### Lesson 11: Configuring DirectAccess

MOAC 70-411: Administering Windows Server 2012



WILEY

### Overview

- Exam Objective 3.4: Configure DirectAccess
- Understanding DirectAccess

### Understanding DirectAccess

Lesson 11: Configuring DirectAccess

© 2013 John Wiley & Sons, Inc.

## DirectAccess

- Overcomes limitations of VPNs
- Automatically establishes a bi-directional connection from client computers to the network using IPsec and IPv6
- Transition mechanisms for IPv6:
  - o 6to4
  - o Teredo
  - Intra-Site Automatic Tunnel Addressing (ISATAP)

# DirectAccess Connection Process

- 1. The DirectAccess client computer running Windows 8, Windows 7 Enterprise, or Windows 7 Ultimate detects that it is connected to a network.
- 2. The DirectAccess client computer determines whether it is connected to the intranet. If the client is connected to the intranet, it does not use DirectAccess.
- 3. The DirectAccess client connects to the DirectAccess server by using IPv6 and IPsec.
- 4. If the client is not using IPv6, it will try to use 6to4 or Teredo tunneling to send IPv4-encapsulated IPv6 traffic.
- 5. If the client cannot reach the DirectAccess server using 6to4 or Teredo tunneling, the client tries to connect using the Internet Protocol over Secure Hypertext Transfer Protocol (IP-HTTPS) protocol. IP-HTTPS uses a Secure Sockets Layer (SSL) connection to encapsulate IPv6 traffic.

# DirectAccess Connection Process

- 6. As part of establishing the IPsec session for the tunnel to reach the intranet DNS server and domain controller, the DirectAccess client and server authenticate each other using computer certificates for authentication.
- 7. If Network Access Protection (NAP) is enabled and configured for health validation, the Network Policy Server (NPS) determines whether the client is compliant with system health requirements. If it is compliant, the client receives a health certificate, which is submitted to the DirectAccess server for authentication.
- 8. When the user logs on, the DirectAccess client establishes a second IPsec tunnel to access the resources of the intranet. The DirectAccess client and server authenticate each other using a combination of computer and user credentials.
- 9. The DirectAccess server forwards traffic between the DirectAccess client and the intranet resources to which the user has been granted access.

# DirectAccess Server Requirements

- The server must be part of an Active Directory domain.
- The server must be running Windows Server 2008 R2 or Windows Server 2012.
- If the DirectAccess server is connected to the intranet and published over Microsoft Forefront Threat Management Gateway (TMG) or Microsoft Forefront Unified Access Gateway 2010 (UAG), a single network adapter is required.
  - If the DirectAccess server is connected as an edge server, it will need two network adapters (one for the Internet and one for the intranet).

# DirectAccess Server Requirements

- Implementation of DirectAccess in Windows Server 2012 does not require two consecutive static, public IPv4 addresses as was required with Windows Server 2008 R2.
  - To achieve two-factor authentication with a smart card or Operational Data Provider (OTP) deployment, DirectAccess server still needs two public IP addresses.

# DirectAccess Server Requirements

- You can deploy Windows Server 2012 DirectAccess behind a NAT support, which avoids the need for additional public addresses.
  - Only IP over HTTPS (IP-HTTPS) is deployed, allowing a secure IP tunnel to be established using a secure HTTP connection.
- With Windows Server 2012, you can use Network Load Balancing (up to eight nodes) to achieve high availability and scalability for both DirectAccess and RRAS.

# Network Infrastructure for DirectAccess

- An Active Directory domain
- Group policy
- One domain controller
- Public Key Infrastructure (PKI)
- IPsec policies

# Network Infrastructure for DirectAccess

- Internet Control Message Protocol Version 6
   (ICMPv6) Echo Request traffic
- IPv6 and transition technologies such as ISATAP, Teredo, or 6to4
- (Optional) Network Access Protection (NAP)

# DirectAccess Client Requirements

#### Operating system

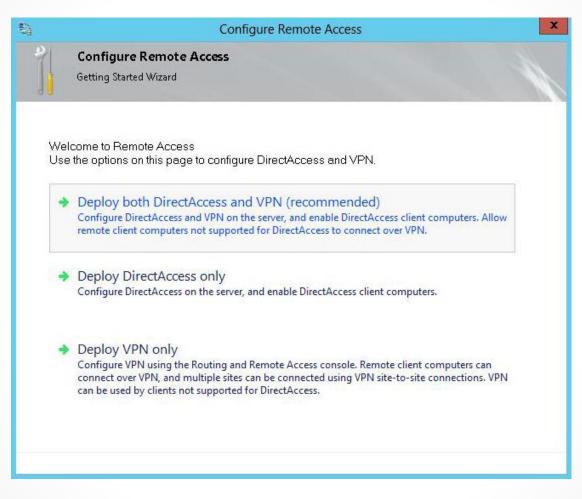
 Windows 7 Enterprise Edition, Windows 7 Ultimate Edition, Windows 8, Windows Server 2008 R2, or Windows Server 2012

Client must be joined to an Active Directory domain

- Configures DirectAccess
- Can run from Remote Access Management console

5	Remote Access Management Console		×
CONFIGURATION	Remote Access Setup	> Tasks	
DASHBOARD		General	^
OPERATIONS STATUS	Configure Remote Access, including DirectAccess and VPN.	Manage a Remote Server	
	01	Reload Configuration	
REMOTE CLIENT STATUS	Configure Remote Access	VPN	^
	DirectAccess & VPN settings have not yet been configured. Select one of the wizard options.	Open RRAS Management	
Win2012Srv2	Run the Getting Started Wizard	Learn About	^
- And	Use this wizard to configure DirectAccess and VPN quickly, with default recommended settings.	Learn About Remote Access	
	→ Run the Remote Access Setup Wizard		
	Use this wizard to configure DirectAccess and VPN with custom settings.		
	The Getting Started Wizard only appears the first time you run the Remote Access Management console. After running this wizard, click the Configuration node to edit DirectAccess and VPN settings using the Remote Access Setup Wizard.		
	[<]		

Opening the Remote Access Management console



Starting the Configure Remote Access Wizard

勒	Configure Remote Access
	Remote Access Server Setup
A A A A A A A A A A A A A A A A A A A	Configure DirectAccess and VPN settings.
Select	the network topology of the server.
O Ed	ge
⊖ Be	hind an edge device (with two network adapters)
🖲 Be	hind an edge device (with a single network adapter)
conne	topology, the Remote Access server is deployed with a single network adapter that is cted to the internal network. the public name or IPv4 address used by clients to connect to the Remote Access server:
	atum.com
	< Back Next > Finish Cancel

#### Selecting a topology on the Configure DirectAccess and VPN Settings page

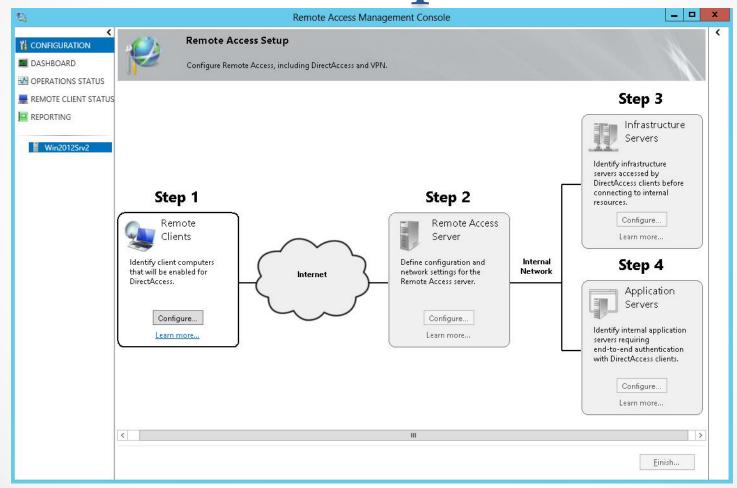
<b>S</b>	Configure Remote Access	x
	Configure Remote Access Getting Started Wizard	
Remo	ote Access settings will be applied.	
	h <u>ere</u> to edit the wizard settings. Configuration settings that can be modified include GPO settings, irectAccess client security group, server adapters, and DNS properties.	
To ar	pply the configuration settings, click Finish.	
	< <u>B</u> ack <u>N</u> ext > <u>F</u> inish Canc	el

Finishing the Getting Started Wizard

5) 5)		Remote Access Review	_ <b>_</b> X
_	Remote Access Revi	ew	
	Summary of Remote Access	configuration settings.	
Review the c	onfiguration settings.		^
💼 gpo	Settings <u>Change</u>		
CONT	roso		
Direc	tAccess server GPO name:	DirectAccess Server Settings	
Clien	t GPO name:	DirectAccess Client Settings	
Semo	ote Clients Change		
		be applied to all mobile computers in security	
			groups.
	CONTOSO\Domain C	Computers Iternal network connectivity:	
	A default web probe to ch	neck corporate connectivity will be created auto name: Workplace Connection	omatically
🛚 Remo	ote Access Server	hange	
Direct	Access configuration:		
	Public name or address to	which remote clients connect: nls.contoso.cor	1
		ed to the Internet (via NAT device): External	
	Internal network subnets:	ed to the internal network: Internal. 2002:180a:1774::/48	
🗱 Infra	structure Servers <u>c</u> r	12020	
	structure servers	lange	
•	DNS suffixes used by Dire	ctAccess clients:	
	Name Suffix	DNS Server Address	
	contoso.com	2002:180a:1774:0:18e7:587c:888b:65cc	
	nls.contoso.com		
	Win2012Srv2.contoso.com	m	~
			Save to a file   Print OK

Viewing the settings applied using the Getting Started Wizard

# Running the Remote Access Setup Wizard



# Implementing Client Configuration

#### DirectAccess Connectivity Assistant (DCA)

• Window 7 and Windows Server 2008 R2

Network Connectivity Assistant (NCA)

• Windows 8

© 2013 John Wiley & Sons, Inc.

3	Remote Access Setup	)
DirectAccess Clier Enable DirectAccess for	nt Setup managed computers in specified security groups, and configure client settings.	1
Deployment Scenario Select Groups Network Connectivity Assistant	<ul> <li>Deploy DirectAccess to allow DirectAccess client computers located on the Internet to connect to internal network resources, and remotely manage DirectAccess clients.</li> <li>Select a deployment scenario: <ul> <li>Deploy full DirectAccess for client access and remote management</li> <li>With this option selected, DirectAccess client computers located on the Internet can connect to the internal network via the Remote Access server. Administrators can remotely manage these clients.</li> <li>Deploy DirectAccess for remote management only</li> <li>Administrators can remotely manage DirectAccess client computers located on the Internet. With this option selected, DirectAccess is not deployed for client access to the internal network.</li> </ul> </li> </ul>	
	< <u>B</u> ack <u>N</u> ext > <u>F</u> inish C	ancel

Specifying the deployment scenario

5	Remote Access Setup	x
DirectAccess Clien Enable DirectAccess for	<b>t Setup</b> managed computers in specified security groups, and configure client settings.	1
Deployment Scenario Select Groups Network Connectivity Assistant	Select one or more security groups containing client computers that will be enabled for DirectAccess.       Add         Add       Remove         Image: Im	]
	< <u>B</u> ack <u>N</u> ext > <u>F</u> inish	Cancel

Selecting client groups

對	Remote Access Setup	x
DirectAccess Clier Enable DirectAccess for	t Setup managed computers in specified security groups, and configur	e client settings.
Deployment Scenario Select Groups Network Connectivity Assistant	The Network Connectivity Assistant (NCA) runs on Direct DirectAccess connectivity information, diagnostics, and r         Resources that validate connectivity to internal network: <ul> <li>Resource</li> <li>Type</li> <li>*</li> <li>Helpdesk email address:</li> <li>DirectAccess connection name:</li> <li>Worl</li> <li>Allow DirectAccess clients to use local name resolution</li> </ul>	emediation support.
		< Back Next > Finish Cancel

Configuring the Network Connectivity Assistant

<b>b</b> i	Configure Corp	orate Resources for NCA	x
Specify a co	rporate URL or FQDN that is	always accessible to DirectAccess (	clients:
HTTP Examples: ht	♥ tp://myserver.domain.com; m	nyserver.domain.com	Validate
		Add	Cancel

Configuring corporate resources for NCA

<b>S</b>	Remote Access Setup	×
	ss Server Setup .ccess and VPN settings.	1
Network Topology Network Adapters Authentication	Select the network topology of the server.  Edge  Select the network topology of the server.  Behind an edge device (with two network adapters) Behind an edge device (with a <u>single</u> network adapter) In this topology, the Remote Access server is deployed behind an edge firewall or device, and is configured with two adapters. One adapter is connected to the internal network. The other is connected to the perimeter network.  Type the public name or IPv4 address used by clients to connect to the Remote Access server:	
	< <u>B</u> ack <u>N</u> ext > <u>F</u> inish	Cancel

Specifying the network topology

Ðj	Remote Access Setup	)	×
Remote Access Configure DirectAcc	Server Setup cess and VPN settings.		
Network Topology Network Adapters Prefix Configuration	Select the network adapters on the Remote Acces	ss server. Adap <u>t</u> er connected to the inte	rnal network:
Authentication	External V Details	Internal 🗸	D <u>e</u> tails
	Select the certificate used to authenticate IP-HTT		Br <u>o</u> wse
	Transition technologies are enabled for I	Pv4 support.	Einish Cancel

Configuring the network adapters

<b>S</b>	Remote Access Setup				×
	s Server Setup cess and VPN settings.				
Network Topology Network Adapters	IPv6 settings displayed on this page have been detected	on the inter	nal network.		
Prefix Configuration Authentication	Internal network IPv6 prefixes:	100	80a:1774::/48 le: 2001:db8:ef:	3e::/48;2001:db	
	IPv6 prefix assigned to DirectAccess client computers:	12	80a:1774:1000:: le: 2001:db8:ef	ALC: NOT THE REAL PROPERTY OF	
	[	< Back	Next >	Finish	Cancel

Specifying the IPv6 prefixes

<b>\$</b> }	Remote Access Setup
Remote Access Configure DirectAcc	s Server Setup cess and VPN settings.
Network Topology Network Adapters Prefix Configuration Authentication	Specify how DirectAccess clients authenticate. If computer certificates are not used for authentication, DirectAccess as a Kerberos proxy on behalf of the client. Enable support for Windows 7 clients and Network Access Protection (NAP) compliance.         User Authentication <ul> <li>Active Directory credentials (username/password)</li> <li>Two-factor authentication (smart card or one-time password (OTP))</li> <li>Use OTP</li> <li>Use computer certificates</li> <li>Select the root or intermediate certification authority (CA) that issues the certificates.</li> <li>Use an intermediate certificate</li> <li>Browse</li> </ul> Enable Windows 7 client computers to connect via DirectAccess         Enable Windows 7 client computers to connect via DirectAccess
	< Back Next > Finish Cancel

Specifying authentication

# Implementing Infrastructure Servers

- DirectAccess clients use the *network location server (NLS)* to determine their locations.
- To configure an NLS:
  - o Install IIS on a Windows server.
  - For a website, bind a name and associate a NLS DNS name to the IP address.
  - Make sure the server is highly available.
- Ensure that DirectAccess clients can correctly detect when they are on the Internet.

€jj	Remote Access Setup
Configure infrastructure S	erver Setup ure servers. DirectAccess clients access these servers before connecting to resources on the internal network.
Network Location Server DNS DNS Suffix Search List Management	Specify settings for the network location server, used to determine the location of DirectAccess client computers. A client computer connecting successfully to the site is assumed to be on the internal network, and DirectAccess is not used. <ul> <li>The network location server is deployed on a remote web server (recommended)             Type in the URL of the network location server:</li></ul>
	< Back Next > Finish Cancel

Specifying the Network Location server

		Remote Acces	s Setup	x
Configure infrastruct			rs before connecting to resources on the internal network.	
Network Location Server DNS DNS Suffix Search List Management	the sp	pecified DNS server for name resolutio ervers are treated as exemptions, and	s. DirectAccess client queries that match a suffix use on. Name suffixes that do not have corresponding I DNS settings on client computers are used for name	
		Name Suffix	DNS Server Address	
	•	contoso.com	2002:180a:1774:0:18e7:587c:888b:65cc	
		Win2012Srv2.contoso.com		
	*			
	ຸ ບ ● ບ ແ	se local name resolution if the name or nreachable when the client computer	does not exist in DNS (most restrictive) does not exist in DNS or DNS servers are is on a private network (recommended) of DNS resolution error (least restrictive)	
			< Back Next > Finish	Cancel

#### Specifying the DNS servers

<b>\$</b> }	Remote Access	s Setup	x
Configure infrastructure S	Server Setup ture servers. DirectAccess clients access these server.	s before connecting to resources on the in	nternal network.
Network Location Server DNS DNS Suffix Search List Management	Add additional suffixes to search for short up suffix, the other suffixes are appended to the Configure DirectAccess clients with DNS	e name and the DNS query is repeated for	
NI *	Detected domain suffixes:	d -> move	×
	New	v Suffix:	Add
		< Back Next >	Finish Cancel

Specifying the DNS Suffix Search List

5) 5	Remote Access Setup	×
Configure infrastructure se	rr Setup rvers. DirectAccess clients access these servers before connecting to resources on the internal network.	
Network Location Server DNS DNS Suffix Search List	Specify management servers used for DirectAccess client management. For example update and remediation servers. —Management servers:	
Management DNS Suffix Search Li	Management Servers (IP Address, IPv6 Prefix, FQDN)	
	▶ <b>*</b>	
	After you complete the wizard and apply the settings, the management servers list will be updated with automatically-discovered System Center Configuration Manager servers.	
	< Back Next > Finish Cance	:1

Specifying the management servers

<b>\$</b> }	Add a Management Server
	Specify the management server name or address. Computer name (FQDN): win2012srv Example: engineeringcomputer1.contoso.com
(	<ul> <li>Address (IPv4;IPv6; IPv6 prefix)</li> <li>Example: 157.60.79.2</li> <li>2001:db8:ef3e:ad45:208:74ff:fe39:6c43</li> <li>2001:db8:ef3e:ad45:208:74ff:fe39:0/112</li> </ul>
	OK Cancel

Adding a management server

### Configure Application Servers for DirectAccess

割	Remote Access Setup	x
-	DirectAccess Application Server Setup	
	Optionally configure authentication between DirectAccess clients and internal application servers.	
	It, DirectAccess requires IPsec authentication and encryption between the DirectAccess client and server. In addition, you can require end-to-end authentication and encryption between DirectAccess clients and selected internal application servers.	
	not extend authentication to application servers	
	nd authentication to selected application servers ect the security groups containing the servers:	
	Add	
	Remove	
	Allow access only to servers included in the security groups	
	ith this option enabled, clients can only access application servers in the specified security groups. Clients can still access rastructure servers, including domain controllers, DNS servers, and servers used for DirectAccess client management.	
	Do not encrypt traffic. Use authentication only	
	ith this setting enabled, end-to-end traffic is authenticated but not encrypted. This option is less secure. Authentication without icryption is supported only for application servers running Windows Server 2008 R2 or a later operating system.	
	Finish Can	cel

Specifying the DirectAccess application servers

# Configuring DNS for DirectAccess

- DirectAccess requires internal and external DNS.
- DirectAccess requires two external DNS A records:
  - DirectAccess server, such as directaccess.contoso.com
  - Certificate Revocation List (CRL), such as crl.contoso.com
- Internally, DNS needs the DNS records for the NLS server and one for the CRL.

## Configuring DNS for DirectAccess

- ISATAP provides a transition between networks that are based on IPv4 to IPv6.
- If you need to use ISATAP, remove ISATAP from the DNS global query block list by executing this command:

dnscmd /config /globalqueryblocklist isatap

## Configuring Certificates for DirectAccess

The DirectAccess server requires these certificates:

- The IP-HTTPS listener on the DirectAccess server requires a Web site certificate
- The DirectAccess client must be able to contact the server hosting the CRL for the certificate.
- The DirectAccess server requires a computer server to establish the IPsec connections with the DirectAccess clients.

Auditing Re Storage   Policy Module (CA) contoso-WIN2012S		Security Managers t Module
Policy Module (CA)	Exit	
(CA)		t Module
	RV-CA-1	
CURIOSU-WINZUTZ5	NV-CA-1	
	View C	ertificate
8		
Microsoft Software K	ley Storage Provi	ider
SHA1		
Cancel	Apply	Help
5	Microsoft Software K SHA1	s Microsoft Software Key Storage Provi SHA1

Displaying the CA certificates

contoso-WIN	2012SRV-C/	A-1 Prop	erties	?	х
Enrollment Agents	Auditing	Recove	ery Agents	Sec	urity
General	Policy Me	odule	Exit	Module	
Extensions	Storage		Certificate M	lanager:	s
Select extension: CRL Distribution Poin Specify locations from (CRL). C:\Windows\system3 Idap:///CN= <catrun http://<serverdnsna< td=""><td>which users car 2\CertSrv\CertB catedName&gt;<c ame&gt;/CertEnrol</c </td><td>Enroll\<can RLNameSu I/<caname< td=""><td>lame&gt;<crln uffix&gt;,CN=<se &gt;<crlnames< td=""><td>ameSufl rverSho Suffix&gt;&lt;[</td><td>fix≻≺l rtNai Delta</td></crlnames<></se </crln </td></caname<></can </td></serverdnsna<></catrun 	which users car 2\CertSrv\CertB catedName> <c ame&gt;/CertEnrol</c 	Enroll\ <can RLNameSu I/<caname< td=""><td>lame&gt;<crln uffix&gt;,CN=<se &gt;<crlnames< td=""><td>ameSufl rverSho Suffix&gt;&lt;[</td><td>fix≻≺l rtNai Delta</td></crlnames<></se </crln </td></caname<></can 	lame> <crln uffix&gt;,CN=<se &gt;<crlnames< td=""><td>ameSufl rverSho Suffix&gt;&lt;[</td><td>fix≻≺l rtNai Delta</td></crlnames<></se </crln 	ameSufl rverSho Suffix><[	fix≻≺l rtNai Delta
< III			dd	Remov	>
Publish CRLs to thi	is location				
<ul> <li>Include in all CRLs when publishing m</li> <li>Include in CRLs. C</li> <li>Include in the CDP</li> <li>Publish Delta CRLs</li> <li>Include in the IDP</li> </ul>	anually. lients use this to extension of iss s to this location	find Delta ( sued certific	CRL locations		ſy
ОК	Cano	el	Apply	He	əlp

Specifying certificate extensions

Add Location	x
A location can be any valid URL or path. Enter an HTTP, LDAP, file addre or enter a UNC or local path. To insert a variable into the URL or path, sele the variable below and click Insert.	
Location:	
Variable:	
<caname> V Insert</caname>	
Description of selected variable:	
Used in URLs and paths Inserts the DNS name of the server Example location: http:// <serverdnsname>/CertEnroll/<caname><crl< td=""><td>Na</td></crl<></caname></serverdnsname>	Na
< III	>
OK Cancel	

Adding a Location for CRL

Add Location	x
A location can be any valid URL or path. Enter an HTTP, LDAP, file addre or enter a UNC or local path. To insert a variable into the URL or path, sele the variable below and click Insert.	
Location:	
ittp://crl.adatum.com/crld/ <caname><crlnamesuffix><deltacrlallowe< td=""><td>;d&gt;</td></deltacrlallowe<></crlnamesuffix></caname>	;d>
Variable:	
<deltacrlallowed> V Insert</deltacrlallowed>	
Description of selected variable:	
Used in URLs and paths Substitutes the Delta CRL file name suffix for the CRL file name suffix, if ap Example location: http:// <servername>/CertEnroll/<caname><crlnam< td=""><td></td></crlnam<></caname></servername>	
<	>
OK Cancel	

An example location for CRL

	Properties	of New	/ Template	X
Subject Name	Se	rver	Issuance	Requirements
Superseded T	emplates	Ex	tensions	Security
Compatibility	General	Reque	st Handling	Cryptography
The template opti versions set in Co			on the earliest o	operating system
Show resulting	; changes			
Compatibility Se	ttings			
Certification Au	athority			
Windows Serv	ver 2003		~	
Certificate recip			~	
These settings ma template.		earlier ope	rating systems	from using this

Opening the properties of a certificate template

	Properties	of New	/ Template	x
Subject Name	Ser	ver	Issuance	Requirements
Superseded To	emplates	Ex	tensions	Security
Compatibility	General	Reque	st Handling	Cryptography
Template display r	name:			
Copy of Web Ser	ver			
Template name: Copy of Web Ser	ver			
Validity period:	~	Renew 6	val period: weeks	·
Publish certifica Do not auto Directory			olicate certificat	e exists in Active
(	ЭК І	Cancel	Apply	Help

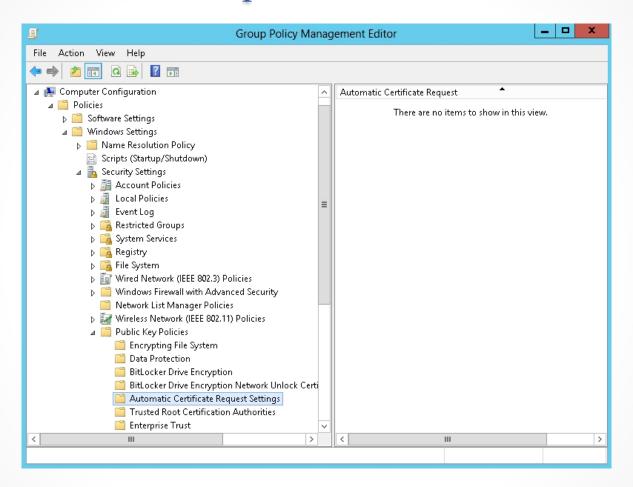
Defining the template display name and template name

	Propertie	s of Nev	v Template	×	5		
Subject Name	e S	erver	Issuance	Requirements			
Superseded 1	Templates	E>	tensions	Security			
Compatibility	General	Reque	est Handling	Cryptography			
Purpose:	Signature and	d encryptior	1	¥			
	Delete revo	oked or exp	ired certificates	(do not archive)			
	 Include svr	nmetric alor	prithms allowed	by the subject			
Authorize add	litional service	accounts t	o access the pr	ivate key (*)			
Key Permiss	sions						
Allow private	key to be expo	orted					
Renew with t	he same key ('	°)					
Renew with the same key (*) For automatic renewal of smart card certificates, use the existing key if a new key cannot be created (*)							
Do the following associated with t			ed and when th	e private key			
Enroll subject	without requiri	ing any use	r input				
O Prompt the us	er during enro	llment					
O Prompt the us private key is		llment and i	equire user inpl	ut when the			
* Control is disab	led due to <u>com</u>	npatibility se	ttings.				
	OK	Cancel	Apply	Help	]		

Specifying the purpose of the certificate

Pro	perties	of New	/ Template		x
Subject Name	Ser	ver	Issuance	Requirements	
Compatibility G	eneral	Reque	st Handling	Cryptograph	y
Superseded Temp	ates	Ex	tensions	Security	
Group or user names:					
Authenticated Us Administrator & Domain Admins (I & Enterprise Admin:	CONTOSO		,		
Permissions for Auther	iticated Use	ers	Add Allow	Remove Deny	
Full Control					
Read			✓		
Write					
Enroll					
Autoenroll					
E For special permission: Advanced. Learn about access co				Advanced	
OK		Cancel	Apply	Help	

Specifying the permissions assigned to the certificate template



#### Viewing the Public Key policies

provided. A certificate template is a set of prede	
A certificate template is a set of prede	
A centineate template is a set of preut	stinged properties for certificates issued to
computers. Select a template from the	
C <u>e</u> rtificate templates:	
Name	Intended Purposes
Computer	Client Authentication, Server Authentication
Domain Controller	Client Authentication, Server Authenticatior
Enrollment Agent (Computer)	Certificate Request Agent
IPSec	IP security IKE intermediate
<	>
< 111	>
< 111	>
< 111	>
< III	<ul> <li>A Back</li> <li>Next &gt;</li> <li>Cancel</li> </ul>

Specifying which certificates are automatically requested

inap-in Active Directory Do	Vendor Microsoft Cor Microsoft Cor	^		Selected snap-ins:	Edit Extensions
Active Directory Use Active Directory Use ActiveX Control		=			Move Up
Authorization Manager Certificates Component Services Computer Managem Device Manager DFS Management Disk Management	Microsoft Cor Microsoft Cor Microsoft Cor		Add >		Move Down
SDNS Event Viewer scription:	Microsoft Cor Microsoft Cor	~			Advanced

Opening the Add or Remove Snap-ins dialog box

	Certifica	tes snap-in		x
This snap-in will always manag	je certificates for:			
My user account				
<ul> <li>Service account</li> </ul>				
O Computer account				
		< Back	Finish	Cancel

Specifying which certificates to manage

	Select	Computer		Ļ
Select the computer you wa	ant this snap-in to m	anage.		
This snap-in will always m	anage:			
Local computer: (the	computer this cons	ole is running on)		
O Another computer:			Browse	Ĩ
Allow the selected co	omputer to be chan	ged when launching from the	command line. This	
only applies if you sa				
		< Back F	inish Cance	el

Selecting which computer to connect to

		ele Root\Certificates (Local	Computer)\Pers	sonal\Certificates]		
🚡 File Action View Favorites 👉 🔿 🙍 🔐 🔏 😭 🗙 🛙	s Window Help					- 8 >
Console Root	Issued To	Issued By contoso-WIN2012SRV-CA-1	Expiration Date 9/1/2013	Intended Purposes Client Authenticati	Certificate Template Computer	Actions Certifica A More A Win201 A More A

Viewing the computer certificate

equest Certificates		
ou can request the following types of cer ick Enroll.	ificates. Select the certificates you want t	o request, and ther
Active Directory Enrollment Policy		
Computer	🤹 STATUS: Available	Details
Contoso Web Server Certificate	i) STATUS: Available	Detail:
A More information is required to	enroll for this certificate. Click here to c	onigure settings.
More information is required to	enroll for this certificate. Click here to c	oningure settings.

Requesting a certificate

		C	ertificate P	Properties	×
🛕 Subject	General	Extensions	Private Key	Certification Authority	Signature
	formation	h about the f		uter to which the certi ect name and alternativ	
Subject of c	ertificate				
The user or	compute	r that is rece	iving the cert	tificate	
Subject nam	ne:				
Type:			-		
Full DN		~	Add	>	
Value:			< Rem	ove	
L Alternative r	name:				
Туре:					
Directory r	name	~			
Value:			Add	>	
			< Rem	ove	
Learn more :	about <u>suk</u>	oject names			
				OK Car	ncel Apply

Specifying the subject of a certificate

	Add Site Bin	ding	? X
Type: https v Host name: nls.contoso.com	IP address: All Unassigned me Indication	Port:	
SSL certificate: nls.contoso.com		✓ Select	View
		ОК	Cancel

Configuring an IIS site binding

## Troubleshooting DirectAccess

- The DirectAccess client computer must run Windows 8, Windows 7 Ultimate, or Windows 7 Enterprise edition.
- The DirectAccess client computer must be a member of an Active Directory Domain Services (AD DS) domain and its computer account must be a member of one of the security groups configured with the DirectAccess Setup Wizard.
- The DirectAccess client computer must have received computer configuration Group Policy settings for DirectAccess.
- The DirectAccess client must have a global IPv6 address, which should begin with a 2 or 3.

## Troubleshooting DirectAccess

- The DirectAccess client must be able to reach the IPv6 addresses of the DirectAccess server.
- The DirectAccess client on the Internet must correctly determine that it is not on the intranet. You can type the netsh dnsclient show state command to view the network location displayed in the Machine Location field (outside corporate network or inside corporate network).
- Use the netsh namespace show policy command to show the NRPT rules as configured on the group policy.
- Use the netsh namespace show effectivepolicy command to determine the results of network location detection and the IPv6 addresses of the intranet DNS servers.

## Troubleshooting DirectAccess

- The DirectAccess client must not be assigned the domain firewall profile.
- The DirectAccess client must be able to reach the organization's intranet DNS servers using IPv6. You can use Ping to attempt to reach the IPv6 addresses of intranet servers.
- The DirectAccess client must be able to communicate with intranet servers using application layer protocols. If File and Printer Sharing is enabled on the intranet server, test application layer protocol access by typing net view \\IntranetFQDN.
- Use the DirectAccess Connectivity Assistant on computers running Windows 7 and Network Connectivity Assistant on computers running Windows 8 to determine the intranet connectivity status and to provide diagnostic information.

# Lesson Summary

- DirectAccess provides seamless intranet connectivity to DirectAccess client computers when they are connected to the Internet; connections are automatically established and they provide always-on seamless connectivity.
- The Name Resolution Policy Table (NRPT) is used to determine the behavior of the DNS clients when issuing queries and processing so that internal resources are not exposed to the public via the Internet, and to separate traffic that is not DirectAccess Internet traffic from traffic that is.
- To use DirectAccess, clients must be Windows 7 Enterprise Edition, Windows 7 Ultimate Edition, Windows 8, Windows Server 2008 R2, or Windows Server 2012.

# Lesson Summary

- In Windows 8, the DCA was replaced by the Network Connectivity Assistant (NCA).
- The DirectAccess Connectivity Assistant (DCA) provides tools to help users reconnect if a problem occurs and helps with diagnostics used by the help desk. It is also used to detect whether one-time passwords (OTP) are required and helps your system determine whether it is connected to the intranet or the Internet.
- DirectAccess clients use the network location server (NLS) to determine their location. NLS is an internal web server.
- Before deploying DirectAccess, you need to make sure that you have IPv6 and any transitional IPv6 technologies in place, a certificate server, and external and internal DNS entries.

#### 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.



