6421B: How to Install and Configure DirectAccess

Demonstration Overview

Introduction

In preparation for this demonstration, the following computers have been configured:

- NYC-DC1 – is an Active Directory Domain Services (AD DS) domain controller and DNS server in the Contoso.com domain. This computer is also configured as an Enterprise Root Certification Authority.
- NYC-NLS – This is a web server in the Contoso.com domain. This computer will be configured as the NLS for DirectAccess deployment.
- NYC-SVR1 – This is a web and file server in the Contoso.com domain. This computer will be used to test the internal and external access to Intranet resources. A website and shared folder have been configured on this server.
- NYC-DAS – This is a server in the Contoso.com domain. This computer will be configured as the DirectAccess server.
- NYC-CL1 – This is a Windows 7 client computer in the Contoso.com domain. This computer will be used as the DirectAccess client computer.
- Web – web is a standalone server. This server will be used as the Internet DNS server, DHCP server, and web server.

Task 1: Configure the AD DS domain controller and DNS

Introduction

In order to install and configure DirectAccess, you need to first configure AD DS and DNS to support the installation. To prepare these components, you should perform the following steps:

1. First, create an AD DS group for DirectAccess clients.
2. Secondly, add the DirectAccess clients to the AD DS group.
3. Thirdly, create firewall rules in a Group Policy Object that enables both inbound and outbound ICMPv6 Echo Requests for all domain members.
4. Fourth, configure required DNS records.
5. And finally, configure the DNS Server service to remove the ISATAP name from its default global block list.

Speaker Script	Demonstration steps
The first step to prepare AD DS is to create a security group that will be used to apply DirectAccess client computer settings to the client computers. When you configure DirectAccess, Group Policy objects will be created and assigned to this group of computers. In this case, I will create a new group called DAClients.	On NYC-DC1: 1. In the Active Directory Users and Computers console tree, right-click **Users**, point to **New**, and then click **Group**. 2. In the **New Object - Group** dialog box, under **Group name**, type **DAClients**. 3. Under **Group scope**, choose **Global**, under **Group type**, choose **Security** and then click **OK**.
Next, you need to add the DirectAccess client computers to the AD DS group that you just created.	1. Click **Computers**, right-click **NYC-CL1**, and click **Properties**. 2. On the **MemberOf** tab, click **Add**, type **DAClients**, and click **OK** twice. 3. Close the Active Directory Users and Computers

	console.
The next step is to configure the Group Policy objects to configure the Windows Firewall Rules. In Group Policy, configure Windows Firewall with Advanced Security rules that allow inbound and outbound ICMPv6 Echo Request messages. These messages need to be sent and received to provide connectivity for Teredo-based DirectAccess clients. By configuring this setting on the Default Domain Policy GPO, the settings will be applied to all computers that are members of the domain. By default, Windows Firewall in Windows 7 and Windows 2008 R2 is configured to restrict both inbound and outbound traffic, so you need to define both an inbound and outbound Windows Firewall rule. In this case, I will create a custom rule that applies to all programs but will limit the protocol to ICMPv6 and only the Echo Request messages. I need to create an Outbound rule with the same settings.	1. Click **Start**, click **Administrative Tools**, and then click **Group Policy Management**. 2. In the console tree, open **Forest: Contoso.com\Domains\contoso.com**. 3. In the console tree, right-click **Default Domain Policy** and then click **Edit**. 4. In the console tree of the Group Policy Management Editor, open **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security**. 5. In the console tree, right-click **Inbound Rules** and then click **New Rule.** 6. On the **Rule Type** page, click **Custom** and then click **Next**. 7. On the **Program** page, click **Next**. 8. On the **Protocols and Ports** page, for **Protocol type**, click **ICMPv6** and then click **Customize**. 9. In the **Customize ICMP Settings** dialog box, click **Specific ICMP types**, select **Echo Request**, and then click **OK**. 10. Click **Next**. 11. On the **Scope** page, click **Next**. 12. On the **Action** page, click **Next**. 13. On the **Profile** page, click **Next**. 14. On the **Name** page, for **Name**, type **Inbound ICMPv6 Echo Requests** and then click **Finish**. 15. In the console tree, right-click **Outbound Rules** and then click **New Rule.** 16. On the **Rule Type** page, click **Custom** and then click **Next**. 17. On the **Program** page, click **Next**. 18. On the **Protocols and Ports** page, for **Protocol type**, click **ICMPv6** and then click **Customize**. 19. In the **Customize ICMP Settings** dialog box, click **Specific ICMP types**, select **Echo Request**, and then click **OK**. 20. Click **Next**. 21. On the **Scope** page, click **Next**. 22. On the **Action** page, click **Allow the connection** and then click **Next**. 23. On the **Profile** page, click **Next**. 24. On the **Name** page, for **Name**, type **Outbound ICMPv6 Echo Requests** and then click **Finish**. 25. Close the Group Policy Management Editor and Group Policy Management consoles.

The next step is to create the DNS records that will be required for DirectAccess. The records that you need to create will depend on your network configuration. In this demonstration, I will create a DNS record just for CRL.contoso.com. This DNS record refers to the CRL distribution point that I will be configuring. When configuring DNS, I also need to ensure that DNS records exist for all other servers that DirectAccess clients need to be able to locate. In this demonstration, I am using dynamic DNS, so records for servers such as the NYC-NLS server and internal web servers are already configured in the contoso.com domain.	1. Click **Start**, point to **Administrative Tools**, and then click **DNS**. 2. In the console tree of DNS Manager, open **NYC-DC1**. 3. Expand **Forward Lookup Zones**. 4. In the console tree, right click **contoso.com** and then click **New Host (A or AAAA)**. 5. In **Name**, type **crl**. In **IP address**, type **10.10.0.20**. Click **Add Host**, click **OK**, and then click **Done**. 6. Close the DNS Manager console.
The final step in configuring DNS is to configure the DNS Server service to remove the ISATAP name from its default global block list. By default, DNS servers running Windows Server 2008 R2 or Windows Server 2008 use the global query block list to block the resolution of the name ISATAP. To allow name resolution for the ISATAP name, you must remove ISATAP from the global query block list of the DNS Server service for each DNS server on your intranet running Windows Server 2008 R2 or Windows Server 2008. By default, the global query block list contains two entries, wpad and isatap. By running this command, I am configuring the setting to only include wpad.	1. Click **Start**, click **All Programs**, click **Accessories**, right-click **Command Prompt**, and then click **Run as administrator**. 2. In the **Command Prompt** window, type **dnscmd /config /globalqueryblocklist wpad** and then press ENTER. 3. Close the **Command Prompt** window.

Task 2: Configure the PKI environment

Introduction

After configuring the DNS and AD DS environment, you also need to configure the PKI deployment in your organization. For this demonstration, I have already deployed an Enterprise Root CA on the domain controller, and I will be using certificates from this CA for all servers and DirectAccess clients. You can use a certificate from a public CA for the server certificates, but the advantage of using an internal CA is that you can automate the deployment of client certificates. To prepare the PKI environment, you need to complete the following steps.

1. First, create a custom certificate template so that requesting computers can specify the subject name and subject alternative name of a certificate

2. Secondly, configure Certificate Revocation List (or CRL) publication.
3. Thirdly configure the root CA so that computer certificates are issued automatically through Group Policy
4. And finally, request and install server certificates on required servers

Speaker Script	Demonstration steps
The DirectAccess and network location servers require the use of certificates for Secure Sockets Layer (SSL) authentication that have customized certificate properties. The servers must be able to request certificates that include both the subject name and additional server names in the subject alternative name attribute. To request and modify certificates from an Active Directory Certificate Services (AD CS)-based certification authority (CA), you must create a customized certificate template that includes the Server Authentication object identifier. To create the new certificate template, I will duplicate the Web Server certificate template. In this case, I need to modify the security tab to ensure that authenticated users and domain computers have permission to request these certificates. I also need to ensure that the private key can be exported from the certificates. After configuring the certificate template, I need to configure the CA to issue certificates based on that template.	1. Click **Start**, point to **Administrative Tools**, and then click **Certification Authority**. 2. In the console tree, expand **Contoso-NYC-DC1-CA**, right-click **Certificate Templates**, and click **Manage**. 3. In the contents pane, right-click the **Web Server** template and then click **Duplicate Template**. 4. Click **Windows Server 2008 Enterprise** and then click **OK**. 5. In **Template display name**, type **Web Server 2008**. 6. Click the **Security** tab. 7. Click **Authenticated Users** and then select **Enroll** in the **Allow** column. 8. Click **Add**, type **Domain Computers**, and then click **OK**. 9. Click **Domain Computers** and then select **Enroll** in the **Allow** column. 10. Click the **Request Handling** tab. 11. Select **Allow private key to be exported**. 12. Click **OK**. 13. Close the MMC window without saving changes. 14. In the console tree, expand **Contoso-NYC-DC1-CA**, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template To Issue**. 15. In the list of certificate templates, click **Web Server 2008** and then click **OK**. 16. Close the Certification Authority console.
DirectAccess clients need to be able to verify the certificate revocation status for the DirectAccess server over the Internet and for the network location server over the intranet. The DirectAccess client, when it is on the Internet, must be able to check the certificate revocation of the SSL certificate issued to the DirectAccess server before establishing an IP-HTTPS-based connection.	On NYC-DAS 1. Click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**. 2. In the console tree, open **NYC-DAS** and then **Sites**. 3. Right-click **Default Web Site** and then click **Add virtual directory**. 4. In **Alias**, type **CRLD**. 5. In **Physical path**, click the ellipsis (…). 6. Click the drive on which Windows Server 2008 R2 is located and then click **Make New Folder**.

By default, when you configure an Enterprise CA, it will configure CRL distribution points on the CA which are accessible to internal clients. For this demonstration, I will create an additional CRL distribution point on the DirectAccess server that is accessible to both internal and external clients. This enables Internet clients to check the status for the DirectAccess server certificate.

To enable the CRL distribution points, you need to:

1. Create a Web-based certificate revocation list distribution point using (IIS). In this case, I am configuring a new virtual directory named CRLD on the DirectAccess-based IIS server that points to the CRLDist folder.
2. Configure permissions on the CRL distribution shared folder. The CA must be able to write to the CRL distribution point folder.

   I need to modify the properties of the new virtual folder to enable directory browsing and to configure security. Next, I need to share that location so that the certification authority has permission to write to that folder.

   After configuring the virtual directory in IIS, the next step is to configure permissions on the distribution folder so that the CA has permission to write to that folder. I need to configure both share level and NTFS permissions.

3. The next step is to configure CA to publish the certificate revocation list to the CRL distribution point.

   After I publish the CRL to the shared folder, all clients with certificates from this CA will check this folder for the CRL.

7. Type **CRLDist**, press ENTER, and then click **OK** twice.
8. In the contents pane, double-click **Directory Browsing**.
9. In the **Actions** pane, click **Enable**.
10. In the console tree, click the **CRLD** folder.
11. In the contents pane, double-click **Configuration Editor**.
12. In **Section**, open **system.webServer\security\requestFiltering**.
13. In the contents pane, double-click **allowDoubleEscaping** to change it from **False** to **True**.
14. In the **Actions** pane, click **Apply**.
15. Close the **Internet Information Services (IIS) Manager** window.
16. Click **Start** and then click **Computer**.
17. Double-click the drive on which Windows Server 2008 R2 is located.
18. In the details pane, right-click the **CRLDist** folder and then click **Properties**.
19. Click the **Sharing** tab and then click **Advanced Sharing**.
20. Select **Share this folder**.
21. In **Share name**, add **$** to the end of the CRLDist name to hide the share and then click **Permissions**.
22. Click **Add** and then click **Object Types**.
23. Select **Computers** and then click **OK**.
24. In **Enter the object names to select**, type **NYC-DC1** and then click **OK**.
25. In **Group or user names**, click the **NYC-DC1** computer. In **Permissions for NYC-DC1**, click **Full Control** and then click **OK** twice.
26. Click the **Security** tab and then click **Edit**.
27. Click **Add** and then click **Object Types**.
28. Select **Computers** and then click **OK**.
29. In **Enter the object names to select**, type **NYC-DC1** and then click **OK**.
30. In **Group or user names**, click the **NYC-DC1** computer. In **Permissions for NYC-DC1**, click **Full Control**, click **OK**, and then click **Close**.
31. Close the **Local Disk** window.
32. On NYC-DC1, click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.
33. Click **Start**, point to **Administrative Tools**, and then click **Certification Authority**.
34. In the console tree, right-click **Contoso-NYC-DC1-CA** and then click **Properties**.
35. Click the **Extensions** tab and then click **Add**.
36. In **Location**, type **http://crl.contoso.com/crld/**.
37. In **Variable**, click **<CAName>** and then click **Insert**.

After restarting the certification services service, I will force an immediate creation of the CRL. I can verify that the CRL has been created and published to the right location by checking the shared folder on NYC-DAS. You'll notice that two CRL files have been published to this location.	38. In **Variable**, click **<CRLNameSuffix>** and then click **Insert**. 39. In **Variable**, click **<DeltaCRLAllowed>** and then click **Insert**. 32. In **Location**, type **.crl** at the end of the Location string and then click **OK**. 33. Select **Include in CRLs. Clients use this to find Delta CRL locations.** and **Include in the CDP extension of issued certificates** and then click **OK**. 34. Click **Add**. 35. In **Location**, type **\\NYC-DAS\crldist$**. 36. In **Variable**, click **<CAName>** and then click **Insert**. 37. In **Variable**, click **<CRLNameSuffix>** and then click **Insert**. 38. In **Variable**, click **<DeltaCRLAllowed>** and then click **Insert**. 39. In **Location**, type **.crl** at the end of the string and then click **OK**. 40. Select **Publish CRLs to this location** and **Publish Delta CRLs to this location** and then click **OK**. 41. Click **Yes** to restart Active Directory Certificate Services. 42. In the console tree, double-click **contoso-NYC-DC1-CA**, right-click **Revoked Certificates**, point to **All Tasks**, and then click **Publish**. 43. If prompted, click **New CRL** and then click **OK**. 44. Click **Start**, type **\\NYC-DAS\crldist$**, and then press ENTER. 45. In the **crldist$** window, you should see two CRL files named **Contoso-NYC-DC1-CA** and **Contoso-NYC-DC1-CA+**. 46. Close the **crldist$** window and the Certification Authority console.
The default connection security rules use a computer certificate for IPSec peer authentication between the DirectAccess clients and any servers accessible by the clients. This requires a certificate on DirectAccess clients, DirectAccess servers, and selected servers with either the Client Authentication or IPSec IKE Intermediate object identifier. The easiest way to deploy certificates containing the Client Authentication OID to both DirectAccess clients and servers is to configure certificate autoenrollment for the built-in Computer Certificate template.	1. Click **Start**, click **Administrative Tools**, and then click **Group Policy Management**. 2. In the console tree, open **Forest: contoso.com\Domains\contoso.com**. 3. In the console tree, right-click **Default Domain Policy** and then click **Edit**. 4. In the console tree of the Group Policy Management Editor, open **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**. 5. In the details pane, right-click **Automatic Certificate Request Settings**, point to **New**, and then click **Automatic Certificate Request**. 6. In the Automatic Certificate Request Wizard, click

After you configure autoenrollment of this certificate, all computers that are members of the domain will be automatically issued a certificate the next time Group Policy is refreshed on the computer.	**Next**. 7. On the **Certificate Template** page, click **Computer**, click **Next**, and then click **Finish**. 8. Close the Group Policy Management Editor and Group Policy Management consoles.
The final step in configuring the PKI environment is to request and install server certificates on any servers that require the certificates. In this demonstration, the DirectAccess server requires an additional certificate using the custom template that I created earlier in the demonstration. In this case, I will configure two separate names for the certificate – using the common name and the DNS name. I will also change the friendly name, or the display name, for this certificate.	1. On NYC-DAS, click **Start**, click **Run**, type **mmc,** and then press ENTER. 2. Click **File** and then click **Add/Remove Snap-in**. 3. Click **Certificates**, click **Add**, click **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**. 4. In the console tree of the Certificates snap-in, open **Certificates (Local Computer)\Personal\Certificates**. 5. Right-click **Certificates**, point to **All Tasks**, and then click **Request New Certificate**. 6. Click **Next** twice. 7. On the Request Certificates page, click **Web Server 2008** and then click **More information is required to enroll for this certificate**. 8. On the **Subject** tab of the **Certificate Properties** dialog box, in **Subject name**, for **Type**, select **Common Name**. 9. In **Value**, type **NYC-DAS.contoso.com** and then click **Add**. 10. In **Alternative name**, for **Type**, select **DNS**. 11. In **Value**, type **NYC-DAS.contoso.com** and then click **Add**. 12. Click **OK**, click **Enroll**, and then click **Finish**. 13. In the details pane of the Certificates snap-in, verify that a new certificate with the name NYC-DAS.contoso.com was enrolled with **Intended Purposes** of **Server Authentication**. 14. Right-click the certificate and then click **Properties**. 15. In **Friendly Name**, type **IP-HTTPS Certificate** and then click **OK**. 16. Close the console window. If you are prompted to save settings, click **No**.

Task 3: Configure the DirectAccess clients and test Intranet and Internet Access

Introduction Now that the environment is configured, you should be able to verify that certificates have been issued to the DirectAccess clients and that network connectivity is working as you expect it. At this point, the

DirectAccess client should have a certificate issued by the CA using the Computer certificate template, and should also be able to access intranet resources. If we move the client to the Internet, the client should not be able to access Intranet resources. To complete this part of the process, you should: 1. Verify the certificate installation 2. Test Intranet access 3. Test Internet access to internal resources	
Speaker Script	**Demonstration steps**
In order for the DirectAccess client to be able to access internal resources from the Internet, it must be issued a certificate from the internal CA. You should verify that this certificate has been issued to the client while it is connected to the internal network. You'll notice that the client has been issued a certificate from the corporate CA for the purpose of client and server authentication.	1. On NYC-CL1, click **Start**, type **mmc,** and then press ENTER. 2. Click **File** and then click **Add/Remove Snap-in**. 3. Click **Certificates**, click **Add**, select **Computer account**, click **Next**, select **Local computer**, click **Finish**, and then click **OK**. 4. In the console tree, open **Certificates (Local Computer)\Personal\Certificates**. 5. In the details pane, verify that a certificate was enrolled with **Intended Purposes** of **Client Authentication** and **Server Authentication**. This certificate will be used for authentication with NYC-DAS. 6. Close the console window. When you are prompted to save settings, click **No**.
In order for the NYC-NLS server to respond to SSL requests to the default website, I need to modify the bindings for the default website to enable https, and to use the appropriate certificate.	1. On NYC-NLS, click **Start**, point to **Administrative Tools**, and then click **Internet Information Services (IIS) Manager**. 2. In the console tree, open **NYC-NLS** and then **Sites**. 3. Click **Default Web Site**. 4. Under **Actions**, click **Bindings**. 5. Click **Add**, and under **Type**, click **https**. 6. Under **SSL certificate**, click **NYC-NLS.contoso.com** and click **OK**. 7. Click **Close**, and then close the **Internet Information Services (IIS) Manager**.
To verify that network connectivity is working as expected, I will attempt to connect to the internal web server, to the NYC-NLS server, and to an internal network share.	1. On NYC-CL1, on the taskbar, click the Internet Explorer® icon. 2. In the Address bar, type **http://NYC-SVR1.contoso.com/** and then press ENTER. You should see the default IIS 7 webpage for NYC-SVR1. 3. In the Address bar, type **https://NYC-NLS.contoso.com** and then press ENTER. You should see the default IIS 7 webpage. 4. Click **Start**, type **\\NYC-SVR1\Files**, and then press ENTER. 5. You should see a folder window with the contents of the Files shared folder. 6. In the **Files** shared folder window, double-click the **File.txt** file. You should see the contents of the File.txt file.

	7. Close the **File.txt - Notepad** and the **Files** shared folder windows.
I don't have DirectAccess enabled yet in the demonstration environment, so I would expect that the client should not be able to access any resources on the internal network from the Internet. To verify this, I will connect the client to the Internet virtual network or VLAN and test connectivity to the internal network. The client is unable to connect to the internal network. I will reset the network configuration to connect the client to the internal network and refresh the IP address again.	1. In Hyper-V Manager, access the network settings for NYC-CL1. Connect the client to the Internet virtual network. 2. Open a command prompt and type **ipconfig /release** and press ENTER. 3. At the command prompt, type **ipconfig /renew** and press ENTER. 4. In the taskbar, click the Internet Explorer icon. 5. In the **Address** bar, type **http://NYC-SVR1.contoso.com/** and then press ENTER. You should see the **Internet Explorer cannot display the webpage** message. 6. Close the Internet Explorer window. 7. In Hyper-V Manager, access the network settings for NYC-CL1. Connect the client to the Internal virtual network. 8. At the command prompt, type **ipconfig /release** and press ENTER. 9. At the command prompt, type **ipconfig /renew** and press ENTER.

Task 4: Configure the DirectAccess server

Introduction

Now that all of the prerequisites for DirectAccess have been configured, I can move on to installing the DirectAccess Management Console and configuring DirectAccess. To implement DirectAccess, you need to:

1. First install the DirectAccess Management Console feature
2. Secondly, run the DirectAccess Setup wizard
3. And thirdly, update the IPv6 configuration and refresh Group Policy for the DirectAccess clients.

In this demonstration, I will be using the DirectAccess Setup wizard to configure DirectAccess. You can also configure the DirectAccess settings manually, but using the wizard is much easier. To show you what was configured by using the Wizard, I will review some of the changes that were made by the DirectAccess Setup wizard.

Speaker Script	Demonstration steps
The first step in configuring the DirectAccess server is to install the DirectAccess Management Console. The installation of this server feature is straightforward with no configuration options available during the installation. Notice that the Group Policy	1. On NYC-DAS, click **Start**, point to **Administrative Tools**, and then click **Server Manager**. 2. In the main window, under **Features Summary**, click **Add features**. 3. On the **Select Features** page, select **DirectAccess Management Console**. 4. In the **Add Features Wizard** window, click **Add Required**

Management console is also installed to enable the modification of Group Policy Objects.	**Features**. 5. On the **Select Features** page, click **Next**. 6. On the **Confirm Installation Selections** page, click **Install**. 7. On the **Installation Results** page, click **Close**.
After installing the DirectAccess Management Console, you can run the DirectAccess Setup wizard. This wizard enables you to select how the DirectAccess environment will be configured, and then the wizard will apply the changes to your environment. The DirectAccess Setup wizard includes the following steps: 1. Step 1: Configure remote clients. In this step, you configure the AD DS groups that contain the computer accounts for Direct Access clients. 2. Step 2: Configure the DirectAccess server. In this step, you will configure the network adapters on the DirectAccess server and configure the certificates for the server. Notice that the DirectAccess wizard automatically detects the network adapter connected to the Internet as well as the network adapter connected to the corpnet. In this case I need to select a certificate that is at the top of the trust path for all certificates that will be trusted for remote clients. I also need to select the certificate that will be used for https connections to the DirectAccess server. 3. Step 3: Configure the infrastructure servers. During this step, you are configuring which servers are accessible or not accessible to DirectAccess clients when the client has established the initial infrastructure tunnel to the	1. Click **Start**, point to **Administrative Tools**, and then click **DirectAccess Management**. 2. In the console tree, click **Setup**. In the details pane, click **Configure** for step 1. 3. On the **DirectAccess Client Setup** page, click **Add**. 4. In the **Select Group** dialog box, type **DAClients**, click **OK**, and then click **Finish**. 5. Click **Configure** for step 2. 6. On the **Connectivity** page, for **Interface connected to the Internet**, select **Internet**. For **Interface connected to the internal network**, select **Corpnet**. Click **Next.** 7. On the **Certificate Components** page, for **Select the root certificate to which remote client certificates must chain**, click **Browse**. In the list of certificates, click the Contoso-NYC-DC1-CA root certificate, and then click **OK**. 8. For **Select the certificate that will be used to secure remote client connectivity over HTTPS**, click **Browse**. In the list of certificates, click the certificate named **IP-HTTPS Certificate** and then click **OK**. Click **Finish**. 9. Click **Configure** for step 3. 10. On the **Location** page, click **Network Location server is run on a highly available server**, type **https://NYC-NLS.contoso.com**, click **Validate**, and then click **Next**. 11. On the **DNS and Domain Controller** page, note the entry for the name **contoso.com** with the IPv6 address **2002:836b:101:1:0:5efe:10.10.0.10**. This IPv6 address is assigned to NYC-DC1 and is composed of a 6to4 network prefix (2002:836b:101:1::/64) and an ISATAP-based interface identifier (::0:5efe:10.0.0.1). Click **Next**. 12. On the **Management** page, click **Finish**. 13. Click **Configure** for step 4. On the **DirectAccess Application Server Setup** page, click **Finish**. 14. Click **Save** and then click **Finish**. 15. In the **DirectAccess Review** dialog box, click **Apply**. In the **DirectAccess Policy Configuration** message box, click **OK**.

DirectAccess server. In this step, you will configure the URL for the Network Location server. This information is required to ensure that an exemption for the Network Location server is configured in the NRPT so that DirectAccess clients will not be able to access the network location server over the DirectAccess connection. During this step, you can also manually configure additional DNS suffixes for any internal domains and add the IP addresses for the internal DNS servers. You can also configure how the client will resolve DNS names that are not listed in DNS. Finally, during this step, you can configure the IPv6 addresses for internal servers that will be used to manage the DirectAccess clients. Notice the IPv6 address is assigned to the Contoso.com domain. This IPv6 address is assigned to NYC-DC1 and is composed of a 6to4 network prefix and the ISATAP-based interface identifier. In this case, we are not adding any additional management servers to the wizard. 4. Step 4: In this step, you are configuring the application servers. During this step, you will configure how the client will access the internal network servers. The default configuration is to not require any additional authentication – with this option, the DirectAccess server will terminate the IPSec tunnels and the client will be able to connect to all IPv6 resources on the intranet. You can modify the	

setting to restrict which servers the clients can access by configuring additional authentication for intranet servers. In this case, we will accept the default configuration. After completing the wizard, we can save the configuration and then finish the wizard. The wizard then presents a summary of the changes you have made. When you click Apply, the changes will be configured to the DirectAccess server and to Group Policy.	
After running the Setup wizard, the DirectAccess environment will be configured. However, to force the immediate application of the network and Group Policy changes, I will refresh the IP configuration and force the Group Policy application for the computers used in the demonstration. One of the changes made by the DirectAccess Setup wizard is to configure the DirectAccess server as an ISATAP router for routing IPv6 traffic across an IPv4 network. By restarting the IP Helper service on the domain controller and application servers, I can verify that they are configured as ISATAP hosts. For the DirectAccess client, I need to restart the IP Helper service as well as force the application of Group Policy settings for DirectAccess clients. Notice that the server has been issued an ISATAP address for routing IPv6 traffic over an IPv4 network.	1. On NYC-SVR1, click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**. 2. In the **Command Prompt** window, type **net stop iphlpsvc**, press ENTER, type **net start iphlpsvc**, and then press ENTER. 3. Close the **Command Prompt** window. 4. On NYC-DC1, click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**. 5. In the **Command Prompt** window, type **net stop iphlpsvc**, press ENTER, type **net start iphlpsvc**, and then press ENTER. 6. Close the **Command Prompt** window. 7. On NYC-CL1, click **Start**, click **All Programs**, click **Accessories**, and then click **Command Prompt**. 8. In the **Command Prompt** window, type **gpupdate** and then press ENTER. 9. In the **Command Prompt** window, type **net stop iphlpsvc**, press ENTER, type **net start iphlpsvc**, and then press ENTER.
Just to make sure that the ISATAP configuration has been applied correctly, I will check if NYC-CL1 client can access the Intranet servers by using the ISATAP-based IPv6 addresses. We will try to ping the IPv6 address for NYC-SVR1. We will also try to ping the server by	1. On NYC-CL1, in the **Command Prompt** window, type **ipconfig /flushdns**, and then press ENTER. 2. In the **Command Prompt** window, type **ping 2002:836b:101:1::5efe:10.10.0.30** and then press ENTER. This is the ISATAP-based address of NYC-SVR1. You should see four successful replies. 3. In the **Command Prompt** window, type **ping NYC-DC1.contoso.com** and then press ENTER. You should see

computer name.	the name NYC-DC1.contoso.com resolved to the IPv6 address 2002:836b:101:1::5efe:10.10.0.10 and four successful replies. 4. In the **Command Prompt** window, type **ping NYC-SVR1.contoso.com** and then press ENTER. You should see the name NYC-SVR1.contoso.com resolved to the IPv6 address 2002:836b:101:1::5efe:10.0.0.30 and four successful replies.
You have seen one of the results of running the DirectAccess Setup wizard. The DirectAccess server is configured as an ISATAP router, and the internal computers are configured as ISATAP hosts. The DirectAccess Setup wizard also created two GPOs in Active Directory. The first of the GPOs is applied to the DirectAccess clients. This GPO configures Windows Firewall with Advanced Security settings, and also configures the Name Resolution Policy table. The other GPO is applied to the DirectAccess server. This policy also configures Windows Firewall with Advanced Security for the Direct Access server.	1. On NYC-DAS, open the Group Policy Management console from the Administrative Tools. 2. Expand **Forest: Contoso.com**, expand **Domains**, expand **Contoso.com**. 3. Click the first DirectAccess Policy listed. Highlight the **Security Filtering** section to show that the policy is applied to the **DAClients** group. 4. Click the **Settings** tab. 5. Beside **Security Settings**, click **Show**. 6. Beside **Windows Firewall with Advanced Security**, click **Show**. 7. Beside **Outbound Rules**, click **Show**. 8. Beside **Name Resolution Policy**, click **Show**. 9. Beside **Rule Settings**, click **Show**. 10. Click the second DirectAccess Policy listed in the left pane and then click the **Scope** tab. Highlight the **Security Filtering** section to show that the policy is applied to the DirectAccess server. 11. Click the **Settings** tab. 12. Beside **Security Settings**, click **Show**. 13. Beside **Windows Firewall with Advanced Security**, click **Show**. 14. Beside **Inbound Rules**, click **Show**. 15. Close the Group Policy Management console.

Task 5: Verify DirectAccess Functionality

Introduction

After you have configured the DirectAccess environment, the final step is to verify that DirectAccess works as expected. To do this, complete the following steps.

1. First, connect the client computer to the Internet subnet
2. Secondly, verify connectivity to the Internet Web resources
3. And thirdly, verify connectivity to the Intranet resources

Speaker Script	Demonstration steps
To test the DirectAccess configuration for external clients, I will modify the	1. In Hyper-V, access the NYC-CL1 network settings and connect the client to the Internet network.

settings for the client computer to connect it to the Internet network. To simulate the client starting up on the internet, I will restart the computer.	2. Restart the client computer. 3. After the computer restarts, log on as Administrator.
The client computer should be configured with an Internet IP address. I can also verify that the client can connect to an Internet website.	1. To verify that the client has an Internet IPv4 address, open a Command Prompt, type **ipconfig**, and then press ENTER. 2. Verify that the interface named Local Area Connection has an IPv4 address that begins with **131.107**. 3. On the taskbar, click the Internet Explorer icon. 4. In the Address bar, type **http://Web.isp.fabrikam.com/** and then press ENTER. You should see the default IIS 7 webpage for WEB.
The client computer can also connect to network resources on the intranet. I can ping servers on the internal network and connect to both internal websites and internal file shares.	1. In the **Command Prompt** window, type **ping NYC-SVR1** and then press ENTER. 2. You should see the name **NYC-SVR1.contoso.com** resolved to the IPv6 address **2002:836b:2:1:0:5efe:10.0.0.30** and four successful replies. 3. In Internet Explorer, in the Address bar, type **http://NYC-SVR1.contoso.com**, press ENTER, and then press **F5**. You should see the default IIS 7 webpage for NYC-SVR1. 4. Close Internet Explorer. 5. Click **Start**, type **\\NYC-SVR1\files**, and then press ENTER. You should see a folder window with the contents of the **Files** shared folder. 6. In the **Files** shared folder window, double-click the **File.txt** file. 7. Close the **example.txt - Notepad** window and the **Files** shared folder window.