Lesson 12: Configuring a Network Policy Server

MOAC 70-411: Administering Windows Server 2012



WILEY

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

© 2013 John Wiley & Sons, Inc.

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 <u>server</u> or <u>device</u> 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

Authentication, Authorization, and Accounting

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

elect server roles	5	DESTINATION SERVE Win2012Srv2.contoso.cor
Before You Begin Installation Type	Select one or more roles to install on the selected server. Roles	Description
Server Selection Server Roles Features Network Policy and Acces Role Services Confirmation Results	 Active Directory Certificate Services Active Directory Domain Services Active Directory Federation Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Application Server DHCP Server DHS Server Fax Server ✓ File And Storage Services (Installed) Hyper-V ✓ Network Policy and Access Services Print and Document Services Remote Access (Installed) Remote Desktop 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 an security of your network.

Installing Network Policy and Access Services

Installing Network Policy Server

b	Add Roles and Features Wizard	_ _ X
Before You Begin Installation Type Server Selection Server Roles Features Network Policy and Acces Role Services Confirmation Results	Add Roles and Features Wizard S Select the role services to install for Network Policy and Acce Role services Image: Metwork Policy Server Image: Health Registration Authority Image: Host Credential Authorization Protocol	DESTINATION SERVER Win2012Srv2.contoso.com ss Services Description 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.
	< Previous Ne	xt > Install Cancel

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

Configuring RADIUS Server Infrastructures

Load balancing options:

- Priority
- Weight
- Advanced settings

Ne	w Remote RADIU	S Server Group	x
Group name: 			
RADIUS Server	Priority	Weight	Add E dit Remove
		OK	Cancel

Creating a new RADIUS server group

Add RADIUS Server
Address Authentication/Accounting Load Balancing
Select an existing Remote RADIUS Servers template:
None v
Type the name or IP address of the RADIUS server you want to add.
Server:
192.168.3.121 Veiny
OK Cancel

Adding a RADIUS server to the RADIUS server group

© 2013 John Wiley & Sons, Inc.

Add RADIUS	S Server ×			
Address Authentication/Accounting Load Ba	alancing			
Authentication port:	1812			
Select an existing Shared Secrets template:				
None	×			
Shared secret:				
Confirm shared secret:				
Request must contain the message authent	icator attribute			
Accounting	1010			
Accounting port:	1813			
✓ Use the same shared secret for authentic	ation and accounting.			
Select an existing Shared Secrets templa	ite:			
None				
Shared secret:				
Confirm shared secret:				
Forward network access server start and stop notifications to this server				
	OK Cancel			

Configuring Authentication and Accounting RADIUS

Add RADIUS Server
Address Authentication/Accounting Load Balancing
The priority of ranking indicates the status of a server. A primary server has a priority of 1.
Weight is used to calculate how often request are sent to a specific server in a group of servers that have the same priority.
Priority: [1 Weight: 50
Advanced settings
Number of seconds without response before request is 3
Maximum number of dropped requests before server is 5
Number of seconds between requests when server is identified 30 as unavailable:
0K Cancel

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 VPN or Dial-Up
	Select Dial-up or Virtual Private Network Connections Type
 Type of conr Dial-up Con When you a Wirtual Priva When you a made by VF Name: This default text or n Virtual Private 	The ections: nections deploy Dial-up servers on your network, NPS can authenticate and authorize connection requests ul-up clients connecting through the servers. the Network (VPN) Connections deploy VPN servers on your network, NPS can authenticate and authorize connection requests N clients connecting through the servers. t is used as part of the name for each of the policies created with this wizard. You can use the nodify it . Network (VPN) Connections
	Previous Next Finish Cancel

Specifying connections on the Dial-up or Virtual Private Network Connections Type page

Configure VPN or Dial-Up	x			
Specify Dial-Up or VPN Server				
RADIUS clients are network access servers, not client computers. If the local computer is running Routing and Remote Access as a VPN server, it is automatically added to the list of RADIUS clients below.				
If you want to add remote VPN servers as RADIUS clients, click Add.				
RADIUS clients:				
	Add			
	Edit			
	Remove			
Previous Next Finish	Cancel			

Showing the RADIUS clients page

	New RADIUS (Client	
ttings			
Select an existing temp	ate:		
			~
Name and Address			
Friendly name:			
[
Address (IP or DNS):			
			Verify
Shared Secret Select an existing Shared	Secrets template:		
None			~
None To manually type a share secret, click Generate. Yo secret entered here. Shar Manual Shared secret:	d secret, click Manual. u must configure the R ed secrets are case-ser Generate	To automatically ger ADIUS client with th nsitive.	verate a sharec
None To manually type a sharer secret, click Generate. Yo secret entered here. Shar Manual Shared secret.	J secret, click Manual. Ju must configure the R ed secrets are case-ser Generate	To automatically ger ADIUS client with th sstrive.	verate a sharec
None To manually type a sharer secret, click Generate. Yo secret entered here. Shar Manual Shared secret: Confirm shared secret:	J secret, click Manual. su must configure the R ed secrets are case-ser Generate	To automatically ger ADIUS client with th sstive.	v ierate a sharec e same sharec
None To manually type a sharer secret, click Generate, Yo secret entered here. Shar Manual Shared secret: Confirm shared secret:	J secret, click Manual. Ju must configure the R ed secrets are case-ser	To automatically ger ADIUS client with th nsitive.	verate a shared

Adding RADIUS clients

Configure VPN or Dial-Up			
Configure Authentication Methods			
The following protocols are supported by servers running Microsoft Routing and Remote Access. If you use a different remote access server, make sure the protocols you select are supported by that software.			
Extensible Authentication Protocol			
Type (based on method of access and network configuration):			
Microsoft: Smart Card or other certificate V Configure			
 Microsoft Encyrpted Authentication version 2 (MS-CHAPv2) Select this option to allow your users to specify a password for authentication. Microsoft Encyrpted Authentication (MS-CHAP) 			
Select this option only if your network runs operating systems that do not support MS-CHAPv2.			
Previous Next Finish Cancel			

Specifying authentication methods

	Configure VPN or Dial-Up	x
	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.	ŧ.,
To select User	Groups, click Add. If no groups are selected, this policy applies to all users.	
Groups	Add Remove	3
	Previous Next Finish Cancel	

Specifying user groups

	Configure VPN or Dial-Up		x
	Specify IP Filters Configure IPv4 and IPv6 packet filters if you want to restrict the and received.	e type of network traffic s	;ent
If you are using IPv4 and IPv6 i	Routing and Remote Access Service configured as a dial-up or VP nput and output filters. Otherwise, click Next.	'N server, you can configu	re
Select an exist None	ing IP <u>F</u> ilter template:	~	
⊡Pv4 To control the	IPv4 packets this interface sends, click Input Filters.	Input Filters	
To control the	IPv4 packets this interface receives, click Output Filters.	Output Filters	
IPv6			
I o control the	IPv6 packets this interface sends, click Input Hilters.	Input Filters	
To control the	IPv6 packets this interface receives, click Output Filters.	Output Filters	
	Previous Next	Finish Cancel	

Specifying IP filters

Inbound Filters ? X	Add IP Filter ? X
These filters control which packets are forwarded or processed by this network.	Source network
Filter action: O not permit packets listed below Permit only the packets listed below	IP address: · · · · · · · · · · · · · · · · · ·
Filters:	Destination network
Source Address Source Network Mask Destination Address Destination Mask P	IP address:
	Subnet mask:
	Protocol:
III > New Edit	
OK Cancel	OK Cancel

Configuring inbound filters

	Configure VPN or Dial-Up
	Specify Encryption Settings
<u>N</u>	Specify the allowed encryption strengths used for traffic between access clients and the network access server.
If you are using encryption stren	Routing and Remote Access Service configured as a dial-up or VPN server, you can configure gth.
The encryption	settings are supported by computers running Microsoft Routing and Remote Access Service.
If you use differe settings you sele	ent network access servers for dial-up or VPN connections, ensure that the encryptions ect are supported by your servers.
If No encryption secured by enci	i is the only option selected, traffic from access clients to the network access server is not yption. This configuration is not recommended.
🖌 Basic encry	ption (MPPE 40-bit)
🖌 Strong encr	yption (MPPE 56-bit)
✔ Strongest e	ncryption (MPPE 128-bit)
	Previous Next Finish Cancel

Specifying encryption settings

	Specify a Realm Name If you specify a realm name, the user account location supplied by users in log on credentials, such as a domain name, is replaced by the value you choose.
Your ISP uses a the user name i If you do not kn	portion of the user name to identify which connection requests to route to this server. This part of the realm name. ow your realm name, contact your ISP. If you do not care about realm name, please click next.
Type the realm forward request Realm name	name, including the separator character (the period or the forward slash), that your ISP uses to s.
Example: ISP.	
✔ Before auth If the realm Windows c	entication, remove the realm name from the user name name is an identifier added to the existing Windows user name, it must be removed before an authenticate the connection request.

Specifying a realm name

Configure NPS for 802.1X Wireless Connections

	Configure 802.1X	x
Si Si	elect 802.1X Connections Type	
Type of 802.1X of Secure Wireless When you deplo connection requinant Secure Wired (E When you deplo connection requi	connections : s Connections by 802.1% wireless access points on your network, NPS can authenticate and author jests made by wireless clients connecting through the access points. Ethernet) Connections by 802.1% authenticating switches on your network, NPS can authenticate and auth jests made by Ethernet clients connecting through the switches.	orize horize
Name: This default text is u default text or modif	used as part of the name for each of the policies created with this wizard. You can u fy it .	se the
	Previous Next Finish Ca	ancel

Selecting the 802.1X connections type

Configure NPS for 802.1X Wireless Connections

Configure 802.1X
Configure an Authentication Method
Select the EAP type for this policy.
Type (based on method of access and network configuration):
Microsoft: Smart Card or other certificate Configure
Microsoft: Smart Card or other certificate Microsoft: Protected EAP (PEAP) Microsoft: Secured password (EAP-MSCHAP v2)
Previous Next Finish Cancel

Configuring authentication methods for 802.1X

Configure NPS for 802.1X Wireless Connections

Configure 802.1X
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 attribute 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. Configure
Previous Next Finish Cancel

Configuring traffic controls

NPS Advanced Configuration



Network Policies

•	Net	work Policy Server			L		×
File Action View Help							
🗢 🄿 🖄 💽 🚺 🗊							
🚯 NPS (Local)	Network Policies						
A RADIUS Clients and Servers RADIUS Clients Remote RADIUS Server Grou E Policies	Network policies allow you they can or cannot conn	ou to designate who is authorized ect.	to connect	to the network and	the circumstance	es under wł	nich
Connection Bequest Policie	Policy Name		Status	Processing Order	Access Type	Source	
Network Policies	Secure Wireless Connections		Enabled	1	Grant Access	Unspecifi	ied
Health Policies	Virtual Private Network (VPN)	Connections	Enabled	2	Grant Access	Remote A	Åc
A Network Access Brotection	🛛 😹 Connections to Microsoft Rout	ing and Remote Access server	Enabled	999999	Deny Access	Unspecifi	ied
N W System Health Validators	🛛 😹 Connections to other access s	ervers	Enabled	1000000	Deny Access	Unspecifi	ied
B Remediation Server Grouns							
Accounting	🤯 Virtual Private Network (VPN) Connections					
A remplaces Management Shared Secrets ADIUS Clients Remote RADIUS Servers IP Filters Health Policies Remediation Server Groups	Conditions - If the following con Condition Value NAS Port Type Virtual (VPI Windows Groups CONTOSC	ditions are met: V) \Domain Users					
	Settings - Then the following se	ttings are applied:					
	Setting	Value	01		a har and a		^
	Authentication Method MS-CHAP v2 OR MS-CHAP v2 (User can change password after it has expired)						
	Access Permission Grant Access						
	NAP Enforcement Allow full network access						
	Eramed-Protocol PPP						
	Service-Tupe	Framed					
	Encruption Basic encruption (MPPE 40-bit) Strong encruption (MPPE 56-bit) Strongest encruption (
	<					>	

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

Managing RADIUS Templates



Templates Configuration options in the NPS console

Managing RADIUS Templates

New RADIUS Client		x
Settings Advanced		
Name and Address		
Friendly name:		
Address (IP or DNS):		
	Verify	
Shared Secret		=1
Select an existing Shared Secrets template:		
None	~]
To manually type a shared secret, click Manual. To automatically ger secret, click Generate. You must configure the RADIUS client with th secret entered here. Shared secrets are case-sensitive.	nerate a shared ne same shared	
Manual Generate		
Shared secret:		
Confirm shared secret:		
OK	Cance	el 🛛

Creating a RADIUS client template

Managing RADIUS Templates

		Ne	w RADIU	IS Client			×
ettings	Advanced						
– Z Enabl	le this BADIU	S client					
		5 GIIGH					
✓ Selec	st an existing	emplate:					
test							~
Name a	and Address						
Friendly	y name:						
test							
Addres	s (IP or DNS)						
192.16	58.3.122					Verify	
Shared	Secret						
Select	an existing SI	nared Secrets	template:				
None							~
To mar secret, secret	nually type a s click Genera entered here. nual	hared secret, :e. You must Shared secre O Ge	, click Manı configure th ets are case enerate	ual. To autr ne RADIUS ⊶sensitive.	omatically ge i client with t	nerate a sha he same sha	ared ared
Shared	l secret:					1	
Confirm	n shared secre	et:					
					ПК	C:	maal

Using the RADIUS client template

Configuring RADIUS Accounting

- 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



© 2013 John Wiley & Sons, Inc.



Accounting configuring options

Accounting Configuration Wizard
Select 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.
Previous Next Finish Cancel

Selecting Accounting options

Accounting Configuration Wizard	x
Configure SQL Server Logging Configure both the SQL Data Link in NPS and the database in SQL Server	
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.	1
Configure Clear	i
 Logging information: Select the information that NPS logs to the SQL Server database. Accounting requests 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. If logging fails, discard connection requests. To continue, click Next. 	
Previous Next Finish Cancel]

Configuring SQL Server logging

💼 Data Link Properties 🗙				
Connection Advanced All				
Specify the following to connect to SQL Server data: 1. Select or enter a server name: Refresh 2. Enter information to log on to the server:				
O Use Windows NT Integrated security				
Use a specific user name and password:				
User name:				
Password: Allow saving password				
3. • Select the database on the server:				
✓				
 Attach a database file as a database name: 				
Using the filename:				
Test Connection				
OK Cancel Help				

Configuring the Data Link properties

Accounting Configuration Wizard
Configure Local File Logging
Logging information: Select the information that will be logged to the configured text file. 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 format Inyymm.log. C:\Windows\system32\LogFiles 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.
Previous Next Finish Cancel

Configuring local file logging

Log File Properties

Log File Properties	Log File Properties
Settings Log File Log the following information: Accounting requests Accounting requests Authentication requests Periodic accounting status Periodic authentication status Logging failure action: If logging fails, discard connection requests.	Settings Log File Name: INyymm.log Directory: Image: Compliant for the state of the
OK Cancel Apply	OK Cancel Apply

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:
 - O Customized using certificate templatesO 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

Properties of New Template					x
Subject Name	Sei	Server Issuance		Requirements	
Compatibility 0	ieneral	Reque	st Handling	Cryptography	
Superseded Temp	olates	Ex	tensions	Security	
Group or user names:	Group or user names:				
& Authenticated U	sers				
Administrator					
Bornain Admins	CONTOSO	NDomain.	Admins)		
Domain Lompute	ars (CONTO) • (CONTO)	20\Extern	ain Computers) price Admine)		
	is (CONTO;	oo verkeit	nse Auninsj		
			LF V	Berroue	
			Auu	nelliuve	
Permissions for Domain Computers Allow Deny					
Full Control					
Read					
Write					
Enroll			✓		
Autoenroll					
Ear appoint permissions or advanced settings, click					
Advanced.					
Learn about access control and permissions					
04		Canaal	Applu	Hala	
UK		Cancel	Apply	Help	

Configuring security for a template

Automatically Add Workstation Authentication Certificates to All Workstations

Certificate Services Client - Auto-Enrollment Pro ? ×				
Enrollment Policy Configuration				
Enroll user and computer certificates automatically				
Configuration Model:	Not configured			
Learn more about Automatic certificate management				
ок	Cancel Apply			

Configuring 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.

Copyright 2013 John Wiley & Sons, Inc.

All rights reserved. Reproduction or translation of this work beyond that named in Section 117 of the 1976 United States Copyright Act without the express written consent of the copyright owner is unlawful. Requests for further information should be addressed to the Permissions Department, John Wiley & Sons, Inc. The purchaser may make back-up copies for his/her own use only and not for distribution or resale. The Publisher assumes no responsibility for errors, omissions, or damages, caused by the use of these programs or from the use of the information contained herein.



