**Test Lab Guide: Demonstrate DirectAccess Single Server Setup with Mixed IPv4 and IPv6 in Windows Server 2012**

Microsoft Corporation

Published: August, 2012

**Abstract**

This paper contains an introduction to Unified Remote Access and step-by-step instructions for extending the Windows Server 2012 Base Configuration test lab to demonstrate DirectAccess deployment in a single server deployment with a mixed environment of IPv4 and IPv6.

**Copyright information**

This document is provided “as-is”. Information and views expressed in this document, including URL and other Internet Web site references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious.  No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2012 Microsoft. All rights reserved.

Active Directory, Hyper-V, Microsoft, MS-DOS, Visual Basic, Visual Studio, Windows, Windows NT, Windows Server, and Windows Vista are trademarks of the Microsoft group of companies.

All other trademarks are property of their respective owners.

Contents

[Introduction 5](#_Toc317799927)

[In this guide 5](#_Toc317799928)

[Test lab overview 6](#_Toc317799929)

[Hardware and software requirements 7](#_Toc317799930)

[Known Issues 8](#_Toc317799931)

[Steps for Configuring the Remote Access Test Lab 8](#_Toc317799932)

[Step 1: Set up the Base Configuration Test Lab 10](#_Toc317799933)

[Step 2: Configure DC1 10](#_Toc317799934)

[Configure an IPv6 address on DC1 10](#_Toc317799935)

[Create a security group for DirectAccess client computers 11](#_Toc317799936)

[Create a network location server DNS record 12](#_Toc317799937)

[Create ICMPv4 and ICMPv6 echo request firewall rules in domain group policy 13](#_Toc317799938)

[Step 3: Configure APP1 15](#_Toc317799939)

[Configure an IPv6 address on APP1 15](#_Toc317799940)

[Configure permissions of the Web Server certificate template 16](#_Toc317799941)

[Obtain an additional certificate on APP1 17](#_Toc317799942)

[Configure the HTTPS security binding 18](#_Toc317799943)

[Step 4: Install and Configure APP2 18](#_Toc317799944)

[Install the operating system on APP2 19](#_Toc317799945)

[Install IIS web services on APP2 19](#_Toc317799946)

[Create a shared folder on APP2 20](#_Toc317799947)

[Step 5: Configure EDGE1 21](#_Toc317799948)

[Configure an IPv6 address on EDGE1 21](#_Toc317799949)

[Provision EDGE1 with a certificate for IP-HTTPS 22](#_Toc317799950)

[Install the Remote Access server role on EDGE1 23](#_Toc317799951)

[Configure DirectAccess on EDGE1 24](#_Toc317799952)

[Confirm Group Policy settings 25](#_Toc317799953)

[Confirm IPv6 settings 26](#_Toc317799954)

[Step 6: Configure CLIENT1 27](#_Toc317799955)

[Connect CLIENT1 to the Corpnet subnet and update group policy 27](#_Toc317799956)

[Connect CLIENT1 to the Internet subnet and test remote access 28](#_Toc317799957)

[Connect CLIENT1 to the Homenet subnet and test remote access 29](#_Toc317799958)

[Monitor the client connection on the EDGE1 DirectAccess server 30](#_Toc317799959)

[Snapshot the Configuration 31](#_Toc317799960)

[Additional Resources 31](#_Toc317799961)

# Introduction

DirectAccess provides users with the experience of being seamlessly connected to their intranet any time they have Internet access. When DirectAccess is enabled, requests for intranet resources (such as email servers, shared folders, or intranet websites) are securely directed to the intranet, without the need for users to connect to a VPN. DirectAccess enables increased productivity for a mobile workforce by offering the same connectivity experience both inside and outside of the office.

The Windows Routing and Remote Access Server (RRAS) provides traditional VPN connectivity for legacy clients and non-domain members. RRAS also provides site-to-site connections between servers. RRAS in Windows Server 2008 R2 cannot coexist on the same edge server with DirectAccess, and must be deployed and managed separately from DirectAccess.

Windows Server 2012 combines the DirectAccess feature and the RRAS role service into a new unified server role. This new Remote Access server role allows for centralized administration, configuration, and monitoring of both DirectAccess and VPN-based remote access services. Additionally, Windows Server 2012 DirectAccess provides multiple updates and improvements to address deployment blockers and provide simplified management.

Windows DirectAccess is an IPv6-only technology from a client perspective. This means that clients can only access intranet resources accessible via IPv6 while connected remotely, and only if the client application itself supports connecting to an IPv6 resource. Intranet applications or resources are accessible directly via IPv6 if they are listening on the internal server's IPv6 interface. For remote management of DirectAccess clients initiated by intranet computers, internal application or management servers must also be fully IPv6 compliant and the server applications they run must be IPv6 compatible.

To allow access to internal IPv4-only resources, Windows Server 2012 DirectAccess includes native support for a protocol translation (NAT64) and name resolution (DNS64) gateway to convert the IPv6 communication from a DirectAccess client to IPv4 for the internal servers. IPv4-only intranet computers cannot initiate connections to DirectAccess clients for remote management because the translation done with NAT64 is unidirectional (for traffic initiated by the DirectAccess client).

## In this guide

This guide provides step-by-step instructions for configuring DirectAccess in a single server deployment with mixed IPv4 and IPv6 resources in a test lab to demonstrate functionality of the deployment experience. You will set up and deploy DirectAccess based on the Windows Server 2012 Base Configuration using five server computers and two client computers. The resulting test lab simulates an intranet, the Internet, and a home network, and demonstrates DirectAccess in different Internet connection scenarios.

Important

The following instructions are for configuring a Remote Access test lab using the minimum number of computers. Individual computers are needed to separate the services provided on the network and to clearly show the desired functionality. This configuration is neither designed to reflect best practices nor does it reflect a desired or recommended configuration for a production network. The configuration, including IP addresses and all other configuration parameters, is designed only to work on a separate test lab network.

Attempting to adapt this Remote Access test lab configuration to a pilot or production deployment can result in configuration or functionality issues.

## Test lab overview

In this test lab, Remote Access is deployed with:

* One computer running Windows Server 2012 named DC1 that is configured as an intranet domain controller, Domain Name System (DNS) server, and Dynamic Host Configuration Protocol (DHCP) server
* One intranet member server running Windows Server 2012 named EDGE1 that is configured as a DirectAccess server
* One intranet member server running Windows Server 2012 named APP1 that is configured as a general application server and web server. APP1 is configured as an enterprise root Certificate Authority (CA), and as the Network Location Server (NLS) for DirectAccess
* One intranet member server running Windows Server 2003 SP2 named APP2 that is configured as a general application server and web server. APP2 is an IPv4-only intranet resource used to demonstrate NAT64 and DNS64 capabilities
* One standalone server running Windows Server 2012 named INET1 that is configured as an Internet DHCP server, DNS server, and web server
* One roaming member client computer running Windows 8 named CLIENT1 that is configured as a DirectAccess client
* One standalone client computer running Windows 8 named NAT1 that is configured as a network address translation (NAT) device using Internet Connection Sharing

The Remote Access test lab consists of three subnets that simulate the following:

* The Internet (131.107.0.0/24).
* An intranet named Corpnet (10.0.0.0/24), (2001:db8:1::/64), separated from the Internet by EDGE1.
* A home network named Homenet (192.168.137.0/24) connected to the Internet subnet by a NAT

Computers on each subnet connect using a hub or switch. See the following figure.

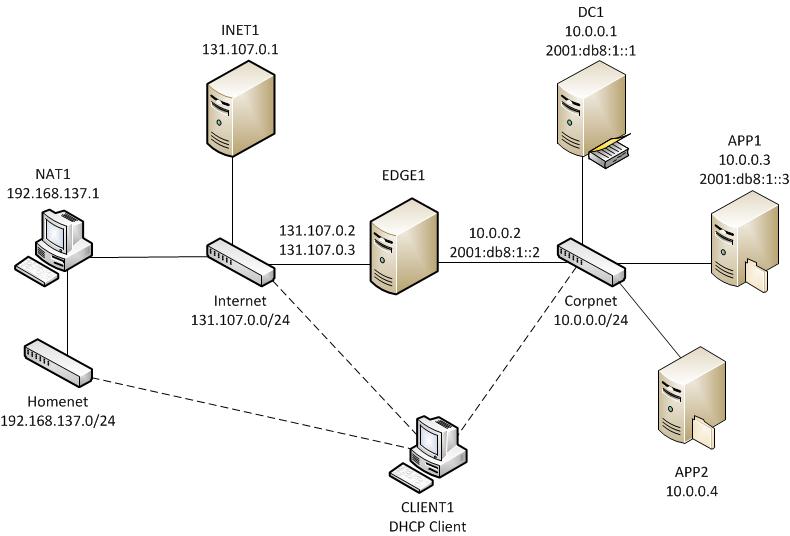


Figure 1 Single server DirectAccess in a mixed IPv4 and IPv6 environment

This test lab demonstrates a single server DirectAccess deployment where intranet resources are a mix of IPv4 and IPv6.

## Hardware and software requirements

The following are required components of the test lab:

* The product disc or files for Windows Server 2012
* The product disc or files for Windows 8
* The product disc or files for Windows Server 2003 SP2
* Six computers or virtual machines that meet the minimum hardware requirements for Windows Server 2012
* One computer or virtual machine that meets the hardware requirements for Windows Server 2003

## Known Issues

The following are known issues when configuring a Single Server DirectAccess lab with Windows Server 2012:

1. Migration of a DirectAccess configuration from one Windows Server 2012 server to another is not supported in this release, and causes the Remote Access Management console to stop responding and close unexpectedly. To work around this issue, do the following:

* Launch Registry Editor (regedit.exe)
* In Registry Editor, locate and then click the following registry subkey: HKLM\System\CurrentControlSet\Services\Ramgmtsvc\Config\Parameters
* Delete the **DaConfigured** DWORD value
* From a command prompt, run **gpupdate /force** on the new DirectAccess server

1. Management from a non-domain-joined computer via RSAT is not possible unless the destination server account is added to the non-domain-joined computer's list of WinRM TrustedHosts

* To add the target DirectAccess server to the non-domain-joined computer's list of WinRM TrustedHosts, run the following command:

**set-item wsman:\localhost\client\trustedhosts "<computerName>" -force**

1. In this release, the Remote Access wizard will always link DirectAccess Group Policy Objects (GPOs) to the domain root, even if the GPOs were previously linked to another container in Active Directory. If you wish to link the GPOs to an OU for deployment, remove the domain root link and relink the GPO to the desired OU after the wizard completes. Alternately, you can remove linking permissions to the domain root for the DirectAccess administrator prior to configuring DirectAccess.

# Steps for Configuring the Remote Access Test Lab

There are six steps to follow when setting up a Remote Access express setup test lab based on the Windows Server 2012 Base Configuration test lab.

1. Set up the Base Configuration test lab.

The DirectAccess Single Server test lab requires the [Test Lab Guide: Windows Server 2012 Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358) with [Optional mini-module: Homenet subnet](http://go.microsoft.com/fwlink/p/?LinkId=244230) and [Optional mini-module: Basic PKI](http://go.microsoft.com/fwlink/p/?LinkId=244229) as its starting point.

1. Configure DC1.

DC1 is already configured as a domain controller with Active Directory, and is the DNS and DHCP server for the intranet subnet. For the single server DirectAccess test lab, DC1 must be configured with a static IPv6 address. A security group will be added to Active Directory for DirectAccess client computers.

1. Configure APP1.

APP1 is already a member server computer that is configured with IIS and also acts as a file server and enterprise root Certificate Authority (CA). For the Remote Access express setup test lab, APP1 must be configured with a static IPv6 address.

1. Configure APP2.

APP2 must be installed and configured as a Windows Server 2003 web and file server to demonstrate an IPv4-only intranet resource.

1. Configure EDGE1.

EDGE1 is already a member server computer. For the single server DirectAccess test lab, EDGE1 must be configured as a Remote Access server with a static IPv6 address.

1. Configure CLIENT1.

CLIENT1 is already a domain member client computer running Windows 8. For the Remote Access express setup test lab, CLIENT1 will be used to test and demonstrate remote access operation.

Note

You must be logged on as a member of the Domain Admins group or a member of the Administrators group on each computer to complete the tasks described in this guide. If you cannot complete a task while you are logged on with an account that is a member of the Administrators group, try performing the task while you are logged on with an account that is a member of the Domain Admins group.

This guide provides steps for configuring the computers of the Windows Server 2012 Base Configuration test lab, configuring Remote Access in Windows Server 2012, and demonstrating remote client connectivity. The following sections provide details about how to perform these tasks.

## Step 1: Set up the Base Configuration Test Lab

Set up the Base Configuration test lab for both the Corpnet and Internet subnets using the procedures in the “Steps for Configuring the Corpnet Subnet” and “Steps for Configuring the Internet Subnet” sections of the [Test Lab Guide: Windows Server 2012 Base Configuration](http://go.microsoft.com/fwlink/p/?LinkId=236358).

Set up the Homenet subnet using the procedures in the [Optional mini-module: Homenet subnet](http://go.microsoft.com/fwlink/p/?LinkId=244230).

Deploy a basic certificate infrastructure using the procedure in the [Optional mini-module: Basic PKI](http://go.microsoft.com/fwlink/p/?LinkId=244229).

## Step 2: Configure DC1

DC1 configuration for the DirectAccess single server deployment test lab consists of the following procedures:

* Configure an IPv6 address on DC1
* Create a security group for DirectAccess client computers
* Create a network location server DNS record
* Create ICMPv4 and ICMPv6 echo request firewall rules in domain group policy

The following sections explain these procedures in detail.

### Configure an IPv6 address on DC1

The Windows Server 2012 Base Configuration test lab does not include IPv6 address configuration. In this step, add IPv6 address configuration to support a DirectAccess deployment.

To configure an IPv6 address on DC1

|  |
| --- |
| 1. In Server Manager, click **Local Server** in the console tree. Scroll to the top of the details pane, and click the link next to **Wired Ethernet Connection**. 2. In **Network Connections**, right-click **Wired Ethernet Connection**, and then click **Properties**. 3. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**. 4. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:1::1**. In **Subnet prefix length**, type **64**. In **Default gateway**, type **2001:db8:1::2**. Click **Use the following DNS server addresses**, and in **Preferred DNS server**, type **2001:db8:1::1**. Click **OK**. 5. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties. 6. In **Default gateway**, type **10.0.0.2**, and then click **OK**. 7. Close the **Wired Ethernet Connection Properties** dialog box. 8. Close the **Network Connections** window. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Note that the "Wired Ethernet Connection" interface name may be different on your computer. Use **ipconfig /all** to list out the interfaces.    **New-NetIPAddress -InterfaceAlias "Wired Ethernet Connection" -IPv6Address 2001:db8:1::1 -PrefixLength 64**  **Set-DnsClientServerAddress -InterfaceAlias "Wired Ethernet Connection" -ServerAddresses 2001:db8:1::1**  **New-NetRoute -DestinationPrefix 2001:db8:1::/64 -InterfaceAlias "Wired Ethernet Connection" -NextHop 2001:db8:1::2 -AddressFamily IPv6**  **New-NetRoute -DestinationPrefix 10.0.0.0/24 -InterfaceAlias "Wired Ethernet Connection" -NextHop 10.0.0.2 -AddressFamily IPv4** |

### Create a security group for DirectAccess client computers

When DirectAccess is configured, it automatically creates group policy objects containing DirectAccess settings, and these are applied to DirectAccess clients and servers. By default, the Getting Started Wizard applies the client GPO to mobile computers only, in the Domain Computers security group. The procedures in this lab do not use the default setting, but instead create an alternate security group for DirectAccess clients.

To create a DirectAccess client security group

|  |
| --- |
| 1. On **DC1**, from the **Start** screen, click **Active Directory Administrative Center**. 2. In the console tree, click the arrow to expand **corp (local)**, and then click **Users**. 3. In the **Tasks** pane, click **New**, and then click **Group**. 4. In the Create Group dialog, type **DirectAccessClients** for Group name. 5. Scroll down to access the **Members** section of the Create Group dialog, and click **Add**. 6. Click **Object Types**, select **Computers**, and click **OK**. 7. Type **CLIENT1**, and then click **OK**. 8. Click **OK** to close the Create Group dialog. 9. Exit the Active Directory Administrative Center. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.    **New-ADGroup -GroupScope global -Name DirectAccessClients**  **Add-ADGroupMember -Identity DirectAccessClients -Members CLIENT1$** |

### Create a network location server DNS record

A DNS record is required to resolve the name of the network location server, which will be located on the APP1 server.

To create the network location server DNS record

|  |
| --- |
| 1. Click **Start**, and then click **DNS**. 2. Expand DC1, Forward Lookup Zones, and select **corp.contoso.com**. 3. Right-click corp.contoso.com, and then click **New Host (A or AAAA)** 4. Under Name, type **NLS**, and under IP address, type **10.0.0.3**. 5. Click **Add Host**, click **OK**, and then click **Done**. 6. Close the DNS Manager console. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.  **Add-DnsServerResourceRecordA -Name NLS -ZoneName corp.contoso.com -IPv4Address 10.0.0.3** |

### Create ICMPv4 and ICMPv6 echo request firewall rules in domain group policy

ICMPv4 and ICMPv6 echo requests inbound and outbound are required for Teredo support. DirectAccess clients use Teredo as their IPv6 transition technology to connect to the DirectAccess server over the IPv4 Internet when they are assigned a private (RFC 1918) IP address and are located behind a NAT device or firewall that allows outbound UDP port 3544. In addition, enabling ping facilitates connectivity testing between participants in the DirectAccess solution.

To create ICMPv4 and ICMPv6 firewall rules

|  |
| --- |
| 1. From the Start screen, click **Group Policy Management**. 2. In the console tree, expand **Forest: corp.contoso.com\Domains\corp.contoso.com**. 3. Select **Group Policy Objects**. 4. In the details pane, right-click **Default Domain Policy**, and then click **Edit**. 5. In the console tree of the Group Policy Management Editor, expand **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security-LDAP://CN=...** 6. In the console tree, select **Inbound Rules**, right-click **Inbound Rules**, and then click **New Rule**. 7. In the New Inbound Rule Wizard, on the Rule Type page, click **Custom**, and then click **Next**. 8. On the Program page, click **Next**. 9. On the Protocols and Ports page, in **Protocol type**, click **ICMPv4**, and then click **Customize**. 10. On the Customize ICMP Settings dialog box, click **Specific ICMP types**, select **Echo Request**, click **OK**, and then click **Next**. 11. Click **Next** three times. 12. On the Name page, in Name, type **Inbound ICMPv4 Echo Requests**, and then click **Finish**. 13. In the console tree, right-click **Inbound Rules**, and then click **New Rule**. 14. On the Rule Type page, click **Custom**, and then click **Next**. 15. On the Program page, click **Next**. 16. On the Protocols and Ports page, in Protocol type, click **ICMPv6**, and then click **Customize**. 17. On the Customize ICMP Settings dialog box, click **Specific ICMP types**, select **Echo Request**, click **OK**, and then click **Next**. 18. Click **Next** three times. 19. On the Name page, in Name, type **Inbound ICMPv6 Echo Requests**, and then click **Finish**. 20. Confirm that the rules you created appear in the Inbound Rules node. Close the Group Policy Management Editor, and close Group Policy Management console. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Note that these commands are required on each corpnet computer, and do not configure Group Policy settings:    **Set-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv4-In)" -Enabled True -Direction Inbound -Action Allow**  **Set-NetFirewallRule -DisplayName "File and Printer Sharing (Echo Request - ICMPv6-In)" -Enabled True -Direction Inbound -Action Allow** |

## Step 3: Configure APP1

APP1 configuration for the DirectAccess single server deployment test lab consists of the following procedures:

* Configure an IPv6 address on APP1
* Configure permissions of the Web Server certificate template
* Obtain an additional certificate for APP1
* Configure the HTTPS security binding

The following sections explain these procedures in detail.

### Configure an IPv6 address on APP1

The Windows Server 2012 Base Configuration test lab does not include IPv6 address configuration. In this step, add IPv6 address configuration to support a DirectAccess deployment.

To configure an IPv6 address on APP1

|  |
| --- |
| 1. In Server Manager, click **Local Server** in the console tree. Scroll to the top of the details pane, and click the link next to **Wired Ethernet Connection**. 2. In **Network Connections**, right-click **Wired Ethernet Connection**, and then click **Properties**. 3. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**. 4. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:1::3**. In **Subnet prefix length**, type **64**. In **Default gateway**, type **2001:db8:1::2**. Click **Use the following DNS server addresses**, and in **Preferred DNS server**, type **2001:db8:1::1**. Click **OK**. 5. Click Internet Protocol Version 4 (TCP/IPv4), and then click Properties. 6. In **Default gateway**, type **10.0.0.2**, and then click **OK**. 7. Close the **Wired Ethernet Connection Properties** dialog box. 8. Close the **Network Connections** window. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints. Note that the "Wired Ethernet Connection" interface name may be different on your computer. Use **ipconfig /all** to list out the interfaces.    **New-NetIPAddress -InterfaceAlias "Wired Ethernet Connection" -IPv6Address 2001:db8:1::3 -PrefixLength 64**  **Set-DnsClientServerAddress -InterfaceAlias "Wired Ethernet Connection" -ServerAddresses 2001:db8:1::1**  **New-NetRoute -DestinationPrefix 2001:db8:1::/64 -InterfaceAlias "Wired Ethernet Connection" -NextHop 2001:db8:1::2 -AddressFamily IPv6**  **New-NetRoute -DestinationPrefix 10.0.0.0/24 -InterfaceAlias "Wired Ethernet Connection" -NextHop 10.0.0.2 -AddressFamily IPv4** |

### Configure permissions of the Web Server certificate template

Next, configure permissions on the Web Server certificate template so that requesting computers can specify the subject name of a certificate.

To configure permissions of the Web Server certificate template

|  |
| --- |
| 1. On APP1, from the Start screen, click **Certification Authority**. 2. In the details pane, expand **corp-APP1-CA**. 3. Right-click **Certificate Templates**, and then click **Manage.** 4. In the Certificate Templates console, right-click the **Web Server** template, and then click **Properties**. 5. Click the **Security** tab, and then click **Authenticated Users**. 6. In **Permissions for Authenticated Users**, click **Enroll** under **Allow**, and then click **OK**.   Note  The **Authenticated Users** group is configured here for simplicity in the test lab. In a real deployment, you would specify the name of a security group that contains the computer accounts of the computers in your organization that can request custom certificates, which includes the DirectAccess server and network location server.   1. Close the Certificate Templates console. |

### Obtain an additional certificate on APP1

Obtain an additional certificate for APP1 with a customized subject and alternative name for network location.

To obtain an additional certificate for APP1

|  |
| --- |
| 1. From the Start screen, 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 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**, 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 **nls.corp.contoso.com**, and then click **Add**. 10. Click **OK**, click **Enroll**, and then click **Finish**. 11. In the details pane of the Certificates snap-in, verify that a new certificate with the name nls.corp.contoso.com was enrolled with Intended Purposes of Server Authentication. 12. 12. Close the console window. If you are prompted to save settings, click No. |

### Configure the HTTPS security binding

Next, configure the HTTPS security binding so that APP1 can act as the network location server.

To configure the HTTPS security binding

|  |
| --- |
| 1. From the Start screen, click **Internet Information Services (IIS) Manager**. 2. In the console tree of Internet Information Services (IIS) Manager, open **APP1**/**Sites**, and then click **Default Web site**. 3. In the **Actions** pane, click **Bindings**. 4. In the **Site Bindings** dialog box, click **Add**. 5. In the **Add Site Binding** dialog box, in the **Type** list, click **https**. In **SSL Certificate**, click the certificate with the name **nls.corp.contoso.com**. Click **OK**,and then click **Close**. 6. Close the Internet Information Services (IIS) Manager console. |

## Step 4: Install and Configure APP2

APP2 is a Windows Server 2003 SP2 Enterprise Edition computer that acts as an IPv4-only host and is used to demonstrate DirectAccess connectivity to IPv4-only resources using the DNS64 and NAT64 features. APP2 hosts both HTTP and SMB resources that the DirectAccess client computer will be able to access from the simulated Internet. The NAT64/DNS64 feature set enables organizations to deploy DirectAccess without requiring them to upgrade network resources to native IPv6 or even IPv6 capable.

APP2 configuration for the DirectAccess single server test lab consists of the following procedures:

* Install the operating system on APP2
* Install IIS web services
* Create a shared folder on APP2

The following sections explain these procedures in detail.

### Install the operating system on APP2

The first step is to install and configure Windows Server 2003 Enterprise Edition SP2 on APP2.

To install the operating system on APP2

|  |
| --- |
| 1. Start the installation of Windows Server 2003. 2. On the Welcome to the Windows Setup Wizard page, click Next. 3. On the Regional and Language Options page, click Next. 4. On the Personalize Your Software page, enter your Name and Organization information, click Next. 5. On the Licensing Modes page, select Per server. Number of concurrent connections option and enter 100. Click Next. 6. On the Computer Name and Administrator Password page, in the Computer name text box, enter APP2. Enter a strong Administrator password and confirm password. Click Next. 7. On the Date and Time Settings page, set the correct date and time and click Next. 8. On the Networking Settings page, select Custom Settings and click Next. 9. On the Networking Components page, select Internet Protocol (TCP/IP) and click Properties. 10. On the Internet Protocol (TCP/IP) Properties page, click Use the following IP address. In the IP address text box, enter 10.0.0.4. In the Subnet mask text box, enter 255.255.255.0. In Default gateway, type 10.0.0.2. Click Use the following DNS server addresses. In the Preferred DNS server text box, enter 10.0.0.1. 11. On the Internet Protocol (TCP/IP) Properties dialog box, click OK. On the Networking Components page, click Next. 12. On the Workgroup or Computer Domain page, click Yes make this computer a member of the following domain. In the text box, enter CORP. 13. On the Join Computer to CORP Domain dialog box, in the User name text box, enter CORP\User1 and in the Password text box, enter the password for User1. Click OK. 14. Log on as CORP\User1. |

### Install IIS web services on APP2

Next, configure APP2 as a web server. APP2 will be used to demonstrate HTTP connectivity over the DirectAccess connection to an IPv4-only host.

To install IIS web services on APP2

|  |
| --- |
| 1. On APP2, click Start, point to Control Panel, and then click Add or Remove Programs. 2. On the Add or Remove Programs dialog box, click Add/Remove Windows Components. 3. In the Windows Components Wizard, on the Windows Components page, select Application Server, and then click Details. 4. On the Application Server dialog box, select the Internet Information Services (IIS) check box. Click OK. 5. On the Windows Components page, click Next. 6. On the Completing the Windows Components Wizard page, click Finish. 7. Close the Add or Remove Programs window. 8. In the Quick Start Bar, click the Internet Explorer icon. 9. On the dialog box that informs you Internet Explorer Enhanced Security Configuration is enabled, select the In the future, do not show this message check box and then click OK. 10. In the Internet Explorer address bar, enter http://localhost and press ENTER. 11. You should see the IIS "Under Construction" page, indicating that the default IIS website is available and running. Close Internet Explorer. |

### Create a shared folder on APP2

Create a shared folder on APP2 to demonstrate SMB connectivity over the DirectAccess connection.

To create a shared folder on APP2

|  |
| --- |
| 1. On APP2, click Start, and then click Windows Explorer. 2. In the left pane of Windows Explorer, expand My Computer and click Local Disk (C:). 3. On the File menu, click New, and then click Folder. 4. Rename New Folder to Files. 5. Right-click the Files folder and click Sharing and Security. 6. On the Files Properties dialog box, on the Sharing tab, click Share this folder. Accept the default share name, which is Files, and then click OK. 7. Double click the Files folder. 8. On the File menu, click New, and then click New Text Document. 9. Double click the New Text Document.txt file. 10. In the New Text Document.txt – Notepad window, enter This is a text document on APP2, an IPv4 only server. 11. Close Notepad. On the **Notepad** dialog box, click **Yes** to save the changes. 12. Close Windows Explorer. |

## Step 5: Configure EDGE1

EDGE1 configuration for the DirectAccess single server deployment test lab consists of the following procedures:

* Configure an IPv6 address on EDGE1
* Provision EDGE1 with a certificate for IP-HTTPS
* Install the Remote Access role on EDGE1
* Configure DirectAccess on EDGE1
* Confirm Group Policy settings
* Confirm IPv6 settings

The following sections explain these procedures in detail.

### Configure an IPv6 address on EDGE1

The Windows Server 2012 Base Configuration test lab does not include IPv6 address configuration. In this step, add IPv6 address configuration to EDGE1 to support a DirectAccess deployment.

To configure an IPv6 address on EDGE1

|  |
| --- |
| 1. In Server Manager, click **Local Server** in the console tree. Scroll to the top of the details pane, and click the link next to **Corpnet**. 2. In **Network Connections**, right-click **Corpnet**, and then click **Properties**. 3. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**. 4. Click **Use the following IPv6 address**. In **IPv6 address**, type **2001:db8:1::2**. In **Subnet prefix length**, type **64**. Click **Use the following DNS server addresses**, and in **Preferred DNS server**, type **2001:db8:1::1**. Click **OK**. 5. Close the **Corpnet Properties** dialog box. 6. Close the **Network Connections** window. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.    **New-NetIPAddress -InterfaceAlias Corpnet -IPv6Address 2001:db8:1::2 -PrefixLength 64**  **Set-DnsClientServerAddress -InterfaceAlias Corpnet -ServerAddresses 2001:db8:1::1** |

### Provision EDGE1 with a certificate for IP-HTTPS

A certificate is required to authenticate the IP-HTTPS listener when clients connect over HTTPS.

To install an IP-HTTPS certificate on EDGE1

|  |
| --- |
| 1. On EDGE1, from the Start screen, 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**, 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 **edge1.contoso.com**, and then click **Add**. 10. In the **Alternative name** area, under **Type**, select **DNS**. 11. In **Value**, type **edge1.contoso.com**, and then click **Add**. 12. On the **General** tab, under **Friendly name**, type **IP-HTTPS Certificate**. 13. Click **OK**, click **Enroll**, and then click **Finish**. 14. In the details pane of the Certificates snap-in, verify that a new certificate with the name **edge1.contoso.com** was enrolled with Intended Purposes of Server Authentication. 15. Close the console window. If you are prompted to save settings, click **No**. |

### Install the Remote Access server role on EDGE1

The Remote Access server role in Windows Server 2012 combines the DirectAccess feature and the RRAS role service into a new unified server role. This new Remote Access server role allows for centralized administration, configuration, and monitoring of both DirectAccess and VPN-based remote access services. Use the following procedure to install the Remote Access role on EDGE1.

To install the Remote Access server role on EDGE1

|  |
| --- |
| 1. In the **Dashboard** console of Server Manager, under **Configure this local server**, click **Add roles and features**. 2. Click **Next** three times to get to the server role selection screen. 3. In the **Select Server Roles** dialog, select **Remote Access**, click **Add Features** when prompted, and then click **Next**. 4. Click **Next** five times to accept the defaults for features, remote access role services, and web server role services. 5. On the Confirmation screen, click **Install**. 6. Wait for the feature installations to complete, and then click **Close**. |

|  |
| --- |
| Description: Description: Description: http://upload.wikimedia.org/wikipedia/en/7/7f/Windows_PowerShell_icon.png **Windows PowerShell equivalent commands** |
| The following Windows PowerShell cmdlet or cmdlets perform the same function as the preceding procedure. Enter each cmdlet on a single line, even though they may appear word-wrapped across several lines here because of formatting constraints.    **Install-WindowsFeature RemoteAccess -IncludeManagementTools** |

### Configure DirectAccess on EDGE1

Configure DirectAccess in a single server deployment using the Remote Access Setup Wizard.

To configure DirectAccess on EDGE1

|  |
| --- |
| 1. From the Start screen, click **Remote Access Management**. 2. In the Remote Access Management console, click **Run the Remote Access Setup Wizard**. 3. In the Configure Remote Access wizard, click **Deploy DirectAccess only**. 4. Under Step 1 Remote Clients, click **Configure**. 5. Select **Deploy full DirectAccess for client access and remote management**, and then click **Next**. 6. On the Select Groups screen, click **Add**, type **DirectAccessClients**, click **OK**, and then click **Next**. 7. On the Network Connectivity Assistant screen, next to **DirectAccess connection name**, type **Contoso DirectAccess Connection**. Click **Finish**. 8. Under Step 2 DirectAccess Server, click **Configure**. 9. Verify that **Edge** is selected as the network topology. Type **edge1.contoso.com** as the public name to which remote access clients will connect. Click **Next**. 10. On the Network Adapters screen, wait for the wizard to populate the Internet and Corpnet interfaces. Verify that **CN=edge1.contoso.com** is the certificate automatically selected to authenticate IP-HTTPS connections. Click **Next**. 11. On the Prefix Configuration screen, click **Next**. 12. On the Authentication screen, select **Use computer certificates**, and then click **Browse**. 13. Select **corp-APP1-CA**, click **OK,** and then click **Finish.** 14. Under Step 3 Infrastructure Servers, click **Configure**. 15. For the URL of the network location server, type **https://nls.corp.contoso.com**, and then click **Validate**. 16. Once connectivity to the NLS URL on APP1 is validated successfully, click **Next**. 17. Click **Next** twice to accept defaults for DNS and Management, and then click **Finish**. 18. At the bottom of the Remote Access Setup screen, click **Finish**. 19. In the Remote Access Review dialog, click **Apply**. 20. After the Remote Access Setup Wizard completes, click **Close**. 21. In the console tree of the Remote Access Management console, select **Operations Status**. Wait until the status of all monitors display as "Working". In the Tasks pane under Monitoring, click **Refresh** periodically to update the display.   **Note:** In this release of Windows Server 2012, the status of Network adapters may be yellow instead of green. To ensure that the status of Network adapters shows as Working, open an elevated command prompt, type the following command and then press ENTER.  **netsh interface ipv6 add route 2001:db8:1::/48 publish=yes interface = "Corpnet"** |

### Confirm Group Policy settings

The DirectAccess wizard configures GPOs and settings that are automatically deployed via Active Directory for the Remote Access server and the DirectAccess clients.

To examine Group Policy settings created by the DirectAccess wizard

|  |
| --- |
| 1. On EDGE1, from the Start screen, click Group Policy Management. 2. Expand Forest: corp.contoso.com, expand Domains, expand corp.contoso.com, and then expand Group Policy Objects. 3. The Remote Access Setup wizard creates two new GPOs. DirectAccess Client Settings is applied to members of the DirectAccessClients security group. DirectAccess Server Settings is applied to the EDGE1 DirectAccess server. Confirm that the correct security filtering is done for each of these GPOs by clicking the GPO and then viewing the entries in the Security Filtering section on the Scope tab in the details pane of the console. 4. From the Start screen, type wf.msc, and then press ENTER. 5. In the Windows Firewall with Advanced Security console, note that the Domain Profile is Active and the Public Profile is Active. It is important that the Windows Firewall is enabled and both the domain and public profiles are active. If the Windows Firewall is disabled, or if domain or public profiles are disabled, DirectAccess will not function correctly. 6. In the Windows Firewall with Advanced Security console tree, click the Connection Security Rules node. The details pane of the console will display two connection security rules: DirectAccess Policy-DaServerToCorp, and DirectAccess Policy-DaServerToInfra. The first rule is used to establish the intranet tunnel and the second rule is for the infrastructure tunnel. Both of these rules are delivered to EDGE1 using Group Policy. 7. Close the Windows Firewall with Advanced Security console. |

### Confirm IPv6 settings

For the DirectAccess solution to function, the IPv6 settings on EDGE1 must be correct.

To confirm IPv6 settings

|  |
| --- |
| 1. On EDGE1, from the desktop taskbar, right-click **Windows PowerShell**, and then click **Run as administrator**.  2. In the Windows PowerShell window, type Get-NetIPAddress and press ENTER.  3. The output displays information related to the EDGE1 networking configuration. There are several sections of interest:   The 6TO4 Adapter section shows information that includes the Global IPv6 address used by EDGE1 on its external interface.   The IPHTTPSInterface section shows information regarding the IP-HTTPS interface.  4. To see information regarding the Teredo interface on EDGE1, type netsh interface Teredo show state and press ENTER. The output should include an entry State: online |

## Step 6: Configure CLIENT1

Use the following procedures to demonstrate remote access connectivity with CLIENT1:

* Connect CLIENT1 to the Corpnet subnet and update group policy
* Connect CLIENT1 to the Internet subnet and test remote access
* Connect CLIENT1 to the Homenet subnet and test remote access
* Monitor the client connection on the EDGE1 DirectAccess server

The following sections explain these procedures in detail.

### Connect CLIENT1 to the Corpnet subnet and update group policy

To receive the DirectAccess settings, CLIENT1 must update its group policy while connected to the Corpnet subnet.

To update group policy on CLIENT1 and apply DirectAccess settings

|  |
| --- |
| 1. Connect CLIENT1 to the Corpnet subnet. 2. Restart the CLIENT1 computer to update group policy and security group membership while connected to the Corpnet subnet. After restarting, log on as CORP\User1. 3. From the Start screen, type **PowerShell**, then right-click **Windows PowerShell**, and click **Run as administrator**. 4. Type **Get-DnsClientNrptPolicy** and hit **ENTER**. The Name Resolution Policy Table (NRPT) entries for DirectAccess are displayed. Note that the NLS server exemption is displayed as NLS.corp.contoso.com. This is the alias used for the APP1 server. All other name resolution for corp.contoso.com will use the internal IPv6 address of the EDGE1 server (2001:db8::1::2) when outside the corporate network. 5. Type **Get-NCSIPolicyConfiguration** and hit **ENTER**. The network connectivity status indicator settings deployed by the wizard are displayed. Note that the value of DomainLocationDeterminationURL is https://nls.corp.contoso.com. Whenever this network location server URL is accessible, the client will determine that it is inside the corporate network, and NRPT settings will not be applied. 6. Type **Get-DAConnectionStatus** and hit **ENTER**. Since the client can reach the network location server URL, the status will display as **ConnectedLocally**. |

### Connect CLIENT1 to the Internet subnet and test remote access

To test remote access connectivity from the Internet, move the CLIENT1 connection to the Internet subnet.

To test remote access from the Internet

|  |
| --- |
| 1. Connect CLIENT1 to the Internet subnet. Once the network determination process completes, the network icon should indicate Internet access. 2. In the PowerShell window, type **Get-DAConnectionStatus** and hit **ENTER**. The status should show as **ConnectedRemotely**. 3. Click the network icon in the System Notification Area. Note that **Contoso DirectAccess Connection** is listed as **Connected**. This is the connection name we provided in the DirectAccess wizard. 4. Right-click **Contoso DirectAccess Connection** and then click **Properties**. Note that Status shows as **Connected**. 5. From the PowerShell prompt, type **ping inet1.isp.example.com** and hit **ENTER** to verify Internet name resolution and connectivity. You should receive four replies from 131.107.0.1. 6. Type **ping app1.corp.contoso.com** and hit **ENTER** to verify corporate intranet name resolution and connectivity. Since APP1 is an IPv6 enabled intranet resource, the ICMP response is from the IPv6 address of APP1 (2001:db8:1::3). 7. Type **ping app2.corp.contoso.com** and hit **ENTER** to verify name resolution and connectivity to the intranet Windows Server 2003 file server. Note the format of the IPv6 address returned. Since APP2 is an IPv4-only intranet resource, the dynamically created NAT64 address of APP2 is returned. The dynamically created prefix assigned by DirectAccess for NAT64 will be in the form fdxx:xxxx:xxxx:7777::/96. 8. Click the Internet Explorer icon to launch IE. Verify that you can access the website on **http://inet1.isp.example.com**. This site is running on the INET1 Internet server, and validates Internet connectivity outside of DirectAccess. 9. Verify that you can access the website on **http://app1.corp.contoso.com**. This site is running on the APP1 server, and validates DirectAccess connectivity to an internal IPv6 web server. 10. Verify that you can access the website on **http://app2.corp.contoso.com**. You should see the default "Under Construction" IIS web page, validating DirectAccess connectivity to an internal IPv4-only web server. 11. From the desktop taskbar, click the **Windows Explorer** icon. 12. In the address bar, type **\\app1\Files**, and then press **ENTER**. 13. You should see a folder window with the contents of the Files shared folder. 14. In the **Files** shared folder window, double-click the **Example.txt** file. You should see the contents of the Example.txt file. 15. Close the **Example - Notepad** window. 16. In the Windows Explorer address bar, type **\\app2\Files**, and then press **ENTER**. 17. In the **Files** shared folder window, double-click the **New Text Document.txt** file. You should see the contents of the document shared on the IPv4-only server. 18. Close the **New Text Document - Notepad** and the **Files** shared folder windows. 19. From the PowerShell window, type **Get-NetIPAddress** and then press **ENTER** to examine the client's IPv6 configuration. 20. Type **Get-NetTeredoState** and hit **ENTER** to examine the Teredo configuration. Note that the Teredo server name is edge1.contoso.com, the externally resolvable DNS name of the EDGE1 server. 21. Type **Get-NetIPHTTPSConfiguration** and hit ENTER. Examine the settings applied by group policy to direct the client to https://edge1.contoso.com:443/IPHTTPS. 22. Type **wf.msc** and then hit **ENTER** to launch the Windows Firewall with Advanced Security console. Expand **Monitoring**, then **Security Associations** to examine the IPsec SAs established. Note that the authentication methods used are Computer Kerberos and User Kerberos, as well as Computer certificate and User Kerberos. 23. Select **Connection Security Rules** in the console tree. Examine the rules used to provide DirectAccess connectivity. 24. Close the Windows Firewall with Advanced Security console. |

### Connect CLIENT1 to the Homenet subnet and test remote access

To test remote access connectivity from a simulated home network behind a NAT, move the CLIENT1 connection to the Homenet subnet.

To test remote access from the home network

|  |
| --- |
| 1. Connect CLIENT1 to the Homenet subnet. Once the network determination process completes, the network icon should indicate Internet access. 2. In the PowerShell window, type **Get-DAConnectionStatus** and hit **ENTER**. The status should show as **ConnectedRemotely**. 3. Click the network icon in the System Notification Area. Note that **Contoso DirectAccess Connection** is listed as **Connected**. Right-click **Contoso DirectAccess Connection** and then click **Properties**. Note that Status shows as **Connected**. 4. Type **ping app1.corp.contoso.com** and hit **ENTER** to verify corporate intranet name resolution and connectivity to an internal IPv6 resource. 5. Type **ping app2.corp.contoso.com** and hit **ENTER** to verify corporate intranet name resolution and connectivity to an internal IPv4 resource. 6. Click the Internet Explorer icon to launch IE. Verify that you can access the websites on **http://inet1.isp.example.com**, **http://app1.corp.contoso.com**, and **http://app2.corp.contoso.com**. 7. From the desktop taskbar, click the **Windows Explorer** icon. 8. Verify that you can access the shared files in **\\APP1\Files** and **\\APP2\Files**. 9. Close the Windows Explorer window. 10. In the PowerShell window, type **Get-NetIPAddress** and then press **ENTER** to examine the client's IPv6 configuration. 11. Type **Get-NetTeredoState** and hit **ENTER** to examine the Teredo configuration. Note that the Teredo state is listed as **qualified**. 12. Type **ipconfig** and hit **ENTER**. Note that in this deployment behind a NAT, the DirectAccess client is connecting via the Teredo tunnel adapter. |

### Monitor the client connection on the EDGE1 DirectAccess server

The Remote Access Management Console in Windows Server 2012 provides remote client status monitoring functionality for both DirectAccess and VPN connections.

To monitor the client connection on EGDE1



|  |
| --- |
| 1. On EDGE1, from the Start screen, click **Remote Access Management**. 2. In the Remote Access Management console, select **Dashboard**. 3. Examine the data collected under **Remote Client Status**. 4. In the Remote Access Management console, select **Remote Client Status**. 5. Double-click the CLIENT1 connection to display the detailed remote client statistics dialog. |

# Snapshot the Configuration

This completes the DirectAccess single server deployment test lab. To save this configuration so that you can quickly return to a working remote access configuration from which you can test other modular test lab guides (TLGs), TLG extensions, or for your own experimentation and learning, do the following:

1. On all physical computers or virtual machines in the test lab, close all windows and then perform a graceful shutdown.
2. If your lab is based on virtual machines, save a snapshot of each virtual machine and name the snapshots **DirectAccess single server**. If your lab uses physical computers, create disk images to save the DirectAccess single server test lab configuration.

# Additional Resources

For more information about DirectAccess, see the [DirectAccess TechNet portal page](http://technet.microsoft.com/en-us/network/dd420463.aspx).

For a list of additional Microsoft TLGs, see [Test Lab Guides](http://go.microsoft.com/fwlink/?LinkID=202817) in the TechNet Wiki.