Module Overview

- Overview of Remote Access
- Implementing DirectAccess by Using the Getting Started Wizard
- Implementing and Managing an Advanced DirectAccess Infrastructure
- Implementing VPN
- Implementing Web Application Proxy
Lesson 1: Overview of Remote Access

- Remote Access Options
- Demonstration: Installing and Managing the Remote Access Role
- Network Address Translation
- Considerations for Deploying a PKI for Remote Access
- Configuring User Settings for Remote Access

Remote Access Options

Remote access options in Windows Server 2012 R2 include:
- DirectAccess
- VPN
- Routing
- Web Application Proxy
Managing Remote Access in Windows Server 2012

You can manage the Remote Access role by using:
• Remote Access Management Console
• Routing and Remote Access console
• Windows PowerShell cmdlets:
  • `Set-DAServer`
  • `Get-DAServer`
  • `Set-RemoteAccess`
  • `Get-RemoteAccess`

Demonstration: Installing and Managing the Remote Access Role

In this demonstration, you will see how to:
• Install the Remote Access role
• Manage the Remote Access role
Network Address Translation

Internet websites

NAT server

Corporate computers

131.107.0.10

172.16.0.51

172.16.0.10

172.16.0.50
## Considerations for Deploying a PKI for Remote Access

- Will you use PKI for encryption of only data and traffic?
- Will you use PKI not just for encryption, but also for authenticating users and their computers?
- Will you use self-signed certificates, certificates provided by internal private CAs, or external public CAs?

## Configuring User Settings for Remote Access

User Settings for Remote Access include:

- **Network Access Permission**
  - Allow access
  - Deny access
  - Control access through NPS Network Policy
- **Verify Caller-ID**
- **Callback Options**
- **Assign Static IP Addresses**
- **Apply Static Routes**
Lesson 2: Implementing DirectAccess by Using the Getting Started Wizard

- DirectAccess Components
- DirectAccess Server Deployment Options
- DirectAccess Tunneling Protocol Options
- How DirectAccess Works for Internal Clients
- How DirectAccess Works for External Clients
- Demonstration: Running the Getting Started Wizard
- Getting Started Wizard Configuration Changes
- Demonstration: Identifying the Getting Started Wizard Settings
- Limitations of DirectAccess Deployments When Using the Getting Started Wizard
DirectAccess Server Deployment Options

DirectAccess server deployment options include:

- Deploying multiple endpoints
- Supporting Multiple domains
- Deploying a server behind a NAT
- Supporting OTP and virtual smart cards
- Supporting NIC Teaming
- Provisioning Off-premise

DirectAccess Tunneling Protocol Options

DirectAccess tunneling protocols include:

- ISATAP – Tunnels IPv6 traffic over IPv4 networks for intranet communication
- 6to4 – Used by DirectAccess clients with a public IP address
- Teredo – Used by DirectAccess clients with a private IP address behind a NAT device
- IP HTTPS – Used by DirectAccess clients if they are not able to use ISATAP, 6to4, or Teredo
How DirectAccess Works for Internal Clients

- Internet websites
- DirectAccess server
- NRPT
- DNS server
- Internal client computers
- Connection security rules
- CRL distribution point
- NLS
- AD DS domain controller

How DirectAccess Works for External Clients

- External client computers
- DNS server
- NRPT
- Connection security rules
- AD DS domain controller
- DNS server
- Internal network resources
- AD DS domain controller
- DNS server
- DirectAccess server
Demonstration: Running the Getting Started Wizard

In this demonstration, you will see how to configure DirectAccess by running the Getting Started Wizard
Getting Started Wizard Configuration Changes

Changes made by the Getting Started Wizard include:

- GPO settings
  - DirectAccess Server Settings GPO
  - DirectAccess Client Settings GPO
- Remote clients
- Remote access servers
- Infrastructure servers
Demonstration: Identifying the Getting Started Wizard Settings

In this demonstration, you will see how to identify changes made by the DirectAccess Getting Started Wizard
Limitations of DirectAccess Deployments When Using the Getting Started Wizard

- Certificates
  - Self-signed certificates cannot be used in multisite deployments
  - Require you to ensure the CRL distribution point for both certificates is available externally
- Network Location Server Design
  - Deploys the Network Location Server on the same server as the DirectAccess server
- Windows client operating system support
  - Getting Started Wizard configuration is applicable for clients running Windows 8 or Windows Server 2012
  - Windows 7 clients require a client certificate for IPsec authentication
Lab A: Implementing DirectAccess by Using the Getting Started Wizard

- Exercise 1: Verifying Readiness for a DirectAccess Deployment
- Exercise 2: Configuring DirectAccess
- Exercise 3: Validating the DirectAccess Deployment

Logon Information
Virtual Machine(s): 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-RTR, 20411D-LON-CL1
User Name: Adatum\Administrator
Password: Pa$$w0rd

Virtual Machine(s): 20411D-INET1
User Name: Administrator
Password: Pa$$w0rd
Estimated Time: 30 minutes

Lab Scenario

Many users at A. Datum Corporation work from outside the organization. This includes mobile users as well as people who work from home. These users currently connect to the internal network by using a third-party VPN solution. The security department is concerned about the security of the external connections and wants to ensure that the connections are as secure as possible. The support team wants to minimize the number of support calls related to remote access, and would like to have more options for managing remote computers.
Lab Scenario

Information Technology (IT) management at A. Datum is considering deploying DirectAccess as the remote access solution for the organization. As an initial proof-of-concept deployment, management has requested that you configure a simple DirectAccess environment that can be used with client computers running Windows 8.

Lab Review

• Why did you create the DA_Clients group?
• How will you configure IPv6 addresses for client computers running the Windows® 8 operating system to use DirectAccess?
Lesson 3: Implementing and Managing an Advanced DirectAccess Infrastructure

- Overview of the Advanced DirectAccess Options
- Integrating a PKI with DirectAccess
- Implementing Client Certificates for DirectAccess
- Internal Network Configuration Options
- Configuring Advanced DNS Settings
- Implementing Network Location Servers
- Implementing Management Servers
- Demonstration: Modifying the DirectAccess Infrastructure
- How to Monitor DirectAccess Connectivity
- How to Troubleshoot DirectAccess Connectivity
- Demonstration: Monitoring and Troubleshooting DirectAccess Connectivity

Overview of the Advanced DirectAccess Options

Advanced DirectAccess configuration options include:
- Scalable and customized PKI infrastructure
- Customized network configuration options
- Scalable and highly-available server deployment
- Customized monitoring and troubleshooting
Integrating a PKI with DirectAccess

Configuring PKI for DirectAccess includes the following steps:
1. Add and configure the CA server role if not already present
2. Create the certificate template
3. Create a CRL distribution point and publish the CRL list
4. Distribute the computer certificates

Implementing Client Certificates for DirectAccess

A computer certificate for IPSec authentication is required for DirectAccess clients running Windows 7

Steps for deploying certificates for client computers:
1. Create a GPO and link it to the organizational unit that contains the DirectAccess clients
2. Configure the GPO for automatic certificate request for the computer account
3. Apply the GPO
4. Verify that the certificates are issued
Internal Network Configuration Options

Planning for internal network configuration requires you to plan for:
• DirectAccess server location (Edge, perimeter network, or internal network)
• IP address assignment
• Firewall configuration
• Active Directory
• Client deployment

Configuring Advanced DNS Settings

DirectAccess uses DNS for resolving:
• Network location server
• IP-HTTPS
• CRL distribution point
• ISATAP
• Connectivity verifiers
You can configure NRPT by using Group Policy with the following settings:
• DNS suffixes
• CRL distribution point
• Split-brain DNS
Implementing Network Location Servers

Network location server can be located on:
- A DirectAccess server
- Another server with IIS installed

Requirements for network location server configuration:
- Network location server web site certificate
- CA that is trusted by DirectAccess clients
- Network location server web site certificate CRL
- Network location server should be accessible by internal clients
- Network location server should not be accessible by Internet clients
- Network location server should be highly available

Implementing Management Servers

Management servers in DirectAccess are:
- Domain controllers
- SCCM servers

Management servers are detected by DirectAccess:
- Automatically
- Manually if modified

Management server requirements:
- Must be accessible for the infrastructure tunnel
- Must fully support IPv6
Demonstration: Modifying the DirectAccess Infrastructure

In this demonstration, you will see how to:
• Modify the DirectAccess infrastructure deployed by using the Getting Started Wizard
• Apply advanced configuration settings
How to Monitor DirectAccess Connectivity

Remote Access Management Console monitoring components:
  - Dashboard
  - Operations Status
  - Remote Access Client Status
  - Remote Access Reporting

How to Troubleshoot DirectAccess Connectivity

You can troubleshoot DirectAccess connectivity by using:
  - A troubleshooting methodology
  - Command-line tools
  - GUI tools
Demonstration: Monitoring and Troubleshooting DirectAccess Connectivity

In this demonstration, you will see how to monitor and troubleshoot DirectAccess connectivity.
Lab B: Deploying an Advanced DirectAccess Solution

• Exercise 1: Preparing the Environment for DirectAccess
• Exercise 2: Implementing the Advanced DirectAccess Infrastructure
• Exercise 3: Validating the DirectAccess Deployment

Logon Information

Virtual Machine(s): 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-RTR, 20411D-LON-CL1, 20411D-LON-CL3
User Name: Adatum\Administrator
Password: Pa$$w0rd

Virtual Machine(s): 20411D-INET1
User Name: Administrator
Password: Pa$$w0rd

Estimated Time: 60 minutes
Lab Scenario

The proof-of-concept deployment of DirectAccess was a success, so IT management has decided to enable DirectAccess for all mobile clients, including computers running Windows 7. IT management also wants to ensure that the DirectAccess deployment is scalable and provides redundancy.

You need to modify the proof-of-concept deployment to meet the new requirements.

Lab Review

• Why did you make the CRL available on the edge server?
• Why did you install a certificate on the client computer?
Lesson 4: Implementing VPN

- VPN Scenarios
- VPN Tunneling Protocol Options
- VPN Authentication Options
- What Is VPN Reconnect?
- VPN Configuration by Using the Getting Started Wizard
- Options for Modifying the VPN Configuration
- Demonstration: Configuring VPN
- What Is the Connection Manager Administration Kit?
- Demonstration: How to Create a Connection Profile

VPN Scenarios

A VPN provides a point-to-point connection between components of a private network, through a public network such as the Internet.
## VPN Tunneling Protocol Options

Windows Server 2012 supports four VPN tunneling protocols:

<table>
<thead>
<tr>
<th>Tunneling protocol</th>
<th>Firewall access</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>PPTP</td>
<td>TCP port 1723</td>
<td>Provides data confidentiality but not data integrity or data authentication.</td>
</tr>
<tr>
<td>L2TP/IPsec</td>
<td>UDP port 500, UDP port 1701, UDP port 4500, and IP protocol ID 50</td>
<td>Uses either certificates or preshared keys for authentication. Certificate authentication is recommended.</td>
</tr>
<tr>
<td>SSTP</td>
<td>TCP port 443</td>
<td>Uses SSL to provide data confidentiality, data integrity, and data authentication.</td>
</tr>
<tr>
<td>IKEv2</td>
<td>UDP port 500</td>
<td>Supports the latest IPsec encryption algorithms to provide data confidentiality, data integrity, and data authentication.</td>
</tr>
</tbody>
</table>

## VPN Authentication Options

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Description</th>
<th>Security level</th>
</tr>
</thead>
<tbody>
<tr>
<td>PAP</td>
<td>Uses plaintext passwords. Typically used if the remote access client and remote access server cannot negotiate a more secure form of validation.</td>
<td>The least secure authentication protocol. Does not protect against replay attacks, remote client impersonation, or remote server impersonation.</td>
</tr>
<tr>
<td>CHAP</td>
<td>A challenge-response authentication protocol that uses the industry-standard MD5 hashing scheme.</td>
<td>An improvement over PAP in that the password is not sent over the PPP link Requires a plaintext version of the password to validate the challenge response. Does not protect against remote server impersonation.</td>
</tr>
<tr>
<td>MS-CHAPv2</td>
<td>An upgrade of MS-CHAP. Provides two-way authentication, also known as mutual authentication. The remote access client receives verification that the remote access server to which it is dialing in to has access to the user's password.</td>
<td>Provides stronger security than CHAP.</td>
</tr>
<tr>
<td>EAP</td>
<td>Allows for arbitrary authentication of a remote access connection through the use of authentication schemes, known as EAP types.</td>
<td>Offers the strongest security by providing the most flexibility in authentication variations.</td>
</tr>
</tbody>
</table>
What Is VPN Reconnect?

VPN Reconnect maintains connectivity across network outages

- VPN Reconnect:
  - Provides seamless and consistent VPN connectivity
  - Uses the IKEv2 technology
  - Automatically reestablishes VPN connections when connectivity is available
  - Maintains the connection if users move between different networks
  - Provides transparent connection status to users

VPN Configuration by Using the Getting Started Wizard

Configure VPN by using the Getting Started Wizard in the Remote Access Management console

VPN server configuration requirements include:
- Two network interfaces (public and private)
- IP Address allocation (static pool or DHCP)
- Authentication provider (NPS/RADIUS or the VPN server)
- DHCP relay agent considerations
- Membership in the local Administrators group or equivalent
Options for Modifying the VPN Configuration

You may need to perform additional steps to help secure the installation of the VPN solution:
- Configure static packet filters
- Configure services and ports
- Adjust logging levels for routing protocols
- Configure number of available VPN ports
- Create a Connection Manager profile for users
- Add AD CS
- Increase remote access security
- Increase VPN security
- Consider implementing VPN Reconnect

Demonstration: Configuring VPN

In this demonstration, you will see how to:
- Review the default VPN configuration
- Verify certificate requirements for IKEv2 and SSTP
- Configure the remote access server
What Is the Connection Manager Administration Kit?

The CMAK:
• Allows you to customize users’ remote connection experiences by creating predefined connections on remote servers and networks
• Creates an executable file that can be run on a client computer to establish a network connection that you have designed
• Reduces Help Desk requests related to the configuration of RAS connections by:
  • Assisting in problem resolution because the configuration is known
  • Reducing the likelihood of user errors when users configure their own connection objects

Demonstration: How to Create a Connection Profile

In this demonstration, you will see how to:
• Install the CMAK feature
• Create a connection profile
• Examine the profile
Lab C: Implementing VPN

- Exercise 1: Implementing VPN
- Exercise 2: Validating the VPN Deployment

Logon Information

**Virtual Machine(s):** 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-RTR, 20411D-LON-CL1

**User Name:** Adatum\Administrator

**Password:** Pa$$w0rd

Estimated Time: 45 minutes

Lab Scenario

The DirectAccess deployment is working very well, but a number of computers at A. Datum cannot connect by using DirectAccess. For example, some home users are using computers that are not members of the A.Datum.com domain. Other users are running operating system versions that do not support DirectAccess. To enable remote access for these computers, you must deploy a VPN solution.
Lab Review

• In the lab, you configured the VPN server to allocate an IP address configuration by using a static pool of addresses. Is there a way to automate IP configuration?
• Why was DirectAccess not working when we removed LON-CL1 from the Adatum.com domain?

Lesson 5: Implementing Web Application Proxy

• What Is Web Application Proxy?
• What is ADFS
• Authentication Options for Web Application Proxy
• Publishing Applications with Web Application Proxy
• Demonstration: Publishing a Secure Website
What Is Web Application Proxy?

Web Application Proxy:
• Is introduced in Windows Server 2012 R2
• Functions as a reverse web proxy
• Uses AD FS proxy functionality
• Is located in a perimeter network

What is AD FS

AD FS is the Microsoft identity federation solution that can use claims-based authentication

AD FS includes the following features:
• Web SSO
• Web services interoperability
• Support for different types of clients
• Extensible architecture
• Enhanced security
Authentication Options for Web Application Proxy

User authentication:
• AD FS pre-authentication
• Pass-through pre-authentication

AD FS benefits:
• Workplace join
• SSO
• Multifactor authentication
• Multifactor access control

Publishing Applications with Web Application Proxy

• Configuring Web Application Proxy settings
  • AD FS server name
  • AD FS administrator credentials
  • AD FS certificate

• Publishing Web Application
  • Type of preauthentication, for example Pass-through
  • Details of the application that will be published
  • The external URL of the application, for example, https://lon-svr1.adatum.com/
  • A certificate whose subject name covers the external URL, for example lon-svr1.adatum.com
  • URL of the back end server
Demonstration: Publishing a Secure Website

In this demonstration, you will see how to:
• Install the Web Application Proxy role service
• Configure access to an internal web site
• Disable DirectAccess on a client computer
• Verify access to the internal web site from the client computer
<table>
<thead>
<tr>
<th>Lab D: Implementing Web Application Proxy</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Exercise 1: Implementing Web Application Proxy</td>
</tr>
<tr>
<td>• Exercise 2: Validating the Web Application Proxy Deployment</td>
</tr>
</tbody>
</table>

Logon Information
**Virtual Machine(s):** 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-SVR4, 20411D-LON-RTR, 20411D-LON-CL1
**User Name:** Adatum\Administrator
**Password:** Pa$$w0rd

**Virtual Machine(s):** 20411D-INET1
**User Name:** Administrator
**Password:** Pa$$w0rd
Estimated Time: 30 minutes
Lab Scenario

The remote access deployment is working very well at A. Datum, but IT management also wants to enable users from partner companies to access some internal applications. These users should not have access to any internal resources except for the specified applications. You need to implement and test Web Application Proxy for these users.

Lab Review

- Where should we deploy the Web Application Proxy server?
- What is required for a client to be able to access a published application?
<table>
<thead>
<tr>
<th>Module Review and Takeaways</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Review Question(s)</td>
</tr>
<tr>
<td>• Tools</td>
</tr>
<tr>
<td>• Best Practices</td>
</tr>
<tr>
<td>• Common Issues and Troubleshooting Tips</td>
</tr>
</tbody>
</table>