Lesson 14: Configuring Network Access Protection (NAP)

MOAC 70-411: Administering Windows Server 2012
Overview

• Exam Objective 4.3: Configure Network Access Protection (NAP)
• Using Network Access Protection (NAP)
Using Network Access Protection (NAP)

Lesson 14: Configuring Network Access Protection (NAP)
Network Access Protection (NAP)

• NAP is Microsoft’s software for controlling network access for computers based on the health of the host.
• NAP can be used on any computer that runs Windows and supports NAP.
• Types of computers that connect to a network:
  o Desktop computers
  o Roaming laptops
  o Unmanaged home computers
  o Visiting laptops
NAP Built-In Enforcement Methods

- DHCP
- IPsec
- VPN
- 802.1x
- Remote Desktop Gateway (RD Gateway)
NAP Architecture Components

- NAP client-side components
- NAP enforcement points
- NAP health policy server
- System Health Agents (SHAs)
NAP Architecture Components (cont.)

- Statement of Health (SoH)
- NAP Agent
- Health Registration Authority (HRA)
- Health requirements server
- Remediation servers
NAP Connection Process

1. When the NAP client connects to a network that requires NAP, each SHA on the NAP client validates its system health and generates an SoH.

2. The NAP client combines the SoHs from multiple SHAs into a SSoH and sends the information to a NAP health policy server that is defined with the NAP enforcement point.

3. The NAP health policy server uses its installed SHVs and the health requirements policies to determine whether the NAP client meets health requirements.
NAP Connection Process

4. The NAP health policy server combines the SoHRs from the multiple SHVs into a System Statement of Health Response (SSoHR) and sends the SSoHR back to the NAP client through the NAP enforcement point.

5. If the client is compliant, the enforcement point allows the connection. If the client is noncompliant, the computer can be connected to a remediation network.

6. If the computer is noncompliant, the noncompliant computer can attempt to come into compliance.

7. If the status of the computer changes, the entire process starts over.
Installing Network Access Protection

- Because NAP is offered through NPS, the installation is similar to installing NPS (discussed in Lesson 12).
- However, you want to add HRA, which is used to issue health certificates to NAP client computers that are compliant with network health requirements.
- For HRA to function, you need to have a CA available.
Install Network Policy Server

Select role services

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Network Policy and Access Services
Role Services
Confirmation
Results

Select the role services to install for Network Policy and Access Services

<table>
<thead>
<tr>
<th>Role services</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Policy Server</td>
<td></td>
</tr>
<tr>
<td>Health Registration Authority</td>
<td></td>
</tr>
<tr>
<td>Host Credential Authorization Protocol</td>
<td></td>
</tr>
</tbody>
</table>

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. With NPS, you can also deploy Network Access Protection (NAP), a client health policy creation, enforcement, and remediation technology.

Selecting the role services
Specifying the Certificate Authority

Health Registration Authority (HRA) requires that at least one Certification Authority (CA) be associated with it.

- Use the local CA to issue health certificates for this HRA server.
  - There is an existing CA on this computer. If you choose to use it, it will be dedicated to issuing health certificates.
- Use an existing remote CA.
  - If you choose to use an existing CA it should be one dedicated to issuing health certificates.
- Select a CA later using the HRA console.

⚠️ You will not be able to issue health certificates to NAP client computers until this CA is configured.
Install Network Policy Server

Configuring the authentication requirements

Authentication Requirements

Before You Begin
Installation Type
Server Selection
Server Roles
Features
Network Policy and Access...
Role Services
Certification Authority
Authentication Requirements

Health Registration Authority can be configured to ensure that only users authenticated to the domain can get health certificates.

Do you want to require that users be authenticated in order to get a health certificate?

- Yes, require requestors to be authenticated as members of a domain. (recommended)
  This option is only available when the computer is joined to a domain.
- No, allow anonymous requests for health certificates.

© 2013 John Wiley & Sons, Inc.
Configuring NAP Enforcement

To configure NAP:

1. Install and configure the server on which you will apply NAP enforcement.
2. Configure NPS and the NAP-related policies.
3. Configure the remediation servers.
DHCP Enforcement

To control network access, DHCP enforcement sets the following:

- DHCP Router option is set to 0.0.0.0 so noncompliant computers do not have a configured default gateway.
- Subnet mask is set to 255.255.255.255 so that there are no routes to the attached subnet.
Configuring NAP Enforcement for DHCP

To configure DHCP enforcement, you must:
1. Configure a DHCP server and create the appropriate DHCP scopes.
2. Install NPS on the DHCP server.
3. Run the NAP Wizard to configure the connection request policy, network policy, and NAP health policy. Define the remediation sever, which noncompliant clients can access.
4. Enable NAP for individual DHCP scopes.
5. Enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on NAP-capable client computers.
Configure the DHCP Server

Opening the DHCP console
Configure the DHCP Server

Defining the scope name

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:
Configure the DHCP Server

Specifying the IP address range

<table>
<thead>
<tr>
<th>IP Address Range</th>
<th>Configuration settings for DHCP Server</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Enter the range of addresses that the scope distributes.</td>
</tr>
<tr>
<td>Start IP address</td>
<td></td>
</tr>
<tr>
<td>End IP address</td>
<td></td>
</tr>
</tbody>
</table>

**Configuration settings that propagate to DHCP Client**

- **Length**: 0-12
- **Subnet mask**: . . . .
Configure the DHCP Server

Specifying the lease duration

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: 0
Hours: 8
Minutes: 0
Configure the DHCP Server

Defining the default gateway

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
Remove
Up
Down

© 2013 John Wiley & Sons, Inc.
Configure the DHCP Server

Authorizing the DHCP server
Configure NAP for DHCP Server

Starting the Network Policy Server console
Configure NAP for DHCP Server

Selecting the network connection method
Configure NAP for DHCP Server

Specifying NAP enforcement servers running DHCP server
Configure NAP for DHCP Server

Specify DHCP Scopes

When you specify one or more NAP-enabled scopes, NPS evaluates client health and performs authorization for client computers requesting an IP address from the designated scopes.

If you do not specify any scopes, the policy applies to all NAP-enabled scopes at the selected DHCP servers. If you specify a scope that is not NAP-enabled, you must enable NAP for the scope after completing this wizard.

To specify one or more scopes, click Add.

DHCP scopes:

Specify the DHCP scopes to apply to NAP
Configure NAP for DHCP Server

Specifying the computer groups that NAP will apply to
Configure NAP for DHCP Server

Specify a NAP Remediation Server Group and URL

Remediation Server Group:
Remediation servers store software updates for NAP clients that need them. Remediation Server Groups contain one or more remediation servers.

Select a Remediation Server Group that you have already configured or, to create a new group, click New Group.

Troubleshooting URL:
If you have a Web page that provides users with instructions to users on how to bring computers and devices into compliance with NAP health policy, type the Uniform Resource Locator (URL) for the Web page.

If you do not have a Help Web page, do not type a URL

http://
Configure NAP for DHCP Server

Adding computers to the Remediation Server group
Configure NAP for DHCP Server

Defining NAP Health Policy

The installed System Health Validators are listed below. Select only the System Health Validators that you want to enforce with this health policy.

- Name
  - Windows Security Health Validator

- Enable auto-remediation of client computers
  - If selected, NAP-capable client computers that are denied full access to the network because they are not compliant with health policy can obtain software updates from remediation servers.
  - If not selected, noncompliant NAP-capable client computers are not automatically updated and cannot gain full network access until they are manually updated.

Network access restrictions for NAP-eligible client computers:
- ( ) Deny full network access to NAP-eligible client computers. Allow access to a restricted network only.
- ( ) Allow full network access to NAP-eligible client computers.
Enable NAP on All DHCP Scopes

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

Enabling NAP for all DHCP scopes
Enable NAP on an Individual DHCP Scope

Enabling NAP for individual DHCP scopes
Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server

Opening the NAP Client Configuration console
Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server

Configuring the enforcement clients
Enable the NAP DHCP Quarantine Enforcement Client and Start NAP Service on a DHCP Server

Enabling enforcement client for DHCP
Configuring NAP Enforcement for VPN

1. Install NPS on the VPN server.
2. Configure the VPN server and have them use PEAP-based authentication (either PEAP-MS-ChAP v2 or PEAP-TLS).
3. Run the NAP Wizard to configure the connection request policy, network policy, and NAP health policy. Define the remediation servers, which noncompliant clients can access.
4. Enable the NAP DHCP Quarantine Enforcement Client and start the NAP service on NAP-capable client computers.
Configure NAP for VPN Servers

Selecting the Virtual Private Network (VPN) for the Network Connection
Configure NAP for VPN Servers

Specifying user and machine groups for NAP
Configure NAP for VPN Servers

Configuring an authentication method for NAP
System Health Validators

- **System Health Validators (SHVs)** settings define the requirements for client computers that connect to your network.
- You configure SHVs using the Network Policy Server console.
- Windows 8 includes a Windows Security Health Validator SHA that monitors the Windows Security Center settings.
- Windows Server 2012 includes a corresponding Windows Security Health Validator SHV.
System Health Validators

Managing the Windows SHV
System Health Validators

Configuring Windows SHV
Configuring System Health Validators

SHV options:
• Firewall Settings
• Antivirus Settings
• Spyware Protection Settings
• Automatic Updates Settings
• Security Updates Settings
System Health Validators

Configuring Security Updates settings
Configuring Health Policies

- Health policies consist of one or more system health validators and other settings that enable you to define client computer configuration requirements for the NAP-capable computers that attempt to connect to your network.

- Health policy pairs:
  - NAP-compliant
  - NAP-noncompliant
Configuring Health Policies

Viewing the health policies

© 2013 John Wiley & Sons, Inc.
Configuring Health Policies

Displaying the conditions of a health policy
Configuring Health Policies

Displaying the network policies
Configuring Health Policies

Viewing NAP Enforcement for a network policy
Configuring Health Policies

NAP enforcement settings:

- **NAP DHCP-compliant**: Allow full network access.
- **NAP DHCP-noncompliant**: Allow limited access.
- **NAP DHCP nonNAPcapable properties**: Allow full network access.
Configuring Isolation and Remediation

• If a computer is noncompliant, it should be isolated from production network.

• When you configure NAP, you can configure either a monitor only policy or an isolation policy.
Remediation servers typically consist of:

- DHCP servers to provide IP configuration
- Naming servers including DNS servers and WINS servers
- Active Directory domain controllers (read-only domain controllers are recommended to minimize security risks)
- Internet proxy servers so that noncompliant NAP clients can access the Internet
Configuring Isolation and Remediation

Remediation servers typically consist of (continued):

• HRAs so that noncompliant NAP clients can obtain a health certificate for the IPsec enforcement method
• Web server that contains the troubleshooting URL server, so users can access information on compliance
• Anti-virus/anti-malware servers to retrieve updated anti-virus/anti-malware updates
• Software update servers so that clients can get Windows updates
Configuring NAP Client Settings

• You can use the Enable Security Center in the Group Policy procedure to enable Security Center on NAP-capable clients using Group Policy.

• Some NAP deployments that use Windows Security Health Validator require Security Center.

• Open the Services console to start and set the startup type to Automatic in the Network Access Protection Agent service.
To verify a client’s configuration, run the following command:

```
netsh nap client show state
```
Configuring NAP Client Settings

Using the `netsh nap client show state` command
Lesson Summary

• Microsoft Network Access Protection (NAP) is software for controlling networked computers based on the host's health.
• NAP includes built-in enforcement methods that define the mechanisms that NAP can use, including DHCP, Internet Protocol Security (IPsec), VPN, 802.1, and more.
• System Health Agents (SHAs) are components that report on one or more elements of the health of a NAP client.
• Each SHA creates a Statement of Health (SoH) that transmits to the NAP Agent. Each SHA generates a new Statement of Health whenever the status is updated.
• NAP Agent maintains information about the health of the NAP client computer and transmits information between the NAP enforcement clients and the SHAs.
Lesson Summary

• System Health Validators (SHVs) settings define requirements for client computers that connect to your computer.

• Health policies consist of one or more system health validators and other settings that enable you to define client computer configuration requirements for NAP-capable computers.

• Typically, you use a monitor-only policy when you first implement NAP to test the implementation so that you can verify which computers are blocked and which are granted access to the production network by viewing the security logs in the Event Viewer on the NAP server.

• A remediation server group and troubleshooting URL will be available to users if they fail the compliance check.

• For clients to use NAP, they must have Security Center enabled and have the NAP Agent service running.