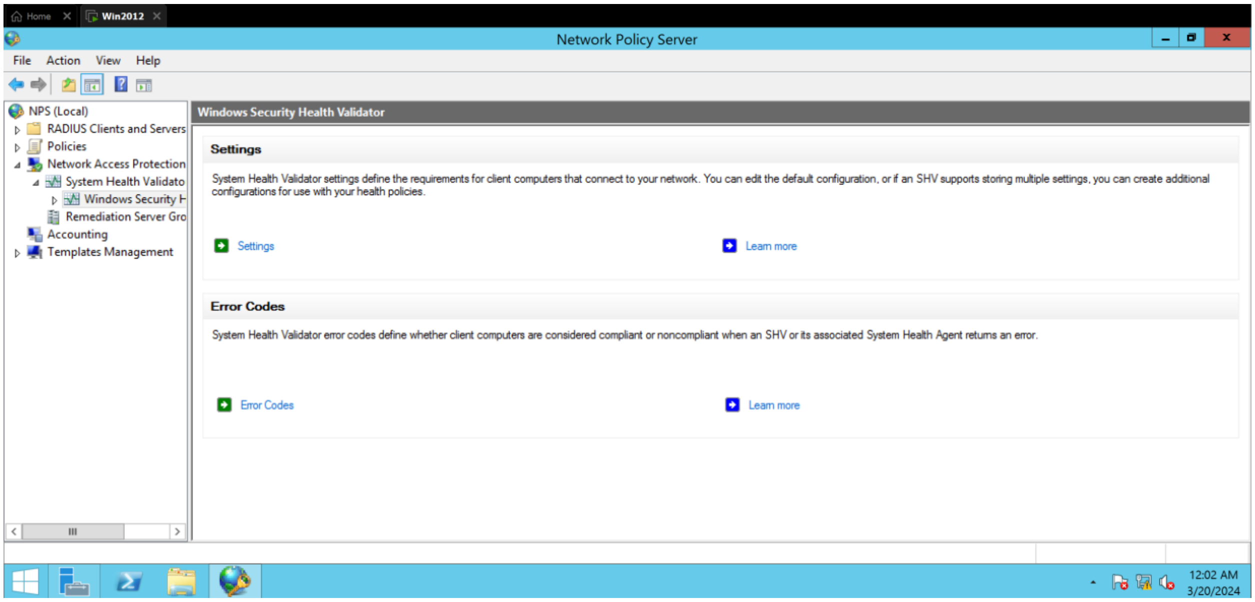
Network Access Protection (NAP)

Network Access Protection (NAP)

When you configure NPS as a NAP health policy server, you create health policies that allow NPS to validate the configuration of NAP-capable client computers before they connect to your network. Clients that are not compliant with health policy can be placed on a restricted network and automatically updated to bring them into compliance.

2. Configure SHVs:

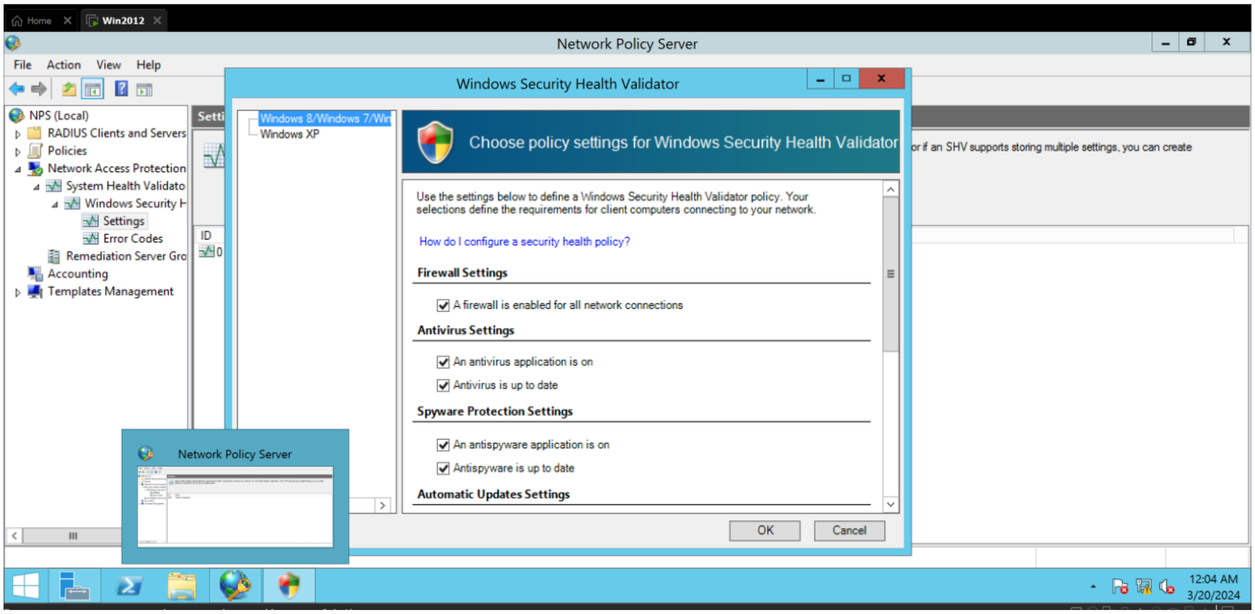
a. Expand Network Access Protection, and then click System Health Validators.



System Health Validator settings define the requirements for client computers that connect to your network. You can edit the default configuration, or if an SHV supports storing multiple settings, you can create additional configurations for use with your health policies.

System Health Validator error codes define whether client computers are considered compliant or noncompliant when an SHV or its associated System Health Agent returns an error.

b. Configure the System Health Validator. Clear all check boxes except A firewall is enabled for all network connections. You do not have to clear the Windows Update check box.



Windows Security Health Validator

Choose policy settings for Windows Security Health Validator

Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.

How do I configure a security health policy?

Firewall Settings

☑ A firewall is enabled for all network connections

Antivirus Settings

☑ An antivirus application is on

☑ Antivirus is up to date

Spyware Protection Settings

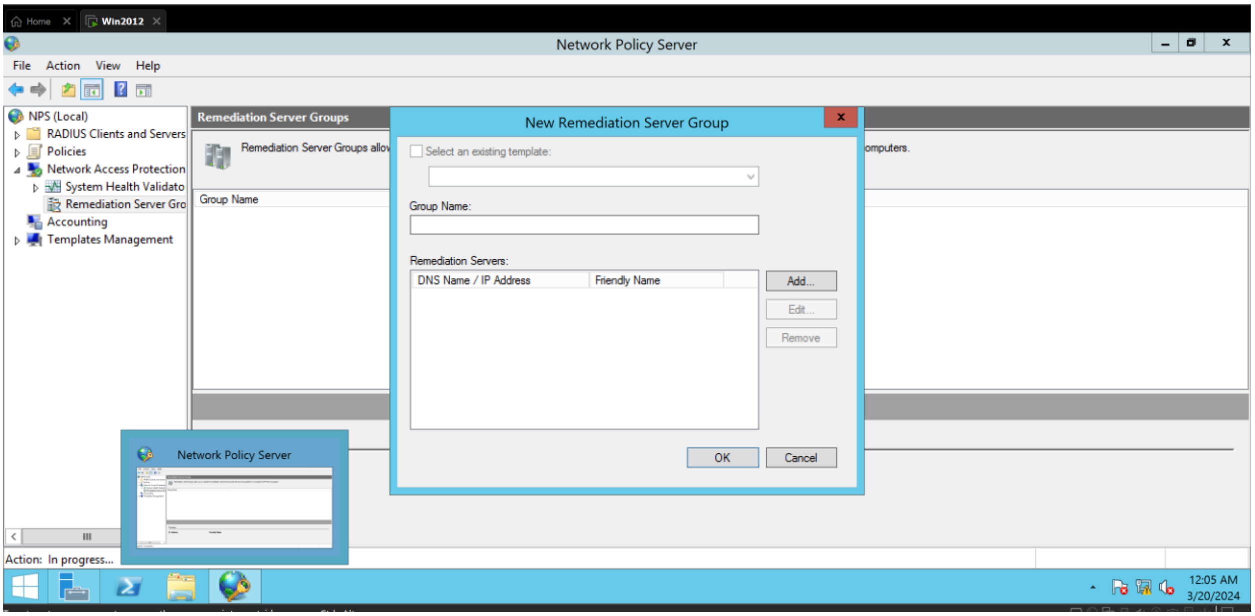
☑ An antispyware application is on

☑ Antispyware is up to date

Automatic Updates Settings

3. Configure remediation server groups:

a. In the console tree, under Network Access Protection, right-click Remediation Server Groups, and then click New.



New Remediation Server Group

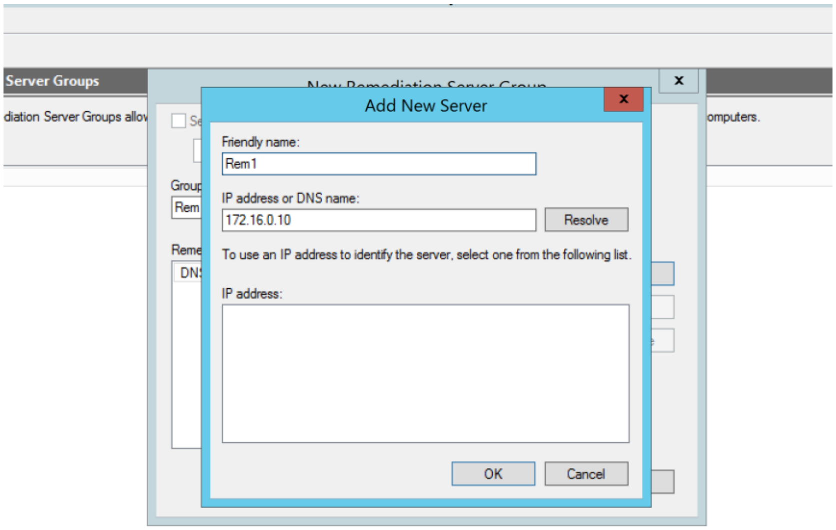
☐ Select an existing template:

Group Name:

Remediation Servers:

DNS Name / IP Address	Friendly Name

b. Create a new remediation group with a group name of Rem1 and add the IP address of 172.16.0.10



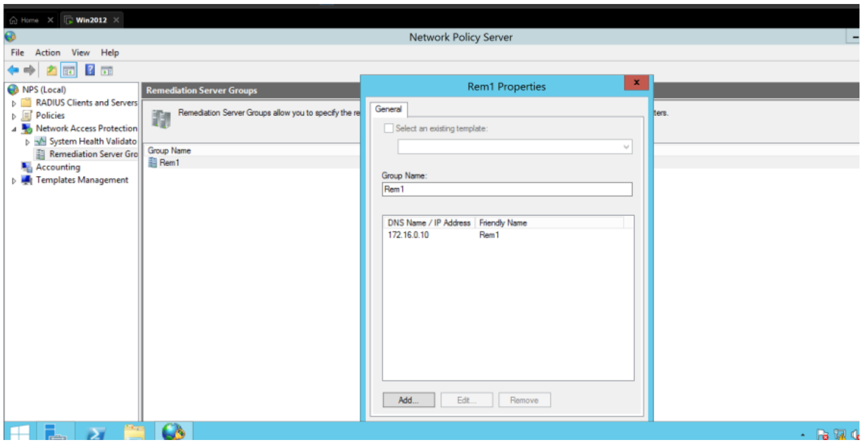
Add New Server

Friendly name: Rem1

IP address or DNS name: 172.16.0.10

To use an IP address to identify the server, select one from the following list.

IP address:



Rem1 Properties

Remediation Server Groups allow you to specify the re

□ Select an existing template:

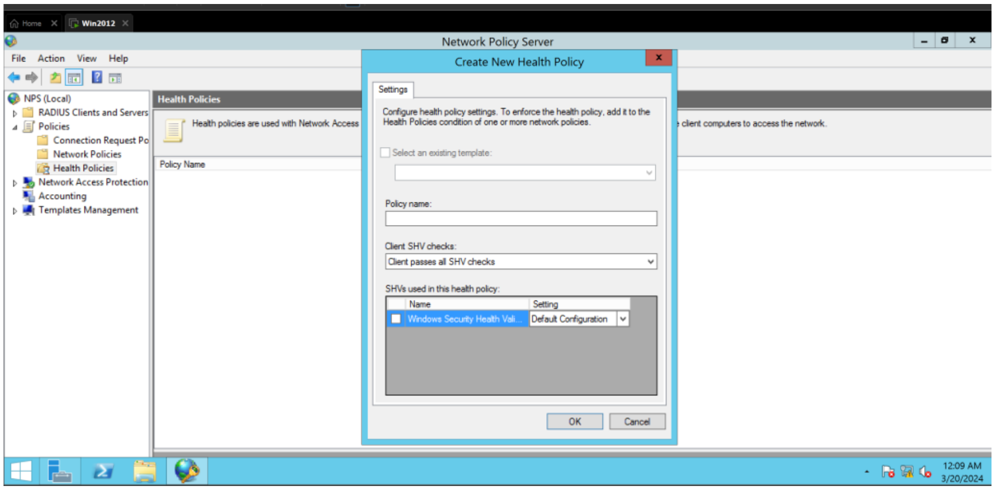
Group Name: Rem1

DNS Name / IP Address	Friendly Name
172.16.0.10	Rem1

4. Configure health policies:

a. Expand Policies.

b. Right-click Health Policies, and then click New.



Create New Health Policy

Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.

Health policies are used with Network Access … client computers to access the network.

□ Select an existing template:

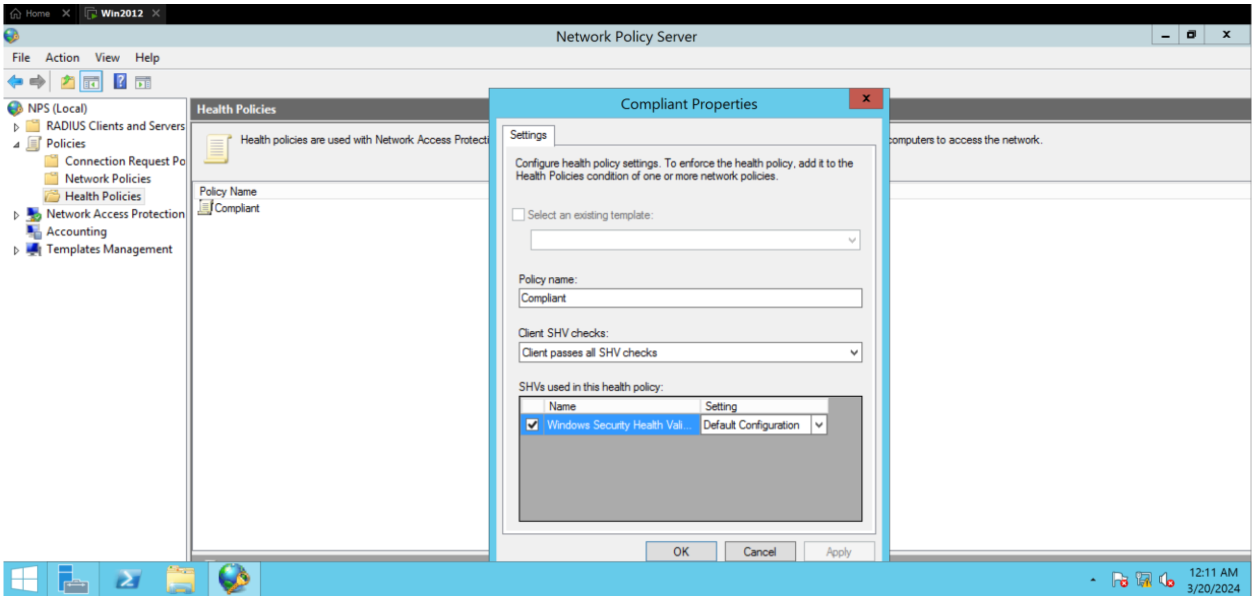
Policy name:

Client SHV checks: Client passes all SHV checks

SHVs used in this health policy:

	Name	Setting
□	Windows Security Health Vali...	Default Configuration

c. Create a new health policy called Compliant that specifies the Client passes all SHV checks and uses the Windows Security Health Validator.



Compliant Properties

Settings

Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.

□ Select an existing template:

Policy name: Compliant

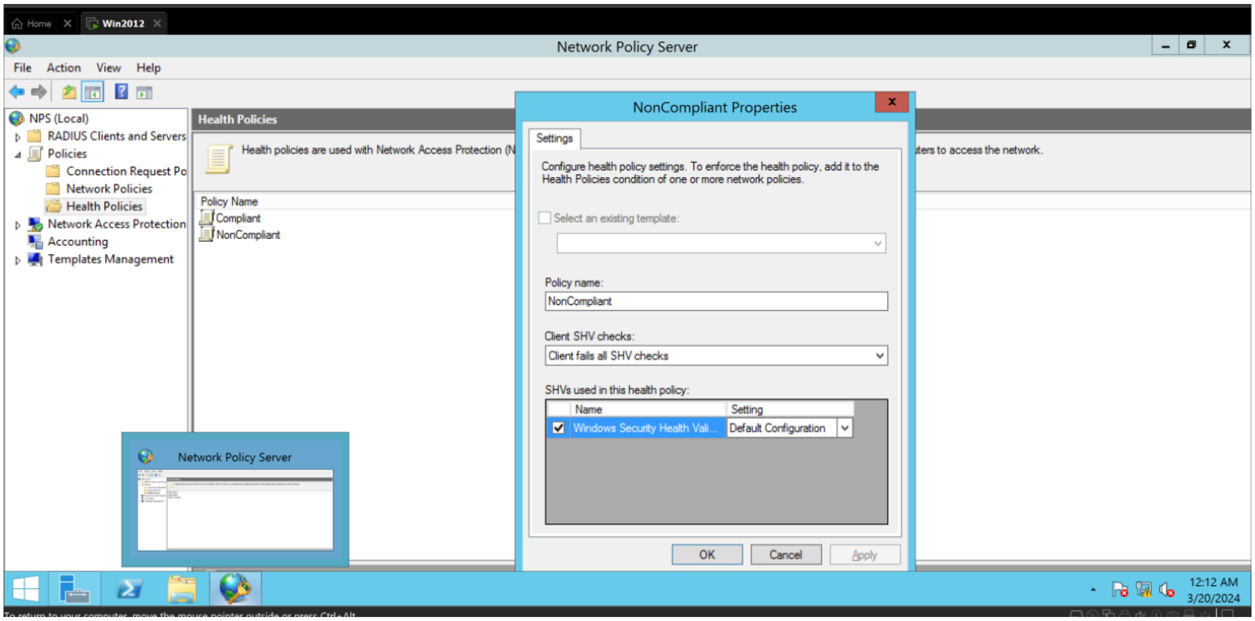
Client SHV checks: Client passes all SHV checks

SHVs used in this health policy:

	Name	Setting
☑	Windows Security Health Vali...	Default Configuration

d. Right-click Health Policies, and then click New.

e. Create a new health policy called NonCompliant that specifies the Client fails one or more SHV checks and uses the Windows Security Health Validator.



NonCompliant Properties

Settings

Configure health policy settings. To enforce the health policy, add it to the Health Policies condition of one or more network policies.

□ Select an existing template:

Policy name: NonCompliant

Client SHV checks: Client fails all SHV checks

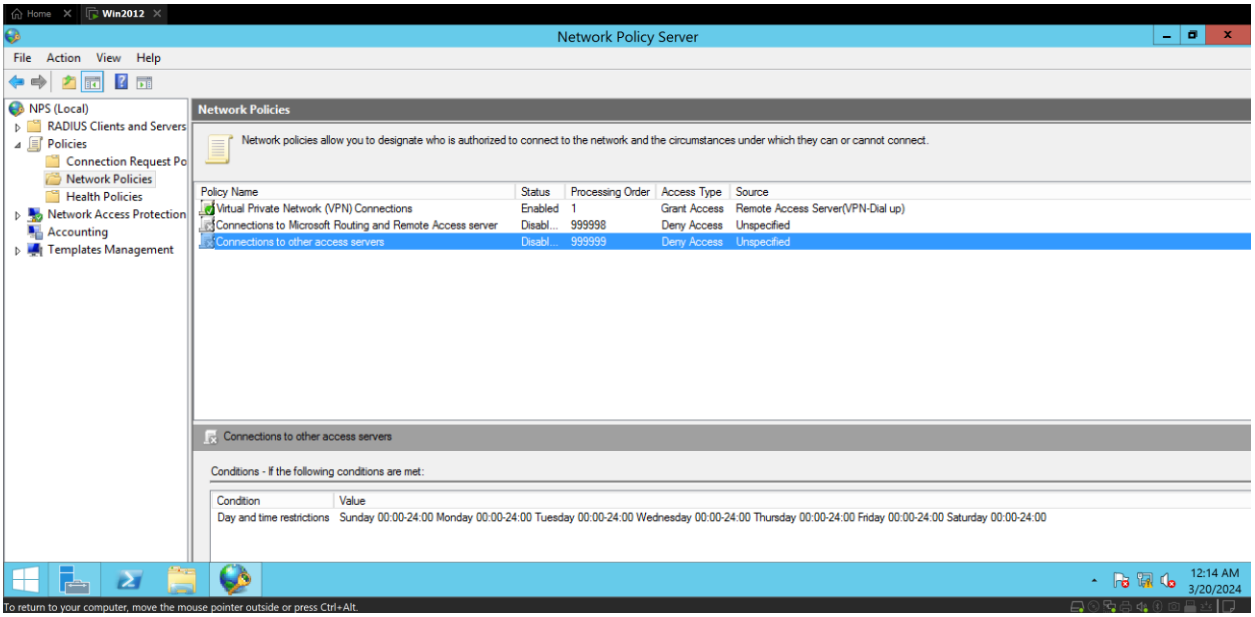
SHVs used in this health policy:

	Name	Setting
☑	Windows Security Health Vali...	Default Configuration

5. Configure a network policy for compliant computers:

a. In the console tree, under Policies, click Network Policies.

b. Disable the two default policies under Policy Name.



Network Policies

Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Virtual Private Network (VPN) Connections	Enabled	1	Grant Access	Remote Access Server(VPN-Dial up)
Connections to Microsoft Routing and Remote Access server	Disabl...	999998	Deny Access	Unspecified
Connections to other access servers	Disabl...	999999	Deny Access	Unspecified

Connections to other access servers

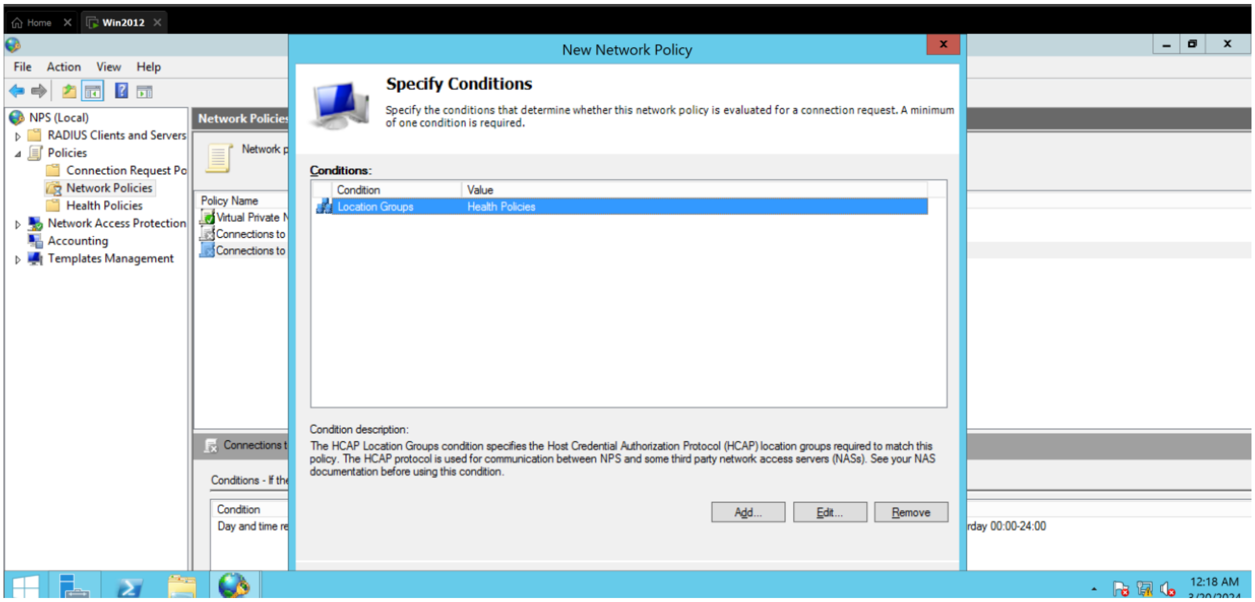
Conditions - If the following conditions are met:

Condition	Value
Day and time restrictions	Sunday 00:00-24:00 Monday 00:00-24:00 Tuesday 00:00-24:00 Wednesday 00:00-24:00 Thursday 00:00-24:00 Friday 00:00-24:00 Saturday 00:00-24:00

c. Create a new Network Policy called Compliant-Full-Access.

d. In the Specify Conditions window, click Add.

e. In the Select condition dialog box, double-click Health Policies, select Compliant, and then click OK.



New Network Policy

Specify Conditions

Specify the conditions that determine whether this network policy is evaluated for a connection request. A minimum of one condition is required.

Conditions:

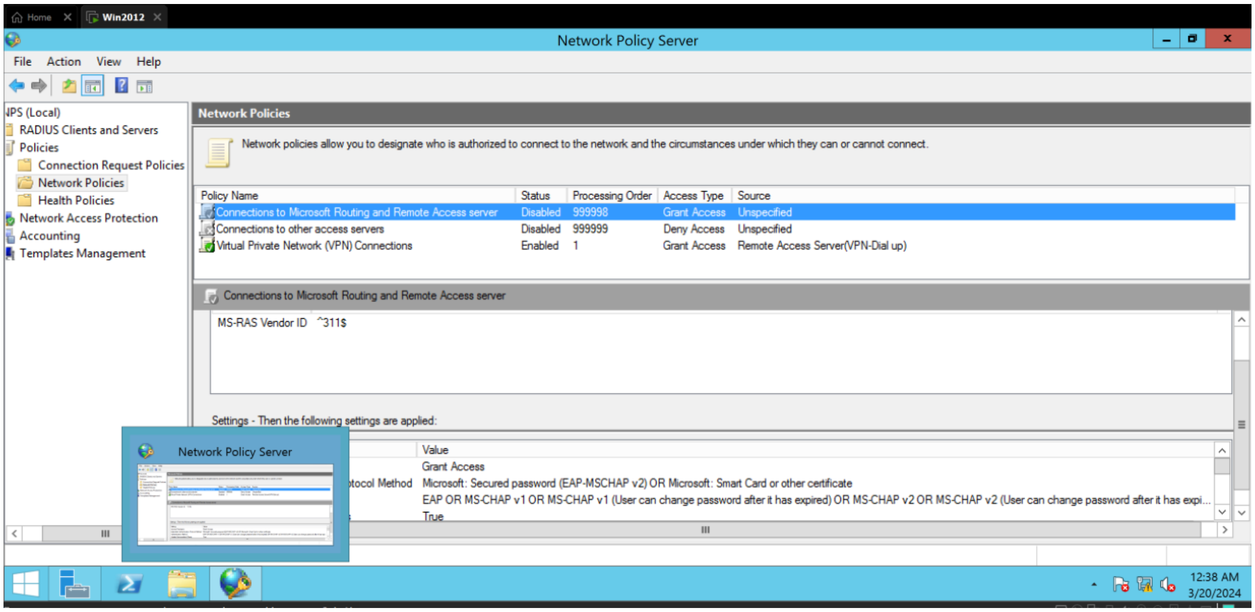
Condition	Value
Location Groups	Health Policies

Condition description:

The HCAP Location Groups condition specifies the Host Credential Authorization Protocol (HCAP) location groups required to match this policy. The HCAP protocol is used for communication between NPS and some third party network access servers (NASs). See your NAS documentation before using this condition.

f. In the Specify Access Permission window, verify that Access granted is selected.

g. In the Configure Authentication Methods window, select the Perform machine health check only check box. Clear all other check boxes. h. In the Configure Settings window, click NAP Enforcement. Verify that Allow full network access is selected.



Network policies allow you to designate who is authorized to connect to the network and the circumstances under which they can or cannot connect.

Policy Name	Status	Processing Order	Access Type	Source
Connections to Microsoft Routing and Remote Access server	Disabled	999998	Grant Access	Unspecified
Connections to other access servers	Disabled	999999	Deny Access	Unspecified
Virtual Private Network (VPN) Connections	Enabled	1	Grant Access	Remote Access Server(VPN-Dial up)

Connections to Microsoft Routing and Remote Access server

MS-RAS Vendor ID ^311$

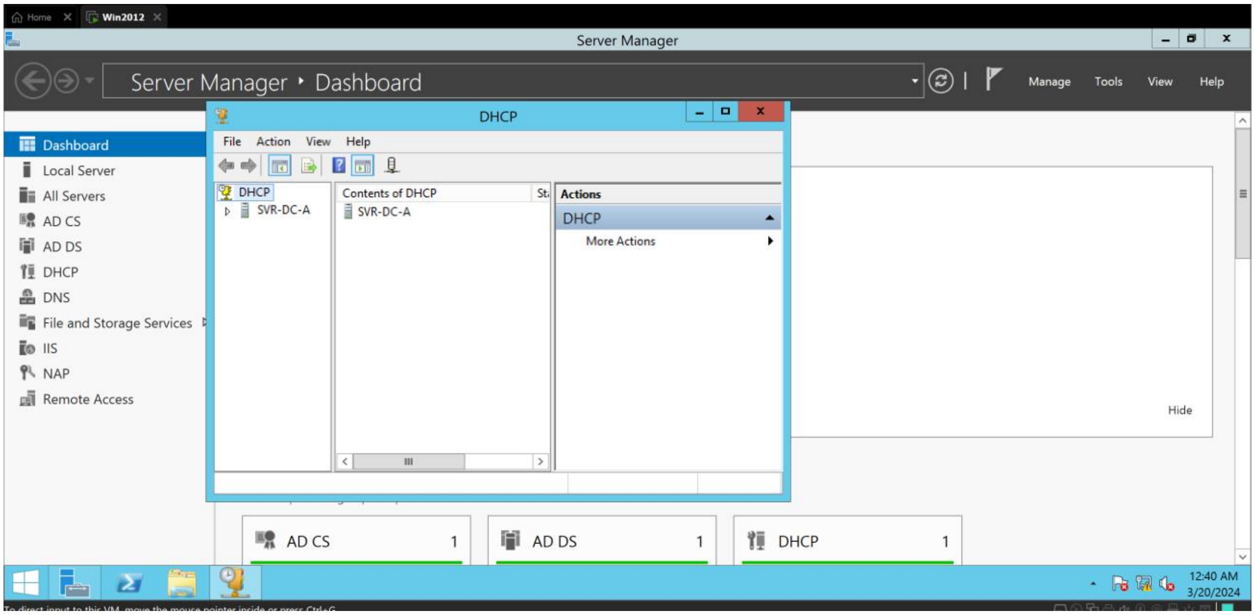
Settings - Then the following settings are applied:

	Value
	Grant Access
tocol Method	Microsoft: Secured password (EAP-MSCHAP v2) OR Microsoft: Smart Card or other certificate
	EAP OR MS-CHAP v1 OR MS-CHAP v1 (User can change password after it has expired) OR MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expi...
	True

i. In the Completing New Network Policy window, click Finish to complete configuration of your network policy for compliant client computers.

Task 5: Configure DHCP service for NAP enforcement

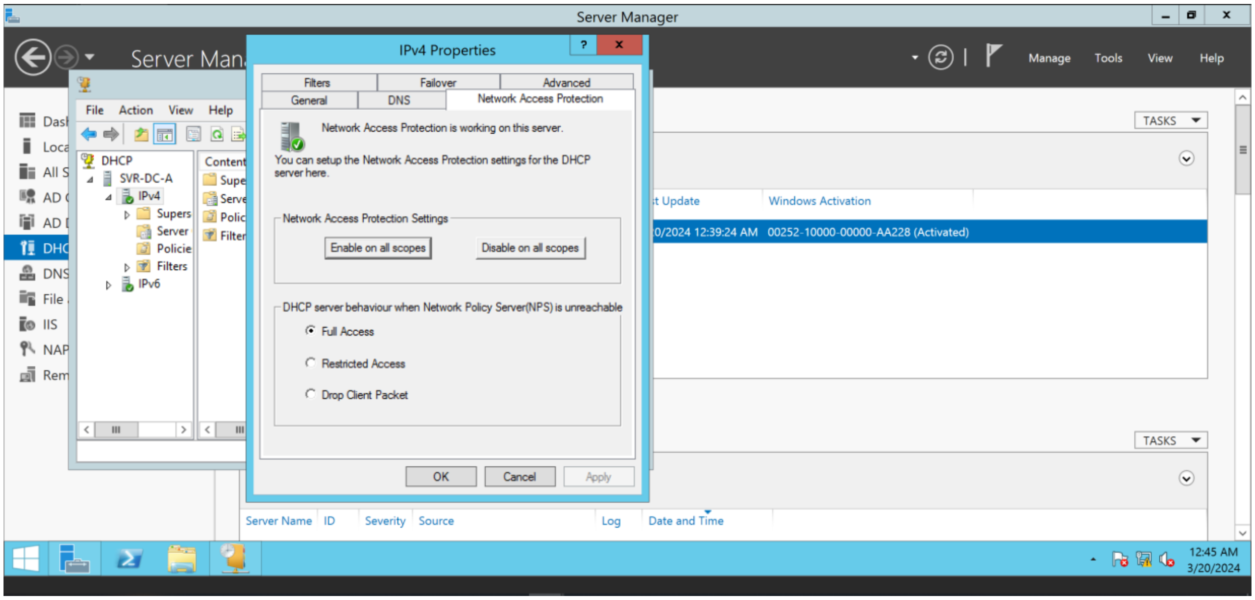
1. On LON-SVR1, open the DHCP Management console by typing dhcpmgmt.msc in the Run box, and then pressing ENTER.



2. In the DHCP Management console, expand LON-SVR1.adatum.com, and then expand IPv4.

3. Open the Properties for the Scope. On the Network Access Protection tab, verify Use

default Network Access Protection profile is selected, and then click OK.



IPv4 Properties

Filters | Failover | Advanced | General | DNS | Network Access Protection

Network Access Protection is working on this server.

You can setup the Network Access Protection settings for the DHCP server here.

Network Access Protection Settings

Enable on all scopes | Disable on all scopes

DHCP server behaviour when Network Policy Server(NPS) is unreachable

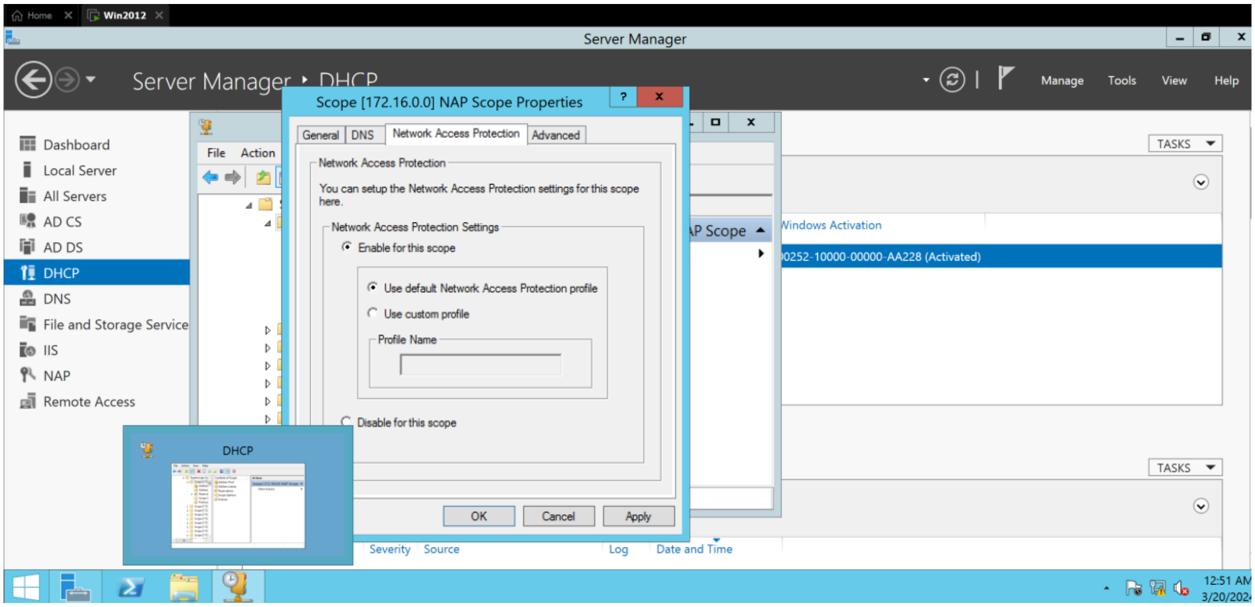
● Full Access

○ Restricted Access

○ Drop Client Packet

OK | Cancel | Apply

4. In the DHCP Management console, configure Scope Options.



Scope [172.16.0.0] NAP Scope Properties

General | DNS | Network Access Protection | Advanced

Network Access Protection

You can setup the Network Access Protection settings for this scope here.

Network Access Protection Settings

● Enable for this scope

● Use default Network Access Protection profile

○ Use custom profile

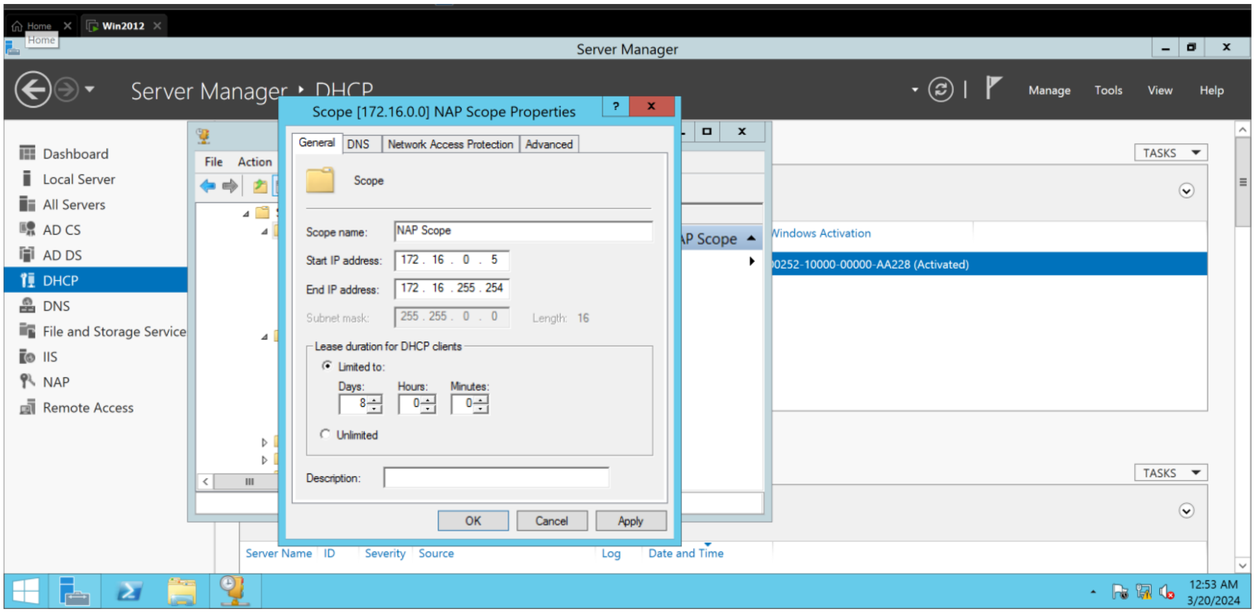
Profile Name

○ Disable for this scope

OK | Cancel | Apply

5. Click on the Advanced tab.

6. Under Available Options, select the 003 Router check box, type 172.16.0.1 in IP Address, select the 015 DNS Domain Name check box, type Adatum.com in String value, and then click OK.



Scope [172.16.0.0] NAP Scope Properties

General | DNS | Network Access Protection | Advanced

Scope

Scope name: NAP Scope

Start IP address: 172 . 16 . 0 . 5

End IP address: 172 . 16 . 255 . 254

Subnet mask: 255 . 255 . 0 . 0 Length: 16

Lease duration for DHCP clients

● Limited to:

Days: 8 Hours: 0 Minutes: 0

○ Unlimited

Description:

Task 6: Configure LON-CL1 as a DHCP and NAP client

1. On LON-CL1, enable Security Centre:

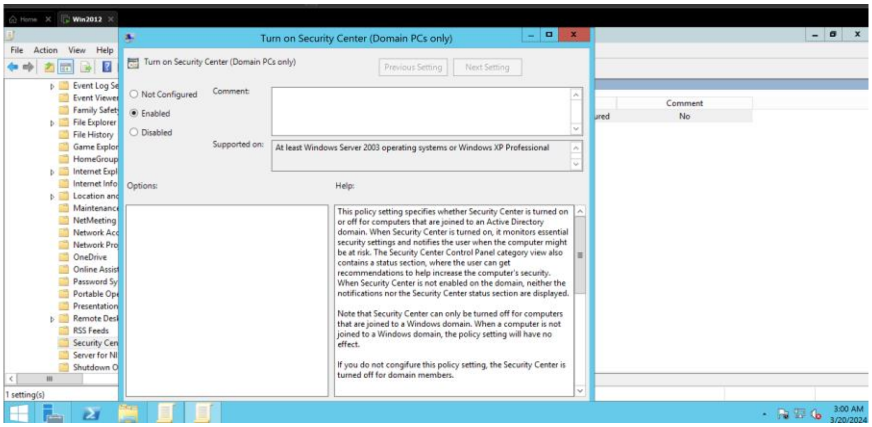
a. Click Start, point to All Programs, click Accessories, and then click Run.

b. Type gpedit.msc, and then press ENTER.

c. In the console tree, open Local Computer Policy/Computer Configuration/Administrative Templates/Windows Components/Security Center.

d. Double-click Turn on Security Center (Domain PCs only), click Enabled, and then click OK.

e. Close the console window. When prompted to save settings, click No.



Turn on Security Center (Domain PCs only)

○ Not Configured
● Enabled
○ Disabled

Comment:

Supported on: At least Windows Server 2003 operating systems or Windows XP Professional

Options:

Help:

This policy setting specifies whether Security Center is turned on or off for computers that are joined to an Active Directory domain. When Security Center is turned on, it monitors essential security settings and notifies the user when the computer might be at risk. The Security Center Control Panel category view also contains a status section, where the user can get recommendations to help increase the computer's security. When Security Center is not enabled on the domain, neither the notifications nor the Security Center status section are displayed.

Note that Security Center can only be turned off for computers that are joined to a Windows domain. When a computer is not joined to a Windows domain, the policy setting will have no effect.

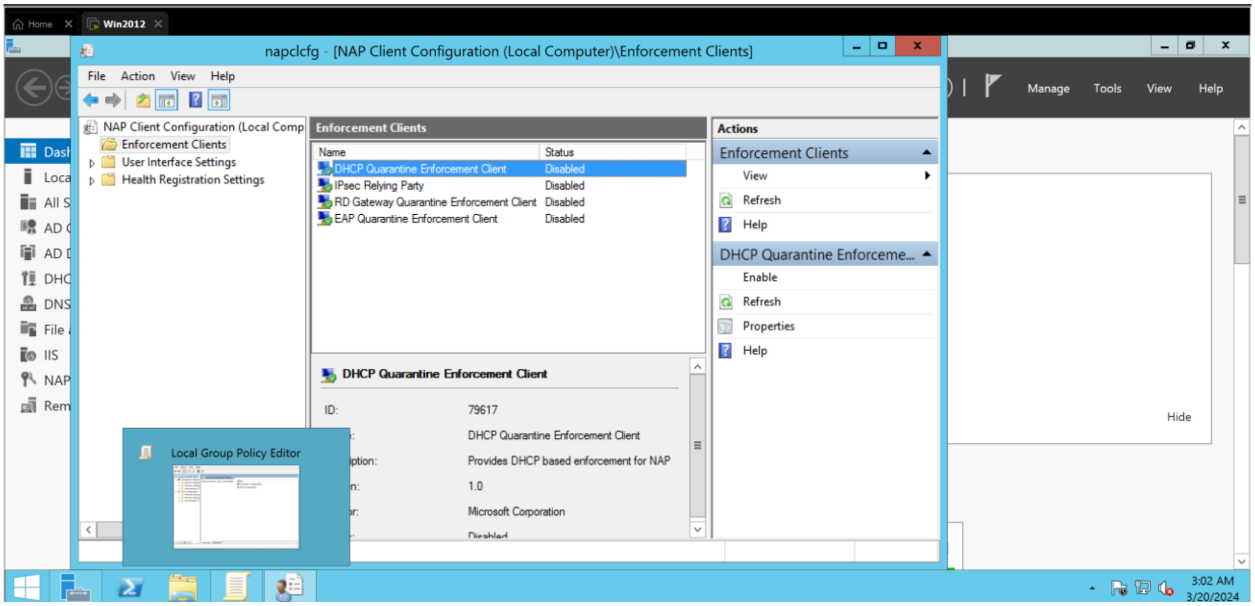
If you do not congifure this policy setting, the Security Center is turned off for domain members.

2. Enable the DHCP enforcement client:

a. Click Start, click All Programs, click Accessories, and then click Run.

b. Type napclcfg.msc, and then press ENTER.

c. In the console tree, click Enforcement Clients.



napclcfg - [NAP Client Configuration (Local Computer)\Enforcement Clients]

Name	Status
DHCP Quarantine Enforcement Client	Disabled
IPsec Relying Party	Disabled
RD Gateway Quarantine Enforcement Client	Disabled
EAP Quarantine Enforcement Client	Disabled

DHCP Quarantine Enforcement Client

ID: 79617

: DHCP Quarantine Enforcement Client

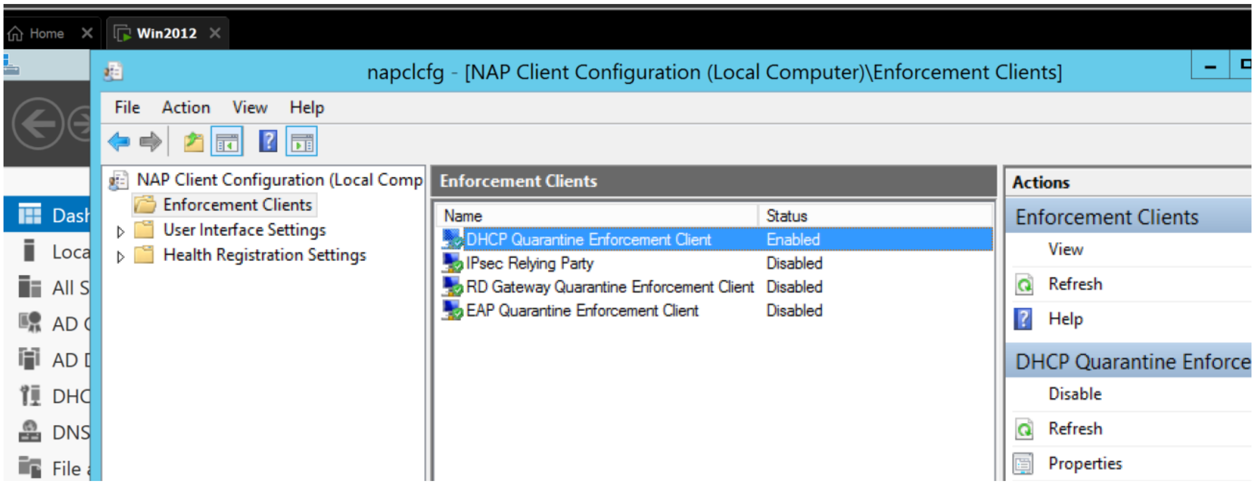
iption: Provides DHCP based enforcement for NAP

n: 1.0

r: Microsoft Corporation

Disabled

d. Enable the DHCP Quarantine Enforcement Client.



napclcfg - [NAP Client Configuration (Local Computer)\Enforcement Clients]

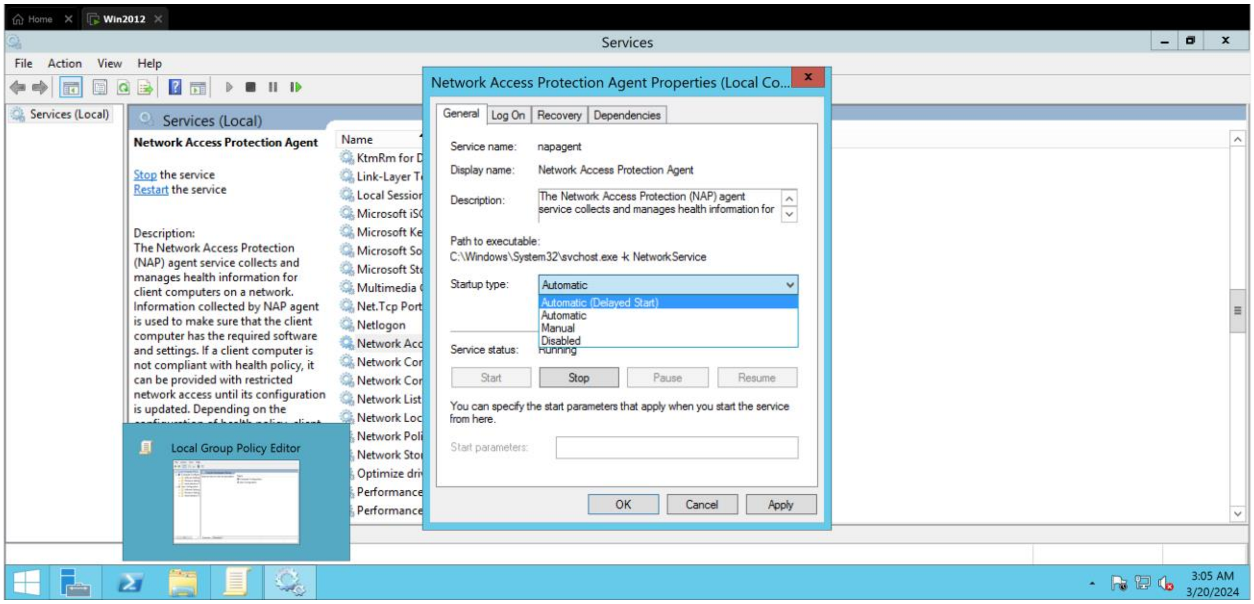
Name	Status
DHCP Quarantine Enforcement Client	Enabled
IPsec Relying Party	Disabled
RD Gateway Quarantine Enforcement Client	Disabled
EAP Quarantine Enforcement Client	Disabled

e. Close the NAP Client Configuration console.

a. Click Start, point to All Programs, click Accessories, and then click Run.

b. Type services.msc, and then press ENTER.

c. In the services list, set Network Access Protection Agent Startup type to Automatic and start the service.



Network Access Protection Agent Properties (Local Co...

Service name: napagent

Display name: Network Access Protection Agent

Description: The Network Access Protection (NAP) agent service collects and manages health information for

Path to executable:
C:\Windows\System32\svchost.exe -k NetworkService

Startup type: Automatic

Service status: Running

You can specify the start parameters that apply when you start the service from here.

Start parameters:

Network Access Protection Agent

Stop the service
Restart the service

Description:
The Network Access Protection (NAP) agent service collects and manages health information for client computers on a network. Information collected by NAP agent is used to make sure that the client computer has the required software and settings. If a client computer is not compliant with health policy, it can be provided with restricted network access until its configuration is updated. Depending on the

d. Wait for the NAP agent service to start, and then click OK.

e. Close the Services console.

4. Configure LON-CL1 for DHCP address assignment:

a. Click Start, and then click Control Panel.

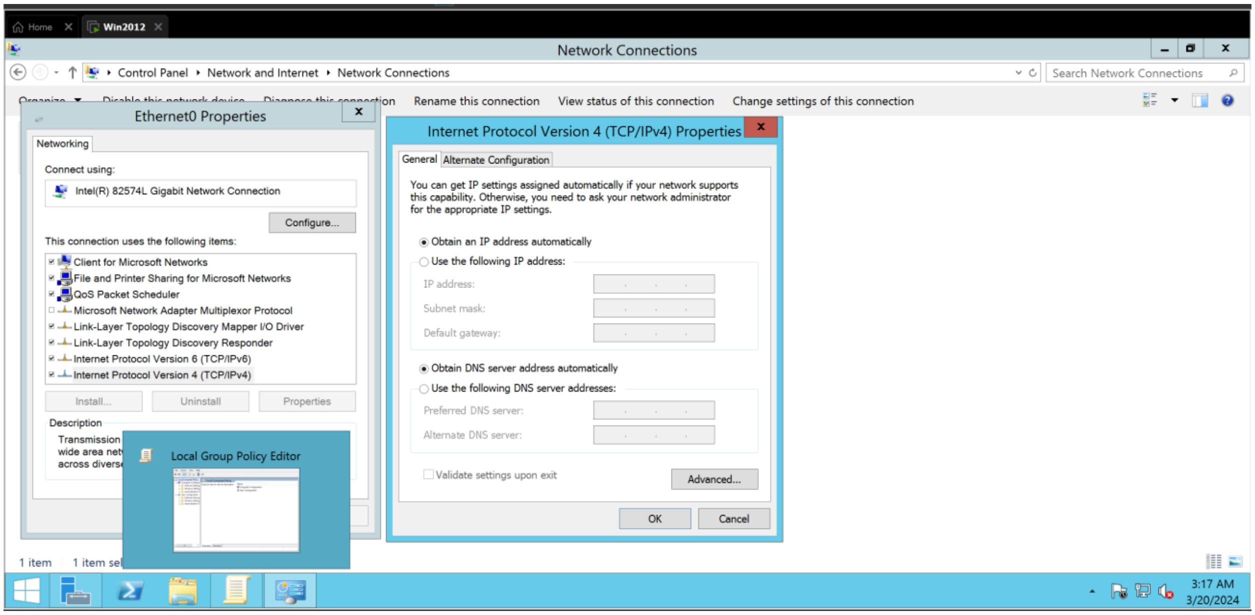
b. Click Network and Internet, click Network and Sharing Center, and then click Manage network connections.

c. Configure Local Area Connection properties with the following:

• Clear the Internet Protocol Version 6 (TCP/IPv6) check box.

• Set properties of Internet Protocol Version 4 (TCP/IPv4) to Obtain an IP address automatically and Obtain DNS server address automatically.

d. Click OK, and then click Close to close the Local Area Connection Properties dialog box.


Home
Win2012
Network Connections
Control Panel ▸ Network and Internet ▸ Network Connections
Search Network Connections
Organize ▾
Disable this network device
Diagnose this connection
Rename this connection
View status of this connection
Change settings of this connection
Local Group Policy Editor
1 item
1 item sel
3:17 AM
3/20/2024

Ethernet0 Properties

Networking

Connect using:

Intel(R) 82574L Gigabit Network Connection

Configure...

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ QoS Packet Scheduler
- □ Microsoft Network Adapter Multiplexor Protocol
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Install... Uninstall Properties

Description

Transmission
wide area net
across divers

Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address:

Subnet mask:

Default gateway:

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server:

Alternate DNS server:

□ Validate settings upon exit

Advanced...

OK Cancel

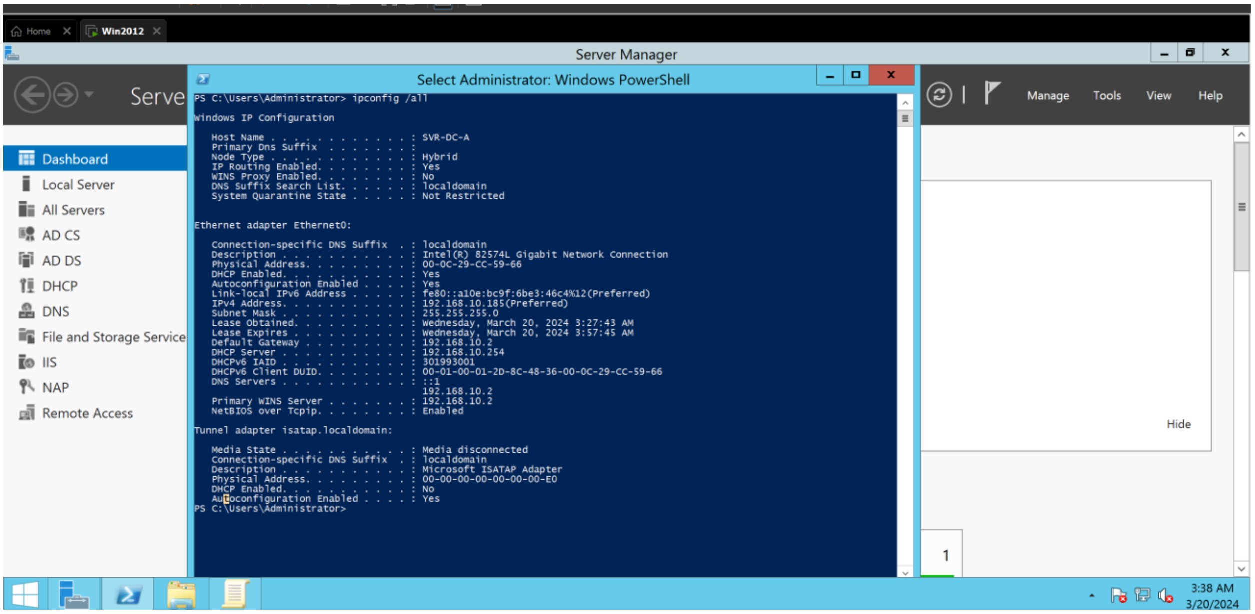
Task 7: Test NAP Enforcement

1. Verify the DHCP assigned address and current Quarantine State:

a. On LON-CL1, open an administrative command prompt using the Run As Administrator command.

b. At the command prompt, type ipconfig /all.

c. Verify that the connection-specific DNS suffix is Adatum.com and the Quarantine State is Not Restricted.

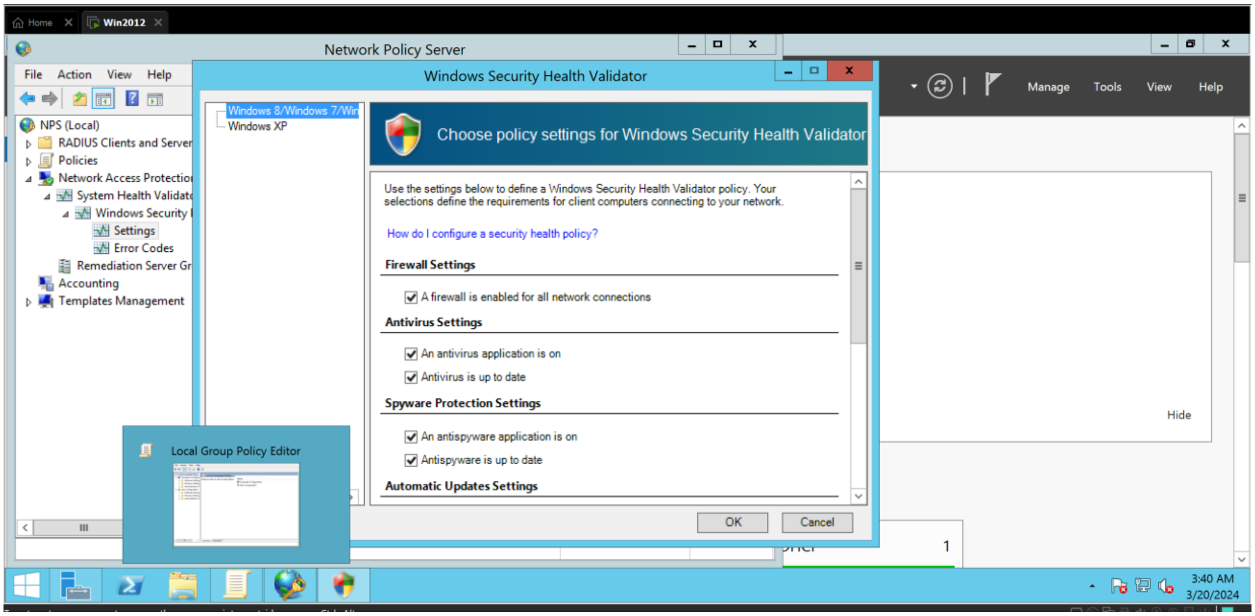


```
PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : SVR-DC-A
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : Yes
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain
   System Quarantine State . . . . . : Not Restricted


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-0C-29-CC-59-66
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::a10e:bc9f:6be3:46c4%12(Preferred)
   IPv4 Address. . . . . . . . . . . : 192.168.10.185(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Wednesday, March 20, 2024 3:27:43 AM
   Lease Expires . . . . . . . . . . : Wednesday, March 20, 2024 3:57:45 AM
   Default Gateway . . . . . . . . . : 192.168.10.2
   DHCP Server . . . . . . . . . . . : 192.168.10.254
   DHCPv6 IAID . . . . . . . . . . . : 301993001
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2D-8C-48-36-00-0C-29-CC-59-66
   DNS Servers . . . . . . . . . . . : ::1
                                       192.168.10.2
   Primary WINS Server . . . . . . . : 192.168.10.2
   NetBIOS over Tcpip. . . . . . . . : Enabled

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Microsoft ISATAP Adapter
   Physical Address. . . . . . . . . : 00-00-00-00-00-00-00-E0
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
PS C:\Users\Administrator>
```

2. Configure the System Health Validator policy to require antivirus software:

a. On LON-SVR1, in the Network Policy Server console, open NPS (Local), open Network Access Protection, and then open System Health Validators.

b. Configure Windows Security Health Validator so that Virus Protection is set to An antivirus application is on.



Windows Security Health Validator

Windows 8/Windows 7/Win
Windows XP

Choose policy settings for Windows Security Health Validator

Use the settings below to define a Windows Security Health Validator policy. Your selections define the requirements for client computers connecting to your network.

How do I configure a security health policy?

Firewall Settings

☑ A firewall is enabled for all network connections

Antivirus Settings

☑ An antivirus application is on

☑ Antivirus is up to date

Spyware Protection Settings

☑ An antispyware application is on

☑ Antispyware is up to date

Automatic Updates Settings

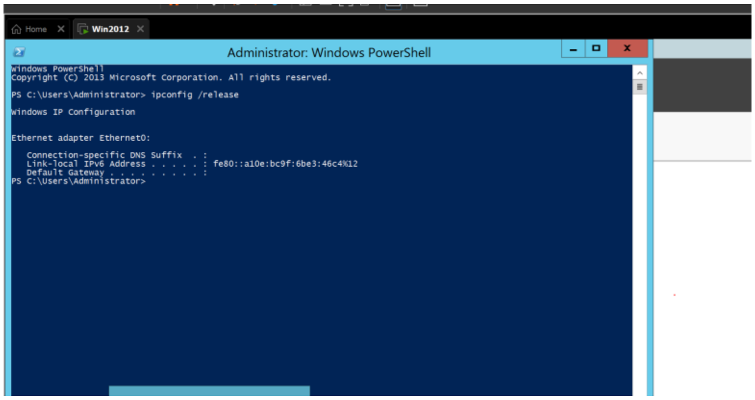
OK Cancel

c. Click OK, and then click OK again to close the Windows Security Health Validator Properties window.

3. Verify the restricted network on LON-CL1:

a. On LON-CL1, open an administrative command prompt using the Run As Administrator command.

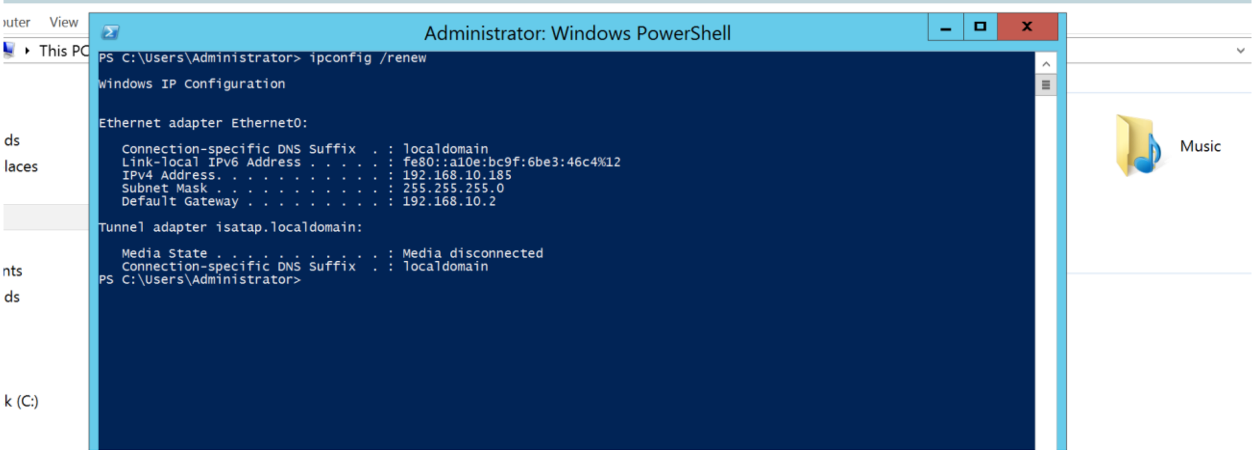
b. At the command prompt, type ipconfig /release.



```
Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> ipconfig /release

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::a10e:bc9f:6be3:46c4%12
   Default Gateway . . . . . . . . . :
PS C:\Users\Administrator>
```

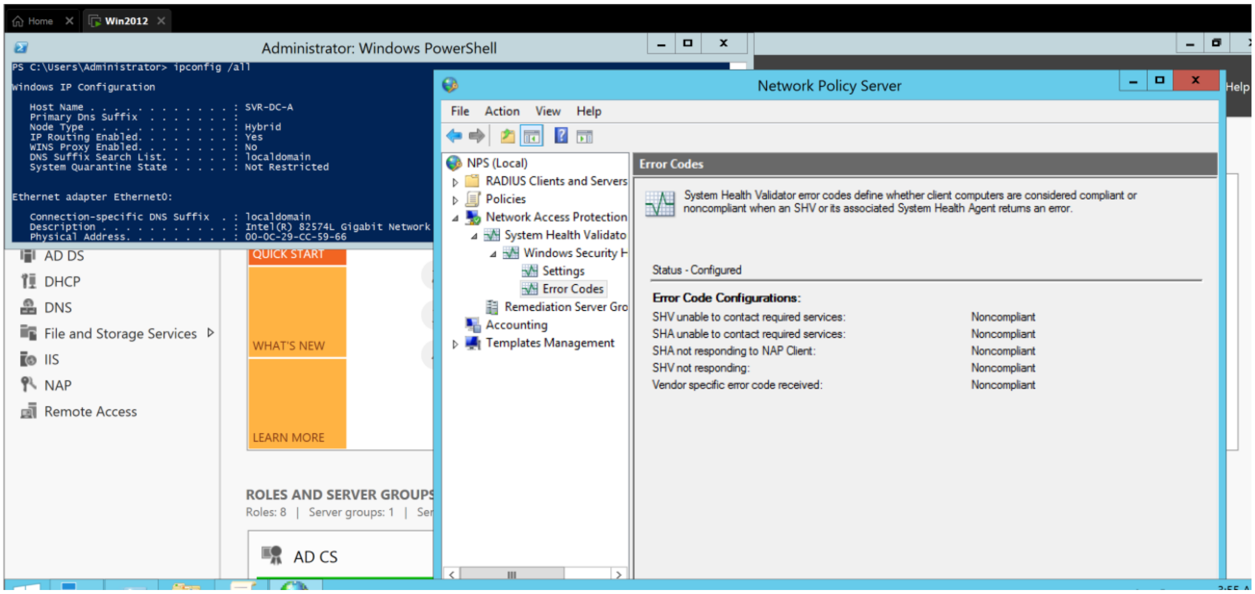
c. At the command prompt, type ipconfig /renew.

d. Verify the quarantine state is restricted



```
PS C:\Users\Administrator> ipconfig /renew

Windows IP Configuration


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Link-local IPv6 Address . . . . . : fe80::a10e:bc9f:6be3:46c4%12
   IPv4 Address. . . . . . . . . . . : 192.168.10.185
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.10.2

Tunnel adapter isatap.localdomain:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : localdomain
PS C:\Users\Administrator>
```

e. Close the command window and double-click the Network Access Protection icon in the system tray. Notice it tells you the computer is not compliant with requirements of the network.



```
PS C:\Users\Administrator> ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : SVR-DC-A
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : Yes
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : localdomain
   System Quarantine State . . . . . : Not Restricted


Ethernet adapter Ethernet0:

   Connection-specific DNS Suffix  . : localdomain
   Description . . . . . . . . . . . : Intel(R) 82574L Gigabit Network
   Physical Address. . . . . . . . . : 00-0C-29-CC-59-66
```

Error Codes

System Health Validator error codes define whether client computers are considered compliant or noncompliant when an SHV or its associated System Health Agent returns an error.

Status - Configured

Error Code Configurations:

SHV unable to contact required services:	Noncompliant
SHA unable to contact required services:	Noncompliant
SHA not responding to NAP Client:	Noncompliant
SHV not responding:	Noncompliant
Vendor specific error code received:	Noncompliant

f. Click Close.

<u>Task 8: Shutdown virtual machines and do not save changes</u>

Close all open windows, turn off all virtual machines and discard changes.

<u>Conclusions:</u>

In this lab, the task was to configure Network Access Protection (NAP) for DHCP clients using Server Manager, NPS, and DHCP Management consoles on designated virtual machines. The process involved setting up NAP health policies, configuring DHCP for enforcement, and testing NAP enforcement to ensure compliance with network requirements.

References:

1- Davies, J., & Northrup, T. (2008). Windows Server 2008 Networking and Network Access Protection-NAP. Microsoft Press.

2- Mrugalski, T., Siodelski, M., Volz, B., Yourtchenko, A., Richardson, M., Jiang, S., ... & Winters, T. (2018). Dynamic host configuration protocol for IPv6 (DHCPv6) (No. rfc8415).

3- Heberlein, L. T., Dias, G. V., Levitt, K. N., Mukherjee, B., Wood, J., & Wolber, D. (1989). A network security monitor (No. UCRL-CR-105095). Lawrence Livermore National Lab.(LLNL), Livermore, CA (United States); California Univ., Davis, CA (USA). Dept. of Electrical Engineering and Computer Science.