Lesson 12: Configuring a Network Policy Server

MOAC 70-411: Administering Windows Server 2012
Overview

• Exam Objective 4.1: Configure Network Policy Server (NPS)

• Configuring a Network Policy Server Infrastructure
Configuring a Network Policy Server Infrastructure

Lesson 12: Configuring a Network Policy Server
RADIUS Terms

Network Policy Server (NPS): Microsoft’s RADIUS server.

Authorization: The process that determines what a user is permitted to do on a computer system or network.

RADIUS client: A server or device that forwards RADIUS requests to a RADIUS server.

Access client: A computer or device that contacts or connects to a RADIUS client, which requires authentication and authorization to connect.
A Network with RADIUS

RADIUS servers and clients
When NPS is used as a RADIUS server, authentication, authorization, and accounting follows these steps:

1. When an access client accesses a VPN server or wireless access point, a connection request is created that is sent to the NPS server.
2. The NPS server evaluates the Access-Request message.
3. If required, the NPS server sends an Access-Challenge message to the access server. The access server processes the challenge and sends an updated Access-Request to the NPS server.
4. The user credentials are checked and the dial-in properties of the user account are obtained by using a secure connection to a domain controller.
Authentication, Authorization, and Accounting

When NPS is used as a RADIUS server, authentication, authorization and accounting follows these steps (cont.):

5. When the connection attempt is authorized with both the dial-in properties of the user account and network policies, the NPS server sends an Access-Accept message to the access server. If the connection attempt is either not authenticated or not authorized, the NPS server sends an Access-Reject message to the access server.

6. The access server completes the connection process with the access client and sends an Accounting-Request message to the NPS server, where the message is logged.

7. The NPS server sends an Accounting-Response to the access server.
Installing Network Policy Server

Installing Network Policy and Access Services

Network Policy and Access Services provides Network Policy Server (NPS), Health Registration Authority (HRA), and Host Credential Authorization Protocol (HCAP), which help safeguard the health and security of your network.
Installing Network Policy Server

Selecting Network Policy and Access Service Role Services
Installing Network Policy Server

Opening the Network Policy Server console
Configuring RADIUS Server Infrastructures

Multiple RADIUS server configurations:

• Primary RADIUS server and alternate RADIUS servers

• A RADIUS proxy located between the RADIUS server and the RADIUS clients
Configuring RADIUS Server Infrastructures

Using a RADIUS proxy server
Load balancing options:

- Priority
- Weight
- Advanced settings
Add a Remote RADIUS Server Group

Creating a new RADIUS server group
Add a Remote RADIUS Server Group

Adding a RADIUS server to the RADIUS server group
Add a Remote RADIUS Server Group

Configuring Authentication and Accounting RADIUS
Add a Remote RADIUS Server Group

Configuring RADIUS load balancing
Configuring RADIUS Clients

The standard configuration includes:

- RADIUS server for dial-up or VPN connections
- RADIUS server for 802.1X wireless or wired connections
- NAP policy server (discussed in Lesson 14)
Configure NPS for RADIUS Server for VPN Connections

Specifying connections on the Dial-up or Virtual Private Network Connections Type page
Configure NPS for RADIUS Server for VPN Connections

Showing the RADIUS clients page
Configure NPS for RADIUS Server for VPN Connections

Adding RADIUS clients
Configure NPS for RADIUS Server for VPN Connections

Specifying authentication methods
Configure NPS for RADIUS Server for VPN Connections

Specify User Groups

Users that are members of the selected group or groups will be allowed or denied access based on the network policy Access Permission setting.

To select User Groups, click Add. If no groups are selected, this policy applies to all users.

Groups

Specify user groups
Configure NPS for RADIUS Server for VPN Connections

Specify IP Filters

Configure IPv4 and IPv6 packet filters if you want to restrict the type of network traffic sent and received.

If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can configure IPv4 and IPv6 input and output filters. Otherwise, click Next.

Select an existing IP filter template:

None

IPv4

To control the IPv4 packets this interface sends, click Input Filters.

To control the IPv4 packets this interface receives, click Output Filters.

IPv6

To control the IPv6 packets this interface sends, click Input Filters.

To control the IPv6 packets this interface receives, click Output Filters.

Specifying IP filters
Configure NPS for RADIUS Server for VPN Connections

Configuring inbound filters

© 2013 John Wiley & Sons, Inc.
Configure NPS for RADIUS Server for VPN Connections

Specify Encryption Settings

Specify the allowed encryption strengths used for traffic between access clients and the network access server.

If you are using Routing and Remote Access Service configured as a dial-up or VPN server, you can configure encryption strength.

The encryption settings are supported by computers running Microsoft Routing and Remote Access Service.

If you use different network access servers for dial-up or VPN connections, ensure that the encryption settings you select are supported by your servers.

If no encryption is the only option selected, traffic from access clients to the network access server is not secured by encryption. This configuration is not recommended.

- Basic encryption (MPPE 40-bit)
- Strong encryption (MPPE 56-bit)
- Strongest encryption (MPPE 128-bit)

Specifying encryption settings
Configure NPS for RADIUS Server for VPN Connections

Specifying a realm name
Configure NPS for 802.1X Wireless Connections

Select 802.1X Connections Type

Type of 802.1X connections:
- Secure Wireless Connections:
  When you deploy 802.1X wireless access points on your network, NPS can authenticate and authorize connection requests made by wireless clients connecting through the access points.

- Secure Wired (Ethernet) Connections:
  When you deploy 802.1X authenticating switches on your network, NPS can authenticate and authorize connection requests made by Ethernet clients connecting through the switches.

Name:
This default text is used as part of the name for each of the policies created with this wizard. You can use the default text or modify it.

Selecting the 802.1X connections type
Configure NPS for 802.1X Wireless Connections

Configuring authentication methods for 802.1X
Configure NPS for 802.1X Wireless Connections

Configure Traffic Controls

Use virtual LANs (VLANs) and access control lists (ACLs) to control network traffic.

If your RADIUS clients (authenticating switches or wireless access points) support the assignment of traffic controls using RADIUS tunnel attributes, you can configure these attributes here. If you configure these attributes, NPS instructs RADIUS clients to apply these settings for connection requests that are authenticated and authorized.

If you do not use traffic controls or you want to configure them later, click Next.

Traffic control configuration

To configure traffic control attributes, click Configure.
NPS Advanced Configuration
Network Policies

Network Policy Server

Network Policies Table:
- Policy Name
- Status
- Processing Order
- Access Type
- Source

Virtual Private Network (VPN) Connections:
- Condition: NAS Port Type, Virtual (VPN)
- Windows Groups: CONTOSO\Domain Users

Settings:
- Authentication Method
- Challenge Method
- Access Permission
- Update Noncompliant Clients
- NAP Enforcement
- Framed Protocol
- Service Type
- Precedence

© 2013 John Wiley & Sons, Inc.
Managing RADIUS Templates

• RADIUS templates:
  o Are designed to reduce the amount of time and cost that it takes to configure RADIUS on one or more servers

• Creating a RADIUS template does not affect the functionality of NPS.

• A RADIUS template affects only the NPS server when the template is selected and applied when configuring RADIUS.
Managing RADIUS Templates

Templates Configuration

Select an item below to create, configure, and manage templates. All templates can be exported to or imported from other NPS servers. To import or export templates, right-click Templates Management and select a command.

Configure NPS Templates

In Templates Management, you create and modify NPS templates. NPS templates allow you to create and save an NPS component configuration for reuse later. The templates are not applied to the NPS server configuration until you select the templates in the appropriate location in the NPS console.

After you create a template, you can apply the NPS component configuration in the NPS console by selecting the template. For example, you can create an IP Filters template, and then apply the same IP Filters configuration to multiple network policies by simply selecting the template.

- Shared Secrets
- RADIUS Clients
- Remote RADIUS Servers
- IP Filters
- Health Policies
- Remediation Server Groups
- IP Filters
- Learn more

Templates Configuration options in the NPS console
Managing RADIUS Templates

Creating a RADIUS client template

New RADIUS Client

Settings

Name and Address
Friendly name:
Address (IP or DNS)

Advanced

Shared Secret
Select an existing Shared Secrets template:
None

To manually type a shared secret, click Manual. To automatically generate a shared secret, click Generate. You must configure the RADIUS client with the same shared secret entered here. Shared secrets are case-sensitive.

Manual
Generate

Shared secret:

Confirm shared secret:
Managing RADIUS Templates

Using the RADIUS client template
NPS can log accounting data to a text log file and/or a SQL Server database.

NPS server generates an Accounting-Start message describing the type of service being delivered and the user it is being delivered to, which is sent to the RADIUS Accounting server.

The RADIUS Accounting server sends back an acknowledgment to the RADIUS client.

At the end of service delivery, the client generates an Accounting-Stop message that describes the type of service that was delivered, and optional statistics, such as elapsed time, input and output octets, or input and output packets. It then sends that data to the RADIUS Accounting server, which sends back an acknowledgment to the RADIUS client.
Configuring RADIUS Accounting

- **NPS Server**
  - Generates an Accounting-Start message

- **RADIUS Accounting Server**
  - Sends an acknowledgment

- **RADIUS Client**
  - Generates an Accounting-Stop message
To Enable and Configure Accounting in NPS

Accounting configuring options
To Enable and Configure Accounting in NPS

Selecting Accounting options

NPS can log accounting data to a local text file, to a SQL Server database, or to both. NPS can also log to a SQL Server database only, and then start logging to a text file if SQL Server logging fails, providing failover.

Select one NPS Accounting configuration option, and then click Next:

- Log to a SQL Server database.
- Log to a text file on the local computer
- Simultaneously log to a SQL Server database and to a local text file
- Log to a SQL Server database using text file logging for failover.

Selecting Accounting options
To Enable and Configure Accounting in NPS

Configuring SQL Server logging

Accounting Configuration Wizard

Configure SQL Server Logging

Configure both the SQL Data Link in NPS and the database in SQL Server

Configure SQL Server Logging: When you configure SQL Logging, you set up the data link between NPS and SQL Server. You also select an existing database in SQL Server or type a name for a new database. Depending on your choice, NPS either modifies the existing database or creates a new database in SQL Server for you. To configure SQL Server Logging, click Configure.

Logging information: Select the information that NPS logs to the SQL Server database.

- [x] Accounting requests
- [x] Authentication requests
- [ ] Periodic accounting status
- [ ] Periodic authentication status

Logging failure action: If logging fails due to network or other problems, NPS can continue to process connection requests or it can discard them to preserve accounting data accuracy. If NPS discards connection requests, users cannot access the network through RADIUS clients.

- [x] If logging fails, discard connection requests

To continue, click Next.
To Enable and Configure Accounting in NPS

Configuring the Data Link properties
To Enable and Configure Accounting in NPS

Configuring local file logging

Logging information:
- Accounting requests
- Authentication requests
- Periodic accounting status
- Periodic authentication status

Log file directory:
Specify a location for your log file. NPS creates the file with the name nps3n.log.

Logging failure action:
- If logging fails due to network or other problems, NPS can continue to process connection requests or it can discard them to preserve accounting data accuracy. If NPS discards connection requests, users cannot access the network through RADIUS clients.
- If logging fails, discard connection requests.

To continue, click Next.
Log File Properties

Log File Properties

Log the following information:
- Accounting requests
- Authentication requests
- Periodic accounting status
- Periodic authentication status

Logging failure action:
- If logging fails, discard connection requests.

Name: [Nyyymm.log]
Directory: [C:\Windows\system32\LogFiles]
Format: DTS Compliant

Create a new log file:
- Daily
- Weekly
- Monthly
- Never (unlimited file size)
- When log file reaches this size: [10 MB]
- When disk is full delete older log files

Configuring Log File properties
Understanding NPS Authentication Methods

Authentication is usually broken down into the following categories:

• Password-based credentials
• Certificate-based credentials
Using Password-Based Authentication

- The network access server passes the username and password to the NPS server.
- The NPS server verifies the credentials against the user account database.
  - Processed from the most secure (Microsoft Challenge-Handshake Authentication Protocol v2 or MS-CHAPv2) to the least secure (unauthenticated access) of those enabled options.
- For stronger security, use certificate authentication or multi-factor authentication.
Using Certificates for Authentication

- Much stronger than password-based authentication methods
- Certificates are:
  - Customized using certificate templates
  - Issued using a Certificate Authority
- If smart cards are used, certificates must include:
  - Smart Card Logon purpose
  - Client Authentication purpose
Using Certificates for Authentication

- Digital certificate required and NPS server must use a server certificate for:
  - Protected Extensible Authentication Protocol Microsoft Challenge-Handshake Authentication Protocol v2 (PEAP-MS-CHAP v2)
  - Protected Extensible Authentication Protocol Transport Layer Security (PEAP-TLS)
  - Extensible Authentication Protocol Transport Layer Security (EAP-TLS)
Automatically Add Workstation Authentication Certificates to All Workstations

Configuring security for a template
Automatically Add Workstation Authentication Certificates to All Workstations

Confusing user and computer certificate—Auto-Enrollment
Lesson Summary

• Microsoft’s RADIUS server is Network Policy Server (NPS).
• By installing and configuring RADIUS, you can create and enforce wide network access policies for client health, connection request authentication, and connection request authorization.
• When you implement RADIUS, Windows Server 2012 computers running Routing and Remote Access and/or wireless access points can forward access requests to a single RADIUS server.
• Installing NPS is a simple process, which is done with Server Manager. After NPS is installed, you use the Network Policy Server console to configure NPS.
Lesson Summary

• With multiple RADIUS servers, you can configure RADIUS clients to use a primary RADIUS server and alternate RADIUS servers. If the primary RADIUS server becomes unavailable, the request is sent to the alternate RADIUS server.

• Much like the use of other templates, RADIUS templates are designed to reduce the amount of time and cost that it takes to configure RADIUS on one or more servers.

• Creating a RADIUS template does not affect the functionality of NPS. It affects the RADIUS server only when the template is selected and applied when configuring NPS.

• NPS supports RADIUS accounting, which you can use to track network usage for auditing and billing purposes.

• Using certificates with the NPS provides strong security for authenticating users and computers and eliminates the need for less secure password-based authentication methods.

© 2013 John Wiley & Sons, Inc.