

Microsoft® Official Course



Module 1

Deploying and Managing Windows
Server 2012

Microsoft®

Module Overview

- Windows Server 2012 Overview
- Installing Windows Server 2012
- Post-Installation Configuration of Windows Server 2012
- Overview of Windows Server 2012 Management
- Introduction to Windows PowerShell

Lesson 1: Windows Server 2012 Overview

- Windows Server 2012 R2 Editions
- What Is Server Core?
- Windows Server 2012 R2 Roles
- What Are the Windows Server 2012 Features?

Windows Server 2012 R2 Editions

Windows Server 2012 editions:

- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 R2 Foundation
- Windows Server 2012 R2 Essentials
- Microsoft Hyper-V Server 2012 R2
- Windows Storage Server 2012 R2 Workgroup
- Windows Storage Server 2012 R2 Standard
- Windows MultiPoint Server 2012 Standard
- Windows MultiPoint Server 2012 Premium

What Is Server Core?

Server Core:

- Is a more secure, less resource-intensive installation option
- Can be converted to full graphical shell version of Windows Server 2012
- Is the default installation option for Windows Server 2012
- Is managed locally using sconfig.cmd

With remote management enabled, you rarely will need to sign in locally

Windows Server 2012 R2 Roles

Roles

- Roles are made up of role services components that provide additional functionality associated with the role
- In Server Manager 2012, console servers with a similar role are grouped together
- Role deployment also includes the configuration of dependencies

What Are the Windows Server 2012 Features?

Features:

- Are components that support the server such as Windows Server Backup or Failover clustering
- Usually do not provide a service directly to clients on the network

Keep in mind the following points:

- Roles can have features as dependencies
- Features on Demand are features that need to be installed using a mounted image as a source

Lesson 2: Installing Windows Server 2012

- Installation Methods
- Installation Types
- Choosing Whether to Upgrade or Migrate
- Hardware Requirements for Windows Server 2012 R2
- Installing Windows Server 2012
- Migrating Server Roles

Installation Methods

**Windows Server 2012 R2 deployment
method options include:**



Optical disk

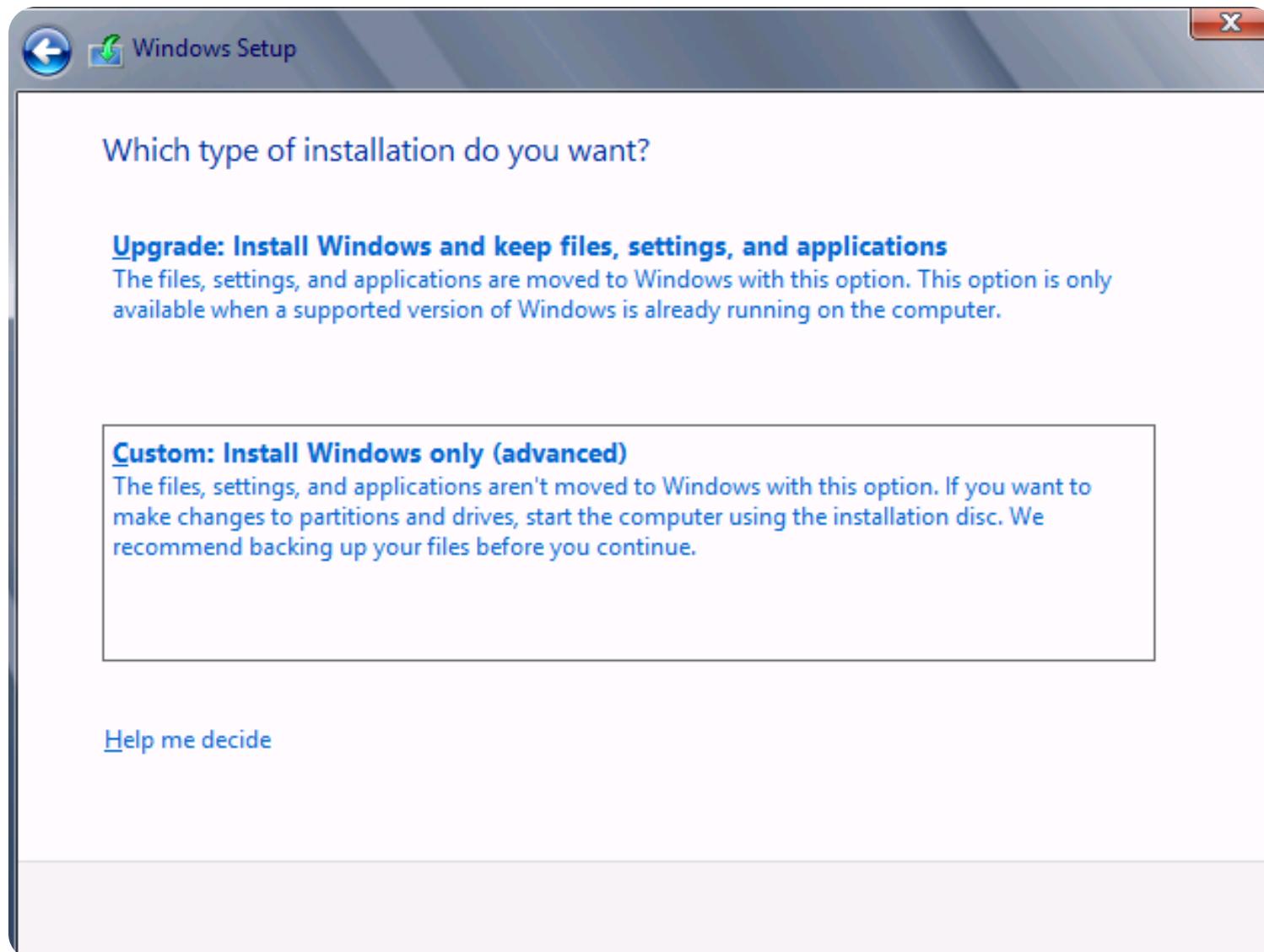


USB flash drive



Windows Deployment Services

Installation Types



Choosing Whether to Upgrade or Migrate

In-place upgrade



Advantages:

- Generally straightforward process that takes less time and planning than a migration strategy
- All server roles, features, data, and application settings are maintained



Disadvantages:

- More difficult to troubleshoot installation failures caused by existing applications or server roles
- Existing problems and configuration issues might be brought into the new operating system

Migration



Advantages:

- Easier to troubleshoot installation failures
- Existing configuration or application issues are not carried forward to the new operating system
- You can easily move to updated versions of applications



Disadvantages:

- Requires all applications to be reinstalled and configured
- Requires planning of migration of server roles
- Requires migration of data
- Requires the purchase of new hardware

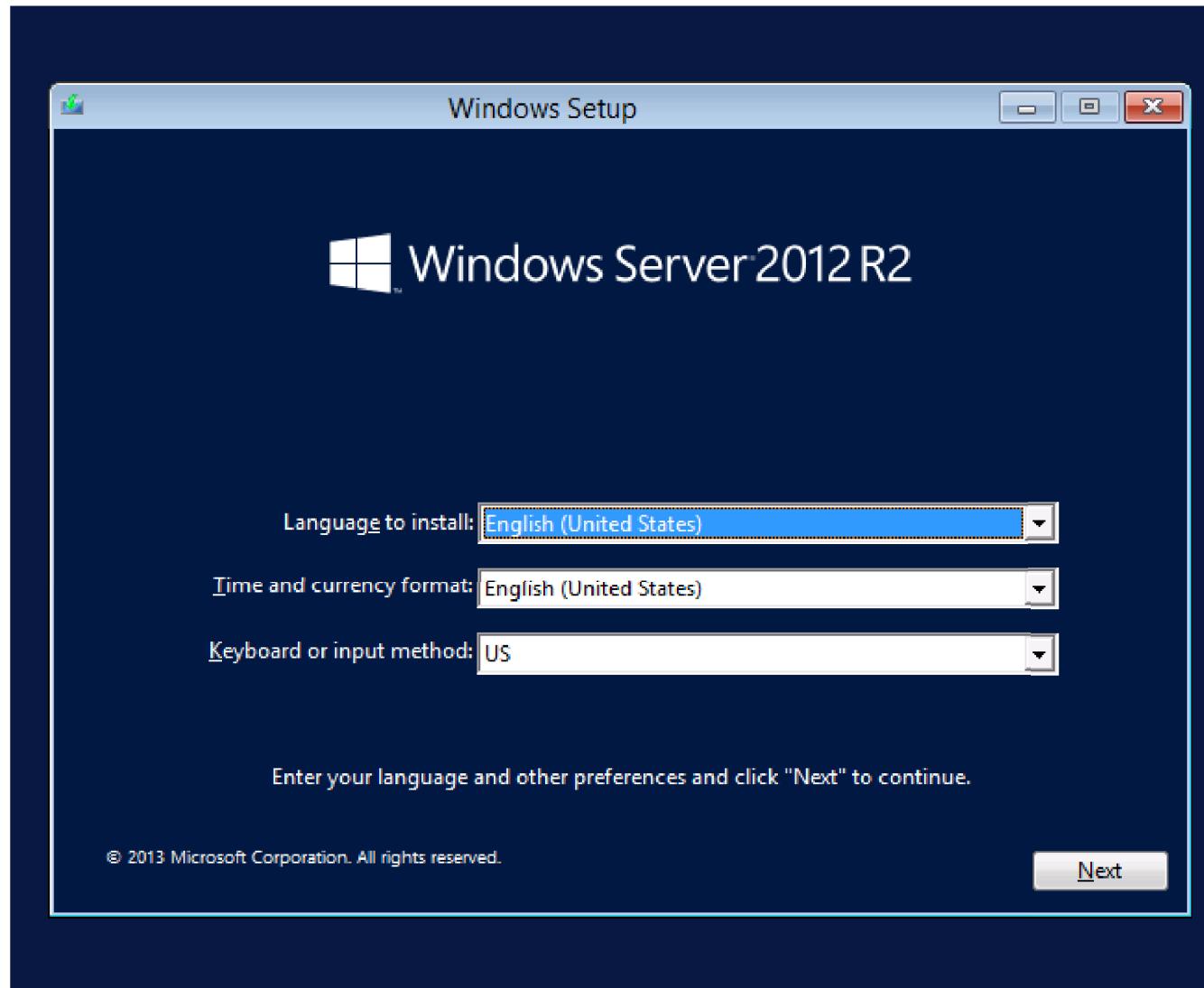
Hardware Requirements for Windows Server 2012 R2

Windows Server 2012 R2 has the following minimum hardware requirements:

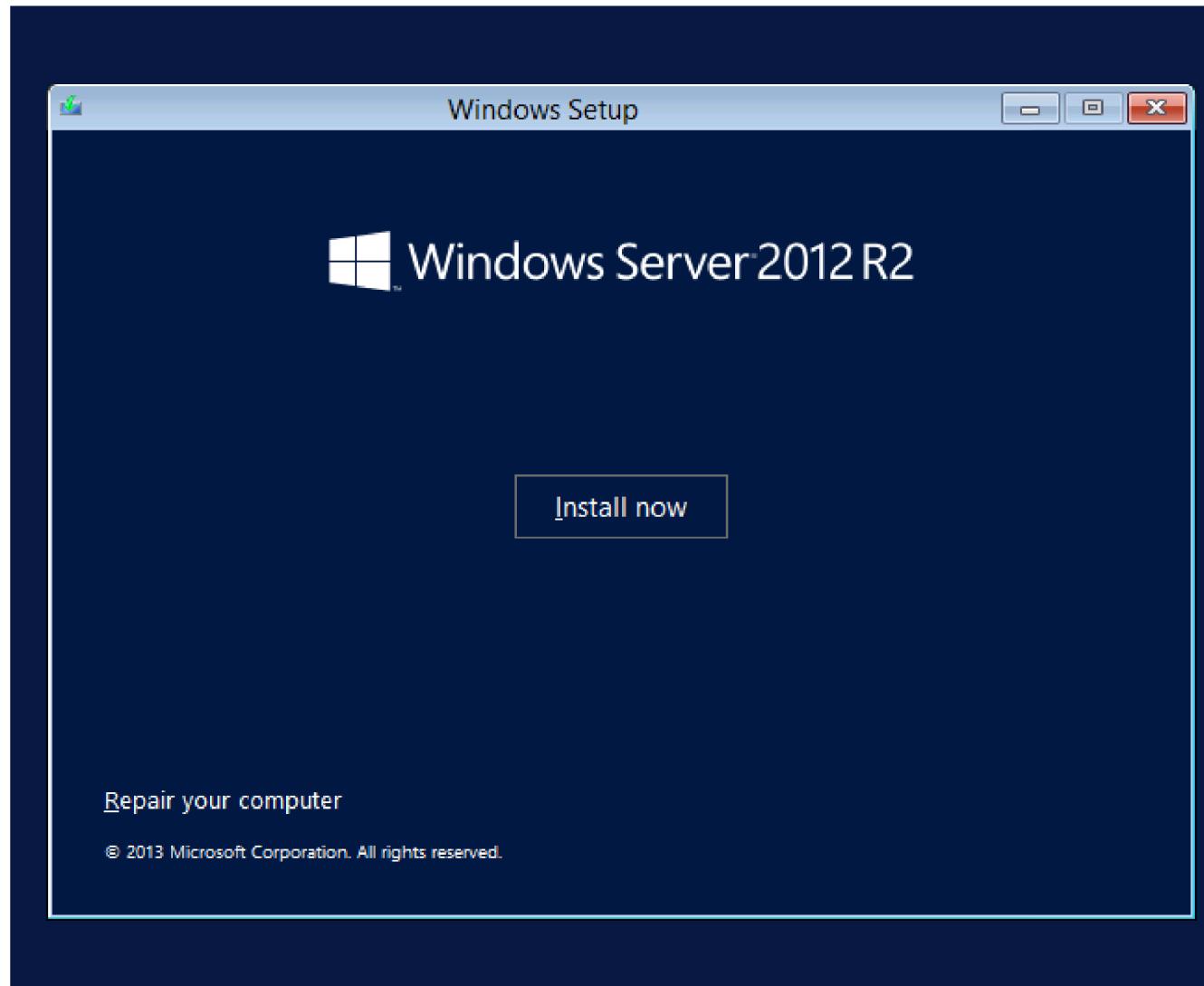
- Processor architecture x64
 - Processor speed 1.4 GHz
 - Memory (RAM) 512 MB
 - Hard disk drive space 32 GB
- More hard disk drive space is needed if the server has more than 16 GB of RAM



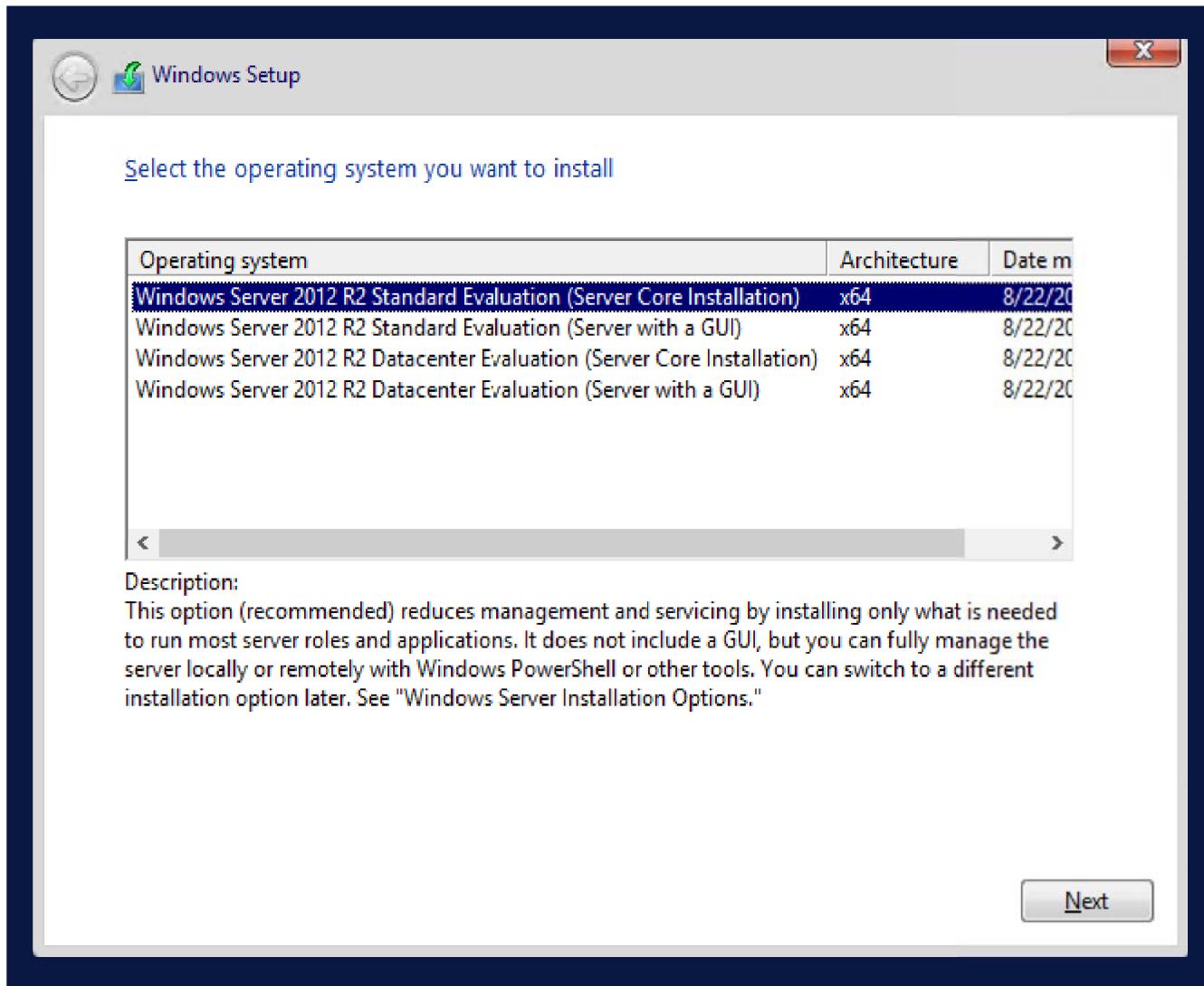
Installing Windows Server 2012



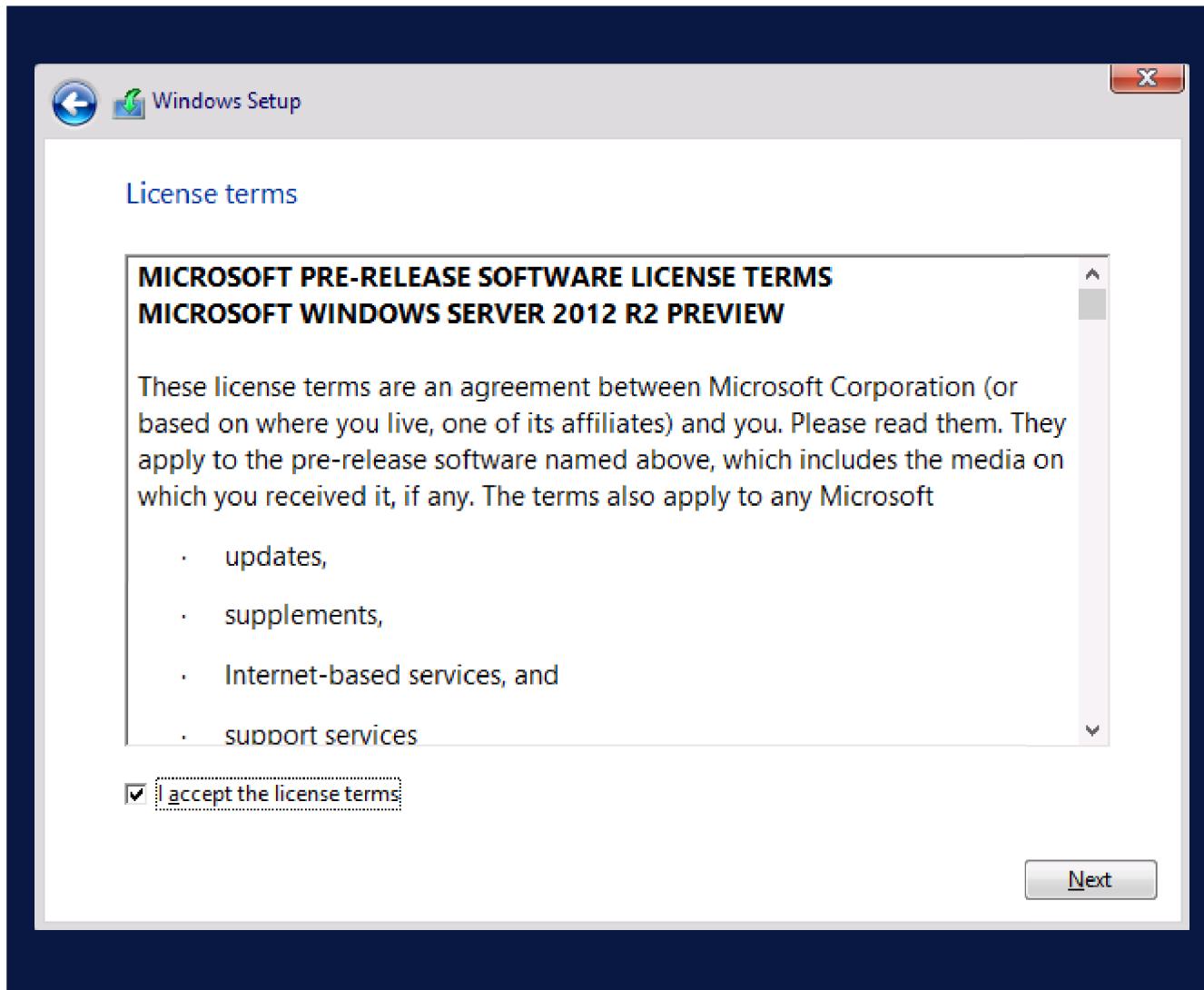
Installing Windows Server 2012



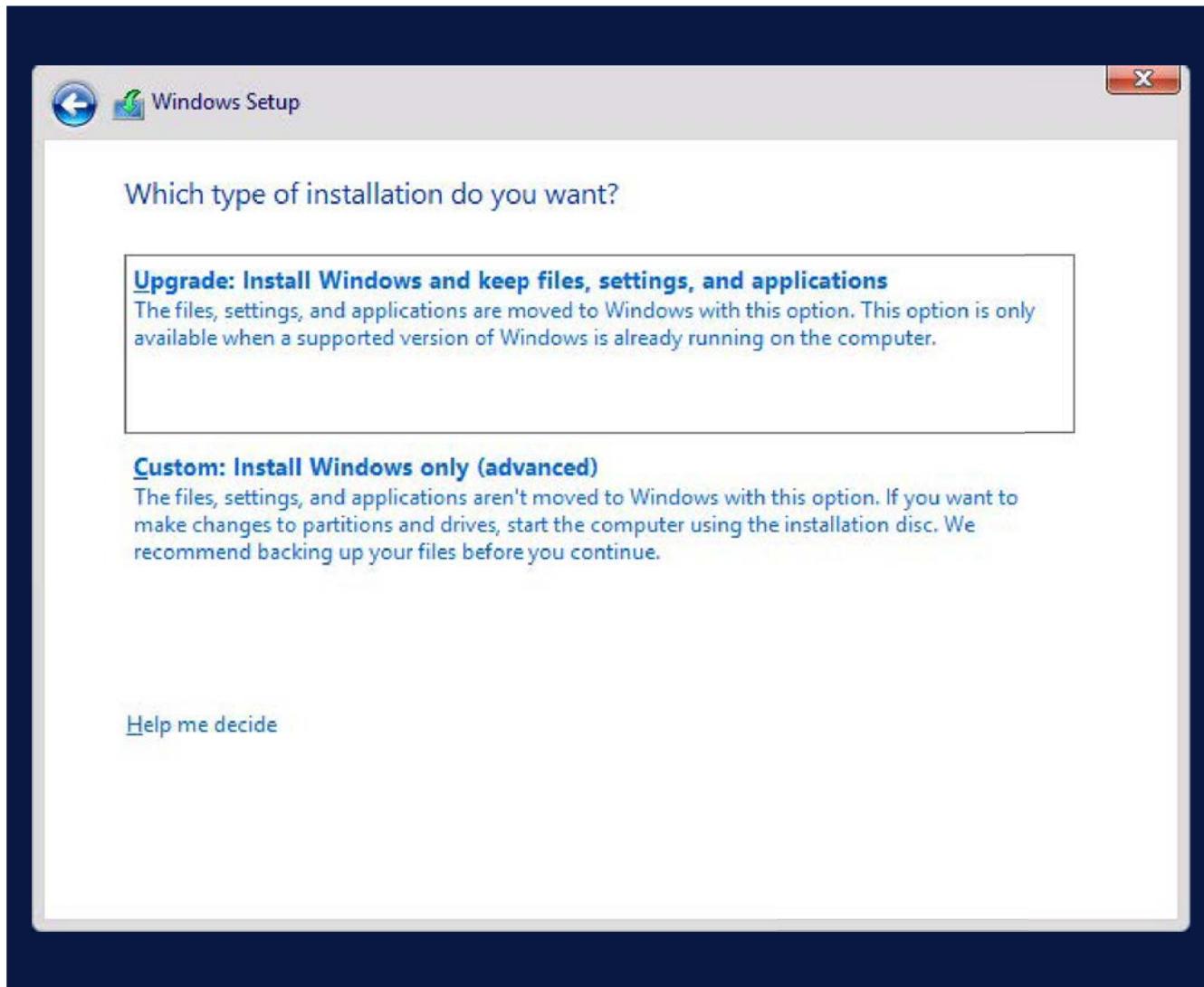
Installing Windows Server 2012



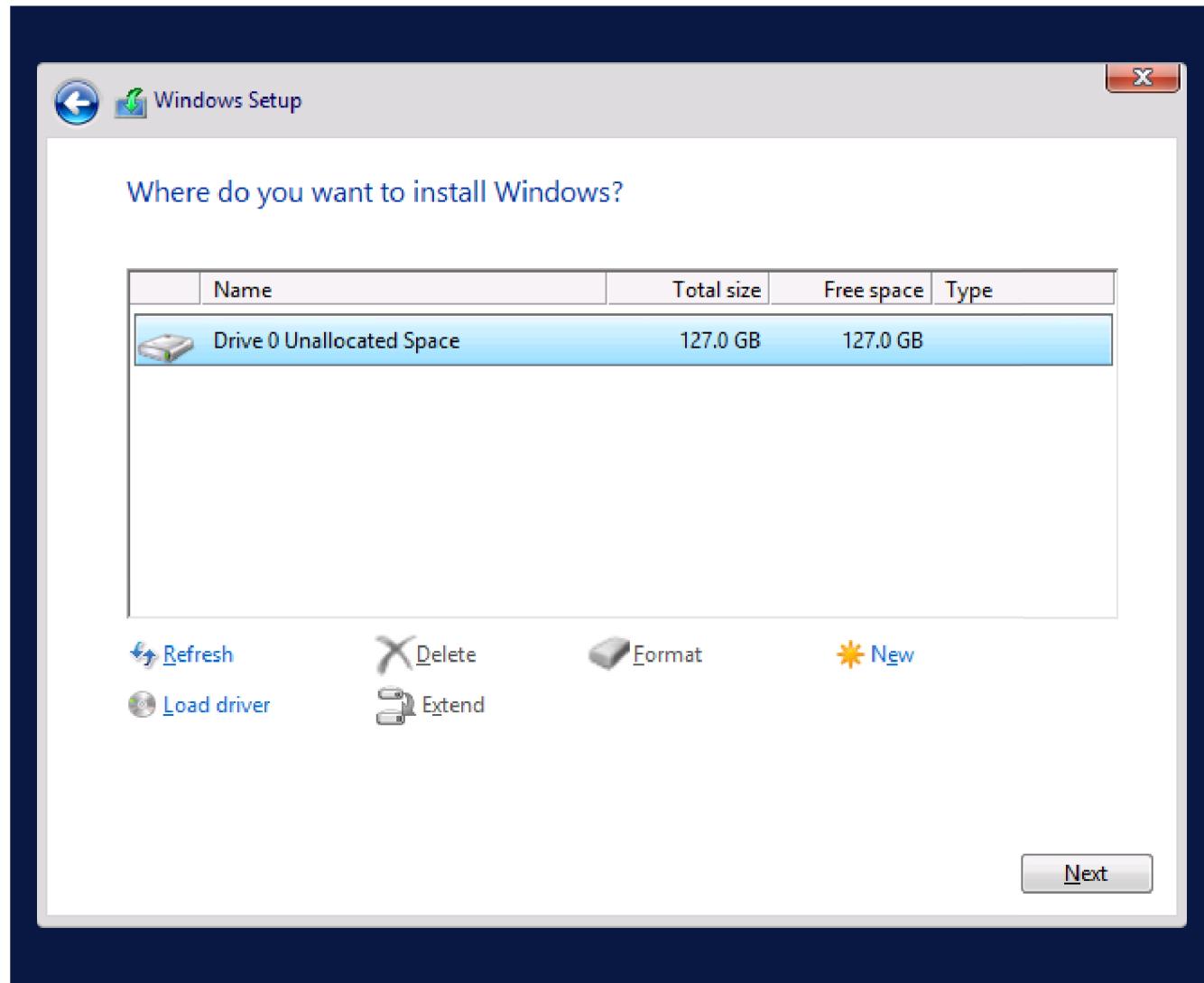
Installing Windows Server 2012



Installing Windows Server 2012



Installing Windows Server 2012



Installing Windows Server 2012

Settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name

Password

Reenter password

Finish



Migrating Server Roles

Windows Server Migration Tools assist in the migration process

Microsoft provides the following guides to assist in migration of roles and services:

- Migrate Active Directory Federation Services Role Services to Windows Server 2012
- Migrate Health Registration Authority to Windows Server 2012
- Migrate Hyper-V[®] to Windows Server 2012
- Migrate IP Configuration to Windows Server 2012
- Migrate Network Policy Server to Windows Server 2012
- Migrate Print and Document Services to Windows Server 2012
- Migrate Remote Access to Windows Server 2012
- Migrate Windows Server Update Services to Windows Server 2012

Lesson 3: Post-Installation Configuration of Windows Server 2012

- Overview of Post-Installation Configuration
- Configuring Server Network Settings
- How to Join a Domain
- Activating Windows Server 2012
- Configuring a Server Core Installation
- Demonstration: Using DISM to Add Windows Features

Overview of Post-Installation Configuration

PROPERTIES			
For WIN-GRUSOCV22M4			
TASKS			
Computer name	WIN-GRUSOCV22M4	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-90000-00000-AA632 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter Evaluation	Processors	AMD FX(tm)-8120 Eight-Core Processor
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	2 GB
		Total disk space	126.66 GB



Overview of Post-Installation Configuration

PROPERTIES			
For WIN-GRUSOCV22M4			
Computer name		Last installed updates	Never
Workgroup		Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-90000-00000-AA632 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter Evaluation	Processors	AMD FX(tm)-8120 Eight-Core Processor
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	2 GB
		Total disk space	126.66 GB



Overview of Post-Installation Configuration

PROPERTIES			
For WIN-GRUSOCV22M4			
Computer name		Last installed updates	Never
Computer name	WIN-GRUSOCV22M4	Windows Update	Not configured
Workgroup	WORKGROUP	Last checked for updates	Never
Windows Firewall	Private: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-90000-00000-AA632 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter Evaluation	Processors	AMD FX(tm)-8120 Eight-Core Processor
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	2 GB
		Total disk space	126.66 GB



Overview of Post-Installation Configuration

PROPERTIES			
For WIN-GRUSOCV22M4			
Computer name		Last installed updates	Never
Workgroup		Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-90000-00000-AA632 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter Evaluation	Processors	AMD FX(tm)-8120 Eight-Core Processor
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	2 GB
		Total disk space	126.66 GB



Overview of Post-Installation Configuration

Properties for WIN-GRUSOCV22M4			
Computer name	WIN-GRUSOCV22M4	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-90000-00000-AA632 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter Evaluation	Processors	AMD FX(tm)-8120 Eight-Core Processor
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	2 GB
		Total disk space	126.66 GB



Overview of Post-Installation Configuration

PROPERTIES		TASKS	
For WIN-GRUSOCV22M4			
Computer name	WIN-GRUSOCV22M4	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-90000-00000-AA632 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter Evaluation	Processors	AMD FX(tm)-8120 Eight-Core Processor
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	2 GB
		Total disk space	126.66 GB



Overview of Post-Installation Configuration

PROPERTIES		TASKS	
For WIN-GRUSOCV22M4			
Computer name	WIN-GRUSOCV22M4	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-90000-00000-AA632 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter Evaluation	Processors	AMD FX(tm)-8120 Eight-Core Processor
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	2 GB
		Total disk space	126.66 GB



Overview of Post-Installation Configuration

PROPERTIES			
For WIN-GRUSOCV22M4			
TASKS			
Computer name	WIN-GRUSOCV22M4	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Not configured
		Last checked for updates	Never
Windows Firewall	Private: On	Windows Error Reporting	Off
Remote management	Enabled	Customer Experience Improvement Program	Not participating
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC-08:00) Pacific Time (US & Canada)
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	00252-90000-00000-AA632 (activated)
Operating system version	Microsoft Windows Server 2012 R2 Datacenter Evaluation	Processors	AMD FX(tm)-8120 Eight-Core Processor
Hardware information	Microsoft Corporation Virtual Machine	Installed memory (RAM)	2 GB
		Total disk space	126.66 GB



Configuring Server Network Settings



PROPERTIES

For LON-DC1

Computer name

LON-DC1

Domain

Adatum.com

Windows Firewall

Domain: On

Remote management

Enabled

Remote Desktop

Disabled

NIC Teaming

Disabled

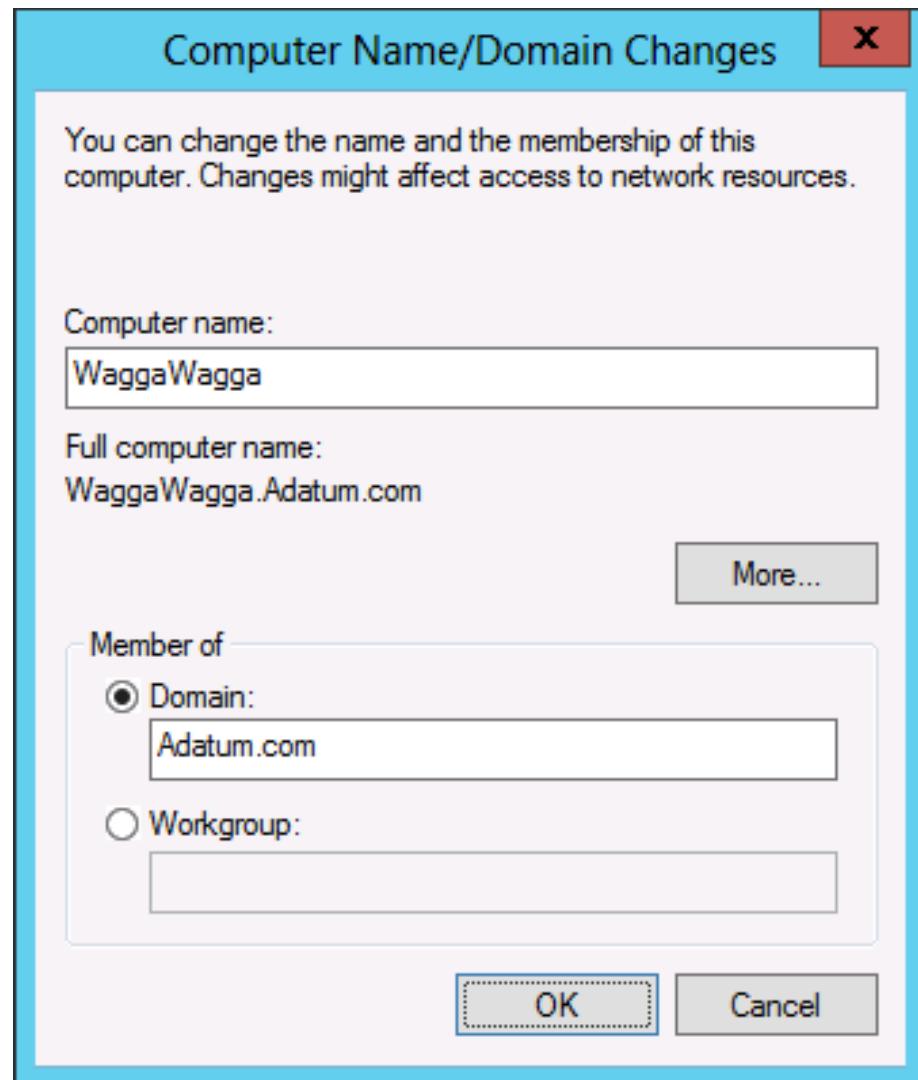
Ethernet

172.16.0.10, IPv6 enabled

How to Join a Domain

Information necessary for a domain join:

- Domain name
- Account with permission to join the computer to the domain



Activating Windows Server 2012

 Windows Activation X

Enter a product key to activate Windows

Your product key should be on the box that the Windows DVD came in or in an email that shows you bought Windows. You need to be signed in as an administrator to enter a product key for Windows activation. It looks similar to this:



A yellow Microsoft product key card with a barcode. The key is printed as: XXXXX-XXXXX-XXXXX-XXXXX-XXXXX. The Microsoft logo is at the top right, and a barcode is in the center.

Product key

DASHES WILL BE ADDED AUTOMATICALLY

[Read the Privacy Statement online](#)

Configuring a Server Core Installation

```
Administrator: C:\Windows\system32\cmd.exe - sconfig

=====
          Server Configuration
=====

1> Domain/Workgroup:           Domain: Adatum.com
2> Computer Name:             LON-CORE
3> Add Local Administrator
4> Configure Remote Management   Enabled
5> Windows Update Settings:    Manual
6> Download and Install Updates
7> Remote Desktop:            Disabled
8> Network Settings
9> Date and Time
10> Help improve the product with CEIP Not participating
11> Windows Activation

12> Log Off User
13> Restart Server
14> Shut Down Server
15> Exit to Command Line

Enter number to select an option:
```

Demonstration: Using DISM to Add Windows Features

In this demonstration, you see how to use the DISM command-line utility to:

- View a list of all Windows features and their current state
- Gather information about the Windows Server Backup feature
- Enable the Windows Server Backup feature

Lesson 4: Overview of Windows Server 2012 Management

- What Is Server Manager?
- Administrative Tools and Remote Server Administration Tools
- Demonstration: Using Server Manager
- Configuring Services
- Configuring Windows Remote Management
- Demonstration: Performing Remote Management

What Is Server Manager?

You can use Server Manager to:

- Manage multiple servers on a network from one console
- Add roles and features
- Launch Windows PowerShell sessions
- View events
- Perform server configuration tasks
- Manage down-level servers



You can use Best Practices Analyzer to:

- Determine whether roles on your network are functioning efficiently
- Query event logs for warning and error events
- Diagnose health issues with specific roles

Administrative Tools and Remote Server Administration Tools

Administrative tools:

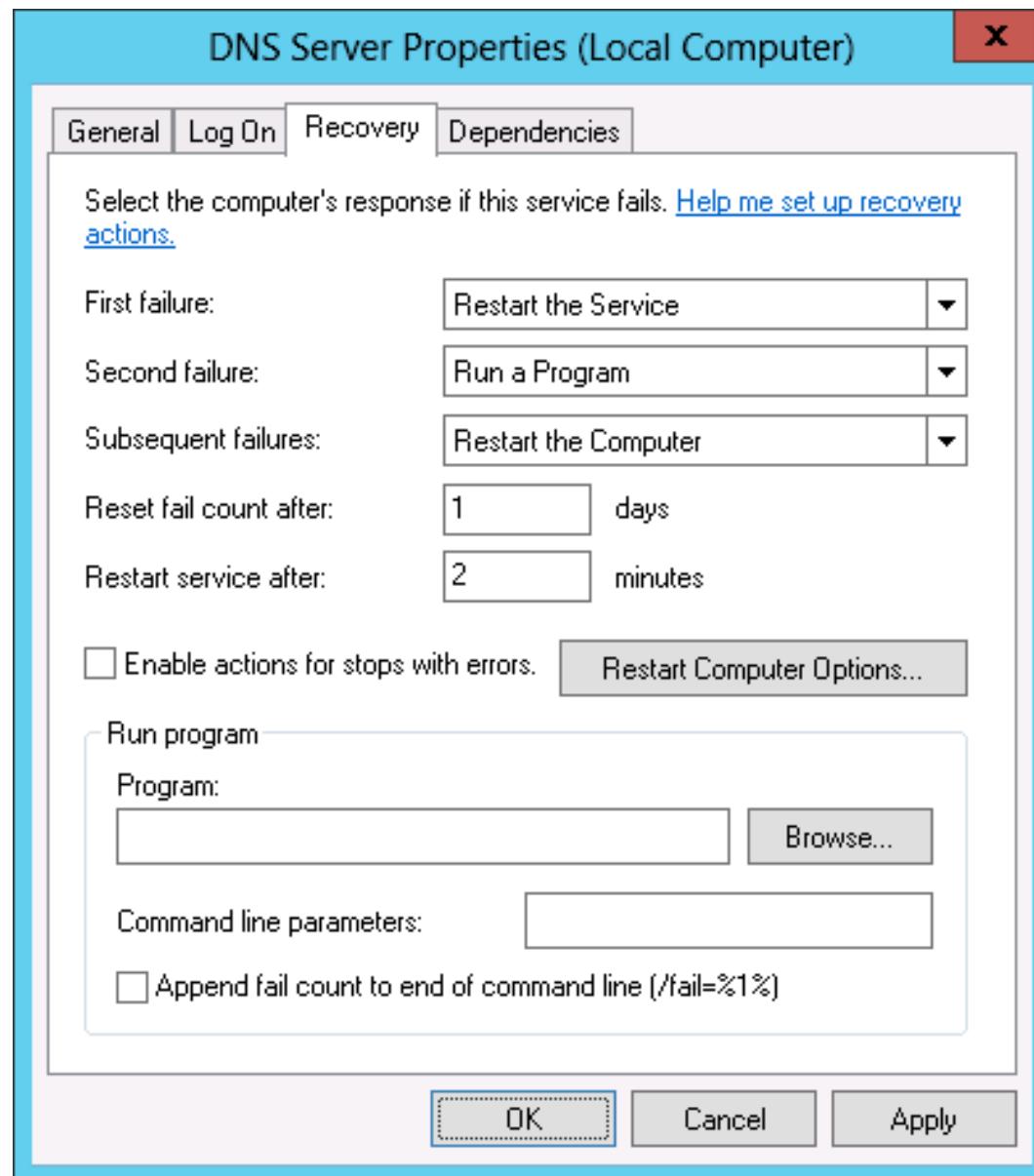
- Active Directory Administrative Center
- Active Directory Users and Computers
- DNS console
- Event Viewer
- Group Policy Management Console
- IIS Manager
- Performance Monitor
- Resource Monitor
- Task Scheduler
- Can be used to manage non-domain joined systems

Demonstration: Using Server Manager

In this demonstration, you will see how to:

- Add a feature by using the Add Roles and Features Wizard
- View role-related events
- Run the Best Practice Analyzer for a role
- List the tools available from Server Manager
- Restart Windows Server 2012

Configuring Services



Configuring Windows Remote Management

When deciding to use Remote Management, consider the following:

- You are more likely to manage a server remotely than by locally signing on
- With WinRM, you can use consoles, command-line utilities, or Windows PowerShell to perform remote management tasks
- With Remote Desktop, you can sign in to a server locally or from across the network

Demonstration: Performing Remote Management

In this demonstration, you will see how to:

- Use Server Manager to manage a remote server
- Add the DNS Server role on a remote server
- Connect to and configure a remote server by using RDP

Lesson 5: Introduction to Windows PowerShell

- What Is Windows PowerShell?
- Windows PowerShell Cmdlet Syntax
- Common Cmdlets for Server Administration
- Demonstration: Using Windows PowerShell
- What Is Windows PowerShell ISE?
- Demonstration: Using Windows PowerShell ISE
- Windows PowerShell Desired State Configuration

What Is Windows PowerShell?

Administrator: Windows PowerShell

Name	ModuleName
Set-BCAuthentication	BranchCache
Set-BCCache	BranchCache
Set-BCDataCacheEntryMaxAge	BranchCache
Set-BCMinSMBLatency	BranchCache
Set-BCSecretKey	BranchCache
Set-ClusteredScheduledTask	ScheduledTasks
Set-DAClientExperienceConfiguration	DirectAccessClientComponents
Set-DAEntryPointTableItem	DirectAccessClientComponents
Set-Disk	Storage
Set-DnsClient	DnsClient
Set-DnsClientGlobalSetting	DnsClient
Set-DnsClientNrptGlobal	DnsClient
Set-DnsClientNrptRule	DnsClient
Set-DnsClientServerAddress	DnsClient
Set-DtcAdvancedHostSetting	MsDtc
Set-DtcAdvancedSetting	MsDtc
Set-DtcClusterDefault	MsDtc
Set-DtcClusterTMMapping	MsDtc
Set-DtcDefault	MsDtc
Set-DtcLog	MsDtc
Set-DtcNetworkSetting	MsDtc
Set-DtcTransaction	MsDtc
Set-DtcTransactionsTraceSession	MsDtc
Set-DtcTransactionsTraceSetting	MsDtc
Set-InitiatorPort	Storage
Set-iSCSIChapSecret	iSCSI
Set-LogProperties	PSDiagnostics
Set-MMAgent	MMAgent
Set-NCNPOLICYConfiguration	NetworkConnectivityStatus
Set-Net6to4Configuration	NetworkTransition
Set-NetAdapter	NetAdapter
Set-NetAdapterAdvancedProperty	NetAdapter
Set-NetAdapterBinding	NetAdapter
Set-NetAdanterChecksumOffload	NetAdanter

Windows PowerShell Cmdlet Syntax

Windows PowerShell Cmdlet Syntax:

- Get-Help -Noun
NounName
- Get-Help -Verb
VerbName
- Help *CmdltName*
- Get-Command

Capability	Name
CIM	Set-BCAuthentication
CIM	Set-BCCache
CIM	Set-BCDataCacheEntryMaxAge
CIM	Set-BCMInSMBLatency
CIM	Set-BCSecretKey
CIM	Set-ClusteredScheduledTask
CIM	Set-DAClientExperienceConfiguration
CIM	Set-DAEntryPointTableItem
CIM	Set-Disk
CIM	Set-DnsClient
CIM	Set-DnsClientGlobalSetting
CIM	Set-DnsClientNrptGlobal
CIM	Set-DnsClientNrptRule
CIM	Set-DnsClientServerAddress
CIM	Set-DtcAdvancedHostSetting
CIM	Set-DtcAdvancedSetting
CIM	Set-DtcClusterDefault
CIM	Set-DtcClusterTMMapping
CIM	Set-DtcDefault
CIM	Set-DtcLog

Common Cmdlets for Server Administration

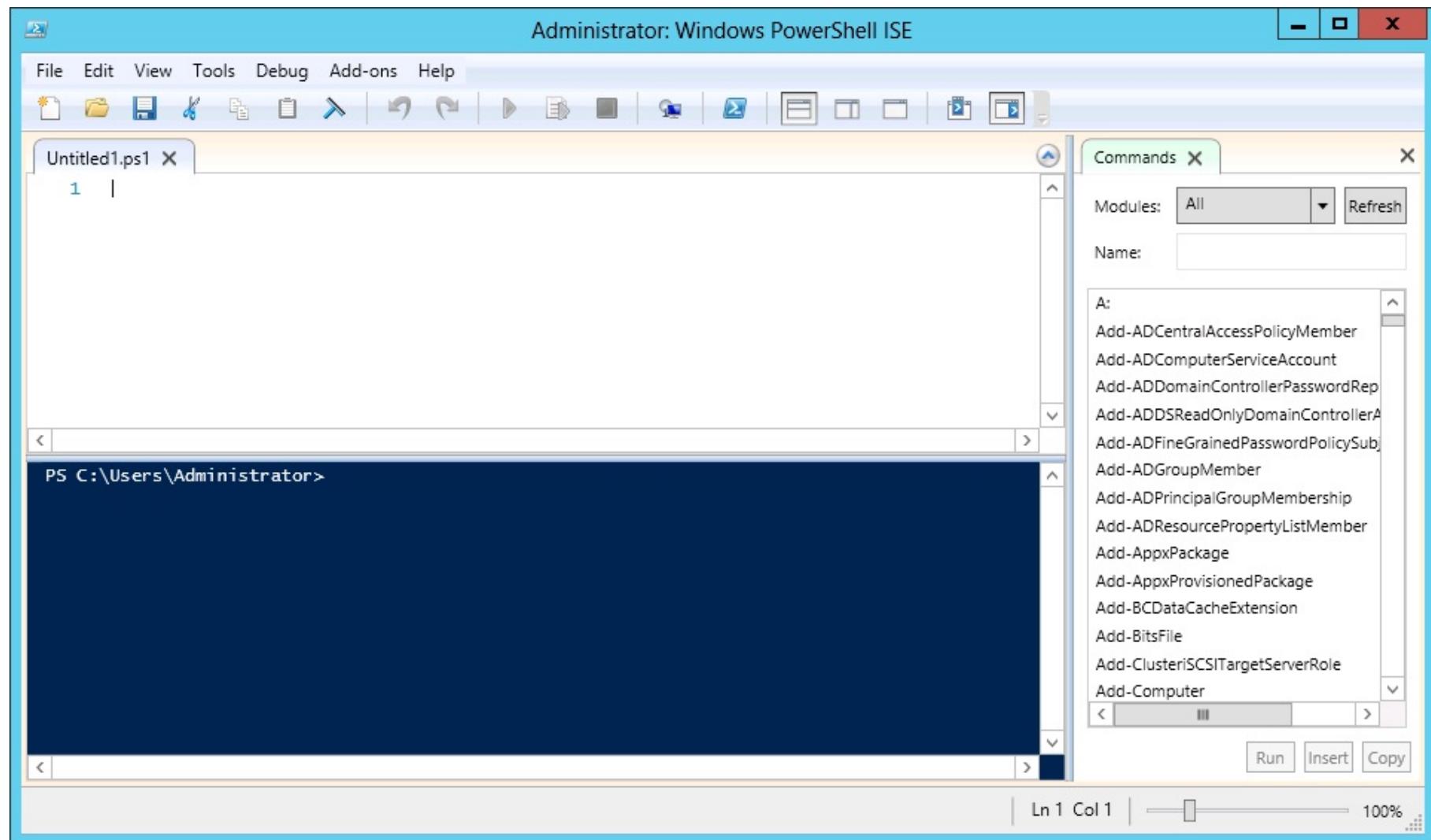
System Administration cmdlets	Details
Service Cmdlets	Use the Service noun
Event Log Cmdlets	Use the Eventlog noun
Process Cmdlets	Use the Process noun
ServerManager module	Allows the WindowsFeature noun
Windows PowerShell Remote Management	Allows cmdlets or scripts to be run on remote computers

Demonstration: Using Windows PowerShell

In this demonstration, you will see how to use Windows PowerShell to:

- Display the running services and processes on a server
- Connect to a remote computer to display all services and their current status
- Invoke commands to multiple computers and display running processes

What Is Windows PowerShell ISE?



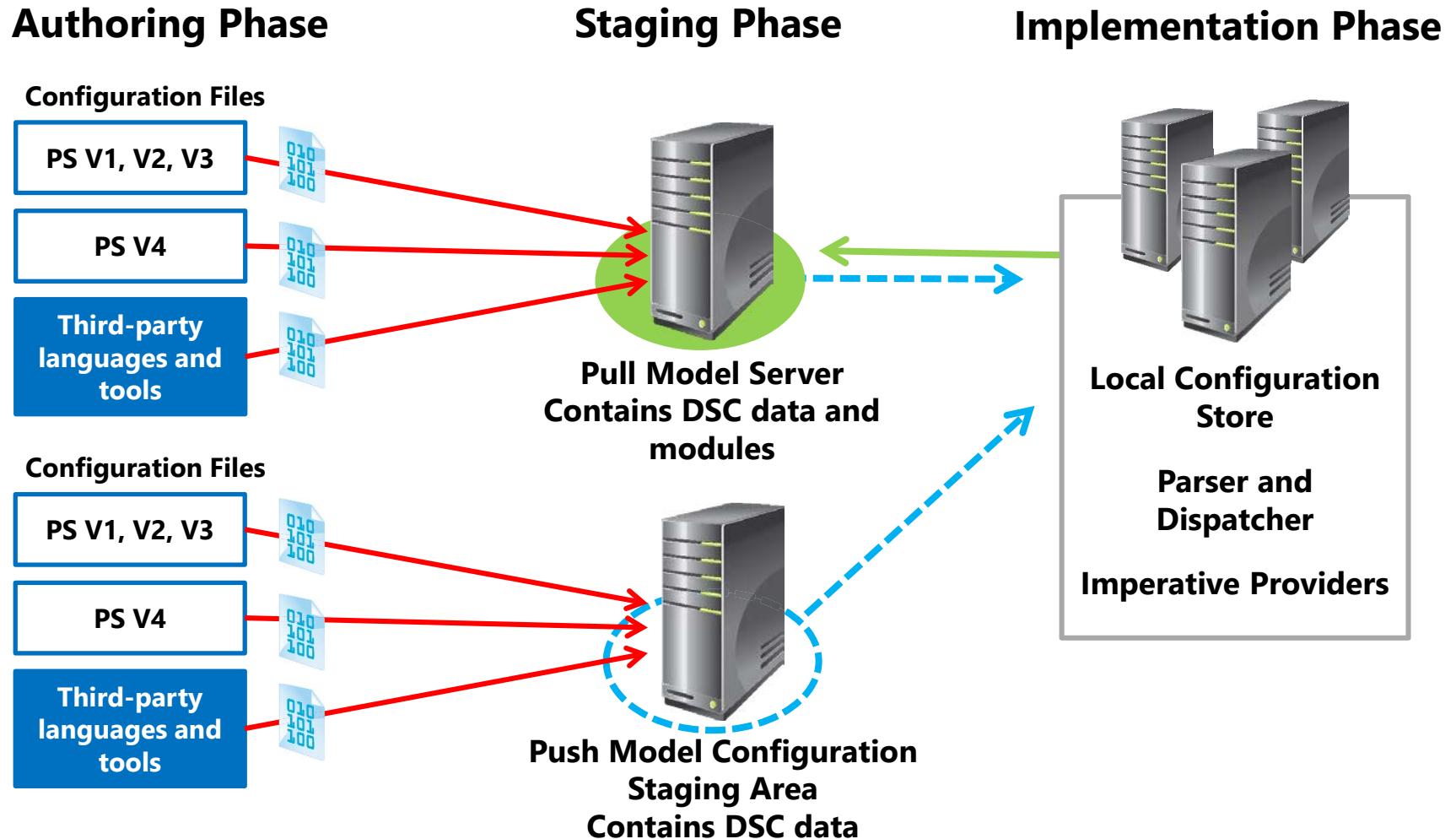
Demonstration: Using Windows PowerShell ISE

In this demonstration, you will see how to:

- Use Windows PowerShell ISE to import the ServerManager module
- View the cmdlets made available in the ServerManager module
- Use the **Get-WindowsFeature** cmdlet from Windows PowerShell ISE
- Run a Windows PowerShell script from the scripting pane to create a universal group named Helpdesk and add members

Windows PowerShell Desired State Configuration

Windows PowerShell DSC Push/Pull Model



Lab: Deploying and Managing Windows Server 2012

- Exercise 1: Deploying Windows Server 2012
- Exercise 2: Configuring Windows Server 2012 Server Core
- Exercise 3: Managing Servers
- Exercise 4: Using Windows PowerShell to Manage Servers

Logon Information

Virtual machines	20410D-LON-DC1 20410D-LON-SVR3 20410D-LON-CORE
User name	Adatum\Administrator
Password	Pa\$\$w0rd

Estimated Time: 75 minutes

Lab Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, England. A. Datum has recently deployed a Windows Server 2012 infrastructure with Windows 8.1 clients.

You have been working for A. Datum for several years as a desktop support specialist and have recently accepted a promotion to the server support team.

The marketing department has purchased a new web-based application. You need to install and configure the servers in the data center for this application. One server has a GUI interface, and the other server is configured as Server Core.

Lab Review

- What IP address range do the computers in the lab use?
- Why must you set the DNS server address prior to joining the domain?
- Besides sconfig.cmd, what other tool can you use to rename a computer running the Server Core operating system?

Module Review and Takeaways

- Review Questions
- Common Issues and Troubleshooting Tips
- Tools

Microsoft® Official Course



Module 2

Introduction to Active Directory Domain Services

Microsoft®

Module Overview

- Overview of AD DS
- Overview of Domain Controllers
- Installing a Domain Controller

Lesson 1: Overview of AD DS

- Overview of AD DS
- What Are AD DS Domains?
- What Are OUs?
- What Is an AD DS Forest?
- What Is the AD DS Schema?
- What Is New for Windows Server 2012 Active Directory?
- What Is New for Windows Server 2012 R2 Active Directory?

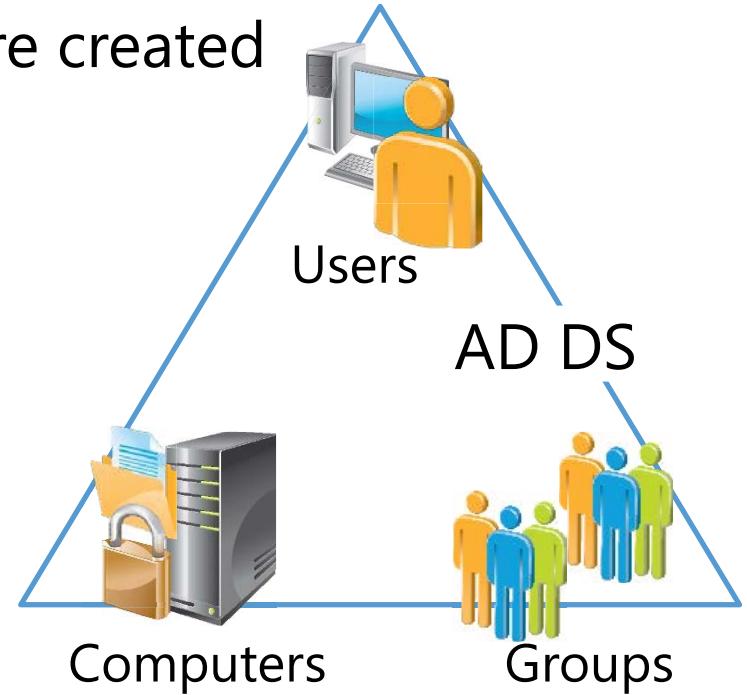
Overview of AD DS

AD DS is composed of both logical and physical components

Logical components	Physical components
<ul style="list-style-type: none">• Partitions• Schema• Domains• Domain trees• Forests• Sites• OUs• Containers	<ul style="list-style-type: none">• Domain controllers• Data stores• Global catalog servers• RODCs

What Are AD DS Domains?

- AD DS requires one or more domain controllers
- All domain controllers hold a copy of the domain database, which is continually synchronized
- The domain is the context within which user accounts, computer accounts, and groups are created
- The domain is a replication boundary
- The domain is an administrative center for configuring and managing objects
- Any domain controller can authenticate any sign-in anywhere in the domain
- The domain provides authorization

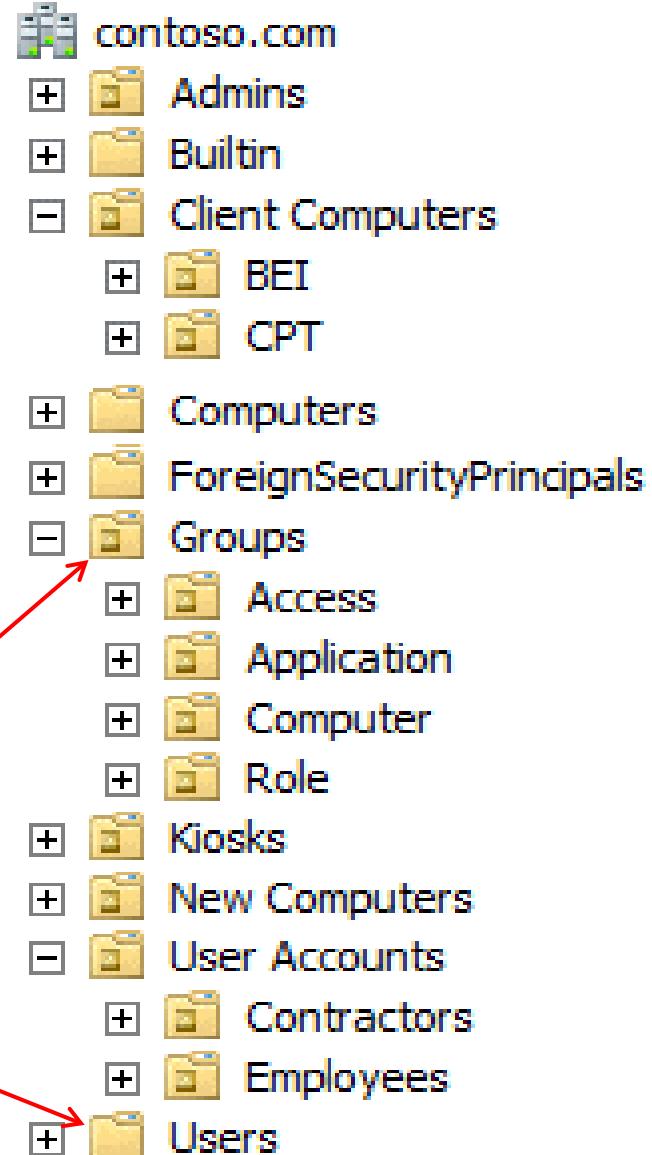


What Are OUs?

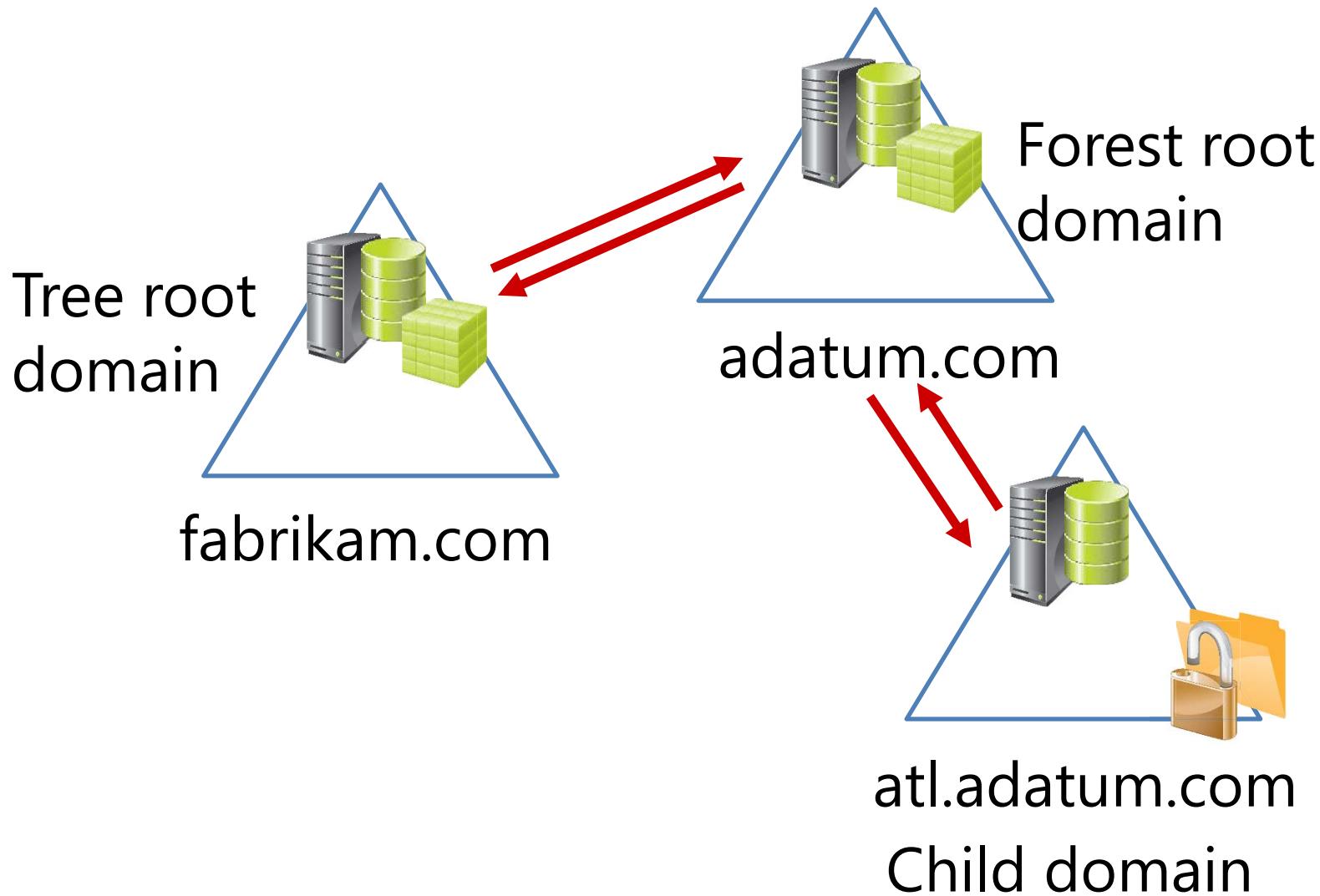
- Containers that can be used to group objects within a domain
- Create OUs to:
 - Configure objects by assigning GPOs
 - Delegate administrative permissions

OUs are represented by a folder with a book on it

Containers are represented by a blank folder

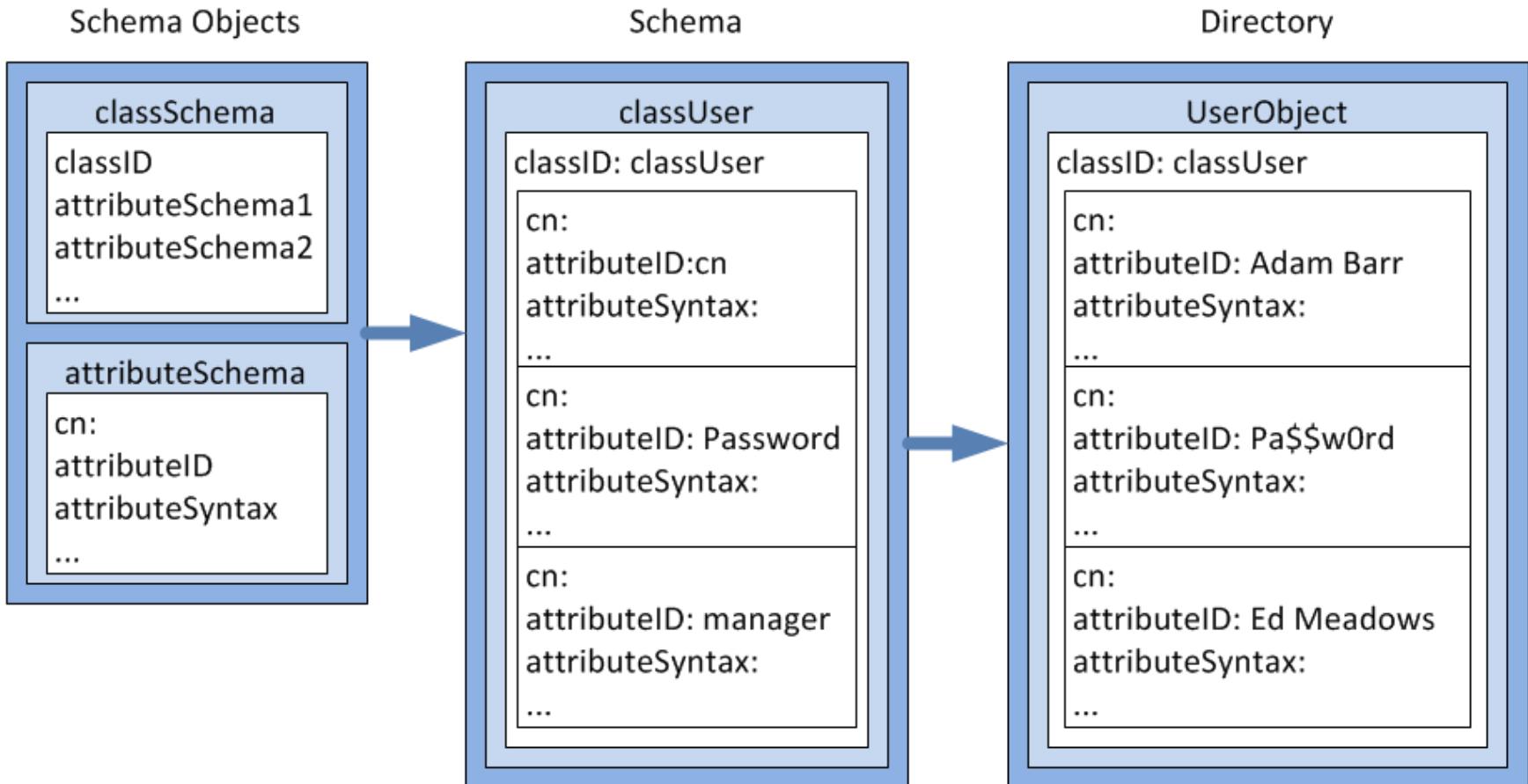


What Is an AD DS Forest?



What Is the AD DS Schema?

The schema defines the objects that can be stored in AD DS



What Is New for Windows Server 2012 Active Directory?

In Windows Server 2012 AD, it is easier to

- Detect events such as a snapshot rollback
- Install and configure cloned virtual machines
- Prepare the system before installing or upgrading domain controllers
- Use Windows PowerShell scripts to automate multiple AD DS installations
- Control who can access resources
- Recover objects from the Active Directory Recycle Bin
- Use and manage the RID pool
- Defer index creation

What Is New for Windows Server 2012 R2 Active Directory?

Improvements for using consumer devices
in the enterprise:

Workplace Join

- Allows consumer devices to participate in the domain

Web Application Proxy

- Allows applications to be published to the Internet

Multi-Factor Access Control

- Allows claims using different factors

Multi-Factor Authentication

- Allows you to specify the use of multiple factors for authentication

Lesson 2: Overview of Domain Controllers

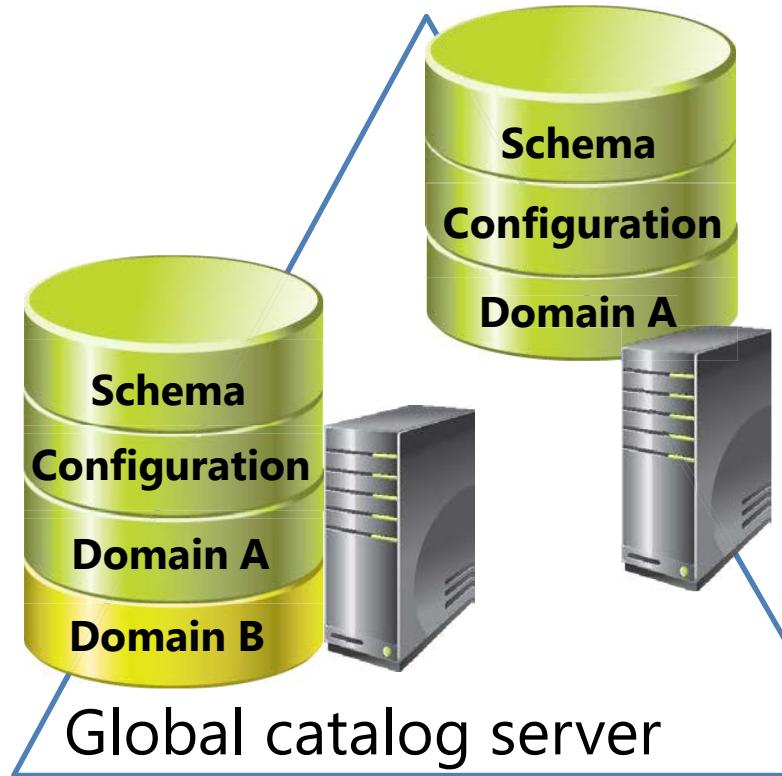
- What Is a Domain Controller?
- What Is the Global Catalog?
- The AD DS Sign-in Process
- Demonstration: Viewing the SRV Records in DNS
- What Are Operations Masters?

What Is a Domain Controller?

Domain controllers

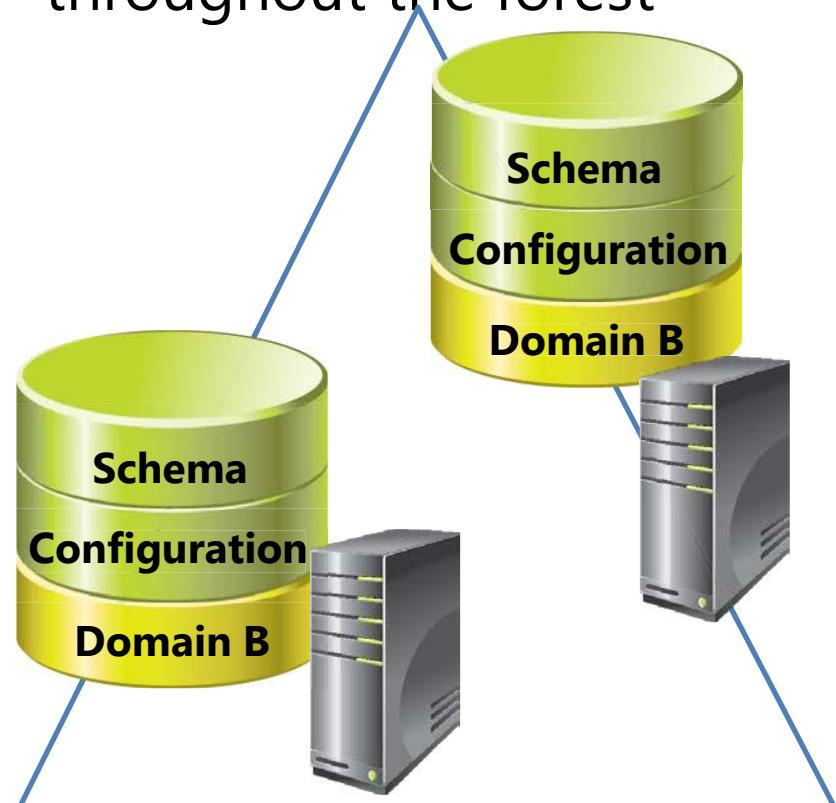
- Servers that host the AD DS database (Ntds.dit) and SYSVOL
- Kerberos authentication service and KDC services perform authentication
- Best practices:
 - Availability:
At least two domain controllers in a domain
 - Security:
RODC and BitLocker

What Is the Global Catalog?



The global catalog:

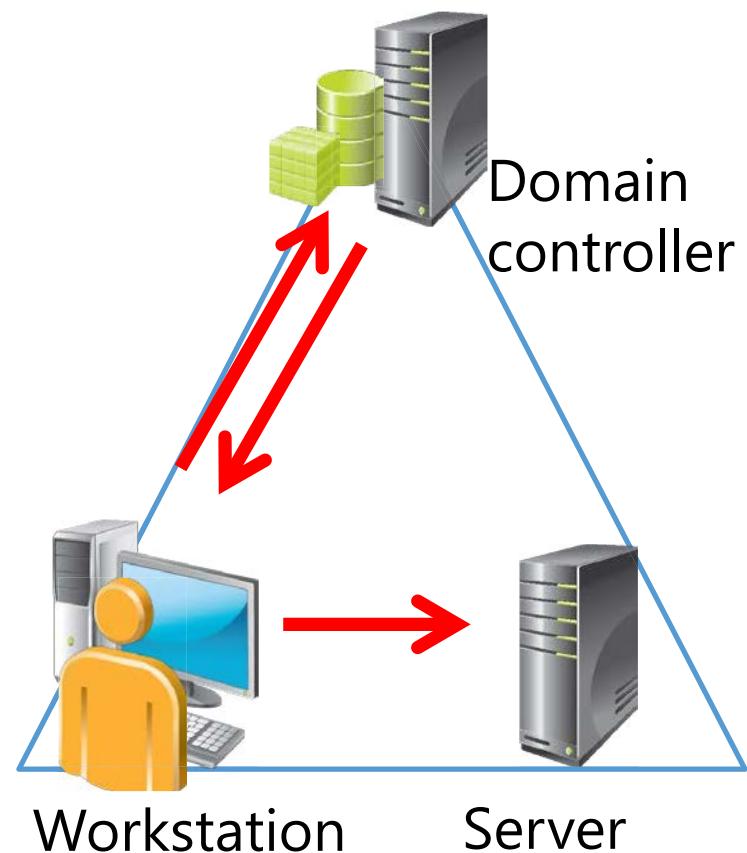
- Hosts a partial attribute set for other domains in the forest
- Supports queries for objects throughout the forest



The AD DS Sign-in Process

The AD DS sign-in process:

1. The user account is authenticated to the domain controller.
2. The domain controller returns a TGT back to client.
3. The client uses TGT to apply for access to the workstation.
4. The domain controller grants access to the workstation.
5. The client uses TGT to apply for access to the server.
6. The domain controller returns access to the server.



Demonstration: Viewing the SRV Records in DNS

In this demonstration, you will see how to use DNS Manager to view SRV records

What Are Operations Masters?

In the multi-master replication model, some operations must be single master

Many terms are used for single master operations in AD DS, including:

- Operations master (or operations master roles)
- Single master roles
- Flexible single master operations (FSMOs)

The five FSMOs are:

- | | |
|---|---|
| <ul style="list-style-type: none">• Forest:<ul style="list-style-type: none">• Domain naming master• Schema master | <ul style="list-style-type: none">• Domain:<ul style="list-style-type: none">• RID master• Infrastructure master• PDC Emulator master |
|---|---|

Lesson 3: Installing a Domain Controller

- Installing a Domain Controller from Server Manager
- Installing a Domain Controller on a Server Core Installation of Windows Server 2012
- Upgrading a Domain Controller
- Installing a Domain Controller by Using Install from Media
- What Is Windows Azure Active Directory?
- Deploying Domain Controllers in Windows Azure

Installing a Domain Controller from Server Manager

Deployment Configuration section of the Active Directory Domain Services Configuration Wizard

Select the deployment operation

- Add a domain controller to an existing domain
- Add a new domain to an existing forest
- Add a new forest

Specify the domain information for this operation

Domain:

*

Select...

Supply the credentials to perform this operation

<No credentials provided>

Change...

Installing a Domain Controller on a Server Core Installation of Windows Server 2012

Installing AD DS is a two-step process regardless of which installation method you use

- Method 1, use Server Manager on a Windows 2012 server with a GUI interface to connect to the system
 1. Install the files by installing the Active Directory Domain Services role
 2. Install the domain controller role by running the Active Directory Domain Services Configuration Wizard
- Method 2, Use Windows PowerShell locally, or remotely using WinRM
 1. Install the files by running the command **Install-WindowsFeature AD-Domain-Services**
 2. Install the domain controller role by running the command **Install-ADDSDomainController**

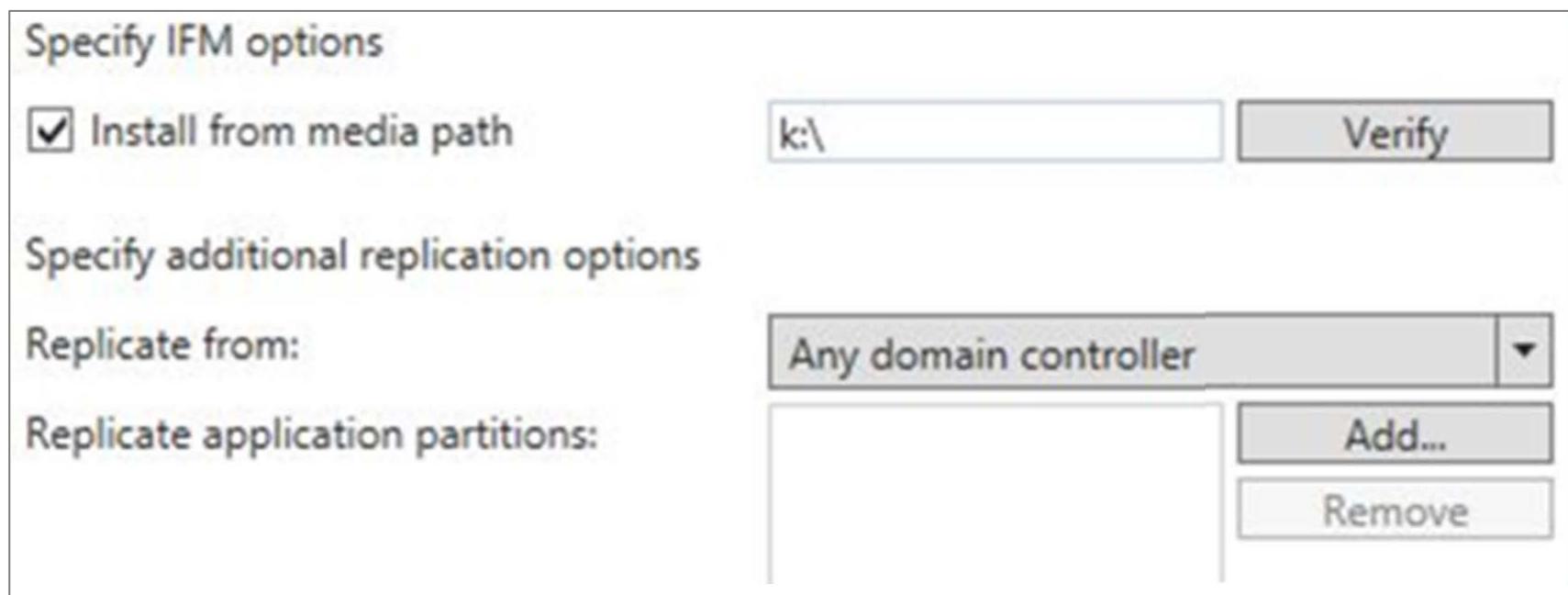
Upgrading a Domain Controller

Options to upgrade AD DS to Windows Server 2012:

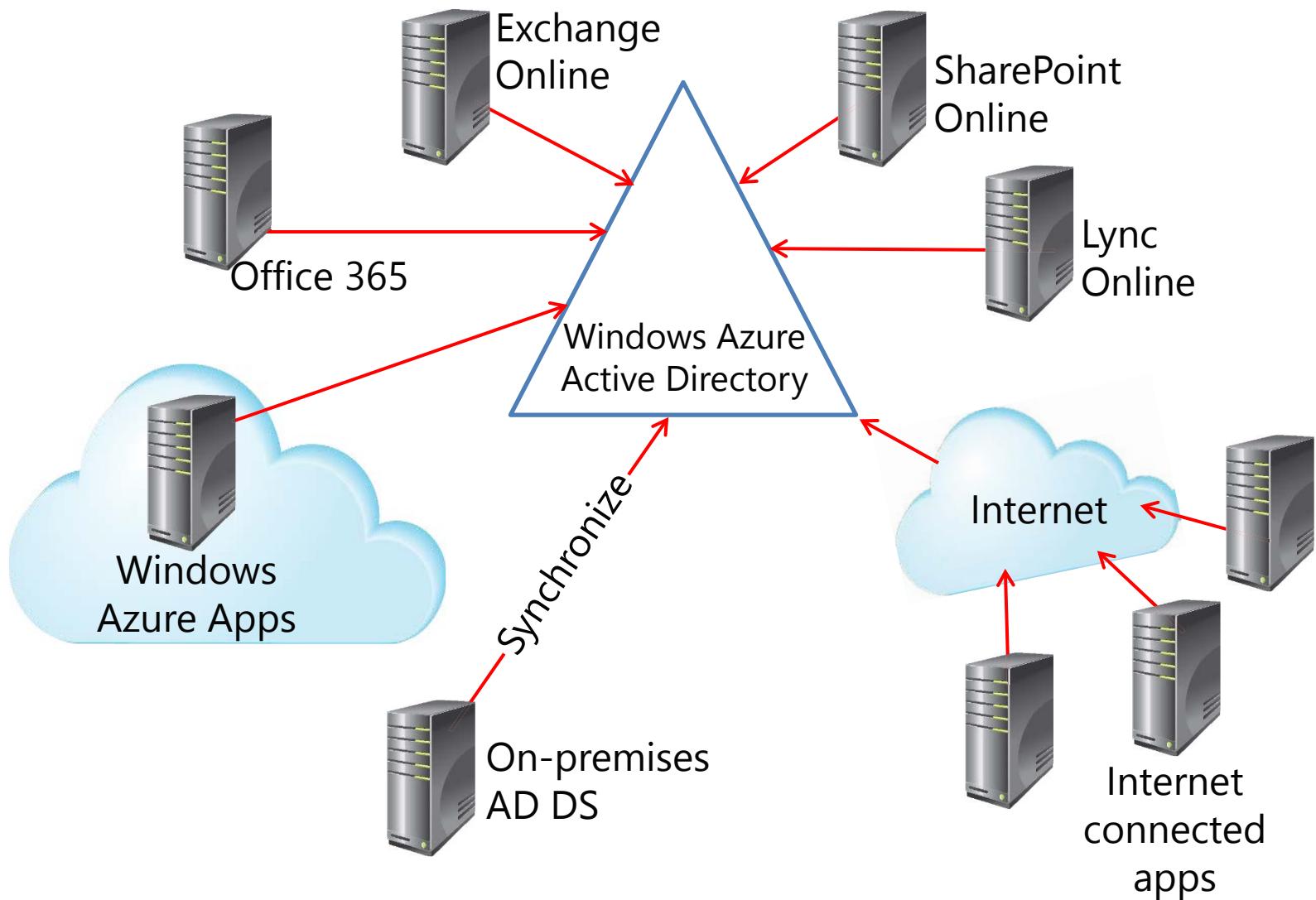
- In-place upgrade from Windows Server 2008 to Windows Server 2012
 - ✓ Benefit: Except for the prerequisite checks, all the files and programs stay in place and there is no additional work required
 - ✗ Risk: May leave legacy files and DLLs
- Introduce a new Windows Server 2012 server into the domain and promote it to be a domain controller
 - This option is usually preferable
 - ✓ Benefit: The new server has no accumulated legacy files and settings
 - ✗ Risk: May need additional work to migrate administrators' files and settings

Installing a Domain Controller by Using Install from Media

Install from Media section on the Additional Options page of the Active Directory Domain Services Configuration Wizard



What Is Windows Azure Active Directory?



Deploying Domain Controllers in Windows Azure

- Windows Server 2012 is cloud-ready and virtualization safe
- Considerations for deploying in Windows Azure include:
 - Rollback
 - Resource limitations
- Virtualization considerations for deploying AD DS
 - Time synchronization
 - Single point of failure

Lab: Installing Domain Controllers

- Exercise 1: Installing a Domain Controller
- Exercise 2: Installing a Domain Controller by Using IFM

Logon Information

Virtual machines	20410D-LON-DC1 20410D-LON-SVR1 20410D-LON-RTR 20410D-LON-SVR2
User name	Adatum\Administrator
Password	Pa\$\$w0rd

Estimated Time: 50 minutes

Lab Scenario

Your manager has asked you to install a new domain controller in the datacenter to improve sign-in performance and to create a new domain controller for a branch office by using IFM

Lab Review

- Why did you use Server Manager and not **dcpromo** when you promoted a server to be a domain controller?
- What are the three operations masters found in each domain?
- What are the two operations masters that are present in a forest?
- What is the benefit of performing an IFM install of a domain controller?

Module Review and Takeaways

- Review Questions

Microsoft® Official Course



Module 3

Managing Active Directory Domain Services Objects

Microsoft®

Module Overview

- Managing User Accounts
- Managing Groups
- Managing Computer Accounts
- Delegating Administration

Lesson 1: Managing User Accounts

- AD DS Administration Tools
- Creating User Accounts
- Configuring User Account Attributes
- Creating User Profiles
- Demonstration: Managing User Accounts
- Demonstration: Using Templates to Manage User Accounts

AD DS Administration Tools

To manage AD DS objects, you can use the following graphical tools:

- Active Directory Administration snap-ins
- Active Directory Administrative Center



You can also use the following command-line tools:

- Active Directory module in Windows PowerShell
- Directory Service commands



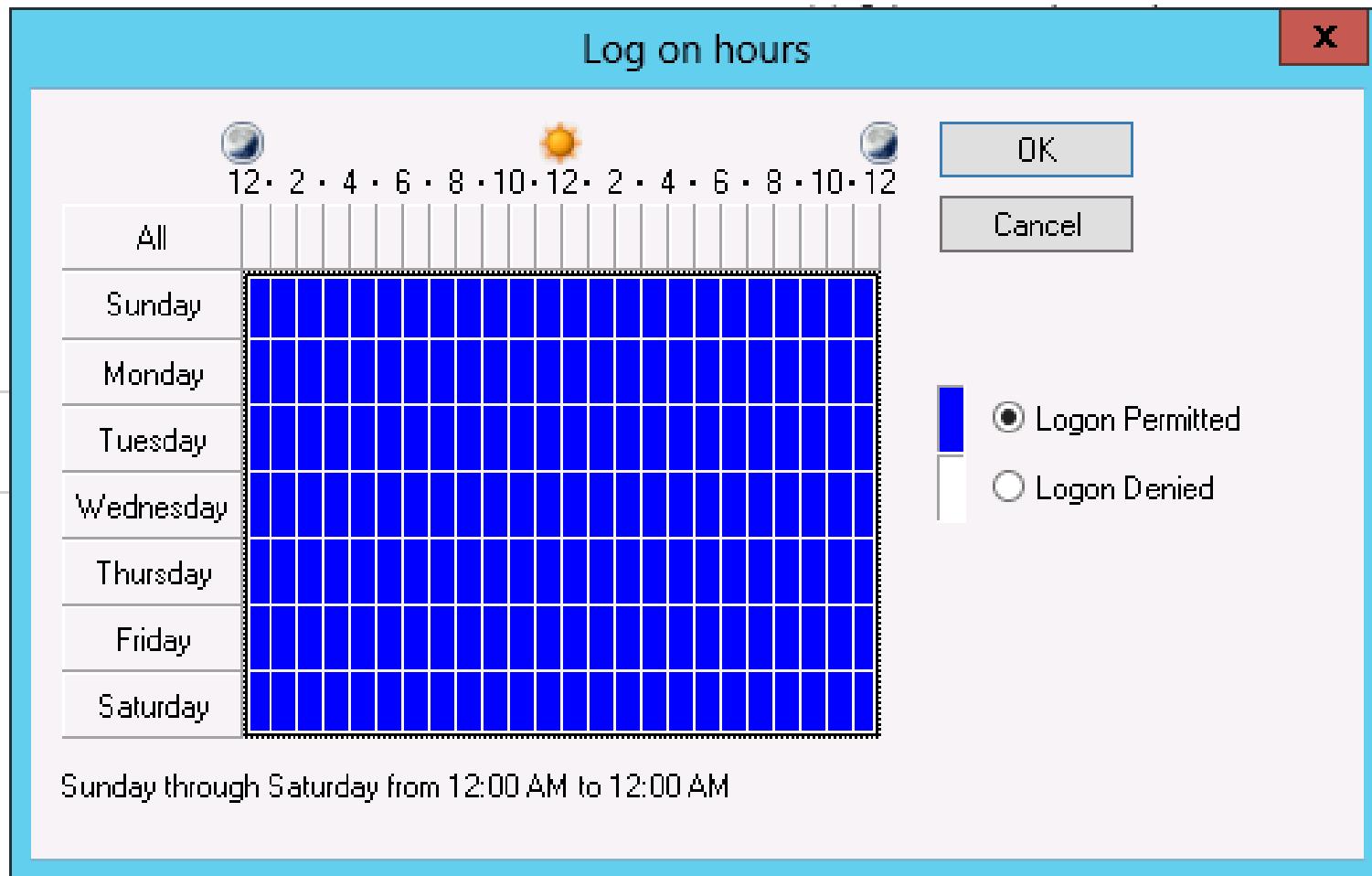
Creating User Accounts

The Account section of the Active Directory Administrative Center Create User window

First name:	<input type="text"/>	Account expires:	<input checked="" type="radio"/> Never <input type="radio"/> End of <input type="text"/>
Middle initials:	<input type="text"/>	▲	
Last name:	<input type="text"/>	▼	
Full name:	<input type="text"/> *	Password options:	<input checked="" type="radio"/> User must change password at next log on <input type="radio"/> Other password options
User UPN logon:	<input type="text"/> @ <input type="text"/>	<input type="checkbox"/> Smart card is required for interactive log on	<input type="checkbox"/> Password never expires
User SamAccount...	<input type="text"/> Adatum *	<input type="checkbox"/> User cannot change password	▼
Password:	<input type="text"/>	Encryption options:	▼
Confirm password:	<input type="text"/>	Other options:	
Create in:	OU=Managers,DC=Adatum,DC=com	▼	
Change...			
<input type="checkbox"/> Protect from accidental deletion			
Log on hours...		Log on to...	

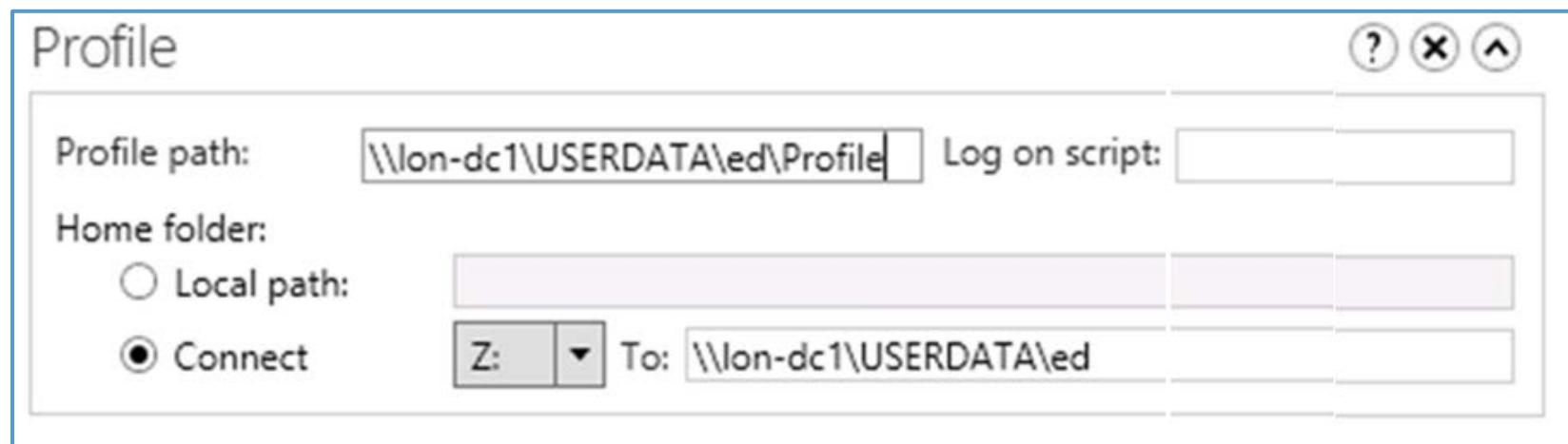
Configuring User Account Attributes

The Log on hours dialog box



Creating User Profiles

The Profile section of the User Properties window



Demonstration: Managing User Accounts

In this demonstration, you will see how to:

- Use the Active Directory Administrative Center to manage user accounts
 - Delete a user account
 - Create a new user account
 - Move the user account
 - View the WINDOWS POWERSHELL HISTORY
- Use Windows PowerShell to manage user accounts
 - Find inactive user accounts
 - Find disabled user accounts
 - Delete disabled user accounts

Demonstration: Using Templates to Manage User Accounts

In this demonstration, you will see how to:

- Create a user template account
- Use Windows PowerShell to create a user from the user template
- Verify the properties of the new user account

Lesson 2: Managing Groups

- Group Types
- Group Scopes
- Implementing Group Management
- Default Groups
- Special Identities
- Demonstration: Managing Groups

Group Types

- Distribution groups
 - Used only with email applications
 - Not security-enabled (no SID); cannot be given permissions



- Security groups
 - Security principal with a SID; can be given permissions
 - Can also be email-enabled



Both security groups and distribution groups can be converted to the other type of group

Group Scopes

Group scope	Members from same domain	Members from domain in same forest	Members from trusted external domain	Can be assigned permissions to resources
Local	U, C, GG, DLG, UG and local users	U, C, GG, UG	U, C, GG	On the local computer only
Domain-local	U, C, GG, DLG, UG	U, C, GG, UG	U, C, GG	Anywhere in the domain
Universal	U, C, GG, UG	U, C, GG, UG	N/A	Anywhere in the forest
Global	U, C, GG	N/A	N/A	Anywhere in the domain or a trusted domain

U
C
GG

User
Computer
Global group

DLG
UG

Domain-local group
Universal group

Implementing Group Management

I Identities

Users or computers,
which are members of

G Global groups

Which collect members
based on members' roles,
which are members of

DL Domain-local groups

Which provide management
such as resource access,
which are

A Assigned access to a resource

This best practice for nesting
groups is known as IGDLA.



Implementing Group Management

I Identities

Users or computers,
which are members of



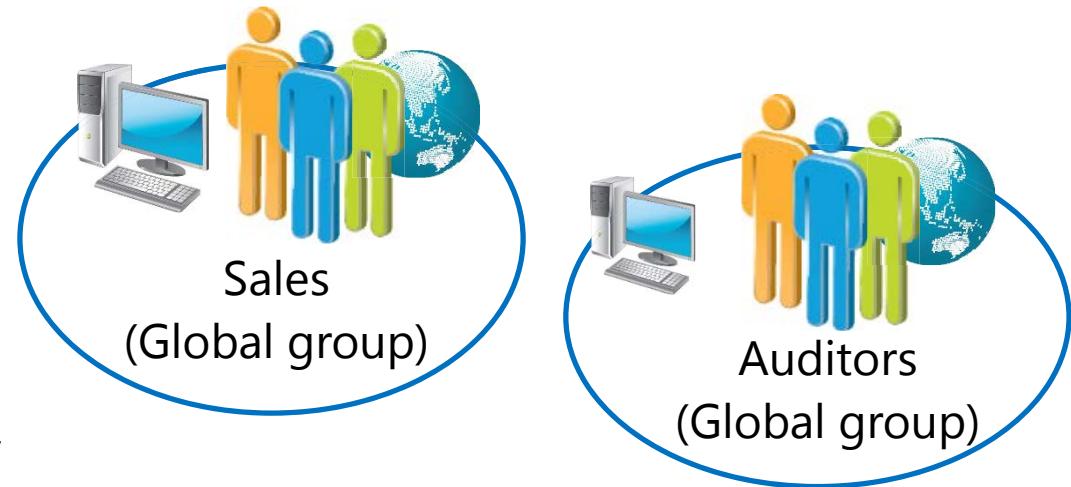
Implementing Group Management

I Identities

Users or computers,
which are members of

G Global groups

Which collect members
based on members' roles,
which are members of



Implementing Group Management

I Identities

Users or computers,
which are members of

G Global groups

Which collect members
based on members' roles,
which are members of

DL Domain-local groups

Which provide management
such as resource access,
which are



Implementing Group Management

I Identities

Users or computers,
which are members of

G Global groups

Which collect members
based on members' roles,
which are members of

DL Domain-local groups

Which provide management
such as resource access,
which are

A Assigned access to a resource



Implementing Group Management

I Identities

Users or computers,
which are members of

G Global groups

Which collect members
based on members' roles,
which are members of

DL Domain-local groups

Which provide management
such as resource access,
which are

A Assigned access to a resource

This best practice for nesting
groups is known as IGDLA



Default Groups

- Carefully manage the default groups that provide administrative privileges, because these groups:
 - Typically have broader privileges than are necessary for most delegated environments
 - Often apply protection to their members

Group	Location
Enterprise Admins	Users container of the forest root domain
Schema Admins	Users container of the forest root domain
Administrators	Built-in container of each domain
Domain Admins	Users container of each domain
Server Operators	Built-in container of each domain
Account Operators	Built-in container of each domain
Backup Operators	Built-in container of each domain
Print Operators	Built-in container of each domain
Cert Publishers	Users container of each domain

Special Identities

- Special identities:
 - Are groups for which membership is controlled by the operating system
 - Can be used by the Windows Server operating system to provide access to resources:
 - Based on the type of authentication or connection
 - Not based on the user account
- Important special identities include:
 - Anonymous Logon
 - Authenticated Users
 - Everyone
 - Interactive
 - Network
 - Creator Owner

Demonstration: Managing Groups

In this demonstration, you will see how to:

- Create a new group
- Add members to the group
- Add a user to the group
- Change the group type and scope
- Modifying the group's Managed By property

Lesson 3: Managing Computer Accounts

- What Is the Computers Container?
- Specifying the Location of Computer Accounts
- Controlling Permissions to Create Computer Accounts
- Performing an Offline Domain Join
- Computer Accounts and Secure Channels
- Resetting the Secure Channel
- Bring Your Own Device

What Is the Computers Container?

Active Directory Administrative Center, opened to the
Adatum (local)\Computers container

Distinguished Name is cn=Computers,DC=Adatum,DC=com

The screenshot shows the Active Directory Administrative Center interface. The title bar indicates the current location is Adatum (local) \ Computers. The left sidebar has a navigation tree with Active Directory..., Overview, Adatum (local) (which is selected and highlighted in blue), Computers, IT, Managers, Dynamic Access Control, and Global Search. The main pane displays a table titled "Computers (6)" with columns for Name, Type, and Description. The table lists six computer objects: LON-CL1, LON-CL2, LON-RTR, LON-SVR1, LON-SVR2, and LON-SVR4, all categorized as Computer type.

	Name	Type	Description
1	LON-CL1	Computer	
2	LON-CL2	Computer	
3	LON-RTR	Computer	
4	LON-SVR1	Computer	
5	LON-SVR2	Computer	
6	LON-SVR4	Computer	

Specifying the Location of Computer Accounts

- Best practice is to create OUs for computer objects
 - Servers
 - Typically subdivided by server role
 - Client computers
 - Typically subdivided by region
 - Divide OUs:
 - By administration
 - To facilitate configuration with Group Policy
-
- ```
graph TD; Clients["Clients"] --> BOS["BOS"]; Clients --> CHI["CHI"]; Clients --> CPT["CPT"]; BOS --> DesktopsB["Desktops"]; BOS --> LaptopsB["Laptops"]; CHI --> DesktopsC["Desktops"]; CHI --> LaptopsC["Laptops"]; CPT --> DesktopsCPT["Desktops"]; CPT --> LaptopsCPT["Laptops"];
```

# Controlling Permissions to Create Computer Accounts

The Delegation of Control Wizard window  
The administrator is creating a custom delegation for computer objects



# Performing an Offline Domain Join

Offline domain join is used to join computers to a domain when they cannot contact a domain controller

- Create a domain join file using:

```
domain.exe /Provision /Domain <DomainName>
/Machine <MachineName> /SaveFile <filepath>
```

- Import the domain join file using:

```
domain.exe /request ODJ /LoadFile <filepath>
/WindowsPath <path to the Windows directory of
the offline image>
```

# Computer Accounts and Secure Channels

- Computers have accounts
  - sAMAccountName and password
  - Used to create a secure channel between the computer and a domain controller
- Scenarios in which a secure channel can be broken
  - Reinstalling a computer, even with same name, generates a new SID and password
  - Restoring a computer from an old backup, or rolling back a computer to an old snapshot
  - Computer and domain disagree about what the password is

# Resetting the Secure Channel

- Do not delete a computer from the domain and then rejoin it
  - This creates a new account, resulting in a new SID and lost group memberships
- Options for resetting the secure channel
  - Active Directory Users and Computers
  - Active Directory Administrative Center
  - **dsmod**
  - **netdom**
  - **nltest**
  - Windows PowerShell

# Bring Your Own Device

AD FS has been enhanced to support BYOD programs

- Workplace Join creates an AD DS object for consumer devices

Limit content access to specific devices

- Using Dynamic Access Control or conditions on permissions you can limit content access to domain-joined devices

Support for iOS

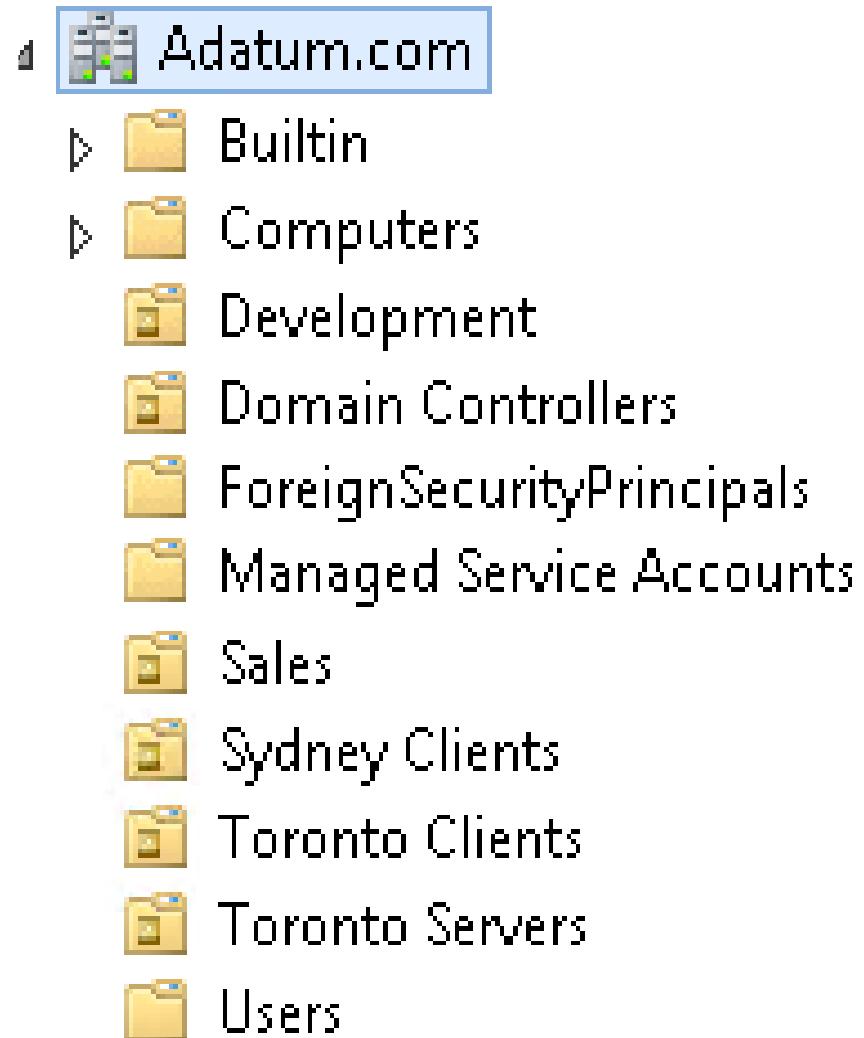
- iOS devices can be workplace-joined as well

# Lesson 4: Delegating Administration

- Considerations for Using Organizational Units
- AD DS Permissions
- Effective AD DS Permissions
- Demonstration: Delegating Administrative Permissions

# Considerations for Using Organizational Units

- OUs allow you to subdivide the domain for management purposes
- OUs are used for:
  - Delegation of control
  - Application of GPOs
- The OU structure can be:
  - Flat, one to two levels deep
  - Deep, more than 5 levels deep
  - Narrow, anything in between



# AD DS Permissions

## Advanced Security Settings for IT

Owner: Domain Admins (ADATUM\Domain Admins) [Change](#)

Permissions [Auditing](#) [Effective Access](#)

For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available).

Permission entries:

| Type  | Principal                     | Access                     | Inherited from | Applies to       |
|-------|-------------------------------|----------------------------|----------------|------------------|
| Deny  | Everyone                      | Special                    | None           | This object only |
| Allow | Account Operators (ADATU...)  | Create/delete InetOrg...   | None           | This object only |
| Allow | Account Operators (ADATU...)  | Create/delete Comput...    | None           | This object only |
| Allow | Account Operators (ADATU...)  | Create/delete Group o...   | None           | This object only |
| Allow | Print Operators (ADATUM\Pr... | Create/delete Printer o... | None           | This object only |
| Allow | Account Operators (ADATU...)  | Create/delete User obj...  | None           | This object only |
| Allow | Domain Admins (ADATUM\...)    | Full control               | None           | This object only |
| Allow | ENTERPRISE DOMAIN CONT...     | Special                    | None           | This object only |
| Allow | Authenticated Users           | Special                    | None           | This object only |
| Allow | SYSTEM                        | Full control               | None           | This object only |

Add

Remove

View

Restore defaults

Disable inheritance

# Effective AD DS Permissions

Permissions assigned to users and groups accumulate

Best practice is to assign permissions to groups, not to individual users

In the event of conflicts:

- Deny permissions override Allow permissions
- Explicit permissions override Inherited permissions
  - Explicit Allow overrides Inherited Deny

To evaluate effective permissions, you can use:

- The Effective Access tab
- Manual analysis

# Demonstration: Delegating Administrative Permissions

In this demonstration, you will see how to:

- Create an OU
- Move objects into an OU
- Delegate a standard task
- Delegate a custom task
- View AD DS permissions resulting from these delegations

# Lab: Managing Active Directory Domain Services Objects

- Exercise 1: Delegating Administration for a Branch Office
- Exercise 2: Creating and Configuring User Accounts in AD DS
- Exercise 3: Managing Computer Objects in AD DS

## Logon Information

|                  |                                                |
|------------------|------------------------------------------------|
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-CL1</b> |
| User name        | <b>Adatum\Administrator</b>                    |
| Password         | <b>Pa\$\$w0rd</b>                              |

**Estimated Time: 70 minutes**

# Lab Scenario

You have been working for A. Datum Corporation as a desktop support specialist and have visited desktop computers to troubleshoot app and network problems. You have recently accepted a promotion to the server support team. One of your first assignments is to configure the infrastructure service for a new branch office.

To begin deployment of the new branch office, you are preparing AD DS objects. As part of this preparation, you need to create an OU for the branch office and delegate permission to manage it. Then you need to create users and groups for the new branch office. Finally, you need to reset the secure channel for a computer account that has lost connectivity to the domain in the branch office.

# Lab Review

- What are the options for modifying the attributes of new and existing users?
- What types of objects can be members of global groups?
- What types of objects can be members of domain-local groups?
- Which two credentials are necessary for any computer to join a domain?

# Module Review and Takeaways

- Review Questions
- Best Practices
- Tools

# Microsoft® Official Course



## Module 4

### Automating Active Directory Domain Services Administration

**Microsoft®**

# Module Overview

- Using Command-line Tools for AD DS Administration
- Using Windows PowerShell for AD DS Administration
- Performing Bulk Operations with Windows PowerShell

# Lesson 1: Using Command-line Tools for AD DS Administration

- Benefits of Using Command-Line Tools for AD DS Administration
- What Is Csvde?
- What Is Ldifde?
- What Are DS Commands?

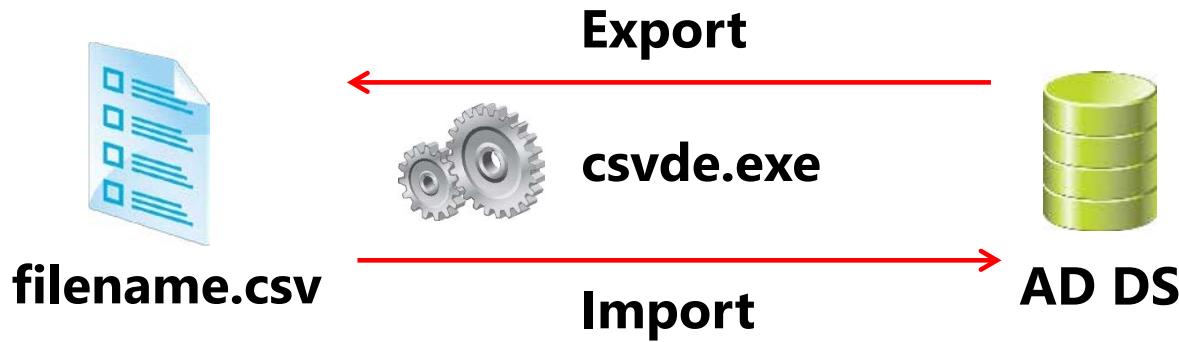
# Benefits of Using Command-Line Tools for AD DS Administration

Command-line tools allow you to automate AD DS administration

Benefits of using command-line tools:

- Faster implementation of bulk operations
- Customized processes for AD DS administration
- AD DS administration on server core

# What Is Csvde?



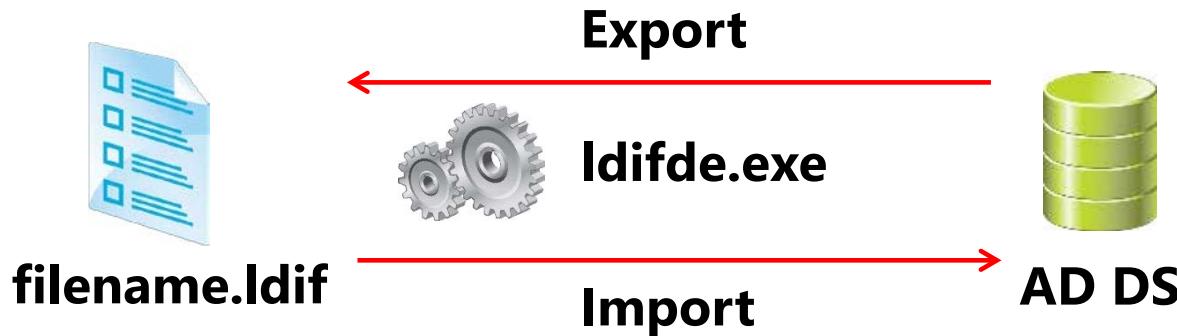
Use csvde to export objects to a .csv file:

- -f filename
- -d RootDN
- -p SearchScope
- -r Filter
- -l ListOfAttributes

Use csvde to create objects from a .csv file:

```
csvde -i -f filename -k
```

# What Is Ldifde?



Use **ldifde** to export objects to a LDIF file:

- -f filename
- -d RootDN
- -r Filter
- -p SearchScope
- -I ListOfAttributesToInclude
- -o ListOfAttributesToExclude

Use **ldifde** to create, modify, or delete objects:

```
ldifde -i -f filename -k
```

# What Are DS Commands?

Windows Server 2012 includes **ds\*** commands that are suitable for use in scripts

- Examples
  - To modify the department of a user account, type:

```
Dsmod user "cn=Joe Healy, ou=Managers,
dc=adatum dc=com" -dept IT
```

- To display the email of a user account, type:

```
Dsget user "cn=Joe Healy, ou=Managers,
dc=adatum dc=com" -email
```

- To delete a user account, type:

```
Dsrm "cn=Joe Healy, ou=Managers, dc=adatum dc=com"
```

- To create a new user account, type:

```
Dsadd user "cn=Joe Healy, ou=Managers, dc=adatum dc=com"
```

## Lesson 2: Using Windows PowerShell for AD DS Administration

- Using Windows PowerShell Cmdlets to Manage User Accounts
- Using Windows PowerShell Cmdlets to Manage Groups
- Using Windows PowerShell Cmdlets to Manage Computer Accounts
- Using Windows PowerShell Cmdlets to Manage OUs

# Using Windows PowerShell Cmdlets to Manage User Accounts

| Cmdlet                  | Description                                                                               |
|-------------------------|-------------------------------------------------------------------------------------------|
| New-ADUser              | Creates user accounts                                                                     |
| Set-ADUser              | Modifies properties of user accounts                                                      |
| Remove-ADUser           | Deletes user accounts                                                                     |
| Set-ADAccountPassword   | Resets the password of a user account                                                     |
| Set-ADAccountExpiration | Modifies the expiration date of a user account                                            |
| Unlock-ADAccount        | Unlocks a user account after it has become locked after too many incorrect login attempts |
| Enable-ADAccount        | Enables a user account                                                                    |
| Disable-ADAccount       | Disables a user account                                                                   |

```
New-ADUser "Steven Faerch" -Account Password (Read-Host
-AsSecureString "Enter password") -Department IT
```

# Using Windows PowerShell Cmdlets to Manage Groups

| Cmdlet                            | Description                             |
|-----------------------------------|-----------------------------------------|
| New-ADGroup                       | Creates new groups                      |
| Set-ADGroup                       | Modifies properties of groups           |
| Get-ADGroup                       | Displays properties of groups           |
| Remove-ADGroup                    | Deletes groups                          |
| Add-ADGroupMember                 | Adds members to groups                  |
| Get-ADGroupMember                 | Displays membership of groups           |
| Remove-ADGroupMember              | Removes members from groups             |
| Add-ADPrincipalGroupMembership    | Adds group membership to objects        |
| Get-ADPrincipalGroupMembership    | Displays group membership of objects    |
| Remove-ADPrincipalGroupMembership | Removes group membership from an object |

```
New-ADGroup -Name "Customer Management" -Path
"ou=managers,dc=adatum,dc=com" -GroupScope Global
-GroupCategory Security
```

```
Add-ADGroupMember -Name "Customer Management"
-Members "Joe"
```

# Using Windows PowerShell Cmdlets to Manage Computer Accounts

| Cmdlet                        | Description                                                                  |
|-------------------------------|------------------------------------------------------------------------------|
| New-ADComputer                | Creates new computer accounts                                                |
| Set-ADComputer                | Modifies properties of computer accounts                                     |
| Get-ADComputer                | Displays properties of computer accounts                                     |
| Remove-ADComputer             | Deletes computer accounts                                                    |
| Test-ComputerSecureChannel    | Verifies or repairs the trust relationship between a computer and the domain |
| Reset-ComputerMachinePassword | Resets the password for a computer account                                   |

```
New-ADComputer -Name "LON-SVR8" -Path
"ou=marketing,dc=adatum,dc=com" -Enabled $true
```

```
Test-ComputerSecureChannel -Repair
```

# Using Windows PowerShell Cmdlets to Manage OUs

| Cmdlet                      | Description                |
|-----------------------------|----------------------------|
| New-ADOrganizationalUnit    | Creates OUs                |
| Set-ADOrganizationalUnit    | Modifies properties of OUs |
| Get-ADOrganizationalUnit    | Views properties of OUs    |
| Remove-ADOrganizationalUnit | Deletes OUs                |

```
New-ADOrganizationalUnit -Name "Sales"
-Path "ou=marketing, dc=adatum, dc=com"
-ProtectedFromAccidentalDelete $true
```

# Lesson 3: Performing Bulk Operations with Windows PowerShell

- What Are Bulk Operations?
- Demonstration: Using Graphical Tools to Perform Bulk Operations
- Querying Objects with Windows PowerShell
- Modifying Objects with Windows PowerShell
- Working with CSV Files
- Demonstration: Performing Bulk Operations with Windows PowerShell

# What Are Bulk Operations?

- A bulk operation is a single action that changes multiple objects
- Sample bulk operations
  - Create user accounts based on data in a spreadsheet
  - Disable all accounts not used in six months
  - Rename the department for many users
- You can perform bulk operations by using:
  - Graphical tools
  - Command-line tools
  - Script

# Demonstration: Using Graphical Tools to Perform Bulk Operations

In this demonstration, you will see how to:

- Create a query for all users
- Configure the Company attribute for all users
- Verify that the Company attribute has been modified

# Querying Objects with Windows PowerShell

| Parameter     | Description                                                             |
|---------------|-------------------------------------------------------------------------|
| SearchBase    | Defines the AD DS path to begin searching                               |
| SearchScope   | Defines at what level below the SearchBase a search should be performed |
| ResultSetSize | Defines how many objects to return in response to a query               |
| Properties    | Defines which object properties to return and display                   |
| Filter        | Defines a filter by using PowerShell syntax                             |
| LDAPFilter    | Defines a filter by using LDAP query syntax                             |

## Descriptions of operators

|     |                       |       |                                     |
|-----|-----------------------|-------|-------------------------------------|
| -eq | Equal to              | -gt   | Greater than                        |
| -ne | Not equal to          | -ge   | Greater than or equal to            |
| -lt | Less than             | -like | Uses wildcards for pattern matching |
| -le | Less than or equal to |       |                                     |



# Querying Objects with Windows PowerShell

Show all the properties for a user account:

```
Get-ADUser -Name "Administrator" -Properties *
```

Show all the user accounts in the Marketing OU and all its subcontainers:

```
Get-ADUser -Filter * -SearchBase
"ou=Marketing, dc=adatum, dc=com" -SearchScope subtree
```

Show all of the user accounts with a last logon date older than a specific date:

```
Get-ADUser -Filter {LastLogondate -lt "January 1, 2012"}
```

Show all of the user accounts in the Marketing department that have a last logon date older than a specific date:

```
Get-ADUser -Filter { (LastLogondate -lt "January 1,
2012") -and (department -eq "Marketing") }
```



# Modifying Objects with Windows PowerShell

Use the pipe character ( | ) to pass a list of objects to a cmdlet for further processing

```
Get - ADUser - Filter { company - not like "*" } |
Set - ADUser - Company "A. Datum"
```

```
Get - ADUser - Filter { LastLogondate - lt "January 1,
2012" } | Disable-ADAccount
```

```
Get - Content C:\users.txt | Disable-ADAccount
```

# Working with CSV Files

The first line of a .csv file defines the names of the columns

```
First Name, Last Name, Department
Greg, Guzik, IT
Robin, Young, Research
Qiong, Wu, Marketing
```

A **foreach** loop processes the contents of a .csv that have been imported into a variable

```
$users=Import-CSV -LiteralPath "C:\users.csv"
foreach ($user in $users) {
 Write-Host "The first name is: "
 $user.FirstName
}
```

# Demonstration: Performing Bulk Operations with Windows PowerShell

In this demonstration, you will see how to:

- Configure a department for users
- Create an OU
- Run a script to create new user accounts
- Verify that new user accounts were created

# Lab: Automating AD DS Administration by Using Windows PowerShell

- Exercise 1: Creating User Accounts and Groups by Using Windows PowerShell
- Exercise 2: Using Windows PowerShell to Create User Accounts in Bulk
- Exercise 3: Using Windows PowerShell to Modify User Accounts in Bulk

## Logon Information

Virtual machines      **20410D-LON-DC1**

**20410D-LON-CL1**

User name              **Adatum\Administrator**

Password              **Pa\$\$w0rd**

**Estimated Time: 45 minutes**

# Lab Scenario

You have been working for A. Datum Corporation for several years as a desktop support specialist. In this role, you visited desktop computers to troubleshoot app and network problems. You have recently accepted a promotion to the server support team. One of your first assignments is configuring the infrastructure service for a new branch office.

As part of configuring a new branch office, you need to create user and group accounts. Creating multiple users with graphical tools is inefficient, so, you will use Windows PowerShell.

# Lab Review

- By default, are new user accounts enabled or disabled when you create them by using the **New-ADUser** cmdlet?
- What file extension do Windows PowerShell scripts use?

# Module Review and Takeaways

- Review Questions
- Tools

# Microsoft® Official Course



Module 5

Implementing IPv4

**Microsoft®**

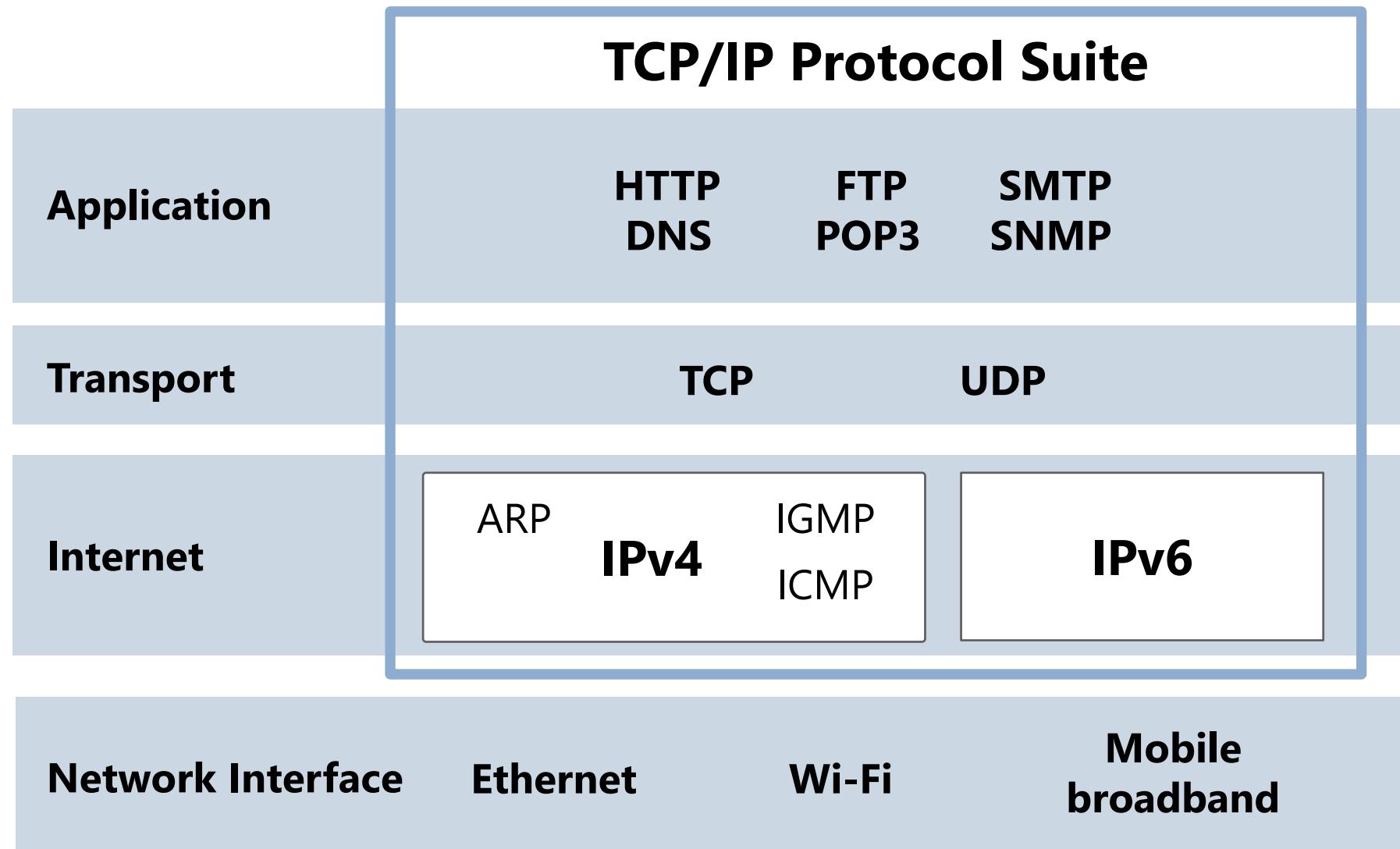
# Module Overview

- Overview of TCP/IP
- Understanding IPv4 Addressing
- Subnetting and Supernetting
- Configuring and Troubleshooting IPv4

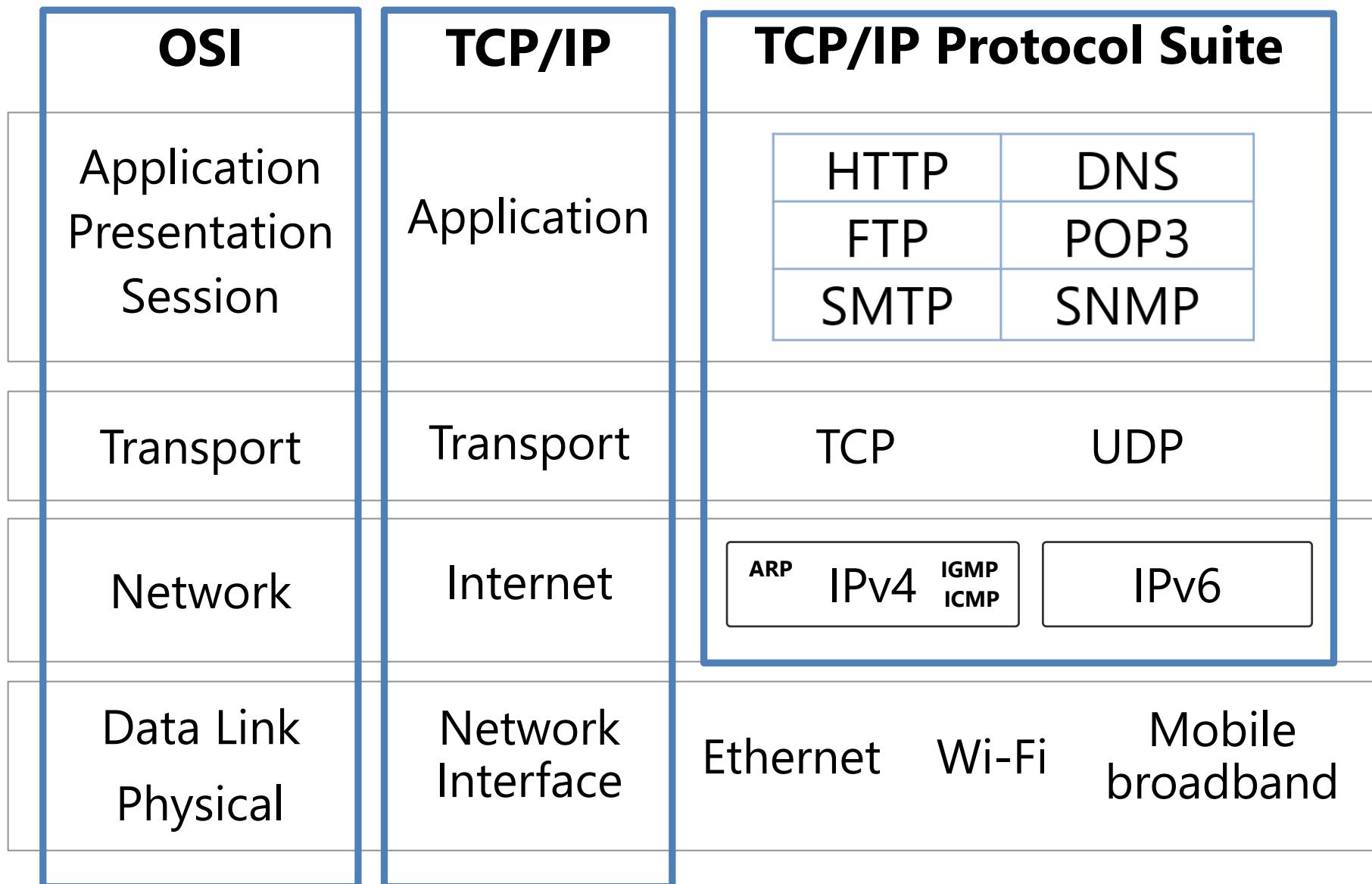
# Lesson 1: Overview of TCP/IP

- The TCP/IP Protocol Suite
- Protocols in the TCP/IP Suite
- TCP/IP Applications
- What Is a Socket?

# The TCP/IP Protocol Suite



# Protocols in the TCP/IP Suite

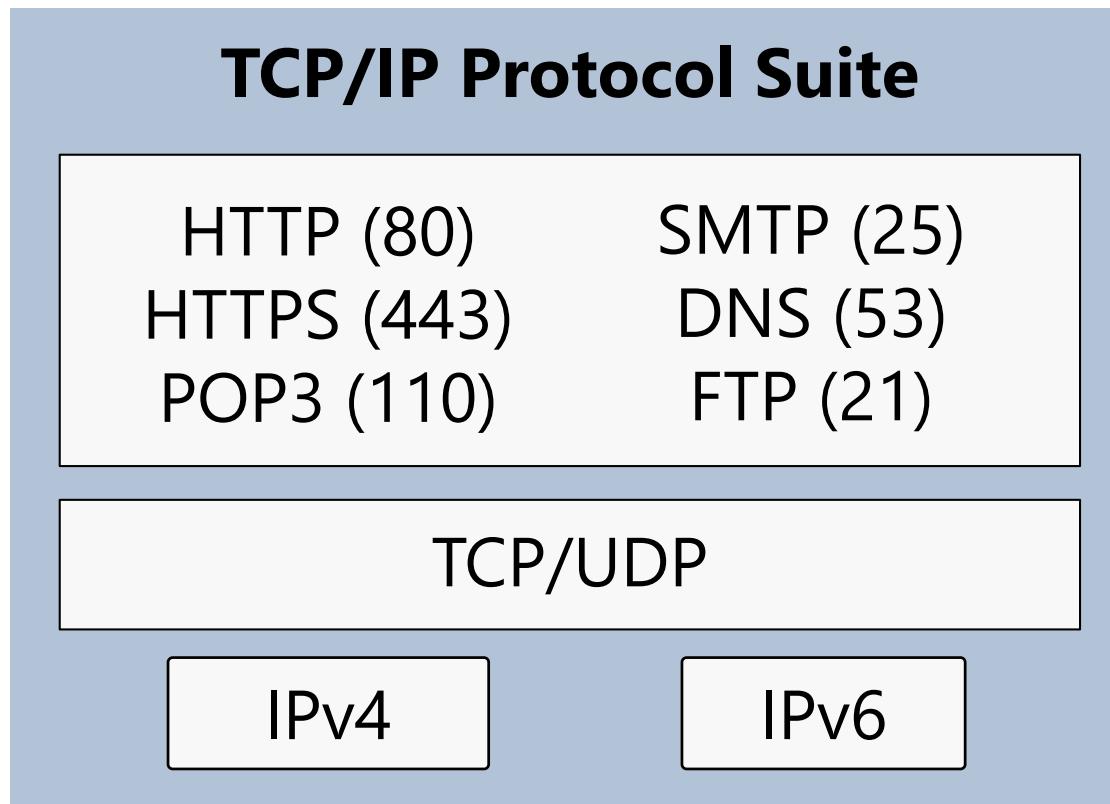


## **Some common application layer protocols:**

- HTTP
- HTTPS
- FTP
- RDP
- SMB
- SMTP
- POP3

# What Is a Socket?

**A socket is a combination of an IP address, a transport protocol, and a port**



# Lesson 2: Understanding IPv4 Addressing

- IPv4 Addressing
- Public and Private IPv4 Addresses
- How Dotted Decimal Notation Relates to Binary Numbers
- Simple IPv4 Implementations
- More Complex IPv4 Implementations

# IPv4 Addressing

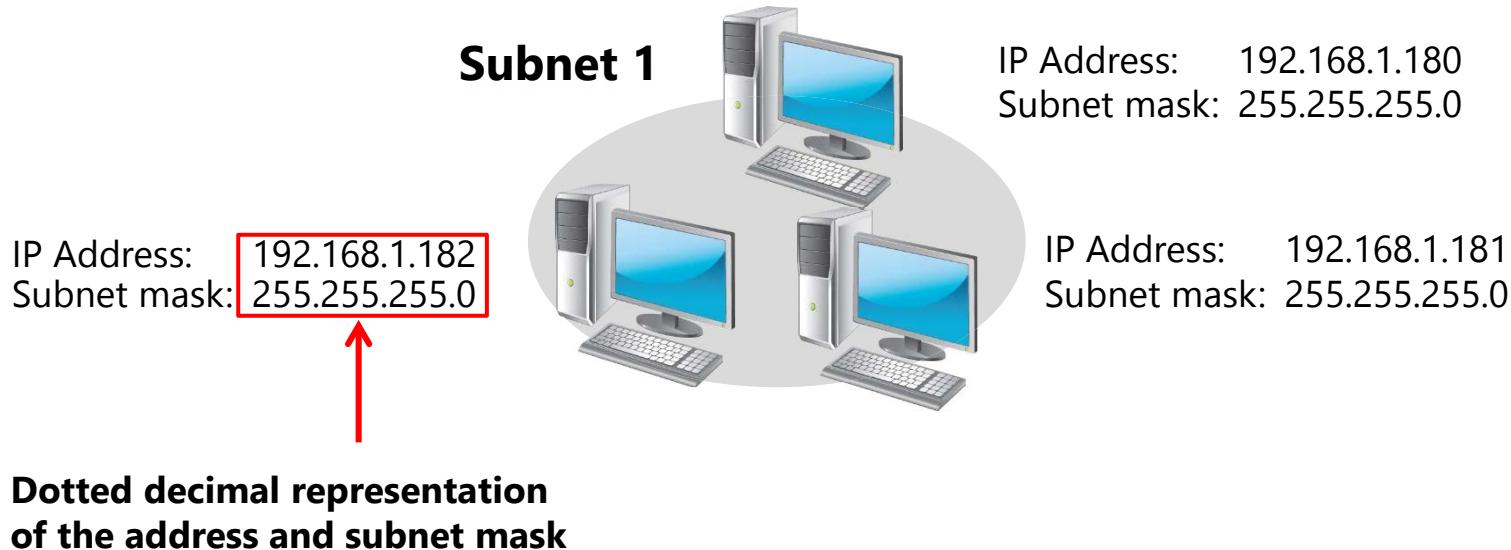
- Each networked computer must be assigned a unique IPv4 address
- Network communication for a computer is directed to the IPv4 address of the computer
- Each IPv4 address contains:
  - ✓ Network ID, identifying the network
  - ✓ Host ID, identifying the computer
- The subnet mask identifies which part of the IPv4 address is the network ID (255) and which is the host ID (0)

|                    |     |     |   |    |
|--------------------|-----|-----|---|----|
| <b>IP address</b>  | 172 | 16  | 0 | 10 |
| <b>Subnet mask</b> | 255 | 255 | 0 | 0  |
| <b>Network ID</b>  | 172 | 16  | 0 | 0  |
| <b>Host ID</b>     | 0   | 0   | 0 | 10 |



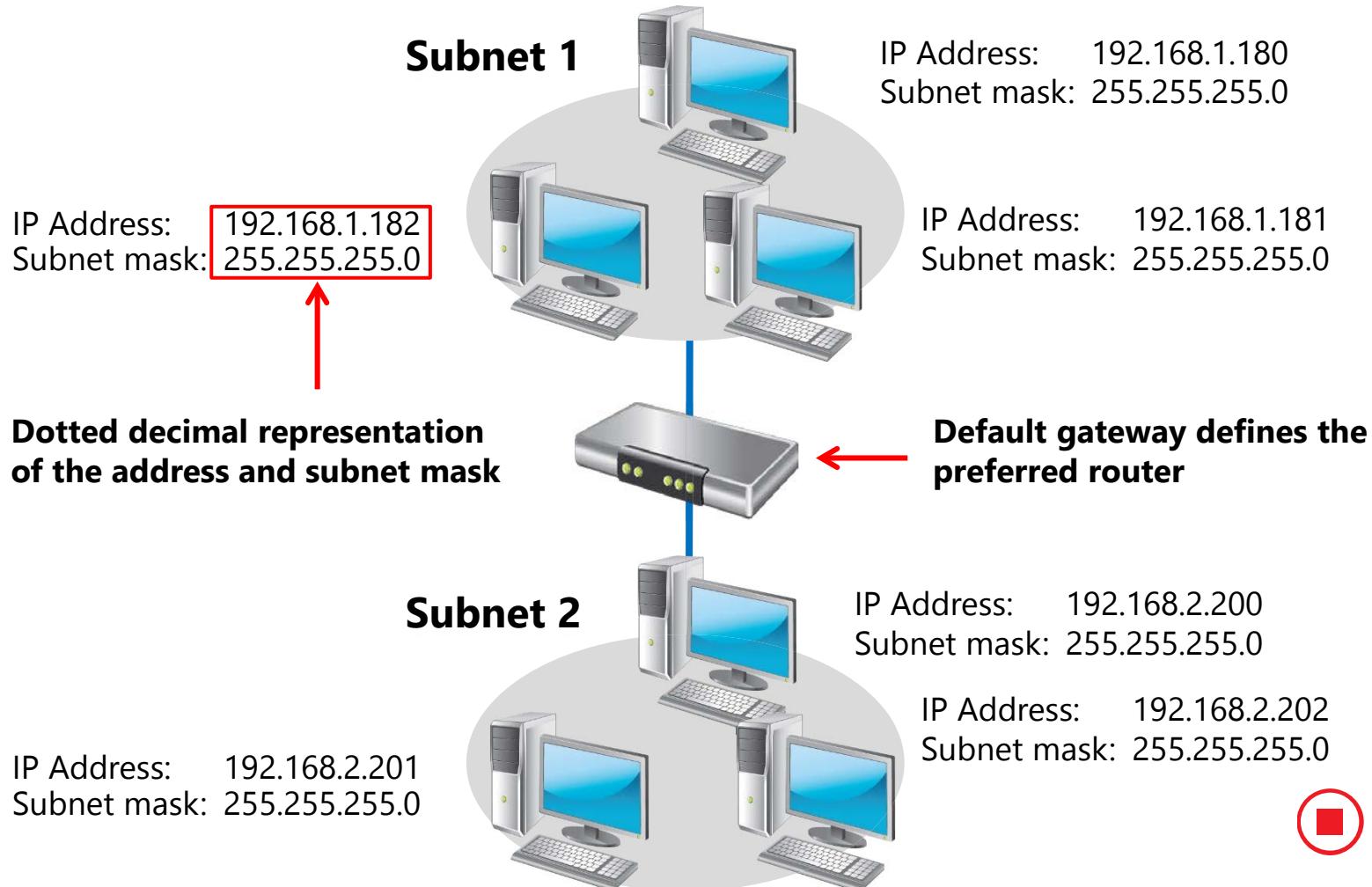
# IPv4 Addressing

**An IPv4 configuration identifies a computer to other computers on a network**



# IPv4 Addressing

**An IPv4 configuration identifies a computer to other computers on a network**



# Public and Private IPv4 Addresses

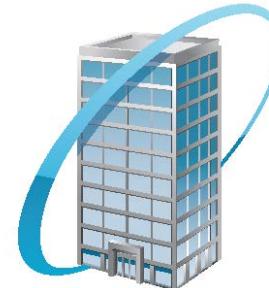
## Public

- Required by devices and hosts that connect directly to the Internet
- Must be globally unique
- Routable on the Internet
- Must be assigned by IANA/RIR



## Private

- Not routable on the Internet
  - 10.0.0.0/8
  - 172.16.0.0/12
  - 192.168.0.0/16
- Can be assigned locally by an organization
- Must be translated to access the Internet



# How Dotted Decimal Notation Relates to Binary Numbers

**Dotted decimal notation is based on the decimal number system, but computers use IP addresses in binary**

Within an 8-bit octet, each bit position has a decimal value:

- A bit that is set to 0 always has a zero value
- A bit that is set to 1 can be converted to a decimal value
- The low-order bit represents a decimal value of 1
- The high-order bit represents a decimal value of 128

If all bits in an octet are set to 1, then the octet's decimal value is 255, the highest possible value of an octet:

$$128 + 64 + 32 + 16 + 8 + 4 + 2 + 1$$



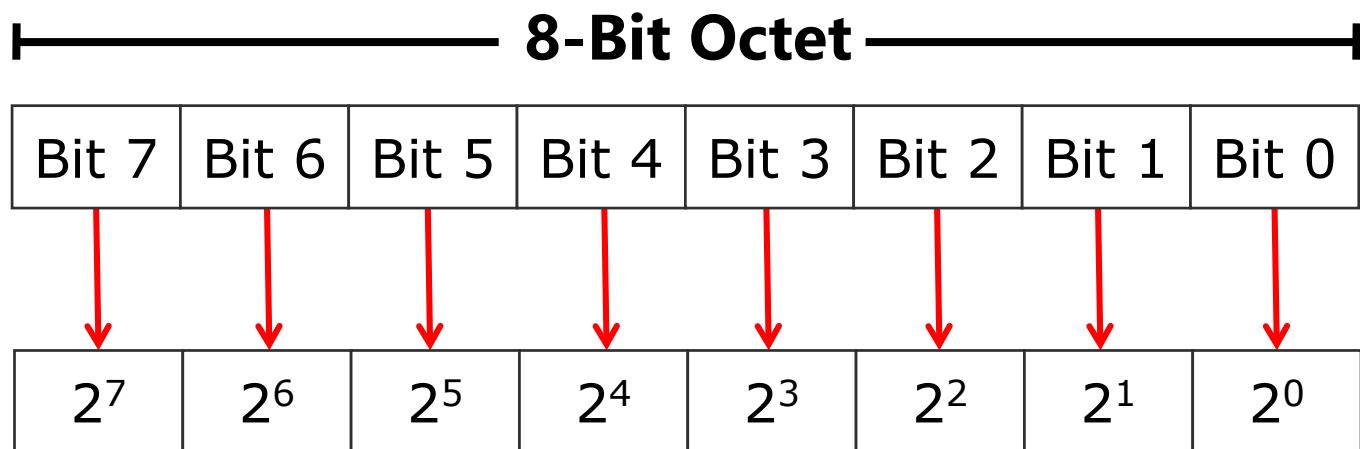
# How Dotted Decimal Notation Relates to Binary Numbers

————— **8-Bit Octet** —————

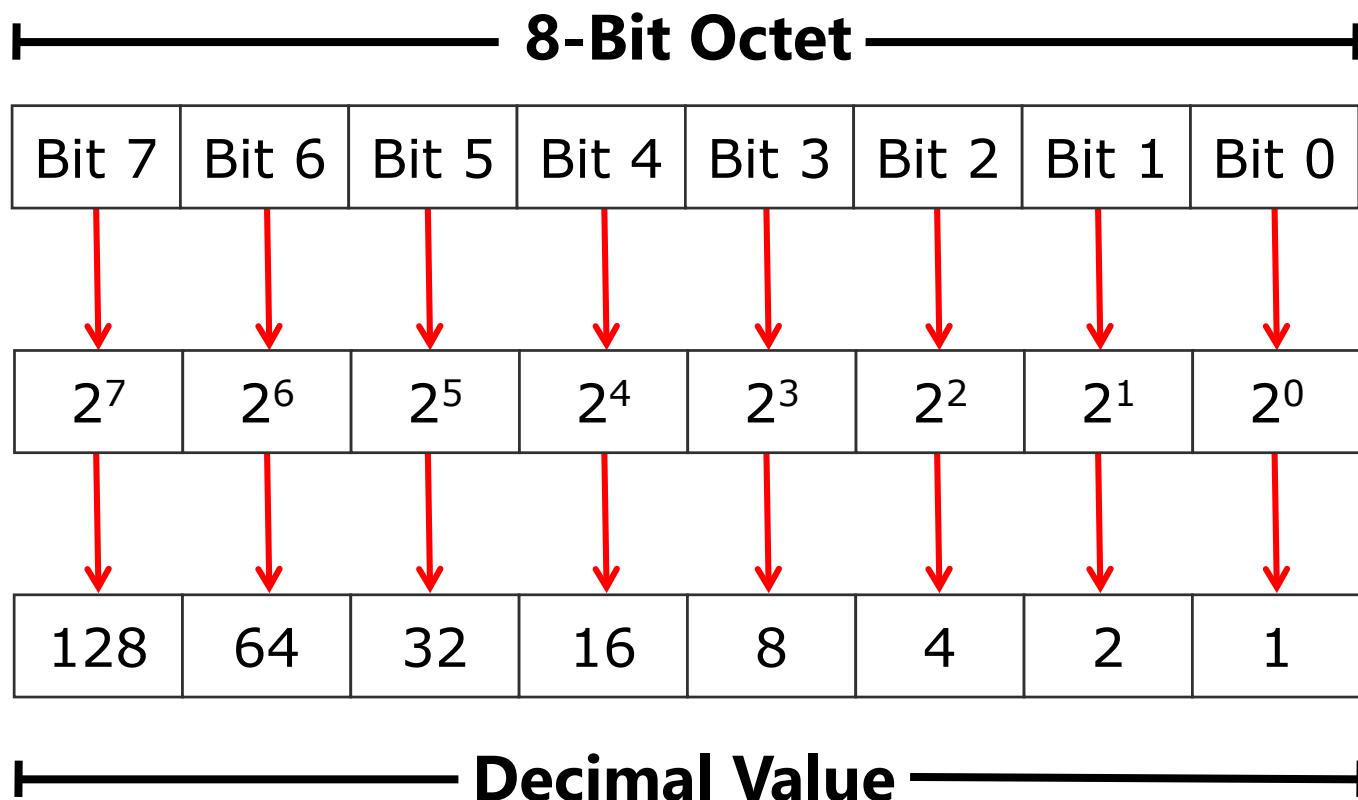
|       |       |       |       |       |       |       |       |
|-------|-------|-------|-------|-------|-------|-------|-------|
| Bit 7 | Bit 6 | Bit 5 | Bit 4 | Bit 3 | Bit 2 | Bit 1 | Bit 0 |
|-------|-------|-------|-------|-------|-------|-------|-------|



# How Dotted Decimal Notation Relates to Binary Numbers

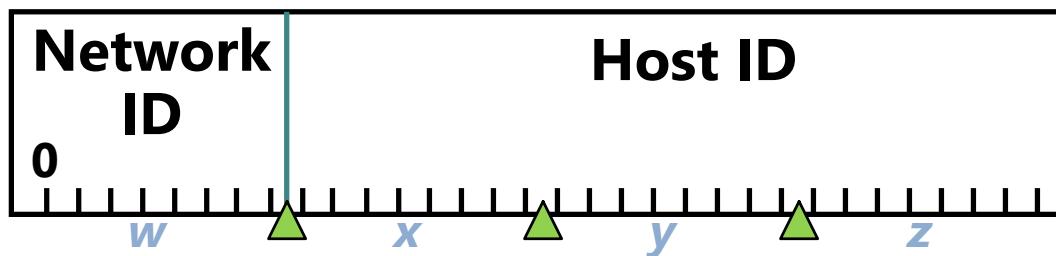


# How Dotted Decimal Notation Relates to Binary Numbers

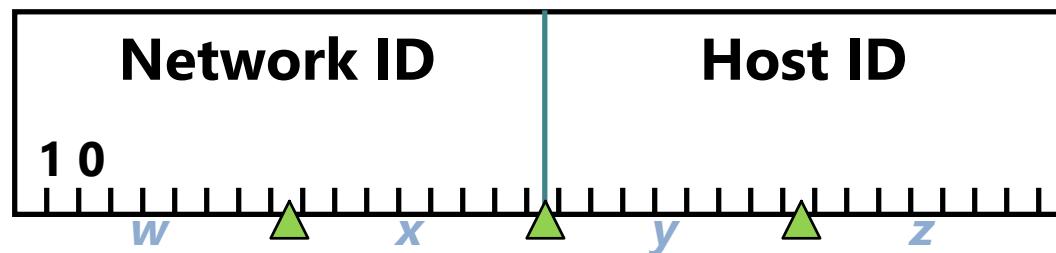


# Simple IPv4 Implementations

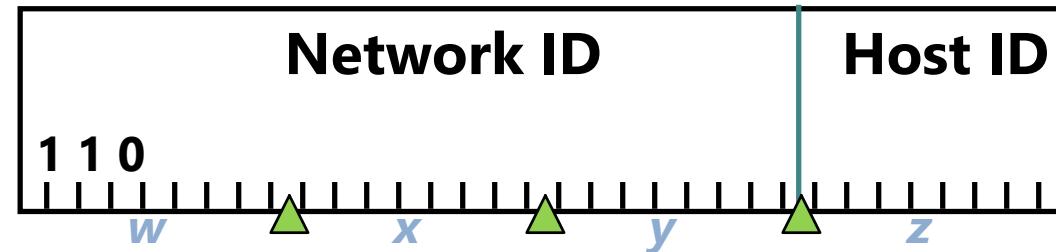
**Class A (/8)**  
**Large Network**



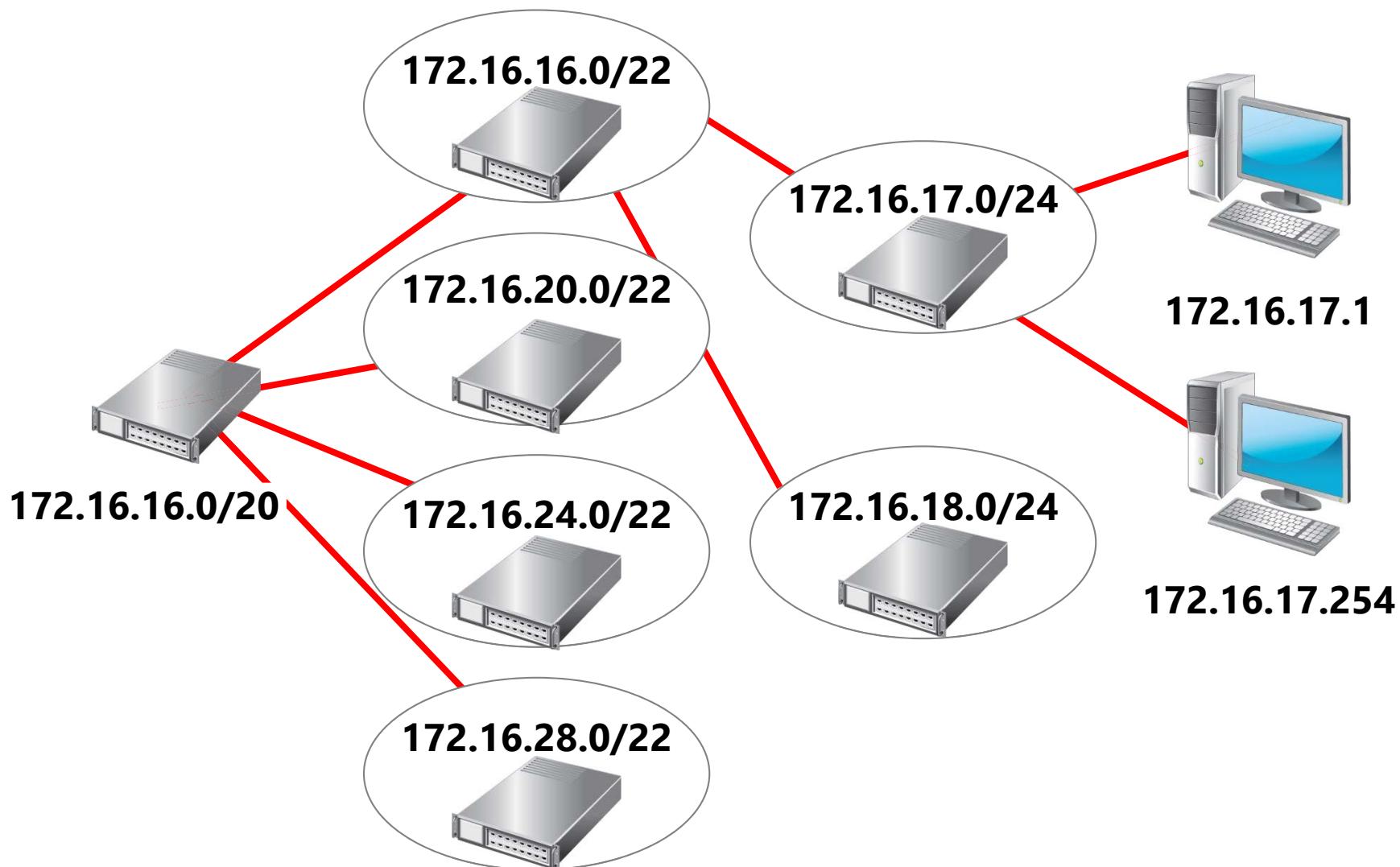
**Class B (/16)**  
**Medium**  
**Network**



**Class C (/24)**  
**Small Network**



# More Complex IPv4 Implementations

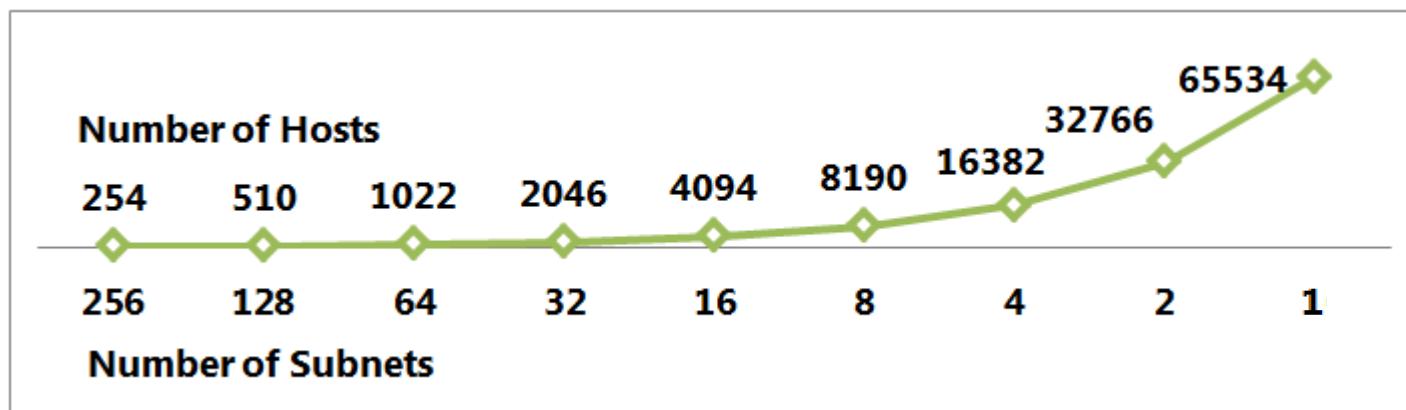
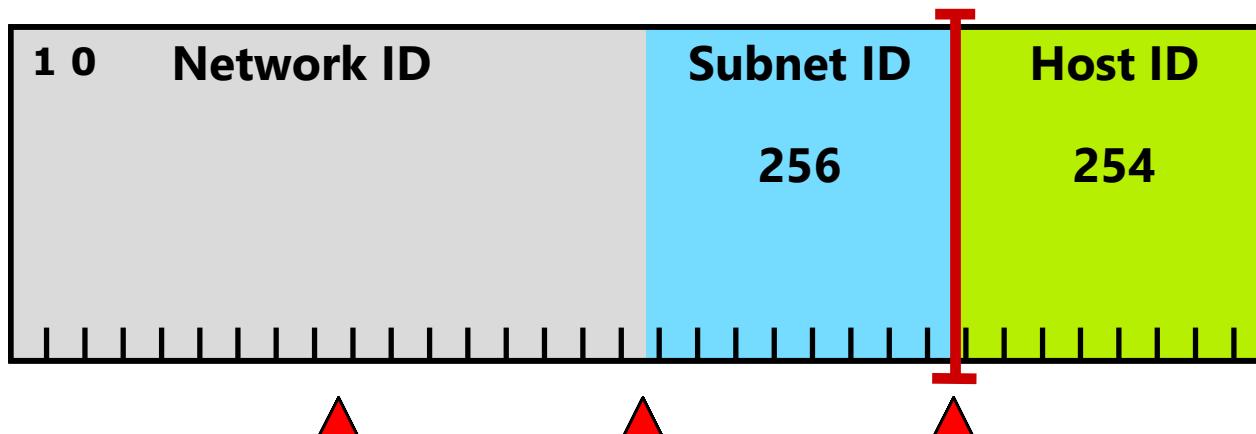


# Lesson 3: Subnetting and Supernetting

- How Bits Are Used in a Subnet Mask or Prefix Length
- The Benefits of Using Subnetting
- Calculating Subnet Addresses
- Calculating Host Addresses
- Discussion: Creating a Subnetting Scheme for a New Office
- What Is Supernetting?

# How Bits Are Used in a Subnet Mask or Prefix Length

## Class B Address with Subnet



# The Benefits of Using Subnetting

When you subdivide a network into subnets, you create a unique ID for each subnet that is derived from the main network ID

By using subnets, you can:

- Use a single network address across multiple locations
- Reduce network congestion by segmenting traffic
- Increase security by using firewalls
- Overcome limitations of current technologies

# Calculating Subnet Addresses

When determining subnet addresses you should:

- Choose the number of subnet bits based on the number of subnets required
- Use  $2^n$  to determine the number of subnets available from n bits

For five locations, the following three subnet bits are required:

- 5 locations = 5 subnets required
- $2^2 = 4$  subnets (not enough)
- $2^3 = 8$  subnets

# Calculating Host Addresses

When determining host addresses you should:

- Choose the number of host bits based on the number of hosts that you require on each subnet
- Use  $2^n - 2$  to determine the number of hosts that are available on each subnet

For subnets with 100 hosts, seven host bits are required:

- $2^6 - 2 = 62$  hosts (not enough)
- $2^7 - 2 = 126$  hosts

# Discussion: Creating a Subnetting Scheme for a New Office

- How many subnets are required?
- How many bits are required to create that number of subnets?
- How many hosts are required on each subnet?
- How many bits are required to support that number of hosts?
- What is an appropriate subnet mask that would satisfy these requirements?



**20 minutes**

# What Is Supernetting?

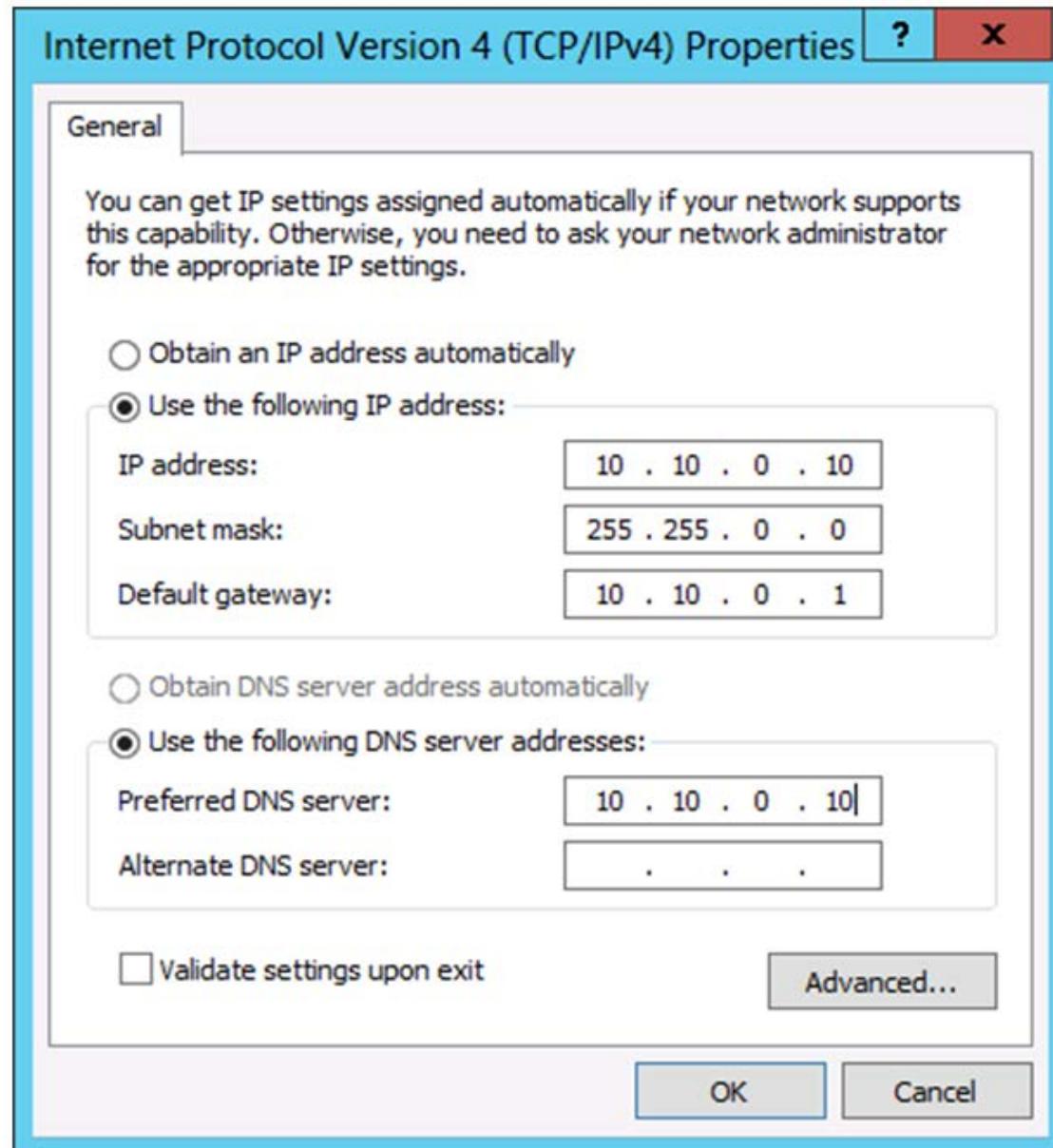
- Supernetting combines multiple small networks into a larger network
- The networks that you combine must be contiguous
- The following table shows an example of supernetting two class C networks

| Network                               | Range                         |
|---------------------------------------|-------------------------------|
| 192.168. <b>00010000</b> .00000000/24 | 192.168.16.0 - 192.168.16.255 |
| 192.168. <b>00010001</b> .00000000/24 | 192.168.17.0 - 192.168.17.255 |
| 192.168. <b>00010000</b> .00000000/23 | 192.168.16.0 - 192.168.17.255 |

# Lesson 4: Configuring and Troubleshooting IPv4

- Configuring IPv4 Manually
- Configuring IPv4 Automatically
- Using Windows PowerShell Cmdlets to Troubleshoot IPv4
- IPv4 Troubleshooting Tools
- The IPv4 Troubleshooting Process
- What Is Microsoft Message Analyzer?
- Demonstration: How to Capture and Analyze Network Traffic by Using Microsoft Message Analyzer

# Configuring IPv4 Manually



# Configuring IPv4 Manually

Examples using Windows PowerShell cmdlets:

```
New-NetIPInterface -InterfaceAlias "Local Area Connection" -IPAddress 10.10.0.10
-PrefixLength 24 -DefaultGateway 10.10.0.1
```

```
Set-DNSClientServerAddresses -InterfaceAlias "Local Area Connection"
-ServerAddresses 10.12.0.1, 10.12.0.2
```

Example using the netsh command-line tool:

```
Netsh interface ip set address name="Local Area Connection" source=static addr=10.10.0.10
mask=255.255.255.0 gateway=10.10.0.1
```



# Configuring IPv4 Automatically



```
Set -NetInterface -InterfaceAlias "Local Area Connection" -Dhcp Enabled
Restart -NetAdapter -Name "Local Area Connection"
```

# Using Windows PowerShell Cmdlets to Troubleshoot IPv4

New Windows PowerShell cmdlets include:

- Get-NetAdapter
- Restart-NetAdapter
- Get-NetIPInterface
- Get-NetIPAddress
- Get-NetRoute
- Get-NetConnectionProfile
- Get-DNSClientCache
- Get-DNSClientServerAddress
- Register-DnsClient
- Set-DnsClient
- Set-DnsClientGlobalSetting
- Set-DnsClientServerAddress
- Set-NetIPAddress
- Set-NetIPv4Protocol
- Set-NetIPInterface
- Test-Connection
- Test-NetConnection
- Resolve-Dnsname

# IPv4 Troubleshooting Tools

Use the following tools to troubleshoot IPv4:

- Ipconfig
- Ping
- Tracert
- Pathping
- Telnet
- Netstat
- Resource Monitor
- Windows Network Diagnostics
- Event Viewer

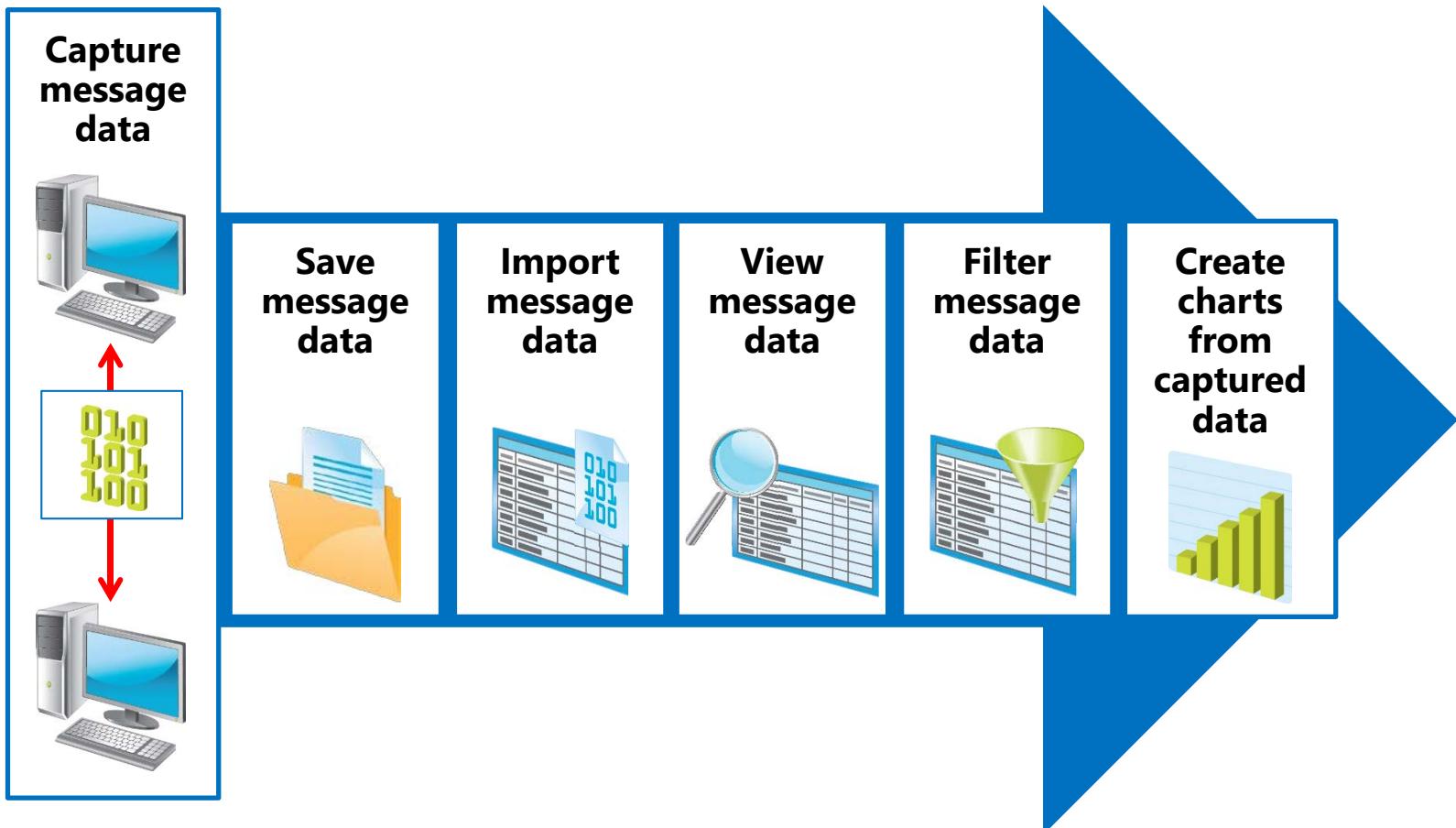
# The IPv4 Troubleshooting Process

After you identify the scope of the problem, use the following tools to troubleshoot network connectivity:

| <b>Step</b>                                 | <b>Windows PowerShell</b>      | <b>Command-line tool</b> |
|---------------------------------------------|--------------------------------|--------------------------|
| Verify the network configuration is correct | Get-NetIPAddress               | ipconfig                 |
| Identify the network path between hosts     | Test-NetConnection -TraceRoute | tracert                  |
| See if the remote host responds             | Test-NetConnection             | ping                     |
| Test the service on a remote host           | Test-NetConnection -Port       | Telnet                   |
| See if the default gateway responds         | Test-NetConnection             | ping                     |

# What Is Microsoft Message Analyzer?

You can use Microsoft Message Analyzer to perform the following network analysis tasks:



# Demonstration: How to Capture and Analyze Network Traffic by Using Microsoft Message Analyzer

In this demonstration, you will see how to:

- Start a new Capture/Trace in Microsoft Message Analyzer
- Capture packets from a ping request
- Analyze the captured network traffic
- Filter the network traffic

# Lab: Implementing IPv4

- Exercise 1: Identifying Appropriate Subnets
- Exercise 2: Troubleshooting IPv4

## Logon Information

|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-RTR</b><br><b>20410D-LON-SVR2</b> |
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

**Estimated Time: 45 minutes**

## Lab Scenario

You have recently accepted a promotion to the server support team. One of your first assignments is configuring the infrastructure service for a new branch office.

After a security review, your manager has asked you to calculate new subnets for the branch office to support segmenting network traffic. You also need to troubleshoot a connectivity problem on a server in the branch office.

# Lab Review

- Why is variable-length subnetting required in this lab?
- Which Windows PowerShell cmdlet can you use to view the local routing table of a computer instead of using route print?

# Module Review and Takeaways

- Review Questions
- Best Practices
- Common Issues and Troubleshooting Tips
- Tools

# Microsoft® Official Course



## Module 6

### Implementing Dynamic Host Configuration Protocol

# Module Overview

- Overview of the DHCP Server Role
- Configuring DHCP Scopes
- Managing a DHCP Database
- Securing and Monitoring DHCP

# Lesson 1: Overview of the DHCP Server Role

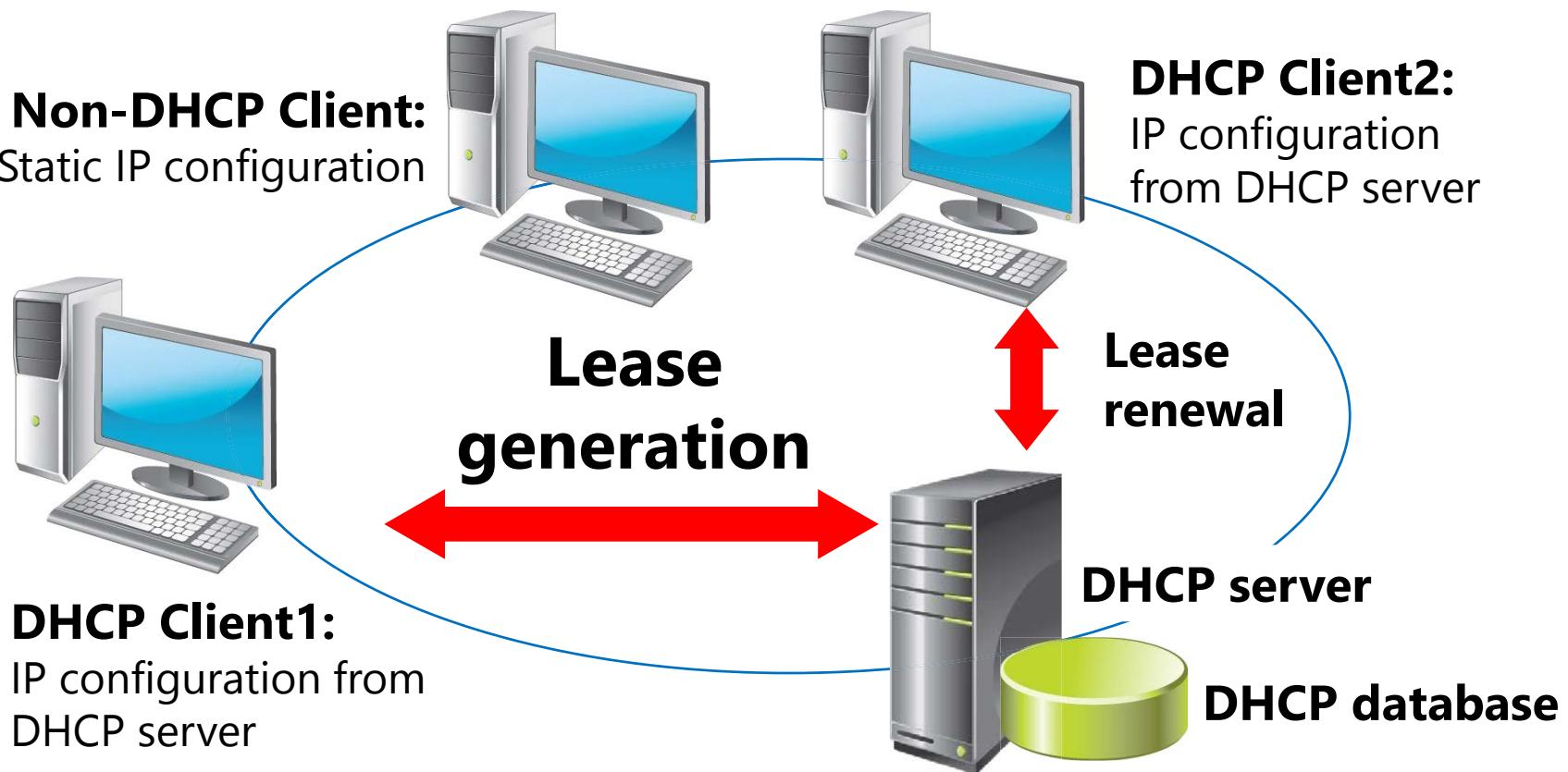
- Benefits of Using DHCP
- How DHCP Allocates IP Addresses
- How DHCP Lease Generation Works
- How DHCP Lease Renewal Works
- Demonstration: Installing the DHCP Server Role
- How DHCP Interacts with DNS
- What Is a DHCP Relay Agent?
- DHCP Server Authorization

# Benefits of Using DHCP

**DHCP reduces the complexity and amount of administrative work by using automatic IP configuration**

| Automatic IP Configuration                        | Manual IP Configuration                                |
|---------------------------------------------------|--------------------------------------------------------|
| IP addresses are supplied automatically           | IP addresses are entered manually                      |
| Correct configuration information is ensured      | IP address could be entered incorrectly                |
| Client configuration is updated automatically     | Communication and network issues can result            |
| A common source of network problems is eliminated | Frequent computer moves increase administrative effort |

# How DHCP Allocates IP Addresses

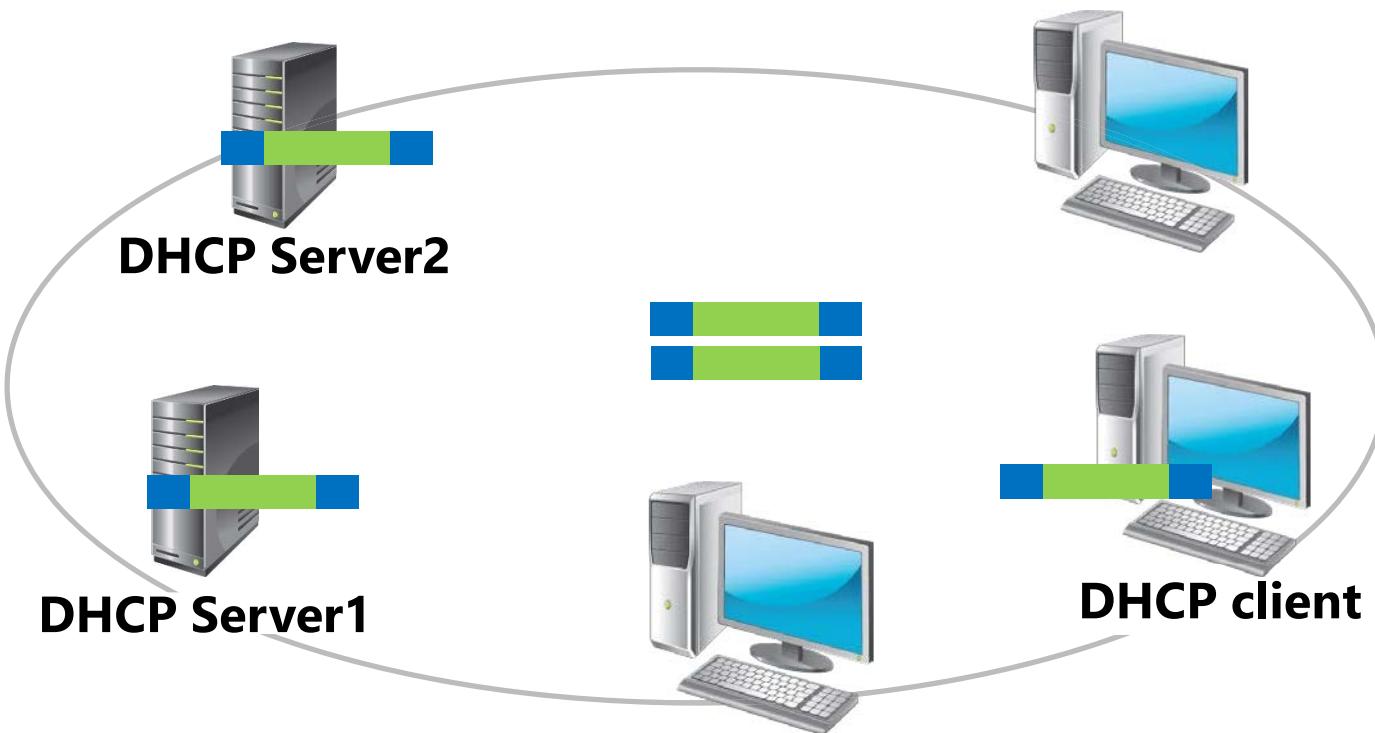


**IP Address1: Leased to DHCP Client1**

**IP Address2: Leased to DHCP Client2**

**IP Address3: Available for lease**

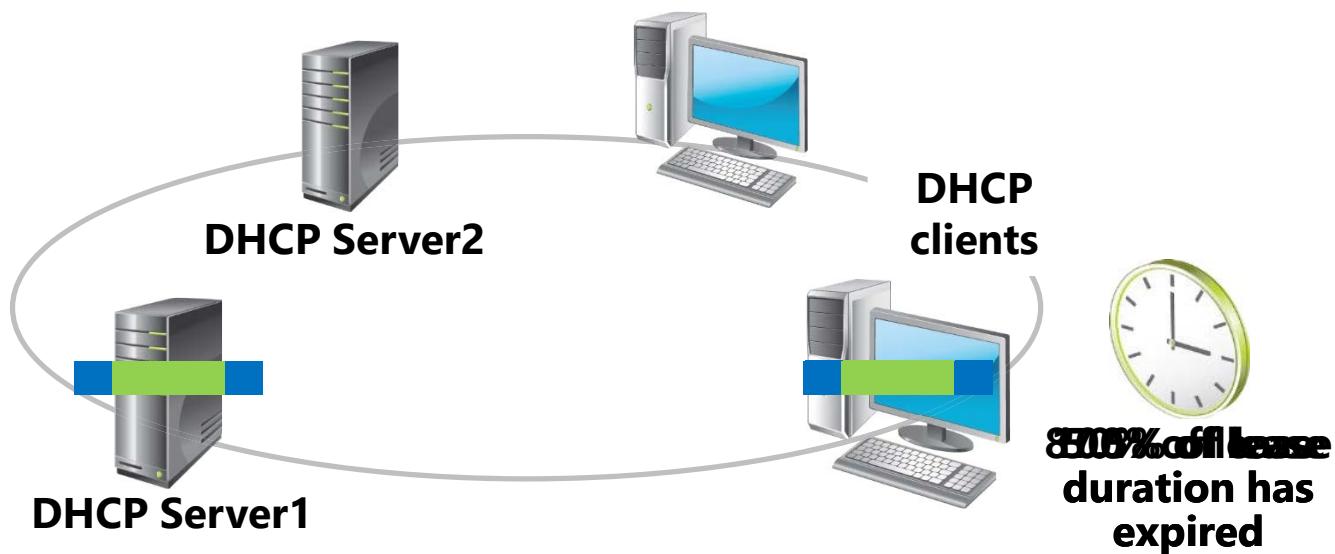
# How DHCP Lease Generation Works



1. DHCP client broadcasts a **DHCPOPTIONS** packet
2. DHCP servers broadcast a **DHCPOFFER** packet
3. DHCP client broadcasts a **DHCPOREQUEST** packet
4. DHCP Server1 broadcasts a **DHCPOACK** packet



# How DHCP Lease Renewal Works



1. DHCP client sends a **DHCPREQUEST** packet
2. DHCP Server1 sends a **DHCPOFFER** packet
3. If the client fails to renew its lease after 50% of the lease duration has expired, the DHCP lease renewal process begins again after 87.5% of the lease duration has expired
4. If the client fails to renew its lease after 87.5% of the lease has expired, the DHCP lease generation process starts over again with a DHCP client broadcasting a **DHCPDISCOVER**



# Demonstration: Installing the DHCP Server Role

In this demonstration, you will see how to:

- Install the DHCP server role
- Authorize the DHCP server

# How DHCP Interacts with DNS

DHCP can:

- Register client records into DNS zones
- Use DNS dynamic update protocol

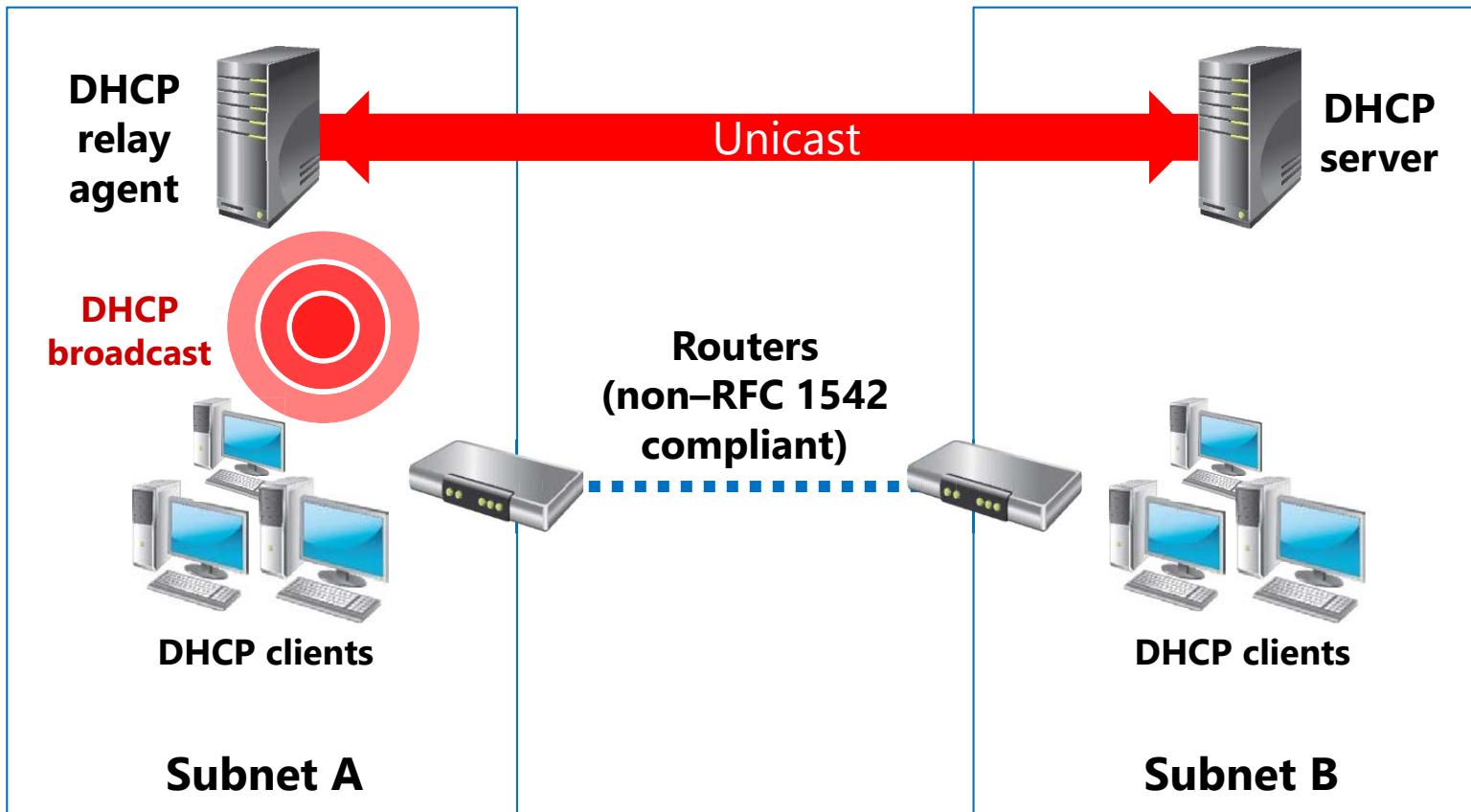
To use secure DNS dynamic updates, add DHCP servers to the AD DS DnsUpdateProxy global group

DHCP policies:

- Automatically assign settings based on FQDN
- Register workgroup computers with guest DNS suffix
- Disable PTR registrations without disabling host record registration

# What Is a DHCP Relay Agent?

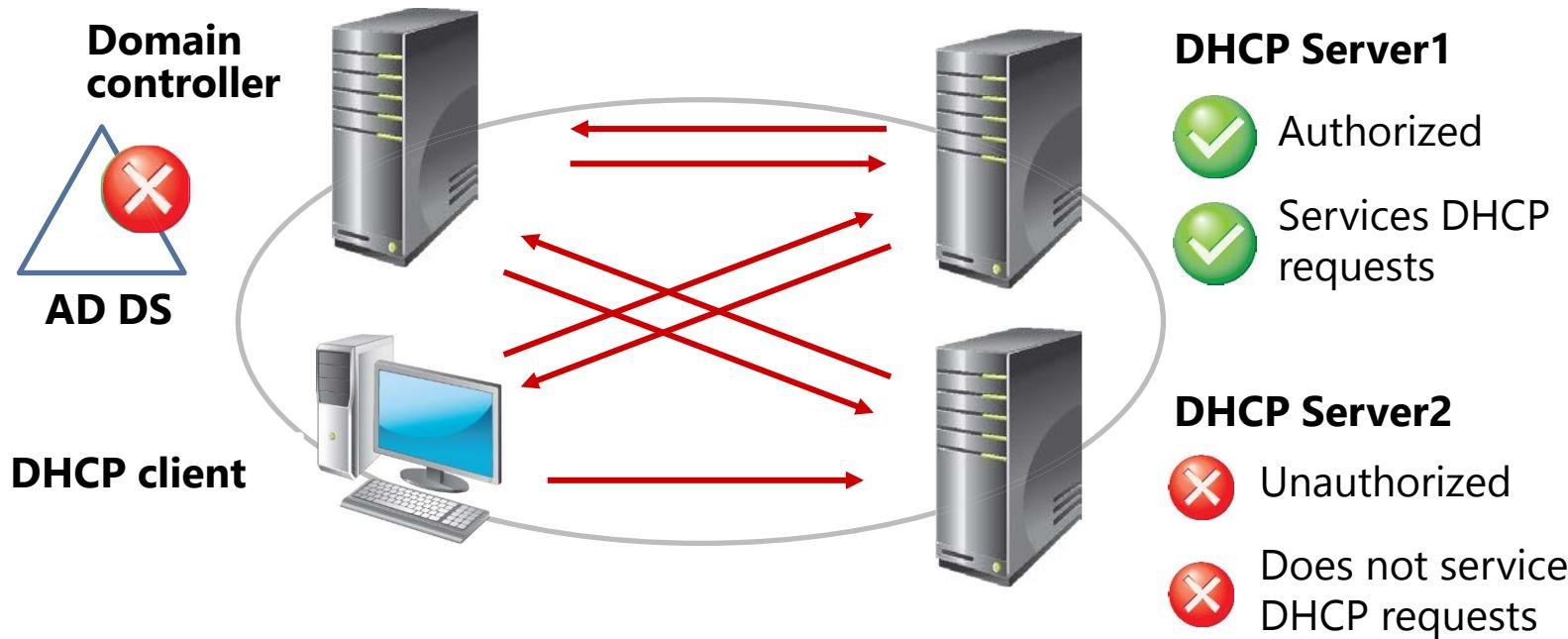
**A DHCP relay agent listens for DHCP broadcasts from DHCP clients and then relays them to DHCP servers in different subnets**



# DHCP Server Authorization

**DHCP authorization registers the DHCP Server service in the Active Directory domain to support DHCP clients**

If DHCP Server1 finds its IP address on the list,  
the service starts and supports DHCP clients



# Lesson 2: Configuring DHCP Scopes

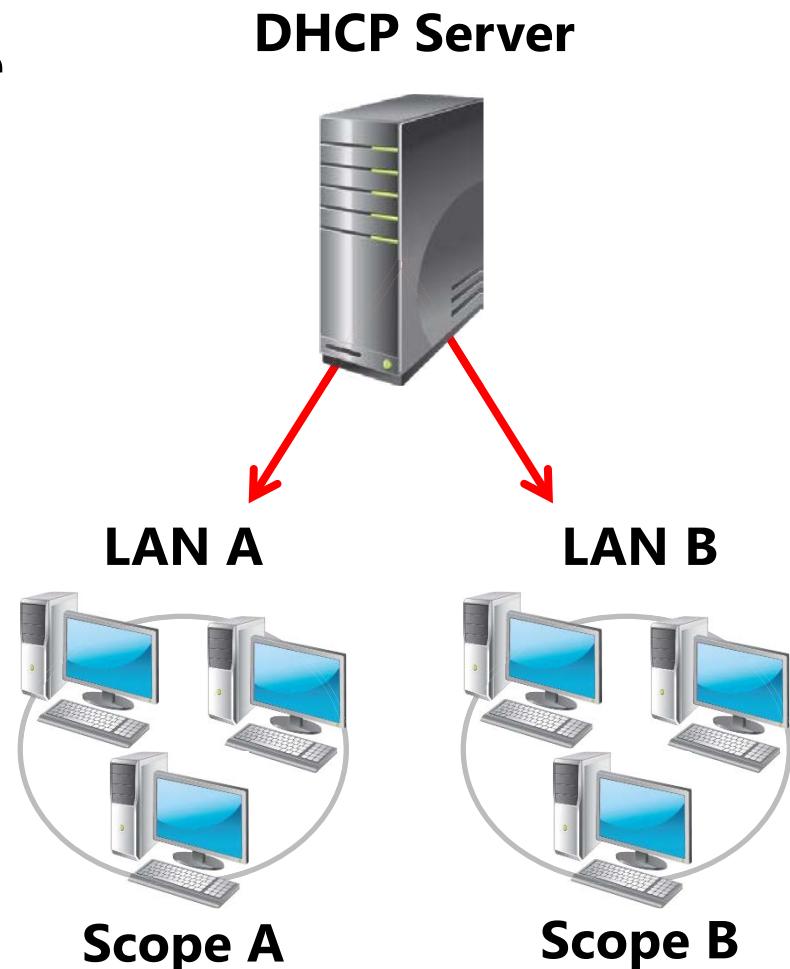
- What Are DHCP Scopes?
- What Is a DHCP Reservation?
- What Are DHCP Options?
- How DHCP Applies Options
- Demonstration: Creating and Configuring a DHCP Scope

# What Are DHCP Scopes?

A **DHCP scope** is a range of IP addresses that are available to be leased

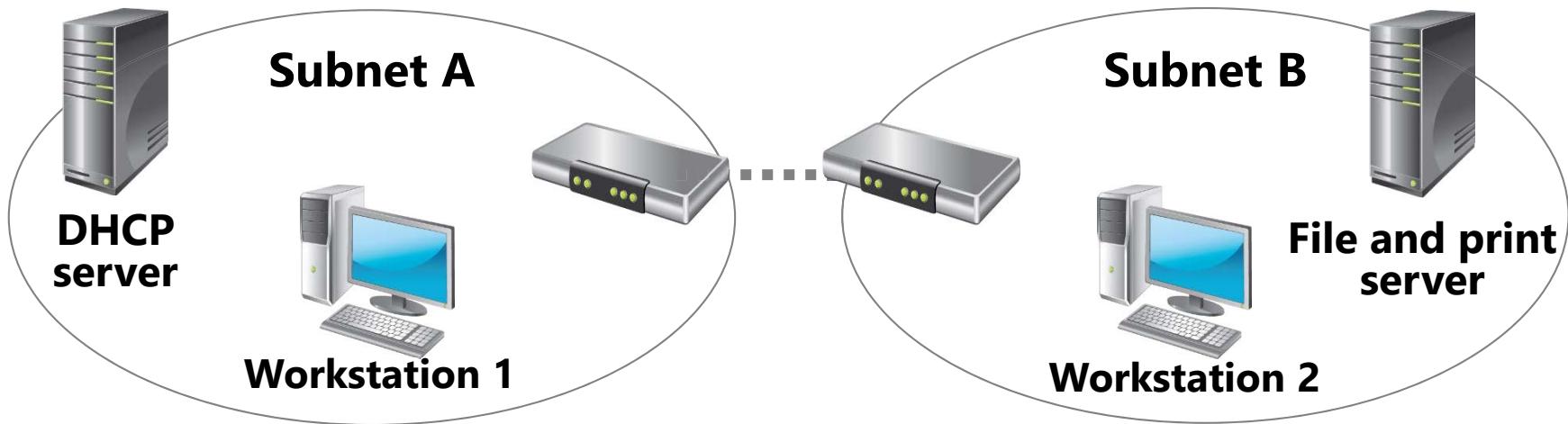
**DHCP scope properties include:**

- Network ID
- Lease duration
- Scope name
- Subnet mask
- Network IP address range
- Exclusion range



# What Is a DHCP Reservation?

**A DHCP reservation occurs when an IP address within a scope is set aside for use with a specific DHCP client**



**IP Address1: Leased to Workstation 1**

**IP Address2: Leased to Workstation 2**

**IP Address3: Reserved for file and print server**

# What Are DHCP Options?

DHCP options:

- Are values for common configuration data
- Apply to the server, scopes, reservations, and class options

Common scope options are:

- Router (Default Gateway)
- DNS Name
- DNS Servers
- WINS Servers

# How DHCP Applies Options

You can apply DHCP options at various levels:

- Server
- Scope
- Class
- Reserved client

Typically, you do not apply the class or reserved client options

# Demonstration: Creating and Configuring a DHCP Scope

In this demonstration, you will see how to configure scope and scope options in DHCP

# Lesson 3: Managing a DHCP Database

- What Is a DHCP Database?
- Backing Up and Restoring a DHCP Database
- Reconciling a DHCP Database
- Moving a DHCP Database

# What Is a DHCP Database?

The *DHCP database* is a dynamic database that contains configuration information such as:

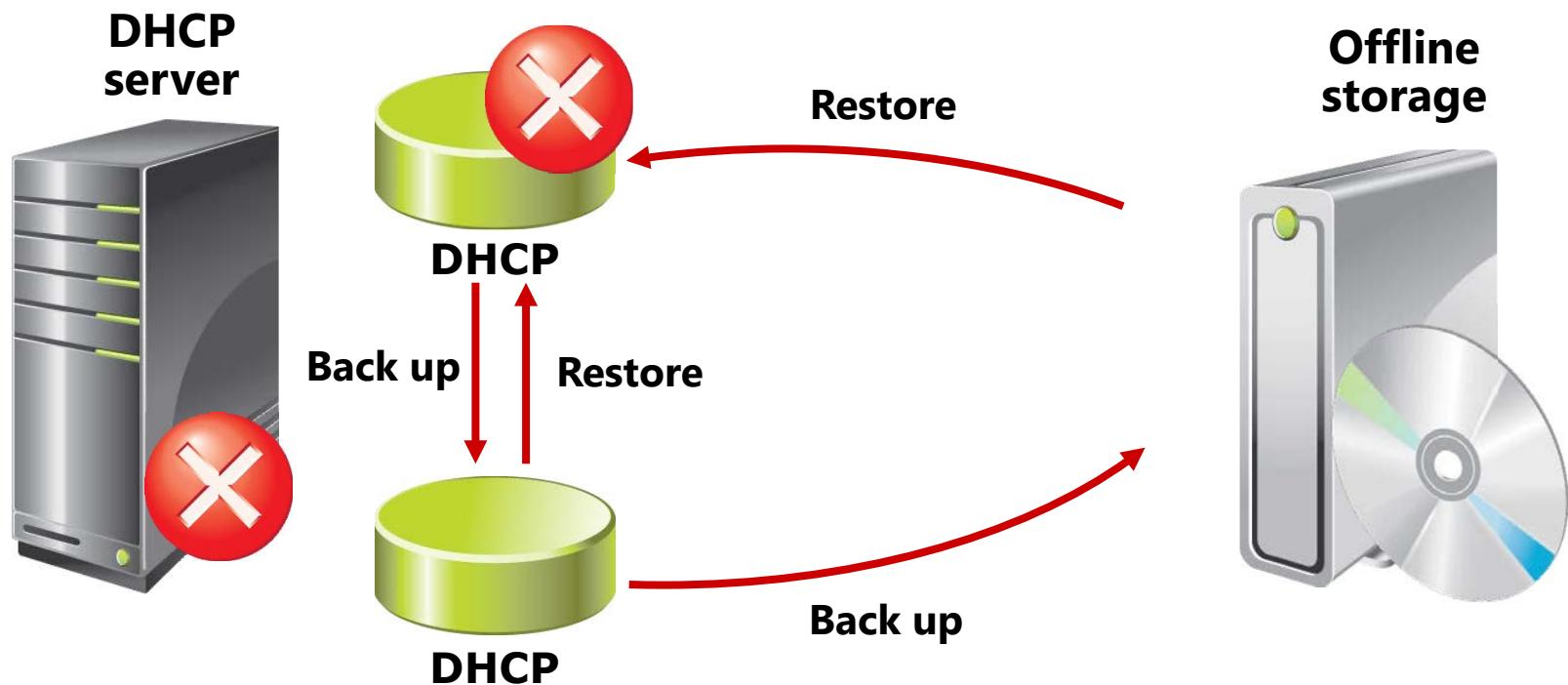
- Scopes
- Reservations
- Address leases

Windows Server 2012 stores the DHCP database in the %Systemroot%\System32\DHcp folder

The DHCP database files include:

- Dhcp.mdb
- J50Res#####.jrs
- temp.edb
- J50.chk
- J50.log and J50\*.log

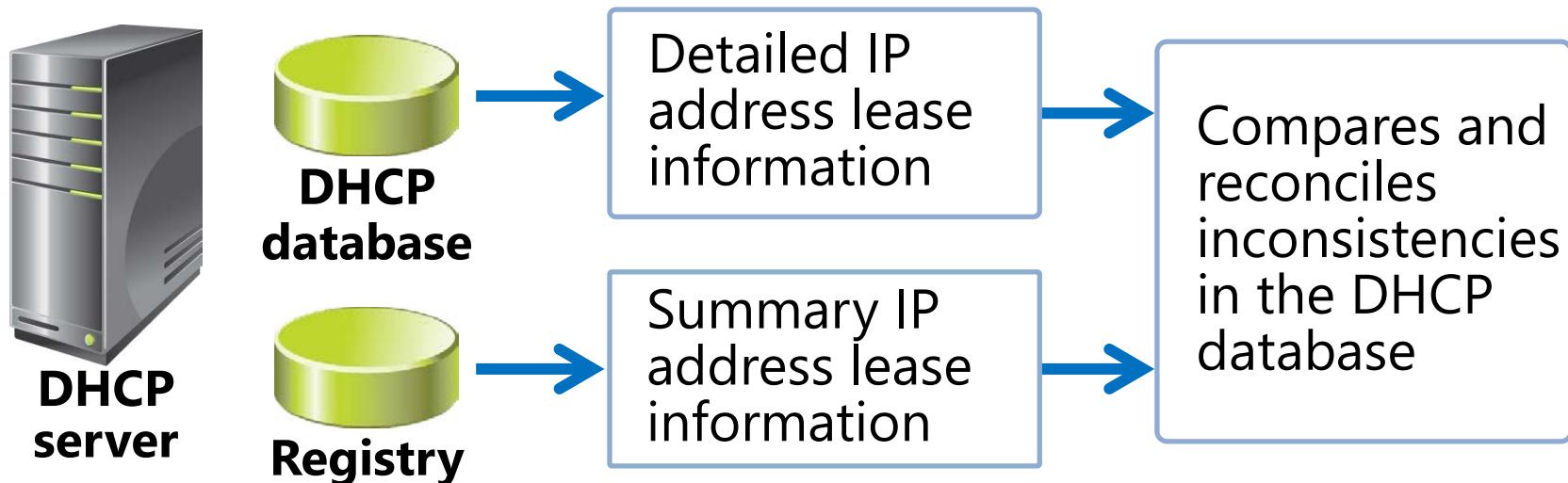
# Backing Up and Restoring a DHCP Database



In the event that the server hardware fails, the administrator can restore the DHCP database only from an offline storage location



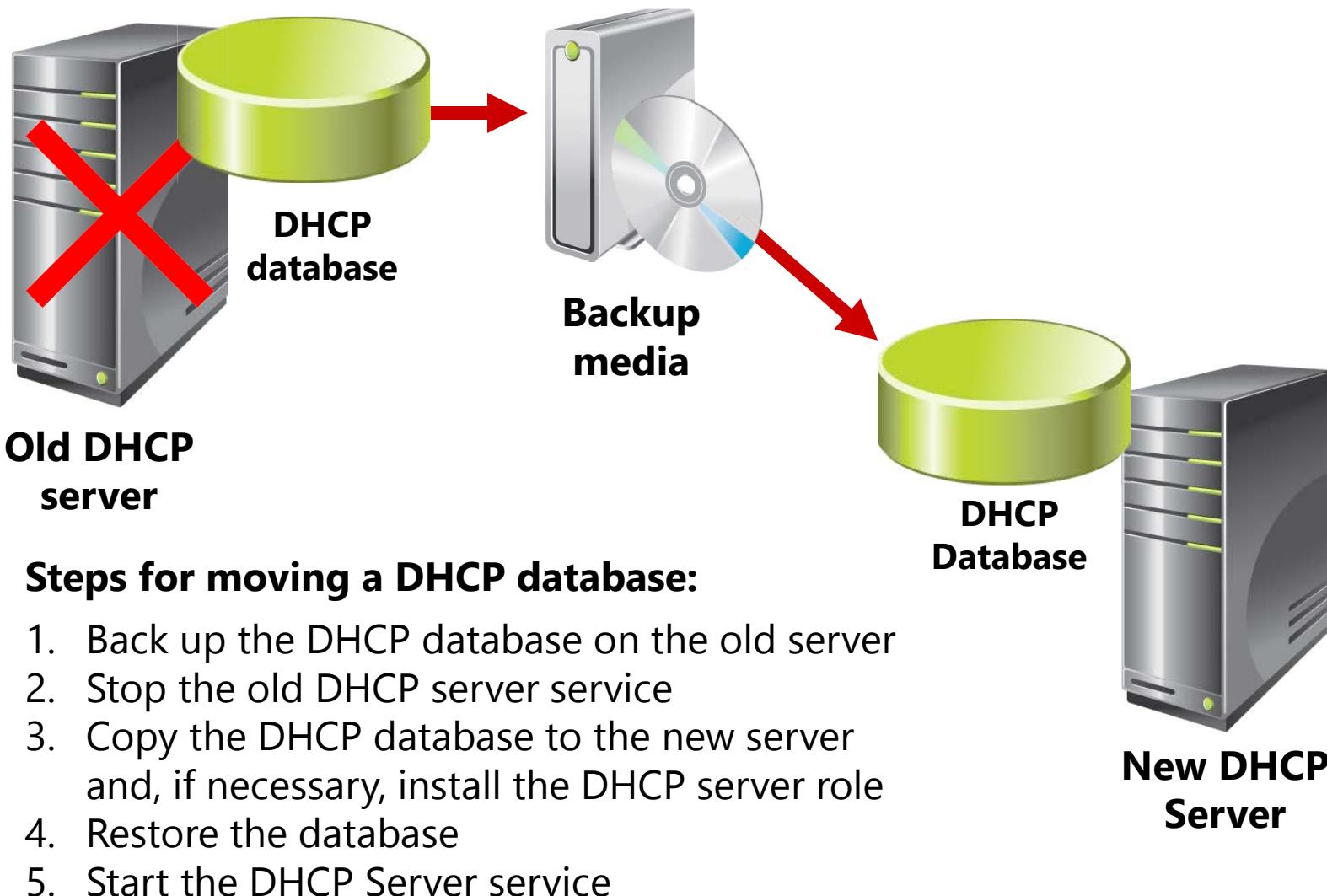
# Reconciling a DHCP Database



Example:

| Registry                           | DHCP database                        | After reconciliation                    |
|------------------------------------|--------------------------------------|-----------------------------------------|
| Client has IP address 192.168.1.34 | IP address 192.168.1.34 is available | Lease entry is created in DHCP database |

# Moving a DHCP Database



# Lesson 4: Securing and Monitoring DHCP

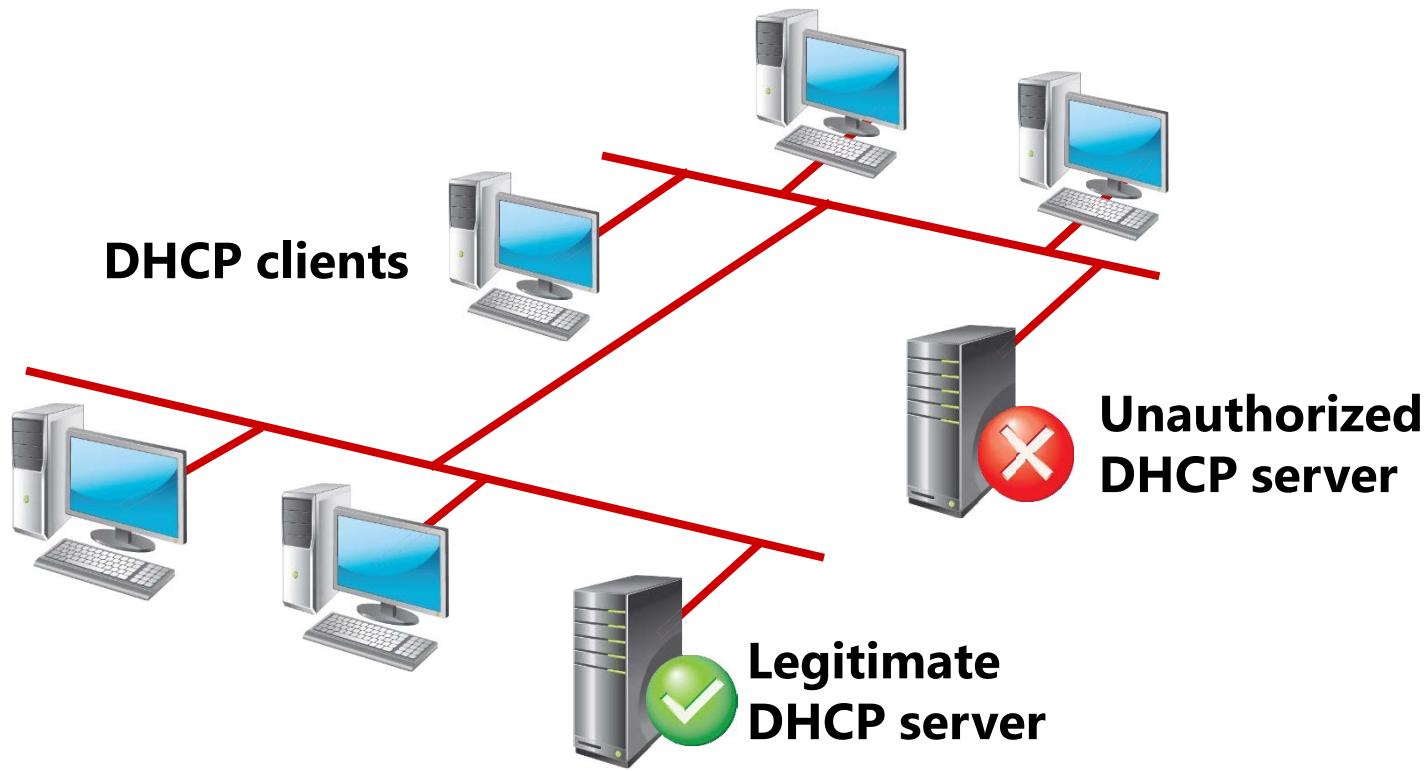
- Preventing an Unauthorized Computer from Obtaining a Lease
- Restricting Unauthorized, NonMicrosoft DHCP Servers from Leasing IP Addresses
- Delegating DHCP Administration
- What Are DHCP Statistics?
- What Is DHCP Audit Logging?
- Discussion: Common DHCP Issues

# Preventing an Unauthorized Computer from Obtaining a Lease

To prevent an unauthorized computer from obtaining a lease:

- Ensure that unauthorized users do not have physical or wireless access to your network
- Enable audit logging for every DHCP server on your network
- Regularly check and monitor audit log files
- Use 802.1X-enabled LAN switches or wireless access points to access the network
- Configure NAP to validate that a client computer is compliant with system health requirements

# Restricting Unauthorized, NonMicrosoft DHCP Servers from Leasing IP Addresses



To eliminate an unauthorized DHCP server, you must locate it and then either physically disable it or disable the DHCP service, to prevent it from communicating on the network

# Delegating DHCP Administration

To delegate who can administer the DHCP service:

- Limit the membership of the DHCP Administrators group
- Add users to the DHCP Users group if they need read-only access to the DHCP console

| Account                   | Permissions                                        |
|---------------------------|----------------------------------------------------|
| DHCP Administrators group | Can view and modify any data about the DHCP server |
| DHCP Users group          | Has read-only DHCP console access to the server    |

# What Are DHCP Statistics?

**DHCP statistics are collected at either the server level or the scope level**

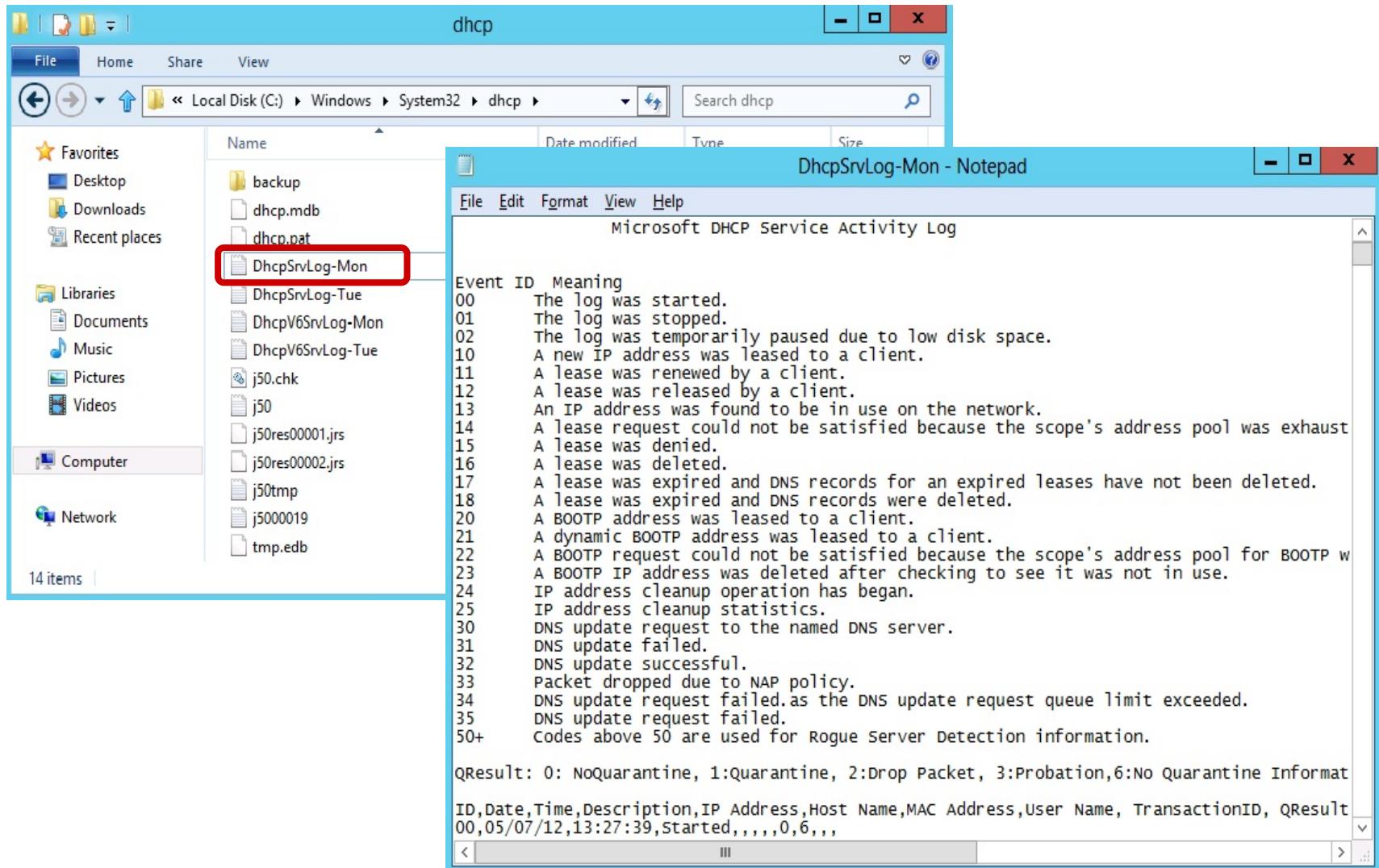


**DHCP  
Server**

| Description                  | Details                          |
|------------------------------|----------------------------------|
| Start Time                   | 5/7/2012 1:27:39 PM              |
| Up Time                      | 17 Hours, 37 Minutes, 10 Seconds |
| Discover                     | 673                              |
| Offer                        | 673                              |
| Delayed Offer                | 0                                |
| Request                      | 1321                             |
| Ack                          | 190                              |
| Nack                         | 600                              |
| Decline                      | 0                                |
| Release                      | 0                                |
| Total Scopes                 | 1                                |
| Scopes with delay configured | 0                                |
| Total Addresses              | 140                              |
| In Use                       | 7 (5%)                           |
| Available                    | 133 (95%)                        |

**Server Statistics window**

# What Is DHCP Audit Logging?



# Discussion: Common DHCP Issues

Common issues that can occur when you do not configure DHCP properly:

- Address conflicts
- Failure to obtain a DHCP address
- Address obtained from an incorrect scope
- DHCP database suffered data corruption or loss
- DHCP server has exhausted its IP address pool



**10 minutes**

# Lab: Implementing DHCP

- Exercise 1: Implementing DHCP
- Exercise 2: Implementing a DHCP Relay Agent  
(Optional Exercise)

## Logon Information

Virtual machines    **20410D-LON-DC1**  
                         **20410D-LON-SVR1**  
                         **20410D-LON-RTR**  
                         **20410D-LON-CL1**  
                         **20410D-LON-CL2**

User name           **Adatum\Administrator**  
Password           **Pa\$\$w0rd**

**Estimated Time: 60 minutes**

# Lab Scenario

A. Datum Corporation has an IT office and data center in London, which supports the London location and other locations as well. A. Datum has recently deployed a Windows 2012 Server infrastructure with Windows 8 clients.

You have recently accepted a promotion to the server support team. One of your first assignments is to configure the infrastructure service for a new branch office. As part of this assignment, you need to configure a DHCP server that will provide IP addresses and configuration to client computers. Servers are configured with static IP addresses and do not use DHCP.

# Lab Review

- What purpose does the DHCP scope have?
- How should you configure a computer to receive an IP address from the DHCP server?
- Why do you need MAC address for a DHCP server reservation?
- What information do you need to configure on a DHCP relay agent?

# Module Review and Takeaways

- Review Questions
- Best Practices
- Tools

# Microsoft® Official Course



## Module 7

### Implementing DNS

**Microsoft®**

# Module Overview

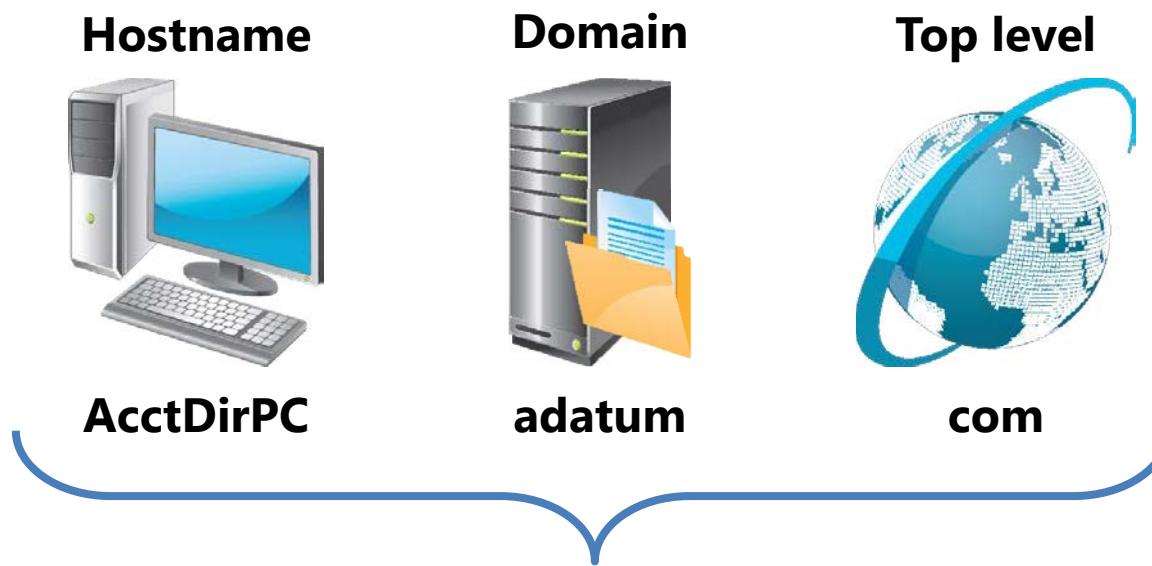
- Name Resolution for Windows Clients and Servers
- Installing a DNS Server
- Managing DNS Zones

# Lesson 1: Name Resolution for Windows Clients and Servers

- What Are the Computer Names Assigned to Computers?
- What Is DNS?
- DNS Zones and Records
- How Internet DNS Names Are Resolved
- What Is Split DNS?
- What Is Link-local Multicast Name Resolution?
- How a Client Resolves a Name
- Troubleshooting Name Resolution
- Demonstration: Troubleshooting Name Resolution

# What Are the Computer Names Assigned to Computers?

A ***hostname*** is a computer name that is added to a domain name and top level domain to make a fully qualified domain name (FQDN)



**Fully qualified domain name = AcctDirPC.adatum.com**

NetBIOS names are rarely used and are being deprecated in Windows operating systems

# What Is DNS?

DNS can be used to:

- Resolve host names to IP addresses
- Locate domain controllers and global catalog servers
- Resolve IP addresses to host names
- Locate mail servers during email delivery

# DNS Zones and Records

**A DNS zone is a specific portion of DNS namespace that contains DNS records**

Zone types:

- Forward lookup zone
- Reverse lookup zone

Resource records in forward lookup zones include:

- A, MX, SRV, NS, SOA, and CNAME

Resource records in reverse lookup zones include:

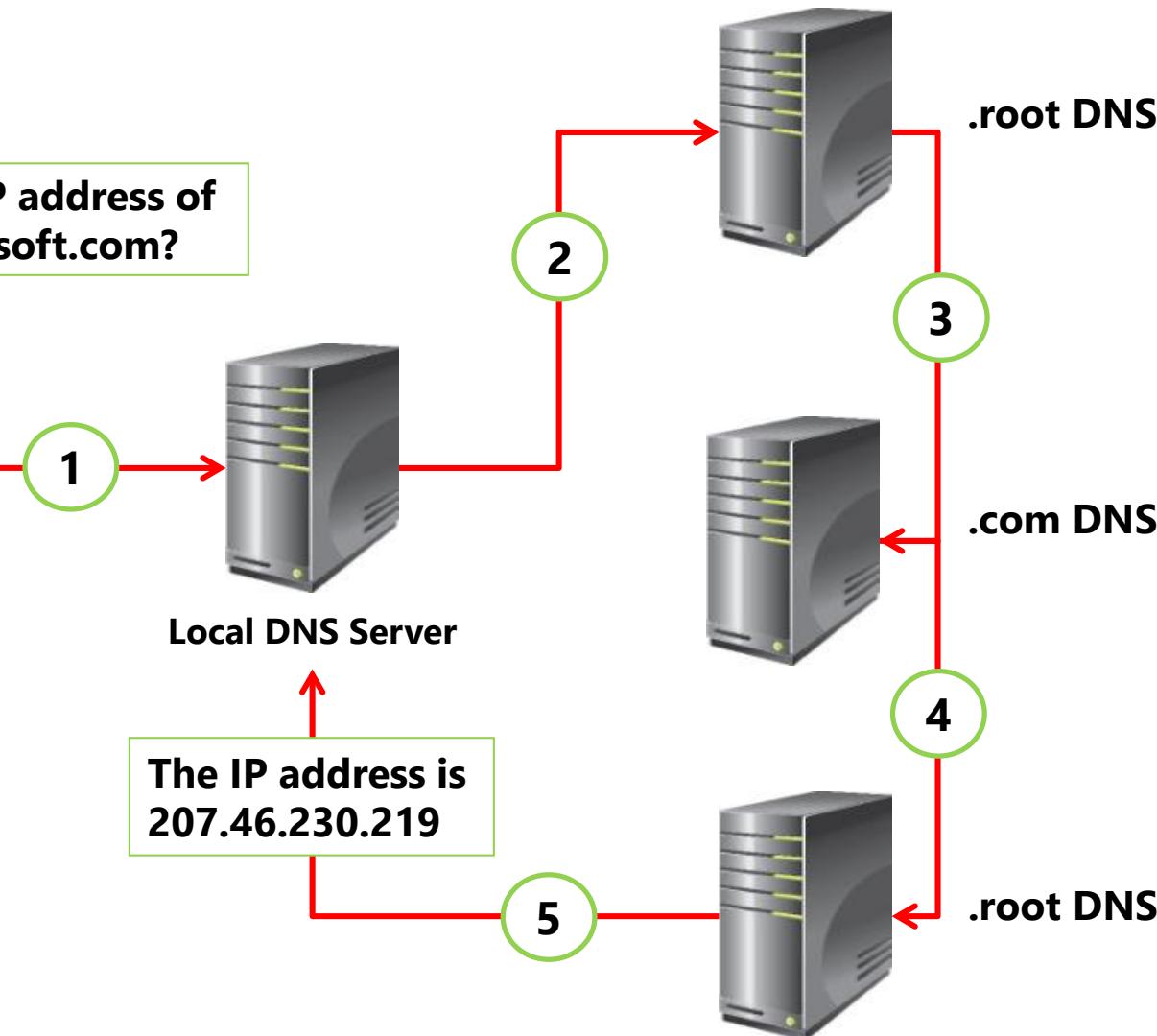
- PTR

# How Internet DNS Names Are Resolved

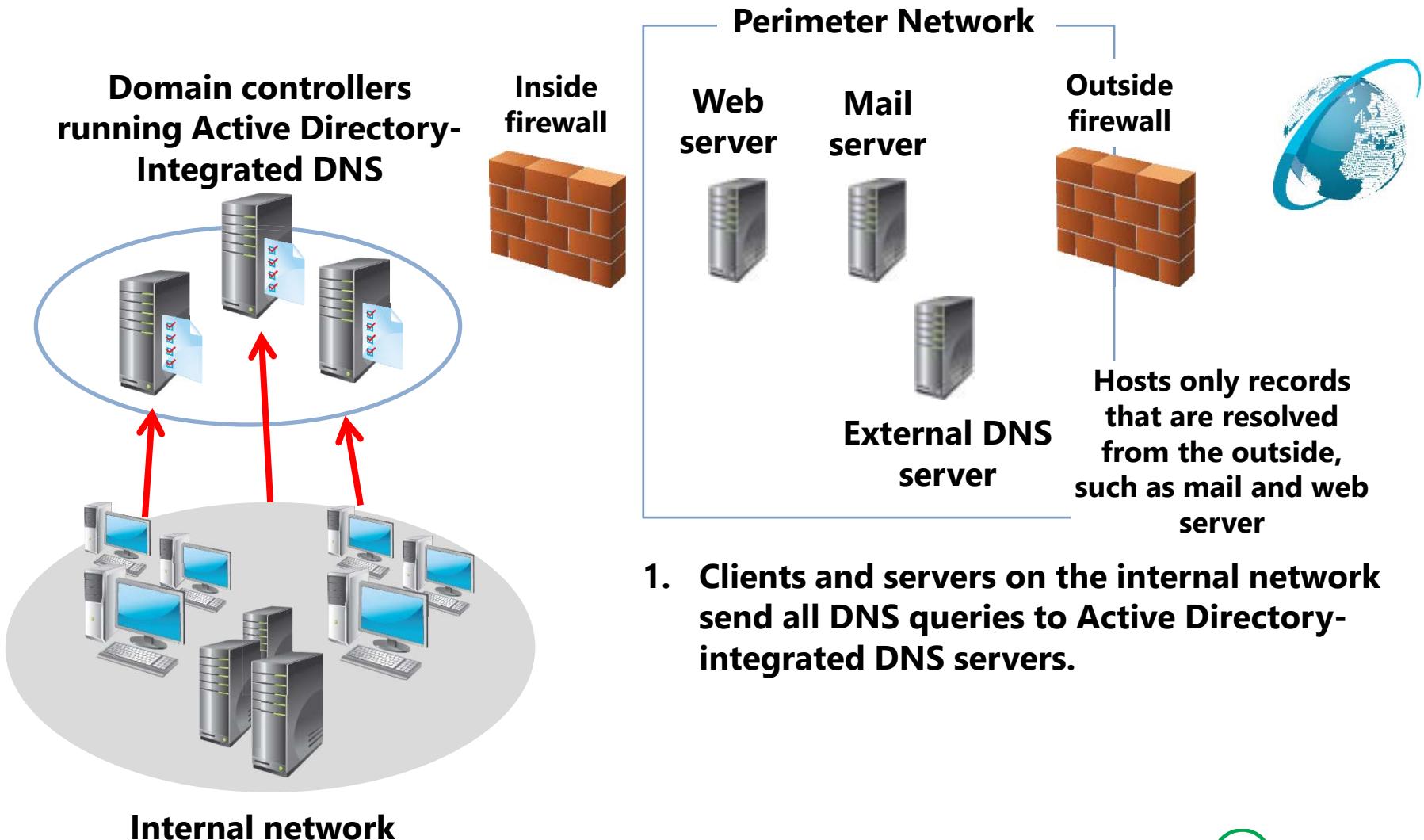
What is the IP address of  
www.microsoft.com?



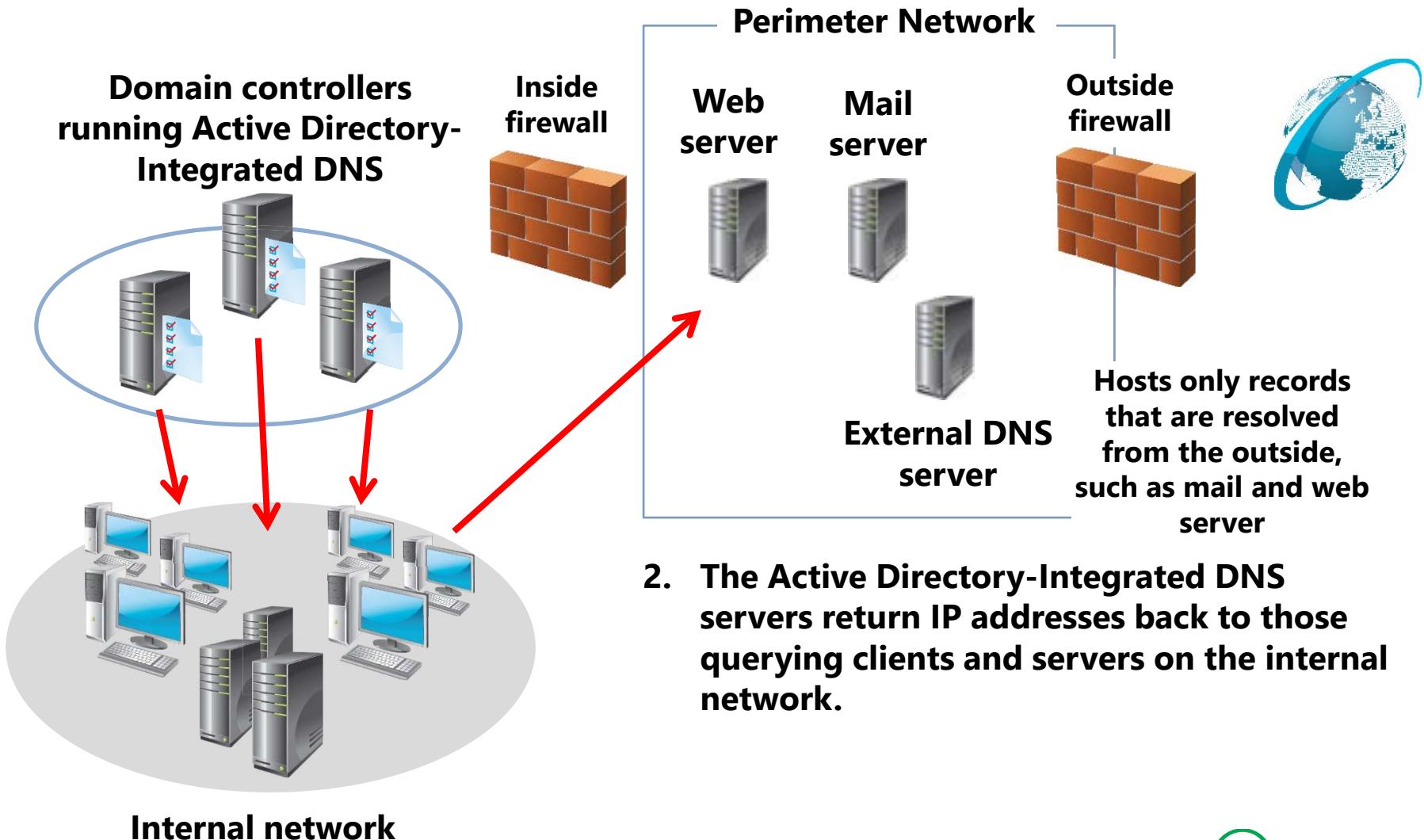
Workstation



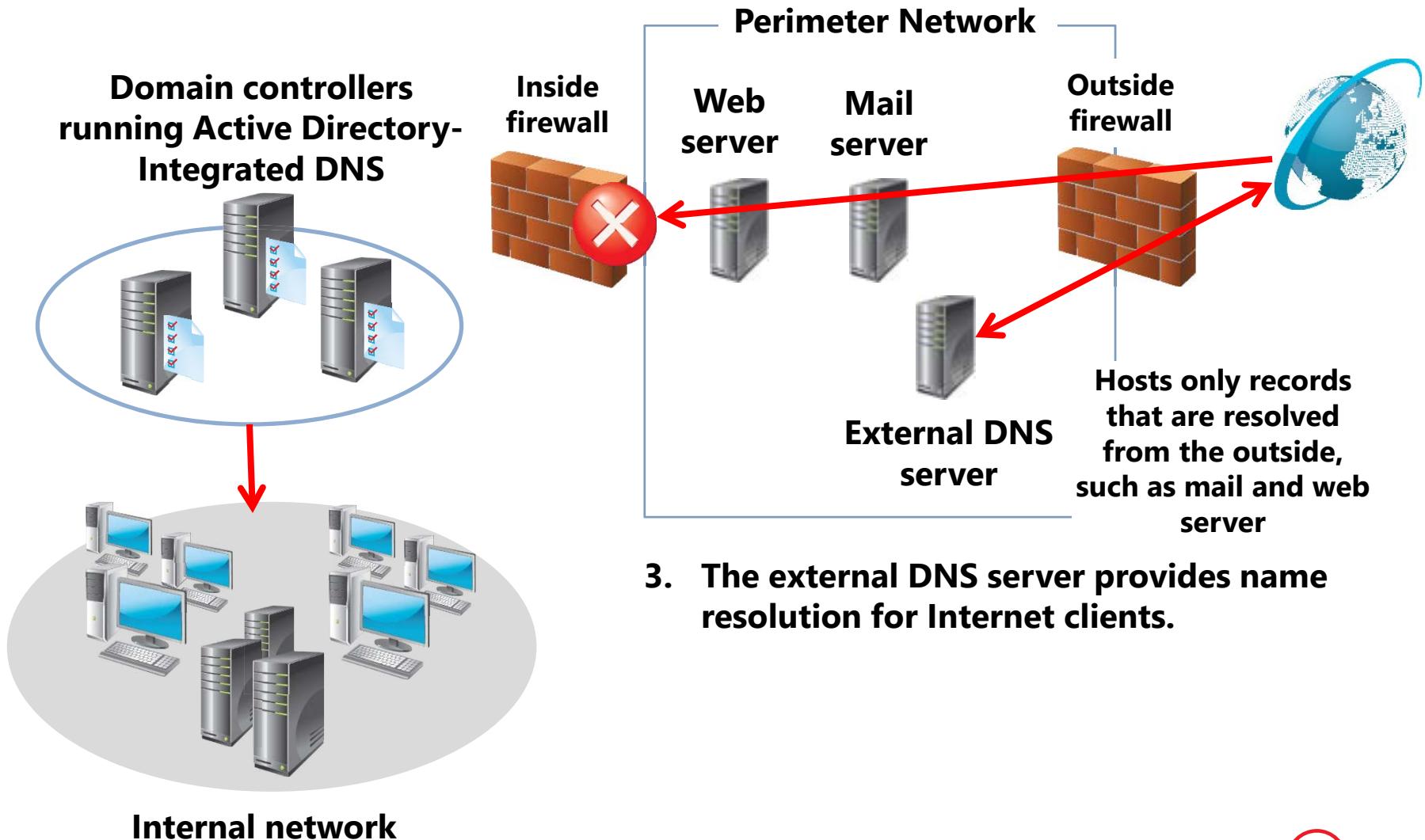
# What Is Split DNS?



# What Is Split DNS?



# What Is Split DNS?

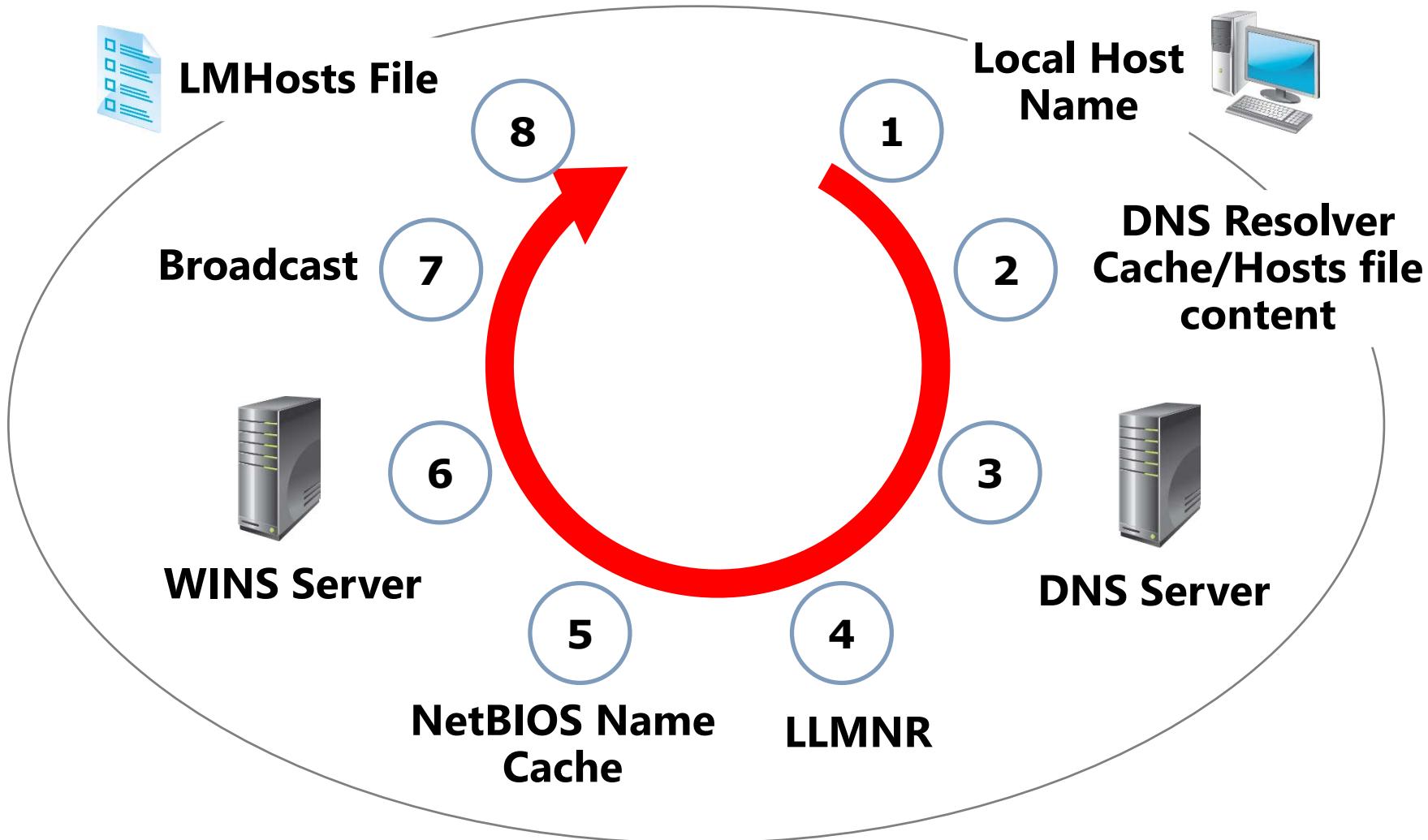


# What Is Link-local Multicast Name Resolution?

LLMNR is an additional method for name resolution that does not use DNS or WINS

- LLMNR is designed for IPv6
- Works only on Windows Vista, Windows Server 2008, and all newer Windows operating systems
- Network Discovery must be enabled
- Can be controlled via Group Policy

# How a Client Resolves a Name



# Troubleshooting Name Resolution

**A new Windows PowerShell DNS module with numerous cmdlets was introduced with Windows Server 2012 R2, including the Get-DNSServerStatistics cmdlet**

```
$statistics = Get-DnsServerStatistics -ZoneName Adatum.com
$statistics.ZoneQueryStatistics
$statistics.ZoneTransferStatistics
$statistics.ZoneUpdateStatistics
```

**Command-line tools to troubleshoot configuration issues:**

- Nslookup
- DNSCmd
- Dnslint
- Ipconfig

**The troubleshooting process:**

- Identify client DNS server with nslookup or Resolve-DnsName
- Communicate via ping
- Use nslookup to verify records

# Demonstration: Troubleshooting Name Resolution

In this demonstration, you will see how to:

- Use Windows PowerShell cmdlets to troubleshoot DNS
- Use command-line tools to troubleshoot DNS

# Lesson 2: Installing a DNS Server

- What Are DNS Queries?
- What Are Root Hints?
- What Is Forwarding?
- How DNS Server Caching Works
- How to Install the DNS Server Role
- Demonstration: Installing the DNS Server Role

# What Are DNS Queries?

- Queries are recursive or iterative
- DNS clients and DNS servers initiate queries
- DNS servers are authoritative or non-authoritative for a namespace
- An authoritative DNS server for the namespace either:
  - Returns the requested IP address
  - Returns an authoritative “No, that name does not exist”
- A non-authoritative DNS server for the namespace either:
  - Checks its cache
  - Uses forwarders
  - Uses root hints

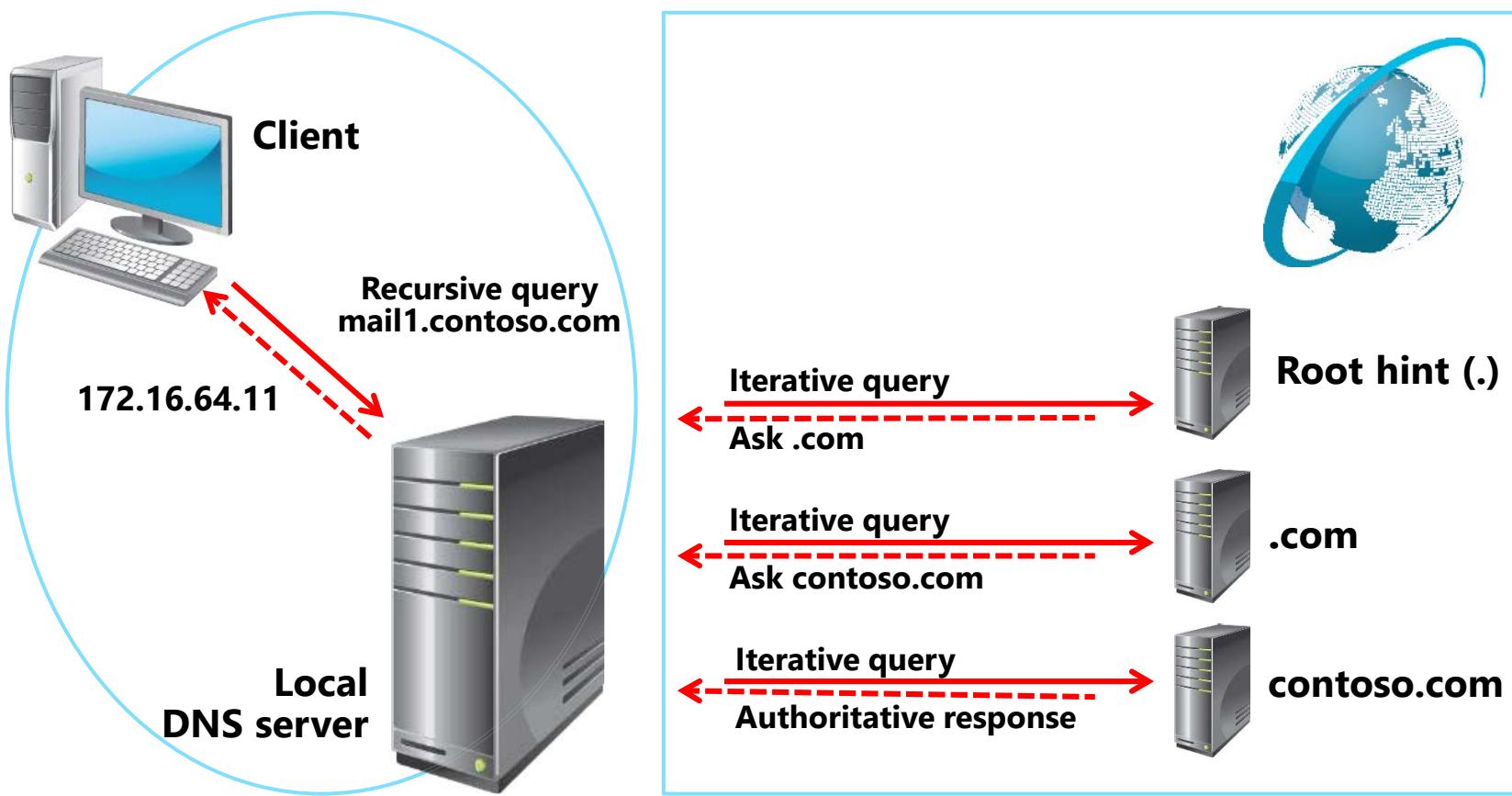


# What Are DNS Queries?

A **recursive query** is sent to a DNS server and requires a complete answer

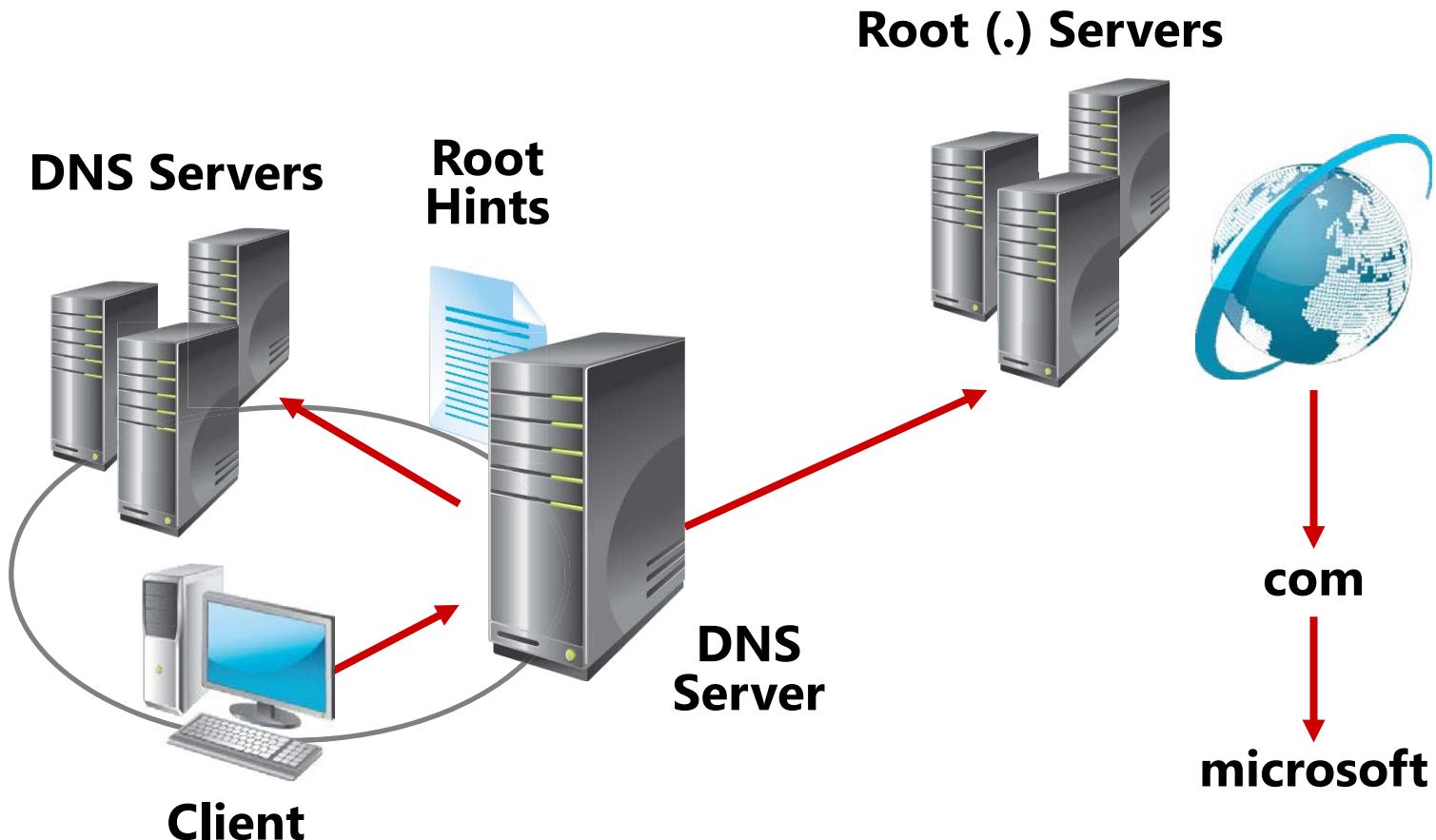


# What Are DNS Queries?



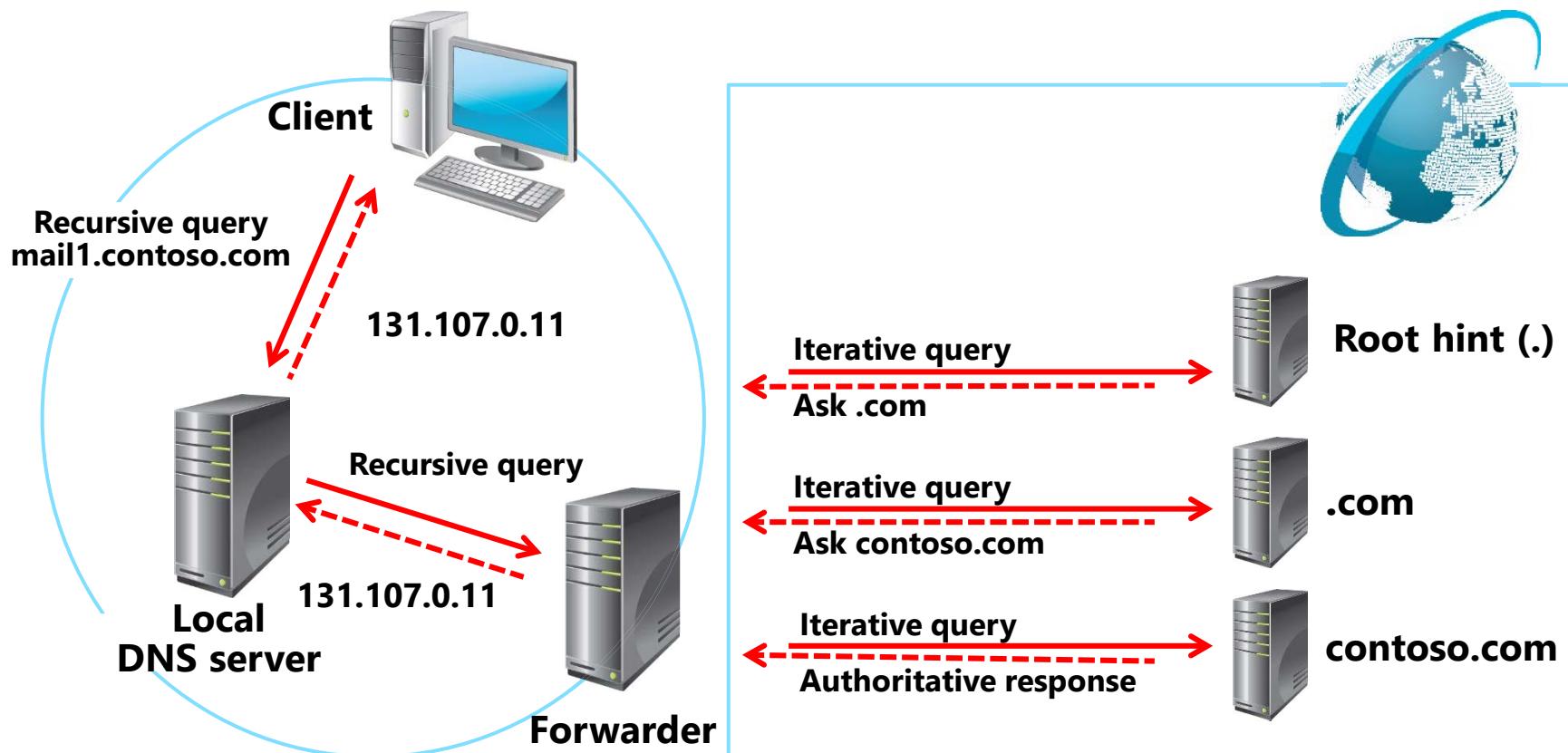
# What Are Root Hints?

***Root hints contain the IP addresses for DNS root servers***



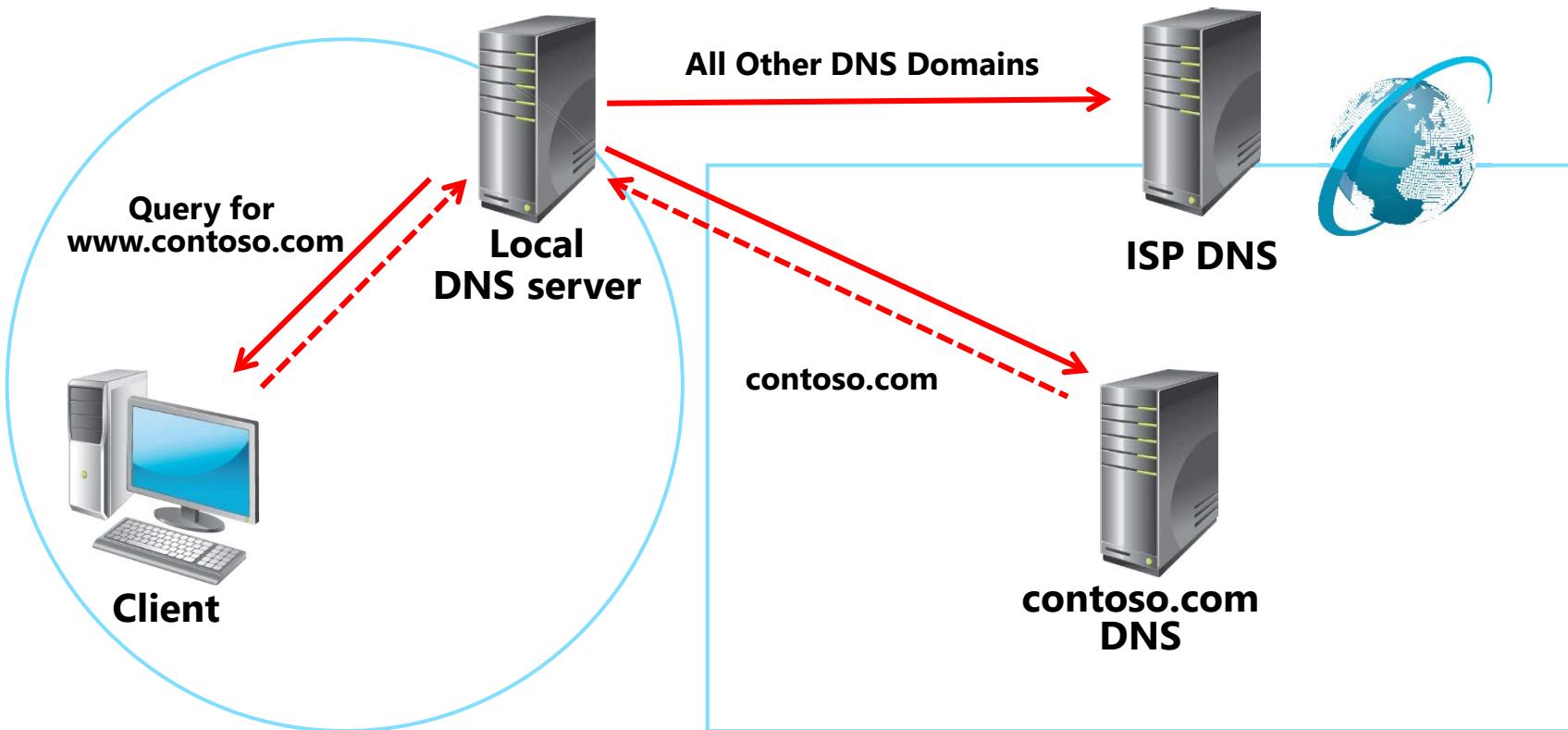
# What Is Forwarding?

A **forwarder** is a DNS server designated to resolve external or offsite DNS domain names



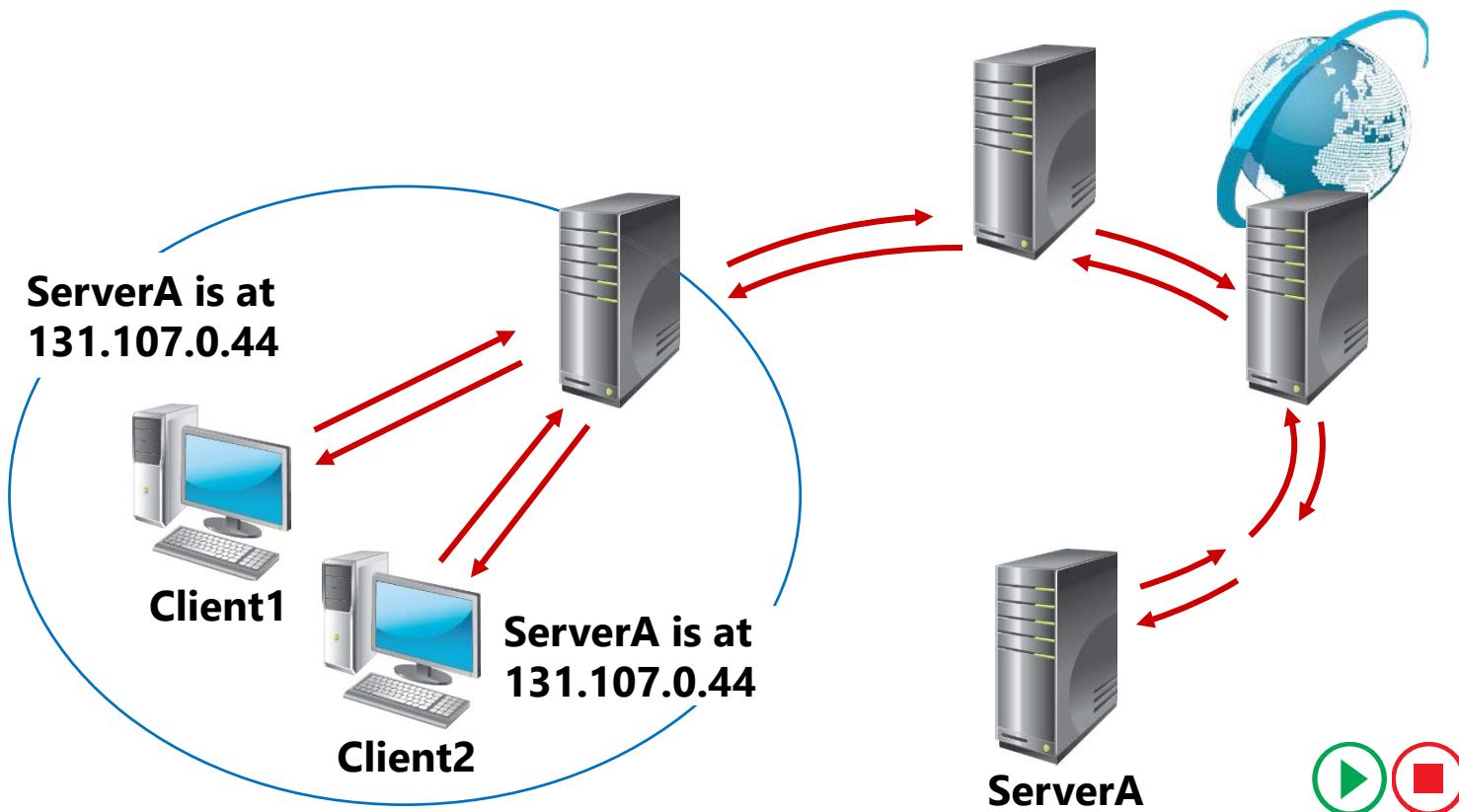
# What Is Forwarding?

***Conditional forwarding forwards requests using a domain name condition***



# How DNS Server Caching Works

| DNS server cache    |              |            |
|---------------------|--------------|------------|
| Host name           | IP address   | TTL        |
| ServerA.contoso.com | 131.107.0.44 | 28 seconds |



# How to Install the DNS Server Role

DNS server installation methods:

- Server Manager
- Active Directory Domain Services Installation Wizard

Tools available to manage DNS Server:

- DNS Manager snap-in
  - Server Manager
  - DNS Manager console (dnsmgmt.msc)
- DNSCmd command-line tool
- Windows Powershell
- Remote Server Administrative Tools

# Demonstration: Installing the DNS Server Role

In this demonstration, you will see how to:

- Install a second DNS server
- Create a forward lookup zone by using Windows PowerShell
- Configure forwarding



# Lesson 3: Managing DNS Zones

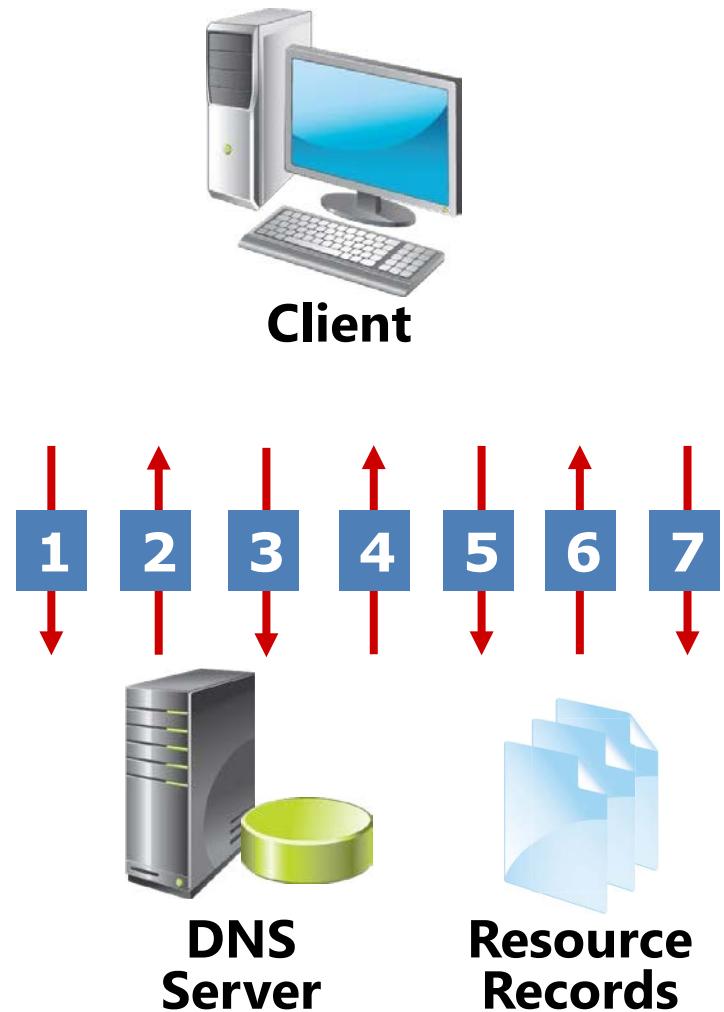
- What Are DNS Zone Types?
- What Are Dynamic Updates?
- What Are Active Directory–Integrated Zones?
- Demonstration: Creating an Active Directory–Integrated Zone

# What Are DNS Zone Types?

| <b>Zones</b>                | <b>Description</b>                                                    |
|-----------------------------|-----------------------------------------------------------------------|
| Primary                     | Read/write copy of a DNS database                                     |
| Secondary                   | Read-only copy of a DNS database                                      |
| Stub                        | Copy of a zone that contains only records used to locate name servers |
| Active Directory-integrated | Zone data is stored in AD DS rather than in zone files                |

# What Are Dynamic Updates?

1. The client sends an SOA query
2. The DNS server returns an SOA resource record
3. The client sends dynamic update request(s) to identify the primary DNS server
5. The DNS server responds that it can perform an update
6. The client sends unsecured update to the DNS server
7. If the zone permits only secure updates, the update is refused
8. The client sends a secured update to the DNS server



# What Are Active Directory–Integrated Zones?

Benefits of an Active Directory–integrated zone:

- Allows multi-master writes to zone
- Replicates DNS zone information by using AD DS replication
  - Leverages efficient replication topology
  - Uses efficient incremental updates for Active Directory replication processes
- Enables secure dynamic updates
- Delegates zones, domains, resource records for increased security

# Demonstration: Creating an Active Directory–Integrated Zone

In this demonstration, you will see how to:

- Promote a server as a domain controller
- Create an Active Directory–integrated zone
- Create a record
- Verify replication to a second DNS server

# Lab: Implementing DNS

- Exercise 1: Installing and Configuring DNS
- Exercise 2: Creating Host Records in DNS
- Exercise 3: Managing the DNS Server Cache

## Logon Information

Virtual machines    **20410D-LON-DC1**  
                         **20410D-LON-SVR1**  
                         **20410D-LON-CL1**

User name           **Adatum\Administrator**

Password           **Pa\$\$w0rd**

**Estimated Time: 60 minutes**

## Lab Scenario

Your manager has asked you to configure the domain controller in the branch office as a DNS server. You also have been asked to create some new host records to support a new app that is being installed. Finally, you need to configure forwarding on the DNS server in the branch office to support Internet name resolution.

# Lab Review

- Can you install the DNS server role on a server that is not a domain controller? If yes, are there any limitations?
- What is the most common way to carry out Internet name resolution on a local DNS?
- How can you browse the content of the DNS resolver cache on a DNS server?

# Module Review and Takeaways

- Review Questions
- Best Practices
- Common Issues and Troubleshooting Tips
- Tools

# Microsoft® Official Course



Module 8

Implementing IPv6

**Microsoft®**

# Module Overview

- Overview of IPv6
- IPv6 Addressing
- Coexistence with IPv4
- IPv6 Transition Technologies

# Lesson 1: Overview of IPv6

- Benefits of IPv6
- Differences Between IPv4 and IPv6
- IPv6 Address Format

# Benefits of IPv6

Benefits of IPv6 include:

- Larger address space
- Hierarchical addressing and routing infrastructure
- Stateless and stateful address configuration
- Required support for IPsec
- End-to-end communication
- Required support for QoS
- Improved support for single-subnet environments
- Extensibility

# Differences Between IPv4 and IPv6

| Feature                           | IPv4                                  | IPv6                                                           |
|-----------------------------------|---------------------------------------|----------------------------------------------------------------|
| Fragmentation                     | Performed by routers and sending host | Performed only by sending host                                 |
| Address resolution                | Broadcast ARP request frames          | Multicast Neighbor Solicitation messages                       |
| Manage multicast group membership | IGMP                                  | Multicast listener discovery                                   |
| Router discovery                  | ICMP Router Discovery (optional)      | ICMPv6 Router Solicitation and Router Advertisement (required) |
| DNS host records                  | A records                             | AAAA records                                                   |
| DNS reverse lookup zones          | IN-ADDR.ARPA                          | IP6.ARPA                                                       |
| Minimum packet size               | 576 bytes                             | 1280 bytes                                                     |

# IPv6 Address Format

- 128-bit address in binary:

**001000000000001000011011011000000000000  
0000001011100110110000010101010100000000  
11111111111110001010001001110001011010**

- 128-bit address divided into 16-bit blocks:

**00100000000001 00001101101100  
00000000000000 001011100111011  
0000001010101010 000000001111111  
1111111000101000 1001110001011010**

- Each 16-bit block converted to hex (base 16):

**2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A**

- Further simplified by removing leading zeros:

**2001:DB8:0:2F3B:2AA:FF:FE28:9C5A**



# IPv6 Address Format

[0010][1111][0011][1011]



# IPv6 Address Format

[0010][1111][0011][1011]

8 4 2 1

[0 0 1 0]

$$0+0+2+0=2$$

[1 1 1 1]

$$8+4+2+1=F$$

[0 0 1 1]

$$0+0+2+1=3$$

[1 0 1 1]

$$8+0+2+1=B$$



# IPv6 Address Format

[0010][1111][0011][1011]

8 4 2 1

[0 0 1 0]

$$0+0+2+0=2$$

[1 1 1 1]

$$8+4+2+1=F$$

[0 0 1 1]

$$0+0+2+1=3$$

[1 0 1 1]

$$8+0+2+1=B$$

= 2F3B



# IPv6 Address Format

- 128-bit address in binary:

**001000000000001000011011011000000000000  
00000010111001110110000010101010100000000  
11111111111110001010001001110001011010**

- 128-bit address divided into 16-bit blocks:

**00100000000001 00001101101100  
00000000000000 001011100111011  
0000001010101010 000000001111111  
1111111000101000 1001110001011010**

- Each 16-bit block converted to hex (base 16):

**2001:0DB8:0000:2F3B:02AA:00FF:FE28:9C5A**

- Further simplified by removing leading zeros:

**2001:DB8:0:2F3B:2AA:FF:FE28:9C5A**



# Lesson 2: IPv6 Addressing

- IPv6 Address Structure
- Global Unicast Addresses
- Unique Local Unicast Addresses
- Link-Local Unicast Addresses
- Autoconfiguring IPv6 Addresses
- Demonstration: Configuring IPv6 Client Settings

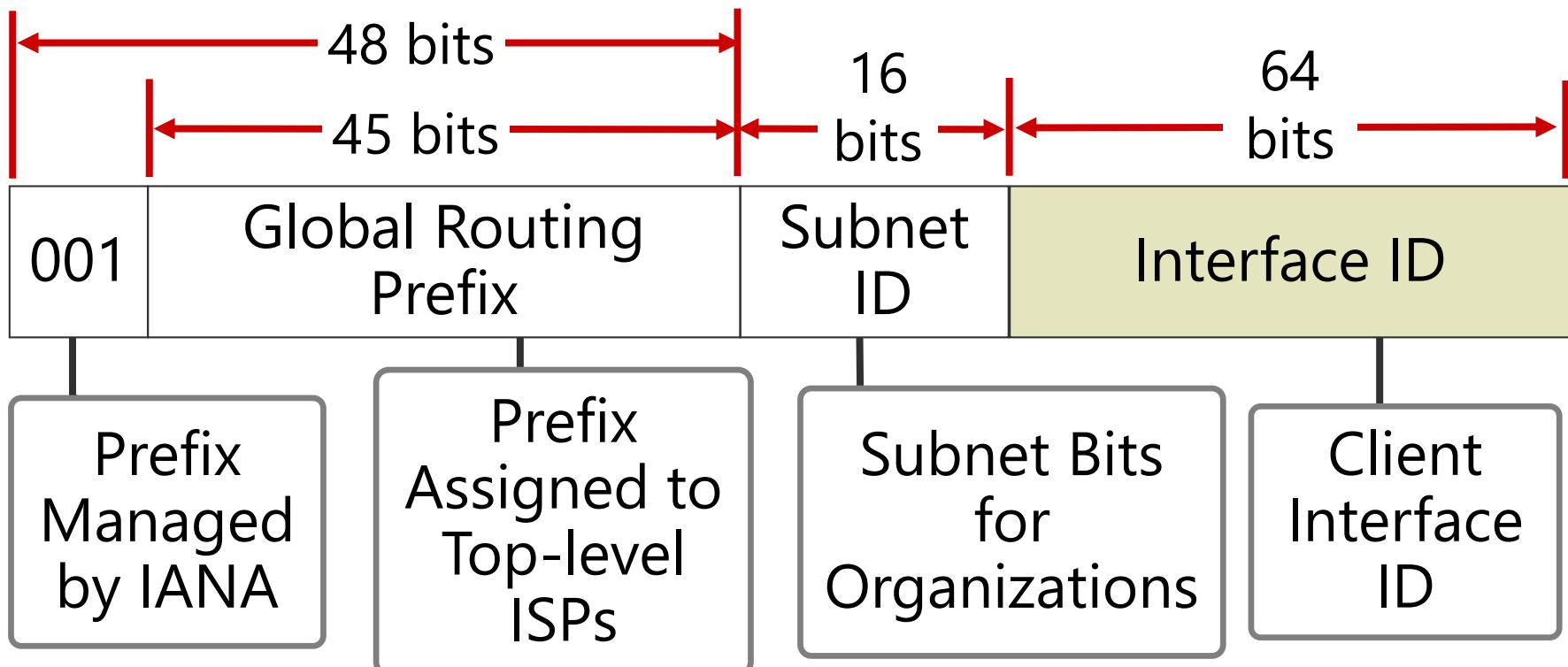
# IPv6 Address Structure

- The number of network bits is defined by the prefix
- Each host has 64-bits allocated to the interface identifier

| Type of address | IPv4 address    | IPv6 address            |
|-----------------|-----------------|-------------------------|
| Unspecified     | 0.0.0.0         | ::                      |
| Loopback        | 127.0.0.1       | ::1                     |
| Autoconfigured  | 169.254.0.0/16  | FE80::/64               |
| Broadcast       | 255.255.255.255 | Uses multicasts instead |
| Multicast       | 224.0.0.0/4     | FF00::/8                |

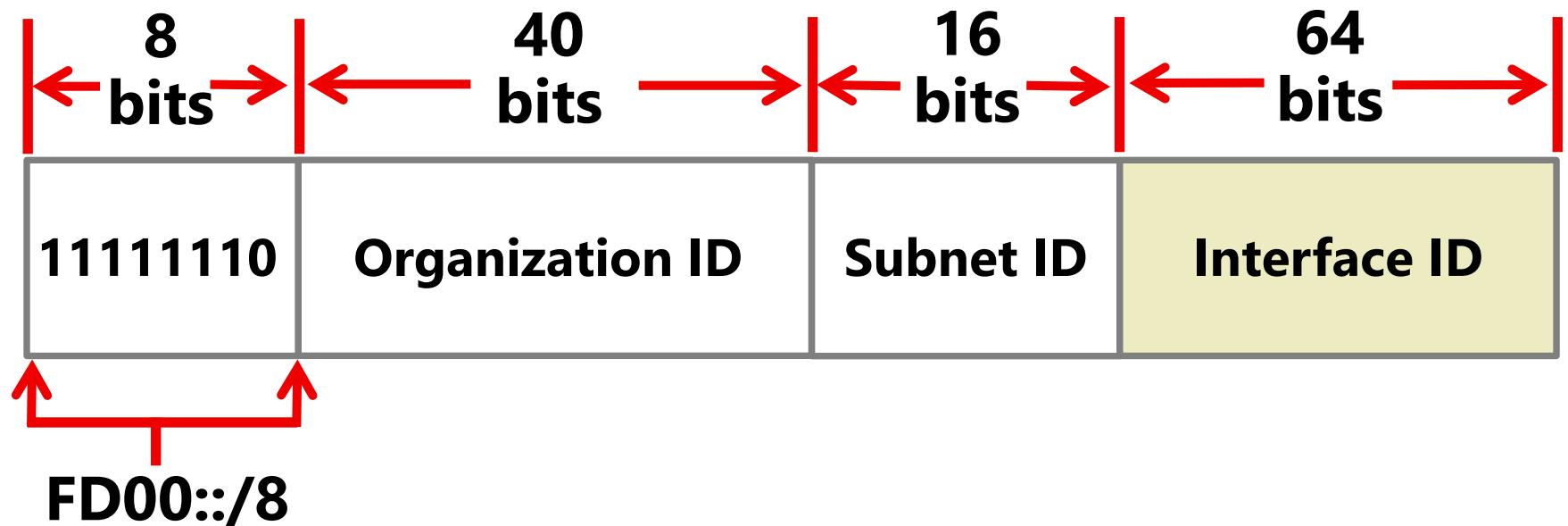
# Global Unicast Addresses

- Are routable on the Ipv6 Internet
- Allocate 16 bits for internal subnetting
- Begin with 2 or 3 (2000::/3)



# Unique Local Unicast Addresses

- Are equivalent to IPv4 private addresses
- Require the organization ID to be randomly generated
- Allocates 16 bits for internal subnetting

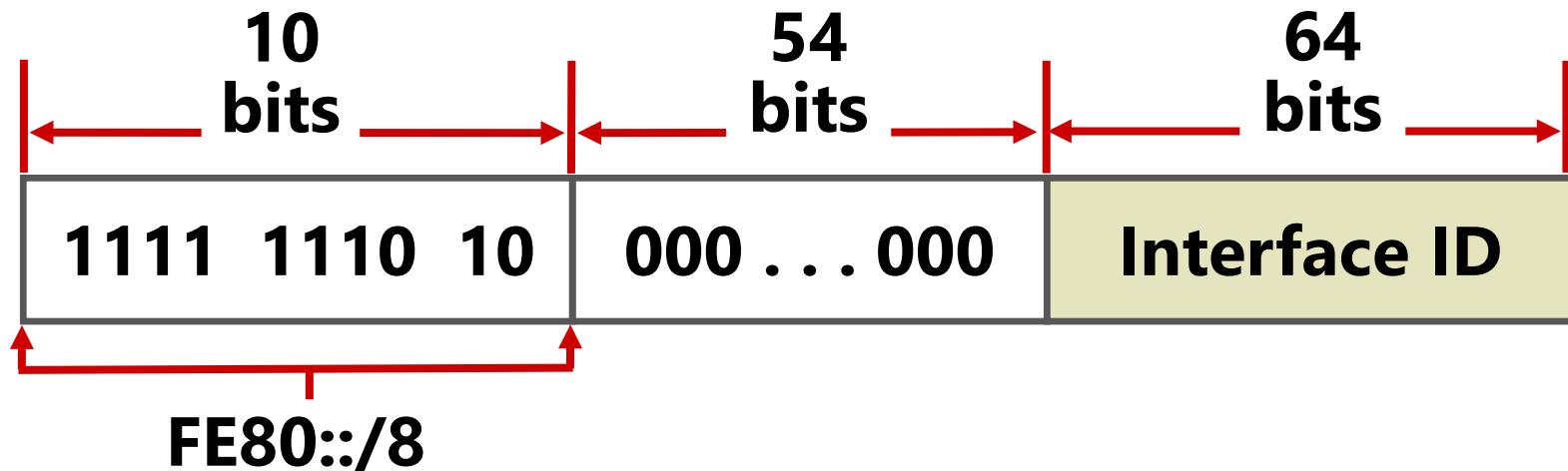


# Link-Local Unicast Addresses

- Are automatically generated on all IPv6 hosts
- Are similar to IPv4 APIPA addresses
- Are sometimes used in place of broadcast messages
- Include a zone ID that identifies the interface

Examples: fe80::2b0:d0ff:fee9:4143%3

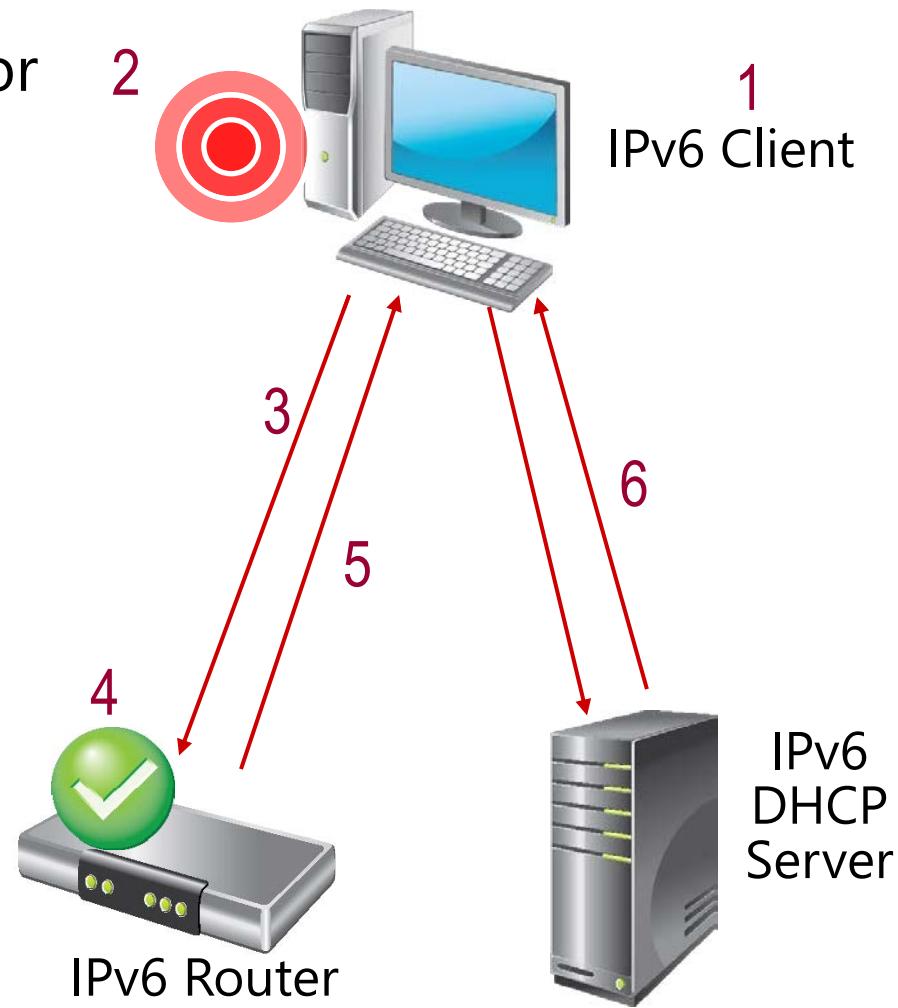
fe80::94bd:21cf:4080:e612%2



# Autoconfiguring IPv6 Addresses

Address autoconfiguration for IPv6 is a six-step process:

- 1 Derive a link-local address
- 2 Check for address conflicts by using neighbor solicitation
- 3 Check for a router on the network
- 4 Check the router for prefixes
- 5 Add prefixes
- 6 If Managed or Other flag set, check DHCPv6



# Autoconfiguring IPv6 Addresses

The six-step process:

1 Derive a link-local address

- fe80::d593:e1e:e612:53e4%10

2 Check for address conflicts by using neighbor solicitation

3 Check for a router on the network

- Router configuration search

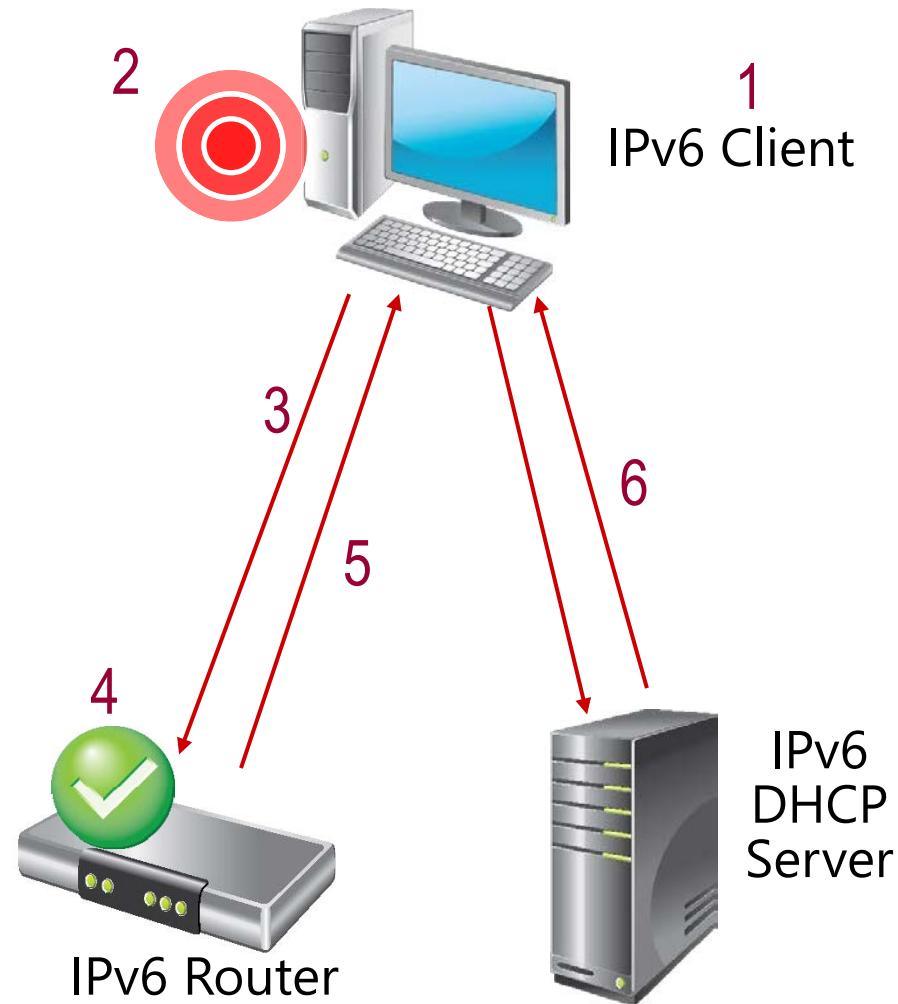
4 Check the router for prefixes

5 Add prefixes

- Additional router prefixes

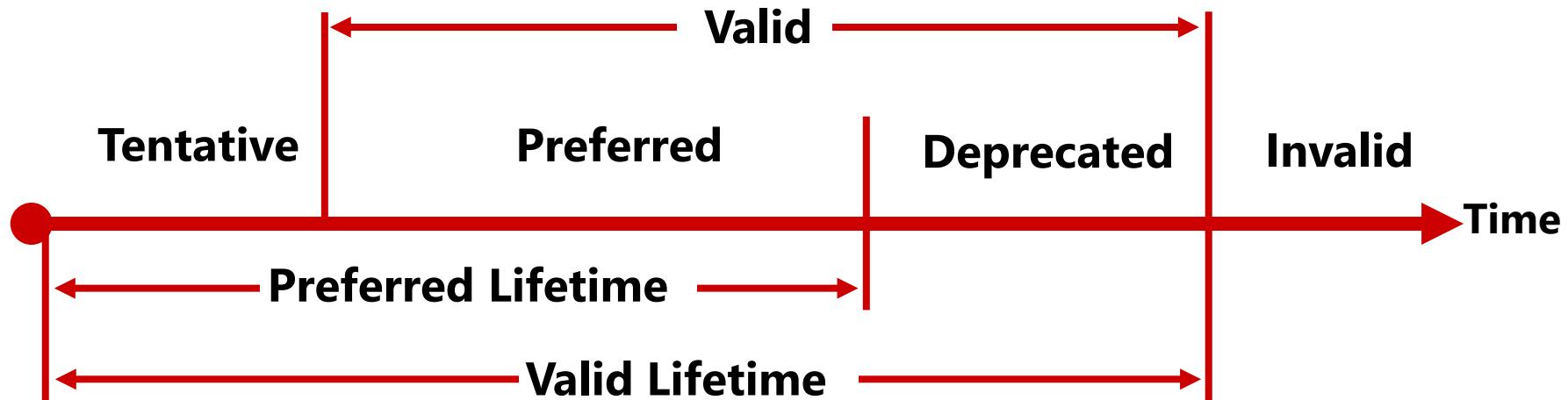
6 If Managed or Other flag set, check DHCPv6

- DHCPv6 information received



# Autoconfiguring IPv6 Addresses

## Autoconfigured IP Timeline



# Demonstration: Configuring IPv6 Client Settings

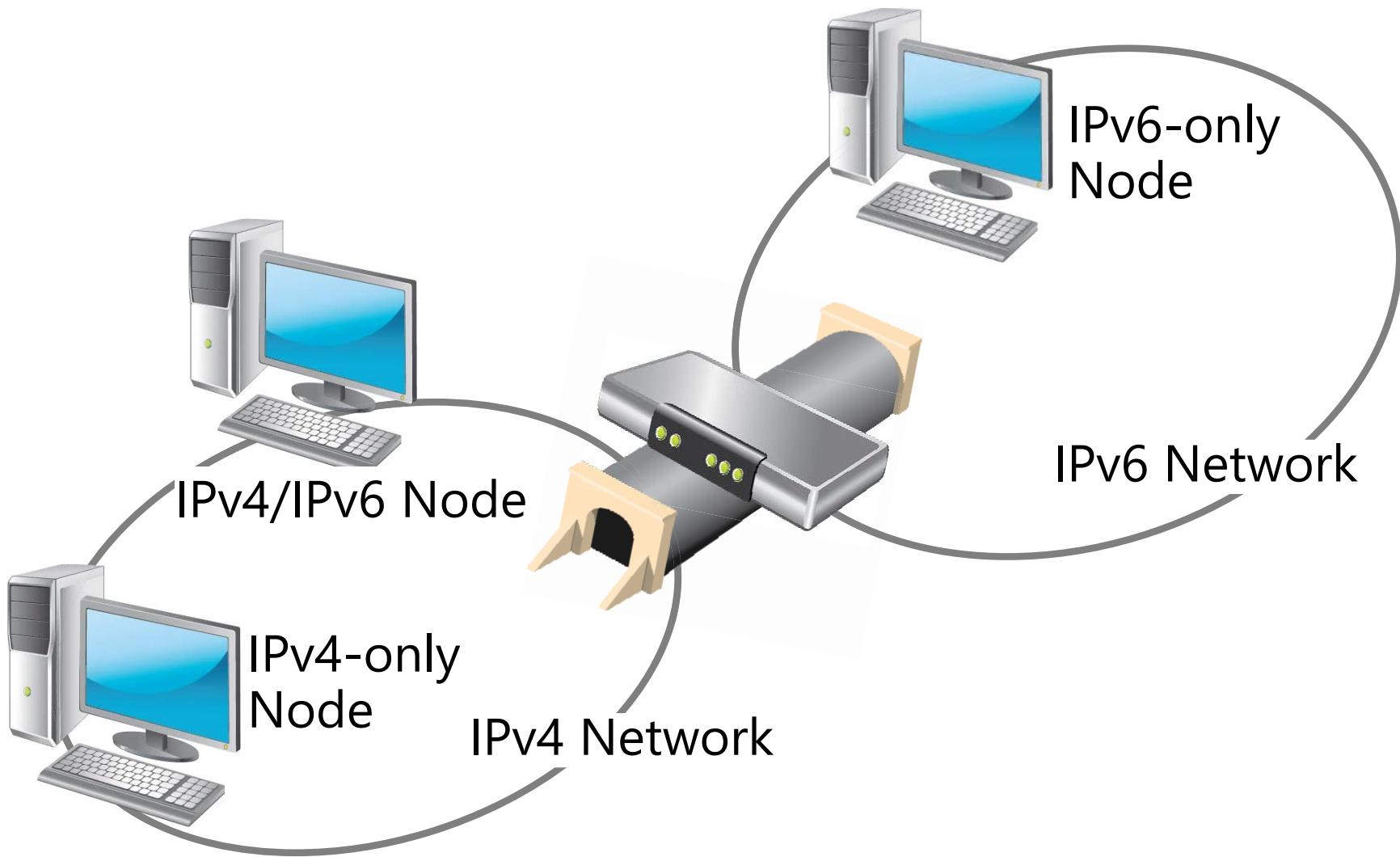
In this demonstration, you will see how to:

- View IPv6 configuration by using **ipconfig** and **Get-NetIPAddress**
- Configure IPv6 on a domain controller and a server
- Verify IPv6 communication is functional

# Lesson 3: Coexistence with IPv4

- What Are Node Types?
- IPv4 and IPv6 Coexistence
- Demonstration: Configuring DNS to Support IPv6
- What Is IPv6 over IPv4 Tunneling?

# What Are Node Types?



# IPv4 and IPv6 Coexistence

Windows Server 2012 uses a dual IP layer architecture that supports IPv4 and IPv6 in a single protocol stack

DNS records required for coexistence are:

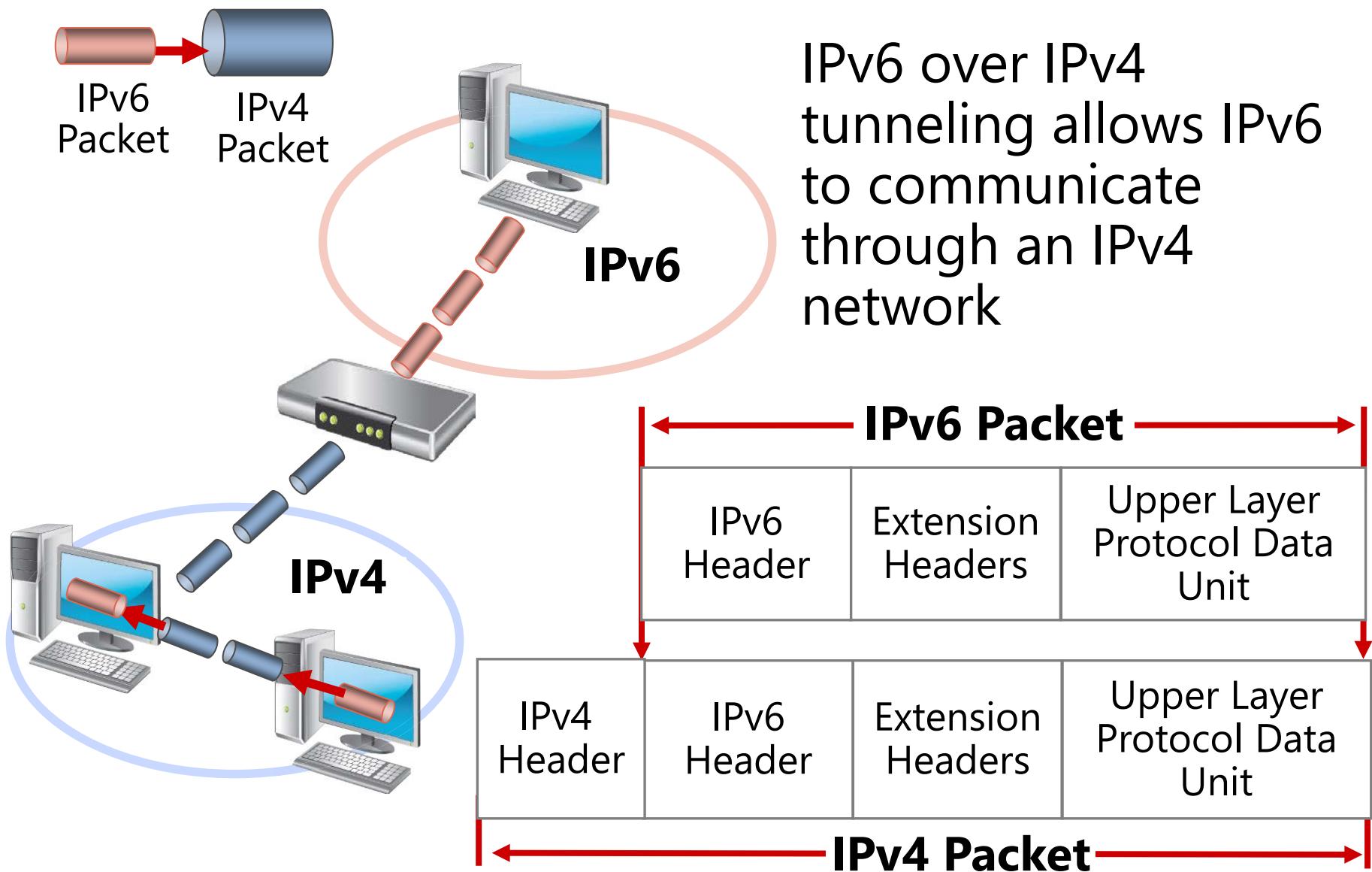
- Host (A) resource records for IPv4 nodes
- IPv6 host (AAAA) resource records
- Reverse lookup pointer (PTR) resource records for IPv4 and IPv6 nodes

# Demonstration: Configuring DNS to Support IPv6

In this demonstration, you will see how to:

- Configure an IPv6 host (AAAA) resource record for an IPv6 address
- Verify name resolution for an IPv6 host (AAAA) resource record

# What Is IPv6 over IPv4 Tunneling?



# Lesson 4: IPv6 Transition Technologies

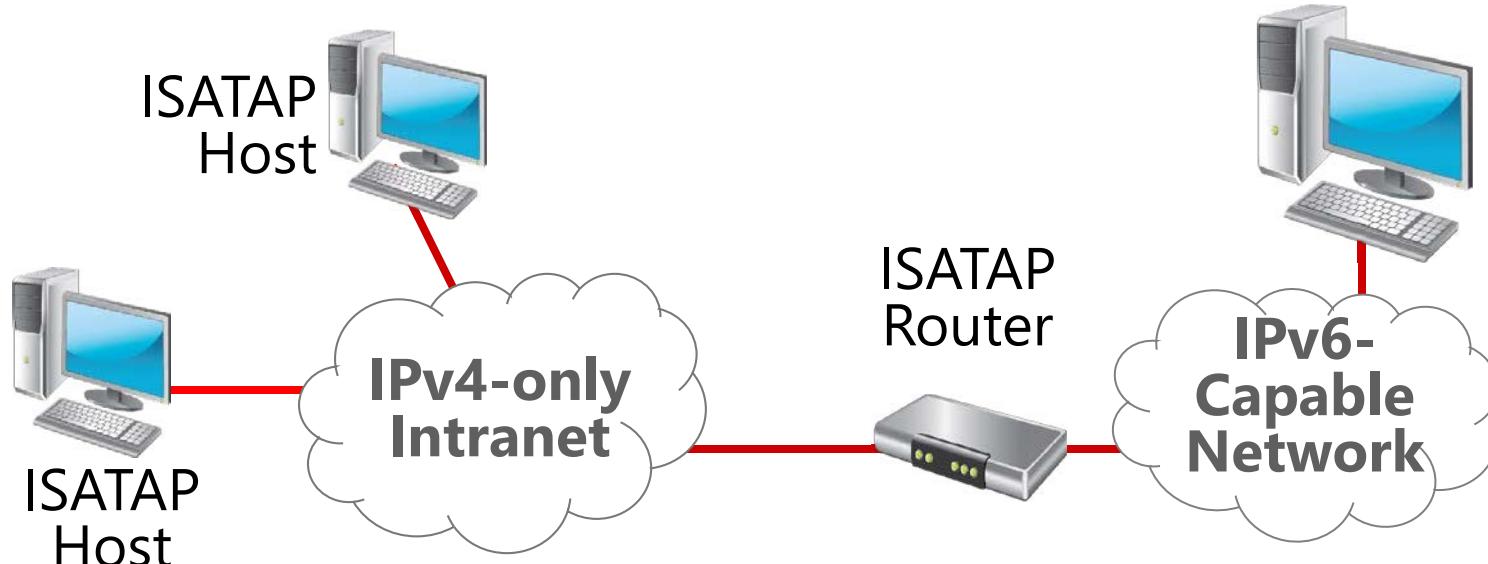
- What Is ISATAP?
- What Is 6to4?
- What Is Teredo?
- What Is PortProxy?
- Process for Transitioning to IPv6

# What Is ISATAP?

- Allows IPv6 communication over an IPv4 intranet
- Can be enabled by configuring an ISATAP host record
- Connects all nodes to a single IPv6 network
- Uses the IPv4 address as part of the IPv6 address

Private address: FD00::0:5EFE:192.168.137.133

Public address: 2001:db8::200:5EFE:131.107.137.133

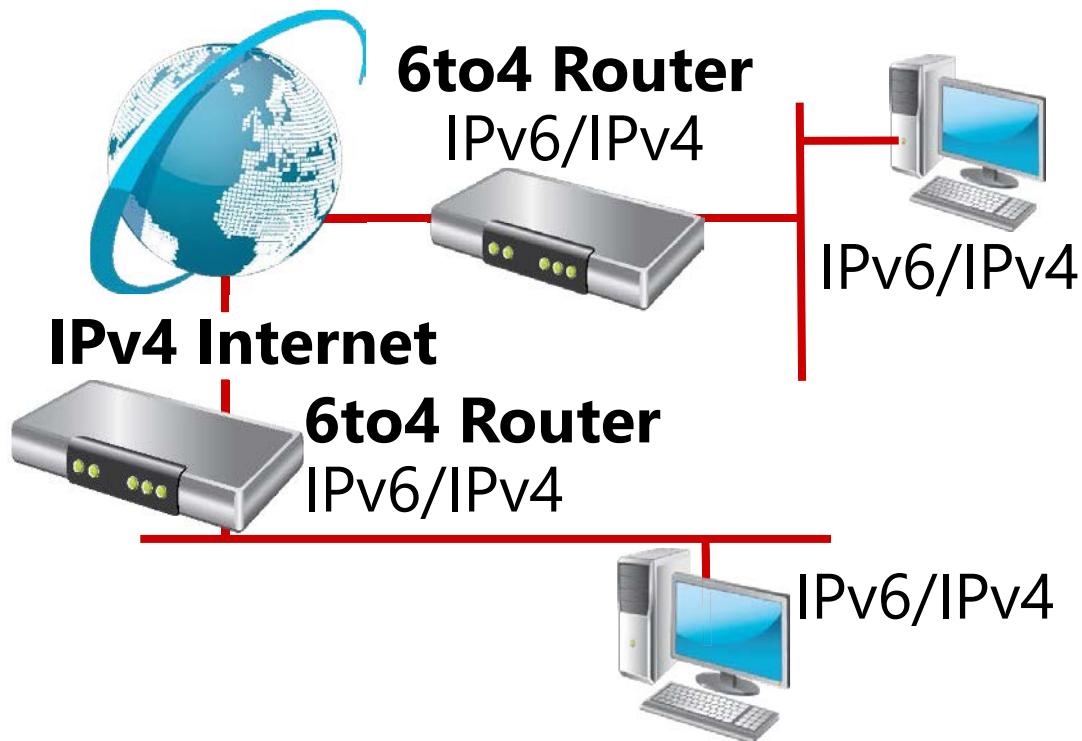


# What Is 6to4?

- Provides IPv6 connectivity over the IPv4 Internet
- Works between sites or from host to site
- Is not suitable for scenarios using NAT
- Uses the following network address format:  
2002:WWXX:YYZZ:Subnet\_ID::/64

To enable  
Windows Server  
2012 as a 6to4  
router:

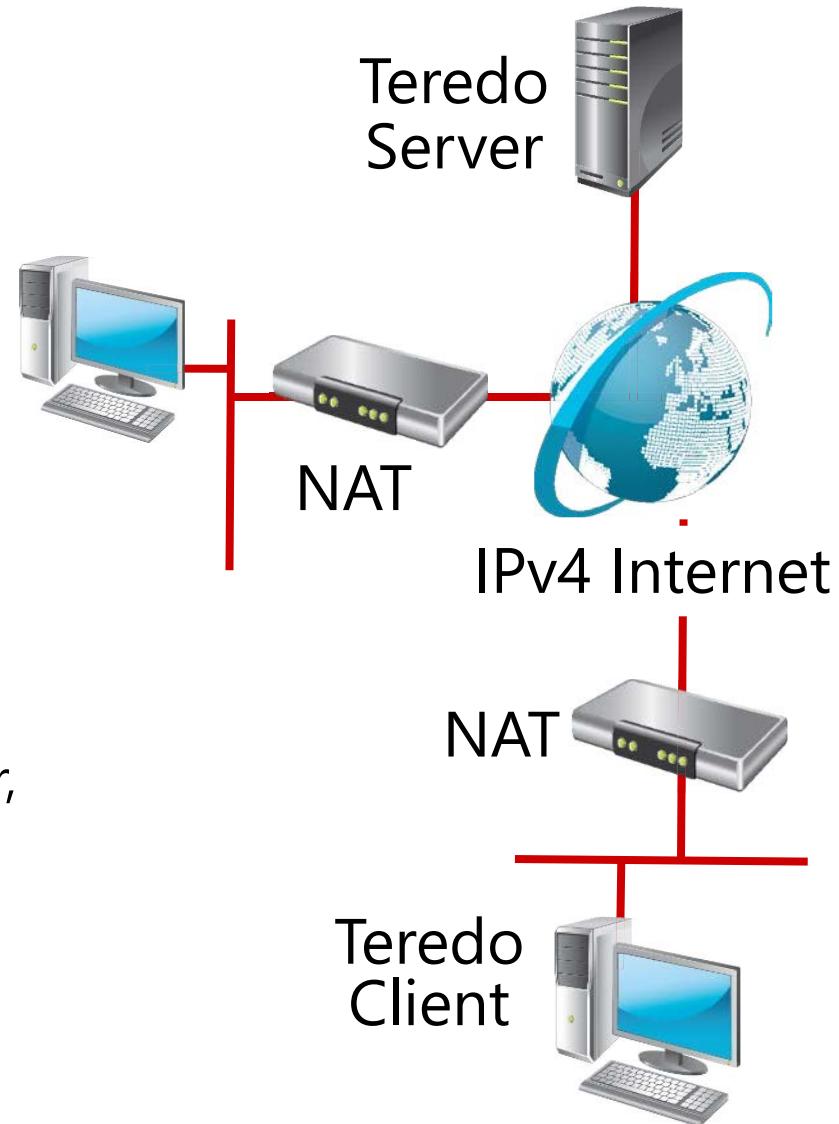
- Enable ICS
- Use Windows  
PowerShell



# What Is Teredo?

## Teredo:

- Enables IPv6 connectivity over the IPv4 Internet through NAT
- Requires a Teredo server to initiate communication
- Can be configured with the cmdlet  
**Set-NetTeredoConfiguration**



## Windows Server 2012:

- Can be configured as a client, server, or relay
- Is configured as a client by default
- Must be an enterprise client on domain networks

# What Is PortProxy?

Use PortProxy to:

- Provide IPv6-only hosts with access to IPv4-only applications
- Provide access between IPv4-only and IPv6-only hosts

Limitations of PortProxy:

- Only TCP applications
- Cannot change embedded address information

# Process for Transitioning to IPv6

To transition from IPv4 to IPv6 you must:

- Update applications to support IPv6
- Update routing infrastructure to support IPv6
- Update devices to support IPv6
- Update DNS with records for IPv6
- Upgrade hosts to IPv4/IPv6 nodes

# Lab: Implementing IPv6

- Exercise 1: Configuring an IPv6 Network
- Exercise 2: Configuring an ISATAP Router

## Logon Information

|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-RTR</b><br><b>20410D-LON-SVR2</b> |
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

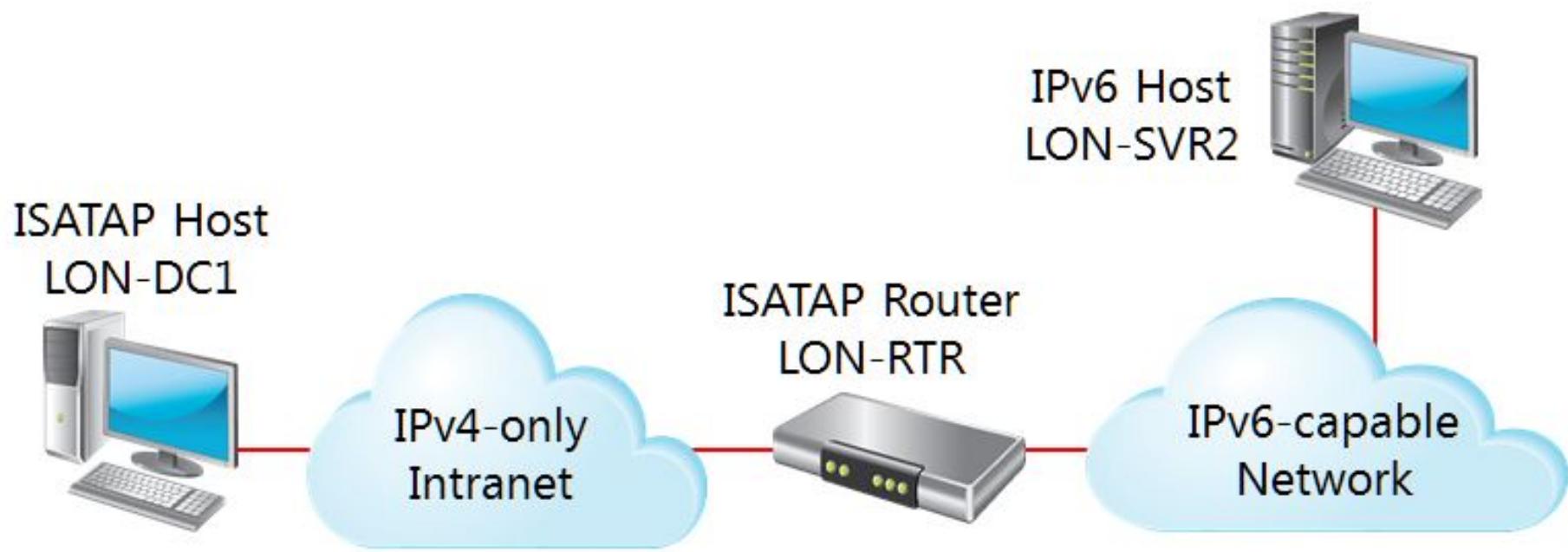
**Estimated Time: 45 minutes**

# Lab Scenario

The IT manager at A. Datum Corporation has been briefed by several program and application vendors about newly added support for IPv6 in their products. A. Datum Corporation does not have IPv6 support currently. However, the IT manager wants you to configure a test lab that uses IPv6. As part of the test lab configuration, you also need to configure ISATAP to allow communication between an IPv4 network and an IPv6 network.

# Lab Scenario

This is the layout of the completed test environment



# Lab Review

- Did you configure IPv6 statically or dynamically in this lab?
- Why did you not need to configure LON-DC1 with the IPv4 address of the ISATAP router?

# Module Review and Takeaways

- Review Questions
- Best Practices

# Microsoft® Official Course



## Module 9

### Implementing Local Storage

**Microsoft®**

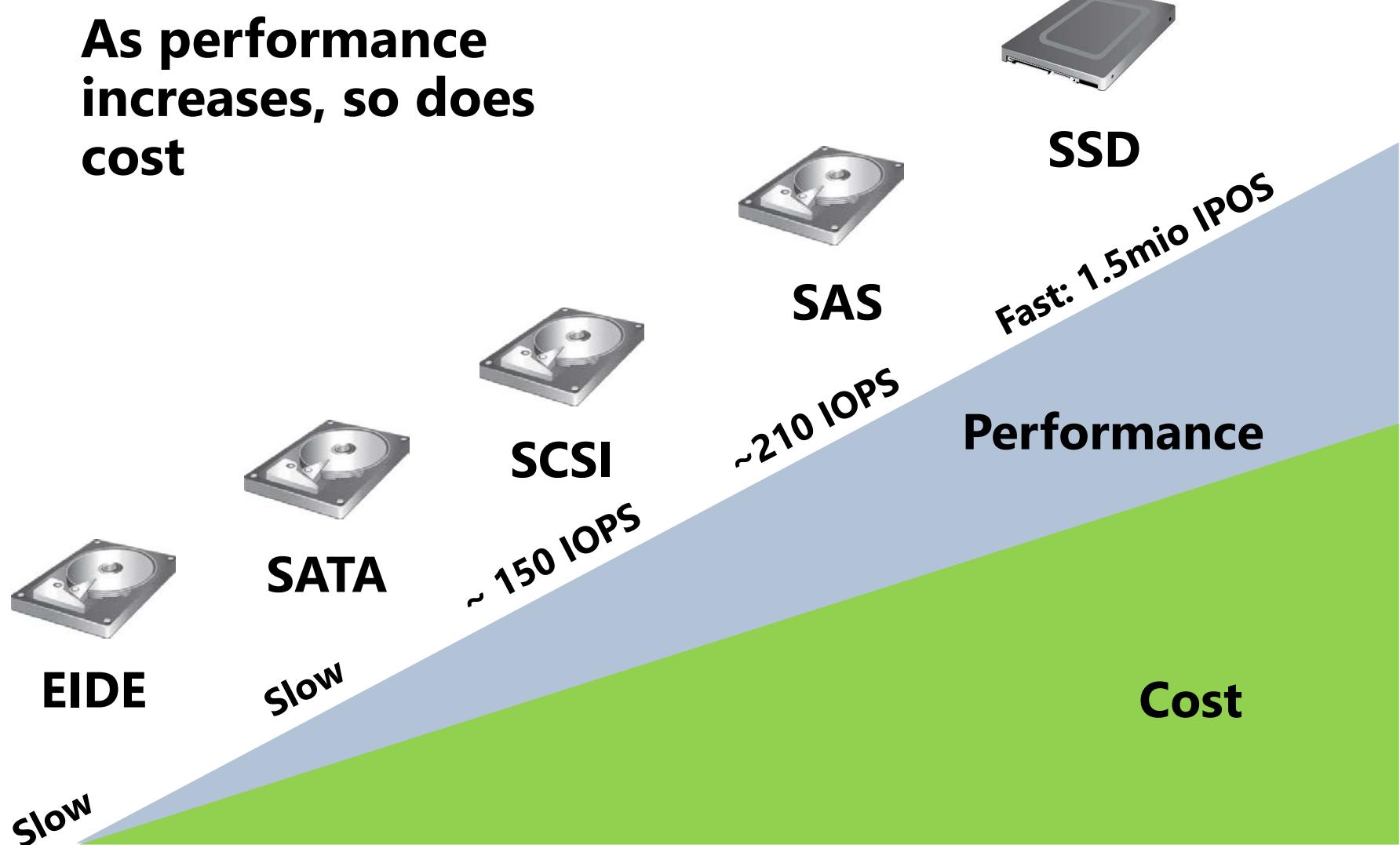
# Module Overview

- Overview of Storage
- Managing Disks and Volumes
- Implementing Storage Spaces

# Lesson 1: Overview of Storage

- Disk Types and Performance
- What Is Direct Attached Storage?
- What Is Network Attached Storage?
- What Is a SAN?
- What Is RAID?
- RAID Levels
- Windows Server 2012 and Windows Server 2012 R2 Storage Features

# Disk Types and Performance



# What Is Direct Attached Storage?

**DAS is physically attached to the server**

## **Advantages:**

- ✓ Easy to configure
- ✓ Inexpensive solution

## **Disadvantages:**

- ✓ Slower
- ✓ Isolated because the disks are attached to a single server



**Server with attached disks**

# What Is Network Attached Storage?

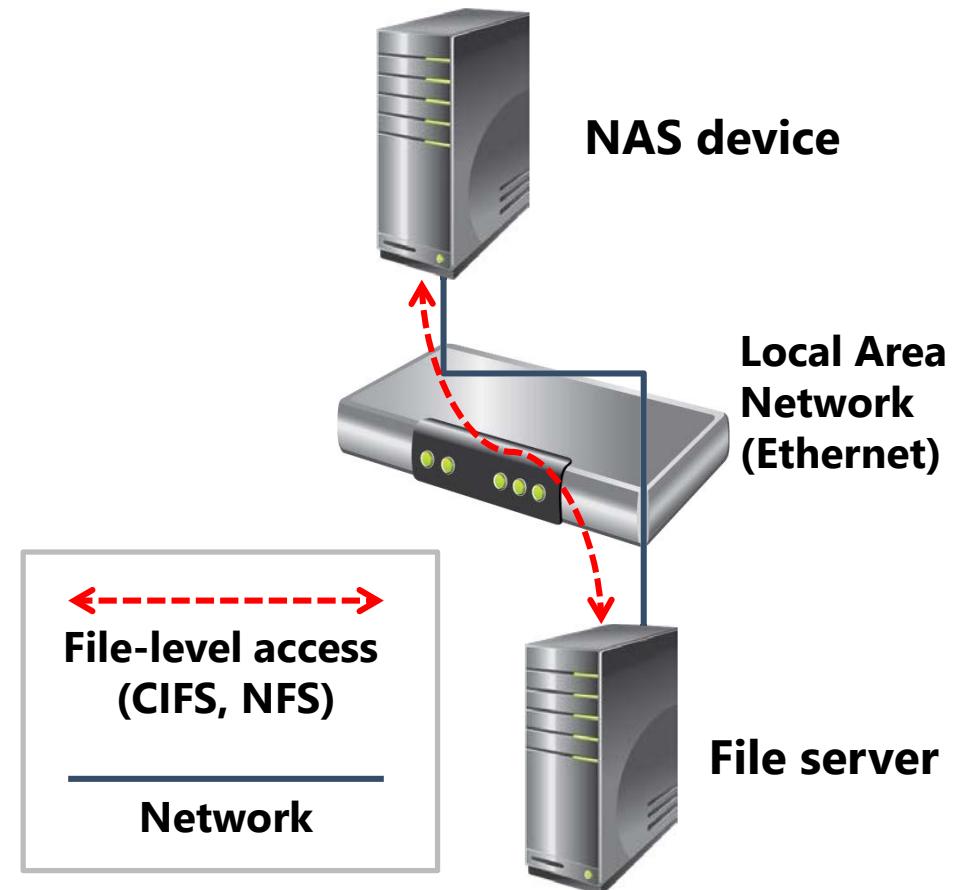
**NAS is storage that is attached to a dedicated storage device and accessed through network shares**

## Advantages:

- Relatively inexpensive, NAS offers centralized storage at an affordable price
- Easy to configure

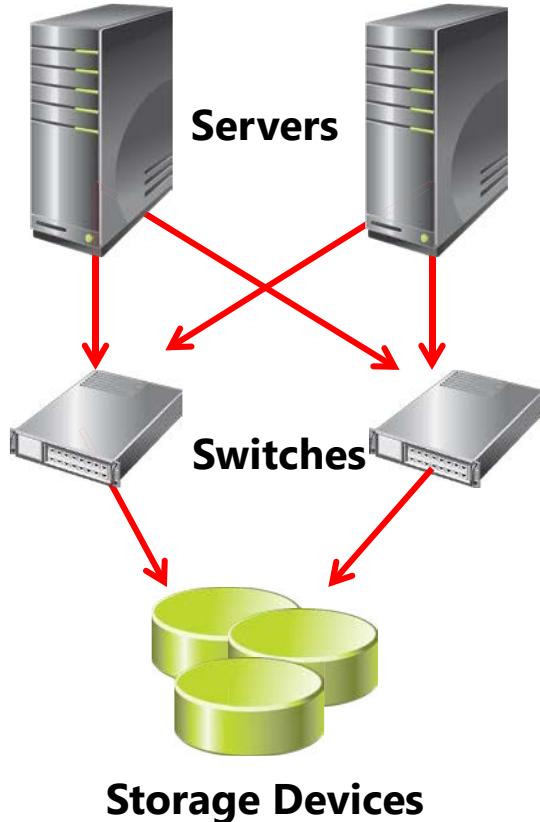
## Disadvantages:

- Slower access times
- Not an enterprise solution



# What Is a SAN?

**SANs offers higher availability with the most flexibility**



## **Advantages:**

- Fastest access times
- Easily expandable
- Centralized storage
- High level of redundancy

## **Disadvantages:**

- More expensive
- Requires specialized skills

**Implement SANs by using Fibre Channel or iSCSI**

# What Is RAID?

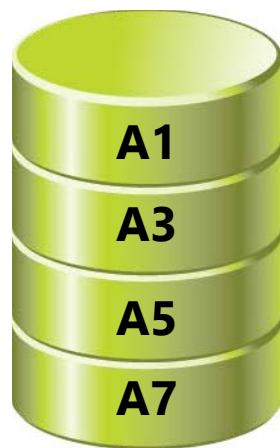
## RAID:

- Combines multiple disks into a single logical unit to provide fault tolerance and performance
- Provides fault tolerance by using:
  - Disk mirroring
  - Parity information
- Can provide performance benefits by spreading disk I/O across multiple disks
- Can be configured using several different levels
- Should not replace server backups

# RAID Levels

## RAID 0

**Striped set without parity or mirroring**



Disk 0



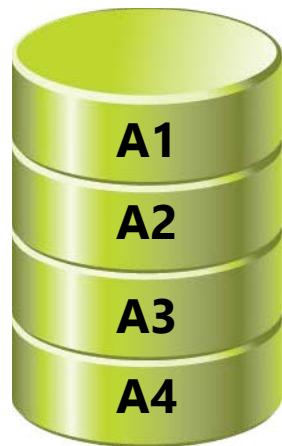
Disk 1



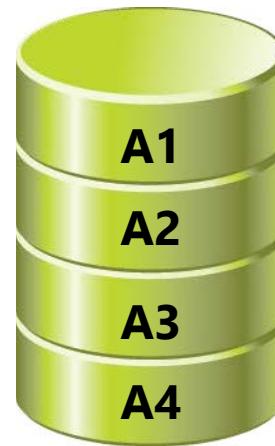
# RAID Levels

## RAID 1

Mirrored drives



Disk 0



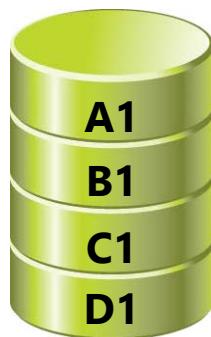
Disk 1



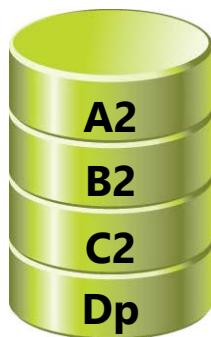
# RAID Levels

## RAID 5

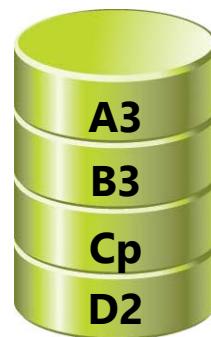
**Block level striped set with parity distributed across all disks**



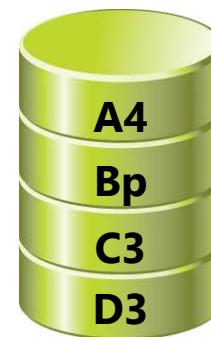
Disk 0



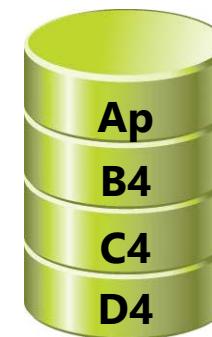
Disk 1



Disk 2



Disk 3



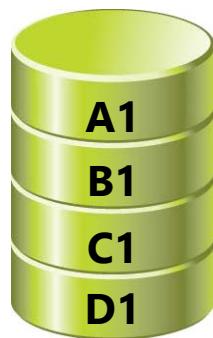
Disk 4



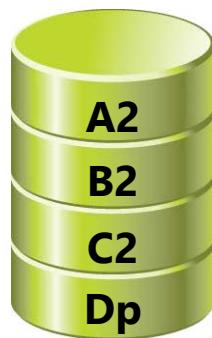
# RAID Levels

## RAID 6

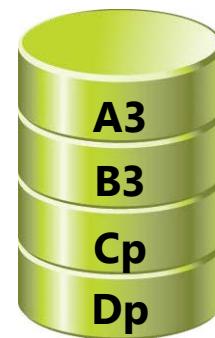
**Block level striped set with parity distributed across all disks**



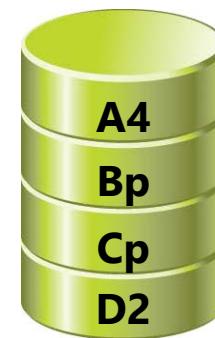
Disk 0



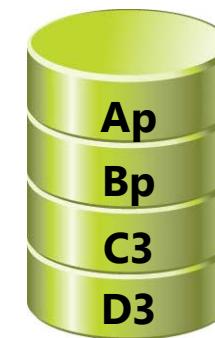
Disk 1



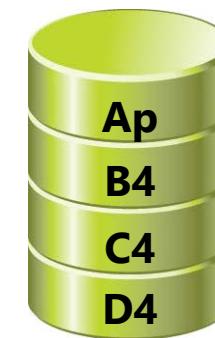
Disk 2



Disk 3



Disk 4



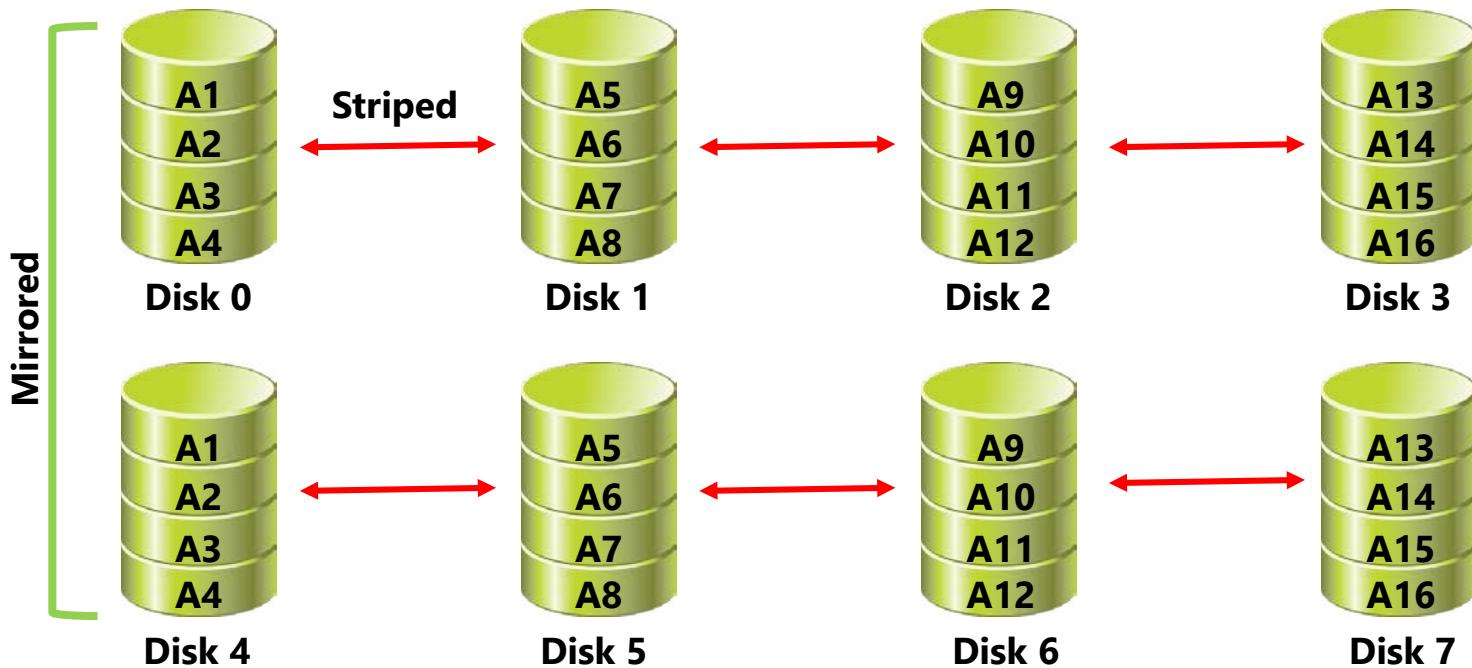
Disk 5



# RAID Levels

## RAID 1 + 0

Each pair of disks is mirrored, then the mirrored disks are striped



# Windows Server 2012 and Windows Server 2012 R2 Storage Features

Windows Server 2012 and Windows Server 2012 R2 provide several file and storage services enhancements including:

- Storage Spaces
- Data deduplication
- iSCSI Target Server
- Management enhancements
- Work Folders
- DFS enhancements

# Lesson 2: Managing Disks and Volumes

- Selecting a Partition Table Format
- Selecting a Disk Type
- Selecting a File System
- What Is ReFS?
- What Are Mount Points and Links?
- Demonstration: Creating Mount Points and Links
- Extending and Shrinking Volumes
- Managing Virtual Hard Disks
- Demonstration: Managing Virtual Hard Disks

# Selecting a Partition Table Format

## MBR

- Standard Partition table format since early 1980s
- Supports a maximum of 4 primary partitions per drive
- Can partition a disk up to 2 TB

## GPT

- GPT is the successor of MBR partition table format
- Supports a maximum of 128 partitions per drive
- Can partition a disk up to 18 EB

- ✓ **Use MBR for disks smaller than 2 TB**
- ✓ **Use GPT for disks larger than 2 TB**

# Selecting a Disk Type

Basic disks are:

- Disks initialized for basic storage
- The default storage for Windows operating system

Dynamic disks can:

- Be modified without restarting Windows
- Provide several options for configuring volumes

Disk volume requirements include:

- A system volume for hardware-specific files that are required to start the server
- A boot volume for the Windows operating system files

# Selecting a File System

**When selecting a file system, consider the differences between FAT, NTFS, and ReFS**

FAT provides:

- Basic file system
- Partition size limitations
- FAT32 to enable larger disks
- exFAT developed for flash drives

NTFS provides:

- Metadata
- Auditing and journaling
- Security (ACLs and encryption)

ReFS provides:

- Backward compatibility support for NTFS
- Enhanced data verification and error correction
- Support for larger files, directories, volumes, and so on

# What Is ReFS?

**ReFS is a new file system that is built in to Windows Server 2012. Advantages include:**

- Metadata integrity with checksums
- Integrity streams with user data integrity
- Allocation on write transactional model
- Large volume, file, and directory sizes ( $2^{78}$  bytes with 16-KB cluster size)
- Storage pooling and virtualization
- Data striping for performance and redundancy
- Disk scrubbing for protection against latent disk errors
- Resiliency to corruptions with recovery
- Shared storage pools across machines

# What Are Mount Points and Links?

**A mount point is a reference to a location on a disk that enables Windows operating system access to disk resources**

Use volume mount points:

- To mount volumes or disks as folders instead of using drive letters
- When you do not have drive letters available for creating new volumes
- To add disk space without changing the folder structure

**A link file contains a reference to another file or directory**

Link options:

- Symbolic file link (or, soft link)
- Symbolic directory link (or, directory junctions)

# Demonstration: Creating Mount Points and Links

In this demonstration, you will see how to:

- Create a mount point
- Create a directory junction for a folder
- Create a hard link for a file



# Extending and Shrinking Volumes

**You can resize NTFS volumes from the Windows operating system, beginning with Windows Vista and Windows Server 2008**

**When you want to resize a disk, consider the following:**

- You can extend or shrink NTFS volumes
- ReFS volumes can only be extended
- FAT/FAT32/exFAT cannot be resized
- You can shrink a volume only up to immovable files
- Bad clusters on a disk prevent you from shrinking a volume

# Managing Virtual Hard Disks

Virtual hard disks are files that you can use like physical hard disks

You can:

- Create and manage virtual hard disks by using Disk Management and Diskpart
- Configure .vhdx or .vhdx files
- Configure computers to start from the virtual hard disk
- Transfer virtual hard disks from Hyper-V servers and start computers from the virtual hard disk
- Use virtual hard disks as a deployment technology

# Demonstration: Managing Virtual Hard Disks

In this demonstration, you will see how to:

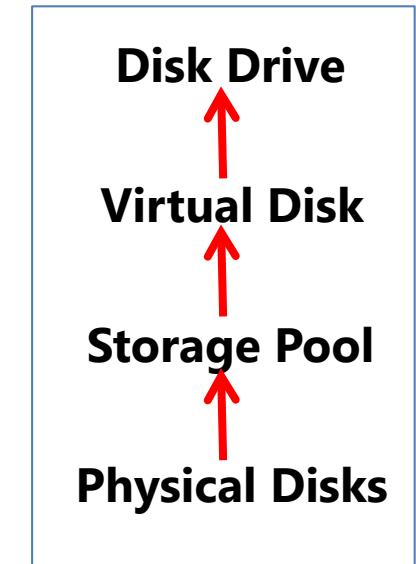
- Create a virtual hard disk
- Manage a virtual hard disk

# Lesson 3: Implementing Storage Spaces

- What Is the Storage Spaces Feature?
- Virtual Disk Configuration Options
- Advanced Management Options for Storage Spaces
- Demonstration: Configuring Storage Spaces
- Discussion: Comparing Storage Spaces with Other Storage Solutions

# What Is the Storage Spaces Feature?

- Use storage spaces to add physical disks of any type and size to a storage pool, and then create highly-available virtual disks from the storage pool
- To create a virtual disk, you need the following:
  - One or more physical disks
  - Storage pool that includes the disks
  - Virtual disk that are created with disks from the storage pool
  - Disk drives that are based on virtual drives
- Virtual disks are not virtual hard disks; they should be considered a drive in Disk Manager
- Windows Server 2012 R2 enables Storage Space tiering and write-back caching

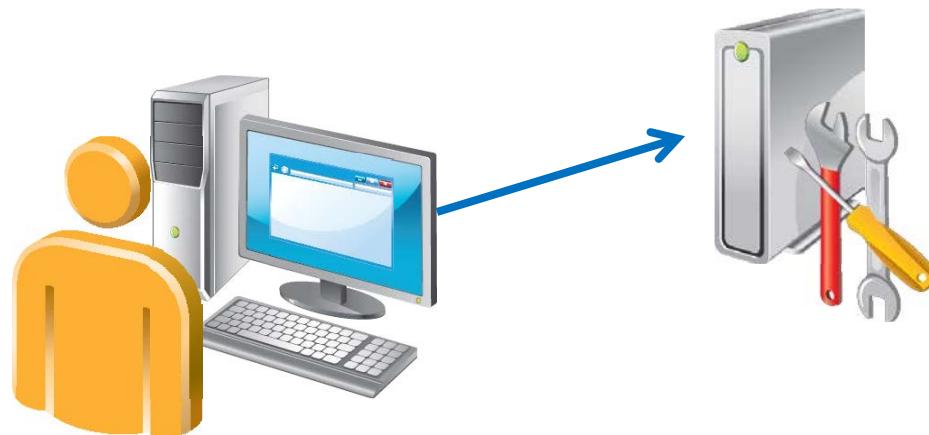


# Virtual Disk Configuration Options

| Feature              | Options                                                                                                         |
|----------------------|-----------------------------------------------------------------------------------------------------------------|
| Storage Layout       | <ul style="list-style-type: none"><li>• Simple</li><li>• Two-way or three-way mirror</li><li>• Parity</li></ul> |
| Disk sector size     | <ul style="list-style-type: none"><li>• 512 or 512e</li></ul>                                                   |
| Drive allocation     | <ul style="list-style-type: none"><li>• Automatic</li><li>• Manual</li><li>• Hot Spare</li></ul>                |
| Provisioning schemes | <ul style="list-style-type: none"><li>• Thin vs. fixed provisioning</li></ul>                                   |

# Advanced Management Options for Storage Spaces

- Basic Management for Storage Spaces is available in Server Manager
- For disk failure:
  - Do not use chkdsk or scan disk
  - Remove the drive and add a new one
- Advanced management requires Windows PowerShell



# Advanced Management Options for Storage Spaces

| Windows PowerShell cmdlet                                   | Description                                 |
|-------------------------------------------------------------|---------------------------------------------|
| Get-StoragePool                                             | List storage pools                          |
| Repair-VirtualDisk                                          | Repair a virtual disk                       |
| Get-PhysicalDisk  <br>Where{\$_.HealthStatus -ne "Healthy"} | List unhealthy physical disks               |
| Reset-PhysicalDisk                                          | Remove a physical disk from a storage pool  |
| Get-VirtualDisk  <br>Get-PhysicalDisk                       | List physical disks used for a virtual disk |

# Demonstration: Configuring Storage Spaces

In this demonstration, you will see how to:

- Create a storage pool
- Create a virtual disk and a volume

# Discussion: Comparing Storage Spaces with Other Storage Solutions

1. Does your organization currently use SANs or NAS?
2. What are the advantages of using Storage Spaces compared to using SANs or NAS?
3. What are the disadvantages of using Storage Spaces compared to using SANs or NAS?
4. In what scenarios would you recommend each option?



**10 minutes**

# Lab: Implementing Local Storage

- Exercise 1: Installing and Configuring a New Disk
- Exercise 2: Resizing Volumes
- Exercise 3: Configuring a Redundant Storage Space

## Logon Information

|                  |                                                 |
|------------------|-------------------------------------------------|
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b> |
| User name        | <b>Adatum\Administrator</b>                     |
| Password         | <b>Pa\$\$w0rd</b>                               |

**Estimated Time: 45 minutes**

## Lab Scenario

Your manager has asked to add disk space to a file server. After creating volumes, your manager has also asked you to resize those volumes based on updated information he has been given. Finally, you need to make data storage redundant by creating a three-way mirrored virtual disk.

# Lab Review

- At a minimum, how many disks must you add to a storage pool to create a three-way mirrored virtual disk?
- You have a USB-attached disk, four SAS disks, and one SATA disk that are attached to a Windows Server 2012 server. You want to provide a single volume to your users that they can use for file storage. What would you use?

# Module Review and Takeaways

- Review Questions
- Best Practices
- Tools

# Microsoft® Official Course



## Module 10

### Implementing File and Print Services

**Microsoft®**

# Module Overview

- Securing Files and Folders
- Protecting Shared Files and Folders by Using Shadow Copies
- Configuring Work Folders
- Configuring Network Printing

# Lesson 1: Securing Files and Folders

- What Are File Permissions?
- What Are Shared Folders?
- Permissions Inheritance
- Effective Permissions
- What Is Access-Based Enumeration?
- What Is the Offline Files Feature?
- Demonstration: Creating and Configuring a Shared Folder

# What Are File Permissions?

- File permissions control access for files and folders on NTFS or ReFS formatted storage volumes
- File Permissions:
  - Are configured for files or folders
  - Can be granted or denied
  - Are inherited from parent folders
- Permissions conflict precedence:
  1. Explicitly assigned Deny
  2. Explicitly assigned Allow
  3. Inherited Deny
  4. Inherited Allow

# What Are Shared Folders?

- Shared folders grant network access to their contents
- Folders can be shared, but individual files cannot
- Shared folders can be hidden by creating a share with a \$ at the end of the share name
- Accessing a shared folder using the UNC path:
  - \\LON-SVR1\Sales (standard share)
  - \\LON-SVR1\Sales\$ (hidden share)
- Administrative shares are hidden shares that allow administrators access to the root of every volume and special system folders, such as the operating system folder

# Permissions Inheritance

- Inheritance is used to manage access to resources without explicitly assigning permissions to each object
- By default, permissions are inherited in a parent/child relationship
- Blocking inheritance:
  - You can block permission inheritance
  - You can apply blocking at the file or folder level
  - You can set blocking on a folder to propagate the new permissions to child objects

# Effective Permissions

- When combining file system and shared folder permissions, the most restrictive permission is applied
  - Example: If a user or group has the shared folder permission of Read and the file system permission of Write, the user or group will only be able to read the files in the folder because it is the more restrictive permission
- The user must have both file system and shared folder permissions, otherwise the user will be denied access to the resource

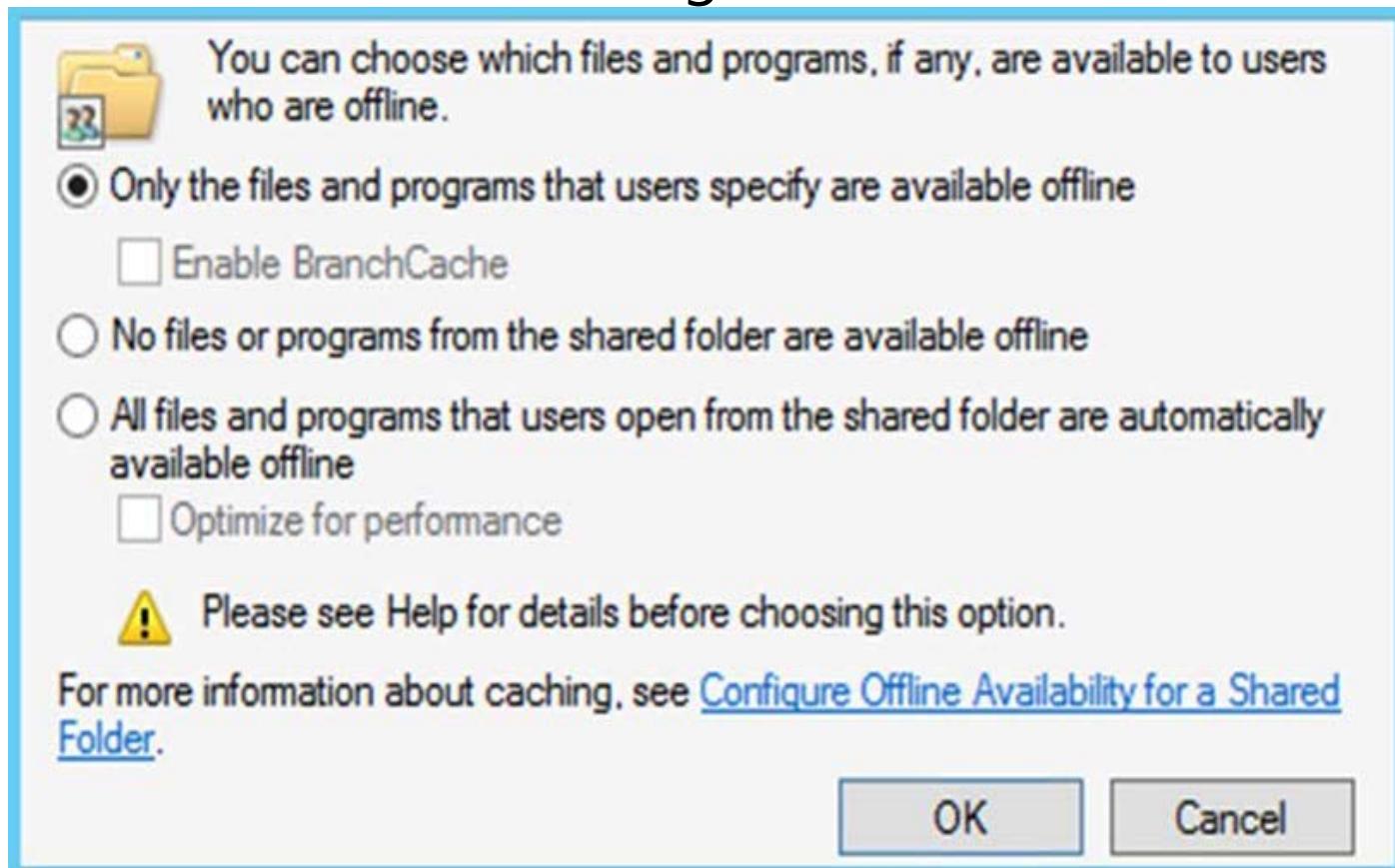
# What Is Access-Based Enumeration?

- Access-based enumeration allows an administrator to control the visibility of shared folders according to the permissions set on the shared folder
- Access Based Enumeration is:
  - Built into Windows Server 2012
  - Available for shared folders
  - Configurable on a per shared folder basis

# What Is the Offline Files Feature?

Offline Files allow a client computer to cache network files locally for offline use when they are disconnected from the network

Offline settings window



# Demonstration: Creating and Configuring a Shared Folder

In this demonstration, you will see how to:

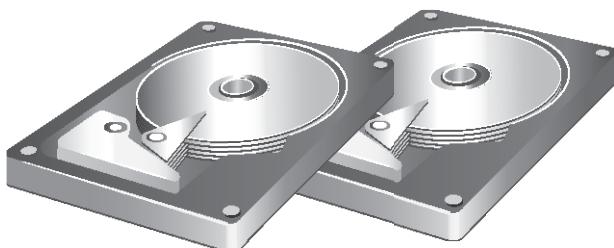
- Create a shared folder
- Assign permissions for the shared folder
- Configure access-based enumeration
- Configure offline files

## Lesson 2: Protecting Shared Files and Folders by Using Shadow Copies

- What Are Shadow Copies?
- Considerations for Scheduling Shadow Copies
- Restoring Data from a Shadow Copy
- Demonstration: Restoring Data from a Shadow Copy

# What Are Shadow Copies?

- Allow access to previous versions of files
- Are based on tracking disk changes
  - Disk space is allocated on the same volume
  - When the space is full, older shadow copies are removed
- Are not a replacement for backups
- Are not suitable for recovering databases



# Considerations for Scheduling Shadow Copies

Default schedule is 7:00 A.M. and noon

Schedule

1. At 7:00 AM every Mon, Tue, Wed, Thu, Fri of every week, starting 5, ▾

New Delete

Schedule Task: Start time:

Weekly 7:00 AM Advanced...

Schedule Task Weekly

Every 1 week(s) on:  Mon  Sat  
 Tue  Sun  
 Wed  
 Thu  
 Fri

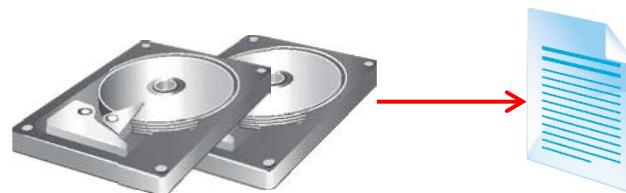
Create a shadow copy schedule based on:

- Capacity of server
- Frequency of changes
- Importance of changes



# Restoring Data from a Shadow Copy

- Previous versions are accessible from the Properties dialog box of a file or folder
  - Administrators can restore previous versions directly on the server
  - Users can restore previous versions over the network
- All users can:
  - Restore a file or folder
  - Browse previous versions to select the correct one
  - Copy a file or folder to an alternate location



# Demonstration: Restoring Data from a Shadow Copy

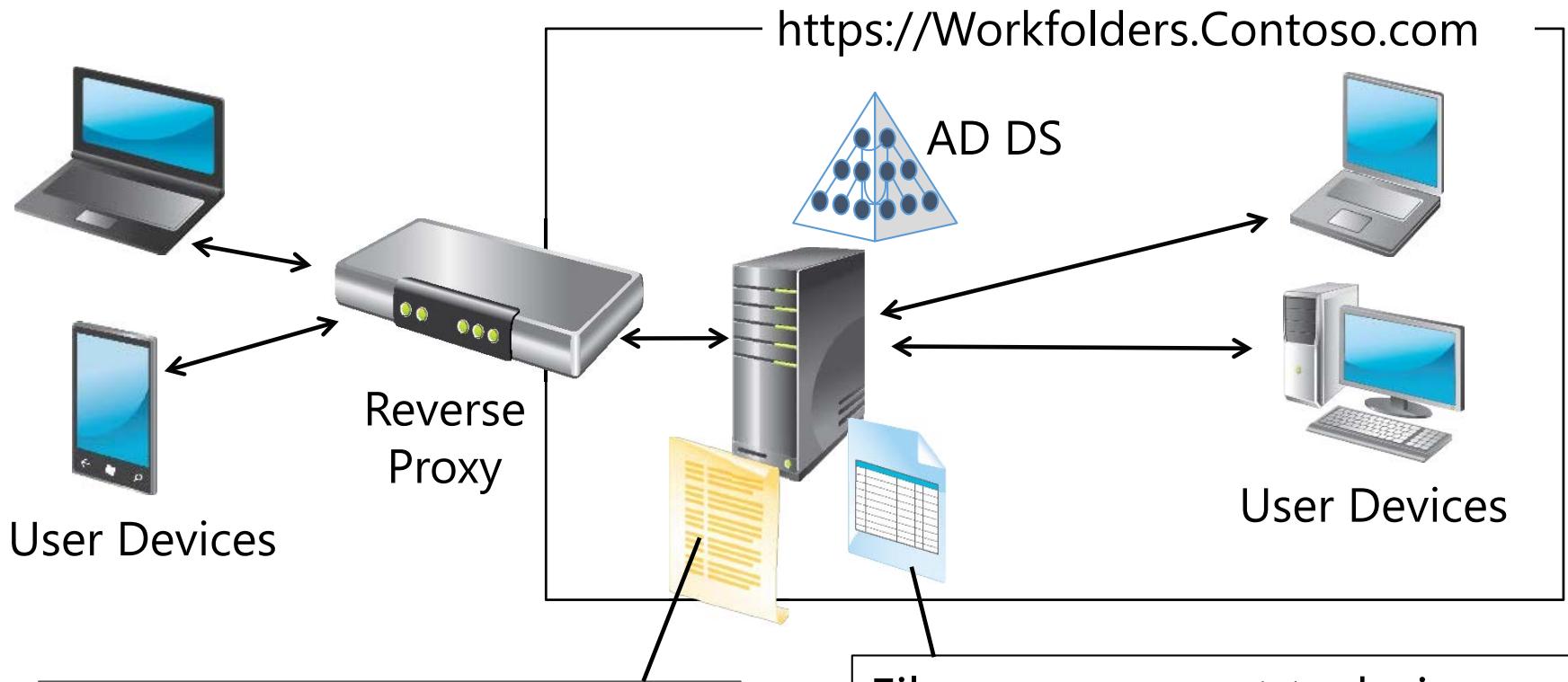
In this demonstration, you will see how to:

- Configure shadow copies
- Create a new file
- Create a shadow copy
- Modify the file
- Restore the previous version

# Lesson 3: Configuring Work Folders

- What Is the Work Folders Role Service?
- Benefits and Limitations of Work Folders
- Components of Work Folders
- Configuring Work Folders
- Demonstration: How to Configure Work Folders

# What Is the Work Folders Role Service?



User Devices

Reverse  
Proxy

User Devices

Security policies to enforce encryption, lock devices, and wipe corporate data off of devices

File management techniques:

- Quotas
- File screens
- Reporting
- Classification

# Benefits and Limitations of Work Folders

- The benefits of Work Folders include:
  - Works on domain-joined devices and devices that are not domain-joined
  - Provides a single point of access to work files
  - Provides offline access to work files
  - Synchronizes files for users
  - Enables data encryption
  - Works with existing data management technologies
- The limitations of Work Folders include:
  - Works on Windows Server 2012 R2 and Windows 8.1 only
  - Does not support collaborative scenarios
  - Does not permit selective synchronization of files
  - Does not synchronize multiple file shares

# Components of Work Folders

- Software requirements
  - Windows Server 2012 R2 file server
  - Windows 8.1 client
  - SSL certificates
  - NTFS or ReFS volume for both client and server
- Server components
  - Work Folders role service
  - File Server role service
  - Web Server (IIS) role
  - IIS Management Console role service
  - IIS Hostable Web Core role service
- Client components
  - Manual deployment using built-in Control Panel item
  - Automatic deployment via Group Policy, Configuration Manager, or Intune

# Configuring Work Folders

- Server configuration
  - Install the Work Folders role service
  - Create a sync share
  - Install a server certificate which has the same common name as the Work Folders URL
- Client configuration
  - For manual configuration, the user enters their email address manually
  - For automatic configuration, you can use Group Policy

# Demonstration: How to Configure Work Folders

In this demonstration, you will see how to:

- Install the Work Folders role service
- Create a sync share for work folders on a file server
- Configure Work Folder access on a Windows 8.1 client
- Create a file in the work folder
- Configure Work Folders to sync data on a second Windows 8.1 client

# Lesson 4: Configuring Network Printing

- Benefits of Network Printing
- What Is Enhanced Point and Print?
- Security Options for Network Printing
- Demonstration: Creating Multiple Configurations for a Print Device
- What Is Printer Pooling?
- What Is Branch Office Direct Printing?
- Deploying Printers to Clients

# Benefits of Network Printing

Benefits of network printing include:

- Centralized management via the Print Management Console
- Simplified troubleshooting
- Lower total costs
- Easier searching

# What Is Enhanced Point and Print?

- Enhanced Point and Print uses the v4 driver model to provide a simplified management structure for network printer drivers
- Benefits of Enhanced Point and Print :
  - Print servers do not need to store client print drivers
  - Driver files are isolated, preventing file naming conflicts
  - A single driver can support multiple devices
  - Driver packages are smaller and install faster
  - The print driver and the printer user interface can be deployed independently

# Security Options for Network Printing

- The default security allows everyone to:
  - Print
  - Manage their own print jobs
- The available permissions are:
  - Print
  - Manage this printer
  - Manage documents

# Demonstration: Creating Multiple Configurations for a Print Device

In this demonstration, you will see how to:

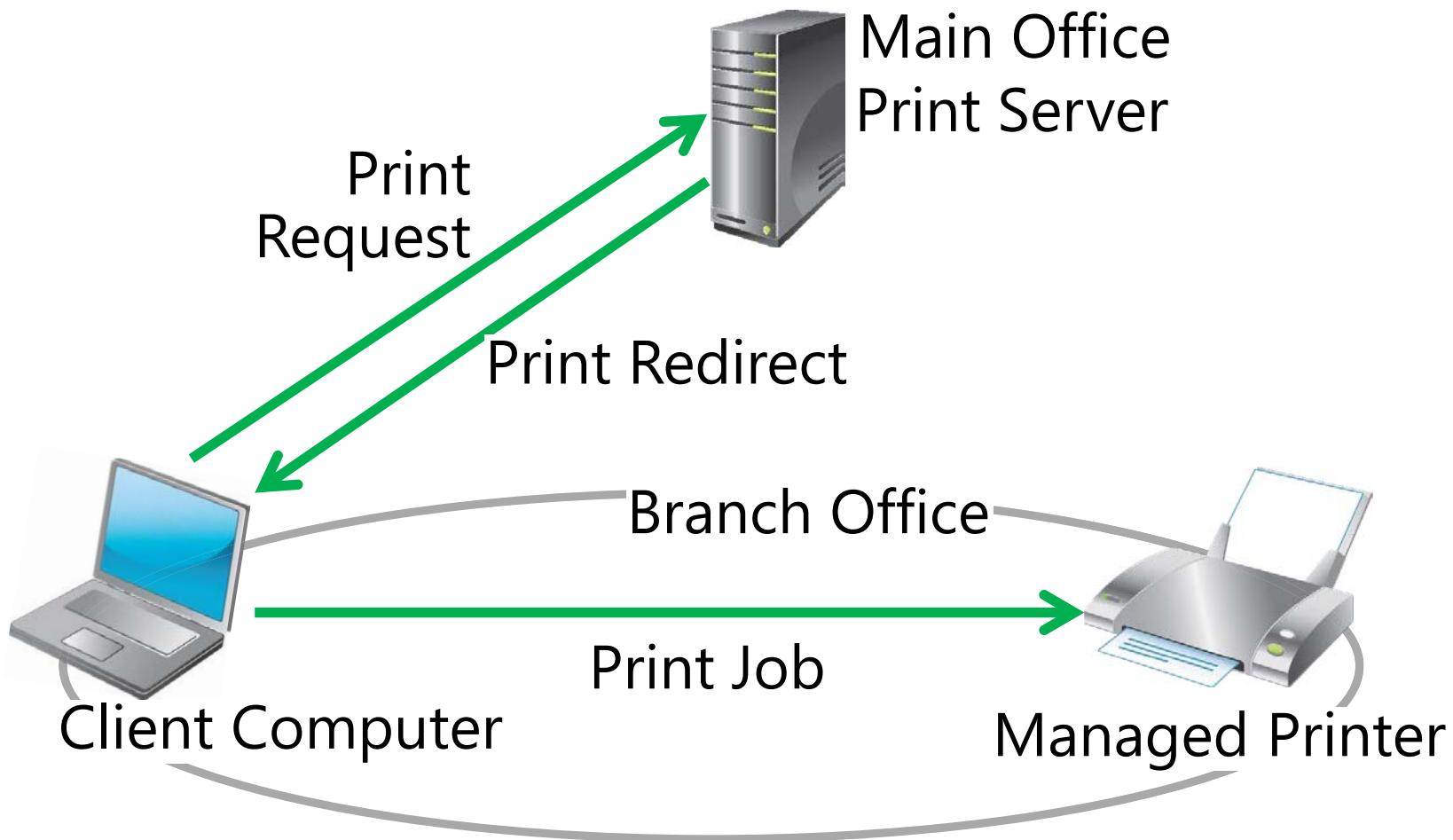
- Create a shared printer
- Create a second shared printer using the same port
- Increase printing priority for a high priority print queue

# What Is Printer Pooling?

- Printer pooling combines multiple physical printers into a single logical unit
- A printer pool increases availability and scalability
- Requirements:
  - All printers must use the same driver
  - All printers should be in the same location

# What Is Branch Office Direct Printing?

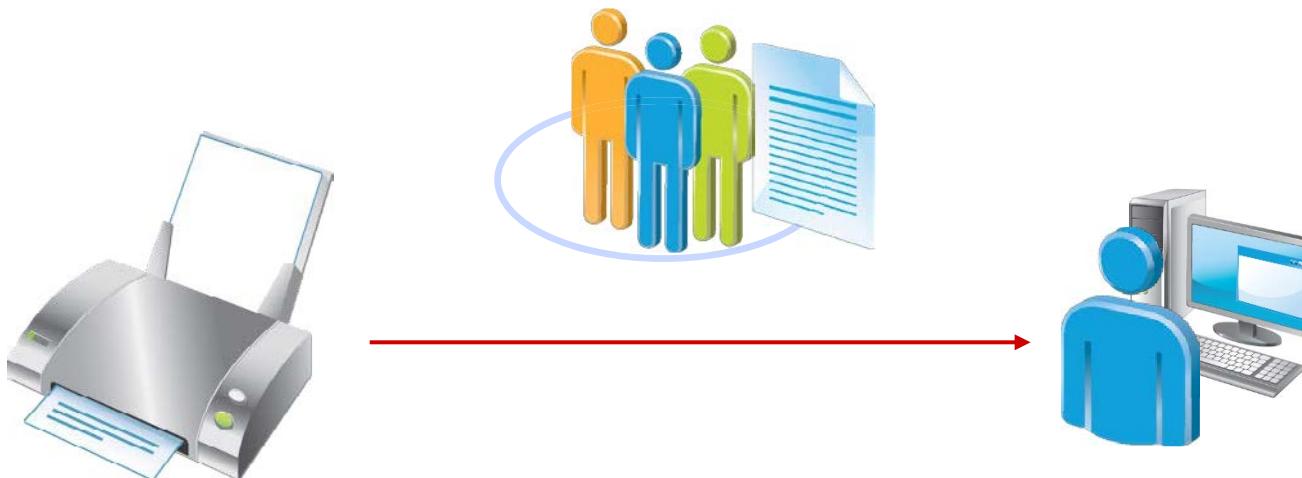
Branch Office Direct Printing enables client computers to print directly to network printers that are shared on a print server



# Deploying Printers to Clients

You can deploy printers to clients by using:

- Group Policy preferences
- GPO created by Print Management
- Manual installation



# Lab: Implementing File and Print Services

- Exercise 1: Creating and Configuring a File Share
- Exercise 2: Configuring Shadow Copies
- Exercise 3: Enabling and Configuring Work Folders
- Exercise 4: Creating and Configuring a Printer Pool

## Logon Information

|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
| Virtual machines | <b>20410D-LON-CL1</b><br><b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b> |
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

**Estimated Time: 60 minutes**

## Lab Scenario

Your manager has recently asked you to configure file and print services for the branch office. This requires you to configure a new shared folder that will have subfolders for multiple departments, configure shadow copies on the file servers, and configure a printer pool.

Additionally, many users want to be able to work on their data files while they are out of the office and working on devices such as on Windows RT-based tablets. You must ensure that these users are able to access their work-related data files from other locations when offline.

# Lab Review

- How does implementing access-based enumeration benefit the users of the Data shared folder in this lab?
- Is there another way you could recover the file in the shadow copy exercise? What benefit do shadow copies provide in comparison?
- In Exercise 3, how could you configure Branch Office Direct Printing if you were in a remote location and did not have access to the Windows Server 2012 GUI for the print server?

# Module Review and Takeaways

- Review Questions
- Tools

# Microsoft® Official Course



## Module 11

### Implementing Group Policy

**Microsoft®**

# Module Overview

- Overview of Group Policy
- Group Policy Processing
- Implementing a Central Store for Administrative Templates

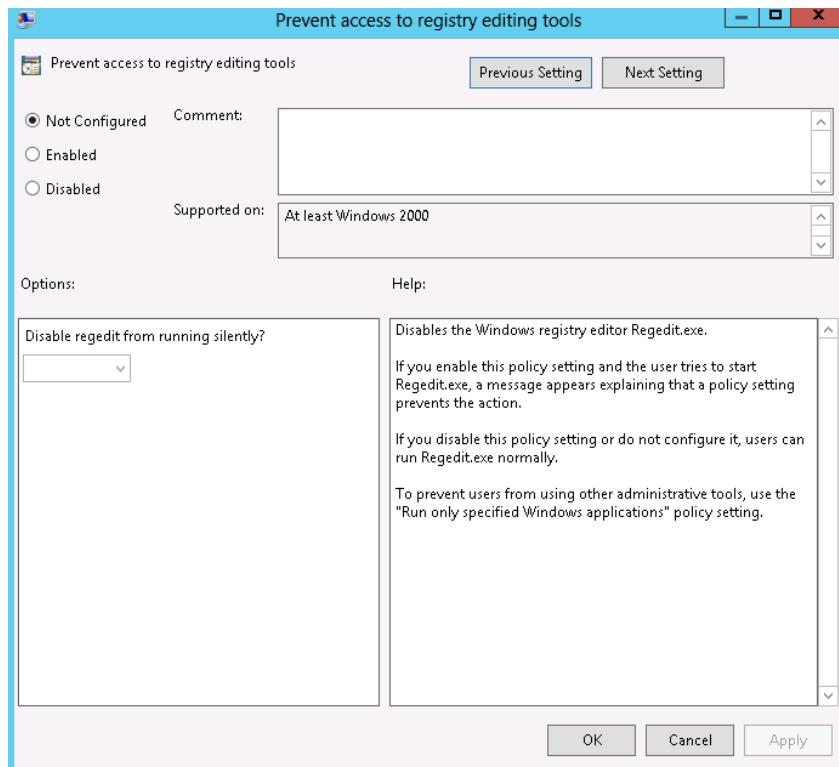
# Lesson 1: Overview of Group Policy

- Components of Group Policy
- Storage of Domain GPOs
- What Are Group Policy Preferences?
- What Are Starter GPOs?
- Delegating Management of GPOs
- Demonstration: Creating and Managing GPOs

# Components of Group Policy

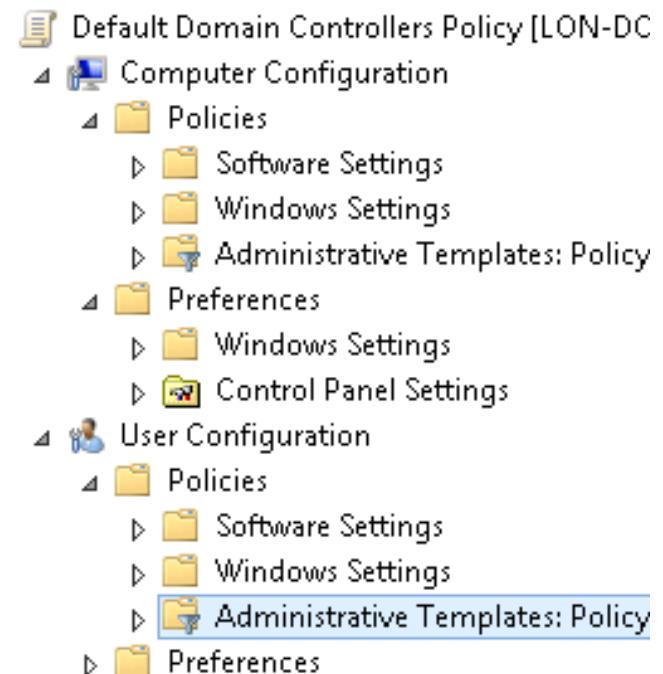
## A Group Policy setting:

- Defines a specific configuration change
- Can be applied to a user or to a computer



## A GPO:

- Is a collection of Group Policy settings
- Can be applied to a user, a computer, or both



# Storage of Domain GPOs

## Group Policy Components



### GPO

- Contains Group Policy settings
- Stores content in two locations



### Group Policy Container

- Stored in AD DS
- Provides version information



### Group Policy Template

- Stored in shared SYSVOL folder
- Provides Group Policy settings

# What Are Group Policy Preferences?

Use Group Policy preferences to:

- Configure, deploy, and manage operating system and application settings that are not manageable by using Group Policy
  - Apply once at startup or sign in, optionally refresh at intervals
  - Target to users or computers
- Expand the range of configurable settings within a GPO

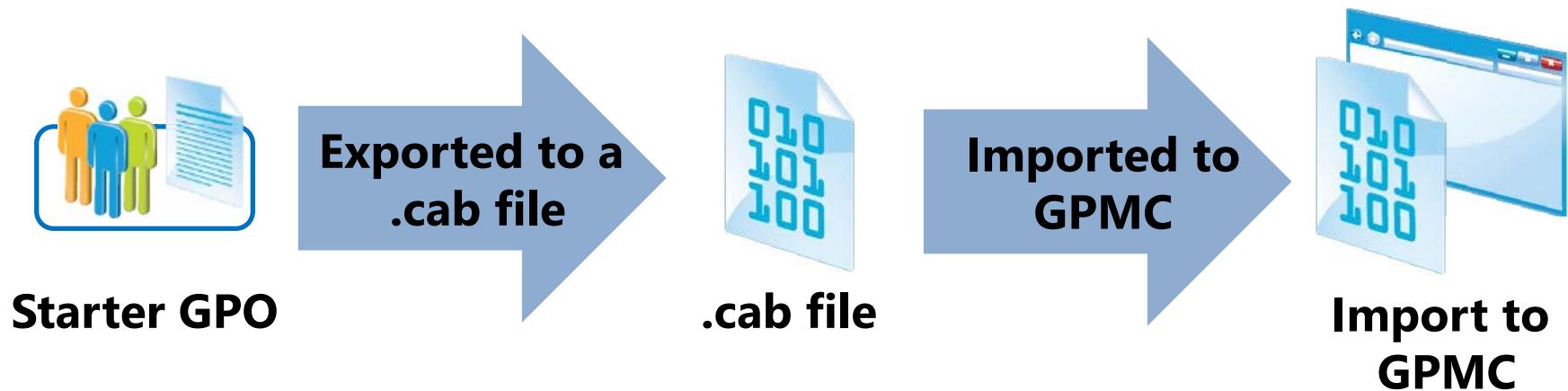
Group Policy preferences:

- Are not enforced
- Are not removed when the GPO no longer applies
- Do not disable the interface of the setting; users can change the setting
- Cannot be used in local group policies

# What Are Starter GPOs?

## A starter GPO:

- Has preconfigured administrative template settings upon which new GPOs can be based
- Can be exported to .cab files
- Can be imported into other areas of the enterprise



# Delegating Management of GPOs

Delegation of GPO-related tasks allows the administrative workload to be distributed across the enterprise

The following Group Policy tasks can be independently delegated:

- Creating GPOs, including Starter GPOs
- Editing GPOs
- Managing Group Policy links for a site, domain, or OU
- Performing Group Policy Modeling analysis in a domain or OU
- Reading Group Policy Results data in a domain or OU
- Creating WMI filters on a domain

# Demonstration: Creating and Managing GPOs

In this demonstration, you will see how to:

- Create a GPO by using the GPMC
- Edit a GPO in the Group Policy Management Editor window
- Use Windows PowerShell to create a GPO

# Lesson 2: Group Policy Processing

- GPO Links
- Applying GPOs
- Group Policy Processing Order
- What Are Multiple Local GPOs?
- What Are the Default GPOs?
- GPO Security Filtering
- Discussion: Identifying Group Policy Application
- Demonstration: Using Group Policy Diagnostic Tools

# GPO Links

When linking GPOs, remember that:

- To deliver settings to an object, a GPO must be linked to a container
- Disabling a link removes the settings from the container
- Deleting a link does not delete the GPO

## **GPOs can be linked to:**

- Sites
- Domains
- OUs

## **GPOs cannot be linked to:**

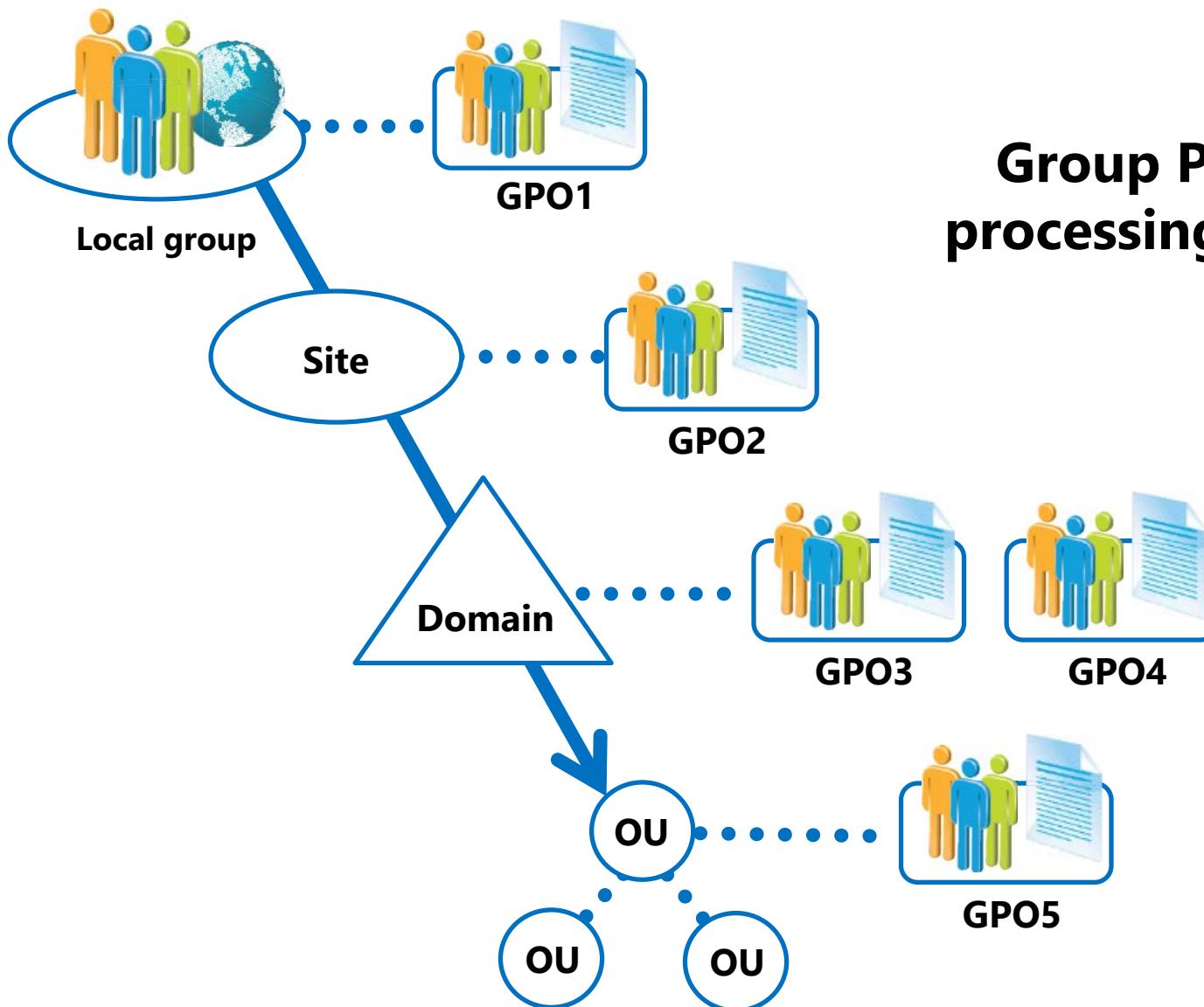
- Users
- Groups
- Computers
- System containers

# Applying GPOs

When you apply GPOs, remember that:

- Computer settings apply at startup
- User settings apply at sign in
- Policies refresh at regular, configurable intervals
- Security settings refresh at least every 16 hours
- Policies refresh manually by using:
  - The Gpupdate command
  - The Windows PowerShell cmdlet Invoke-Gpupdate
- Since Windows Server 2012 and Windows 8, a new Remote Policy Refresh feature allows you to remotely refresh policies

# Group Policy Processing Order



**Group Policy  
processing order**

# What Are Multiple Local GPOs?

## Multiple Local Group Policies:

- Have a single computer configuration that applies to the computer for all users who log on
- Have layers of user settings that can apply only to individual users, not to groups

**There are three layers of user configurations:**



**Administrator**



**Standard user**



**User-specific**

# What Are the Default GPOs?

**There are two default GPOs:**

- Default Domain Policy
  - Used to define the account policies for the domain:
    - Password
    - Account lockout
    - Kerberos protocol
- Default Domain Controllers Policy
  - Used to define auditing policies
  - Defines user rights on domain controllers

# GPO Security Filtering

## **Apply Group Policy permissions**

- GPO has an ACL (Delegation tab, click Advanced)
- Default: Authenticated Users have Allow Apply Group Policy

## **Scope only to users in selected global or universal groups**

- Remove Authenticated Users
- Add appropriate global or universal groups (GPOs do not scope to domain local groups)

## **Scope to users except for those in selected groups**

- On the Delegation tab, click Advanced
- Add appropriate global groups
- Deny the Apply Group Policy permission

# Discussion: Identifying Group Policy Application

Review the scenario and the AD DS structure graphic in the handbook to answer the following questions:

What power options will the servers in the Servers OU receive?

What power options will the laptops in the Sales Laptops OU receive?

What power options will all other computers in the domain receive?

Will users in the Sales Users OU who have created local policies to grant access to Control Panel be able to access Control Panel?

If you needed to grant access to Control Panel to some users, how would you do it?

Can GPO2 be applied to other department OUs?



**20 minutes**

# Demonstration: Using Group Policy Diagnostic Tools

In this demonstration, you will see how to:

- Use Gpupdate to refresh Group Policy
- Use the Gpresult command to output the results to an HTML file
- Use the Group Policy Modeling Wizard to test the policy

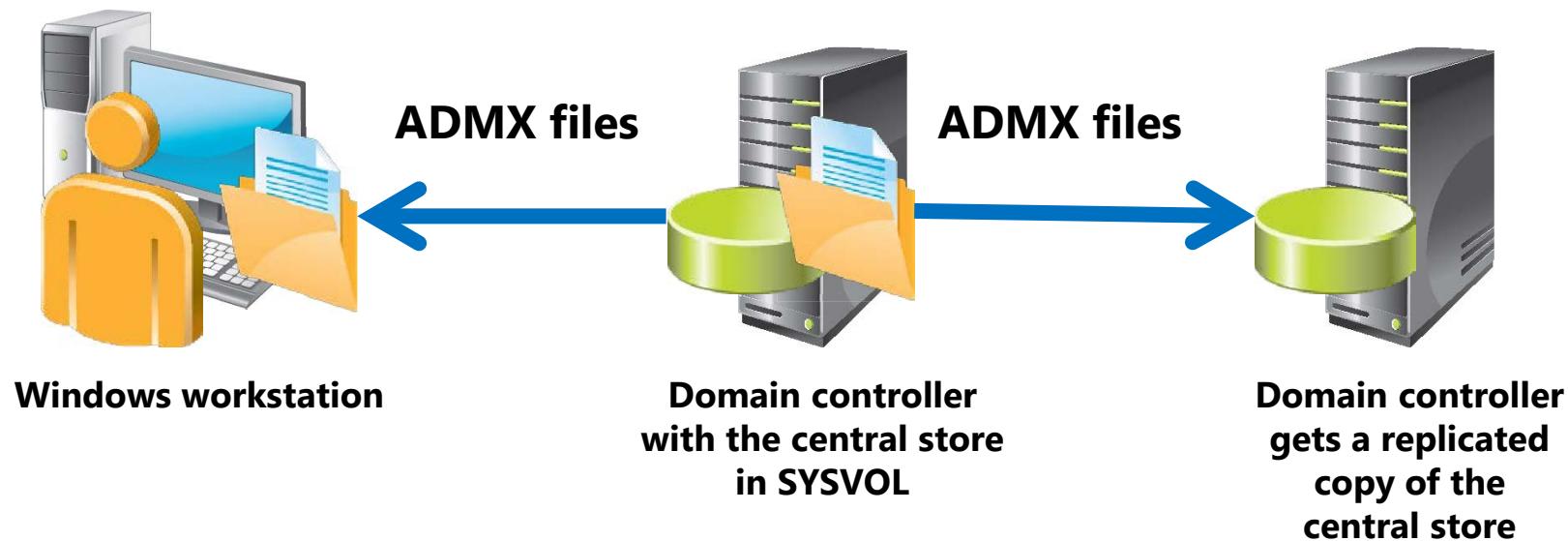
# Lesson 3: Implementing a Central Store for Administrative Templates

- What Is the Central Store?
- What Are Administrative Templates?
- How Administrative Templates Work
- Managed and Unmanaged Policy Settings

# What Is the Central Store?

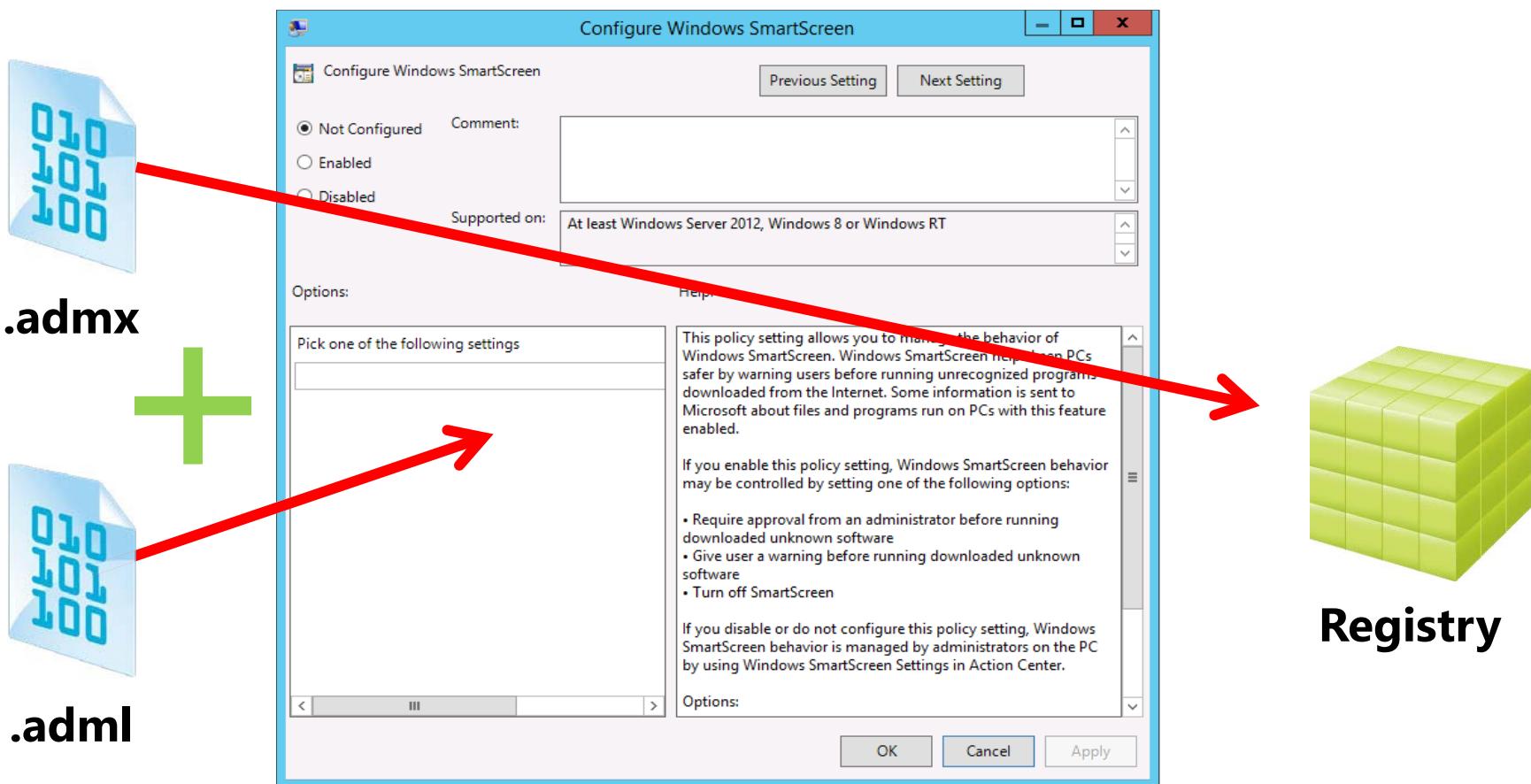
The central store:

- Is a central repository for ADMX and ADML files
- Is stored in SYSVOL
- Must be created manually
- Is detected automatically by Windows operating systems



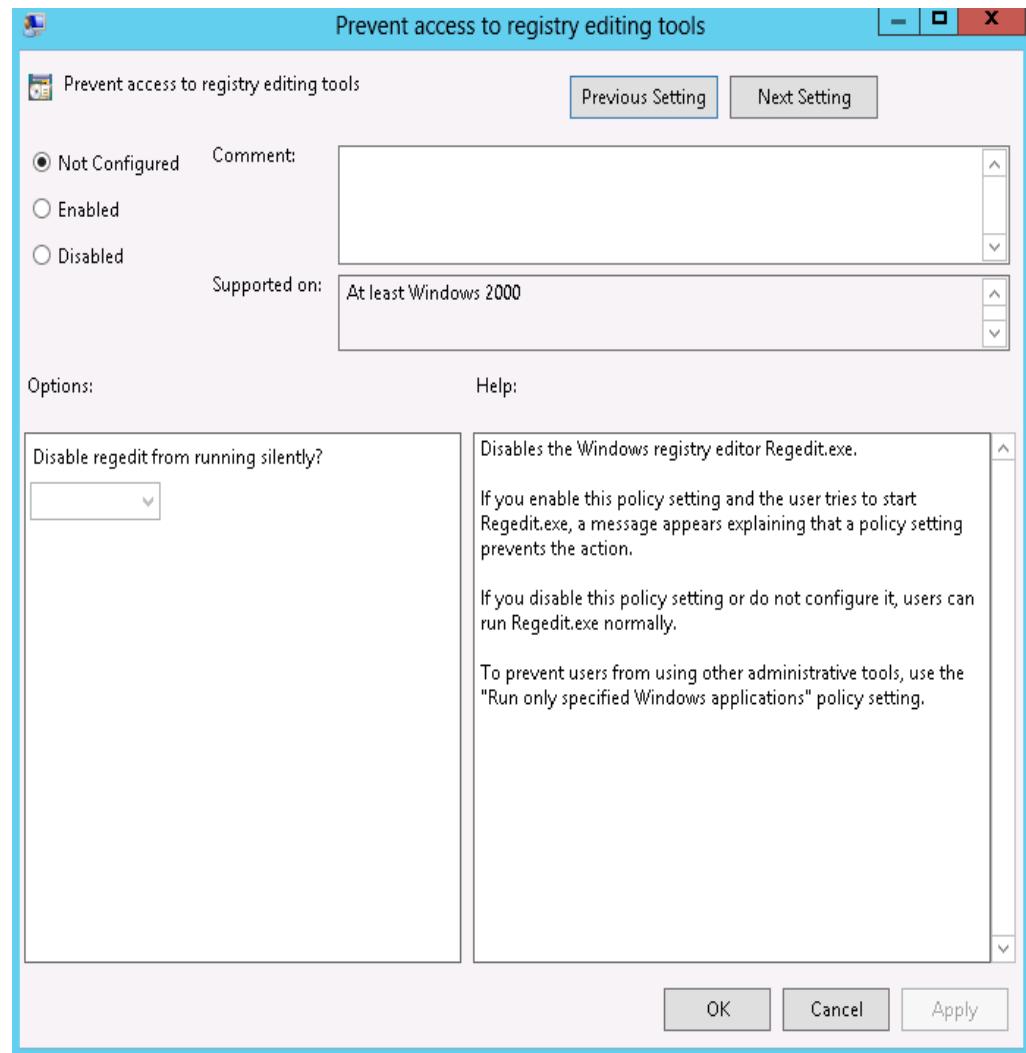
# What Are Administrative Templates?

**Administrative Templates determine what settings appear and how they are grouped in the Group Policy Management Editor window**



# How Administrative Templates Work

- Changing policy settings in the Administrative Templates node also changes the registry
- Changing the Prevent access to registry editing tools setting changes the value of HKLM\Software\Classes\Regedit



# Managed and Unmanaged Policy Settings

## Managed policy settings:

- UI is locked; user cannot make a change to the setting
- Changes are made in one of four reserved registry keys
- Change and UI locks are released when the user/computer falls out of scope

## Unmanaged policy settings:

- UI is not locked
- Changes made are persistent: tattoos the registry
- Only managed settings are shown by default
- Set Filter options to view unmanaged settings

# Lab: Implementing Group Policy

- Exercise 1: Configuring a central store
- Exercise 2: Creating GPOs

## Logon Information

Virtual machines      **20410D-LON-DC1**

**20410D-LON-CL1**

User name              **Adatum\Administrator**

Password                **Pa\$\$w0rd**

**Estimated Time: 45 minutes**

# Lab Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, England. An IT office and a data center are located in London to support the London location and other locations. A. Datum has recently deployed a Windows Server 2012 infrastructure with Windows 8 clients.

In your role as a member of the server support team, you help to deploy and configure new servers and services into the existing infrastructure based on the instructions given to you by your IT manager.

Your manager has asked you to create a central store for ADMX files to ensure that everyone can edit GPOs that have been created with customized ADMX files. You also need to create a starter GPO that includes Internet Explorer settings, and then configure a GPO that applies GPO settings for the Marketing department and the IT department.

# Lab Review

- What is the difference between ADMX and ADML files?
- The Sales Managers group should be exempted from the desktop lockdown policy that is being applied to the entire Sales OU. All sales user accounts and sales groups reside in the Sales OU. How would you exempt the Sales Managers group?
- What Windows command can you use to force the immediate refresh of all GPOs on a client computer?

# Module Review and Takeaways

- Review Questions
- Best Practices
- Common Issues and Troubleshooting Tips
- Tools

# Microsoft® Official Course



## Module 12

Securing Windows Servers by  
Using Group Policy Objects

# Module Overview

- Security Overview for Windows Operating Systems
- Configuring Security Settings
- Restricting Software
- Configuring Windows Firewall with Advanced Security

# Lesson 1: Security Overview for Windows Operating Systems

- Discussion: Identifying Security Risks and Costs
- Applying Defense-In-Depth to Increase Security
- Best Practices for Increasing Security

# Discussion: Identifying Security Risks and Costs

- What are some of security risks in Windows-based networks?

10 minutes



# Applying Defense-In-Depth to Increase Security

Defense-in-depth uses a layered approach to security

- Reduces an attacker's chance of success
- Increases an attacker's risk of detection

|                                            |                                                 |
|--------------------------------------------|-------------------------------------------------|
| <b>Policies, procedures, and awareness</b> | Security documents, user education              |
| <b>Physical security</b>                   | Guards, locks, tracking devices                 |
| <b>Perimeter</b>                           | Firewalls, network access quarantine control    |
| <b>Networks</b>                            | Network segments, IPsec, Reverse proxy servers  |
| <b>Host</b>                                | Hardening, authentication, update management    |
| <b>Application</b>                         | Application hardening, antivirus                |
| <b>Data</b>                                | ACLs, EFS, BitLocker, backup/restore procedures |

# Best Practices for Increasing Security

Some best practices for increasing security are:

- Apply all available security updates quickly
- Follow the principle of least privilege
- Use separate administrative accounts
- Restrict administrator console sign-in
- Restrict physical access



# Lesson 2: Configuring Security Settings

- Configuring Security Templates
- Configuring User Rights
- Configuring Security Options
- Configuring User Account Control
- Configuring Security Auditing
- Configuring Restricted Groups
- Configuring Account Policy Settings
- What Is Security Compliance Manager?

# Configuring Security Templates

## **Security Templates categories:**

- Account policies
- Local policies
- Event log
- Restricted groups
- System services
- Registry
- File system

## **Security templates are distributed by using:**

- The **secedit** command-line tool
- The Security Templates snap-in
- The Security Configuration and Analysis Wizard
- Group Policy
- The Security Compliance Manager

# Configuring User Rights

## User Rights Types:

- Privileges
- Logon rights



## Examples of common user rights:

- Add workstations to domain
- Allow log on locally
- Allow log on through Remote Desktop Services
- Back up files and directories
- Change the system time
- Force shutdown from a remote computer
- Shut down the system

# Configuring Security Options

## **Security options settings:**

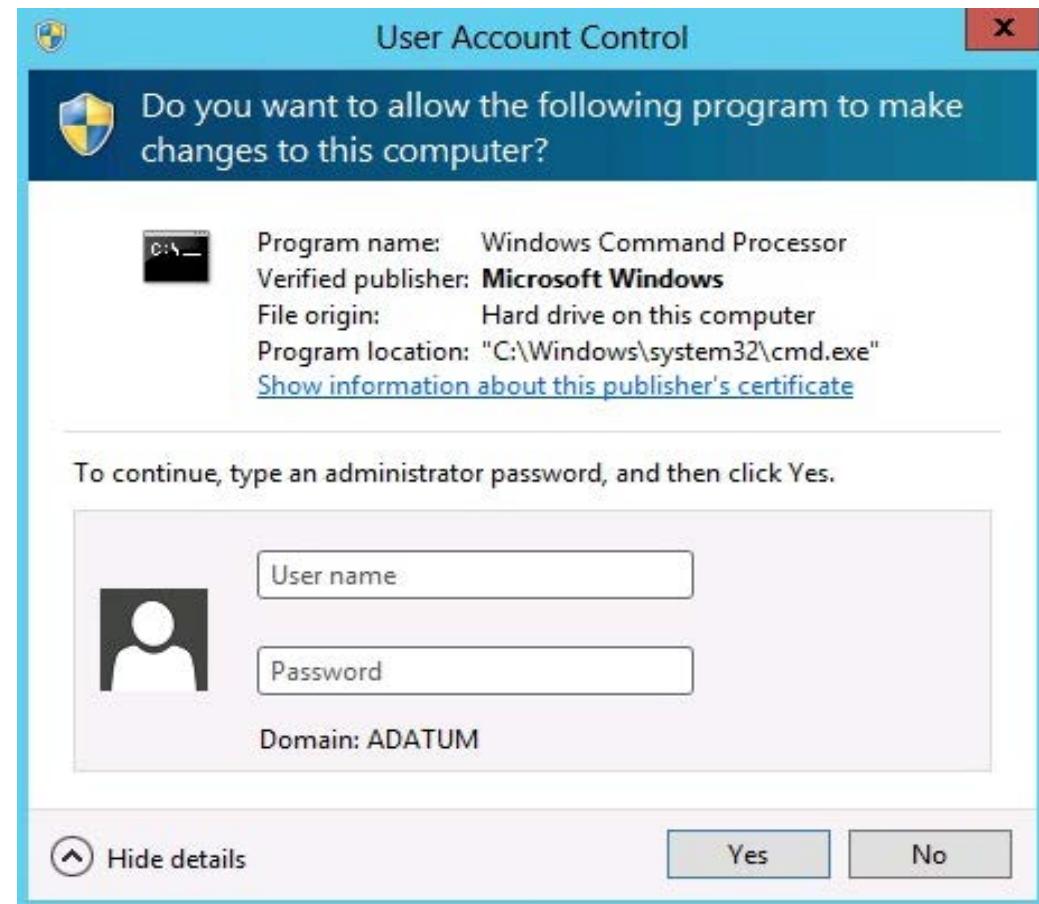
- Administrator and Guest account names
- Access to CD/DVD drives
- Digital data signatures
- Driver installation behavior
- Logon prompts
- UAC

## **Examples:**

- Prompt user to change password before expiration
- Do not display last user name
- Specify a message to be displayed when users are logging on
- Rename administrator account

# Configuring User Account Control

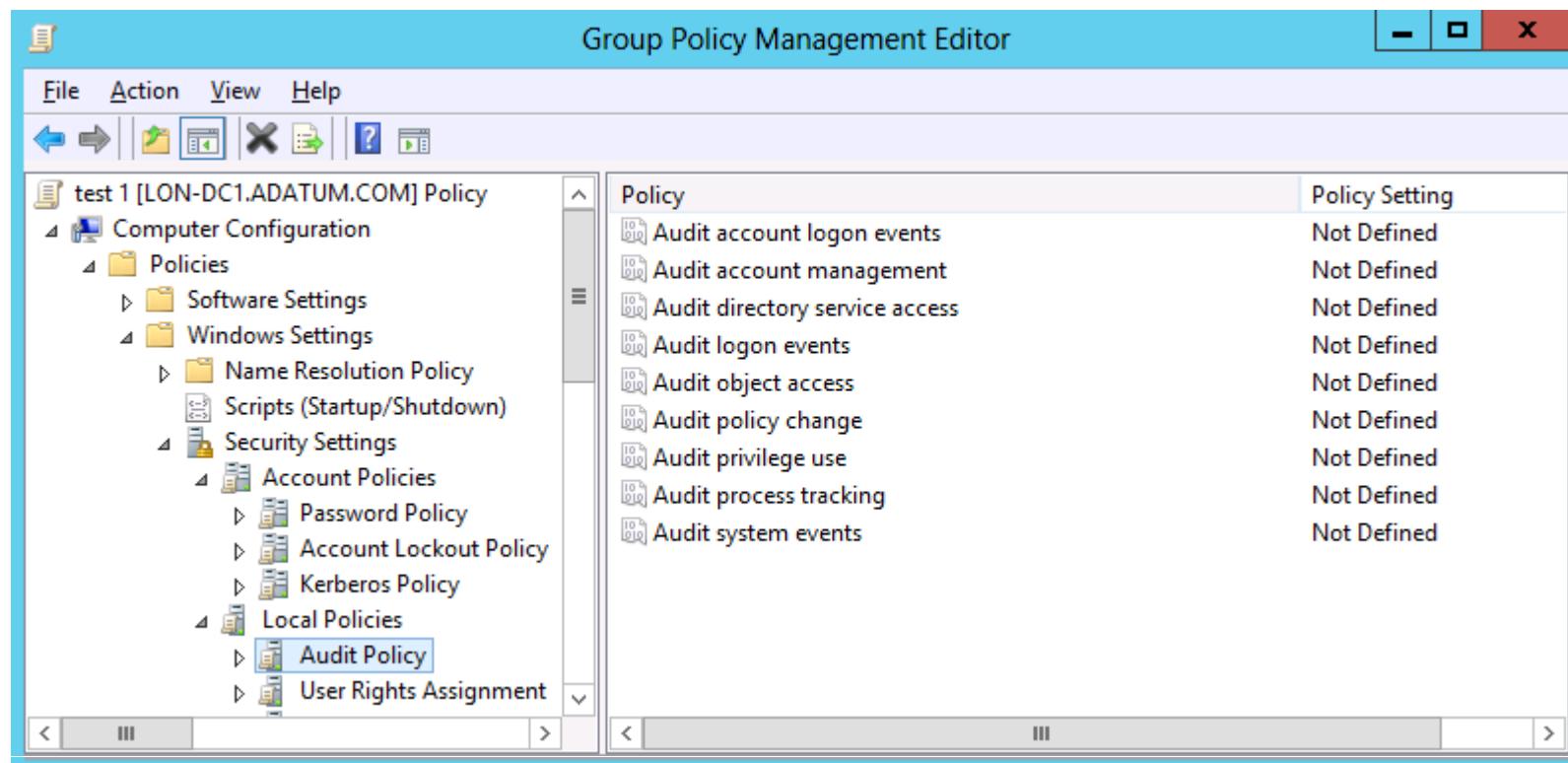
- UAC is a security feature that prompts the user for an administrative user's credentials if the task requires administrative permissions
- UAC enables users to perform common daily tasks as non-administrators



# Configuring Security Auditing

When using security auditing to log security-related events, you can:

- Configure security auditing according to your company's security regulations
- Filter the Security Event Log in Event Viewer to find specific security related events



# Configuring Restricted Groups

Group Policy can control group membership:

- For any group on a domain-joined computer, by applying a GPO to the OU that contains the computer account
- For any group in AD DS, by applying a GPO to the domain controller's OU

Be aware of problems that might arise from using policies for domain-based groups, and refer to the student handbook for more information

# Configuring Account Policy Settings

Account policies reduce the threat of brute force guessing of account passwords

| Policies        | Default settings                                                                                                                                                                                                                                                                                                     |
|-----------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Password        | <ul style="list-style-type: none"><li>• Controls complexity and lifetime of passwords</li><li>• Max password age: 42 days</li><li>• Min password age: 1 day</li><li>• Min password length: 7 characters</li><li>• Complex password: enabled</li><li>• Store password using reversible encryption: disabled</li></ul> |
| Account lockout | <ul style="list-style-type: none"><li>• Controls how many incorrect attempts can be made</li><li>• Lockout duration: not defined</li><li>• Lockout threshold: 0 invalid logon attempts</li><li>• Reset account lockout after: not defined</li></ul>                                                                  |
| Kerberos        | <ul style="list-style-type: none"><li>• Subset of the attributes of domain security policy</li><li>• Can only be applied at the domain level</li></ul>                                                                                                                                                               |

# What Is Security Compliance Manager?

SCM is a free tool from Microsoft that helps you secure local, remote, or virtualized computers. It features:

- Baselines
- Security guides
- Support for standalone computers
- Support for import GPO backups

You can use SCM to:

- Validate that computers are configured for compliance
- Reduce the work involved in configuring computers for compliance
- Move, compare and merge settings across two independent environments
- Formulate and update your security policies

# Lab A: Increasing Security for Server Resources

- Exercise 1: Using Group Policy to Secure Member Servers
- Exercise 2: Auditing File System Access
- Exercise 3: Auditing Domain Logons

## Logon Information

|                  |                                                                                                    |
|------------------|----------------------------------------------------------------------------------------------------|
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b><br><b>20410D-LON-SVR2</b><br><b>20410D-LON-CL1</b> |
| User name        | <b>Adatum\Administrator</b>                                                                        |
| Password         | <b>Pa\$\$w0rd</b>                                                                                  |

**Estimated Time: 50 minutes**

## Lab Scenario

Your manager has given you some security-related settings that need to be implemented on all member servers. You also need to implement file system auditing for a file share used by the Marketing department. Finally, you need to implement auditing for domain logons.

# Lab Review

- What happens if you configure the Computer Administrators group, but not the Domain Admins group, to be a member of the Local Administrators group on all of a domain's computers?
- Why do you need to restrict local logon to some computers?
- What happens when an unauthorized user tries to access a folder that has auditing enabled for both successful and unsuccessful access attempts?
- What happens when you configure auditing for domain logons for both successful and unsuccessful logon attempts?

# Lesson 3: Restricting Software

- What Are Software Restriction Policies?
- What Is AppLocker?
- AppLocker Rules
- Demonstration: Creating AppLocker Rules

# What Are Software Restriction Policies?

- SRPs allow administrators to identify which apps are allowed to run on client computers
- SRPs can be based on the following:
  - Hash
  - Certificate
  - Path
  - Zone
- SRPs are applied through Group Policy

# What Is AppLocker?

AppLocker applies Application Control Policies in Windows Server 2012 and Windows 8

AppLocker contains capabilities and extensions that:

- Reduce administrative overhead
- Help administrators control how users access and use files:
  - .exe files
  - scripts
  - DLLs
  - Windows Installer files
  - Packaged apps

Benefits of AppLocker:

- Controls how users can access and run all types of apps
- Allows the definition of rules based on a wide variety of variables
- Provides for importing and exporting entire AppLocker policies

# AppLocker Rules

**AppLocker defines rules based on file attributes such as:**

- Publisher name
- Product name
- File name
- File version

**Rule actions**

- Allow or Deny conditions
- Enforce or Audit Only policies

# Demonstration: Creating AppLocker Rules

In this demonstration, you will see how to:

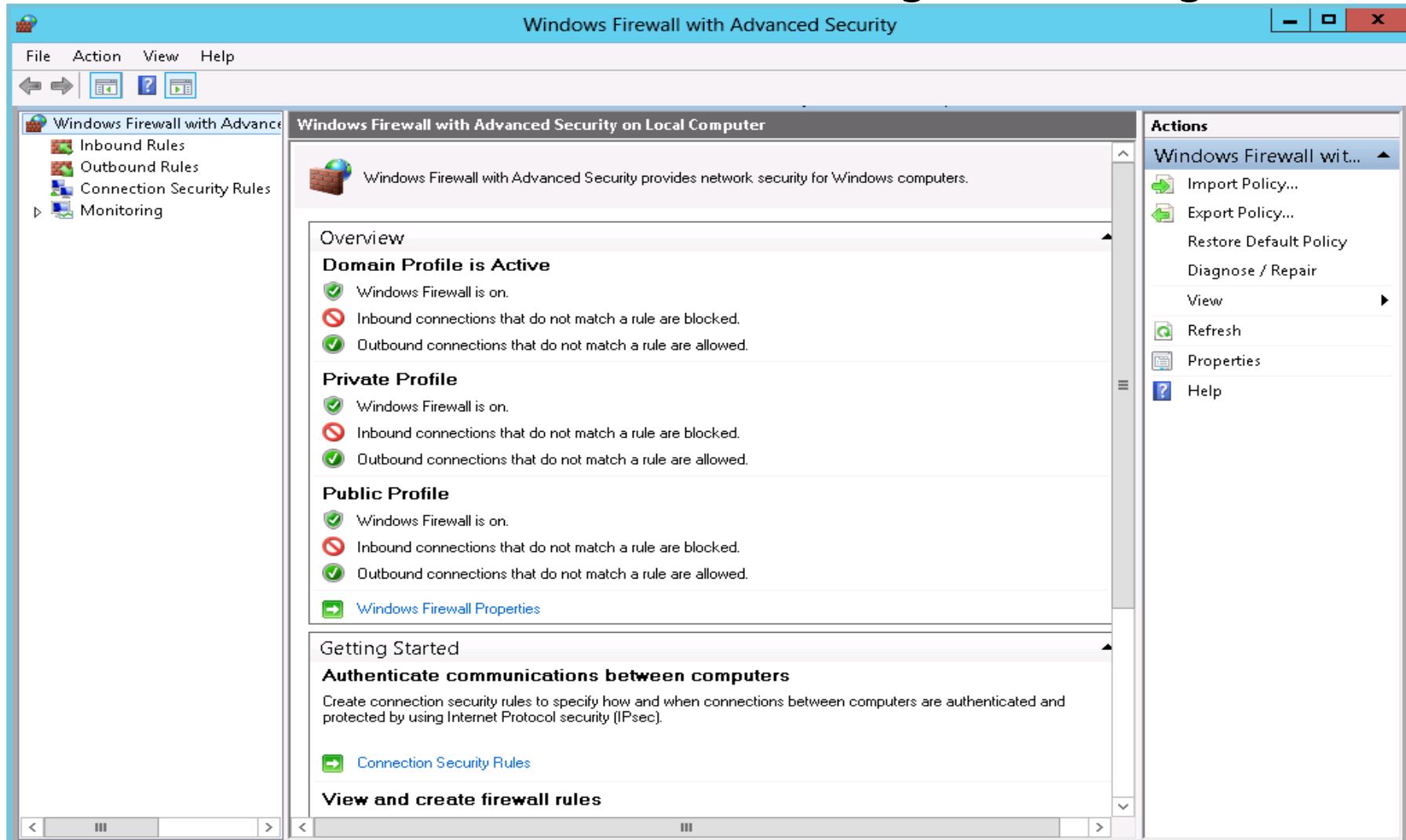
- Create a GPO to enforce the default AppLocker Executable rules
- Apply the GPO to the domain
- Test the AppLocker rule

# Lesson 4: Configuring Windows Firewall with Advanced Security

- What Is Windows Firewall with Advanced Security?
- Discussion: Why Is a Host-Based Firewall Important?
- Firewall Profiles
- Connection Security Rules
- Deploying Firewall Rules
- Demonstration: Implementing Secured Network Traffic with Windows Firewall

# What Is Windows Firewall with Advanced Security?

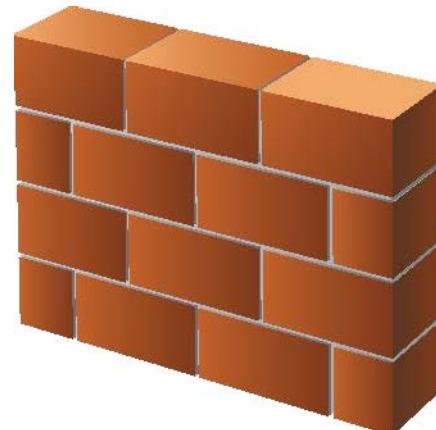
Windows Firewall is a stateful, host-based firewall that allows or blocks network traffic according to its configuration



# What Is Windows Firewall with Advanced Security?

The benefits of Windows Firewall include that it:

- Supports filtering for both incoming and outgoing traffic
- Integrates firewall filtering and IPsec protection settings
- Enables you to configure rules to control network traffic
- Provides network location-aware profiles
- Enables you to import or export policies



# Discussion: Why Is a Host-Based Firewall Important?

- Why is it important to use a host-based firewall such as Windows Firewall with Advanced Security?

10 minutes



# Firewall Profiles

- Firewall profiles are a set of configuration settings that apply to a particular network type
- The firewall profiles are:
  - Domain
  - Public
  - Private
- Windows Server 2012 includes the ability to have multiple active firewall profiles

# Connection Security Rules

## Connection security rules:

- Authenticate two computers before they begin communications
- Secure information being sent between two computers
- Use key exchange, authentication, data integrity, and data encryption (optionally)

## How firewall rules and connection rules are related:

- Firewall rules allow traffic through, but do not secure that traffic
- Connection security rules can secure the traffic, but only if a firewall rule was previously configured

# Deploying Firewall Rules

You can deploy Windows Firewall rules:

- **Manually.** Used during testing, troubleshooting, or for individual computers.
- **By using Group Policy.** The preferred way. Create and test the rules, and then deploy them to a large number of computers.
- **By exporting and importing.** Uses Windows Firewall with Advanced Security.

When you import rules, they replace all current rules.

Always test firewall rules in an isolated, nonproduction environment before you deploy them in production.



# Demonstration: Implementing Secured Network Traffic with Windows Firewall

In this demonstration, you will see how to:

- Check to see if ICMP v4 is blocked
- Enable ICMP v4 from LON-CL2 to LON-SVR2
- Create a connection security rule so that traffic is authenticated to the destination host
- Validate ICMP v4 after the connection security rule is in place

# Lab B: Configuring AppLocker and Windows Firewall

- Exercise 1: Configuring AppLocker Policies
- Exercise 2: Configuring Windows Firewall

## Logon Information

|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b><br><b>20410D-LON-CL1</b> |
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

**Estimated Time: 60 minutes**

## Lab Scenario

Your manager has asked you to implement AppLocker to restrict nonstandard applications from running. He also has asked you to create new Windows Firewall rules for any member servers running web-based applications.

# Lab Review

- You configured an AppLocker rule that prevents users from running software in a specified file path. How can you prevent users from moving the folder containing the software so that they can circumvent the rule and still run it?
- You want to introduce a new application that needs to use specific ports. What information do you need to configure Windows Firewall with Advanced Security, and from what source can you get it?

# Module Review and Takeaways

- Review Questions
- Best Practices
- Common Issues and Troubleshooting Tips
- Tools

# Microsoft® Official Course



## Module 13

### Implementing Server Virtualization with Hyper-V

**Microsoft®**

# Module Overview

- Overview of Virtualization Technologies
- Implementing Hyper-V
- Managing Virtual Machine Storage
- Managing Virtual Networks

# Lesson 1: Overview of Virtualization Technologies

- Server Virtualization
- What Is Windows Azure?
- Desktop Virtualization
- Presentation Virtualization
- What Is Microsoft Application Virtualization?

# Server Virtualization

Benefits of server virtualization with Hyper-V include:

- Invisible to users
- Guest machines can use different operating systems
- More efficient use of hardware
- Service and application isolation
- Workload consolidation
- Simplifies server deployment by using:
  - Virtual machine templates
  - App-Controller virtual machine self-service portal

# What Is Windows Azure?

- Windows Azure is a cloud-based platform for hosting virtual machines and applications
- You pay only for the resources that you use
- You can increase and decrease capacity automatically and swiftly
- You can use Windows Azure to:
  - Host websites
  - Host production applications
  - Host virtual machines
  - Test proof-of-concept solutions

# Desktop Virtualization

Desktop virtualization includes the following technologies:

- Client (Local) Hyper-V
- VDI

RemoteFX allow virtual machines to display rich graphics and video capabilities

RemoteFX requires:

- GPU that supports DirectX 9.0c or newer
- CPU that supports SLAT

# Presentation Virtualization

## Differences between desktop virtualization and presentation virtualization

### Desktop virtualization:

- Users are assigned their own virtual machines that are running a client operating system
- The desktop and apps run within virtual machines

### Presentation virtualization:

- Users sign in and run separate sessions on the server
- The desktop and apps run on the host server

## Presentation virtualization technologies include:

- Remote Desktop Services
- Full Desktop with RDC
- Applications using RemoteApp
- Remote Access through RD Gateway

# What Is Microsoft Application Virtualization?

## Benefits of App-V

- App isolation
- Incompatible programs can run on the same server
- App streaming
- App deployment is quicker
- App portability
- Apps can follow users across multiple computers

## UE-V

- App and operating system settings follow users across multiple computers

## Lesson 2: Implementing Hyper-V

- What Is Hyper-V?
- Hardware Requirements for Hyper-V
- Virtual Machine Hardware
- Generation 2 Virtual Machines
- What Is Dynamic Memory?
- Configuring Virtual Machine Integration Services
- Configuring Virtual Machine Start and Stop Actions
- Hyper-V Resource Metering
- What's New with Hyper-V in Windows Server 2012 R2

# What Is Hyper-V?

Hyper-V:

- Is the hardware virtualization role in Windows Server 2012
- Gives virtual machine guests direct access to the host's hardware

Compatible Windows Server operating systems:

- Windows Server 2012
- Microsoft Hyper-V Server 2012

# Hardware Requirements for Hyper-V

Factors to consider when planning hardware for servers running Hyper-V:

- Processor characteristics
  - Must have an x64 platform that supports hardware assisted virtualization and Data Execution Protection
- Processing capacity
- Memory
- Storage subsystem performance
- Network throughput (typically multiple network interface cards)

# Virtual Machine Hardware

Virtual machines have the following simulated hardware by default:

- BIOS
- Memory
- Processor
- IDE Controller 0 and 1
- SCSI Controller
- Synthetic Network Adapter
- COM 1 and 2
- Diskette Drive

You can add the following hardware to a virtual machine:

- SCSI Controller (up to 4)
- Network Adapter
- Legacy Network Adapter
- Fibre Channel adapter
- RemoteFX 3D video adapter

# Generation 2 Virtual Machines

Generation 2 virtual machines differ from generation 1 virtual machines:

- Emulated devices are removed
- UEFI firmware instead of BIOS
  - Secure Boot
  - Boots from SCSI controller
  - PXE boot uses a standard network adapter
- Faster boot and operating system installation
- Can run side-by-side with generation 1
  - Generation 1 must be used for legacy systems
- Supported guest operating systems:
  - Windows Server 2012 and Windows Server 2012 R2
  - 64-bit versions of Windows 8 and Windows 8.1

# What Is Dynamic Memory?

## Dynamic Memory settings for a virtual machine

 Memory

You can configure options for assigning and managing memory for this virtual machine. Specify the amount of memory that this virtual machine will be started with.

Startup RAM:  MB

Dynamic Memory

You can manage the amount of memory assigned to this virtual machine dynamically within the specified range.

Enable Dynamic Memory

Minimum RAM:  MB

Maximum RAM:  MB

Specify the percentage of memory that Hyper-V should try to reserve as a buffer. Hyper-V uses the percentage and the current demand for memory to determine an amount of memory for the buffer.

Memory buffer:  %

Memory weight

Specify how to prioritize the availability of memory for this virtual machine compared to other virtual machines on this computer.

Low  High

# Configuring Virtual Machine Integration Services

Possible integration services include:

- Operating system shutdown
- Time synchronization
- Data exchange
- Heartbeat
- Backup (volume snapshot)

Enhanced session mode allows a connection to a virtual machine that is similar to remote desktop because it:

- Enables device redirection
- Uses a shared clipboard
- Enables folder redirection

# Configuring Virtual Machine Start and Stop Actions

Possible automatic start actions:

- Nothing
- Automatically start if it was running when the service stopped
- Always start this virtual machine automatically

Possible automatic stop actions:

- Save the virtual machine state
- Turn off the virtual machine
- Shut down the guest operating system

# Hyper-V Resource Metering

Parameters that you can measure with resource metering:

- Average CPU use
- Average physical memory use, including:
  - Minimum memory use
  - Maximum memory use
- Maximum disk space allocation
- Incoming network traffic for a network adapter
- Outgoing network traffic for a network adapter

# What's New with Hyper-V in Windows Server 2012 R2

---

| New or Improved                       | Feature                                                                                                                                                                                                                                          |
|---------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| New to<br>Windows Server 2012 R2      | <ul style="list-style-type: none"><li>• Shared virtual hard disk</li><li>• Automatic virtual machine activation</li><li>• Enhanced session mode</li><li>• Storage quality of service</li><li>• Virtual machine generation</li></ul>              |
| Improved in<br>Windows Server 2012 R2 | <ul style="list-style-type: none"><li>• Resize virtual hard disk</li><li>• Live migration</li><li>• Failover Clustering</li><li>• Integration services</li><li>• Export</li><li>• Replica</li><li>• Linux support</li><li>• Management</li></ul> |

# Lesson 3: Managing Virtual Machine Storage

- What Is a Virtual Hard Disk?
- Creating Virtual Disk Types
- Managing Virtual Hard Disks
- Reducing Storage Needs with Differencing Virtual Hard Disks
- Using Checkpoints

# What Is a Virtual Hard Disk?

**.vhdx format provides several benefits compared to the .vhd format, including that the:**

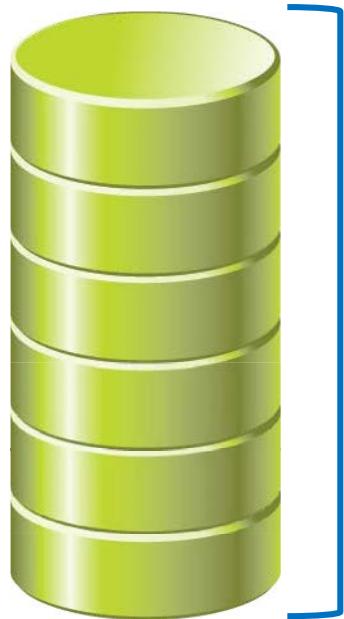
- Disks can be larger (64 TB versus 2 TB)
- Disk corruption is less likely to occur
- Format supports better alignment when deployed to a large sector disk
- Format supports larger block size for dynamic and differencing disks

**Multiple virtual machines can use shared virtual hard disks**

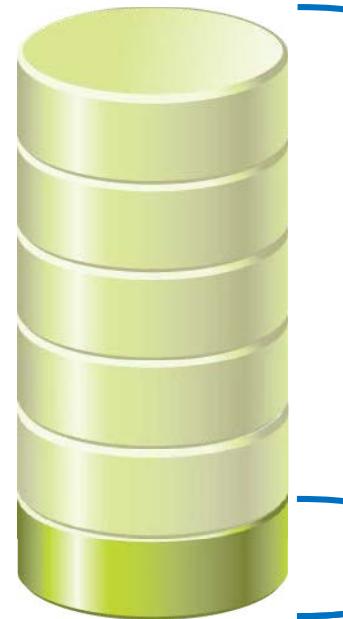
**Storage QoS allows you to limit virtual hard disk IOPS**

# Creating Virtual Disk Types

Fixed-size virtual hard disks vs.  
dynamic virtual hard disks



100 GB used  
600 GB allocated  
600 GB fixed-size disk



100 GB used  
100 GB allocated  
600 GB dynamic disk

# Managing Virtual Hard Disks

The following are maintenance operations that you can perform on virtual hard disks:

- Convert from fixed to dynamic
- Convert from dynamic to fixed
- Convert from .vhdx to .vhdx format
- Convert from .vhdx to .vhdx format
- Shrink a dynamic virtual hard disk
- Expand a dynamic or fixed virtual hard disk

# Reducing Storage Needs with Differencing Virtual Hard Disks

When using differencing disks, you:

- Can reduce space that is used by storage, but at the cost of performance
- Can link multiple differencing disks to a single parent disk
- Cannot modify the parent disk
- Can use the Inspect Disk tool to reconnect a differencing disk to a missing parent

# Using Checkpoints

## Checkpoints:

- Are static images of the data on a virtual machine at a given moment
- Are not replacements for backups
- Were called snapshots in previous versions

## Using checkpoints:

- When you create a checkpoint, Hyper-V writes to a differencing virtual hard disk
- When you apply a checkpoint, the virtual machine reverts to the configuration as it existed at the time the checkpoint was created
- You can perform a virtual machine export of a checkpoint

# Using Checkpoints

1. A checkpoint is created every day



# Using Checkpoints

1. A checkpoint is created every day
2. You locate a problem after Tuesday's checkpoint is created



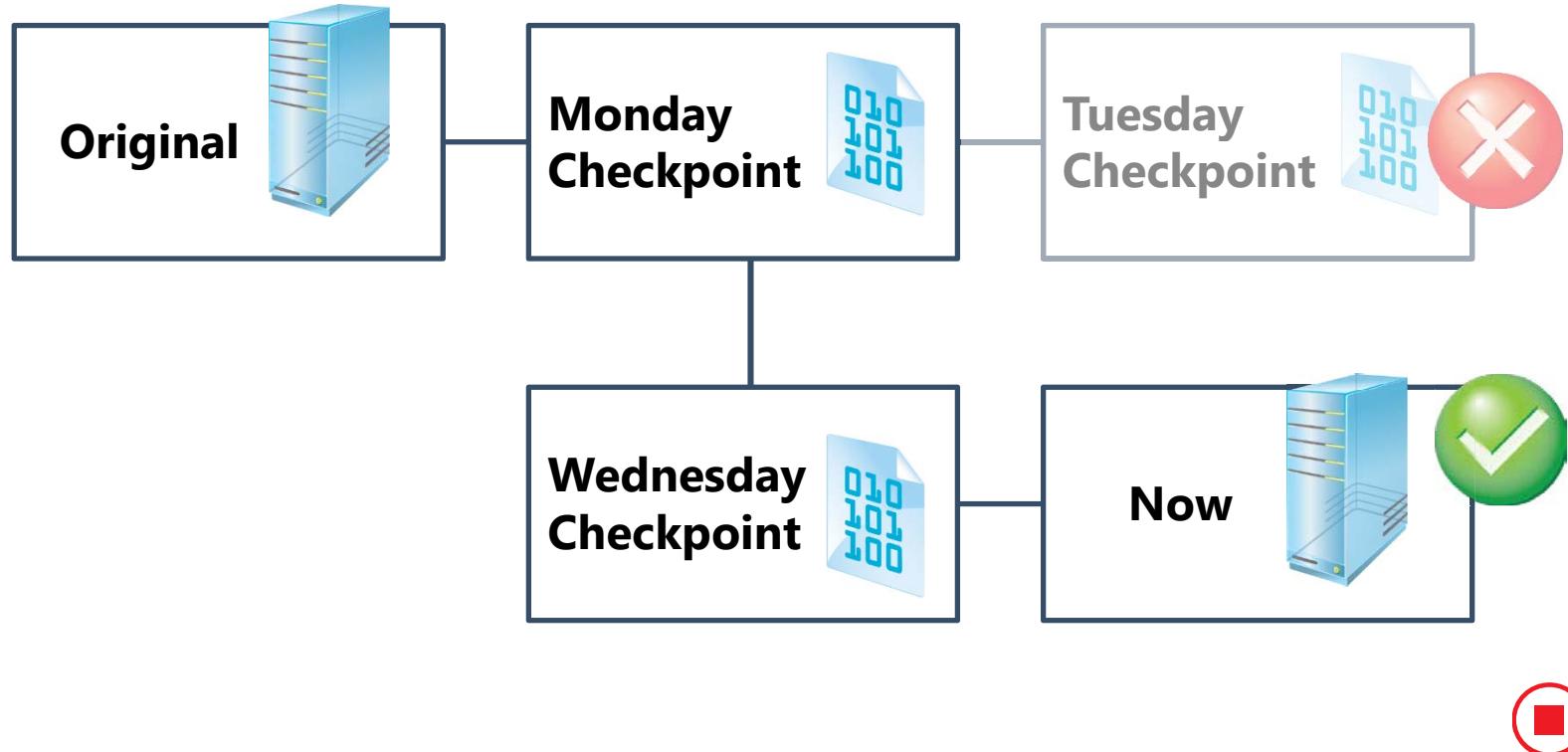
# Using Checkpoints

- 1. A checkpoint is created every day**
- 2. You locate a problem after Tuesday's checkpoint is created**
- 3. You solve the problem by reverting back to the Monday checkpoint**



# Using Checkpoints

1. A checkpoint is created every day
2. You locate a problem after Tuesday's checkpoint is created
3. You solve the problem by reverting back to the Monday checkpoint
4. The next checkpoint is created on Wednesday



# Lesson 4: Managing Virtual Networks

- What Is a Virtual Switch?
- What Are Virtual Local Area Networks?
- Virtual Switch Extensions
- Managing Virtual Machine MAC Addresses
- Configuring Virtual Network Adapters
- Network Adapter Advanced Features
- What Is NIC Teaming?

# What Is a Virtual Switch?

Hyper-V on Windows Server 2012 supports the following three types of virtual switches:

- External** Used to map a network to a specific network adapter or network adapter team
- Internal** Used to communicate between the virtual machines on the host and between the virtual machines and the host itself
- Private** Used to communicate between virtual machines, but not between the virtual machines and the host itself

# What Are Virtual Local Area Networks?

When you use VLANs, you can:

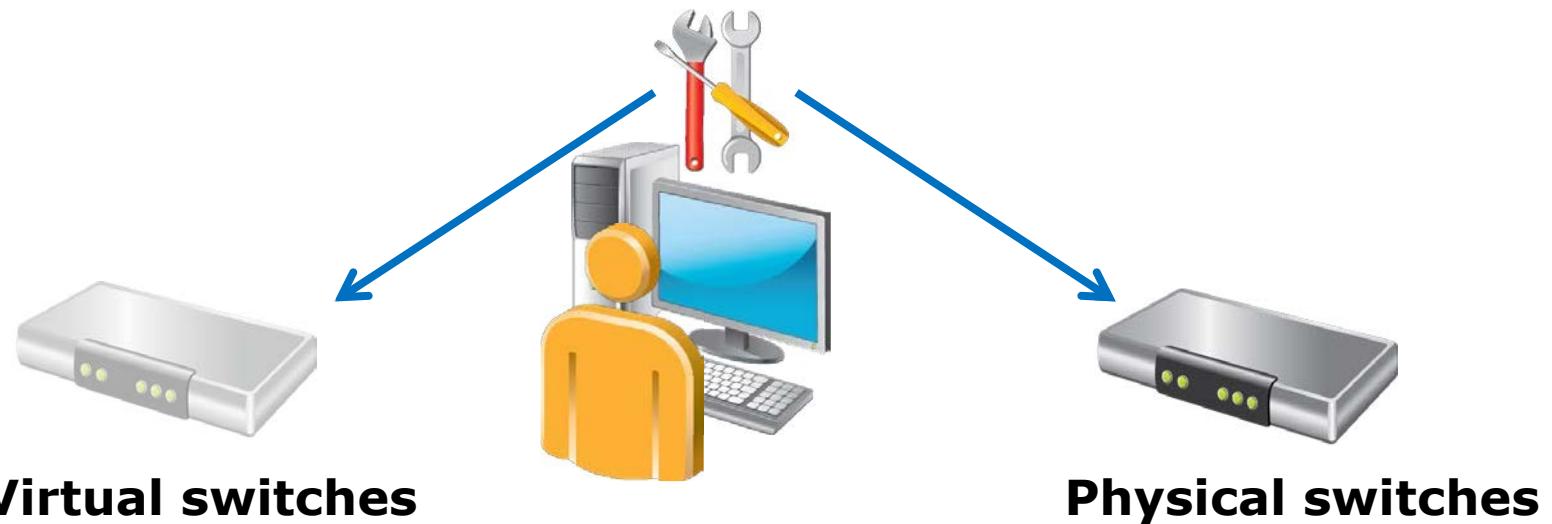
- Logically segment network traffic running on the same physical and virtual networks
- Configure tagging on each virtual switch
- Configure tagging on each virtual network adapter

Note that host network interface cards must support VLAN tagging

VLAN IDs extend VLANs within the host's network switch to VLANs on the external network

# Virtual Switch Extensions

- Virtual switch extensions enable third-party vendors to create virtual switches
- You can manage virtual switches by using the same toolset that you use to manage physical switches



# Managing Virtual Machine MAC Addresses

## Virtual Switch Manager Window

The screenshot shows the 'Virtual Switches' section of the Virtual Switch Manager. It lists several network switches: 'New virtual network switch', 'Switch for External Adapter' (Qualcomm Atheros AR8131 PCI-E ...), 'Private Network' (Private virtual switch), and 'Internal Network' (Internal only). Below this is the 'Global Network Settings' section, which displays the current MAC Address Range as '00-15-5D-0F-AB-00 to 00-15-5D-0...'. On the right, the 'MAC Address Range' configuration page is shown. It includes a descriptive text about defining a range for dynamically assigned MAC addresses, and two sets of input fields for 'Minimum' and 'Maximum' MAC addresses, both currently set to '00-15-5D-0F-AB-00' and '00-15-5D-0F-AB-FF' respectively. A note at the bottom states that changing the setting does not affect already configured adapters, and it suggests recreating the adapter if a new setting needs to be applied.

**Virtual Switches**

- New virtual network switch
- Switch for External Adapter  
Qualcomm Atheros AR8131 PCI-E ...
- Private Network  
Private virtual switch
- Internal Network  
Internal only

**Global Network Settings**

MAC Address Range  
00-15-5D-0F-AB-00 to 00-15-5D-0...

**MAC Address Range**

You can define the range of media access control (MAC) addresses that can be assigned dynamically to virtual network adapters.

Minimum:  -  -  -  -  -

Maximum:  -  -  -  -  -

**i** Changing this setting does not affect network adapters that have already been configured. To apply a new setting to an existing network adapter, recreate the network adapter by removing it and adding it again.

# Configuring Virtual Network Adapters

Properties of a network adapter:

- Virtual Switch
- VLAN ID
- Bandwidth Management

Features of a virtual network adapter:

- MAC address allocation
- DHCP Guard
- Router Guard
- Port Mirroring
- NIC Teaming

# Network Adapter Advanced Features

- Virtual Machine Queue delivers network traffic directly to the guest
- IPsec task offloading enables the host's network adapter to perform calculation-intensive security association tasks
- SR-IOV enables multiple virtual machines to share the same PCI Express physical hardware resources
- vRSS balances the network processing across multiple virtual processor cores in a virtual machine

# What Is NIC Teaming?

## NIC Teaming:

- Provides redundancy and aggregates bandwidth
- Is supported at the host and virtual machine level

## NIC Teaming in virtual machines:

- Requires multiple virtual network adapters
- Must be enabled on virtual network adapters
- Can then be implemented in the virtual machine's operating system (if supported)

# Lab: Implementing Server Virtualization with Hyper-V

- Exercise 1: Installing the Hyper-V Role onto a Server
- Exercise 2: Configuring Virtual Networking
- Exercise 3: Creating and Configuring a Virtual Machine
- Exercise 4: Using Virtual Machine Checkpoints

## Logon Information

|                 |                         |
|-----------------|-------------------------|
| Virtual machine | <b>20410D-LON-HOST1</b> |
| User name       | <b>Administrator</b>    |
| Password        | <b>Pa\$\$w0rd</b>       |

**Estimated Time: 70 minutes**

# Lab Scenario

Your assignment is to configure the infrastructure service for a new branch office.

To use the server hardware that is available currently at branch offices more effectively, your manager has decided that all branch office servers will run as virtual machines. You must now configure a virtual network and a new virtual machine for these branch offices.

# Lab Review

- What type of virtual network switch would you create if you want to allow the virtual machine to communicate with the LAN that is connected to the Hyper-V virtualization server?
- How can you ensure that no single virtual machine uses all of the available bandwidth that the Hyper-V virtualization server provides?
- What Dynamic Memory configuration task was not possible on previous versions of Hyper-V, but which you can now perform on a virtual machine that is hosted on the Hyper-V role on a Windows Server 2012 server?

# Module Review and Takeaways

- Review Questions
- Best Practices
- Common Issues and Troubleshooting Tips
- Tools

# Course Evaluation



# Microsoft® Official Course



## Module 1

### Configuring and Troubleshooting Domain Name System

**Microsoft®**

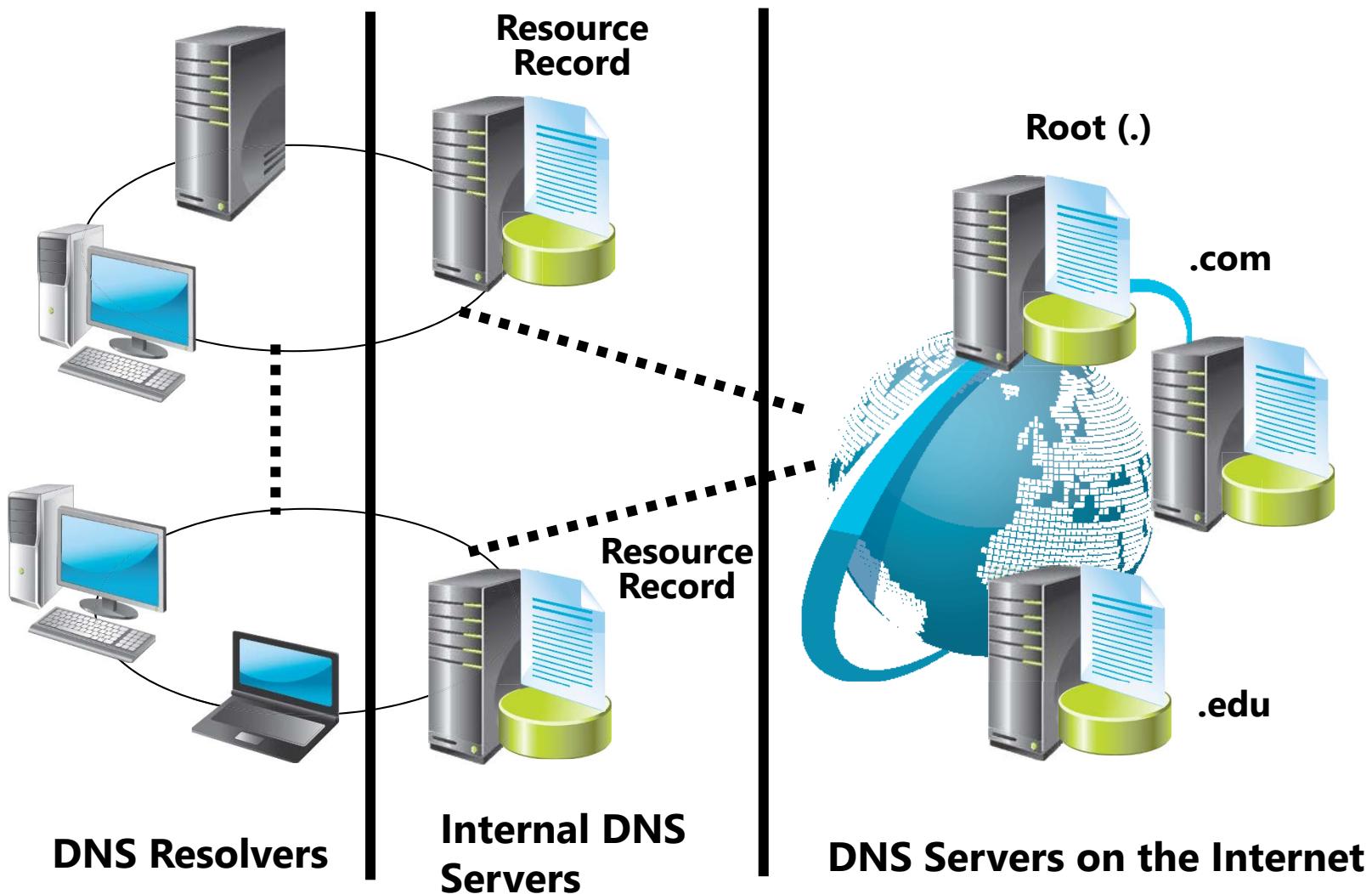
# Module Overview

- Configuring the DNS Server Role
- Configuring DNS Zones
- Configuring DNS Zone Transfers
- Managing and troubleshooting DNS

# Lesson 1: Configuring the DNS Server Role

- Components of a DNS Solution
- Demonstration: Installing the DNS Server Role
- What Are DNS Queries?
- What Are Root Hints?
- What Is Forwarding?
- How DNS Server Caching Works
- Demonstration: Configuring the DNS Server Role
- What Is DNS Round Robin?
- Considerations for Deploying the DNS Server Role

# Components of a DNS Solution



# Demonstration: Installing the DNS Server Role

In this demonstration, you will see how to install the DNS server role

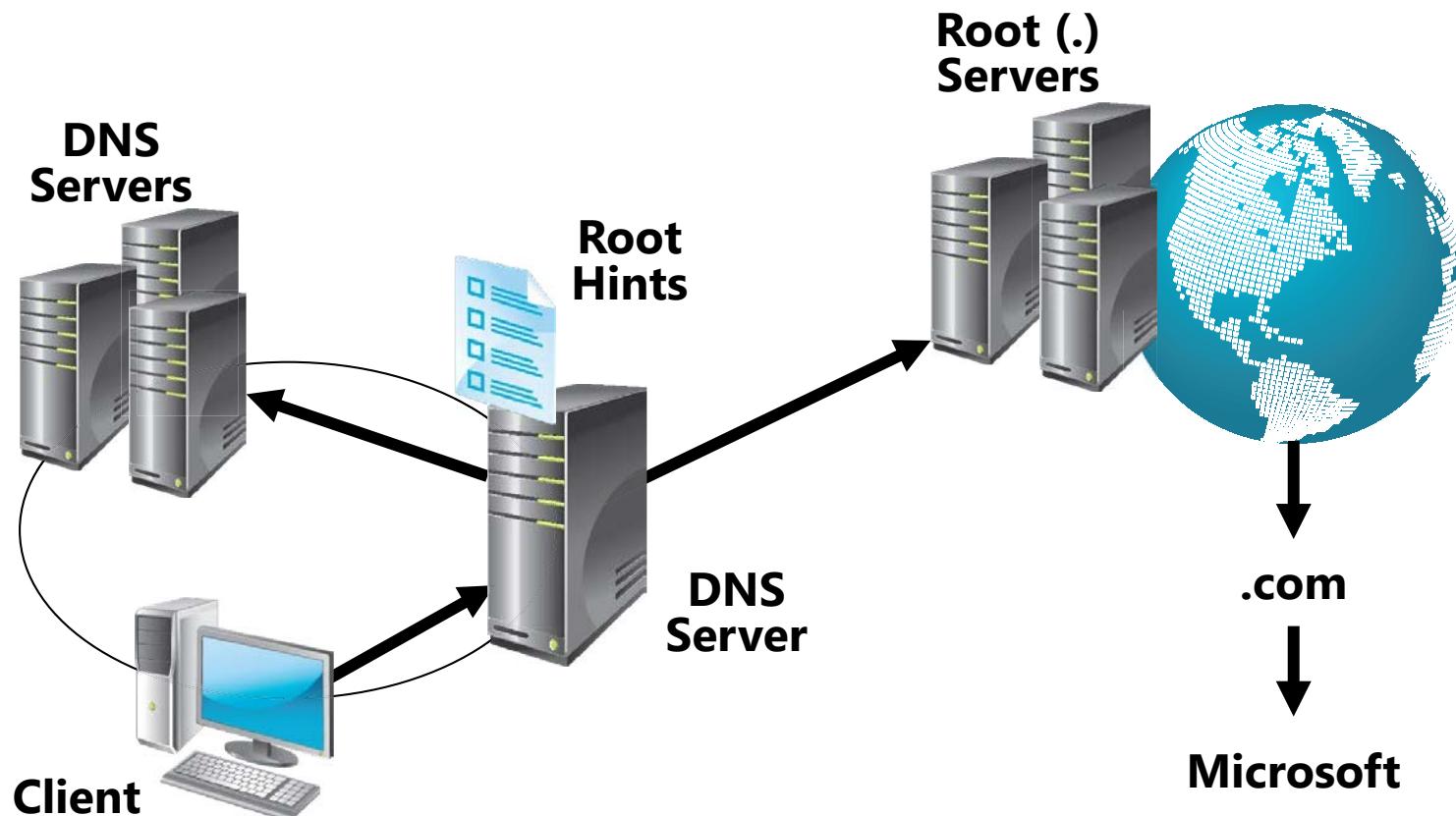
# What Are DNS Queries?

A *query* is a request for name resolution and is directed to a DNS server:

- Queries are recursive or iterative
- DNS clients and DNS servers initiate queries
- DNS servers are authoritative or nonauthoritative for a namespace
- An authoritative DNS server for the namespace will do one of the following:
  - Return the requested IP address
  - Return an authoritative “No”
- A nonauthoritative DNS server for the namespace will do one of the following:
  - Check its cache
  - Use forwarders
  - Use root hints

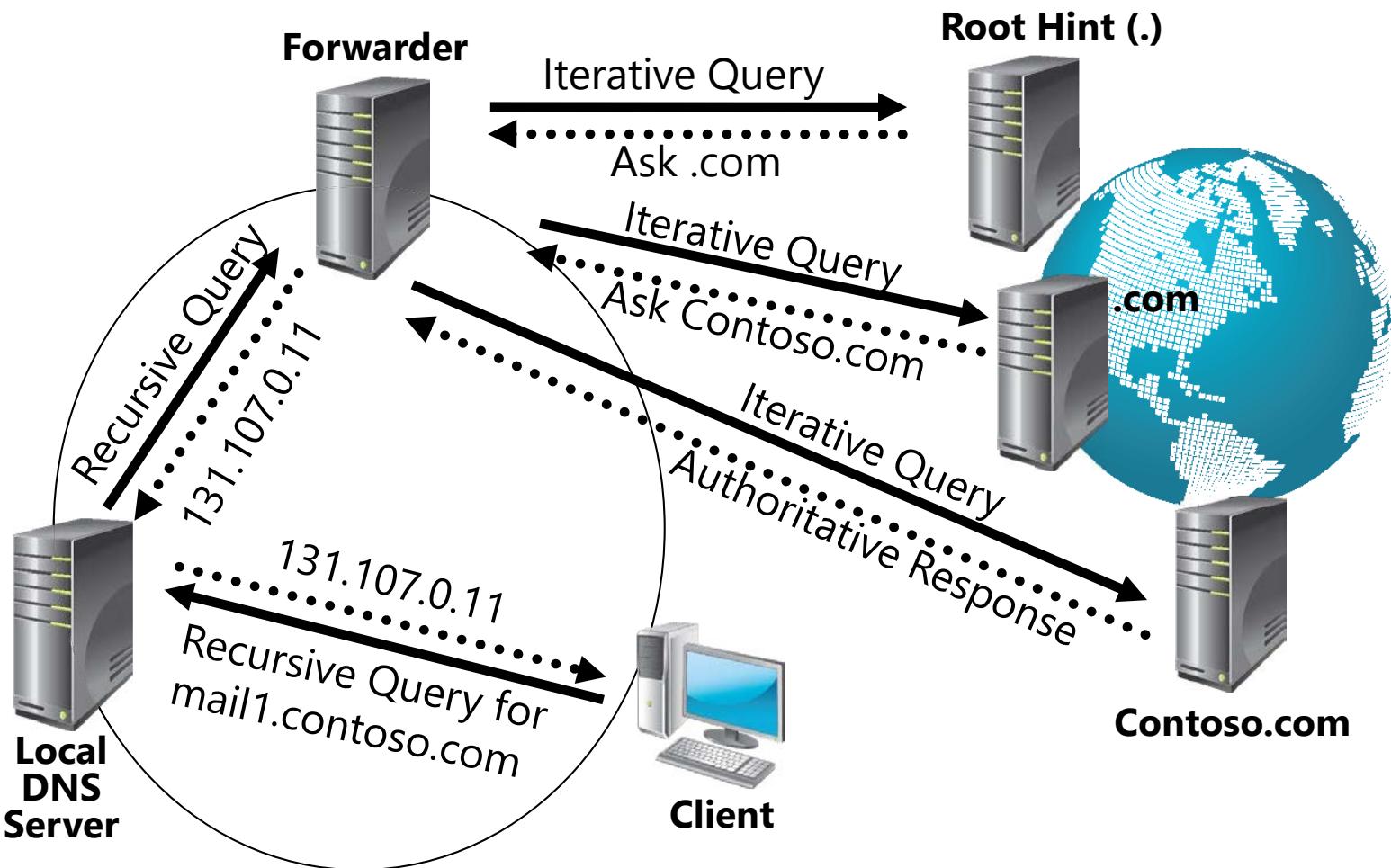
# What Are Root Hints?

Root hints contain the IP addresses for DNS root servers



# What Is Forwarding?

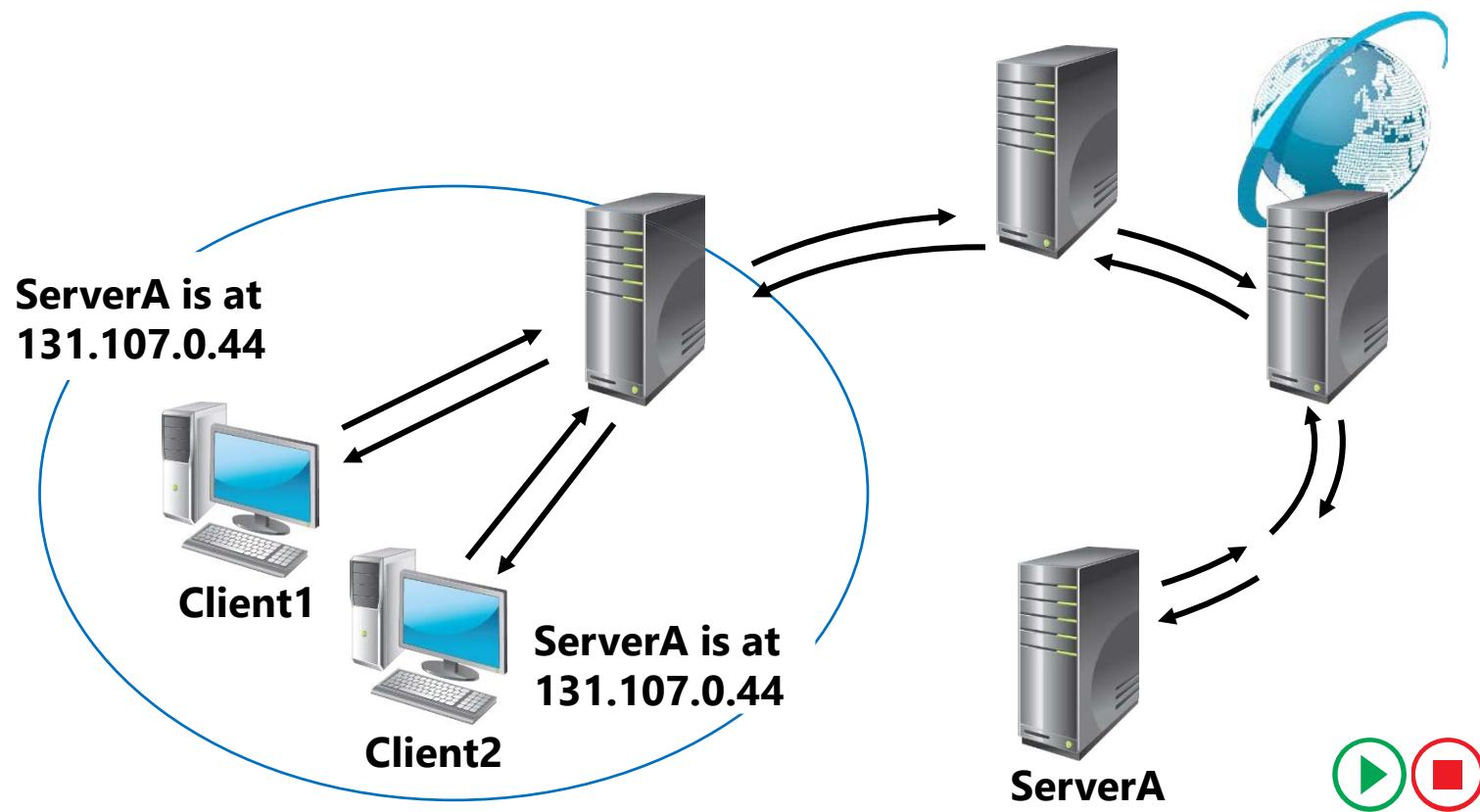
A forwarder is a DNS server that is designated to resolve external or offsite DNS domain names



# How DNS Server Caching Works

## DNS server cache

| Host name           | IP address   | TTL        |
|---------------------|--------------|------------|
| ServerA.contoso.com | 131.107.0.44 | 28 seconds |

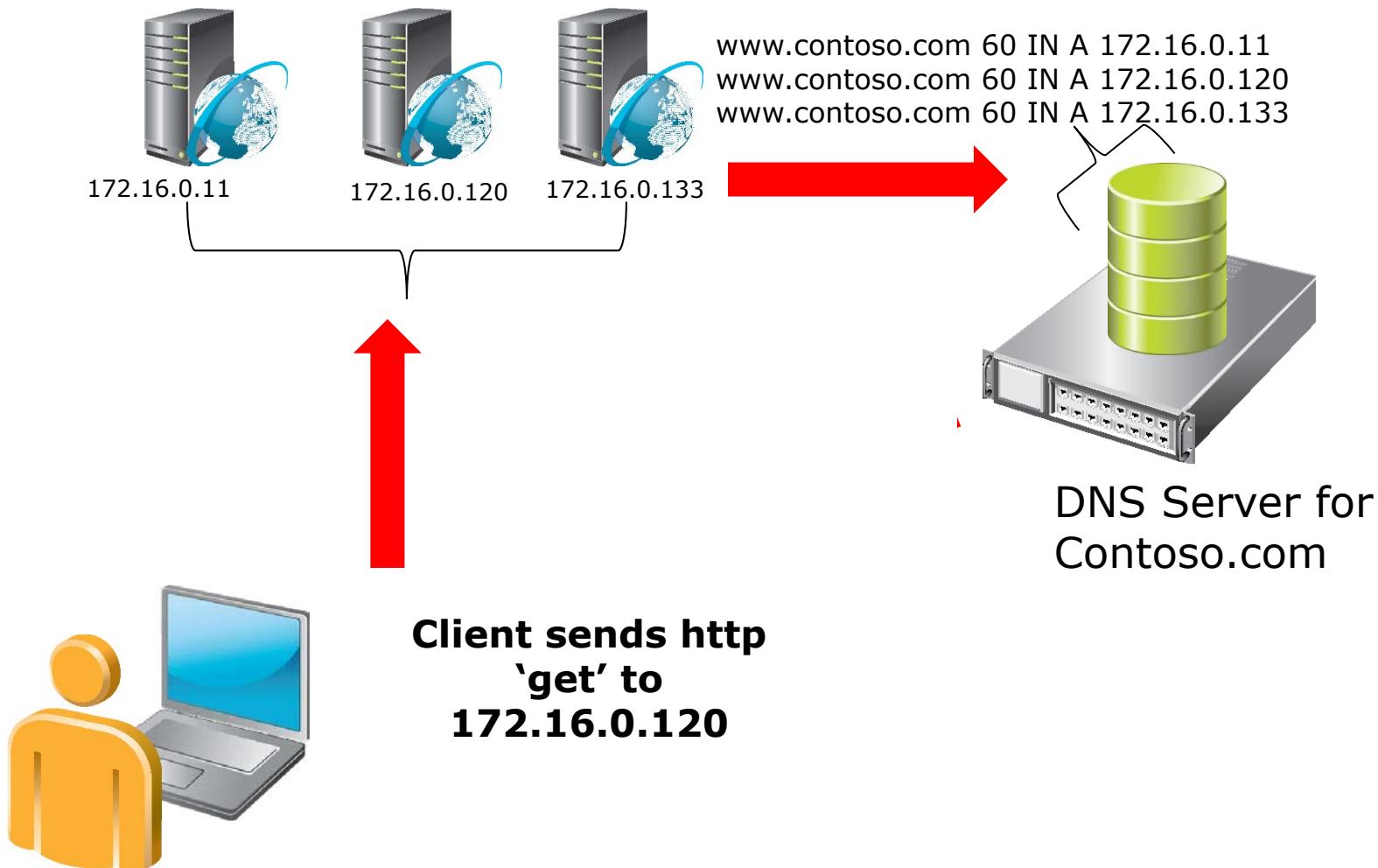


# Demonstration: Configuring the DNS Server Role

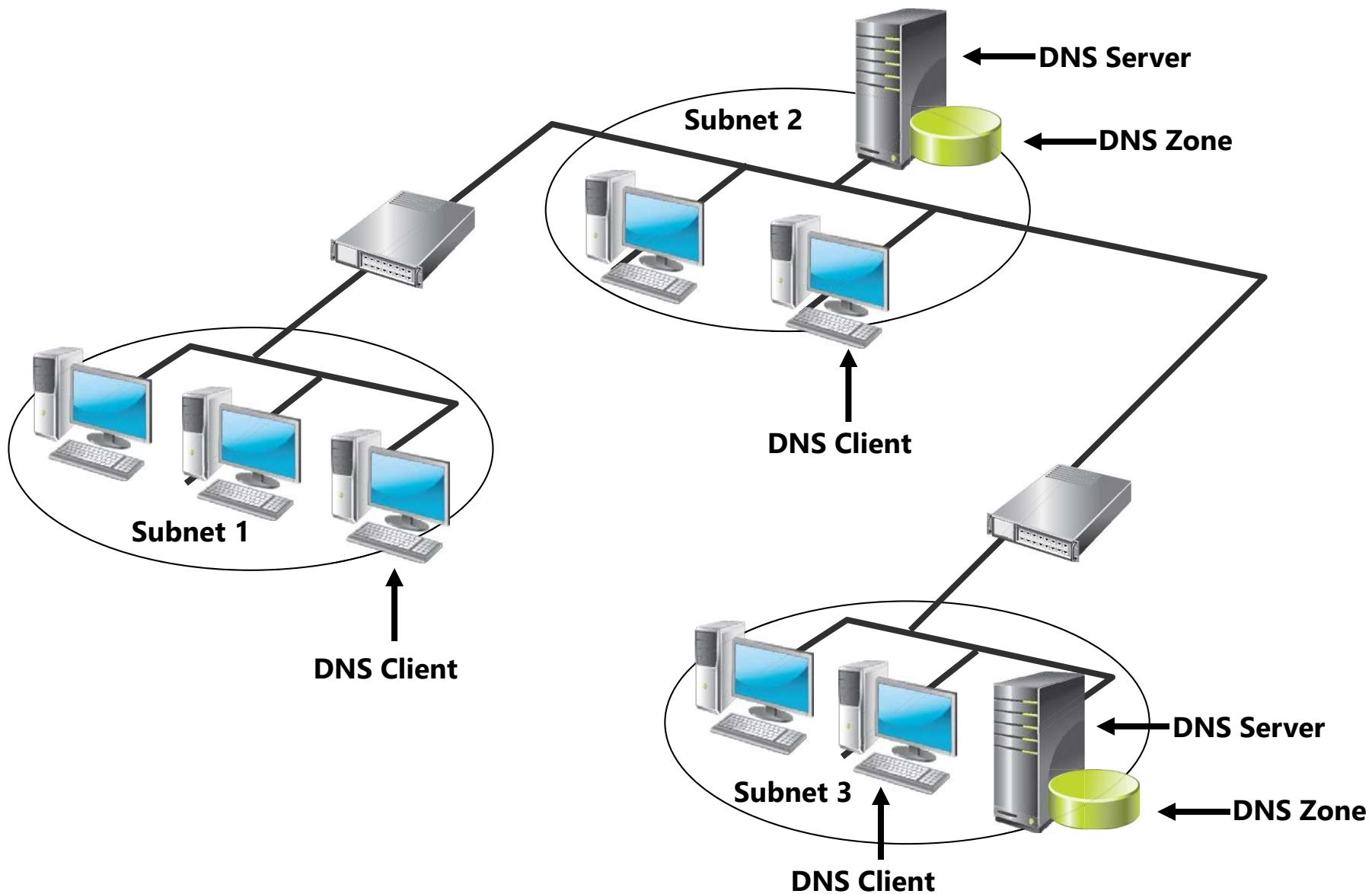
In this demonstration, you will see how to:

- Configure DNS server properties
- Configure conditional forwarding
- Clear the DNS cache

# What Is DNS Round Robin?



# Considerations for Deploying the DNS Server Role



# Lesson 2: Configuring DNS Zones

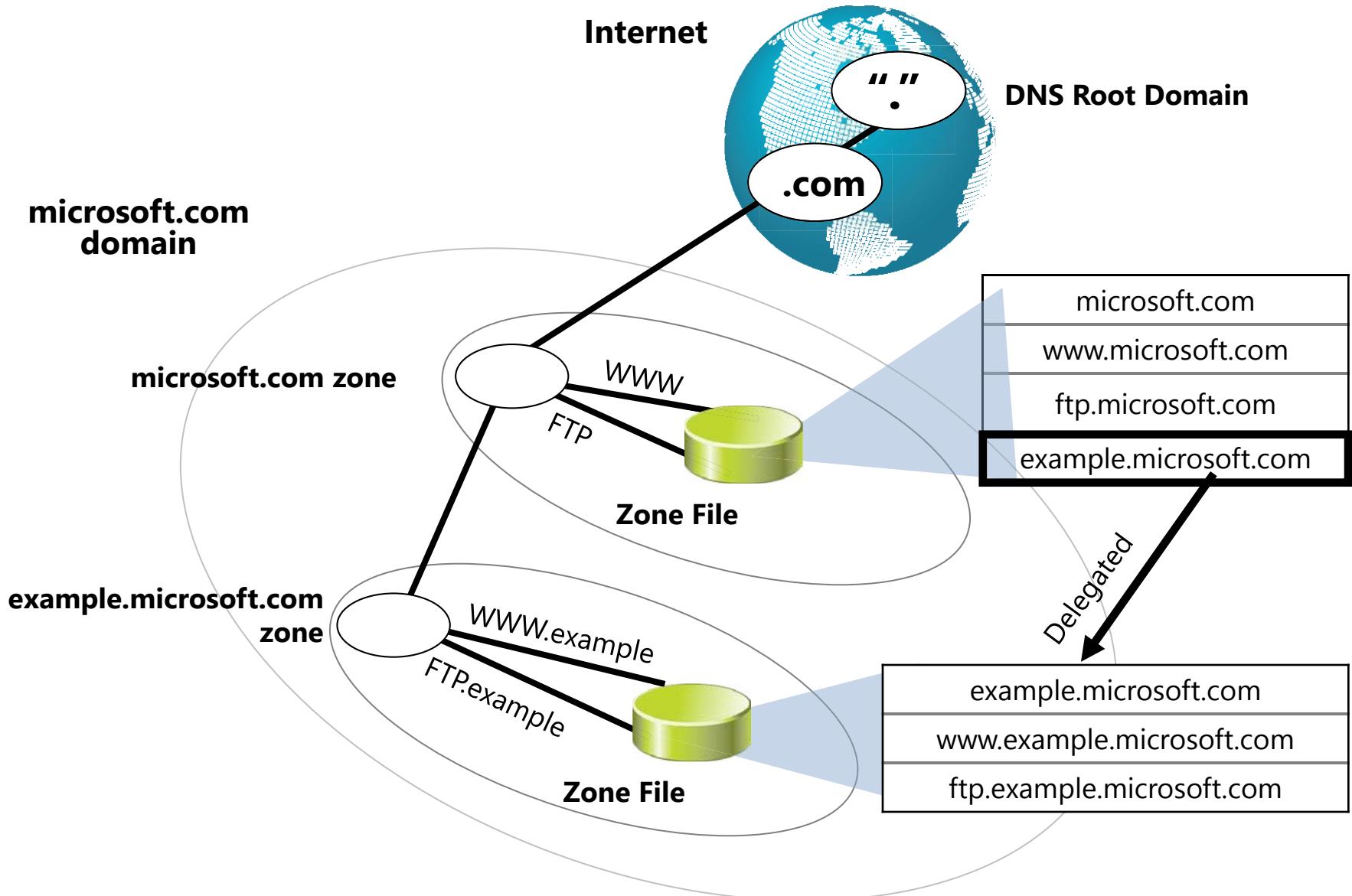
- DNS Resource Records
- What Is a DNS Zone?
- DNS Zone Types
- What Are Active Directory–Integrated Zones?
- Forward and Reverse Lookup Zones
- Overview of Stub Zones
- Demonstration: Creating Zones
- DNS Zone Delegation
- What Is Split DNS?

# DNS Resource Records

DNS resource records include:

- SOA: Start of authority resource record
- A: Host address resource record
- CNAME: Alias resource record
- MX: Mail exchanger resource record
- SRV: Service locator resource record
- NS: Name server resource record
- AAAA: IPv6 host address resource record
- PTR: Pointer resource record

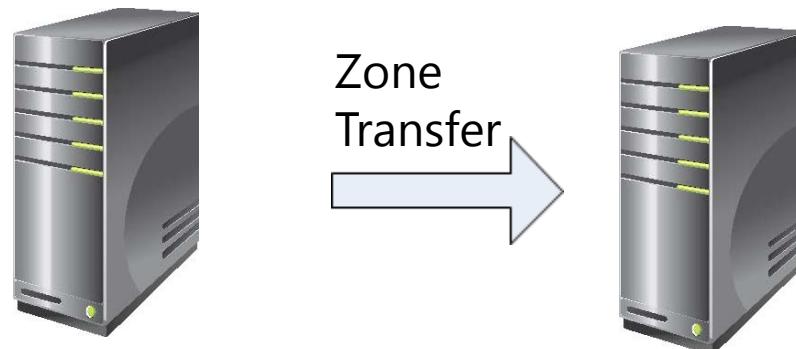
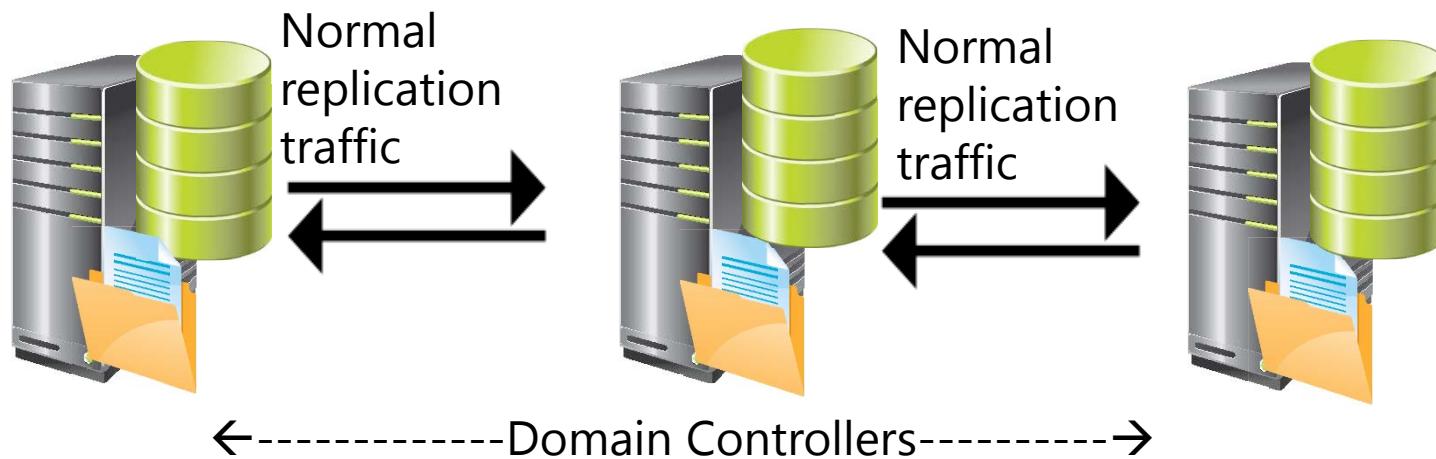
# What Is a DNS Zone?



# DNS Zone Types

| <b>Zones</b>                | <b>Description</b>                                                    |
|-----------------------------|-----------------------------------------------------------------------|
| Primary                     | Read/write copy of a DNS database                                     |
| Secondary                   | Read-only copy of a DNS database                                      |
| Stub                        | Copy of a zone that contains only records used to locate name servers |
| Active Directory-integrated | Zone data is stored in AD DS rather than in zone files                |

# What Are AD DS Integrated Zones?



Primary DNS Server

Secondary DNS Server



# Forward and Reverse Lookup Zones

Namespace: **training.contoso.com**

**DNS Server Authorized  
for Training**



**Forward  
zone**

**Training**

**Reverse  
zone**

**2.168.192.in-  
addr.arpa**

DNS Client1

DNS Client2

DNS Client3

192.168.2.45

192.168.2.46

192.168.2.47

192.168.2.45

192.168.2.46

192.168.2.47

DNS Client1

DNS Client2

DNS Client3

**DNS Client2 = ?**

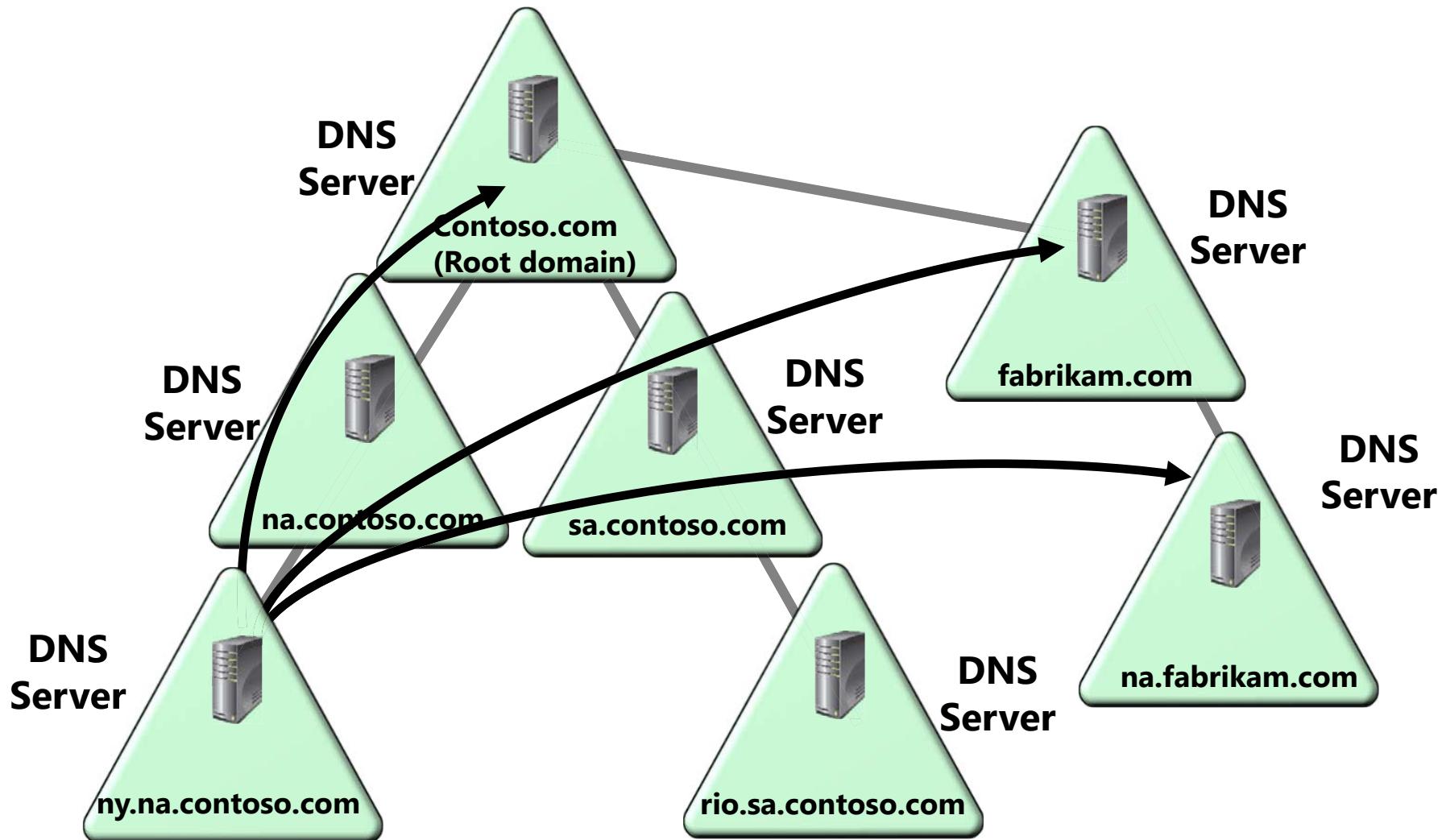
**192.168.2.46 = ?**



**DNS Client1**

# Overview of Stub Zones

Without stub zones, the ny.na.contoso.com server must query several servers to find the server that hosts the na.fabrikam.com zone

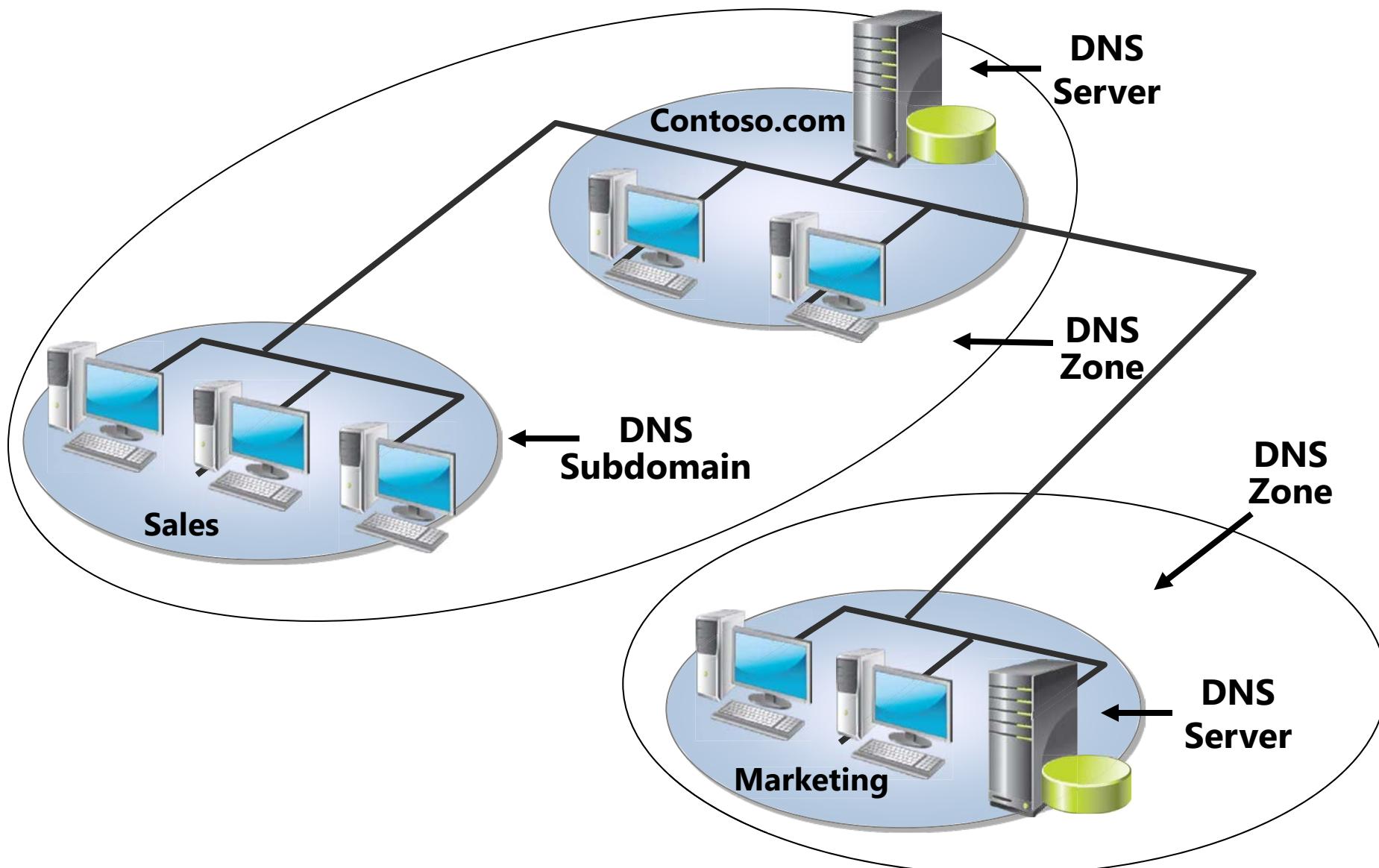


# Demonstration: Creating Zones

In this demonstration, you will see how to:

- Create a reverse lookup zone
- Create a forward lookup zone

# DNS Zone Delegation



# What Is Split DNS?

**Internal DNS servers host domain computer records, plus mail and Web server in perimeter subnet**

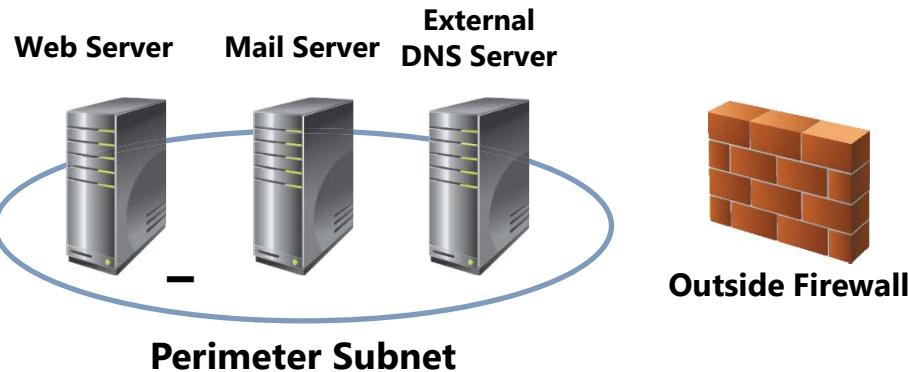


**Domain Controllers  
Running ADI DNS**



**Servers and Computers on  
Domain-Joined, Internal Network**

**External DNS server hosts only records that are resolved from the outside mail and Web server**



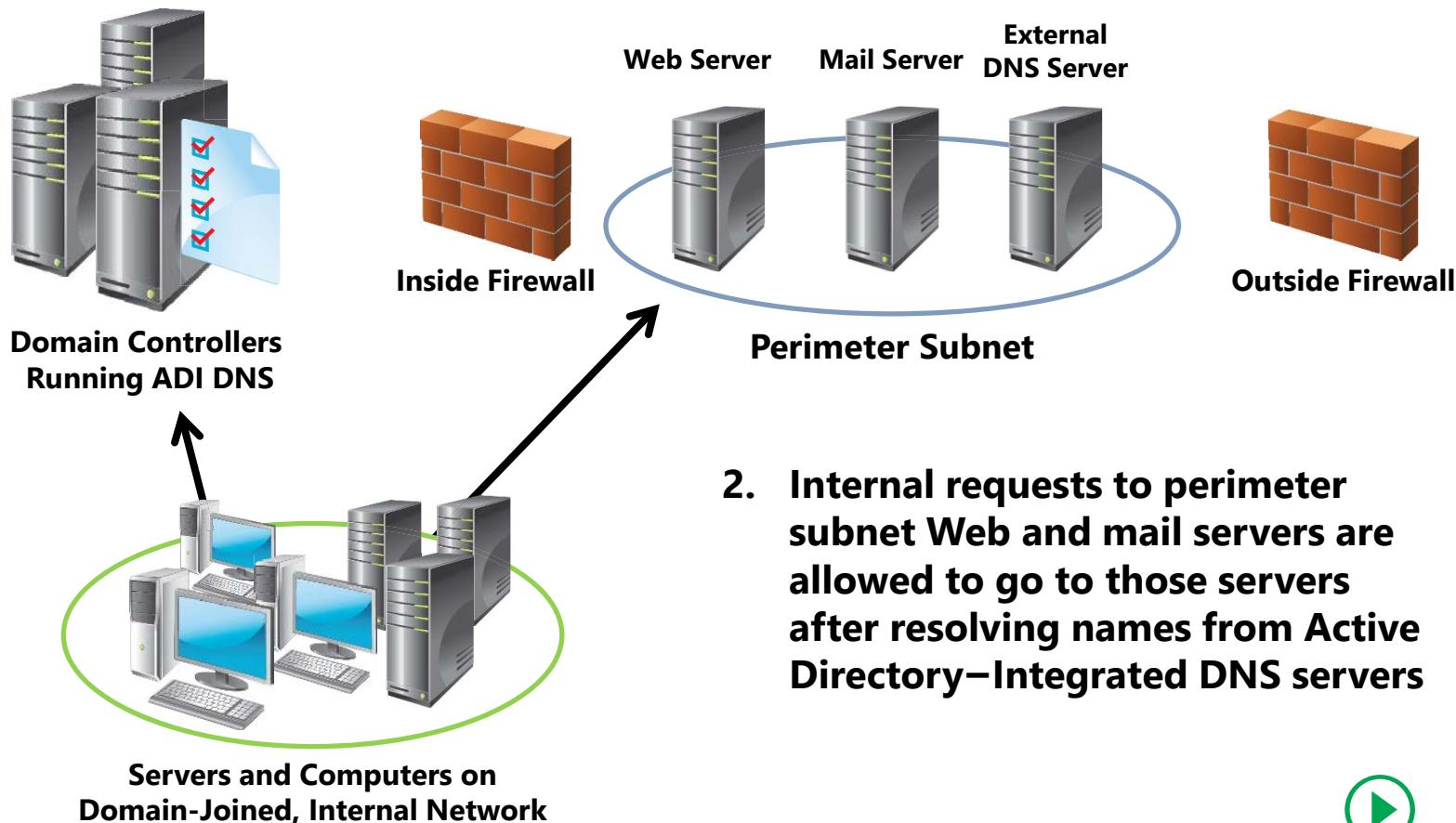
- 1. Clients and servers on the internal network send all DNS queries to Domain controllers/Active Directory–Integrated servers.**



# What Is Split DNS?

**Internal DNS servers host domain computer records, plus mail and Web server in perimeter subnet**

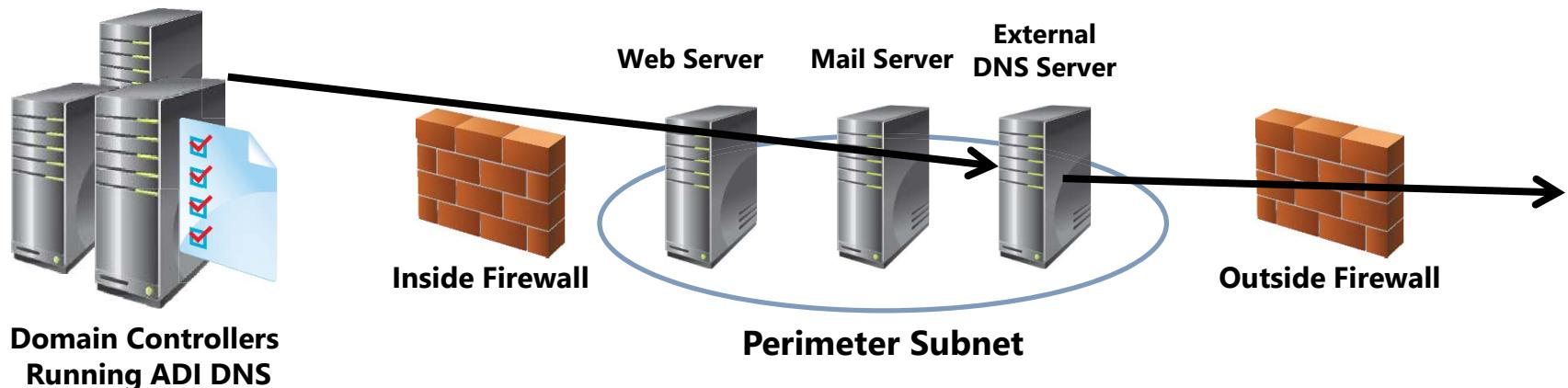
**External DNS server hosts only records that are resolved from the outside: mail and Web server**



# What Is Split DNS?

**Internal DNS servers host domain computer records, plus mail and Web server in perimeter subnet**

**External DNS server hosts only records that are resolved from the outside: mail and Web server**



3. Requests to resolve resources outside of the domain and perimeter subnet are forwarded to the external DNS server, which uses iterative queries to root hints or another forwarder to resolve those queries.



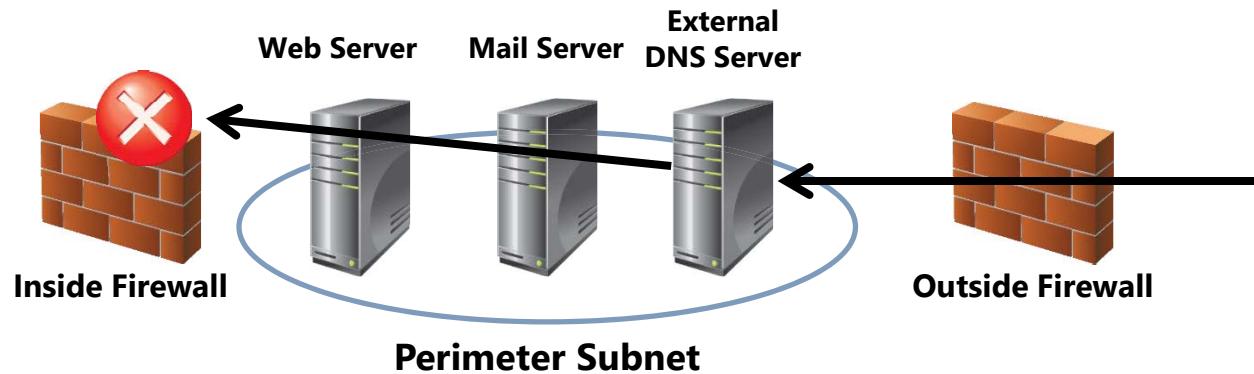
# What Is Split DNS?

**Internal DNS servers host domain computer records, plus mail and Web server in perimeter subnet**



**Domain Controllers  
Running ADI DNS**

**External DNS server hosts only records that are resolved from the outside: mail and Web server**



**Servers and Computers on  
Domain-Joined, Internal Network**

4. **Clients and servers on the internal network send all DNS queries to Domain controllers/Active Directory–Integrated DNS servers**

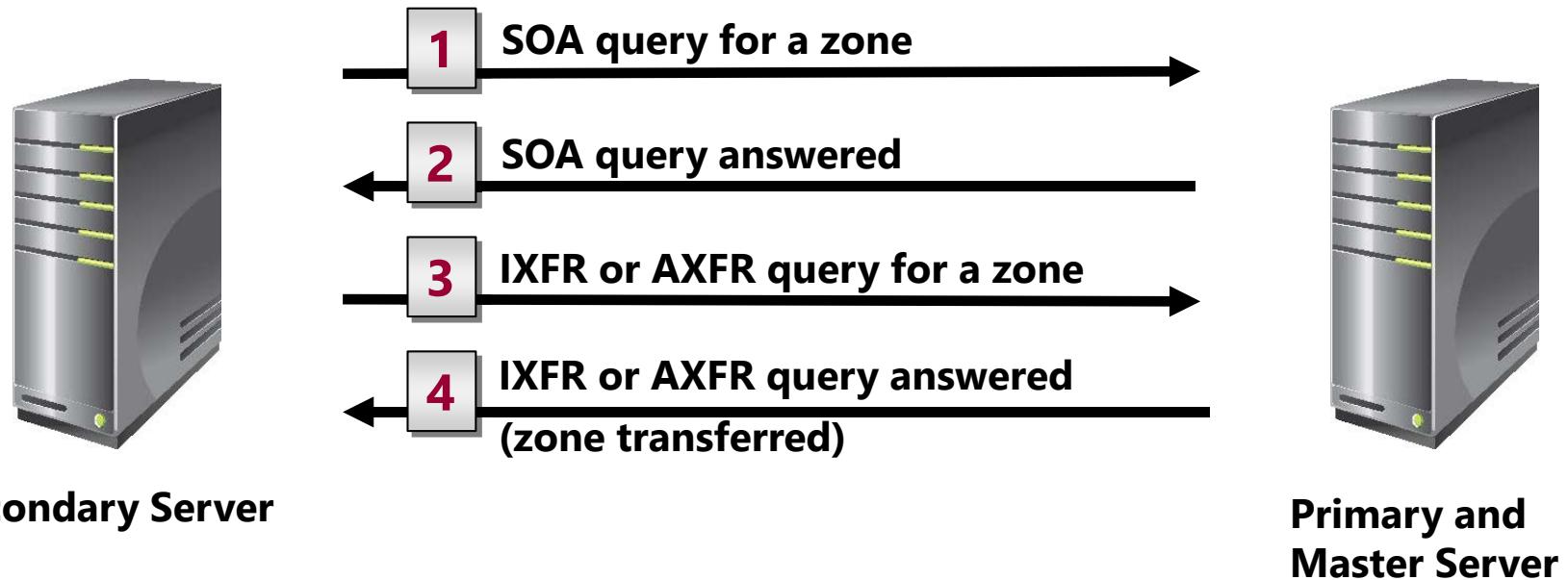


# Lesson 3: Configuring DNS Zone Transfers

- What Is a DNS Zone Transfer?
- Configuring Zone Transfer Security
- Demonstration: Configuring DNS Zone Transfers

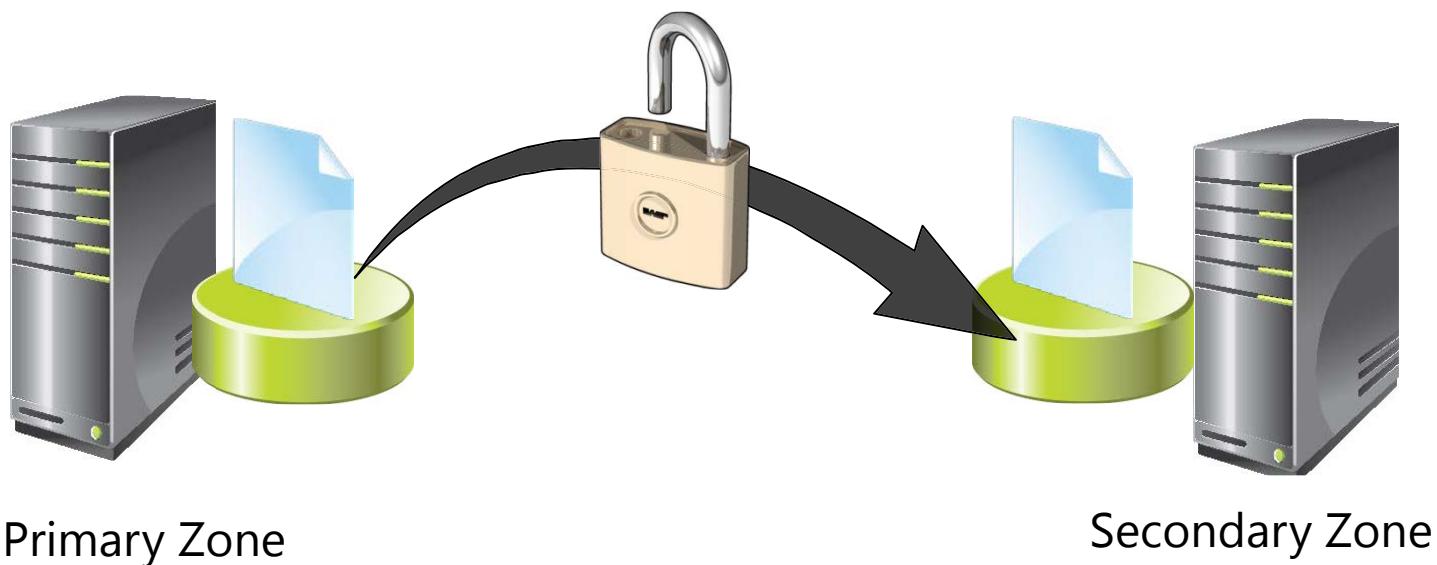
# What Is a DNS Zone Transfer?

A *DNS zone transfer* is the synchronization of authoritative DNS zone data between DNS servers



# Configuring Zone Transfer Security

- Restrict zone transfer to specified servers
- Encrypt zone transfer traffic
- Consider using Active Directory–integrated zones



# Demonstration: Configuring DNS Zone Transfers

In this demonstration, you will see how to:

- Enable DNS zone transfers
- Update the secondary zone from the master server
- Update the primary zone, and verify the change on the secondary zone

# Lesson 4: Managing and troubleshooting DNS

- TTL, Aging, and Scavenging
- Demonstration: Managing DNS Records
- Demonstration: Testing the DNS Server Configuration
- Monitoring DNS by Using the DNS Event Log
- Monitoring DNS by Using Debug Logging
- Monitoring DNS with Windows PowerShell

# TTL, Aging, and Scavenging

| <b>Feature</b> | <b>Description</b>                                                                                     |
|----------------|--------------------------------------------------------------------------------------------------------|
| TTL            | Indicates how long a DNS record will remain valid                                                      |
| Aging          | Occurs when records that have been inserted into the DNS server reach their expiration and are removed |
| Scavenging     | Performs DNS server resource record grooming for old records in DNS                                    |

# Demonstration: Managing DNS Records

In this demonstration, you will see how to:

- Configure TTL
- Enable and configure scavenging and aging

# Demonstration: Testing the DNS Server Configuration

In this demonstration, you will see how to use Nslookup.exe to test the DNS server configuration

# Monitoring DNS by Using the DNS Event Log

Event Viewer

File Action View Help

Custom Views Windows Logs Applications and Services Logs Active Directory Web Server DFS Replication Directory Service **DNS Server** Hardware Events Internet Explorer Key Management Service Microsoft Windows PowerShell Subscriptions

DNS Server Number of events: 20

| Level       | Date and Time        | Source          | Event ID | Task Category |
|-------------|----------------------|-----------------|----------|---------------|
| Information | 6/28/2012 1:01:37 PM | DNS-Server-S... | 4        | None          |
| Information | 6/28/2012 1:01:37 PM | DNS-Server-S... | 2        | None          |
| Warning     | 6/28/2012 1:01:31 PM | DNS-Server-S... | 4013     | None          |
| Information | 6/10/2012 4:11:00 AM | DNS-Server-S... | 4        | None          |
| Information | 6/10/2012 4:10:59 AM | DNS-Server-S... | 2        | None          |
| Warning     | 6/10/2012 4:10:43 AM | DNS-Server-S... | 4013     | None          |
| Information | 6/9/2012 9:00:46 AM  | DNS-Server-S... | 4        | None          |
| Information | 6/9/2012 9:00:45 AM  | DNS-Server-S... | 2        | None          |
| Warning     | 6/9/2012 9:00:31 AM  | DNS-Server-S... | 4013     | None          |
| Information | 6/9/2012 8:59:15 AM  | DNS-Server-S... | 4        | None          |
| Information | 6/9/2012 8:59:14 AM  | DNS-Server-S... | 2        | None          |
| Warning     | 6/9/2012 8:59:00 AM  | DNS-Server-S... | 4013     | None          |
| Information | 6/6/2012 5:59:31 PM  | DNS-Server-S... | 4500     | None          |
| Information | 6/6/2012 5:59:31 PM  | DNS-Server-S... | 4500     | None          |
| Information | 6/6/2012 5:57:29 PM  | DNS-Server-S... | 2        | None          |
| Information | 6/6/2012 5:57:29 PM  | DNS-Server-S... | 4        | None          |
| Warning     | 6/6/2012 5:57:13 PM  | DNS-Server-S... | 4013     | None          |
| Information | 6/6/2012 5:55:58 PM  | DNS-Server-S... | 3150     | None          |

Event 4, DNS-Server-Service

General Details

The DNS server has finished the background loading and signing of zones. All zones are now available for DNS updates and zone transfers, as allowed by their individual zone configuration.

|                |                      |
|----------------|----------------------|
| Log Name:      | DNS Server           |
| Source:        | DNS-Server-Service   |
| Event ID:      | 4                    |
| Level:         | Information          |
| User:          | N/A                  |
| Logged:        | 6/28/2012 1:01:37 PM |
| Task Category: | None                 |
| Keywords:      | Classic              |
| Computer:      | ION-DC1 \datum.com   |

Actions

DNS Server

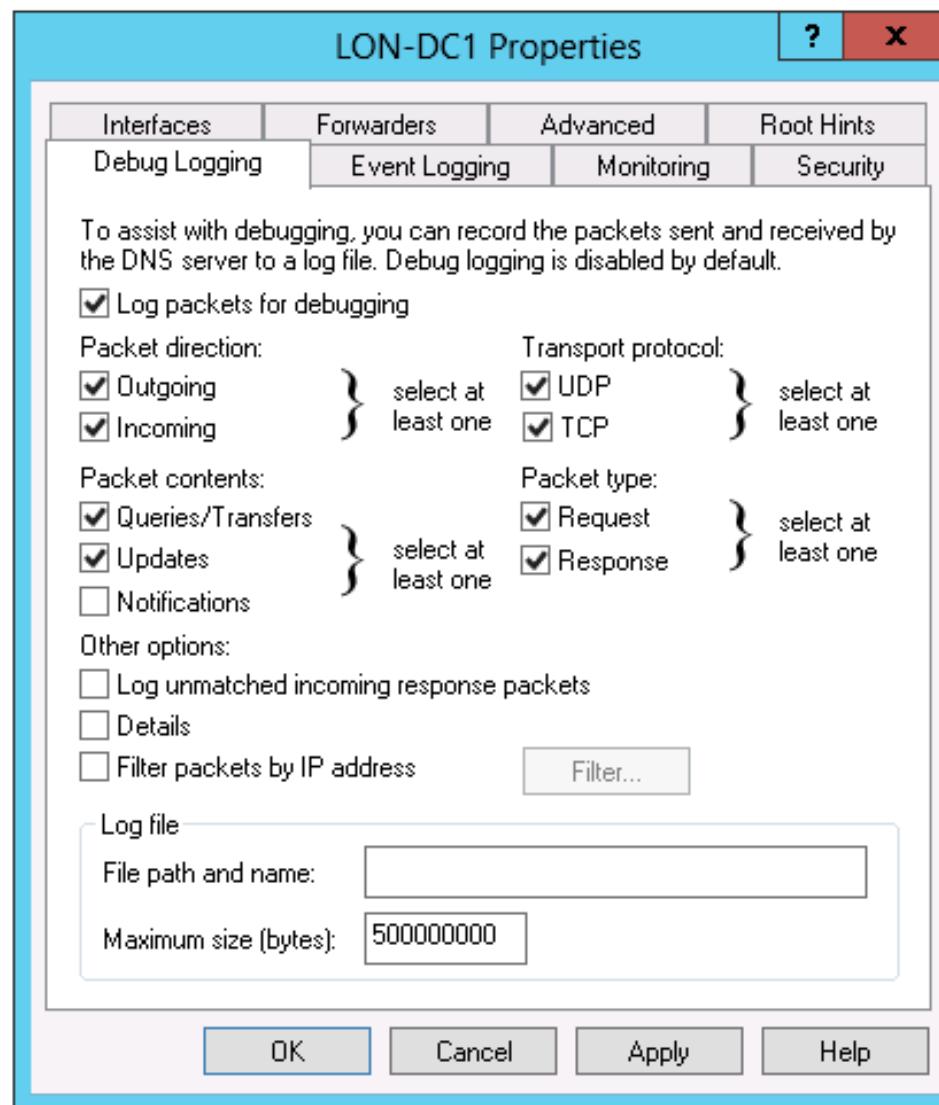
- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 4, DNS-Server-Service

- Event Properties
- Attach Task To This Ev...
- Save Selected Events...
- Copy
- Refresh
- Help

ENG

# Monitoring DNS by Using Debug Logging



# Monitoring DNS with Windows PowerShell

- Windows Server 2012 has added Windows PowerShell cmdlets for DNS configuring, managing, monitoring, and troubleshooting
- Windows Server 2012 R2 has added DnsServerStatistics parameters
- Windows Server 2012 R2 also added Windows PowerShell cmdlets for DNSSEC

# Lab: Configuring and Troubleshooting DNS

- Exercise 1: Configuring DNS Resource Records
- Exercise 2: Configuring DNS Conditional Forwarding
- Exercise 3: Installing and Configuring DNS Zones
- Exercise 4: Troubleshooting DNS

## Logon Information

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1,  
20411D-LON-CL1

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 60 minutes

## Lab Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, United Kingdom. An Information Technology office and a data center are located in London to support the head office and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure.

Management has asked you to add several new resource records to the DNS service that is installed on LON-DC1. Records include a new MX record for Exchange Server 2013 and a SRV record for a Microsoft Lync® Server 2013 deployment that is occurring.

## Lab Scenario

A. Datum is working with a partner organization, Contoso, Ltd. You have been asked to configure internal name resolution between the two organizations. A small branch office has reported that name resolution performance is poor. The branch office contains a Windows Server 2012 server that performs several roles. However, there is no plan to implement an additional domain controller. You have been asked to install the DNS server role at the branch office and to create a secondary zone of Adatum.com. To maintain security, you have been instructed to configure the branch office server to be on the Notify list for

## Lab Scenario

Adatum.com zone transfers. You also should update all branch office clients to use the new name server in the branch office.

You should configure the new DNS server role to perform standard aging and scavenging, as necessary and as specified by corporate policy. After implementing the new server, you need to test and verify the configuration by using standard DNS troubleshooting tools.

## Lab Review

In the lab, you were required to deploy a secondary zone because you were not going to deploy any additional domain controllers. If this condition changed—that is, if LON-SVR1 was a domain controller—how would that change your implementation plan?

# Module Review and Takeaways

- Review Question(s)
- Tools

# Microsoft® Official Course



## Module 2

### Maintaining Active Directory® Domain Services

**Microsoft®**

# Module Overview

- Overview of AD DS
- Implementing Virtualized Domain Controllers
- Implementing RODCs
- Administering AD DS
- Managing the AD DS Database

# Lesson 1: Overview of AD DS

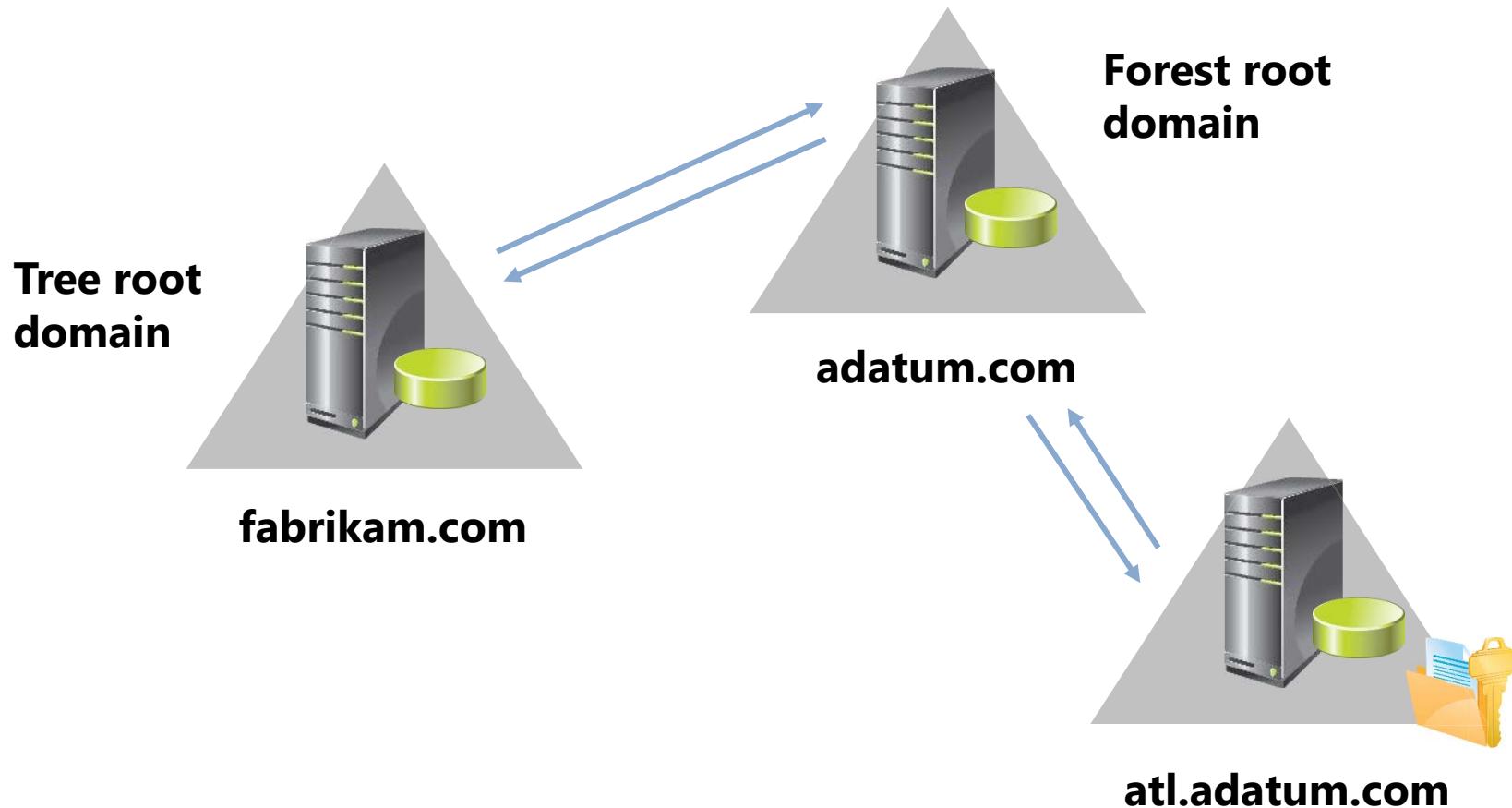
- Overview of AD DS Components
- Understanding AD DS Forest and Schema Structure
- Understanding AD DS Domain Structure
- Extending the AD DS Deployment with Windows Azure Virtual Machines

# Overview of AD DS Components

AD DS is composed of both physical and logical components

| <b>Physical components</b>                                                                                                                | <b>Logical components</b>                                                                                                                                              |
|-------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Data store</li><li>• Domain controllers</li><li>• Global catalog server</li><li>• RODCs</li></ul> | <ul style="list-style-type: none"><li>• Partitions</li><li>• Schema</li><li>• Domains</li><li>• Domain trees</li><li>• Forests</li><li>• Sites</li><li>• OUs</li></ul> |

# Understanding AD DS Forest and Schema Structure



# Understanding AD DS Domain Structure

- AD DS requires one or more domain controllers
- All domain controllers hold a copy of the domain database which is continually synchronized
  - The domain is the context within which users, groups, and computers are created
  - The domain is a replication boundary
  - The domain is an administrative center for configuring and managing objects
  - Any domain controller can authenticate any logon in the domain



# Extending the AD DS Deployment with Windows Azure Virtual Machines

Extending AD DS to the Windows Azure Virtual Machine clouds enables new scenarios, including:

- Cloud-only deployments, to enable a new forest in the cloud to:
  - Support applications in the cloud that are accessible from the intranet and Internet
  - Run applications and AD DS isolated from the corporate directory
  - Support extranet applications
- Hybrid deployments, to extend an existing domain to the cloud to:
  - Support corporate applications in the cloud
  - Support business-to-business authentication by using AD FS
  - Support high availability and disaster recovery scenarios

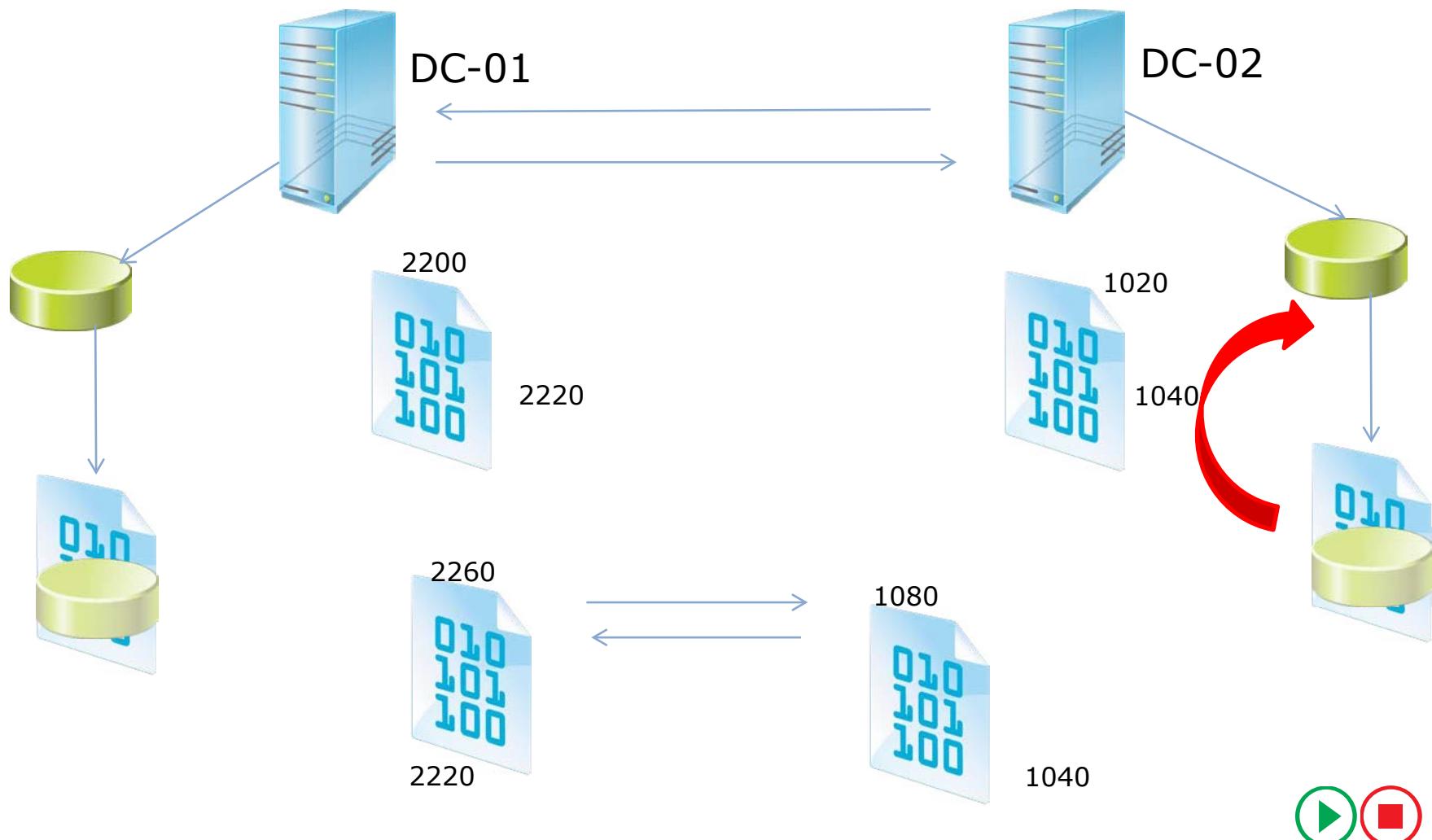
## Lesson 2: Implementing Virtualized Domain Controllers

- Considerations for Virtual Domain Controller Deployment
- How Checkpoints Affect Domain Controllers
- Domain Controller Virtualization in Windows Server 2012
- Domain Controller Cloning
- Demonstration: Cloning Domain Controllers
- Domain Controller Virtualization Best Practices

# Considerations for Virtual Domain Controller Deployment

- Virtualization benefits of domain controllers:
  - Scalability
  - Independence from hardware
  - Quicker recovery
- Windows Server 2012 is cloud-ready and virtualization aware
- Considerations for virtualization include:
  - Time synchronization
  - Domain membership of the virtualization host
  - Single point of failure
  - Moving AD DS to the cloud

# How Checkpoints Affect Domain Controllers



# Domain Controller Virtualization in Windows Server 2012

To support safe virtualization of domain controllers:

- Hypervisor needs to support a Virtual Machine Generation Identifier, such as Hyper-V on Windows Server 2012
- Virtual guest domain controller needs to be on Windows Server 2012 or newer

Safeguards are triggered when:

- A snapshot is restored during guest shutdown
- A snapshot is restored while machine is running

Guest employs virtualization safeguards by:

- Invalidating the local RID pool
- Setting a new invocation ID for the domain controller database, effectively presenting itself as a new domain controller and verifying all objects and attributes

# Domain Controller Cloning

- Domain controllers can be cloned for:
  - Rapid deployment
  - Private clouds
  - Recovery strategies
- To clone a source domain controller:
  - Add the domain controller to the Cloneable Domain Controllers group
  - Verify application and service compatibility
  - Create a DCCloneConfig.xml file
  - Export once and create as many clones as needed
  - Start the clones

# Demonstration: Cloning Domain Controllers

- In this demonstration, you will see how to:
  - Prepare a source domain controller that is to be cloned
  - Export the source virtual machine
  - Create and start the cloned domain controller

# Domain Controller Virtualization Best Practices

- Avoid single points of failure
- Ensure that all computers participate in the same time services infrastructure
- Use virtualization technology with the Virtual Machine Generation Identifier feature
- Use Windows Server 2012 or Windows Server 2012 R2 as virtualization guests
- Avoid or disable snapshots
- Ensure that the virtualization administrators are as trusted as your Domain Admins
- Consider taking advantage of cloning in your deployment or recovery strategy
- Start a maximum of 10 new clones at the same time
- Consider using virtualization technologies that allow virtual machine guests to move between sites
- Adjust your naming strategy to allow domain controller clones

## Lesson 3: Implementing RODCs

- Considerations for Implementing RODCs
- Managing Credential Caching on an RODC
- Managing Local Administration for RODCs
- Demonstration: Configuring RODC Credential Caching

# Considerations for Implementing RODCs

- RODCs provide several important functions:
  - Credential caching
  - Administrative role separation
  - Read-only DNS
- To deploy an RODC:
  1. Ensure there is no computer account in AD DS for the new RODC
  2. Precreate the RODC account in AD DS in the Domain Controllers container
  3. Run the AD DS Installation Wizard on the new RODC

# Managing Credential Caching on an RODC

- Credential caching is managed through Password Replication Policies
- Password Replication Policies:
  - Determine which credentials to cache on an RODC
    - User accounts
    - Computer accounts
  - Contain an allowed and denied list
    - Allowed RODC Password Replication Group
    - Denied RODC Password Replication Group
- Do not cache domain administrative accounts

# Managing Local Administration for RODCs

- Delegate RODC administration to local administrators
- Set a single security principal as an administrator
  - User
  - Group
- Enable by using the following methods:
  - Managed By tab of RODC
  - dsmgmt
  - ntsdutil
- Cache the credentials of delegated administrators

# Demonstration: Configuring RODC Credential Caching

- In this demonstration, you will see how to:
  - Configure password replication groups
  - Create a group to manage password replication to the remote office RODC
  - Configure a password replication policy for the remote office
  - Evaluate the resulting password replication policy
  - Monitor credential caching

# Lesson 4: Administering AD DS

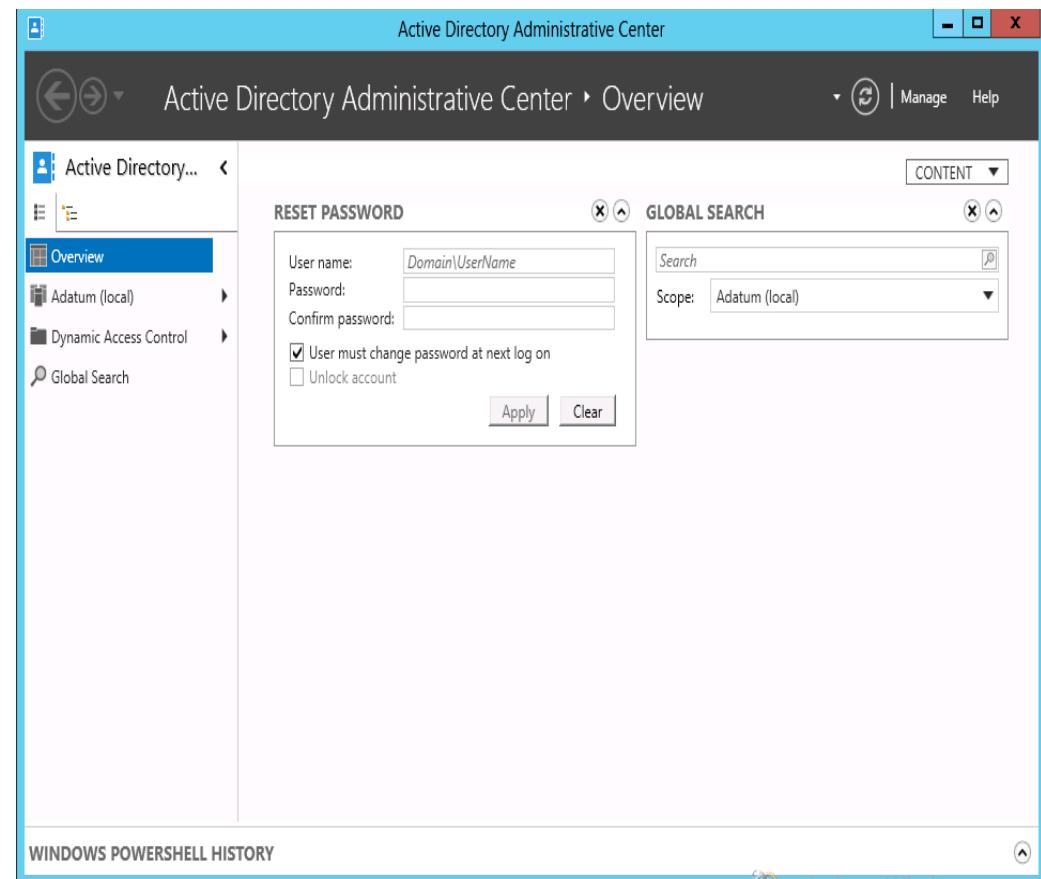
- Overview of Active Directory Administration Snap-ins
- Overview of the Active Directory Administrative Center
- What Is Ntdsutil?
- Overview of the Active Directory Module for Windows PowerShell
- Demonstration: Managing AD DS by Using Management Tools
- Managing Operations Master Roles
- Managing AD DS Backup and Recovery

# Overview of Active Directory Administration Snap-ins

- Active Directory administration snap-ins consist of four different MMC consoles:
  - Active Directory Users and Computers
  - Active Directory Sites and Services
  - Active Directory Domains and Trusts
  - Active Directory Schema
- Use RSAT Windows Update to install Snap-ins on computers that are not non-domain controllers

# Overview of the Active Directory Administrative Center

- Active Directory Administrative Center is a task-oriented tool based on Windows PowerShell
- New features in Windows Server 2012
  - Active Directory Recycle Bin
  - Fine-Grained Password Policy
  - Windows PowerShell History Viewer



# What Is Ntdsutil?

By using Ntdsutil you can:

- Manage and control single master operations
- Perform AD DS database maintenance
  - Perform offline defragmentation
  - Create and mount snapshots
  - Move database files
- Maintain domain controller metadata
- Reset Directory Services Restore Mode password

# Overview of the Active Directory Module for Windows PowerShell

- The Active Directory module for Windows PowerShell provides full administrative functionality for:
  - User management
  - Computer management
  - Group management
  - OU management
  - Password policy management
  - Searching and modifying objects
  - Forest and domain management
  - Domain controller and operations-masters management
  - Managed service account management
  - Site-replication management
  - Central access and claims management

# Demonstration: Managing AD DS by Using Management Tools

- In this demonstration, you will see how to:
  - Create objects in Active Directory Users and Computers
  - View object attributes in Active Directory Users and Computers
  - Navigate within Active Directory Administrative Center
  - Perform an administrative task in Active Directory Administrative Center
  - Use the Windows PowerShell Viewer in Active Directory Administrative Center
  - Manage AD DS objects with Windows PowerShell

# Managing Operations Master Roles

Operations Master Roles are assigned to the domain controller that is responsible for performing a specific task on the forest or domain

- Forest-wide Operations Master Roles
  - Domain Naming Master Role
  - Schema Master Role
- Domain-wide Operations Master Roles
  - RID Master Role
  - Infrastructure Master Role
  - PDC Emulator Role

# Managing AD DS Backup and Recovery

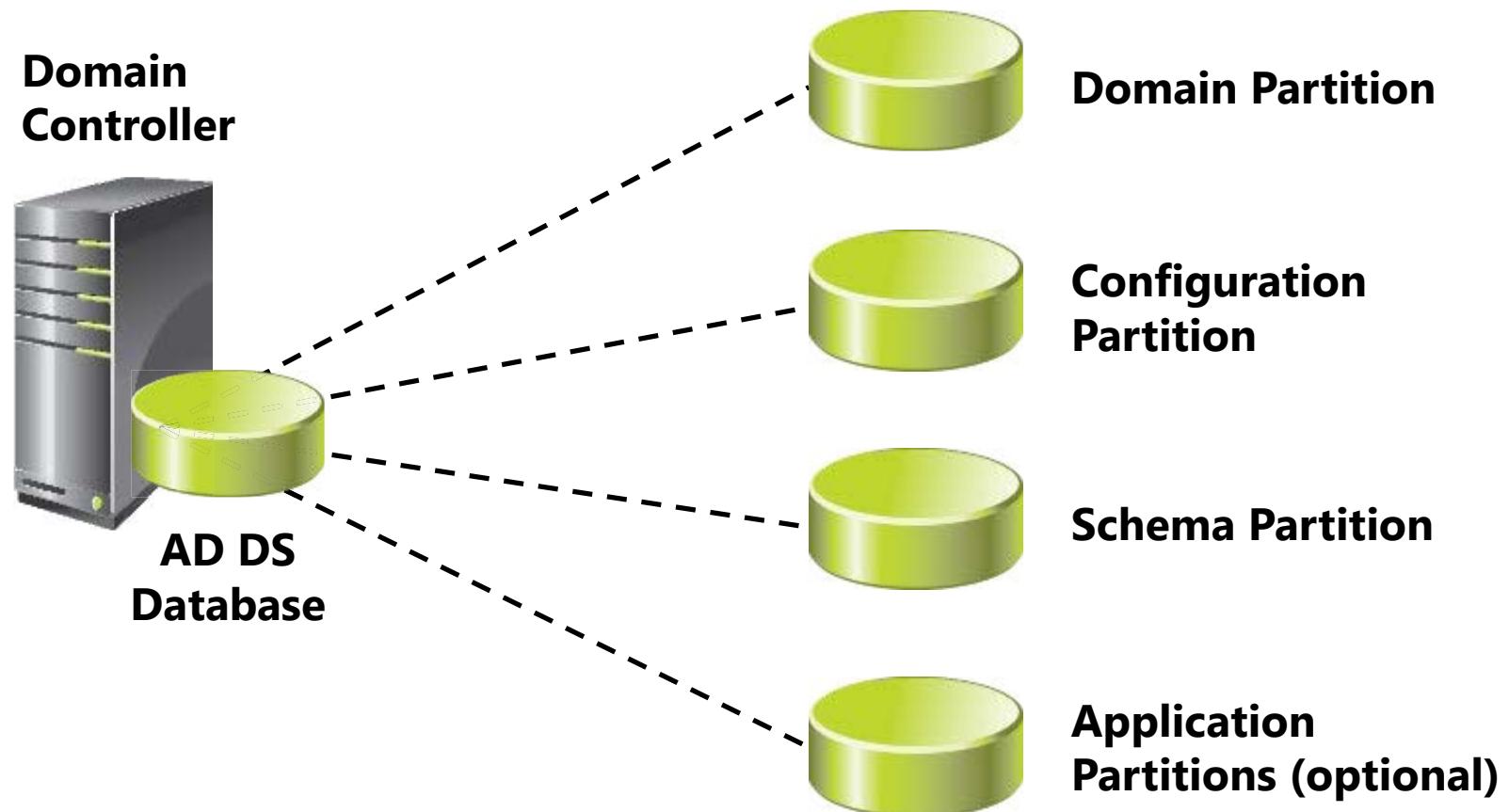
- System State or Full backups of the Domain controllers allow the following types of restores:
  - Nonauthoritative or normal restore
  - Authoritative restore
    - Allows deleted objects to be returned on all domain controllers
  - Full server restore
    - Typically performed in Windows RE
- Some tasks require you to stop AD DS service
- Use Ntdsutil commands to optimize AD DS and clean up metadata
  - Offline AD DS database defragmentation
  - Remove records on deleted domain controllers

# Lesson 5: Managing the AD DS Database

- Understanding the AD DS Database
- Understanding Restartable AD DS
- Demonstration: Performing AD DS Database Maintenance
- Creating AD DS Snapshots
- Understanding How to Restore Deleted Objects
- Configuring the Active Directory Recycle Bin
- Demonstration: Using the Active Directory Recycle Bin

# Understanding the AD DS Database

The AD DS database holds all domain-based information in four partitions



# Understanding Restartable AD DS

- AD DS can be started or stopped by using the Services console
- AD DS can be in one of three states :
  - AD DS Started
  - AD DS Stopped
  - DSRM
- It is not possible to perform a system state restore while AD DS is in Stopped state

# Demonstration: Performing AD DS Database Maintenance

In this demonstration, you will see how to:

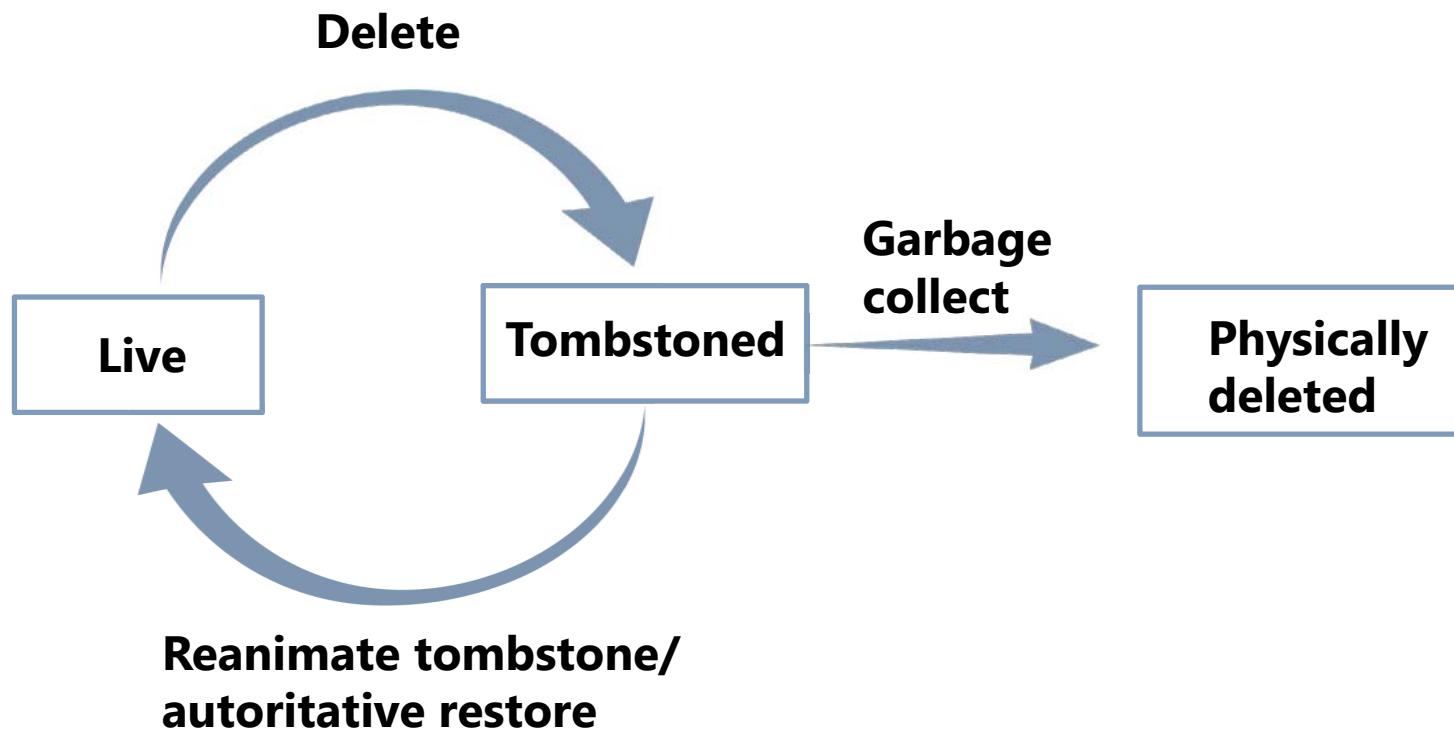
- Stop AD DS
- Perform offline defragmentation of the AD DS database
- Check the integrity of the AD DS database
- Start AD DS

# Creating AD DS Snapshots

- Create a snapshot of the AD DS
  - Use NTDSUtil
- Mount the snapshot to a unique port
  - Use NTDSUtil
- Expose the snapshot
  - Right-click the root node of Active Directory Users and Computers, and choose Connect to Domain Controller
  - Enter serverFQDN:port
- View (read-only) snapshot
  - Cannot directly restore data from the snapshot
- Recover data
  - Connect to the mounted snapshot, and export/reimport objects with LDIFDE
  - Restore a backup from the same date as the snapshot
  - Manually re-enter data

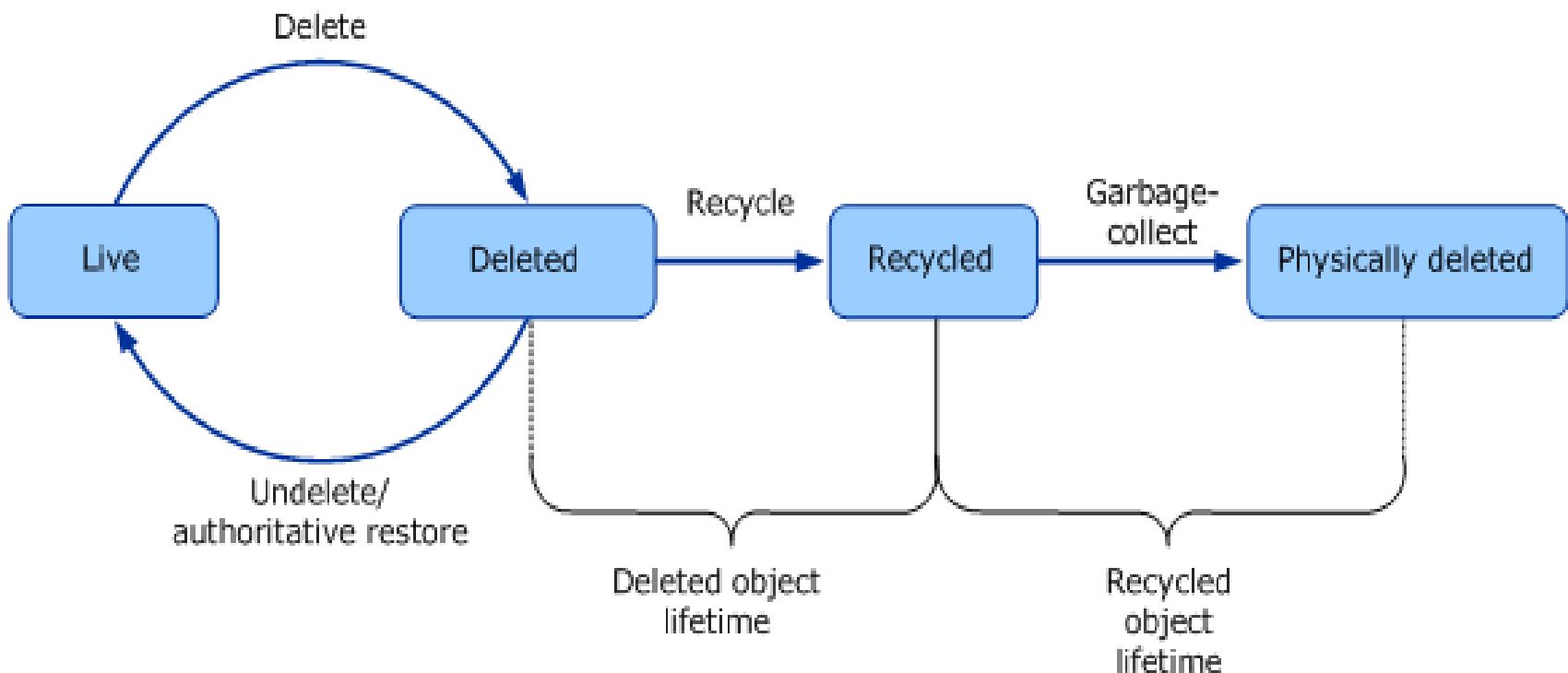
# Understanding How to Restore Deleted Objects

- Deleted objects are recovered through tombstone reanimation
- When an object is deleted, most of attributes are cleared
- Authoritative restore requires AD DS downtime



# Configuring the Active Directory Recycle Bin

- Active Directory Recycle Bin
  - Provides a way to restore deleted objects without AD DS downtime
  - Uses Windows PowerShell with Active Directory Module or the Active Directory Administrative Center to restore



# Demonstration: Using the Active Directory Recycle Bin

In this demonstration, you will see how to:

- Enable the Active Directory Recycle Bin
- Create and then delete test accounts
- Restore deleted accounts

# Lab: Maintaining AD DS

- Exercise 1: Installing and Configuring an RODC
- Exercise 2: Configuring AD DS Snapshots
- Exercise 3: Configuring the Active Directory Recycle Bin
- Exercise 4: Optional Exercise: Cloning a Domain Controller

## Logon Information

**Virtual machines:** 20411D-LON-DC1,  
20411D-LON-SVR1,  
**User Name:** Adatum\Administrator  
**Password:** Pa\$\$w0rd

Estimated Time: 75 minutes

# Lab Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, United Kingdom. An IT office and data center in London support the head office and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure, and is making several organizational changes that require modifications to the AD DS infrastructure. A new location requires a secure method of providing onsite AD DS. A. Datum is opening a new branch office that does not yet have a secure data center, but does now require a domain controller.

# Lab Scenario

You need to deploy a domain controller for this office. In addition, you have been asked to extend the capabilities of Active Directory Recycle Bin to the entire organization. As part of an overall virtualization strategy, IT management also wants you to perform a proof of concept deployment of a domain controller using domain controller cloning.

# Module Review and Takeaways

- Review Question(s)
- Tools
- Best Practices

# Microsoft® Official Course



## Module 3

### Managing User and Service Accounts

**Microsoft®**

# Module Overview

- Configuring Password Policy and User Account Lockout Settings
- Configuring Managed Service Accounts

# Lesson 1: Configuring Password Policy and User Account Lockout Settings

- User Account Policies
- Kerberos Policies
- Configuring User Account Policies
- What Are Password Settings Objects?
- Configuring PSOs
- Demonstration: Configuring PSOs
- Discussion: Planning Password Policies

# User Account Policies

Use the following settings to set password requirements:

- Enforce password history
- Maximum password age
- Minimum password age
- Minimum password length
- Password complexity requirements
- Account lockout duration
- Account lockout threshold

# Kerberos Policies

- Kerberos policy settings determine timing for Kerberos tickets and other events

| <b>Setting</b>                                       | <b>Default</b> |
|------------------------------------------------------|----------------|
| Enforce user logon restrictions                      | Enabled        |
| Maximum lifetime for service ticket                  | 600 minutes    |
| Maximum lifetime for user ticket                     | 10 hours       |
| Maximum lifetime for user ticket renewal             | 7 days         |
| Maximum tolerance for computer clock synchronization | 5 minutes      |

- Kerberos claims and compound authentication for DAC requires Windows Server 2012 domain controllers

# Configuring User Account Policies

- Local Security Policy account settings:
  - Configured with secpol.msc
  - Apply to local user accounts
- Group Policy account settings
  - Configured with the Group Policy Management console
  - Apply to all accounts in AD DS and local accounts on computers joined to the domain
  - Can only be applied once, in Default Domain Policy
  - Take precedence over Local Security Policy settings

# What Are Password Settings Objects?

- You can use fine-grained password policies to specify multiple password policies within a single domain
- Fine-grained password policies:
  - Apply only to user objects (or inetOrgPerson objects) and global security groups
  - Cannot be applied to an OU directly
  - Do not interfere with custom password filters that you might use in the same domain

# Configuring PSOs

- Windows Server 2012 provides two tools for configuring PSOs
  - Windows PowerShell cmdlets
    - New-ADFineGrainedPasswordPolicy
    - Add-FineGrainedPasswordPolicySubject
  - Active Directory Administrative Center
    - Graphical user interface
    - Uses Windows PowerShell cmdlets to create and manage PSOs

# Demonstration: Configuring PSOs

In this demonstration, you will see how to create a Password Settings Object for the ITAdmins group

# Discussion: Planning Password Policies

**What password policies would you recommend for...?**



- Woodgrove Bank
- New account lockout policy
- Tailspin Toys
- Best practices

# Lesson 2: Configuring Managed Service Accounts

- Service Account Overview
- Challenges of Using Standard User Accounts for Services
- Managed Service Account and Virtual Accounts
- What Are Group Managed Service Accounts?
- Demonstration: Configuring Group Managed Service Accounts
- Kerberos Delegation and Service Principal Names

# Service Account Overview

- Applications need resource access
  - Can create domain or local accounts to manage such access, but can potentially compromise security
- Use Service Accounts Instead
  - Local System
    - Most privileged, still vulnerable if compromised
  - Local Service
    - Least privileged, may not have enough permissions to access all required resources
  - Network Service
    - Can access network resources with proper credentials

# Challenges of Using Standard User Accounts for Services

- Challenges to using standard user accounts for services include:
  - Extra administration effort to manage the service account password
  - Difficulty in determining where a domain-based account is used as a service account
  - Extra administration effort to mange the SPN

# Managed Service Account and Virtual Accounts

- Use managed service accounts to automate password and SPN management for service accounts used by services and applications
- Requires a Windows Server 2008 R2 or Windows Server 2012 server installed with:
  - .NET Framework 3.5.x
  - Active Directory module for Windows PowerShell
- Recommended to run with AD DS configured at the Windows Server 2008 R2 functional level or higher
- Can be used in a Windows Server 2003 or 2008 AD DS environment:
  - With Windows Server 2008 R2 schema updates
  - With Active Directory Management Gateway Service

# What Are Group Managed Service Accounts?

- Group managed service accounts extend the capability of standard managed service accounts by
  - Enabling managed service accounts to be used on more than one computer in the domain
  - Storing managed service accounts authentication information on domain controllers
- Group managed service accounts requirements:
  - Must have at least one Windows Server 2012 domain controller
  - Must have a KDS root key created for the domain

# Demonstration: Configuring Group Managed Service Accounts

In this demonstration, you will see how to:

- Create the KDS root key for the domain
- Create and associate a managed service account

# Kerberos Delegation and Service Principal Names

- Kerberos delegation of authentication
  - Services can delegate service tickets issued to them by the KDC to another service
- Constrained delegation
  - Allows administrators to define which services can use service tickets issued to other services
- SPNs help identify services uniquely
- Windows 2012 allows
  - Constrained delegation across domains
  - Ability of service administrators to configure constrained delegation

# Lab: Managing User and Service Accounts

- Exercise 1: Configuring Password Policy and Account Lockout Settings
- Exercise 2: Creating and Associating a Managed Service Account

Logon Information

**Virtual machines:** 20411D-LON-DC1

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 45 minutes

# Lab Scenario

- A. Datum is a global engineering and manufacturing company with their head office based in London, United Kingdom. An IT office and data center are located in London to support the London location and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.
- A. Datum has completed a security review for passwords and account lockout policies. You need to implement the recommendations contained in the report to control password complexity and length. You also need to configure appropriate account lockout settings. Part of your password

## Lab Scenario

policy configuration will include a specific password policy you need to assign to the Executive security group. This group requires a different password policy than the policy applied at the domain level.

You need to configure a new group managed service account to support a new Web-based program. Using a group managed service account will help maintain the password security requirements for the account.

# Module Review and Takeaways

- Review Question(s)
- Real-world Issues and Scenarios
- Tools
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 4

### Implementing a Group Policy Infrastructure

**Microsoft®**

# Module Overview

- Introducing Group Policy
- Implementing and Administering GPOs
- Group Policy Scope and Group Policy Processing
- Troubleshooting the Application of GPOs

# Lesson 1: Introducing Group Policy

- What Is Configuration Management?
- Overview of Group Policies
- Benefits of Using Group Policy
- Group Policy Objects
- GPO Scope
- Group Policy Client and Client-Side Extensions
- Demonstration: How to Create a GPO and Configure GPO Settings

# What Is Configuration Management?

- Configuration management is a centralized approach to applying one or more changes to one or more users or computers
- The key elements of configuration management are:
  - Setting
  - Scope
  - Application

# Overview of Group Policies

- The most granular component of Group Policy is known as a *policy* and defines a specific configuration change
- Most policy settings can have three states:
  - Not Configured
  - Enabled
  - Disabled
- Many policy settings are complex, and the effect of enabling or disabling them might not be obvious

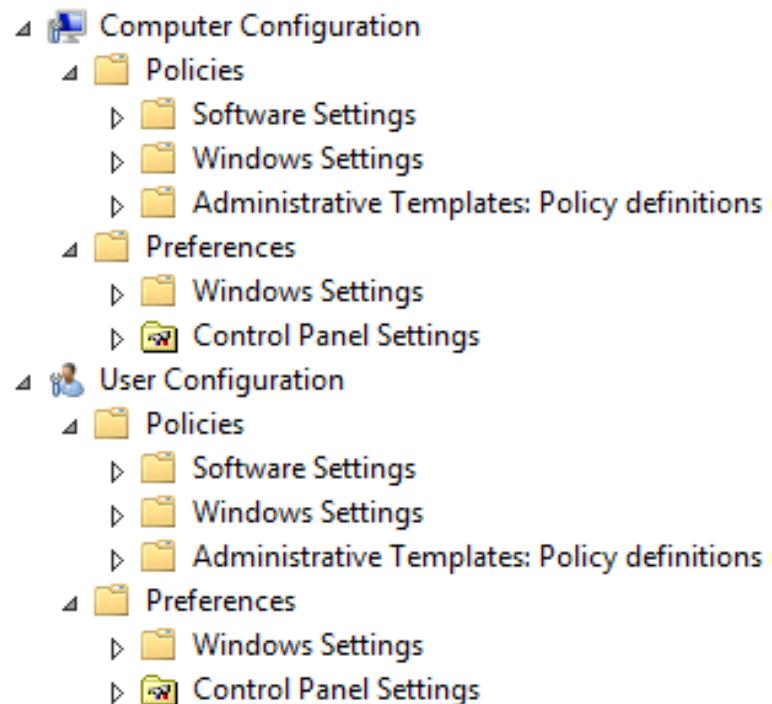
# Benefits of Using Group Policy

- GPOs are very powerful administrative tools and you can use them to enforce various types of settings to a large number of users and computers
- Typically, GPOs are used in the following way:
  - Apply security settings
  - Manage desktop application settings
  - Deploy application software
  - Manage Folder Redirection
  - Configure network settings

# Group Policy Objects

A GPO is:

- A container for one or more policy settings
- Managed with the GPMC
- Stored in the GPOs container
- Edited with the Group Policy Management Editor (GPME)
- Applied to a specific level in the AD DS hierarchy



# GPO Scope

- The scope of a GPO is the collection of users and computers that will apply the settings in the GPO.
- You can use several methods to scope a GPO:
  - Link the GPO to a container, such as an OU
  - Filter by using security settings
  - Filter by using WMI filters

# Group Policy Client and Client-Side Extensions

1. Group Policy Client retrieves GPOs
2. Client downloads and caches GPOs
3. CSEs process the settings
  - Policy settings in the Computer Configuration node are applied at system startup and every 90–120 minutes thereafter
  - User Configuration policy settings are applied at logon and every 90–120 minutes thereafter

# Demonstration: How to Create a GPO and Configure GPO Settings

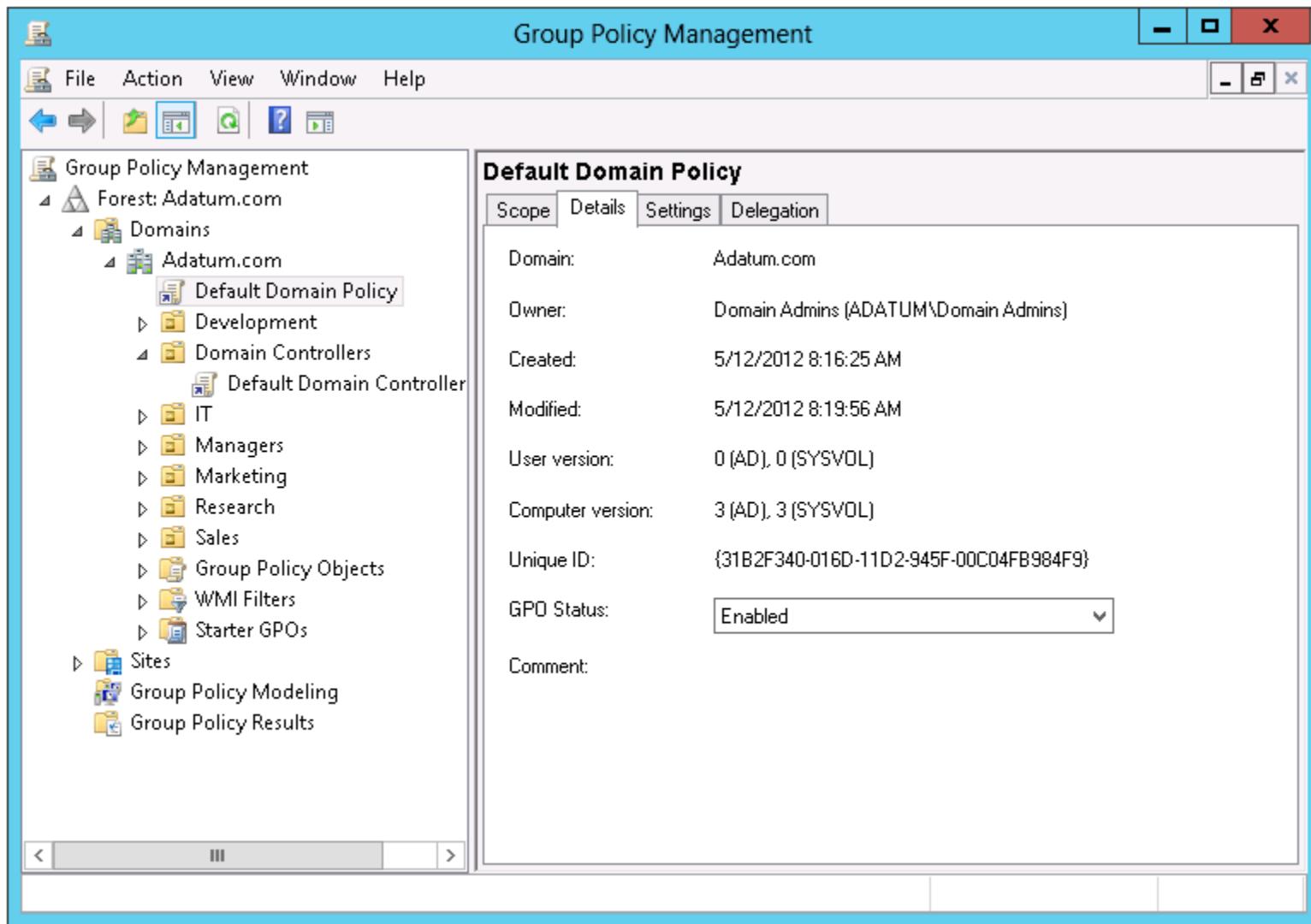
In this demonstration, you will see how to:

- Use the GPMC to create a new GPO
- Configure Group Policy settings

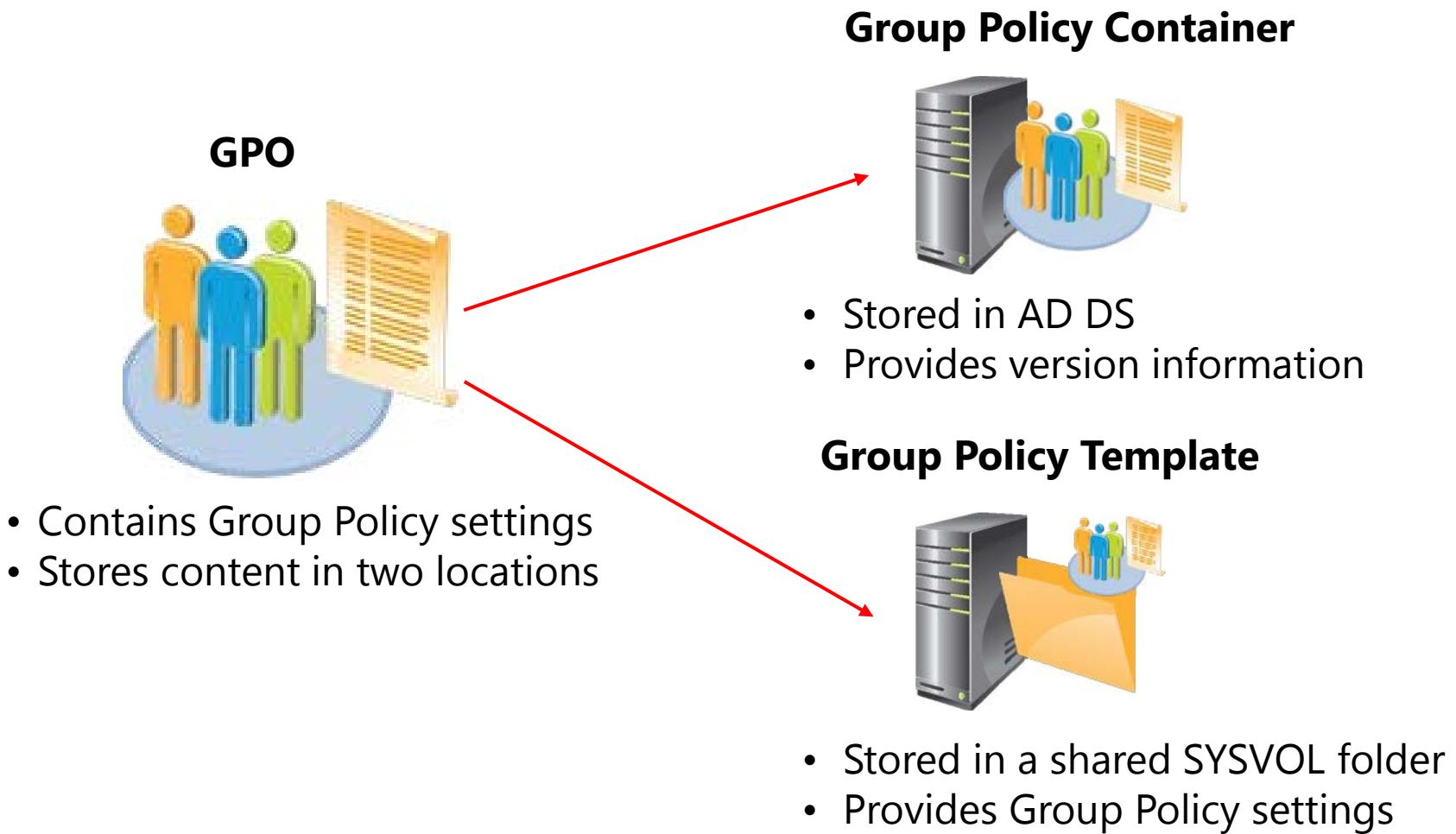
# Lesson 2: Implementing and Administering GPOs

- Domain-Based GPOs
- GPO Storage
- Starter GPOs
- Common GPO Management Tasks
- Delegating Administration of Group Policies
- Managing GPOs with Windows PowerShell

# Domain-Based GPOs



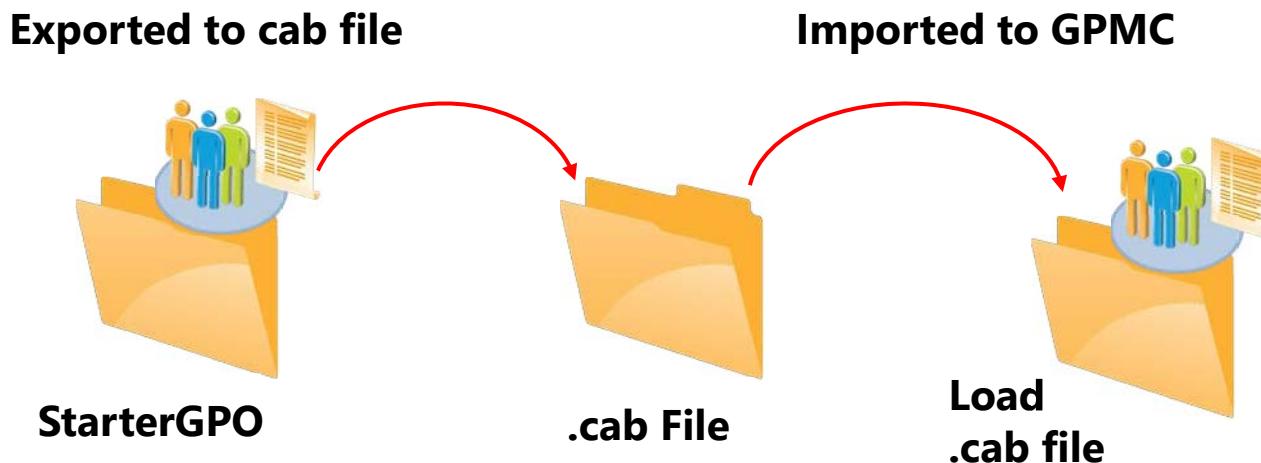
# GPO Storage



# Starter GPOs

## A Starter GPO:

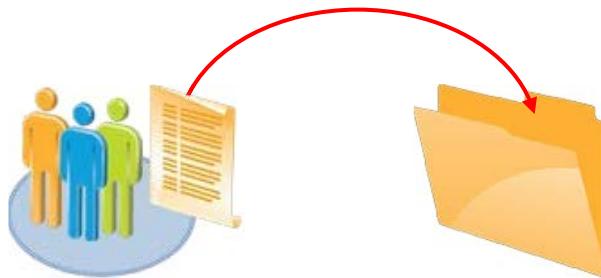
- Stores Administrative Template settings on which the new GPOs will be based
- Can be exported to .cab files
- Can be imported into other areas of the enterprise



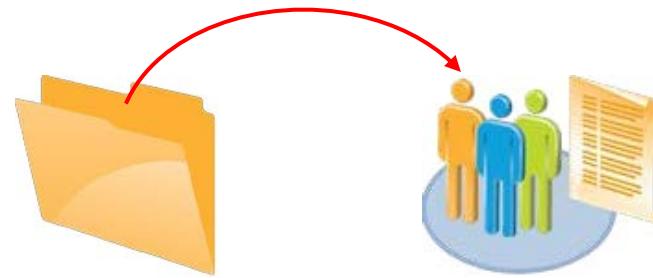
# Common GPO Management Tasks

GPMC provides several options for managing the state of GPOs

**Backup GPOs**



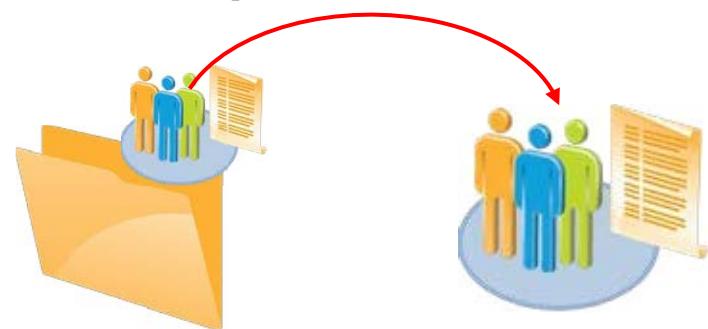
**Restore GPOs**



**Copy GPOs**



**Import GPOs**



# Delegating Administration of Group Policies

- Delegation of GPO-related tasks allows the administrative workload to be distributed across the enterprise
- The following Group Policy tasks can be independently delegated:
  - Creating GPOs
  - Editing GPOs
  - Managing Group Policy links for a site, domain, or OU
  - Performing Group Policy Modeling analysis on a domain or OU
  - Reading Group Policy Results data in a domain or OU
  - Creating WMI filters in a domain

# Managing GPOs with Windows PowerShell

In addition to using GPMC and the Group Policy Management Editor, you can also perform common GPO administrative tasks by using Windows PowerShell

## Examples:

- Create a new GPO called Sales:

***New-GPO -Name Sales -comment "This is the sales GPO"***

- Import the settings from the backup Sales GPO in the C:\Backups folder into the NewSales GPO:

***import-gpo -BackupGpoName Sales -TargetName NewSales -path c:\backups***

# Lesson 3: Group Policy Scope and Group Policy Processing

- GPO Links
- Demonstration: Linking GPOs
- Group Policy Processing Order
- Configuring GPO Inheritance and Precedence
- Using Security Filtering to Modify Group Scope
- What Are WMI Filters?
- Demonstration: Filtering Policies
- Enable and Disable GPOs and GPO Nodes
- Loopback Policy Processing
- Strategies for Slow Links and Disconnected Systems
- Identifying When Settings Become Effective
- Considerations For Managing Group Policy In A Multi-Domain Environment

# GPO Links

Group Policy Management

File Action View Window Help

Group Policy Management

Forest: Adatum.com

Domains

Adatum.com

- Default Domain Policy
- Security Settings
- Development
- Domain Controllers
  - Default Domain Controllers
  - IT
  - Managers
  - Marketing
  - Research
  - Sales
- Group Policy Objects
- WMI Filters
- Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Adatum.com

Status Linked Group Policy Objects Group Policy Inheritance Delegation

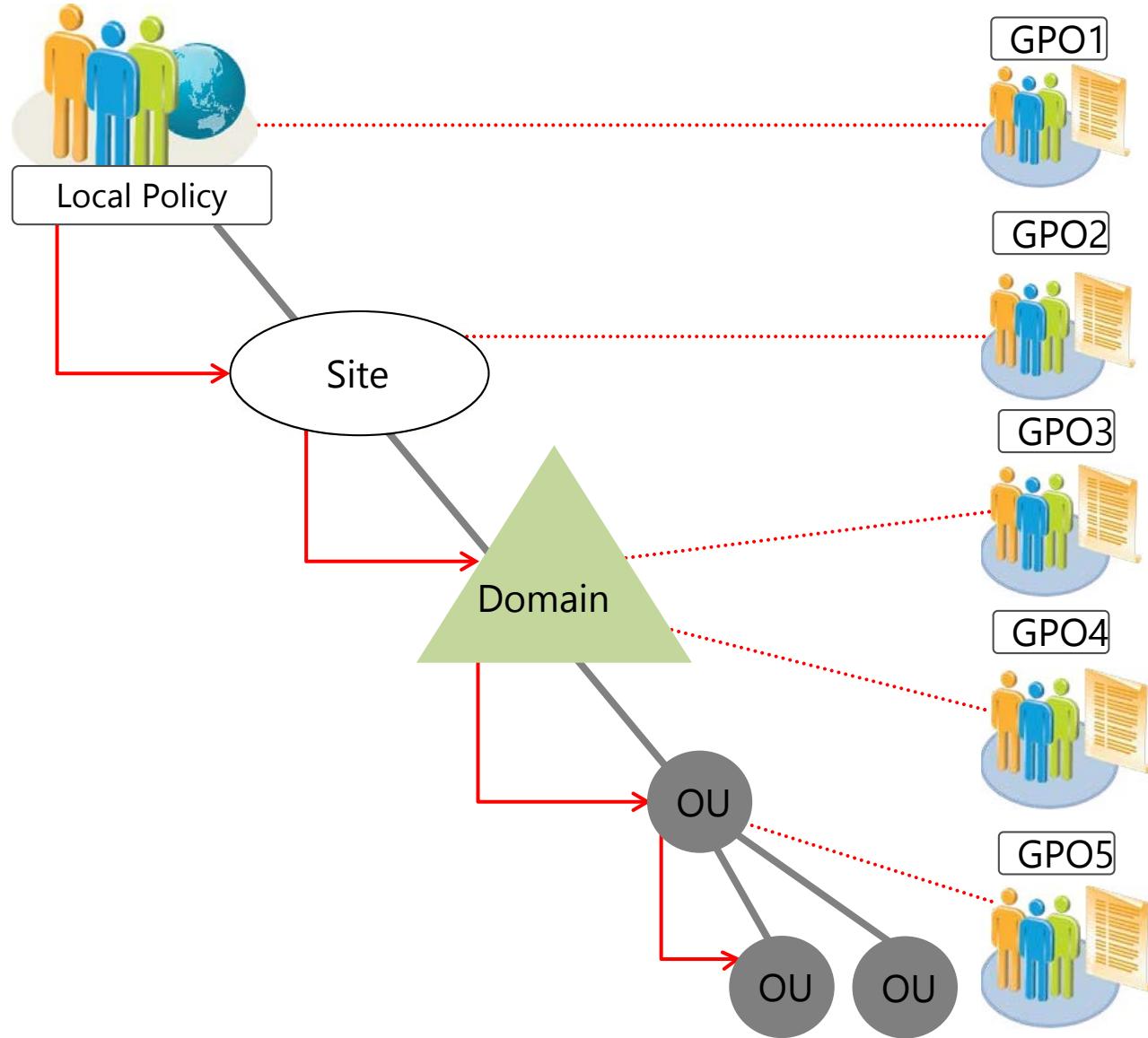
| Link Order | GPO                   | Enforced | Link Enabled | GPO Status | WMI    |
|------------|-----------------------|----------|--------------|------------|--------|
| 1          | Default Domain Policy | No       | Yes          | Enabled    | Normal |
| 2          | Security Settings     | No       | Yes          | Enabled    | Normal |

# Demonstration: Linking GPOs

In this demonstration, you will see how to:

- Create and link GPOs to different locations
- Disable a GPO link
- Delete a GPO link

# Group Policy Processing Order



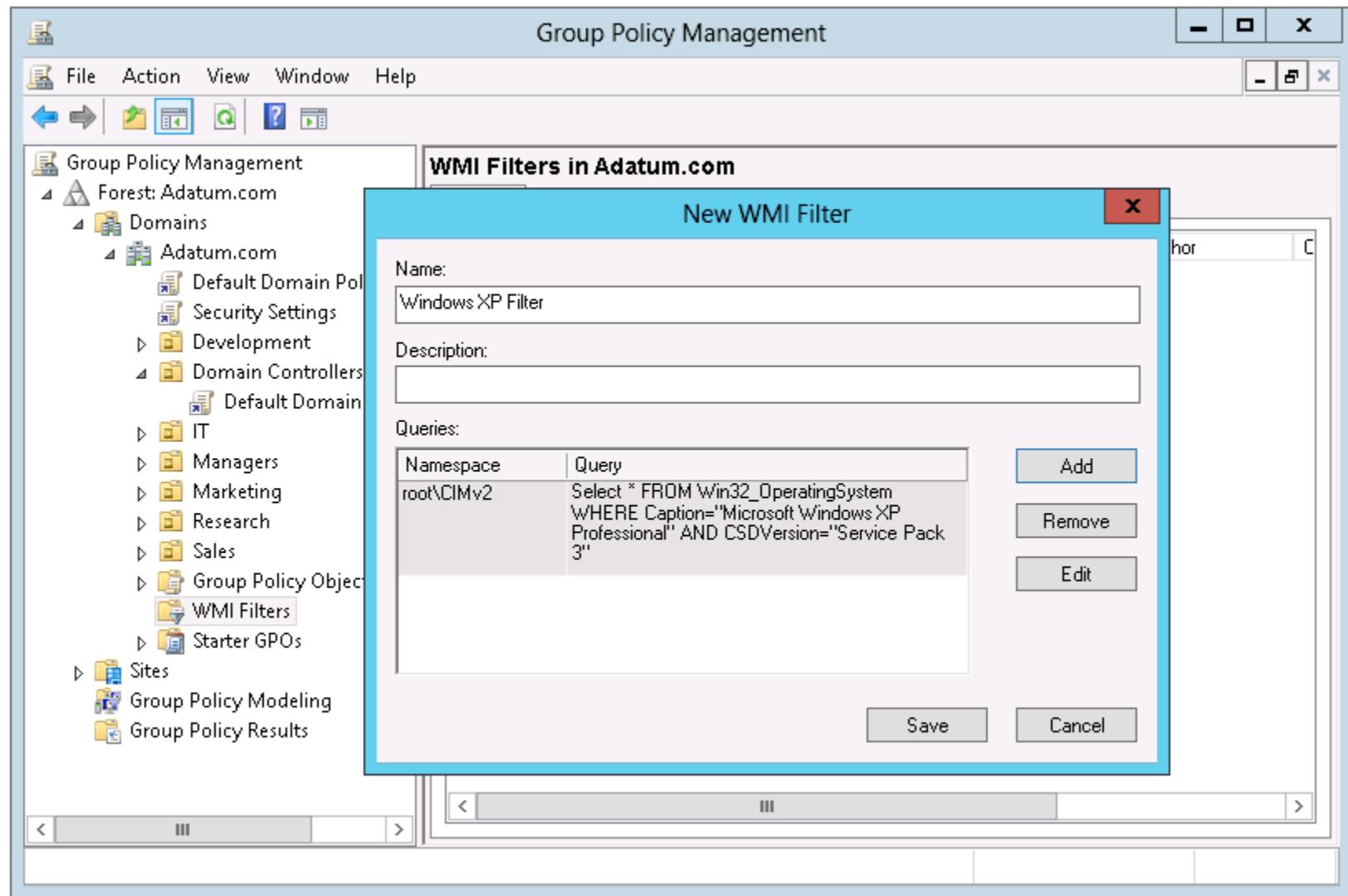
# Configuring GPO Inheritance and Precedence

1. The application of GPOs that are linked to each container results in a cumulative effect called *inheritance*
  - Default Precedence: Local → Site → Domain → OU → OU... (LSDOU)
  - Seen on the Group Policy Inheritance tab
2. Link order (attribute of GPO Link)
  - Lower number → Higher on list → Precedent
3. Block Inheritance (attribute of OU)
  - Blocks the processing of GPOs from above
4. Enforced (attribute of GPO link)
  - Enforced GPOs “blast through” Block Inheritance
  - Enforced GPO settings win over conflicting settings in lower GPOs

# Using Security Filtering to Modify Group Scope

- Apply Group Policy permission
  - GPO has an ACL (Delegation tab → Advanced)
  - Default: Authenticated Users have Allow Read and Allow Apply Group Policy
- Scope only to users in selected global groups
  - Remove Authenticated Users
  - Add appropriate global groups
    - Must be global groups (GPOs do not scope to domain local)
- Scope to users except for those in selected groups
  - On the Delegation tab, click Advanced
  - Add appropriate global groups
  - Deny Apply Group Policy permission
  - Does not appear on the Delegation tab or in filtering section

# What Are WMI Filters?

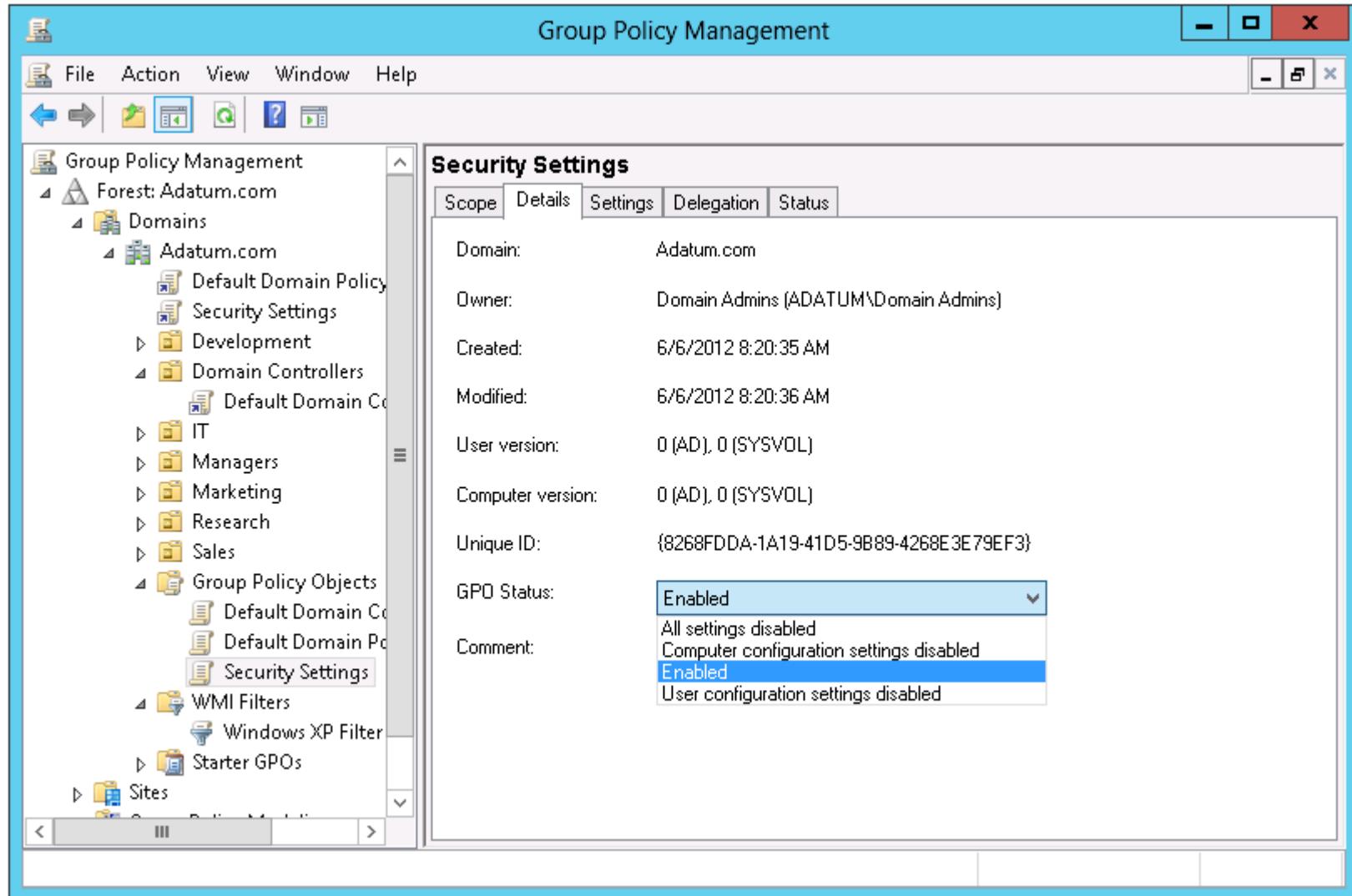


# Demonstration: Filtering Policies

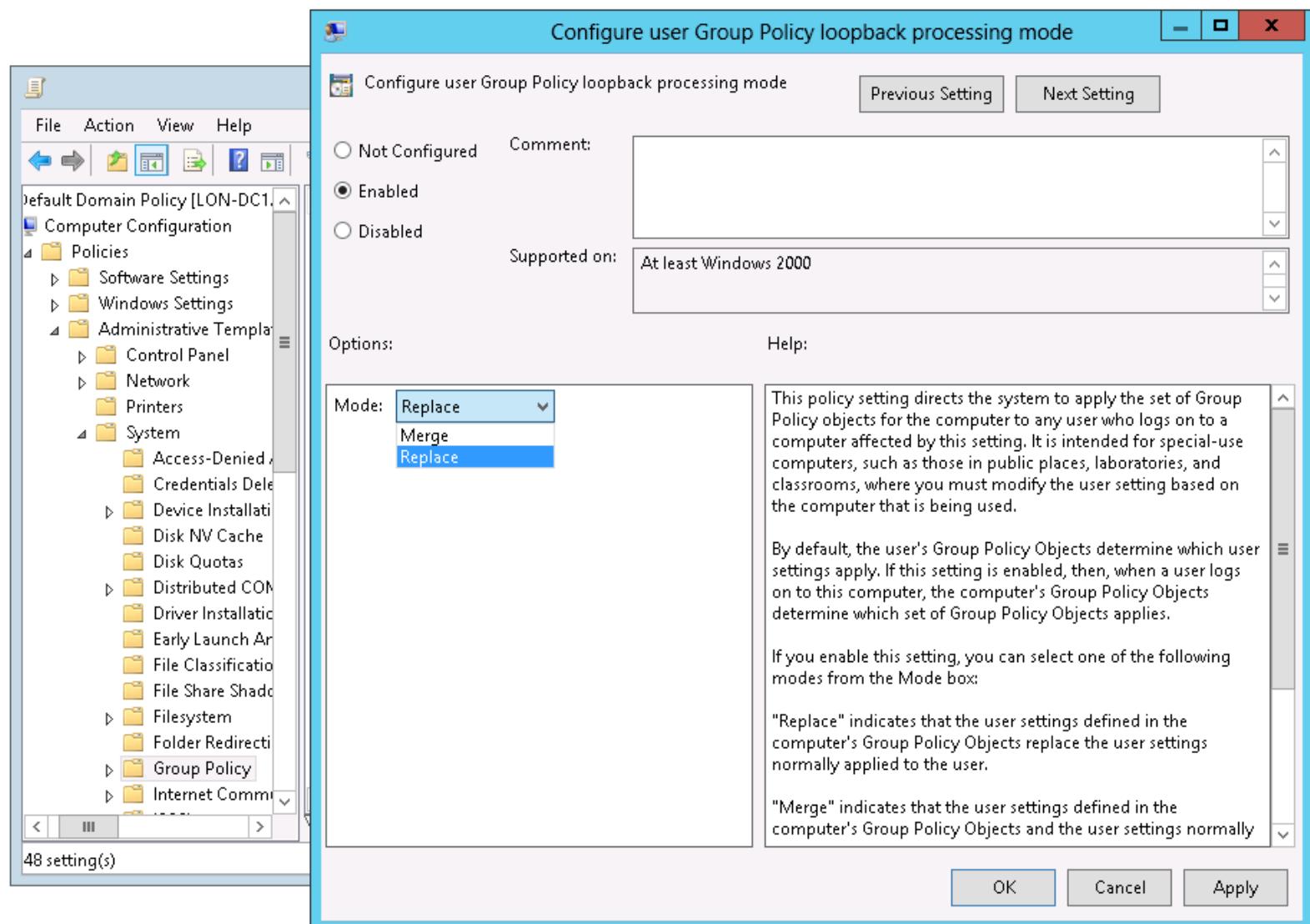
In this demonstration, you will see how to:

- Filter group policy application by using security group filtering
- Filter Group Policy application by using WMI filtering

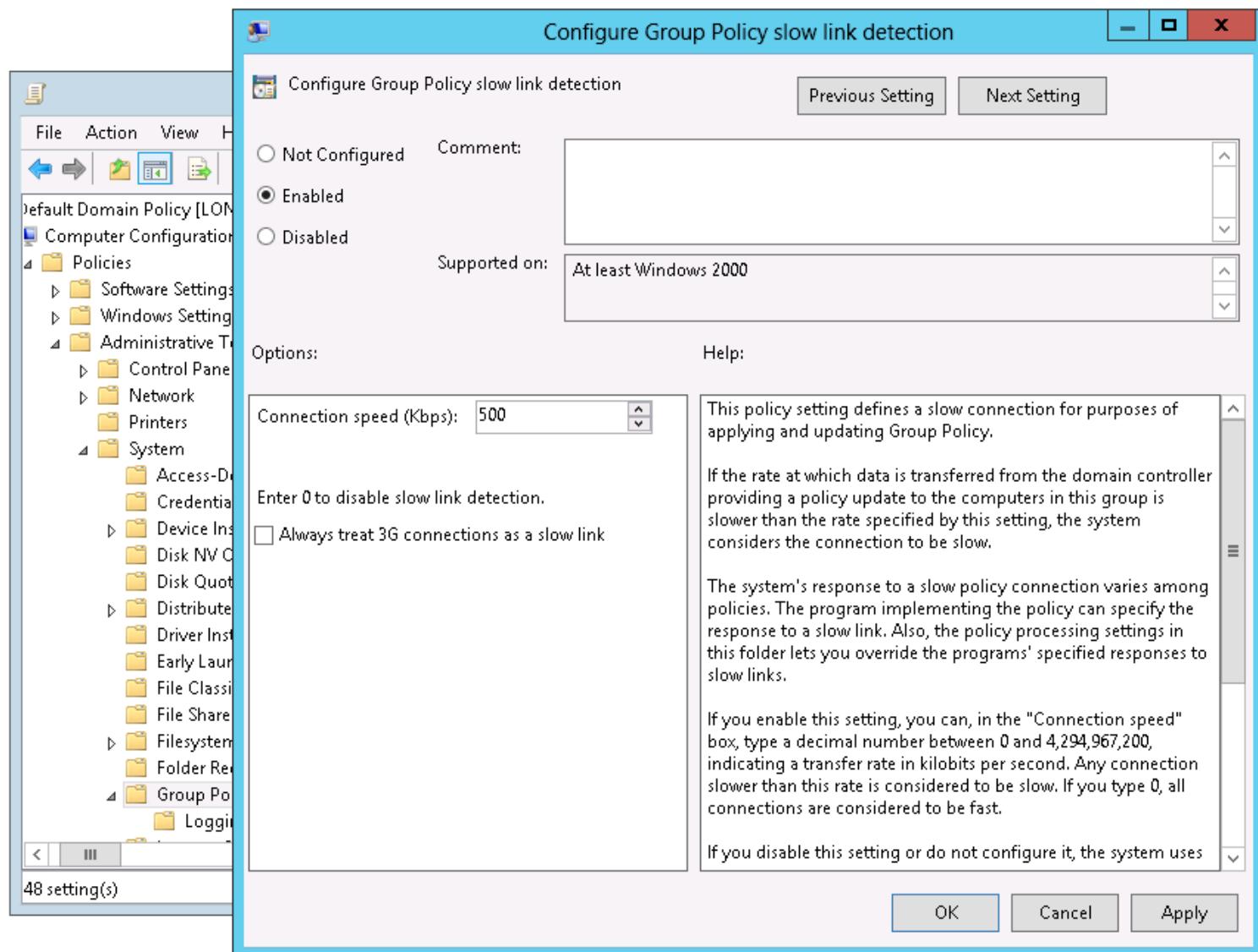
# Enable and Disable GPOs and GPO Nodes



# Loopback Policy Processing



# Strategies for Slow Links and Disconnected Systems



# Identifying When Settings Become Effective

- GPO replication must happen
- Group changes must be replicated
- Group Policy refresh must occur
- User must log off or log on, or the computer must restart
- Manual refresh
- Most CSEs do not reapply unchanged GPO settings

# Considerations For Managing Group Policy In A Multi-Domain Environment

- Domain trust is required for simplifying multi-domain management of Group Policy
  - Use migration tables to automate the updates to UNC paths and security principals
- Common GPO management techniques are valid across domains
  - Copy GPOs (**Copy-GPO**)
  - Import GPOs (**Import-GPO**)
  - Backing up and restoring (**Backup-GPO, Restore-GPO**)
- Multi-domain environment may be made up of an internal test implementation of AD DS and a production implementation of AD DS

# Lesson 4: Troubleshooting the Application of GPOs

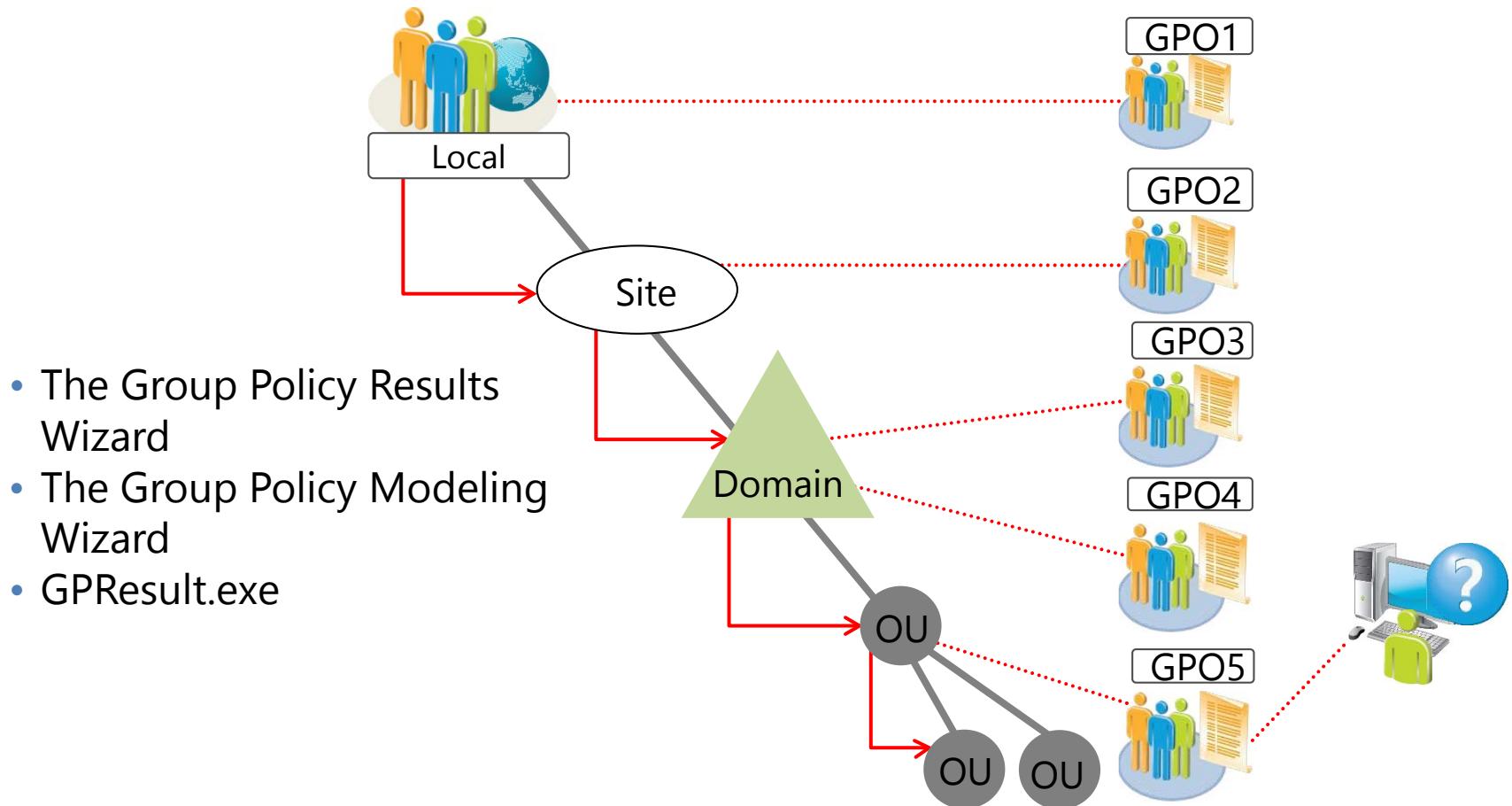
- Refreshing GPOs
- What is RSoP?
- Generate RSoP Reports
- Demonstration: Performing What-If Analysis with the Group Policy Modeling Wizard
- Examine Policy Event Logs

# Refreshing GPOs

- When you apply GPOs, remember that:
  - Computer settings apply at startup
  - User settings apply at logon
  - Policies refresh at regular, configurable intervals
  - Security settings refresh at least every 16 hours
  - Policies refresh manually by using:
    - The **Gupdate** command
    - The Windows PowerShell cmdlet **Invoke-GPUpdate**
  - With the new Remote Policy Refresh feature in Windows Server 2012, you can remotely refresh policies

# What is RSOP?

Windows Server 2012 provides the following tools for performing RSOP analysis:



# Generate RSoP Reports

Group Policy Management

File Action View Window Help

Administrator on LON-CL1

Summary Details Policy Events

Group Policy Results

ADATUM\administrator on ADATUM\LON-CL1

Data collected on: 6/6/2012 9:05:16 AM

[show all](#) [hide](#)

**Computer Details**

[General](#) [hide](#)

|                           |                         |
|---------------------------|-------------------------|
| Computer name             | ADATUM\LON-CL1          |
| Domain                    | Adatum.com              |
| Site                      | Default-First-Site-Name |
| Security Group Membership | <a href="#">show</a>    |

[Component Status](#) [hide](#)

| Component Name              | Status  | Time Taken         | Last Process Time    | Event Log                |
|-----------------------------|---------|--------------------|----------------------|--------------------------|
| Group Policy Infrastructure | Success | 3 Second(s)        | 6/6/2012 9:01:22 AM  | <a href="#">View Log</a> |
| Registry                    | Success | 703 Millisecond(s) | 5/14/2012 6:12:58 AM | <a href="#">View Log</a> |
| Security                    | Success | 47 Millisecond(s)  | 5/14/2012 6:12:58 AM | <a href="#">View Log</a> |

Adatum.com

- Default Domain Policy
- Security Settings
- Development
- Domain Controllers
  - Default Domain Controller
- IT
- Managers
- Marketing
- Research
- Sales
- Group Policy Objects
  - Default Domain Controller
  - Default Domain Policy
  - Security Settings
- WMI Filters
  - Windows XP Filter
- Starter GPOs

Sites

Group Policy Modeling

Group Policy Results

Administrator on LON-CL1

# Demonstration: Performing What-If Analysis with the Group Policy Modeling Wizard

In this demonstration, you will see how to:

- Use GPResult.exe and the Group Policy Reporting Wizard
- Use the Group Policy Modeling Wizard

# Examine Policy Event Logs

Event Viewer

File Action View Help

Operational Number of events: 6,991

| Level       | Date and Time       | Source            | Event ID | Task Category |
|-------------|---------------------|-------------------|----------|---------------|
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5314     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5327     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 4257     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 4126     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5311     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5310     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5309     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5326     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5308     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5017     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 4017     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5320     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 4326     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5320     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 5017     | None          |
| Information | 9/3/2013 1:13:57 PM | GroupPolicy (...) | 4017     | None          |

Actions

Operational

- Open Saved Log...
- Create Custom View...
- Import Custom View...
- Clear Log...
- Filter Current Log...
- Properties
- Disable Log
- Find...
- Save All Events As...
- Attach a Task To this L...
- View
- Refresh
- Help

Event 4257, GroupPolicy (Microsoft-Windows-GroupPolicy)

General Details

Starting to download policies.

Log Name: Microsoft-Windows-GroupPolicy/Operational  
Source: GroupPolicy (Microsoft-Win  
Event ID: 4257  
Level: Information  
Logged: 9/3/2013 1:13:57 PM  
Task Category: None  
Keywords:

Actions

Event 4257, GroupPolicy (Microsoft-Windows-GroupPolicy)

- Event Properties
- Attach Task To This Ev...
- Copy
- Save Selected Events...
- Refresh
- Help

# Lab: Implementing a Group Policy Infrastructure

- Exercise 1: Creating and Configuring GPOs
- Exercise 2: Managing GPO Scope
- Exercise 3: Verifying GPO Application
- Exercise 4: Managing GPOs

## Logon Information

Virtual machines: 20411D-LON-DC1,

20411D-LON-CL1

User name:

**Adatum\Administrator**

Password:

**Pa\$\$w0rd**

Estimated Time: 90 minutes

# Lab Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, England. An IT office and a data center are located in London to support the London office and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure.

You have been asked to use Group Policy to implement standardized security settings to lock computer screens when users leave computers unattended for 10 minutes or more. You also have to configure a policy setting that will prevent

## Lab Scenario

access to certain programs on local workstations.

After some time, you have been made aware that a critical application fails when the screensaver starts, and an engineer has asked you to prevent the setting from applying to the team of Research engineers that uses the application every day. You also have been asked to configure conference room computers to use a 45-minute timeout.

After creating the policies, you need to evaluate the RSoPs for users in your environment to ensure that the Group Policy infrastructure is optimal and that all policies apply as intended.

# Lab Review

- Which policy settings are already being deployed by using Group Policy in your organization?
- Many organizations rely heavily on security group filtering to scope GPOs, rather than linking GPOs to specific OUs. In these organizations, GPOs typically are linked very high in the Active Directory logical structure—to the domain itself or to a first-level OU. What advantages do you gain by using security group filtering rather than GPO links to manage a GPO's scope?

# Lab Review

- Why might it be useful to create an exemption group—a group that is denied the Apply Group Policy permission—for every GPO that you create?
- Do you use loopback policy processing in your organization? In which scenarios and for which policy settings can loopback policy processing add value?
- In which situations have you used RSoP reports to troubleshoot Group Policy application in your organization?
- In which situations have you used, or might you anticipate using, Group Policy Modeling?

# Module Review and Takeaways

- Review Question(s)
- Tools
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 5

### Managing User Desktops with Group Policy

**Microsoft®**

# Module Overview

- Implementing Administrative templates
- Configuring Folder Redirection and Scripts
- Configuring Group Policy Preferences
- Managing Software with Group Policy

# Lesson 1: Implementing Administrative templates

- What Are Administrative templates?
- What Are ADM and ADMX Files?
- The Central Store
- Discussion: Practical Uses of Administrative templates
- Demonstration: Configuring Settings with Administrative templates
- Extending Administrative templates
- Demonstration: Configuring Administrative templates

# What Are Administrative templates?

Administrative Templates provide you with the ability to control both the environment of the operating system and user experience

## **Administrative Templates sections for computers are:**

- Control Panel
- Network
- Printers
- Server
- Start Menu and Taskbar
- System
- Windows components

## **Administrative Templates sections for users are:**

- Control panel
- Desktop
- Network
- Shared Folders
- Start Menu and Taskbar
- System
- Windows components

Each of these main sections contains many subfolders to help you further organize settings

# What Are ADM and ADMX Files?

## ADM files:

- Are copied into every GPO in SYSVOL
- Are difficult to customize

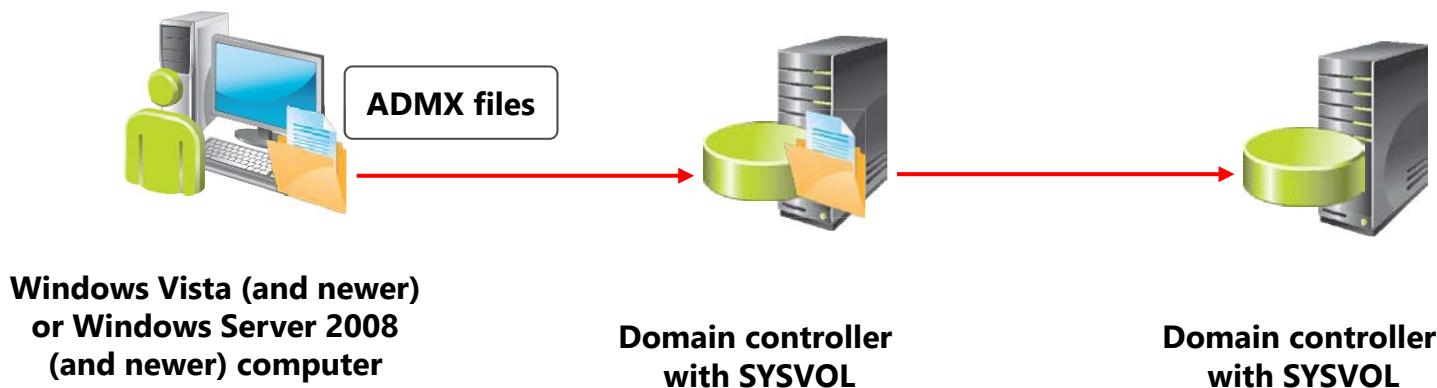
## ADMX files:

- Include language-neutral ADML files that provide the localized language
- Are not stored in the GPO
- Are extensible through XML

# The Central Store

## The Central Store:

- Is a central repository for ADMX and ADML files
- Is stored in SYSVOL
- Must be created manually
- Is detected automatically by Windows Vista (and newer) or Windows Server 2008 (and newer)



# Discussion: Practical Uses of Administrative templates

- How do you currently provide desktop security?
- How much administrative access do users have to their systems?
- Which Group Policy settings will you find useful in your organization?



# Demonstration: Configuring Settings with Administrative templates

In this demonstration, you will see how to:

- Filter Administrative Template policy settings
- Apply comments to policy settings
- Add comments to a GPO
- Create a new GPO by copying an existing GPO
- Create a new GPO by importing settings that were exported from another GPO

# Extending Administrative templates

- Extend administrative templates by creating new templates or downloading available templates
- Add the templates to a GPO so that the settings become available
- Customize the settings
- Deploy the GPO

# Demonstration: Configuring Administrative templates

In this demonstration, you will see how to:

- Import the Office 2013 administrative template files
- Customize Office 2013 settings by using the administrative template

# Lesson 2: Configuring Folder Redirection and Scripts

- What Is Folder Redirection?
- Settings for Configuring Folder Redirection
- Security Settings for Redirected Folders
- Demonstration: Configuring Folder Redirection
- Group Policy Settings for Applying Scripts
- Demonstration: Configuring Scripts with GPOs

# What Is Folder Redirection?

Folder redirection is a feature that allows folders to be located on a network server, but appear as if they are located on the local drive

Folders that can be redirected in Windows Vista and later are:

- Desktop
- Start Menu
- Documents
- Pictures
- AppData\Roaming
- Contacts
- Downloads
- Favorites
- Saved Games
- Searches
- Links
- Music
- Videos

# Settings for Configuring Folder Redirection

## Folder redirection configuration options:

Use Basic folder redirection when all users save their files to the same parent location

Use Advanced folder redirection when the server hosting the folder location is based on group membership

Use the Follow the Documents folder to force certain folders to become subfolders of Documents

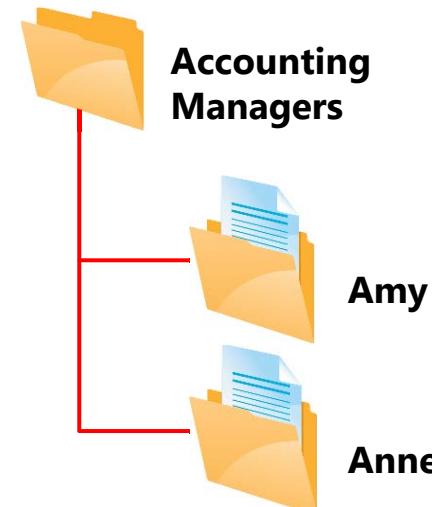
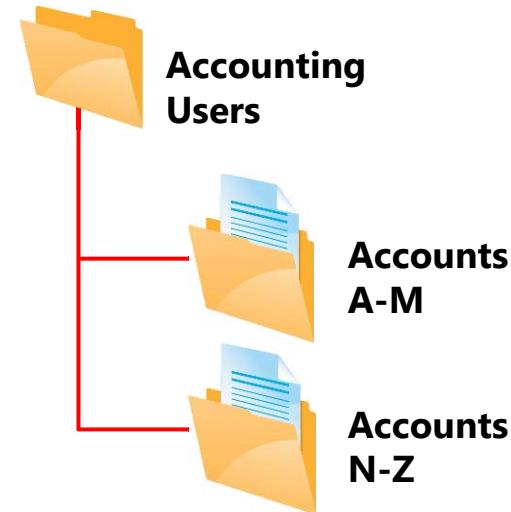
## Target folder location options:

Redirect to the users' home directory  
(Documents folder only)

Create a folder for each user under the root path

Redirect to the following location

Redirect to the local user profile location



# Security Settings for Redirected Folders

## NTFS permissions for root folder

| Creator/Owner                                       | Full control – subfolders and files only                           |
|-----------------------------------------------------|--------------------------------------------------------------------|
| Administrator                                       | None                                                               |
| Security group of users that save data on the share | List Folder/Read Data, Create Folders/Append Data-This Folder Only |
| System                                              | Full control                                                       |

## Share permissions for root folder

| Creator/Owner                                       | Full control – subfolders and files only |
|-----------------------------------------------------|------------------------------------------|
| Security group of users that save data on the share | Full control                             |

## NTFS permissions for each user's redirected folder

| Creator/Owner  | Full control – subfolders and files only |
|----------------|------------------------------------------|
| %Username%     | Full control, owner of folder            |
| Administrators | None                                     |
| System         | Full control                             |

# Demonstration: Configuring Folder Redirection

In this demonstration, you will see how to:

- Create a shared folder for folder redirection
- Create a GPO to redirect the Documents folder
- Test folder redirection

# Group Policy Settings for Applying Scripts

You can use scripts to perform many tasks, such as clearing page files or mapping drives, and clearing temp folders for users

You can assign Group Policy script settings to assign:

- For computers:
  - Startup scripts
  - Shutdown scripts
- For users:
  - Logon scripts
  - Logoff scripts

# Demonstration: Configuring Scripts with GPOs

In this demonstration, you will see how to:

- Create a login script to map a network drive
- Create and link a GPO to use the script and store the script in the Netlogon share
- Log on to client computer and test results

# Lesson 3: Configuring Group Policy Preferences

- What Are Group Policy Preferences?
- Comparing Group Policy Preferences and Administrative templates
- Features of Group Policy Preferences
- Item-Level Targeting Options
- Demonstration: Configuring Group Policy Preferences

# What Are Group Policy Preferences?

Group Policy preferences expand the range of configurable settings within a GPO

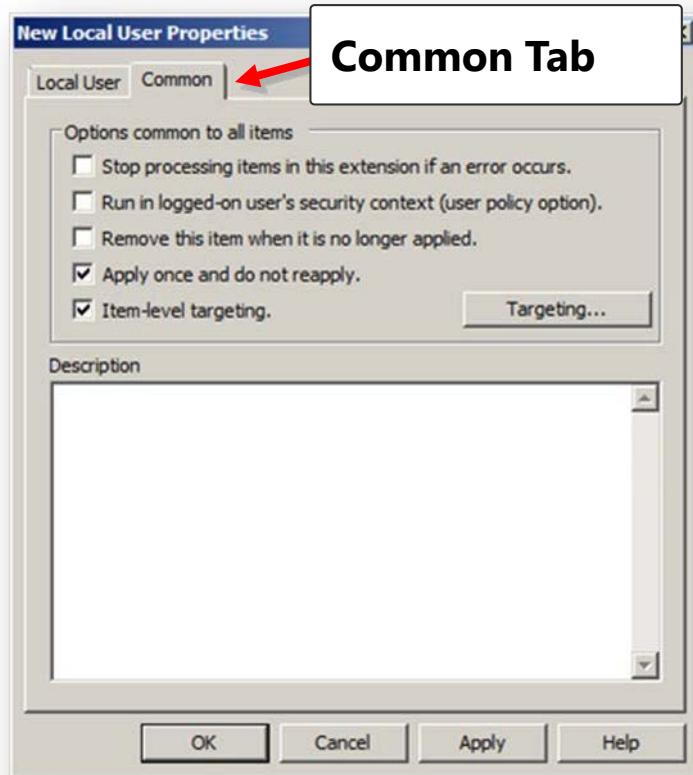
Group Policy preferences:

- Enable IT professionals to configure, deploy, and manage settings that were not manageable by using Group Policy
- Are natively supported on Windows Server 2008 and Windows Vista SP2 or newer
- Can be created, deleted, replaced, or updated

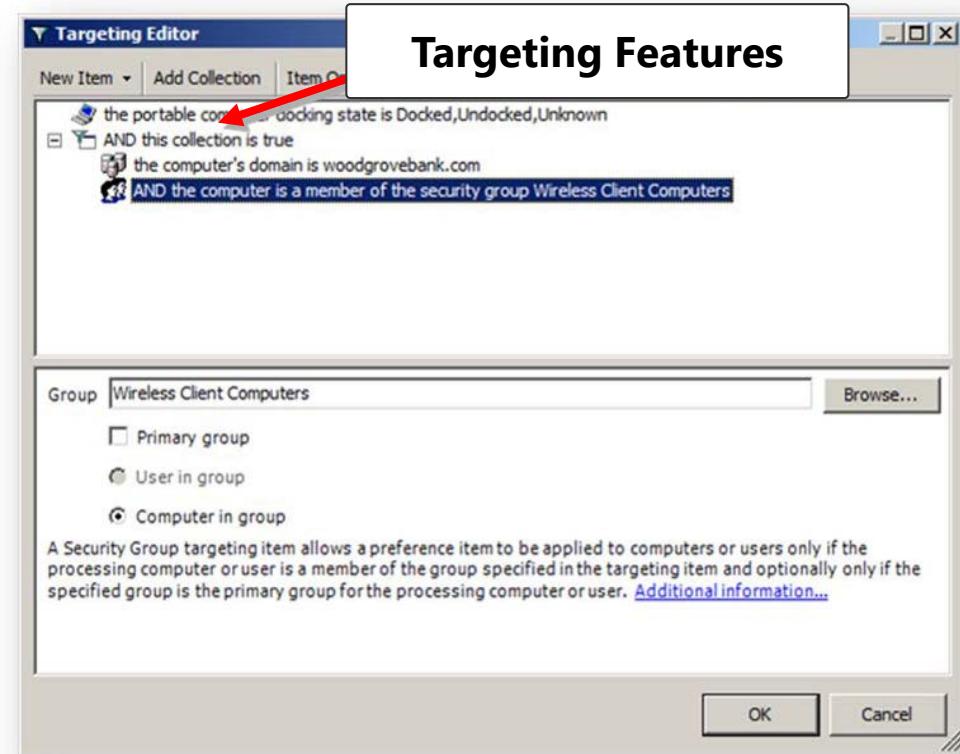
# Comparing Group Policy Preferences and Administrative templates

| <b>Group Policy settings</b>                                                                                        | <b>Group Policy Preferences</b>                                                                                                |
|---------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Strictly enforce policy settings by writing the settings to areas of the registry that standard users cannot modify | Are written to the normal locations in the registry that the application or operating system feature uses to store the setting |
| Typically disable the user interface for settings that Group Policy is managing                                     | Do not cause the application or operating system feature to disable the user interface for the settings they configure         |
| Refresh policy settings at a regular intervals                                                                      | Refresh preferences by using the same interval as Group Policy settings by default                                             |

# Features of Group Policy Preferences



**Common Tab**



**Targeting Features**

**Is used to configure additional options that control the behavior of a Group Policy preference item**

**Determines to which users and computers a preference item applies**

# Item-Level Targeting Options

- Target 27 different categories
- Combine different categories together by using AND or OR Boolean logic. Instead of using a single category for targeting, you can use multiple categories
- Item-level targeting is refreshed during the Group Policy background refresh

# Demonstration: Configuring Group Policy Preferences

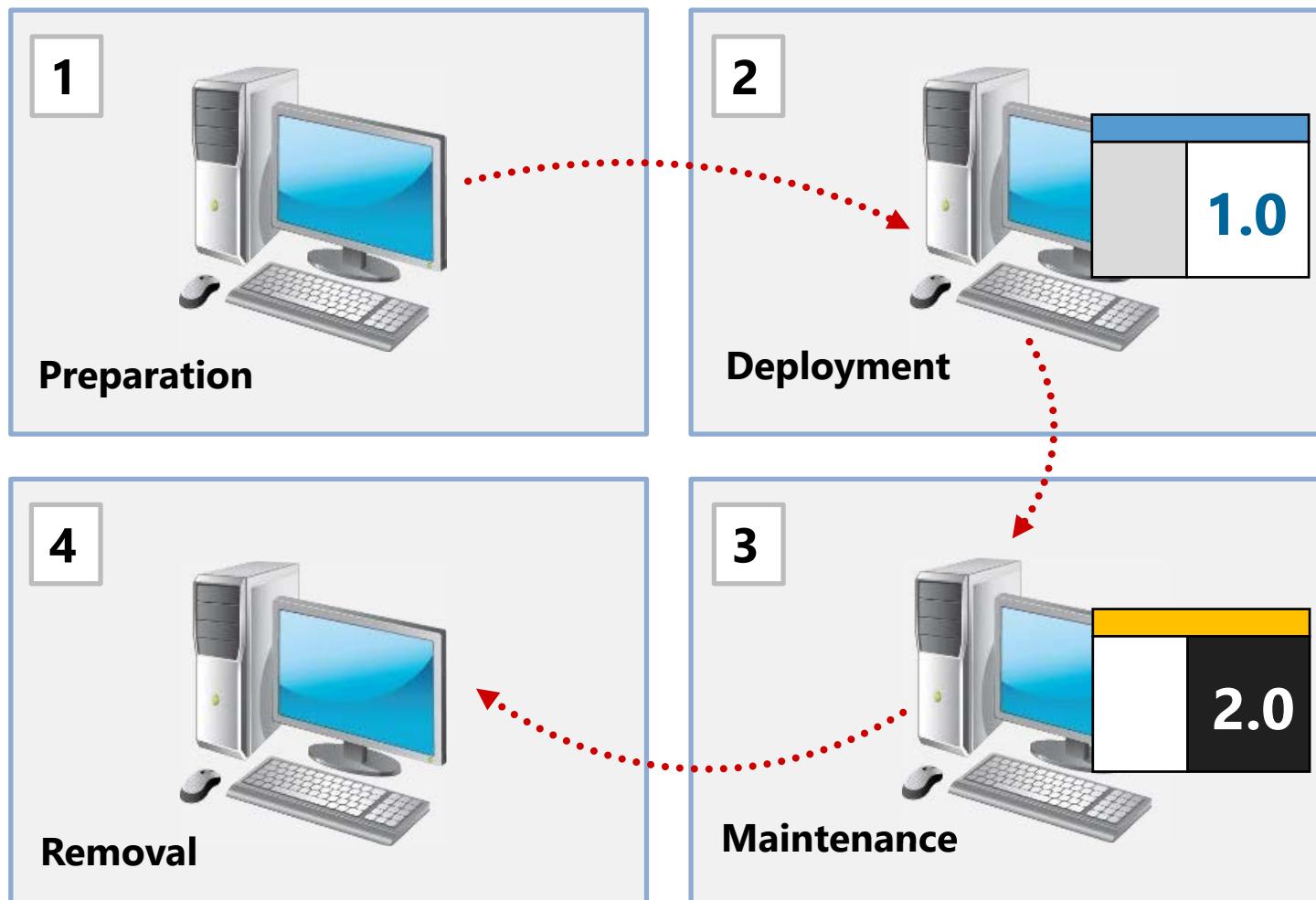
In this demonstration, you will see how to:

- Configure a desktop shortcut with Group Policy preferences
- Target the preference
- Configure a new folder with Group Policy preferences
- Target the preference
- Test the preferences

# Lesson 4: Managing Software with Group Policy

- How Group Policy Software Distribution Helps to Address the Software Lifecycle
- How Windows Installer Enhances Software Distribution
- Assigning and Publishing Software
- Managing Software Upgrades by Using Group Policy

# How Group Policy Software Distribution Helps to Address the Software Lifecycle



# How Windows Installer Enhances Software Distribution

## Windows Installer:

### Windows Installer service:

- Fully automates the software installation and configuration process
- Modifies or repairs an existing application installation

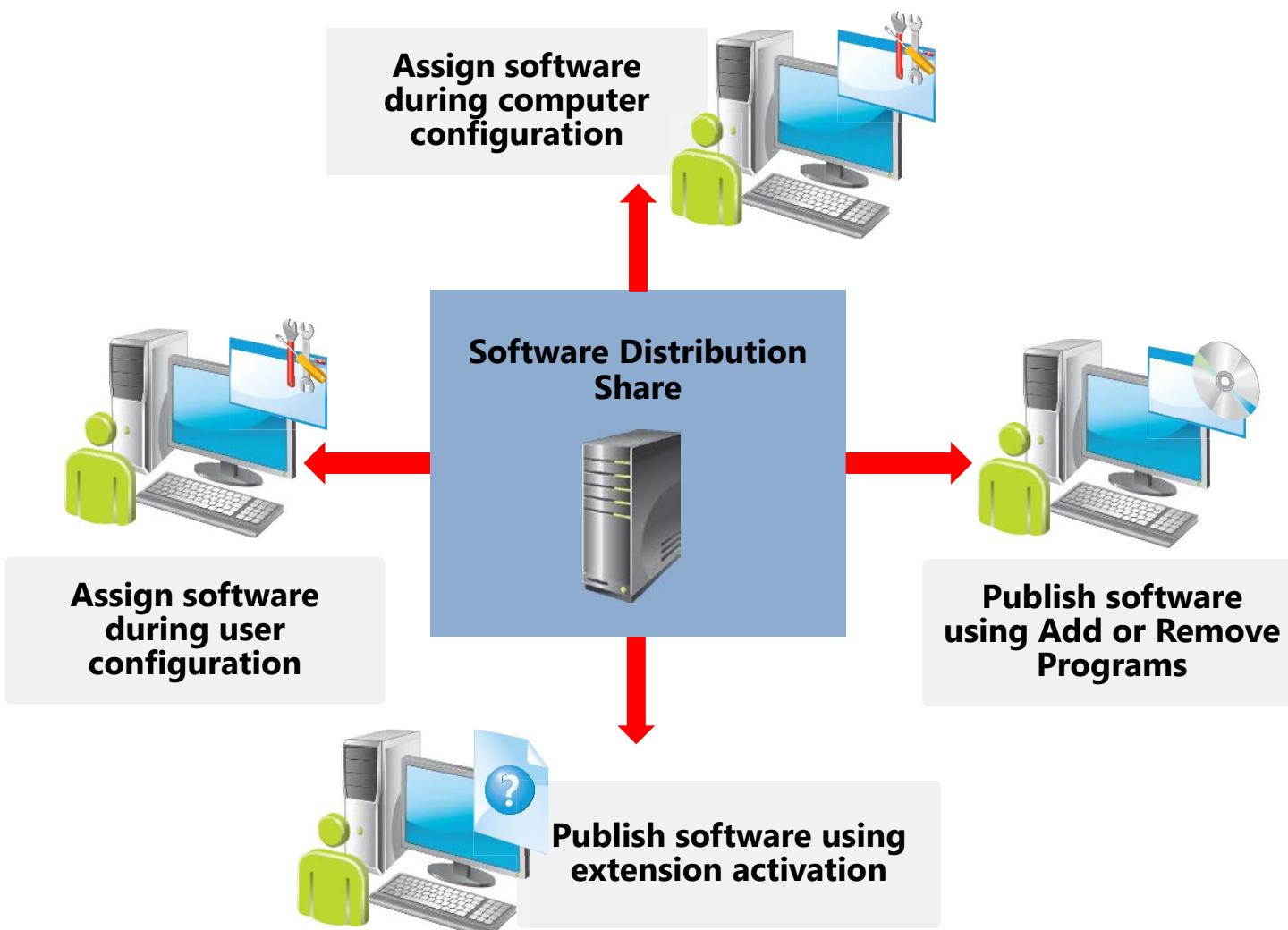
### Windows Installer package contains:

- Information about installing or uninstalling an application
- An .msi file and any external source files
- Summary information about the application
- A reference to an installation point

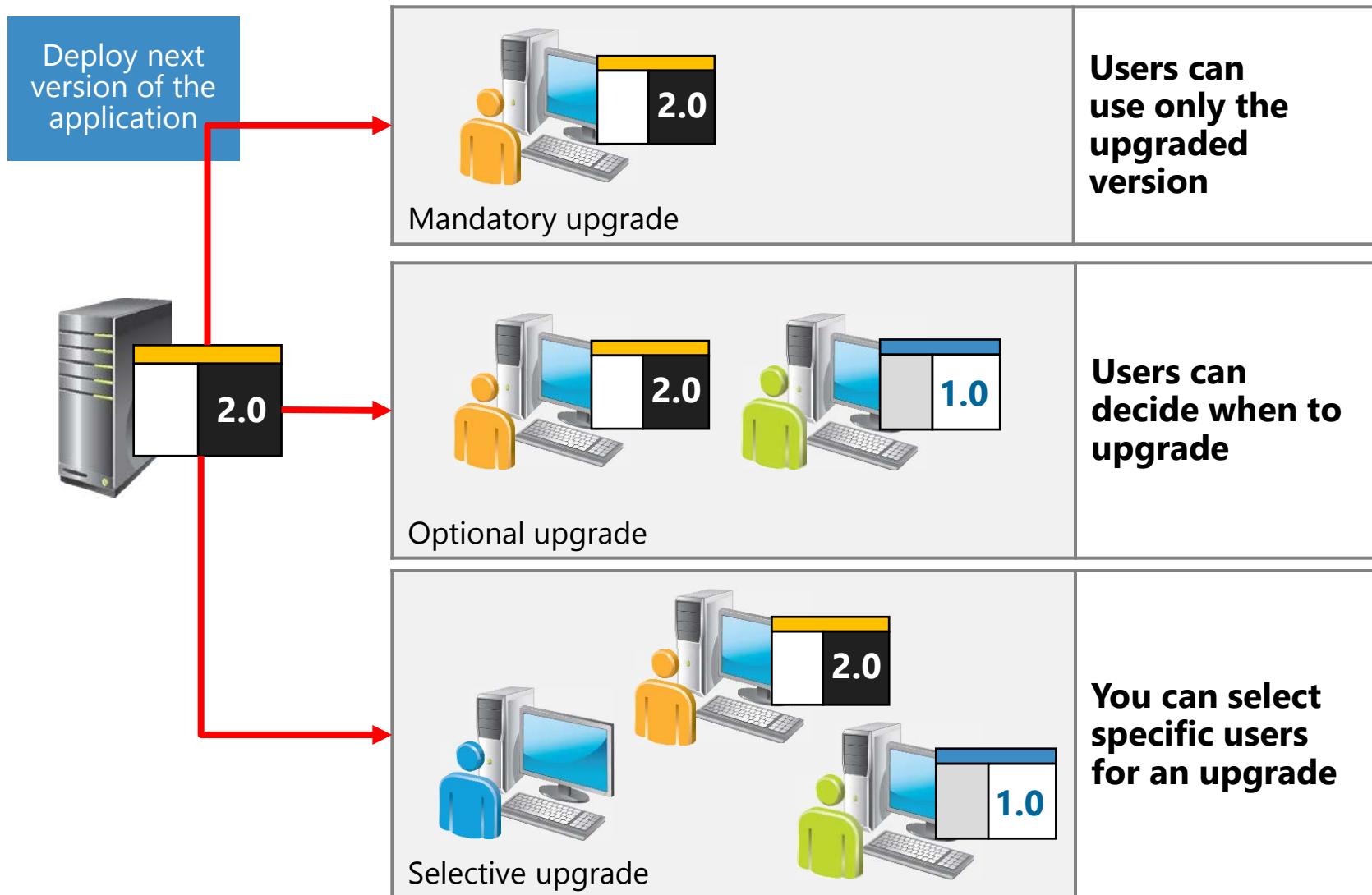
## Benefits of using Windows Installer:

- Custom installations
- Resilient applications
- Clean removal

# Assigning and Publishing Software



# Managing Software Upgrades by Using Group Policy



# Lab: Managing User Desktops with Group Policy

- Exercise 1: Implementing Settings by Using Group Policy Preferences
- Exercise 2: Managing Microsoft Office 2013 by Using Administrative templates
- Exercise 3: Deploying Software by Using Group Policy
- Exercise 4: Configuring Folder Redirection

Logon Information

Virtual Machines:

20411D-LON-DC1,

20411D-LON-CL1

User Name:

**Adatum\Administrator**

Password:

**Pa\$\$w0rd**

Estimated Time: 45 minutes

# Lab Scenario

- A. Datum Corporation is a global engineering and manufacturing company with its head office in London, England. An IT office and a data center are located in London to support the London head office and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.
- A. Datum has been using logon scripts to provide users with drive mappings to file shares. The maintenance of these scripts is an ongoing problem because they are large and complex.

## Lab Scenario

Your manager has asked you to implement the drive mappings by using Group Policy preferences so that logon scripts can be removed.

Your manager has also asked you to place a shortcut to the Notepad application for all users that belong to the IT security group and to add a new Computer Administrators security group as a local Administrator on all servers.

A. Datum wants to be able to manage Office 2013 settings for all client computers. They have decided to use Administrative templates to do this.

# Lab Review

- Which options can you use to separate a user's redirected folders to different servers?
- Can you name two methods you could use to assign a GPO to selected objects within an organizational unit (OU)?
- You have created Group Policy preferences to configure new power options. How can you ensure that they will be applied only to laptop computers?

# Module Review and Takeaways

- Review Question(s)
- Best Practices
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 6

Installing, Configuring, and  
Troubleshooting the Network  
Policy Server Role

# Module Overview

- Installing and Configuring a Network Policy Server
- Configuring RADIUS Clients and Servers
- NPS Authentication Methods
- Monitoring and Troubleshooting a Network Policy Server

# Lesson 1: Installing and Configuring a Network Policy Server

- What Is a Network Policy Server?
- Demonstration: Installing the Network Policy Server Role Service
- Tools for Configuring a Network Policy Server
- Demonstration: Configuring General NPS Settings

# What Is a Network Policy Server?

A Windows Server 2012 Network Policy Server provides the following functions:

- RADIUS server. NPS performs centralized connection authentication, authorization, and accounting for wireless, authenticating switch, and dial-up and VPN connections
- RADIUS proxy. You configure connection request policies that indicate which connection requests the NPS server will forward to other RADIUS servers and to which RADIUS servers you want to forward connection requests
- NAP policy server. NPS evaluates statements of health sent by NAP-capable client computers that attempt to connect to the network

# Demonstration: Installing the Network Policy Server Role Service

In this demonstration, you will see how to:

- Install the NPS role service
- Register NPS in AD DS

# Tools for Configuring a Network Policy Server

Tools used to manage NPS include:

- NPS management console snap-in
- Netsh command-line tool:
  - NPS server commands
  - RADIUS client commands
  - Connection request policy commands
  - Remote RADIUS server group commands
  - Network policy commands
  - NAP commands
  - Accounting commands
- Windows PowerShell



# Demonstration: Configuring General NPS Settings

In this demonstration, you will see how to:

- Configure a RADIUS server for VPN connections
- Save the configuration

# Lesson 2: Configuring RADIUS Clients and Servers

- What Is a RADIUS Client?
- What Is a RADIUS Proxy?
- Demonstration: Configuring a RADIUS Client
- What Is a Connection Request Policy?
- Configuring Connection Request Processing
- Demonstration: Creating a Connection Request Policy

# What Is a RADIUS Client?

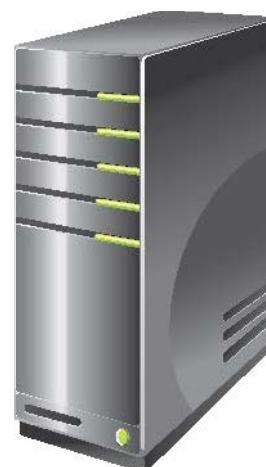
**NPS is a RADIUS server**



**Wireless access point  
(RADIUS client)**



**Client computer**



**RADIUS server**

# What Is a RADIUS Proxy?

- A RADIUS proxy receives connection attempts from RADIUS clients, and then forwards them to the appropriate RADIUS server or another RADIUS proxy for further routing
- A RADIUS proxy is required for:
  - Offering outsourced dial-up, VPN, or wireless network-access services by service providers
  - Providing authentication and authorization for user accounts that are not Active Directory members
  - Performing authentication and authorization by using a database that is not a Windows account database
  - Load-balancing connection requests among multiple RADIUS servers
  - Providing RADIUS for outsourced service providers and limiting traffic types through the firewall

# Demonstration: Configuring a RADIUS Client

In this demonstration, you will see how to configure a RADIUS client

# What Is a Connection Request Policy?

- Connection request policies are sets of conditions and settings that designate which RADIUS servers perform the authentication and authorization of connection requests that NPS receives from RADIUS clients
- Connection request policies include:
  - Conditions, such as:
    - Framed Protocol
    - Service Type
    - Tunnel Type
    - Day and Time restrictions
  - Settings, such as:
    - Authentication
    - Accounting
    - Attribute Manipulation
    - Advanced settings

# Configuring Connection Request Processing

| Configuration                                                   | Description                                                                                                                                                                                                                                                                |
|-----------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Local vs. RADIUS authentication                                 | <ul style="list-style-type: none"><li>• Local authentication takes place against the local security account database or Active Directory Domain Services.</li><li>• RADIUS authentication forwards the connection request to a RADIUS server for authentication.</li></ul> |
| RADIUS server groups                                            | <ul style="list-style-type: none"><li>• Used where one or more RADIUS servers are capable of handling connection requests. The connection requests are load-balanced on specified criteria.</li></ul>                                                                      |
| Default ports for accounting and authentication by using RADIUS | <ul style="list-style-type: none"><li>• The ports required for accounting and authentication requests being forwarded to a RADIUS server are UDP 1812/1645 and UDP 1813/1646, respectively.</li></ul>                                                                      |

# Demonstration: Creating a Connection Request Policy

In this demonstration, you will see how to create a VPN connection request policy

# Lesson 3: NPS Authentication Methods

- Password-Based Authentication Methods
- Using Certificates for Authentication
- Required Certificates for Authentication
- Deploying Certificates for PEAP and EAP

# Password-Based Authentication Methods

Authentication methods for an NPS server from the most secure to the least secure:

**MS-CHAPv2**

**MS-CHAP**

**CHAP**

**PAP**

**Unauthenticated  
access**

# Using Certificates for Authentication

With NPS, you use certificates for network access authentication because they:

- Provide stronger security
- Eliminate the need for less secure, password-based authentication



# Required Certificates for Authentication

You require the following certificates to deploy certificate-based authentication in NPS:

| Certificate                                                                         | Description                                                                                                                             |
|-------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
|    | <b>CA certificate.</b> Resides in the Trusted Root Certification Authorities certificate store for the Local Computer and Current User. |
|    | <b>Client computer certificate.</b> Resides in the certificate store of the client.                                                     |
|   | <b>Server certificate.</b> Resides in the certificate store of the NPS server.                                                          |
|  | <b>User certificate.</b> Used on a smart card.                                                                                          |

# Deploying Certificates for PEAP and EAP

- For Domain Computer and User accounts, use the autoenrollment feature in Group Policy
- Nondomain member enrollment requires an administrator to request a user or computer certificate by using the CA Web Enrollment tool
- The administrator must save the computer or user certificate to removable media, and manually install the certificate on the nondomain member computer
- The administrator can distribute user certificates on a smart card

# Lesson 4: Monitoring and Troubleshooting a Network Policy Server

- Methods Used to Monitor NPS
- Logging NPS Accounting
- Configuring Microsoft SQL Server Logging
- Configuring NPS Events to Record in the Event Viewer

# Methods Used to Monitor NPS

NPS monitoring methods include:

- Event logging
  - This method is the process of logging NPS events in the System Event log
  - This method is useful for auditing and troubleshooting connection attempts
- Logging user authentication and accounting requests
  - This method is useful for connection analysis and billing purposes
  - This method can be in a text format
  - This method can be in a database format within an instance of SQL Server

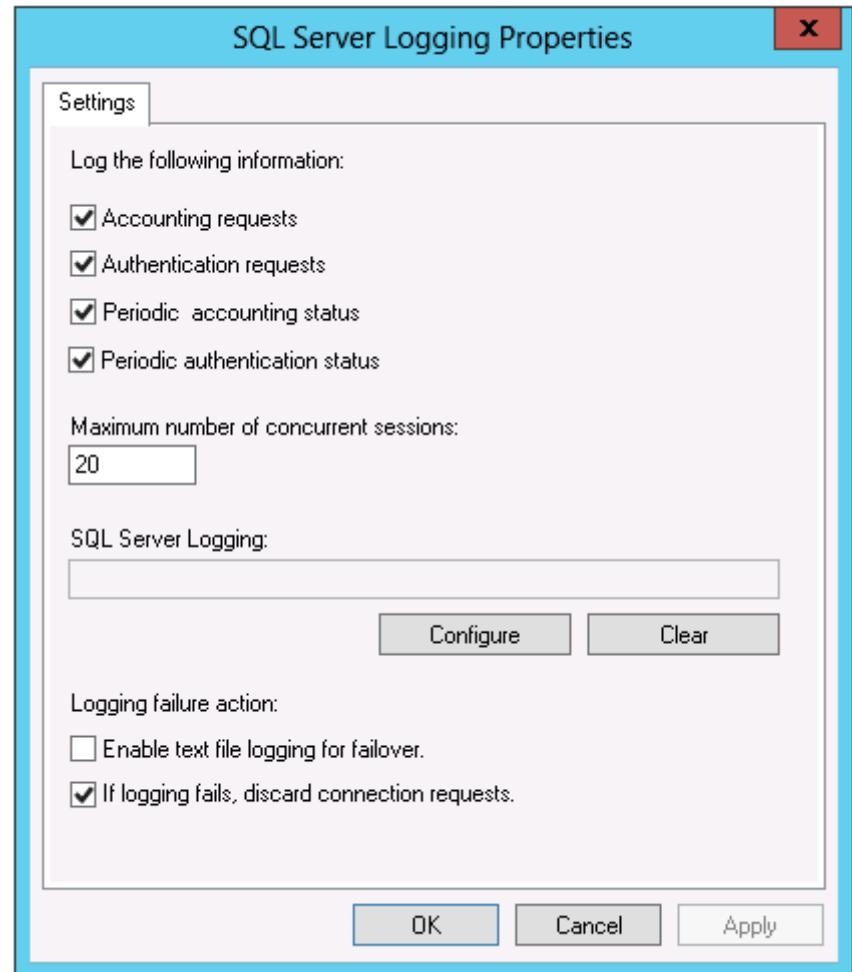
# Logging NPS Accounting

- Use the NPS console to configure logging:
  1. On the **Administrative Tools** menu, open **NPS**.
  2. In the console tree, click **Accounting**.
  3. In the details pane, click **Change Log File Properties**.
- Log files should be stored on a separate partition from the system partition.

# Configuring Microsoft SQL Server Logging

You can use SQL Server to log RADIUS accounting data:

- The SQL Server database must have a stored procedure named `report_event`
- NPS formats accounting data as an XML document
- The SQL Server database can be on a local computer or a remote server



# Configuring NPS Events to Record in the Event Viewer

- How do I configure NPS events to be recorded in Event Viewer?
  - NPS is configured by default to record failed connections and successful connections in the event log
    - You can change this behavior on the General tab of the Properties sheet for the network policy
  - Common request failure events consist of requests that NPS rejects or discards; both failure and success events are recorded
- What is Schannel logging, and how do I configure it?
  - Schannel is a security support provider that supports a set of Internet security protocols
  - You can configure Schannel logging in the following Registry key:
    - HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\SCHANNEL\EventLogging

# Lab: Installing and Configuring a Network Policy Server

- Exercise 1: Installing and Configuring NPS to Support RADIUS
- Exercise 2: Configuring and Testing a RADIUS Client

## Logon Information

**Virtual Machines:** 20411D-LON-DC1, 20411D-LON-RTR,  
20411D-LON-CL2

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 45 minutes

# Lab Scenario

- A. Datum is a global engineering and manufacturing company with its head office in London, United Kingdom. An Information Technology (IT) office and data center located in London supports the London office and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.
  
- A. Datum is expanding its remote-access solution to the entire organization. This will require multiple VPN servers that are located at different

## Lab Scenario

points to provide connectivity for its employees. You are responsible for performing the tasks necessary to support these VPN connections.

# Lab Review

- What does a RADIUS proxy provide?
- What is a RADIUS client, and what are some examples of RADIUS clients?

# Module Review and Takeaways

- Review Question(s)
- Tools
- Best Practice

# Microsoft® Official Course



## Module 7

### Implementing Network Access Protection

**Microsoft®**

# Module Overview

- Overview of Network Access Protection
- Overview of NAP Enforcement Processes
- Configuring NAP
- Configuring IPsec Enforcement for NAP
- Monitoring and Troubleshooting NAP

# Lesson 1: Overview of Network Access Protection

- What Is Network Access Protection?
- NAP Scenarios
- NAP Enforcement Methods
- NAP Platform Architecture

# What Is Network Access Protection?

NAP can:

- Enforce health-requirement policies on client computers
- Ensure client computers are compliant with policies
- Offer remediation support for computers that do not meet health requirements

NAP cannot:

- Prevent authorized users with compliant computers from performing malicious activities on the network
- Restrict network access for computers that are running Windows versions older than Windows XP SP2, when exception rules are configured for those computers

# NAP Scenarios

NAP helps you to verify the health state of:



**Roaming laptops**



**Visiting laptops  
and devices**



**Desktop computers**

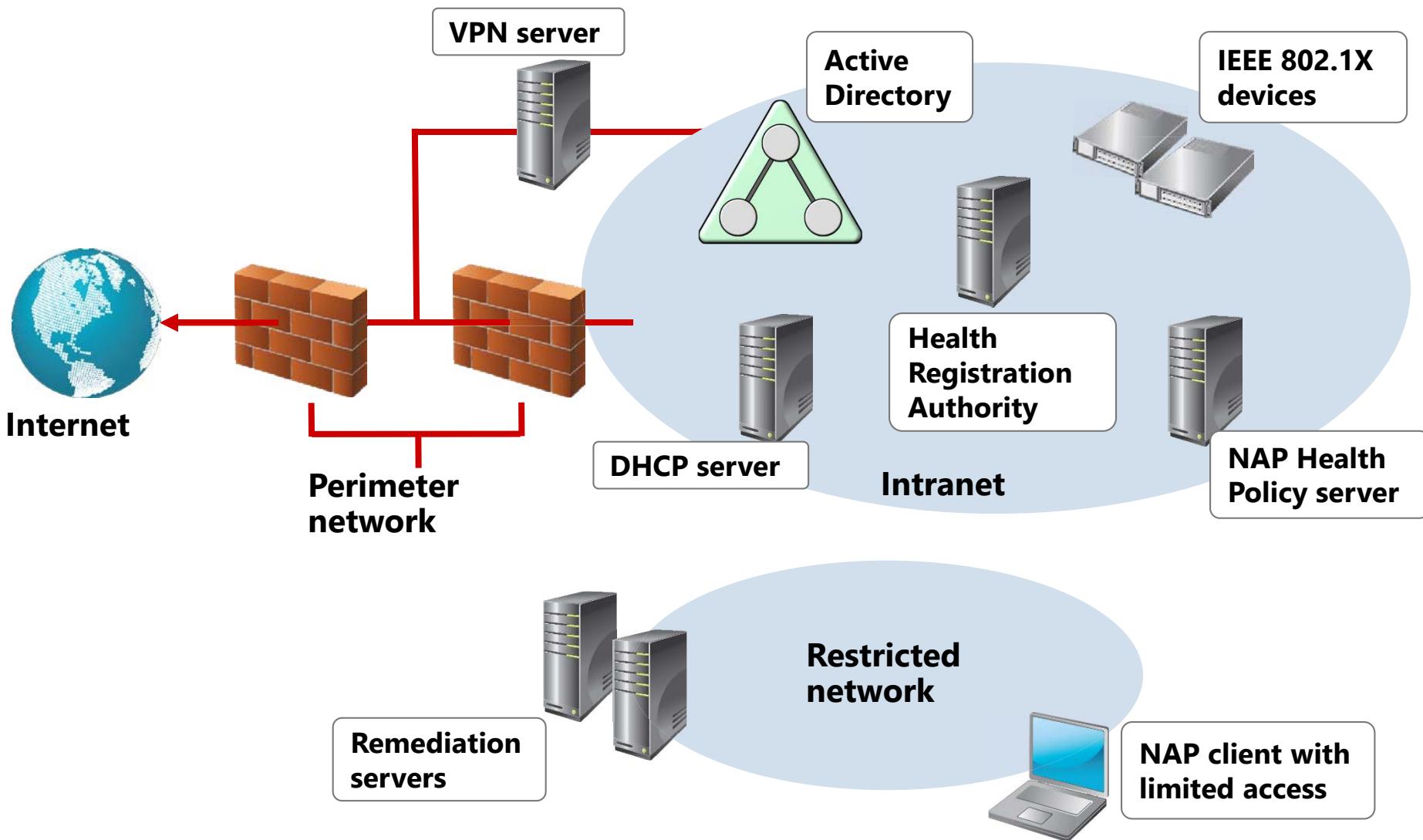


**Unmanaged home  
computers**

# NAP Enforcement Methods

| Method                                                                         | Key points                                                                                                                                                                                                                             |
|--------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| IPsec enforcement for IPsec-protected communications                           | <ul style="list-style-type: none"><li>Computer must be compliant to communicate with other compliant computers</li><li>This is the strongest NAP enforcement type, and can be applied per IP address or protocol port number</li></ul> |
| 802.1X enforcement for IEEE 802.1X-authenticated wired or wireless connections | <ul style="list-style-type: none"><li>Computer must be compliant to obtain unlimited access through an 802.1X connection (authentication switch or access point)</li></ul>                                                             |
| VPN enforcement for remote access connections                                  | <ul style="list-style-type: none"><li>Computer must be compliant to obtain unlimited access through a Remote Access Service connection</li></ul>                                                                                       |
| DirectAccess                                                                   | <ul style="list-style-type: none"><li>Computer must be compliant to obtain unlimited network access</li><li>For noncompliant computers, access is restricted to a defined group of infrastructure servers</li></ul>                    |
| DHCP enforcement for DHCP-based address configuration                          | <ul style="list-style-type: none"><li>Computer must be compliant to receive an unlimited access IPv4 address configuration from DHCP</li><li>This is the weakest form of NAP enforcement</li></ul>                                     |

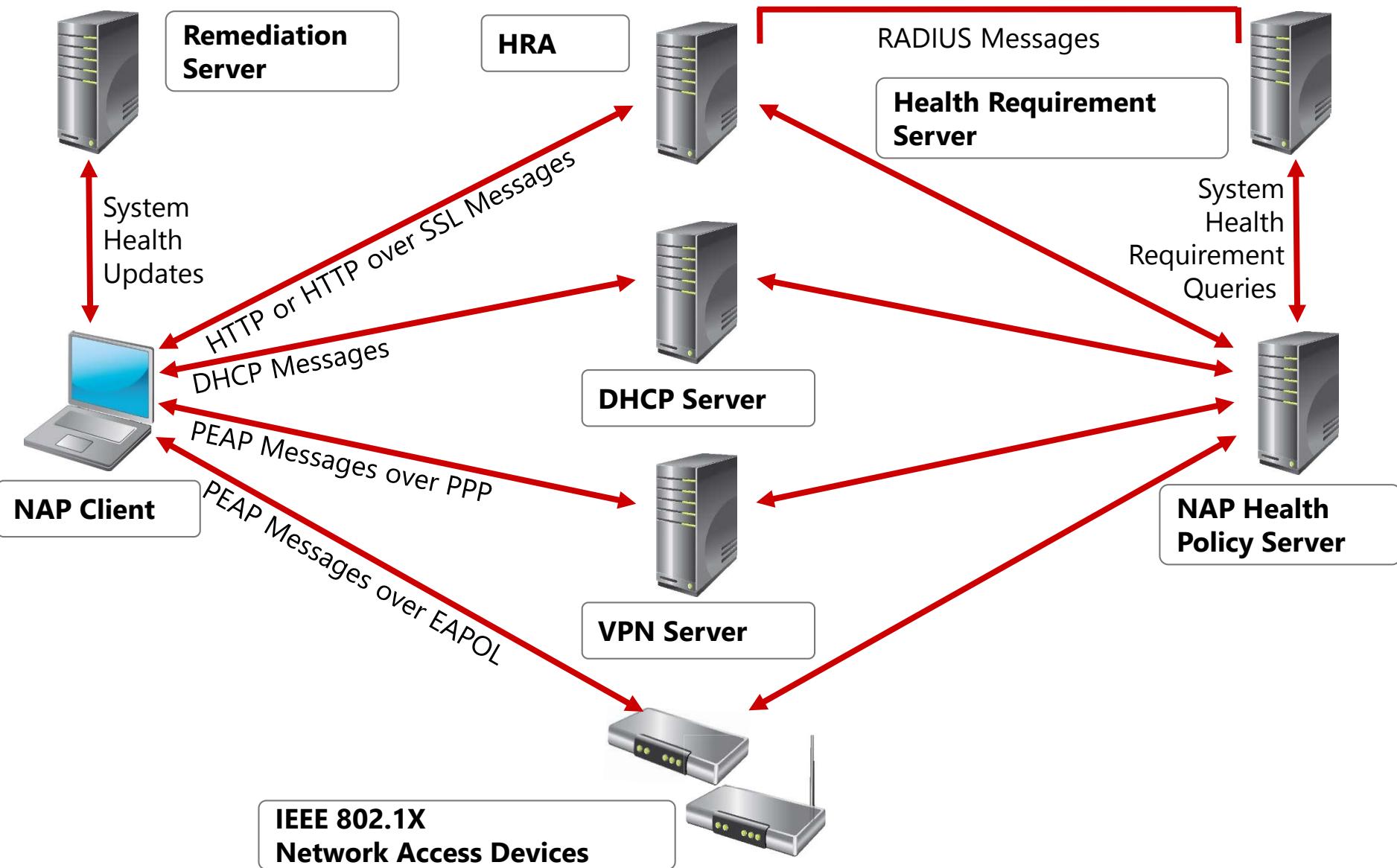
# NAP Platform Architecture



# Lesson 2: Overview of NAP Enforcement Processes

- NAP Enforcement Processes
- IPsec Enforcement
- 802.1X Enforcement
- VPN Enforcement
- DHCP Enforcement

# NAP Enforcement Processes



# IPsec Enforcement

## Key points of IPsec NAP enforcement include:

- The IPsec NAP enforcement is comprised of a health certificate server and an IPsec NAP enforcement client
  - The health-certificate server issues X.509 certificates to quarantine clients when they are verified as compliant. Certificates are then used to authenticate NAP clients when they initiate IPsec-secured communications with other NAP clients on an intranet.
- IPsec enforcement confines the communication on a network to those nodes that are considered compliant
- You can define requirements for secure communications with compliant clients on a per-IP address or a per-TCP/UDP port-number basis

# 802.1X Enforcement

Key points of 802.1X wired or wireless NAP enforcement:

- Computer must be compliant to obtain unlimited network access through an 802.1X-authenticated network connection
- Noncompliant computers are limited through a restricted-access profile that the Ethernet switch or wireless AP places on the connection
- Restricted access profiles can specify IP packet filters or a VLAN identifier that corresponds to the restricted network
- 802.1X enforcement actively monitors the health status of the connected NAP client and applies the restricted access profile to the connection if the client becomes noncompliant

# VPN Enforcement

## Key points of VPN NAP enforcement:

- Computer must be compliant to obtain unlimited network access through a remote access VPN connection
- Noncompliant computers have network access limited through a set of IP packet filters that the VPN server applies to the VPN connection
- VPN enforcement actively monitors the health status of the NAP client and then applies the IP packet filters for the restricted network to the VPN connection if the client becomes noncompliant

# DHCP Enforcement

## Key points of DHCP NAP enforcement:

- Computers must be compliant to obtain an unlimited access IPv4 address configuration from a DHCP server
- Noncompliant computers have IPv4 address configuration, allowing access to restricted network only
- DHCP enforcement actively monitors the health status of the NAP client, renewing the IPv4 address configuration for access to the restricted networks only if the client becomes noncompliant

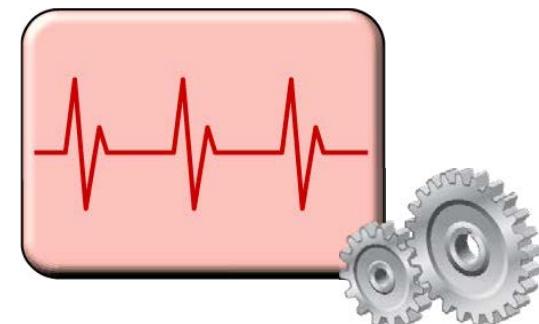
# Lesson 3: Configuring NAP

- What Are System Health Validators?
- What Is a Health Policy?
- What Are Remediation Server Groups?
- NAP Client Configuration
- Demonstration: Configuring NAP

# What Are System Health Validators?

System health validators are server software counterparts to system health agents

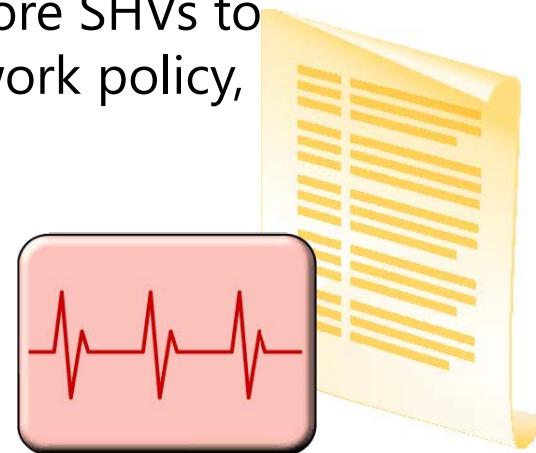
- Each SHA on the client has a corresponding SHV in NPS
- SHVs allow NPS to verify the SoH made by its corresponding SHA on the client
- SHVs contain the required configuration settings on client computers
- The Windows Security SHV corresponds to the Microsoft SHA on client computers



# What Is a Health Policy?

To make use of the Windows Security Health Validator, you must configure a health policy and assign the SHV to it

- Health policies consist of one or more SHVs and other settings, which you can use to define configuration requirements for NAP-capable computers that attempt to connect to your network
- You can define client health policies in NPS by adding one or more SHVs to the health policy
- NAP enforcement is accomplished by NPS on a per-network policy basis
- After you create a health policy by adding one or more SHVs to the policy, you can add the health policy to the network policy, and enable NAP enforcement in the policy



# What Are Remediation Server Groups?

With NAP enforcement in place, you should specify remediation server groups so the clients have access to resources that bring noncompliant NAP-capable clients into compliance

- A remediation server hosts the updates that the NAP agent can use to bring noncompliant client computers into compliance with the health policy that NPS defines
- A remediation server group is a list of servers on the restricted network that noncompliant NAP clients can access for software updates



# NAP Client Configuration

- Some NAP deployments that use Windows Security Health Validator require that you enable Security Center
- The Network Access Protection service is required when you deploy NAP to NAP-capable client computers
- You must configure the NAP enforcement clients on the NAP-capable computers
- Most NAP client settings can be configured with Group Policy Objects

# Demonstration: Configuring NAP

In this demonstration, you will see how to:

- Install the NPS server role
- Configure NPS as an NAP health policy server
- Configure health policies
- Configure network policies for compliant computers
- Configure network policies for noncompliant computers
- Configure the DHCP server role for NAP
- Configure client NAP settings
- Test NAP

# Lesson 4: Configuring IPsec Enforcement for NAP

- What Is IPsec?
- IPsec Authentication and Encryption Options
- NAP with IPsec Enforcement Components
- How IPsec Enforcement Works
- Planning IPsec Logical Networks
- Configuring the HRA Server
- Configuring the Certification Authority

# What Is IPsec?

- IPsec is a protocol suite for protecting IP communications.
- IETF standardized IPsec with a series of Request For Comments (RFCs).
- IPsec is built in to most operating systems.
- Protection of IP communications happens seamlessly and does not require configuration of applications and services for support.

# IPsec Authentication and Encryption Options

- Authentication:
  - Kerberos v5
  - Certificate authentication
  - Preshared key
- Encryption:
  - DES
  - Triple DES
  - AES
- Data integrity:
  - Same encryption standards as IPsec encryption

# NAP with IPsec Enforcement Components

You can implement NAP with IPsec enforcement by configuring the following components:

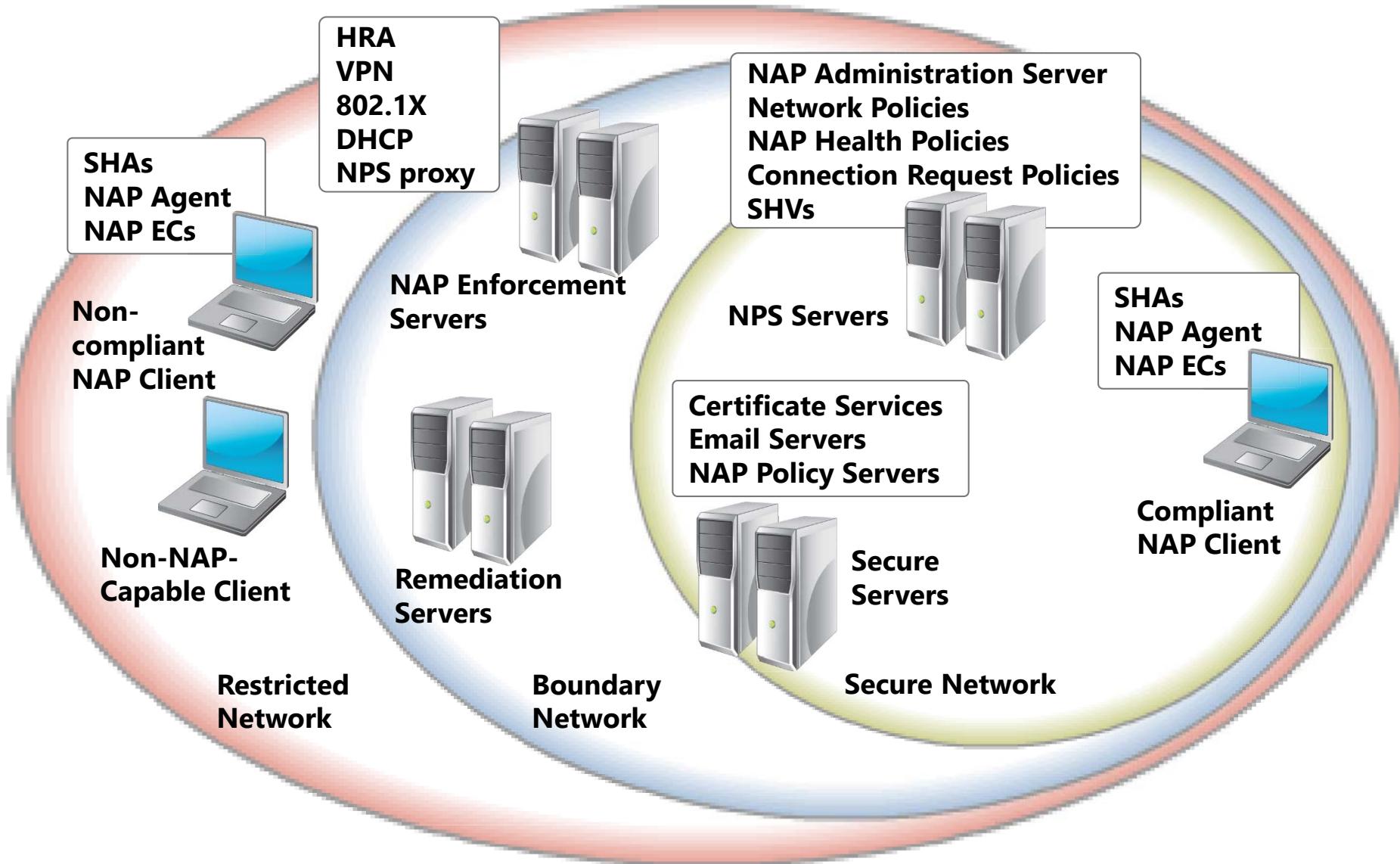
- Certification authority
- HRA server
- Computer running NPS role
- IPsec enforcement client

# How IPsec Enforcement Works

IPsec NAP enforcement includes:

- Policy validation
- NAP enforcement
- Network restriction
- Remediation
- Ongoing monitoring of compliance

# Planning IPsec Logical Networks



# Configuring the HRA Server

To support IPsec NAP enforcement, you must configure an HRA server. This process involves the following steps:

1. Configure authentication requirements
2. Configure CAs
3. Configure the request policy

# Configuring the Certification Authority

To obtain and issue certificates, the HRA must be associated with a CA. To configure the HRA to issue health certificates, complete the following tasks:

1. Choose a CA type
2. Verify CA security settings
3. Configure additional settings such as CA wait time and health certificate validity period

# Lesson 5: Monitoring and Troubleshooting NAP

- What Is NAP Tracing?
- Demonstration: Configuring NAP Tracing
- Troubleshooting NAP
- Troubleshooting NAP with Event Logs

# What Is NAP Tracing?

- NAP tracing identifies NAP events and records them to a log file based on one of the following tracing levels:
  - Basic
  - Advanced
  - Debug
- You can use tracing logs to:
  - Evaluate the health and security of your network
  - Troubleshooting and perform maintenance
- NAP tracing is disabled by default, which means that no NAP events are recorded in the trace logs

# Demonstration: Configuring NAP Tracing

In this demonstration, you will see how to:

- Configure tracing from the GUI
- Configure tracing from the command line

# Troubleshooting NAP

You can use the following netsh NAP commands to help you to troubleshoot NAP issues:

- Netsh NAP client show state
- Netsh NAP client show config
- Netsh NAP client show group

# Troubleshooting NAP with Event Logs

| Event ID | Meaning                                    |
|----------|--------------------------------------------|
| 6272     | Successful authentication has occurred     |
| 6273     | Successful authentication has not occurred |
| 6274     | A configuration problem exists             |
| 6276     | NAP client quarantined                     |
| 6277     | NAP client is on probation                 |
| 6278     | NAP client granted full access             |

# Lab: Implementing Network Access Protection

- Exercise 1: Configuring NAP Components
- Exercise 2: Configuring Virtual Private Network Access
- Exercise 3: Configuring the Client Settings to Support NAP

## Logon Information

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-RTR,  
20411D-LON-CL2

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 60 minutes

# Lab Scenario

A. Datum is a global engineering and manufacturing company with its head office in London, United Kingdom. An Information Technology (IT) office and data center in London support the head office and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

To help increase security and meet compliance requirements, A. Datum is required to extend their VPN solution to include NAP. You need to establish a way to verify and, if required, automatically bring client computers into

## Lab Scenario

compliance whenever they connect remotely by using the VPN connection. You will accomplish this goal by using NPS to create system health validation settings and network and health policies, and to configure NAP to verify and remediate client health.

# Lab Review

- The DHCP NAP enforcement method is the weakest enforcement method in Windows Server 2012. Why is it a less preferable enforcement method than other available methods?
- Could you use the remote access NAP solution alongside the IPsec NAP solution? What benefit would this scenario provide?
- Could you have used DHCP NAP enforcement for the client? Why or why not?

# Module Review and Takeaways

- Review Question(s)
- Tools
- Best Practice

# Microsoft® Official Course



## Module 8

### Implementing Remote Access

**Microsoft®**

# Module Overview

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

# Lesson 1: Overview of Remote Access

- Remote Access Options
- Managing Remote Access in Windows Server 2012
- Demonstration: Installing and Managing the Remote Access Role
- Network Address Translation
- Considerations for Deploying a PKI for Remote Access
- Configuring User Settings for Remote Access

# Remote Access Options

Remote access options in Windows Server 2012 R2 include:

- DirectAccess
- VPN
- Routing
- Web Application Proxy

# Managing Remote Access in Windows Server 2012

You can manage the Remote Access role by using:

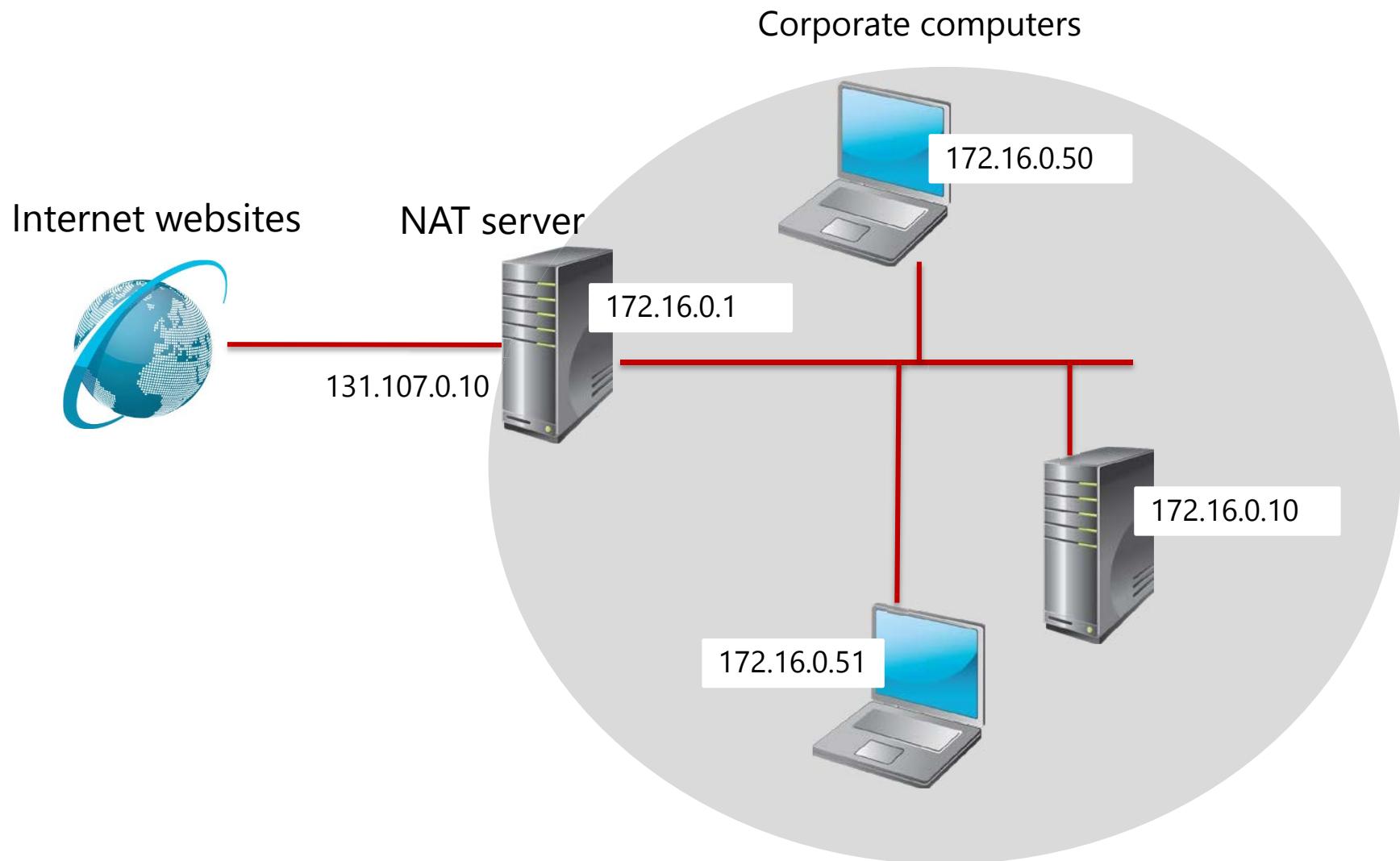
- Remote Access Management Console
- Routing and Remote Access console
- Windows PowerShell cmdlets:
  - **Set-DAServer**
  - **Get-DAServer**
  - **Set-RemoteAccess**
  - **Get-RemoteAccess**

# Demonstration: Installing and Managing the Remote Access Role

In this demonstration, you will see how to:

- Install the Remote Access role
- Manage the Remote Access role

# Network Address Translation



# Considerations for Deploying a PKI for Remote Access

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

# Configuring User Settings for Remote Access

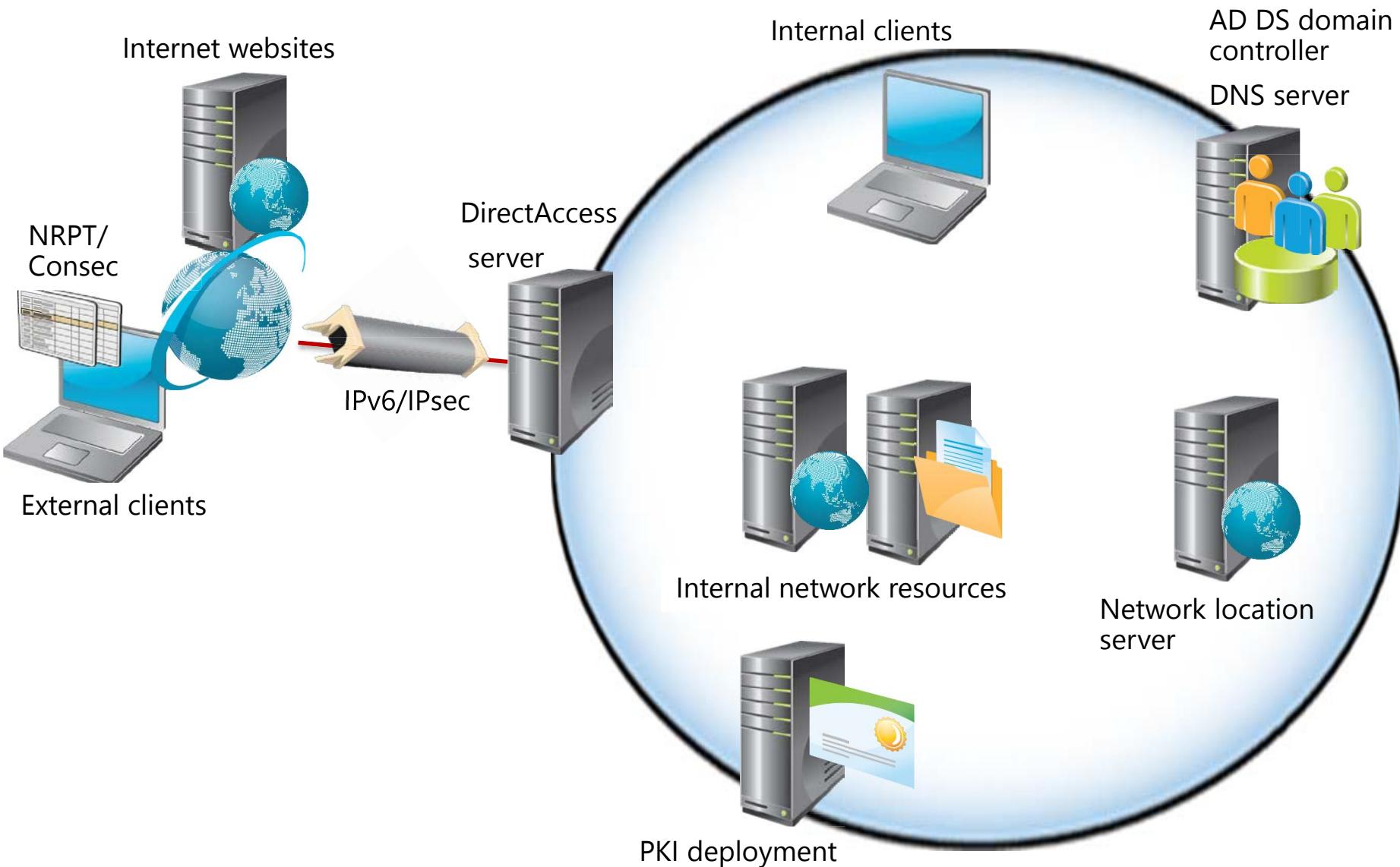
User Settings for Remote Access include:

- Network Access Permission
  - Allow access
  - Deny access
  - Control access through NPS Network Policy
- Verify Caller-ID
- Callback Options
- Assign Static IP Addresses
- Apply Static Routes

## Lesson 2: Implementing DirectAccess by Using the Getting Started Wizard

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

# DirectAccess Components



# DirectAccess Server Deployment Options

DirectAccess server deployment options include:

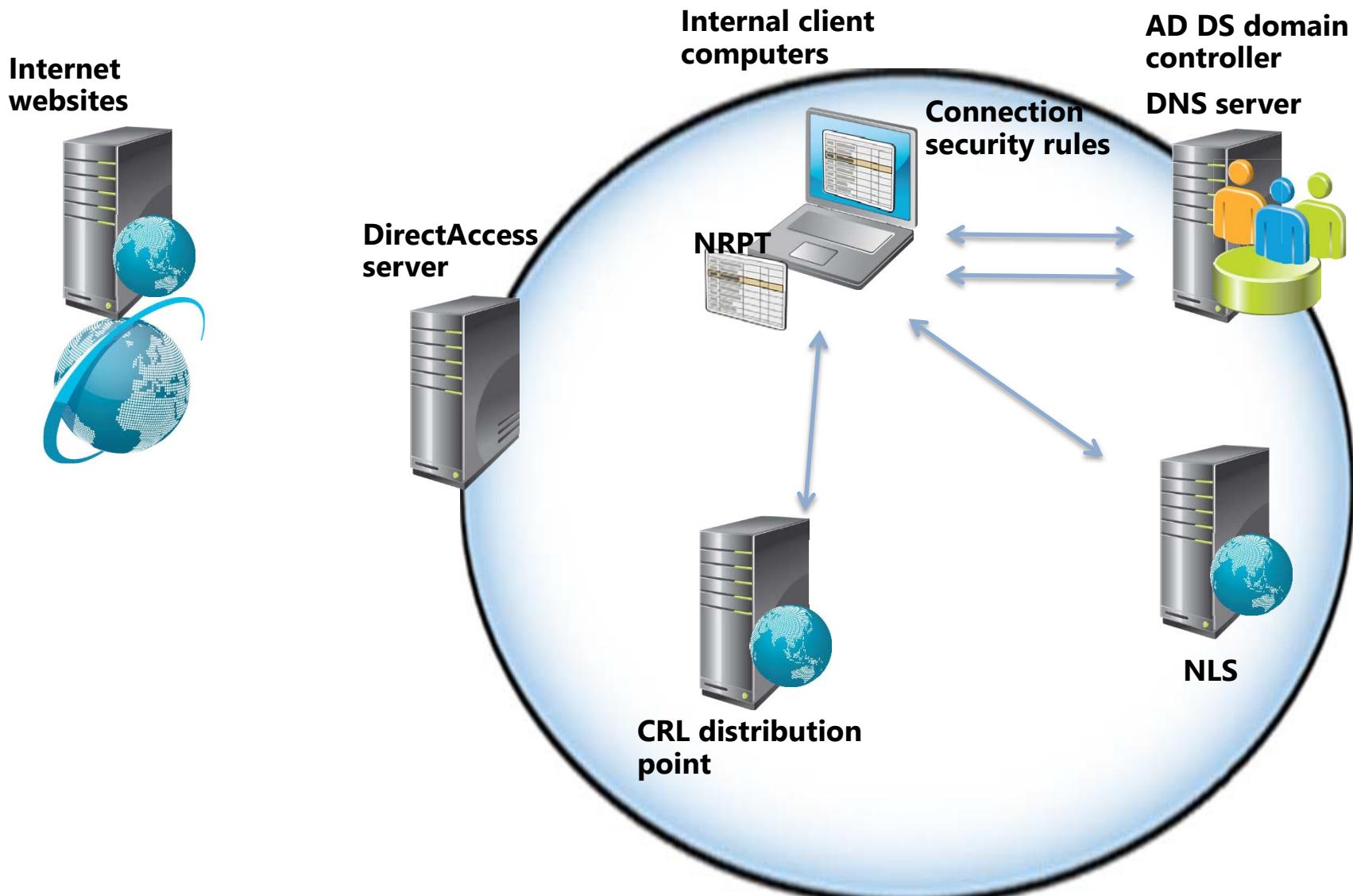
- Deploying multiple endpoints
- Supporting Multiple domains
- Deploying a server behind a NAT
- Supporting OTP and virtual smart cards
- Supporting NIC Teaming
- Provisioning Off-premise

# DirectAccess Tunneling Protocol Options

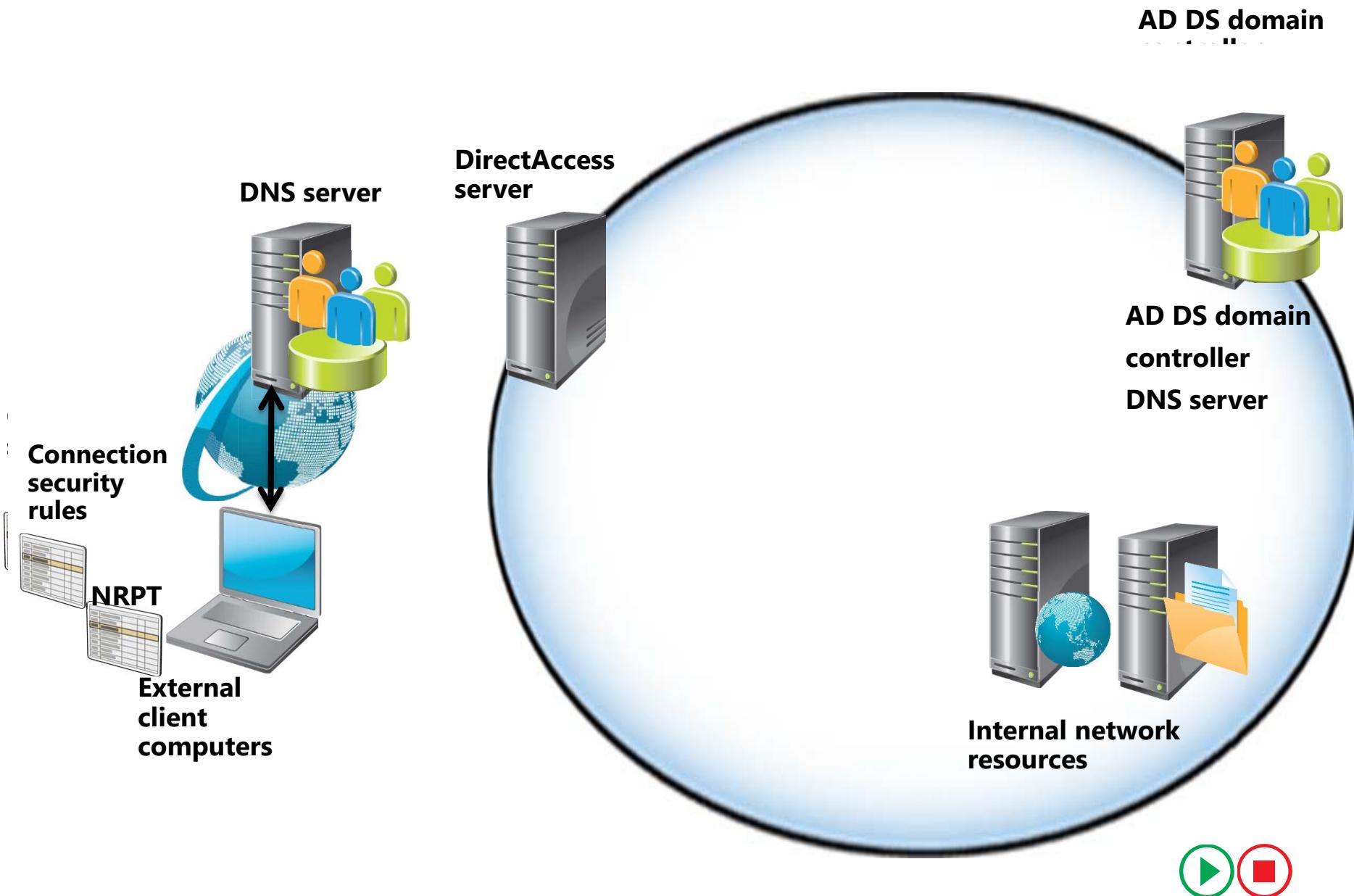
DirectAccess tunneling protocols include:

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

# How DirectAccess Works for Internal Clients



# How DirectAccess Works for External Clients



# Demonstration: Running the Getting Started Wizard

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

# Getting Started Wizard Configuration Changes

Changes made by the Getting Started Wizard include:

- GPO settings
  - DirectAccess Server Settings GPO
  - DirectAccess Client Settings GPO
- Remote clients
- Remote access servers
- Infrastructure servers

# Demonstration: Identifying the Getting Started Wizard Settings

In this demonstration, you will see how to identify changes made by the DirectAccess Getting Started Wizard

# Limitations of DirectAccess Deployments When Using the Getting Started Wizard

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

# Lab A: Implementing DirectAccess by Using the Getting Started Wizard

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

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

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

**Virtual Machine(s):** 20411D-INET1

**User Name:** Administrator

**Password:** Pa\$\$w0rd

**Estimated Time:** 30 minutes

# Lab Scenario

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

## Lab Scenario

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

# Lab Review

- Why did you create the DA\_Clients group?
- How will you configure IPv6 addresses for client computers running the Windows® 8 operating system to use DirectAccess?

# Lesson 3: Implementing and Managing an Advanced DirectAccess Infrastructure

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

# Overview of the Advanced DirectAccess Options

Advanced DirectAccess configuration options include:

- Scalable and customized PKI infrastructure
- Customized network configuration options
- Scalable and highly-available server deployment
- Customized monitoring and troubleshooting

# Integrating a PKI with DirectAccess

Configuring PKI for DirectAccess includes the following steps:

1. Add and configure the CA server role if not already present
2. Create the certificate template
3. Create a CRL distribution point and publish the CRL list
4. Distribute the computer certificates

# Implementing Client Certificates for DirectAccess

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

Steps for deploying certificates for client computers:

1. Create a GPO and link it to the organizational unit that contains the DirectAccess clients
2. Configure the GPO for automatic certificate request for the computer account
3. Apply the GPO
4. Verify that the certificates are issued

# Internal Network Configuration Options

Planning for internal network configuration requires you to plan for:

- DirectAccess server location (Edge, perimeter network, or internal network)
- IP address assignment
- Firewall configuration
- Active Directory
- Client deployment

# Configuring Advanced DNS Settings

DirectAccess uses DNS for resolving:

- Network location server
- IP-HTTPS
- CRL distribution point
- ISATAP
- Connectivity verifiers

You can configure NRPT by using Group Policy with the following settings:

- DNS suffixes
- CRL distribution point
- Split-brain DNS

# Implementing Network Location Servers

Network location server can be located on:

- A DirectAccess server
- Another server with IIS installed

Requirements for network location server configuration:

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

# Implementing Management Servers

Management servers in DirectAccess are:

- Domain controllers
- SCCM servers

Management servers are detected by DirectAccess:

- Automatically
- Manually if modified

Management server requirements:

- Must be accessible for the infrastructure tunnel
- Must fully support IPv6

# Demonstration: Modifying the DirectAccess Infrastructure

In this demonstration, you will see how to:

- Modify the DirectAccess infrastructure deployed by using the Getting Started Wizard
- Apply advanced configuration settings

# How to Monitor DirectAccess Connectivity

Remote Access Management Console monitoring components:

- Dashboard
- Operations Status
- Remote Access Client Status
- Remote Access Reporting

# How to Troubleshoot DirectAccess Connectivity

You can troubleshoot DirectAccess connectivity by using:

- A troubleshooting methodology
- Command-line tools
- GUI tools

# Demonstration: Monitoring and Troubleshooting DirectAccess Connectivity

In this demonstration, you will see how to monitor and troubleshoot DirectAccess connectivity

# Lab B: Deploying an Advanced DirectAccess Solution

- Exercise 1: Preparing the Environment for DirectAccess
- Exercise 2: Implementing the Advanced DirectAccess Infrastructure
- Exercise 3: Validating the DirectAccess Deployment Logon Information

**Virtual Machine(s):** 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-RTR, 20411D-LON-CL1, 20411D-LON-CL3

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

**Virtual Machine(s):** 20411D-INET1

**User Name:** Administrator

**Password:** Pa\$\$w0rd

**Estimated Time:** 60 minutes

## Lab Scenario

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

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

# Lab Review

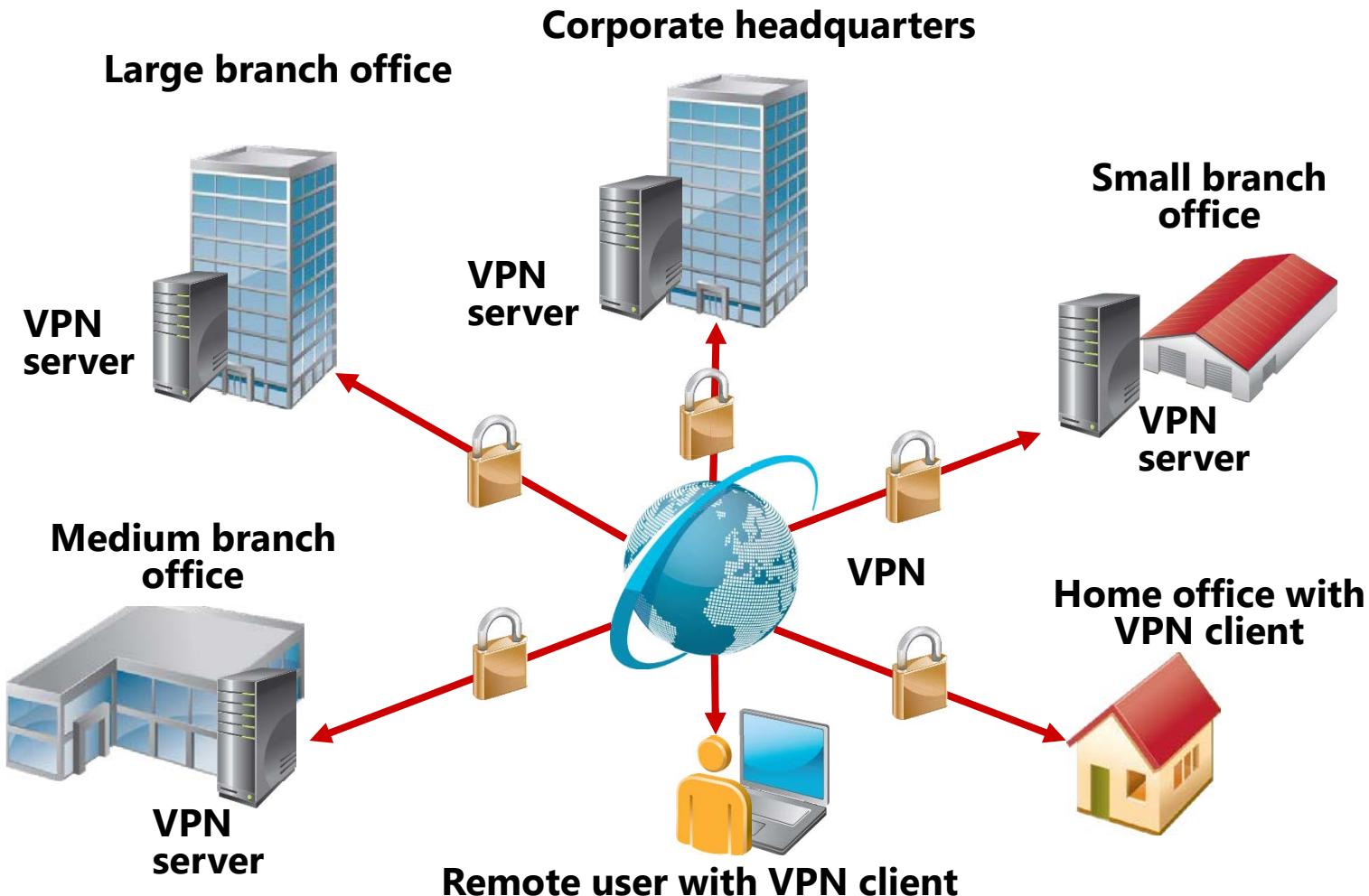
- Why did you make the CRL available on the edge server?
- Why did you install a certificate on the client computer?

# Lesson 4: Implementing VPN

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

# VPN Scenarios

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



# VPN Tunneling Protocol Options

Windows Server 2012 supports four VPN tunneling protocols

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

# VPN Authentication Options

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

# What Is VPN Reconnect?

VPN Reconnect maintains connectivity across network outages

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

# VPN Configuration by Using the Getting Started Wizard

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

VPN server configuration requirements include:

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

# Options for Modifying the VPN Configuration

You may need to perform additional steps to help secure the installation of the VPN solution:

- Configure static packet filters
- Configure services and ports
- Adjust logging levels for routing protocols
- Configure number of available VPN ports
- Create a Connection Manager profile for users
- Add AD CS
- Increase remote access security
- Increase VPN security
- Consider implementing VPN Reconnect

# Demonstration: Configuring VPN

In this demonstration, you will see how to:

- Review the default VPN configuration
- Verify certificate requirements for IKEv2 and SSTP
- Configure the remote access server

# What Is the Connection Manager Administration Kit?

The CMAK:

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

# Demonstration: How to Create a Connection Profile

In this demonstration, you will see how to:

- Install the CMACK feature
- Create a connection profile
- Examine the profile

# Lab C: Implementing VPN

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

## Logon Information

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

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 45 minutes

## Lab Scenario

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

# Lab Review

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

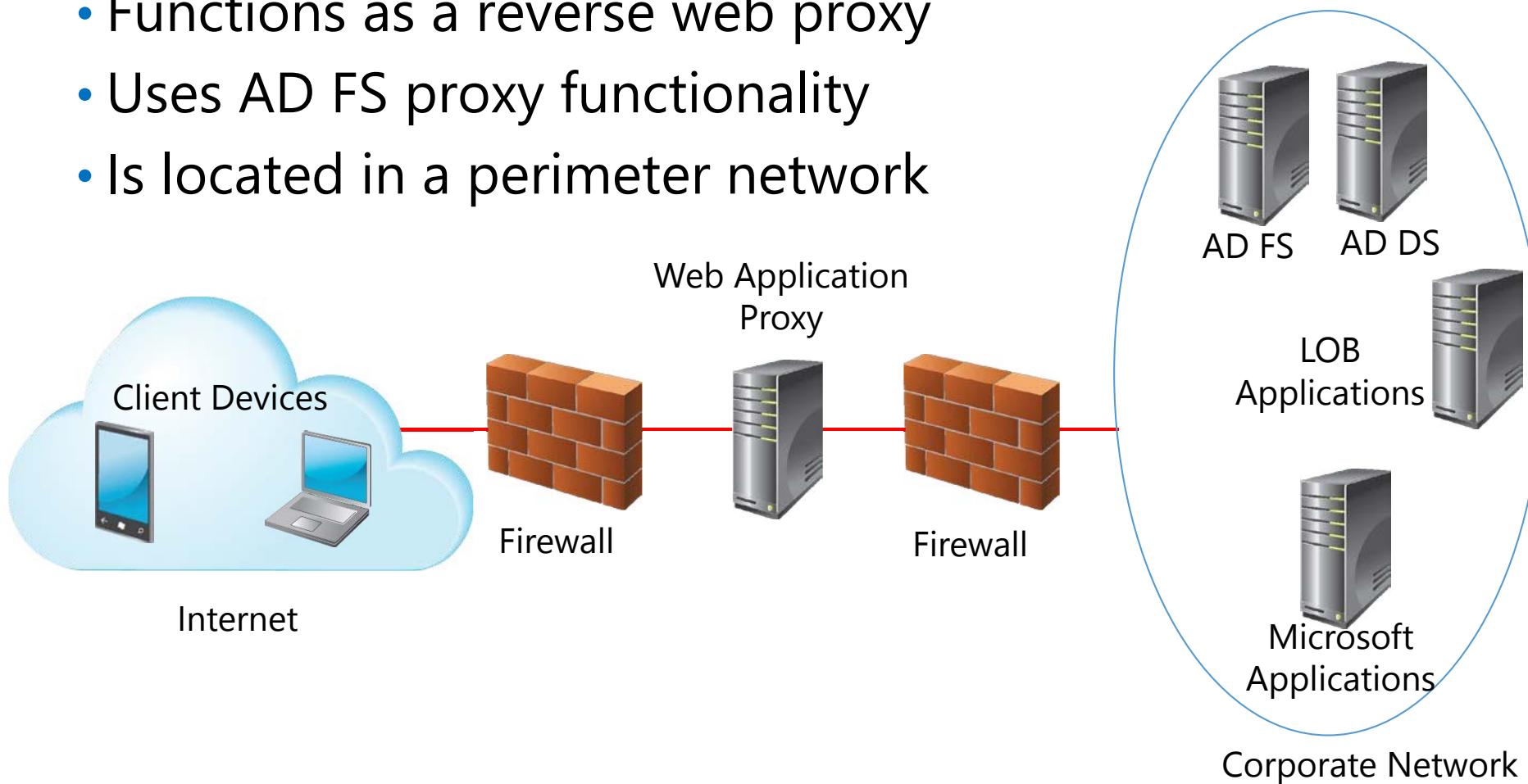
# Lesson 5: Implementing Web Application Proxy

- What Is Web Application Proxy?
- What is AD FS
- Authentication Options for Web Application Proxy
- Publishing Applications with Web Application Proxy
- Demonstration: Publishing a Secure Website

# What Is Web Application Proxy?

## Web Application Proxy:

- Is introduced in Windows Server 2012 R2
- Functions as a reverse web proxy
- Uses AD FS proxy functionality
- Is located in a perimeter network



# What is AD FS

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

AD FS includes the following features:

- Web SSO
- Web services interoperability
- Support for different types of clients
- Extensible architecture
- Enhanced security

# Authentication Options for Web Application Proxy

User authentication:

- AD FS pre-authentication
- Pass-through pre-authentication

AD FS benefits:

- Workplace join
- SSO
- Multifactor authentication
- Multifactor access control

# Publishing Applications with Web Application Proxy

- Configuring Web Application Proxy settings
  - AD FS server name
  - AD FS administrator credentials
  - AD FS certificate
- Publishing Web Application
  - Type of preauthentication, for example Pass-through
  - Details of the application that will be published
  - The external URL of the application, for example,  
<https://lon-svr1.adatum.com/>
  - A certificate whose subject name covers the external URL, for example lon-svr1.adatum.com
  - URL of the back end server

# Demonstration: Publishing a Secure Website

In this demonstration, you will see how to:

- Install the Web Application Proxy role service
- Configure access to an internal web site
- Disable DirectAccess on a client computer
- Verify access to the internal web site from the client computer

# Lab D: Implementing Web Application Proxy

- Exercise 1: Implementing Web Application Proxy
- Exercise 2: Validating the Web Application Proxy Deployment

## Logon Information

**Virtual Machine(s):** 20411D-LON-DC1, 20411D-LON-SVR1,  
20411D-LON-SVR4, 20411D-LON-RTR, 20411D-LON-CL1

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

**Virtual Machine(s):** 20411D-INET1

**User Name:** Administrator

**Password:** Pa\$\$w0rd

**Estimated Time:** 30 minutes

# Lab Scenario

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

# Lab Review

- Where should we deploy the Web Application Proxy server?
- What is required for a client to be able to access a published application?

# Module Review and Takeaways

- Review Question(s)
- Tools
- Best Practices
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



Module 9

Optimizing File Services

**Microsoft®**

# Module Overview

- Overview of FSRM
- Using FSRM to Manage Quotas, File Screens, and Storage Reports
- Implementing Classification and File Management Tasks
- Overview of DFS
- Configuring DFS Namespaces
- Configuring and Troubleshooting DFS Replication

# Lesson 1: Overview of FSRM

- Understanding Capacity Management Challenges
- What Is FSRM?
- Demonstration: How to Install and Configure FSRM

# Understanding Capacity Management Challenges

Capacity management challenges include:

- Determining existing storage use
- Establishing and enforcing storage use with policies
- Anticipating future requirements

Address capacity management challenges by:

- Analyzing how storage is used
- Defining storage resource management policies
- Implementing policies to manage storage growth
- Implementing a system for reporting and monitoring

# What Is FSRM?

FSRM enables the following functionality:

- Storage quota management
- File screening management
- Storage reports management
- Classification management
- File management tasks

# Demonstration: How to Install and Configure FSRM

In this demonstration, you will see how to install and configure FSRM

## Lesson 2: Using FSRM to Manage Quotas, File Screens, and Storage Reports

- What Is Quota Management?
- What Are Quota Templates?
- Monitoring Quota Usage
- What Is File Screening Management?
- What Are File Groups?
- What Are a File Screen Templates and File Screen Exceptions?
- What Are Storage Reports?
- What Is a Report Task?
- Demonstration: Using FSRM to Manage Quotas and File Screens, and to Generate On-Demand Storage Reports

# What Is Quota Management?

Use quota management to limit disk space usage and provide notifications when thresholds are reached

Quota notifications can do any of the following:

- Send email notifications
- Log an event in Event Viewer
- Run a command or script
- Generate storage reports

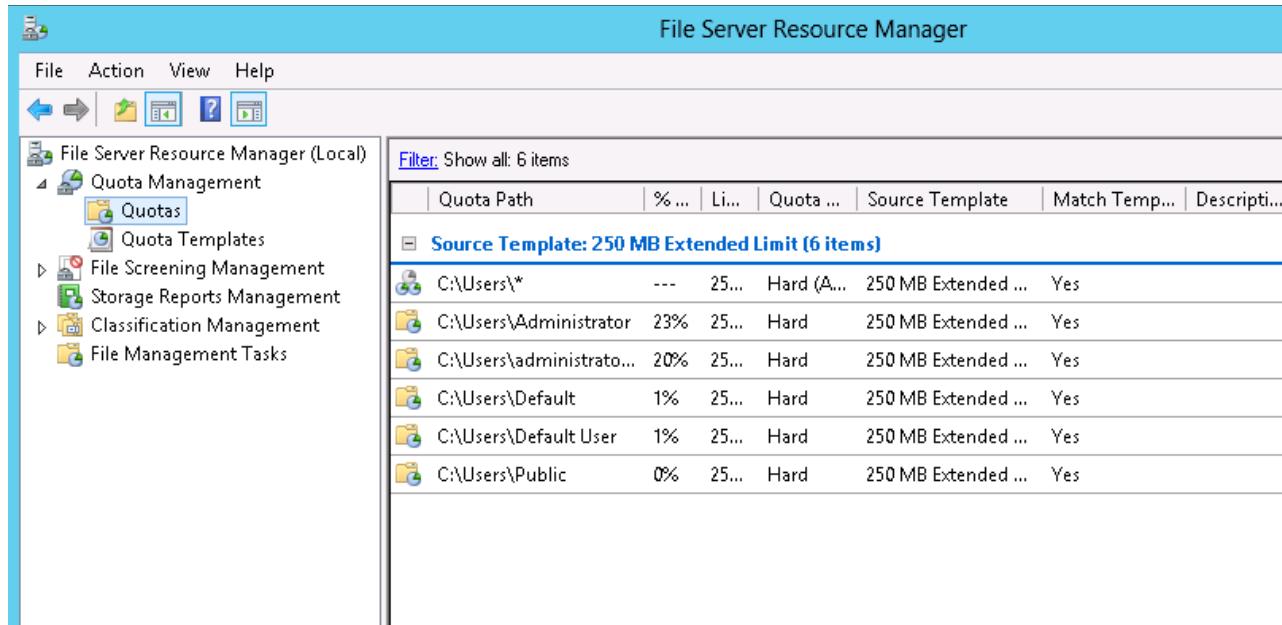
# What Are Quota Templates?

A quota template defines:

- A space limit
- The type of quota (hard or soft)
- A set of notifications to be generated when the quota limit is approached

FSRM provides a set of default quota templates in the Quota Templates node

# Monitoring Quota Usage



In File Server Resource Manager you can monitor quota usage by:

- Viewing quota information in the FSRM console
- Generating a quota usage report
- Creating soft quotas
- Using the **Get-FSRMQuota** Windows PowerShell cmdlet

# What Is File Screening Management?

File screen management provides a method for controlling the types of files that can be saved on file servers

File screen management consists of:

- Creating file screens
- Defining file screen templates
- Creating file screen exceptions
- Creating file groups

# What Are File Groups?

File groups are used to define a namespace for a file screen, file screen exception, or storage report

A file group consists of a set of file name patterns that are grouped into:

- Files to include
- Files to exclude

# What Are File Screen Templates and File Screen Exceptions?

## File screen templates:

- Provide a definition for newly created file screens
- Enable control over file screens created from templates

File screen exceptions enable you to override file screens for a specific location or file group

# What Are Storage Reports?

Storage reports provide information about file usage on a file server

Types of storage reports include:

- Duplicate Files
- File Screening Audit
- Files by File Group, Owner, or Property
- Folders by Property
- Large Files
- Least- and most- recently accessed files
- Quota Usage

# What Is a Report Task?

You can schedule reports by creating a Report Task, which specifies:

- The volumes and folders to report on
- Which reports to generate
- Which parameters to use
- How often to generate the reports
- Which file formats to save the reports in

# Demonstration: Using FSRM to Manage Quotas and File Screens, and to Generate On-Demand Storage Reports

In this demonstration, you will see how to:

- Create a quota
- Test a quota
- Create a file screen
- Test a file screen
- Generate a storage report

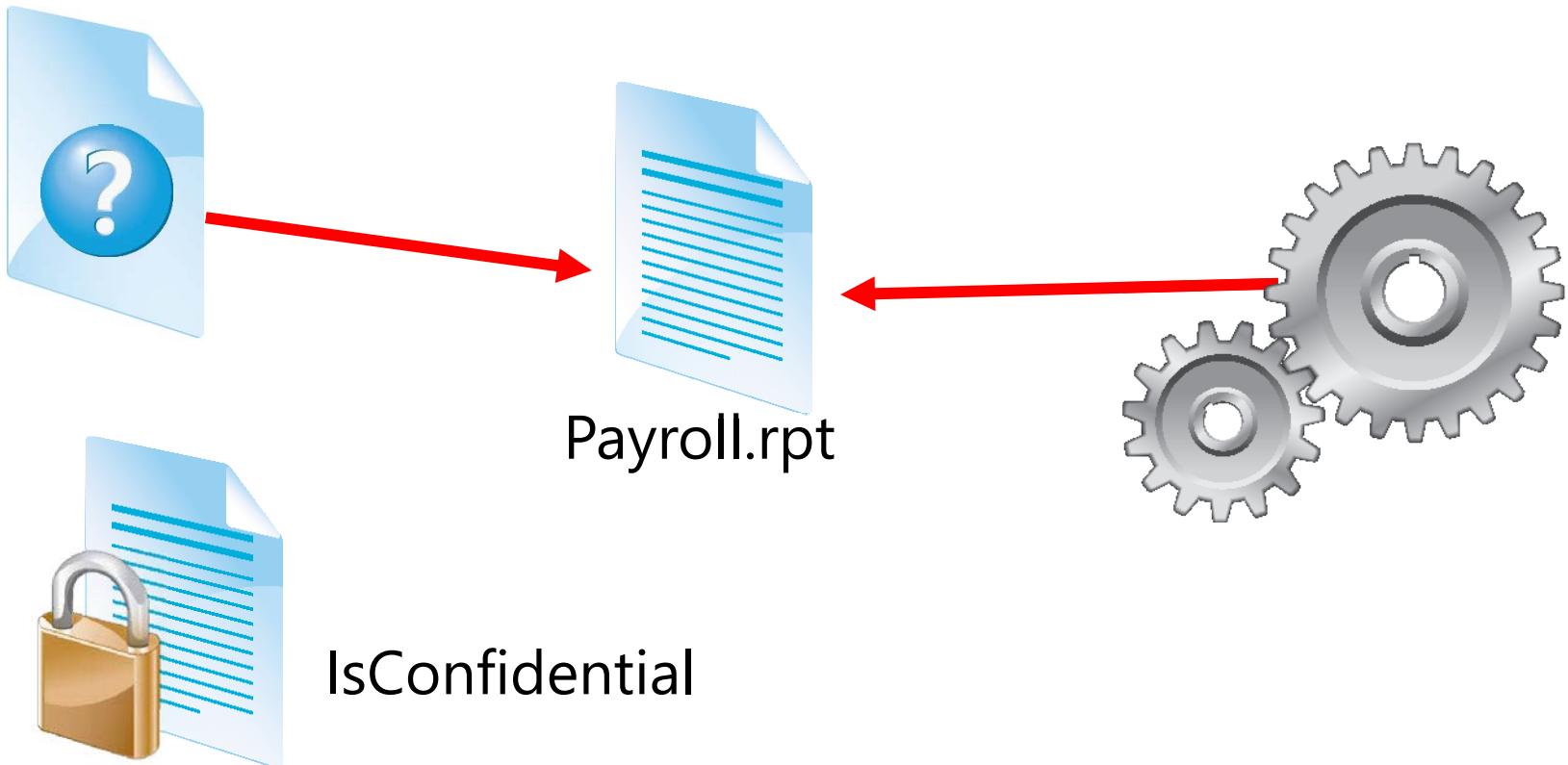
# Lesson 3: Implementing Classification and File Management Tasks

- What Is File Classification?
- What Are Classification Rules?
- Demonstration: Configuring File Classification
- What Are File Management Tasks?
- Demonstration: How to Configure File Management Tasks

# What Is File Classification?

Classification management allows you to use an automated mechanism to create and assign classification properties to files

## Classification Rule



# What Are Classification Rules?

The file classification infrastructure scans files automatically, and then classifies them according to the contents of a file

When planning for file classification implementation, do the following:

- Identify classifications
- Determine classification method
- Determine schedule
- Perform review

# Demonstration: Configuring File Classification

In this demonstration you will see how to:

- Create a classification property
- Create a classification rule

# What Are File Management Tasks?

File Management Tasks enable administrators to perform operations on files based on assigned Classification Properties

File Management Tasks can:

- Move files to other locations
- Archive expired files
- Delete unwanted files
- Rename files

# Demonstration: How to Configure File Management Tasks

In this demonstration, you will see how to:

- Create a file management task
- Configure a file management task to expire documents

# Lab A: Configuring Quotas and File Screening Using File Server Resource Manager

- Exercise 1: Configuring File Server Resource Manager Quotas
- Exercise 2: Configuring File Screening and Storage Reports

## Logon Information

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 30 minutes

# Lab Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, England. An IT office and data center in London support the London location and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

Each network client within the Adatum domain is provided with a server-based home folder that is used for storing personal documents or files that are works-in-progress. It has come to your

## Lab Scenario

attention that home folders are becoming quite large, and may contain file types such as MP3 files that are not approved under corporate policy. You decide to implement FSRM quotas and file screening to help address this issue.

# Lesson 4: Overview of DFS

- What Is DFS?
- What Is a DFS Namespace?
- What Is DFS Replication?
- How DFS Namespace and DFS Replication Works
- What Is Data Deduplication?
- DFS Scenarios
- Demonstration: How to Install the DFS Role

# What Is DFS?

DFS incorporates technologies that provide fault-tolerant access to geographically dispersed files

DFS technologies include:

- DFS namespace
- DFS Replication

# What Is a DFS Namespace?

A DFS namespace can be configured as either a:

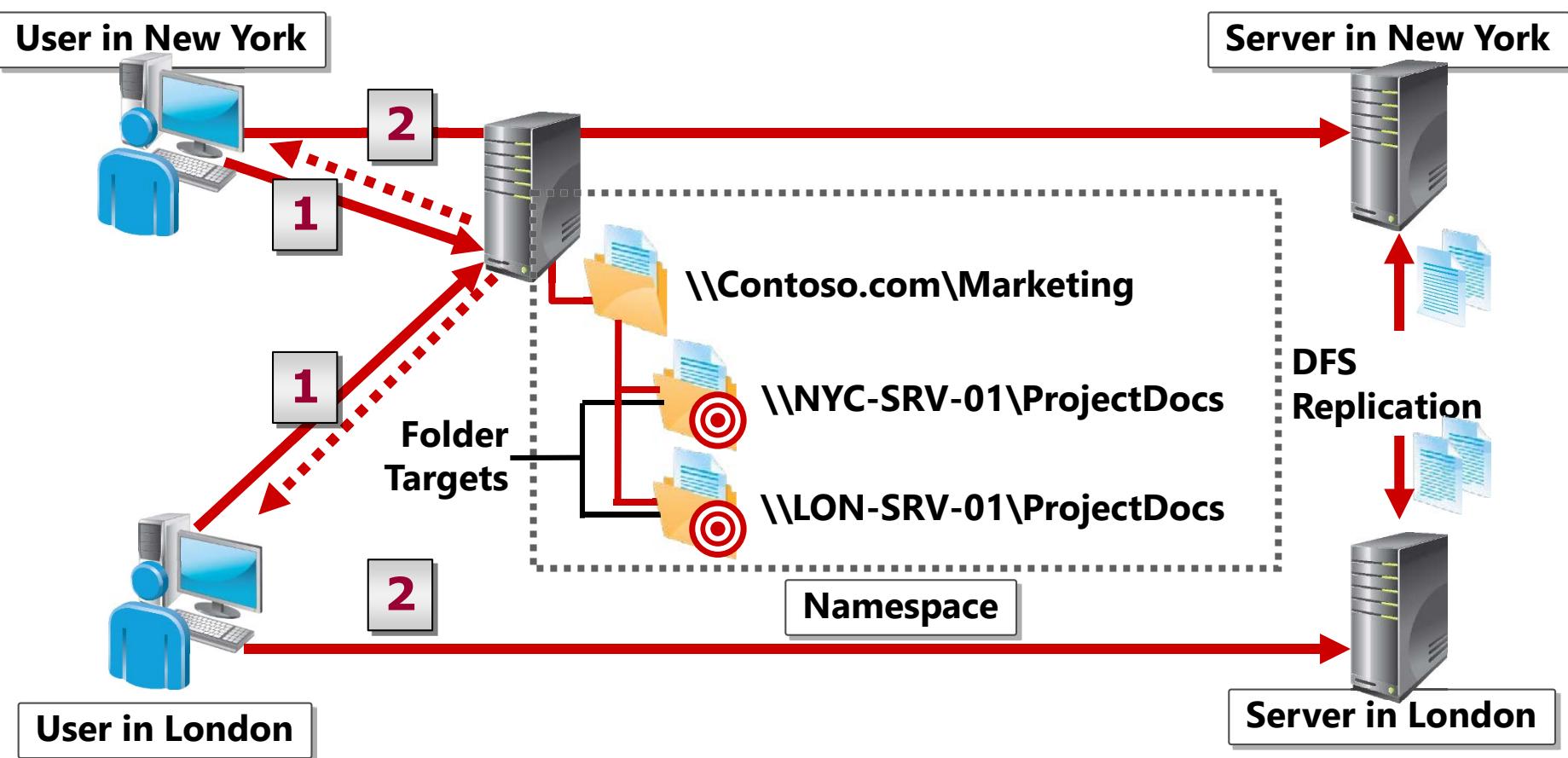
- Domain-based namespace
  - Namespace is stored in AD DS
  - Increased redundancy for namespace hosting
- Standalone namespace
  - Namespace is stored on the local server
  - Only redundant if stored on a failover cluster

# What Is DFS Replication?

Characteristics of DFS Replication include:

- Uses RDC
- Uses a staging folder to stage a file before sending or receiving it
- Detects changes on the volume by monitoring the USN journal
- Uses a vector version exchange protocol
- Recovers from failure

# How DFS Namespace and DFS Replication Works



1. User types: \\contoso.com\marketing  
Client computers contact a namespace server, and receive a referral
2. Client computers cache the referral, and then contact the first server in the referral

# What Is Data Deduplication?

Data deduplication optimizes volume storage by redirecting redundant data to a single storage point

Data deduplication provides:

- Capacity optimization
- Scale and performance
- Reliability data integrity
- Bandwidth efficiency
- Simple optimization management

# DFS Scenarios

| Scenario                            | Example                                                                                                                                                                                                                                                                                                                         |
|-------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Sharing files across branch offices | <p>Branch Office</p>  <p>Hub Site</p>                                                                                                                       |
| Data collection                     | <p>Branch Office</p>  <p>Hub Site</p>                                                                                                                       |
| Data distribution                   | <p>Hub Office</p>  <p>Branch Office 1</p>  <p>Branch Office 2</p>  |

# Demonstration: How to Install the DFS Role

In this demonstration, you will see how to install the DFS Role

# Lesson 5: Configuring DFS Namespaces

- Deploying Namespaces to Publish Content
- Permissions Required to Create and Manage a Namespace
- Demonstration: How to Create Namespaces
- Optimizing a Namespace

# Deploying Namespaces to Publish Content

To configure a namespace for publishing content:

1. Create a namespace
2. Create a folder in the namespace
3. Add folder targets
4. Set the ordering method for targets in referrals

Optional tasks:

- Set target priority to override referral ordering
- Enable client fallback
- Replicate folder contents using DFS Replication
- Delegate namespace administration

# Permissions Required to Create and Manage a Namespace

| Task                                                             | Default group                                      |
|------------------------------------------------------------------|----------------------------------------------------|
| Create a domain-based namespace                                  | Domain Admins                                      |
| Add a namespace server to a domain-based namespace               | Domain Admins                                      |
| Manage a domain-based namespace                                  | Local Administrators on each namespace server      |
| Create a standalone namespace                                    | Local Administrators group on the namespace server |
| Manage a standalone namespace                                    | Local Administrators group on the namespace server |
| Create a replication group or enable DFS replication on a folder | Domain Admins                                      |

# Demonstration: How to Create Namespaces

In this demonstration, you will see how to:

- Create a new namespace
- Create a new folder and folder target

# Optimizing a Namespace

Methods for optimizing a namespace include:

- Renaming or moving a folder
- Disabling referrals to a folder
- Specifying referral cache duration
- Configuring namespace polling

# Lesson 6: Configuring and Troubleshooting DFS Replication

- New Features For Windows Server 2012 R2
- Replication Groups and Replicated Folders
- Initial Replication Process
- Demonstration: How to Configure DFS Replication
- Troubleshooting DFS

# New Features For Windows Server 2012 R2

## New or updated functionality in Windows Server 2012 R2:

- Windows PowerShell module for DFS
- Database cloning for initial synchronization
- Database corruption recovery
- Cross-file RDC disable
- File staging tuning
- Preserved file restoration
- Unexpected shutdown database recovery improvements
- Membership disabling improvements

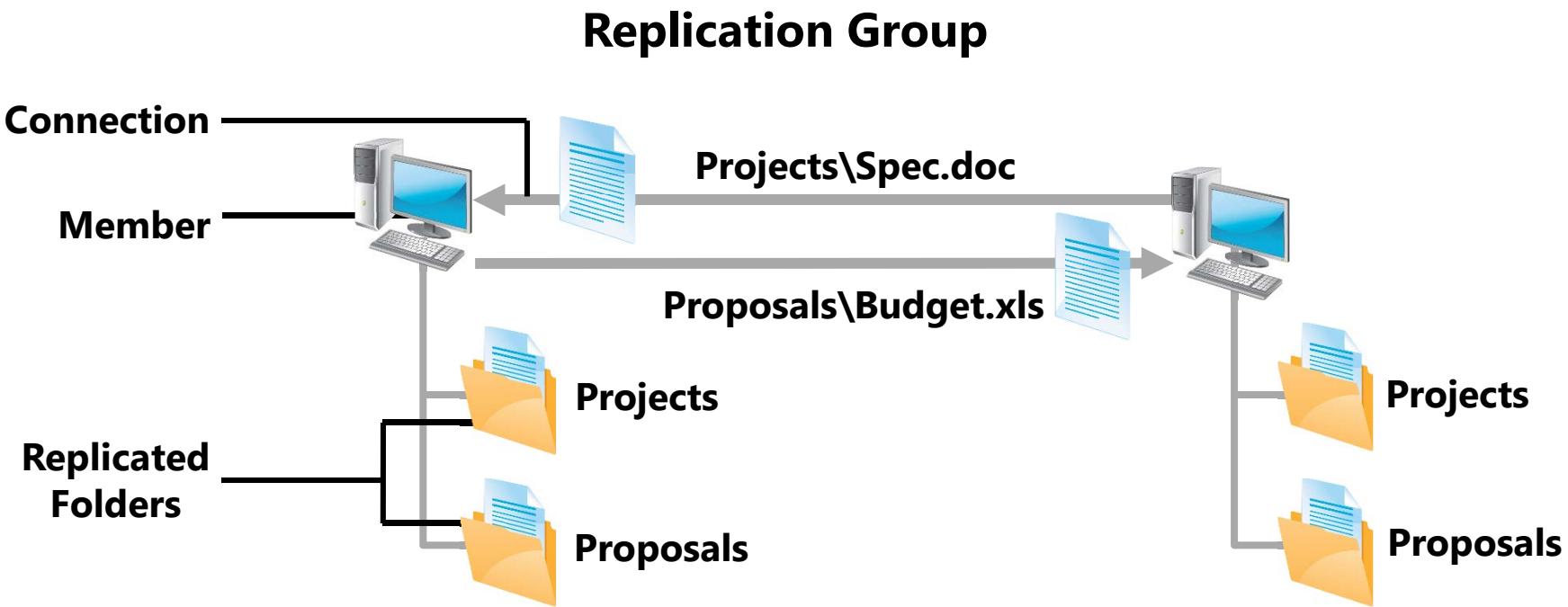
# Replication Groups and Replicated Folders

## Replication Group:

- A set of servers that participate in replicating one or more replicated folders

## Replicated Folder

- A folder that is kept replicated on each server



# Initial Replication Process

The initial replication process consists of:

1. Replication of DFS Replication settings
  2. Primary member starts replication
  3. Files are moved to DfsrPrivate\PreExisting
  4. Files are compared and replicated
  5. Primary member designation is removed
- New Windows PowerShell cmdlets allow the replication database to be cloned and seeded on new DFS members to reduce the impact of initial synchronization on the network.
  - File staging tuning allows you to control what minimum size of files will be staged before replication to optimize replication

# Demonstration: How to Configure DFS Replication

In this demonstration, you will see how to:

- Create a new folder target for replication
- Create a new replication group

# Troubleshooting DFS

| Tool               | Used to                                                           |
|--------------------|-------------------------------------------------------------------|
| Health Report      | Report replication statistics and general health of the topology  |
| Propagation Test   | Generate a test file to verify replication                        |
| Propagation Report | Report on the propagation test and provide replication statistics |
| Verify Topology    | Report on the current status of the members of the topology       |
| Dfsrdiag.exe       | Monitor replication state of the DFS Replication service          |

# Lab B: Implementing Distributed File System

- Exercise 1: Installing the DFS Role Service
- Exercise 2: Configuring a DFS Namespace
- Exercise 3: Configuring DFS Replication

## Logon Information

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1,  
20411D-LON-SVR4

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 45 minutes

## Lab Scenario

A. Datum Corporation has deployed a new branch office. This office has a single server. To support the requirements of a branch staff, you must configure DFS. To avoid performing backups remotely, a departmental file share in the branch office will be replicated back to the head office for centralized backup, and branch data files will be replicated to the branch server to provide quicker access.

# Module Review and Takeaways

- Review Question(s)
- Best Practice
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 10

Configuring Encryption and  
Advanced Auditing

**Microsoft®**

# Module Overview

- Encrypting Drives by Using BitLocker
- Encrypting Files by Using EFS
- Configuring Advanced Auditing

# Lesson 1: Encrypting Drives by Using BitLocker

- What is BitLocker?
- How BitLocker Works
- BitLocker Requirements
- Configuring BitLocker
- Using Group Policy to Manage BitLocker
- Demonstration: Configuring BitLocker
- Recovering Drives Encrypted with BitLocker

# What is BitLocker?

BitLocker is full drive encryption that has the following characteristics:

- Can be used to encrypt an entire hard drive or only the used parts of a hard drive
- Can be combined with EFS
- Protects the integrity of the Windows boot process
- Some features of BitLocker are only usable when a TPM is available on the computer

# How BitLocker Works

- Advanced Encryption Standard (AES)
  - 128-bit or 256-bit encryption key
- Automated deployment with Windows PowerShell for computers already in production
- New operating system deployments can use BitLocker before the operating system files are written to the volume
- BitLocker encrypts entire hard drive:
  - Only used space encrypted (fastest)
  - Entire hard drive encrypted (most secure for existing computers)

# BitLocker Requirements

- BitLocker is supported on
  - Windows Vista and newer Windows client operating systems
  - Windows Server 2008 and newer Windows server operating systems
- Windows XP supports the ability to read and copy data from a portable hard drive encrypted with BitLocker To Go
- A TPM offers additional features such as
  - System integrity verification
  - Multifactor authentication

# Configuring BitLocker

- Enable TPM on the computer (optional)
- Add the BitLocker Drive Encryption feature on the server
- Configure Group Policy or local Group Policy for BitLocker settings which is required if the computer does not have a TPM chip
- Turn on BitLocker on the desired volume(s)

# Using Group Policy to Manage BitLocker

- Group Policy offers approximately 40 settings to manage and configure BitLocker.
- Some common policy settings are:
  - Choose drive encryption method and cipher strength.
  - Deny write access to fixed data drives/removable drives not protected by BitLocker.
  - Configure use of passwords for fixed data drives/removable data drives.
  - Require additional authentication at startup.
  - Allow network unlock at startup.

# Demonstration: Configuring BitLocker

In this demonstration, you will see how to

- Edit Group Policy to configure BitLocker
- Add the BitLocker Drive Encryption feature
- Turn on BitLocker and then validate that BitLocker is encrypting the data volume

# Recovering Drives Encrypted with BitLocker

- The best way to ensure recoverability is to plan properly before deploying BitLocker
- Recovery options include:
  - Using the recovery key file to obtain the key
  - Obtaining the recovery key from AD DS
  - Using a Data Recovery Agent
  - Using the original BitLocker password

# Lesson 2: Encrypting Files by Using EFS

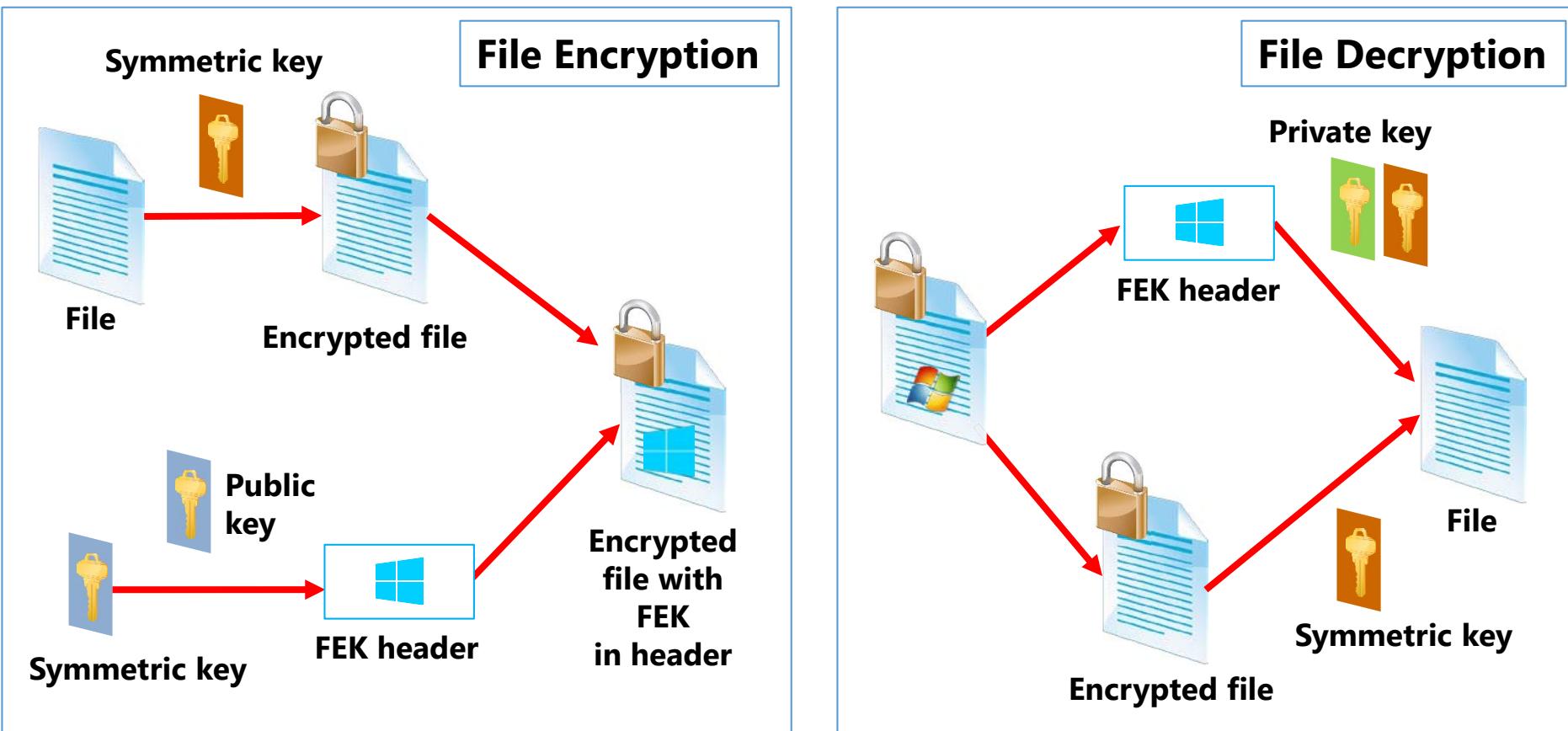
- What Is EFS?
- How EFS Works
- Recovering EFS–Encrypted Files
- Demonstration: Encrypting a File by Using EFS
- EFS vs. BitLocker

# What Is EFS?

- EFS can encrypt files that are stored on an NTFS-formatted partition
- EFS encryption acts as an additional layer of security
- EFS can be used with no preconfiguration

# How EFS Works

- Symmetric encryption is used to protect the data
- Public key encryption is used to protect the symmetric key



# Recovering EFS–Encrypted Files

- To ensure that you can recover EFS-encrypted files, you should:
  - Back up user certificates
  - Configure a recovery agent
- You must back up the recovery key to:
  - Secure against system failure
  - Make the recovery key portable

# Demonstration: Encrypting a File by Using EFS

In this demonstration, you will see how to:

- Verify that a computer account supports EFS on a network share
- Use EFS to encrypt a file on a network share
- View the certificate used for encryption
- Test access to an encrypted file

# EFS vs. BitLocker

- Shared Computers
  - *Use EFS*: offers folder encryption and ensures that users on shared computers cannot view other users' data.
- Portable Computers
  - *Use BitLocker*: protects the entire hard drive which ensures that data is protected no matter where it is stored on the hard drive.
- High Security Environment
  - *Combine EFS and BitLocker*: provides more data protection than just EFS or BitLocker alone.

# Lesson 3: Configuring Advanced Auditing

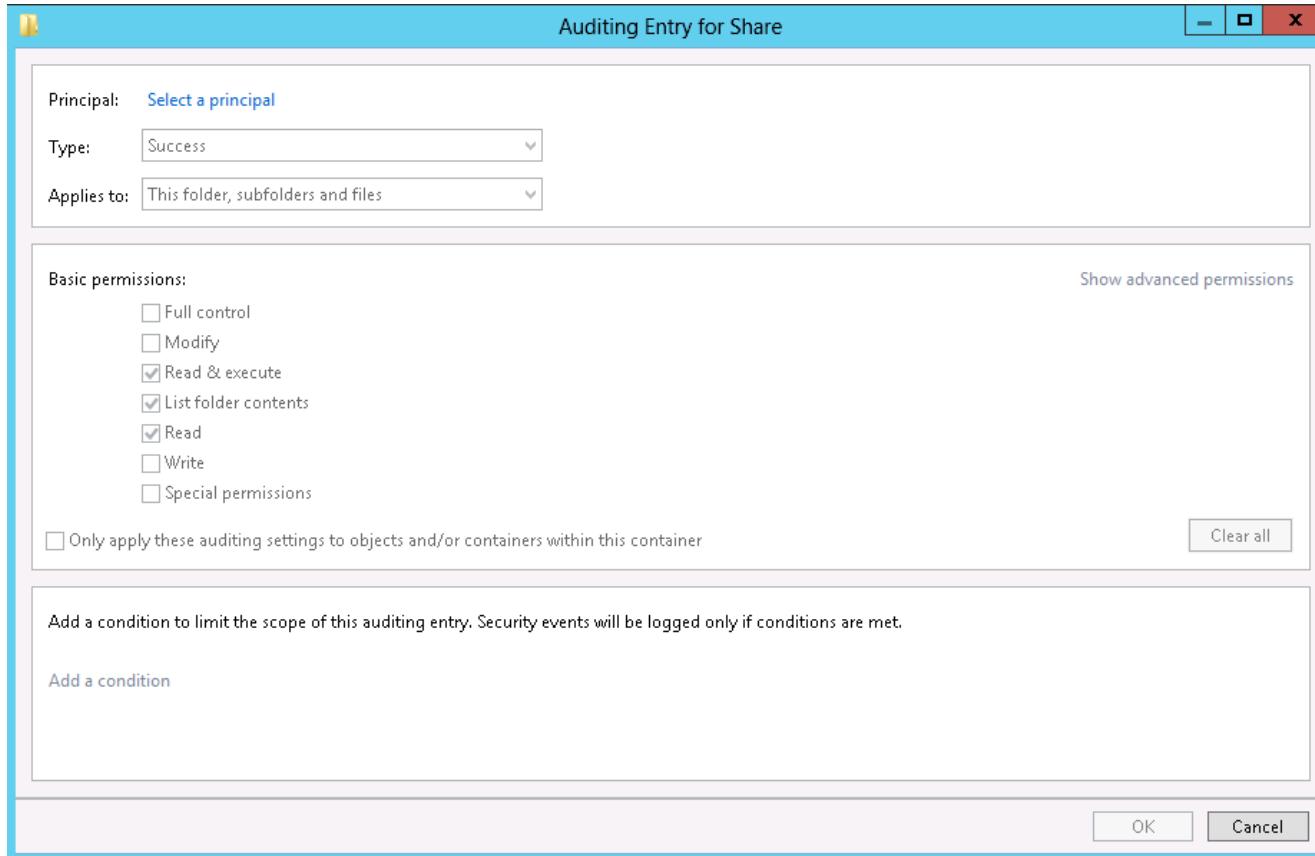
- Overview of Audit Policies
- Specifying Auditing Settings on a File or Folder
- Enabling Audit Policy
- Evaluating Events in the Security Log
- Advanced Audit Policies
- Demonstration: Configuring Advanced Auditing

# Overview of Audit Policies

- Audit events by activity category, such as:
  - Access to NTFS/ReFS files and folders
  - Account or object changes in Active Directory Domain Services
  - Logon
  - Assignment of use of user rights
- By default, domain controllers audit successful events for most categories
- Goal: Align audit policies with corporate security policies:
  - Over-auditing: logs are too big to find important events
  - Under-auditing: important events are not logged

# Specifying Auditing Settings on a File or Folder

- Auditing settings for a file or folder are specified by modifying the SACL:



- Full control will record all associated events
- Recording audit events will not occur until the audit policy is enabled

# Enabling Audit Policy

To enable audit policy by configuring Audit Policy settings in a GPO:

- Enable the appropriate settings in the GPO
- Apply the GPO to the AD DS container where your servers are located

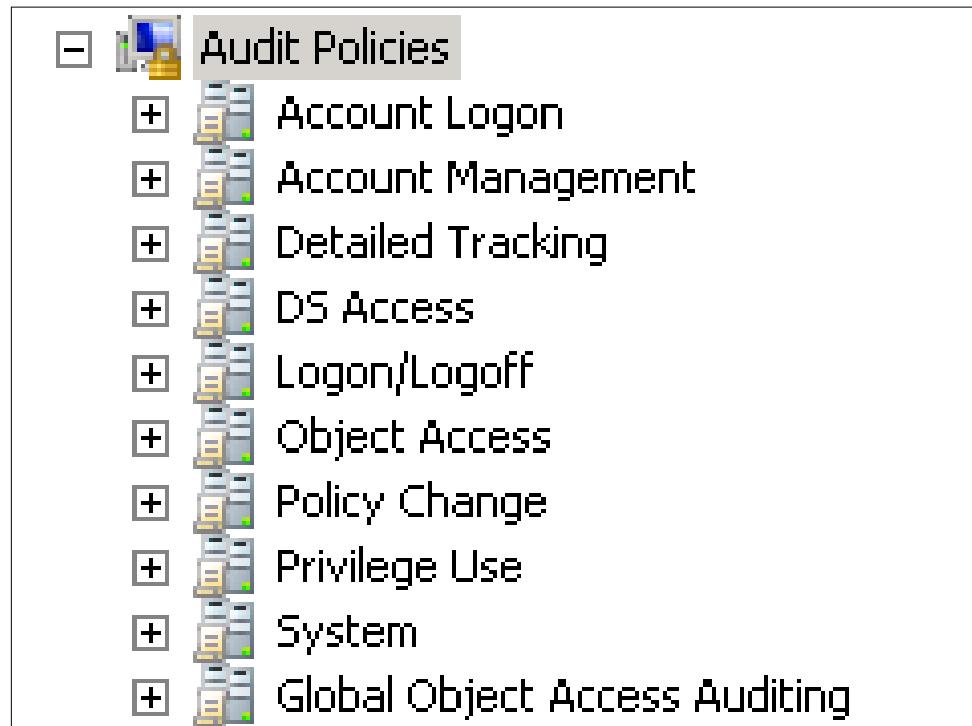
# Evaluating Events in the Security Log

View the audit events in the Details field in Security log, and filter to reduce the number of events to examine:

| Keywords      | Date and Time        | Source                | Event ID | Task Category |
|---------------|----------------------|-----------------------|----------|---------------|
| Audit Success | 9/20/2013 3:37:44 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:37:43 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:36:43 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:36:04 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:35:47 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:34:44 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:34:23 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:34:10 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:33:43 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:32:53 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:32:43 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:32:42 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:31:43 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:31:02 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:30:43 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:29:43 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:29:21 PM | Microsoft Windows ... | 5140     | File Share    |
| Audit Success | 9/20/2013 3:28:43 PM | Microsoft Windows ... | 5140     | File Share    |

# Advanced Audit Policies

Windows Server 2012 and Windows Server 2008 R2 provide an additional set of Advanced Audit Policies to configure



# Demonstration: Configuring Advanced Auditing

In this demonstration, you will see how to create and edit a GPO for audit policy configuration

# Lab: Configuring Encryption and Advanced Auditing

- Exercise 1: Using BitLocker® Drive Encryption to Secure Data Drives
- Exercise 2: Encrypting and Recovering Files
- Exercise 3: Configuring Advanced Auditing

## Logon Information

Virtual machines: 20411D-LON-DC1,  
20411D-LON-CL1, and 20411D-LON-SVR1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 40 minutes

# Lab Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, England. An IT office and data center are located in London to support the London location and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure.

You have been asked to configure the Windows Server 2012 environment to protect sensitive files, and to ensure that access to files on the network is audited appropriately. You also have been asked to configure auditing for the new server.

# Lab Review

- In Exercise 3, Task 1, why were you asked to generate a new data recovery agent certificate by using the AdatumCA CA?
- What are the benefits of placing servers in an OU and then applying audit policies to that OU?
- What is the reason for applying audit policies across the entire organization?

# Module Review and Takeaways

- Review Question(s)
- Tools

# Microsoft® Official Course



## Module 11

### Deploying and Maintaining Server Images

# Module Overview

- Overview of Windows Deployment Services
- Managing Images
- Implementing Deployment with Windows Deployment Services
- Administering Windows Deployment Services

# Lesson 1: Overview of Windows Deployment Services

- What Is Windows Deployment Services?
- Windows Deployment Services Components
- Why Use Windows Deployment Services?
- Discussion: How to Use Windows Deployment Services
- Discussion: How to Use Windows Deployment Services

# What Is Windows Deployment Services?

Windows Deployment Services is a server role that is provided with Windows Server 2012

- Windows Deployment Services:
  - Enables you to perform network-based installations
  - Simplifies the deployment process
  - Supports deployment to computers with no operating system
  - Uses existing technologies, such as Windows PE, .wim, .vhdx and .vhdx files, and image-based deployment

# Windows Deployment Services Components

- Transport Server
  - Multicast engine
  - Windows PowerShell cmdlets for session management
- Deployment Server
  - PXE server
  - Image store
  - Windows Deployment Services client
  - TFTP server

# Why Use Windows Deployment Services?

Consider the following scenarios:

- In a small network consisting of a single server and approximately 25 Windows XP computers, you want to expedite the upgrade process of the client computers to Windows 8.1
- A medium-sized organization wants to deploy multiple servers in branch offices that are geographically dispersed. It would be time-consuming and expensive to send experienced IT staff to each location to deploy the servers

# Discussion: How to Use Windows Deployment Services

The A. Datum Corporation IT staff is about to deploy Windows Server 2012 to various branch offices. The following information has been provided to the IT staff by management:

- The configuration of the various branch office servers is expected to be fairly consistent.
- There is no requirement to upgrade settings from existing servers, as these are new branch offices with no current IT infrastructure in place.
- Automation of the deployment process is important, as there are many servers to deploy

**How should you  
configure Windows  
Deployment Services?**



# Discussion: How to Use Windows Deployment Services

A. Datum Corporation wants to deploy several new servers in their head offices which will have Windows Server 2012 installed on them.

Following are the requirements provided to the IT staff:

- Configuration of the various servers is expected to vary slightly.
- The two basic server configurations are: full server, and Server Core installation
- Managing network traffic is critical, as the network is near capacity.

**How should you  
configure Windows  
Deployment Services?**



# Lesson 2: Managing Images

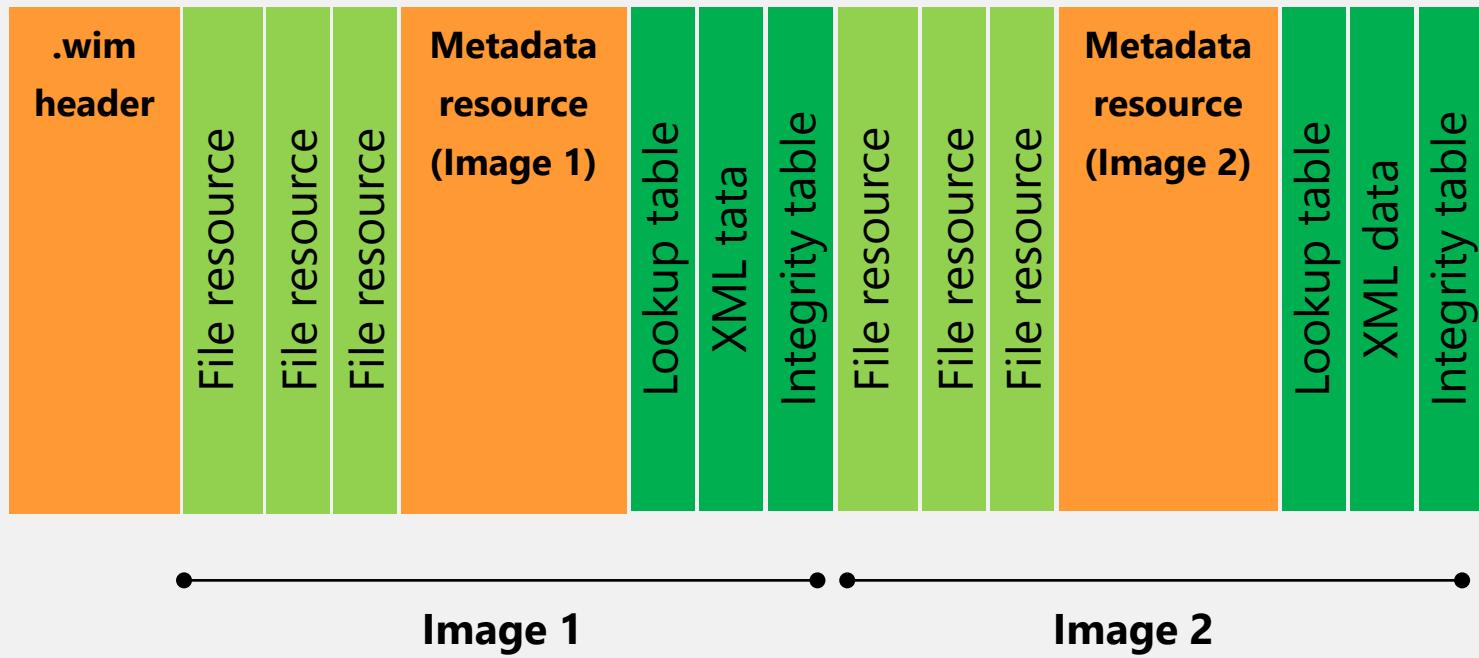
- The Role of Images in Windows Deployment Services
- Windows ADK Tools for Image Management
- Image Types
- Creating an Install Image
- Managing and Maintaining Images
- Demonstration: Using DISM to Configure an Image

# The Role of Images in Windows Deployment Services

Three types of image files in Windows Deployment Services are used as boot or install images

- wim, .vhd, and .vhdx

## Windows Imaging (WIM) File



# Windows ADK Tools for Image Management

Windows ADK includes the following tools

- Windows SIM
- Windows PE
- USMT
- DISM
- Windows PowerShell module for DISM

# Image Types

- Thin Image
  - Contains only the operating system and possibly a few agents, such as Configuration Manager 2012 agent
- Thick Image
  - Contains every application required by an end-user
- Hybrid Image
  - Contains some of the applications required by most users

# Creating an Install Image

- The process of creating an install image can be summarized as follows:
  - Create a capture image
  - Install Windows on a reference computer
  - Customize settings on the reference computer
  - Generalize the reference computer
  - Capture the reference image

# Managing and Maintaining Images

Use DISM to manage and maintain images including:

- Apply updates, drivers, and language packages
- Add, remove, or enumerate packages and drivers
- Enable or disable Windows features
- Configure locale settings
- Upgrade an image to a different edition of Windows

# Demonstration: Using DISM to Configure an Image

- In this demonstration, you will see how to:
  - Mount a .wim image
  - List the features enabled on an image
  - Enable a feature on an image

# Lesson 3: Implementing Deployment with Windows Deployment Services

- Understanding Windows Deployment Services Components
- Installing and Configuring Windows Deployment Services
- Managing Deployments with Windows Deployment Services

# Understanding Windows Deployment Services Components

- Windows Deployment Services prerequisites include:
  - AD DS
  - DHCP
  - DNS
  - NTFS/ReFS volume
- Use Windows Assessment and Deployment Kit to create answer files for automated deployment

# Installing and Configuring Windows Deployment Services

Install and configure Windows Deployment Services by:

- Installing the Windows Deployment Services server role
  - Install the Deployment Server or Transport Server role service
  - Perform post-installation configuration of Windows Deployment Services by:
    - Specifying an image store location
    - Configuring the DHCP server options, if required
    - Configuring PXE server configuration

# Managing Deployments with Windows Deployment Services

- To service client computers with Windows Deployment Services, you must:
  - Configure boot settings
  - Configure install settings
  - Configure transmission settings
  - Configure drivers

# Lesson 4: Administering Windows Deployment Services

- Common Administration Tasks
- Demonstration: How to Administer Images
- Automating Deployments
- Demonstration: How to Configure Multicast Transmission

# Common Administration Tasks

- Tasks
  - Configure DHCP
  - Create and service images
  - Manage the boot menu
  - Prestage client computers
  - Automate deployment
  - Configure transmission
- Tools
  - Windows Deployment Services console
  - WDSUtil.exe
  - Dism.exe
  - Sysprep.exe
  - ImageX.exe
  - Windows SIM

# Demonstration: How to Administer Images

In this demonstration, you will see how to:

- Install and configure the Windows Deployment Services role.
- Add a boot image.
- Add an install image.

# Automating Deployments

To automate the Windows Setup process:

1. Create the Unattend.xml file
2. Copy the file to the Windows Deployment Services server
3. View the properties of the appropriate install image
4. Enable unattended mode and select the answer file

# Demonstration: How to Configure Multicast Transmission

In this demonstration, you will see how to configure multicast transmission

# Lab: Using Windows Deployment Services to Deploy Windows Server 2012

- Exercise 1: Installing and Configuring Windows® Deployment Services
- Exercise 2: Creating Operating System Images with Windows Deployment Services
- Exercise 3: Configuring Custom Computer Naming
- Exercise 4: Deploying Images with Windows Deployment Services

Logon Information

**Virtual Machines:** 20411D-LON-DC1,  
20411D-LON-SVR1, 20411D-LON-SVR3

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 75 minutes

# Lab Scenario

- A. Datum Corporation is a global engineering and manufacturing company with its head office in London, England. An IT office and data center are in London to support the head office and other branch locations. A. Datum has recently deployed a Windows Server 2012 R2 server and client infrastructure.
- A. Datum is deploying servers to branch offices throughout the region for the Research department. Management selected you to automate this deployment. You suggest using

## Lab Scenario

Windows Deployment Services to deploy Windows Server 2012 R2 to the branch offices. Management has sent you some instructions by email regarding the deployment. You must read these instructions, and then install and configure Windows Deployment Services to support the deployment.

# Lab Review

- How do You Use Windows Deployment Services in your organization?
- For what two categories of images do you need to use Windows Deployment Services to deploy an operating system to a computer over the network?
- How can you avoid name conflicts when deploying an operating system to multiple computers in the same transmission?

# Module Review and Takeaways

- Review Question(s)
- Tools

# Microsoft® Official Course



Module 12

Implementing Update  
Management

**Microsoft®**

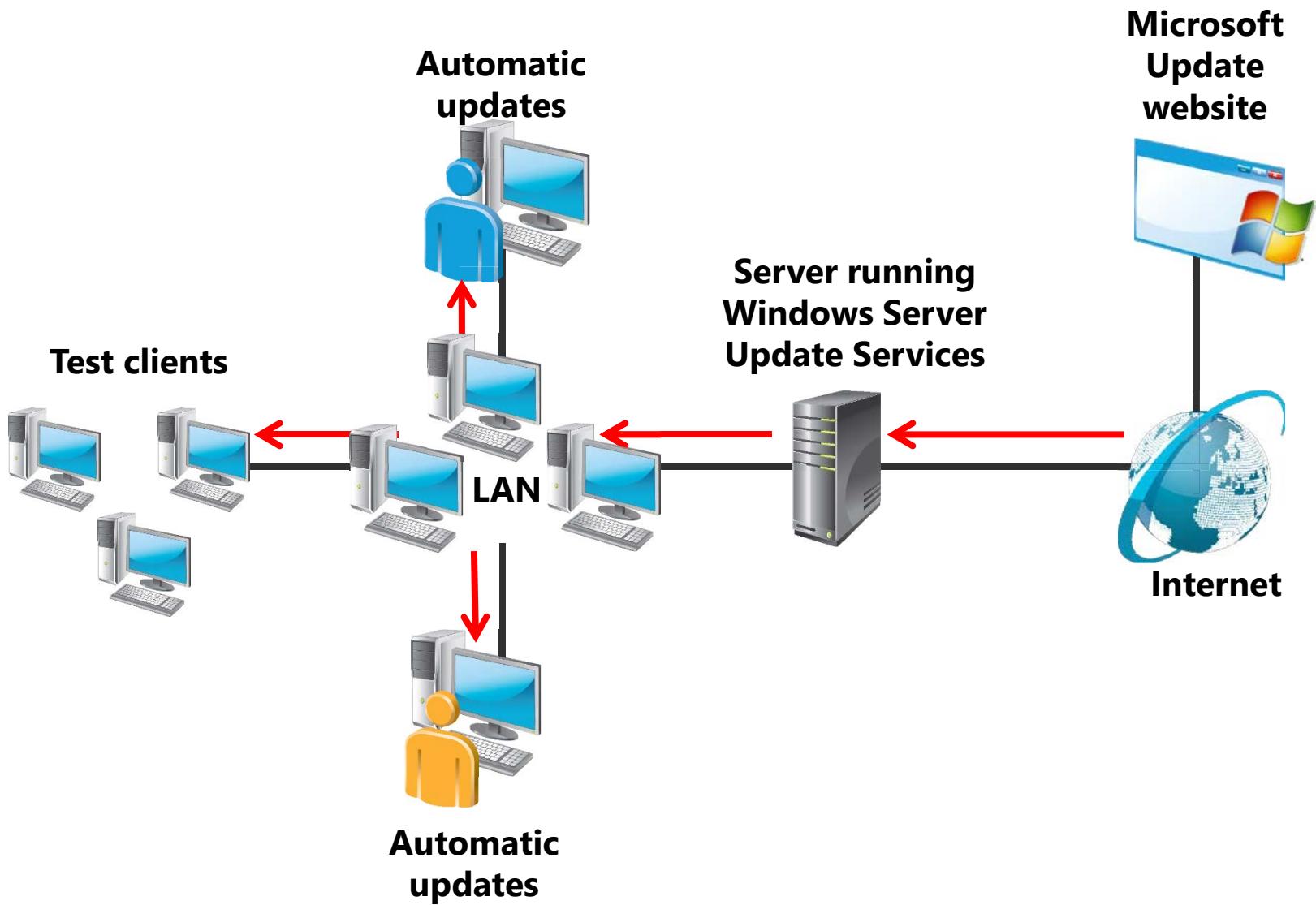
# Module Overview

- Overview of WSUS
- Deploying Updates with WSUS

# Lesson 1: Overview of WSUS

- What Is WSUS?
- WSUS Server Deployment Options
- The WSUS Update Management Process
- Server Requirements for WSUS
- Configuring Clients to Use WSUS

# What Is WSUS?



# WSUS Server Deployment Options

- WSUS Implementation

- Single server
- Multiple servers
- Disconnected servers

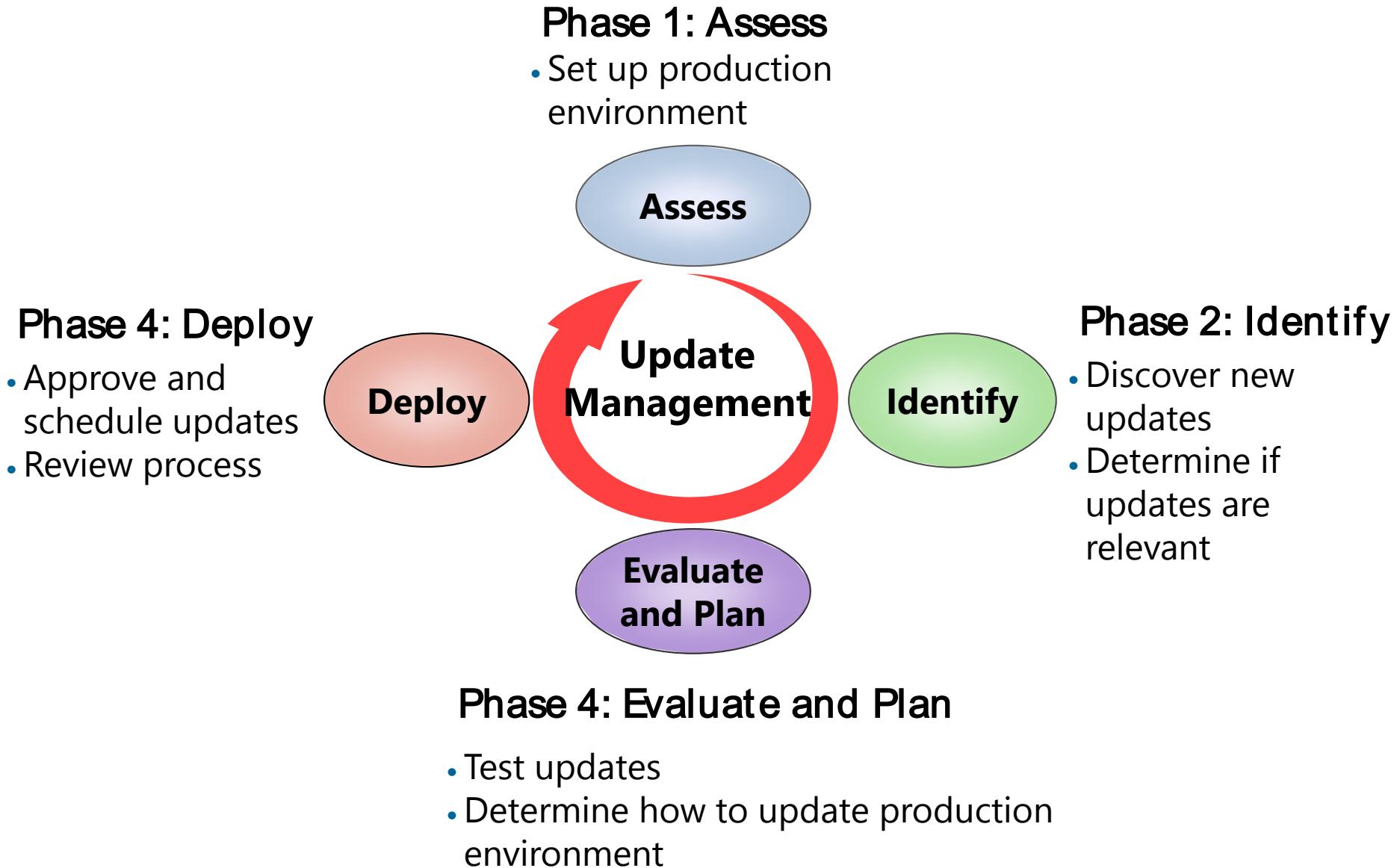
- WSUS hierarchies

- Autonomous mode
- Replica mode

- WSUS database

- Windows Internal Database
- SQL Server database

# The WSUS Update Management Process



# Server Requirements for WSUS

## Software requirements:

- Internet Information Services 6.0 or newer
- Microsoft .NET Framework 2.0 or newer
- Microsoft Management Console 3.0
- Microsoft Report Viewer Redistributable 2008 or newer
- SQL Server 2012, SQL Server 2008, SQL Server 2005 SP2, or Windows Internal Database

## Hardware requirements:

- 1.4 GHz or faster x64 processor
- 2 GB of RAM or greater
- 10 GB available disk space (40 GB or greater is recommended)

# Configuring Clients to Use WSUS

- Use a GPO to:
  - Configure automatic updates
  - Specify intranet Microsoft update service location
- For computers running Windows 8, Windows Server 2012 (this does not apply to Windows 8.1 and Windows Server 2012 R2) you should:
  - Automatically download updates
  - Do not automatically install updates
- For computers running older operating systems, you should:
  - Automatically download updates
  - Automatically install updates

# Lesson 2: Deploying Updates with WSUS

- WSUS Administration
- What Are Computer Groups?
- Approving Updates
- Configuring Automatic Updates
- Demonstration: Deploying Updates by Using WSUS
- WSUS Reporting
- WSUS Troubleshooting

# WSUS Administration

You can use the WSUS Administration console to:

- Manage updates
- Configure computer groups
- View computer status
- View synchronization information
- Configure and view WSUS reports
- Configure WSUS settings and options

In Windows Server 2012, WSUS also includes Windows PowerShell cmdlets for administration

# What Are Computer Groups?

- You can use computer groups to organize WSUS clients
- The default computer groups include:



**All Computers**



**Unassigned Computers**

- You can create custom computer groups to control how updates are applied

# Approving Updates

Updates can be:

- Approved automatically, but it is not recommended
- Declined if they are not needed
- Removed if they cause problems

Updates should be tested before they are approved for production

# Configuring Automatic Updates

You must configure the client computers to use the WSUS server as the source for updates

You can use Group Policy to configure clients, including the following settings:

- Update frequency
- Update installation schedule
- Automatic restart behavior
- Default computer group in WSUS

# Demonstration: Deploying Updates by Using WSUS

In this demonstration, you will learn how to:

- Approve an update
- Deploy an update

# WSUS Reporting

- Update Reports
  - Update Status Summary
  - Update Detailed Status
  - Update Tabular Status
  - Update Tabular Status for Approved Updates
- Computer Updates
  - Computer Status Summary
  - Computer Detailed Status
  - Computer Tabular Status for Approved Updates
- Synchronization Updates
  - Synchronization Results

# WSUS Troubleshooting

- Clients not appearing in WSUS
  - Check GPO and client settings
- When the WSUS server stops, you should:
  - Check database server
  - Reinstall WSUS
- When you cannot connect to WSUS, you should:
  - Check network connectivity
  - Telnet to HTTP and HTTPS ports
- If you encounter other problems you should use the:
  - Server diagnostics tool
  - Client diagnostics tool

# Lab: Implementing Update Management

- Exercise 1: Implementing the WSUS Server Role
- Exercise 2: Configuring Update Settings
- Exercise 3: Approving and Deploying an Update by Using WSUS

## Logon Information

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1,  
20411D-LON-SVR4, 20411D-LON-CL1

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 60 minutes

# Lab Scenario

- A. Datum is a global engineering and manufacturing company with a head office in London, United Kingdom. An IT office and a data center are located in London to support the London location and other branch office locations.
- A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.
- A. Datum has been manually applying updates to servers in a remote location. This has resulted in difficulty identifying which servers have updates applied and which do not. This is a potential

## Lab Scenario

security issue. You have been asked to automate the update process by extending A. Datum's WSUS deployment to include the branch office.

# Module Review and Takeaways

- Review Question(s)
- Tools
- Best Practice

# Microsoft® Official Course



Module 13

Monitoring Windows Server 2012

**Microsoft®**

# Module Overview

- Monitoring Tools
- Using Performance Monitor
- Monitoring Event Logs

# Lesson 1: Monitoring Tools

- Overview of Task Manager
- Overview of Performance Monitor
- Overview of Resource Monitor
- Overview of Reliability Monitor
- Overview of Event Viewer
- Monitoring a Server With Server Manager

# Overview of Task Manager

Task Manager helps you to identify and resolve performance-related issues

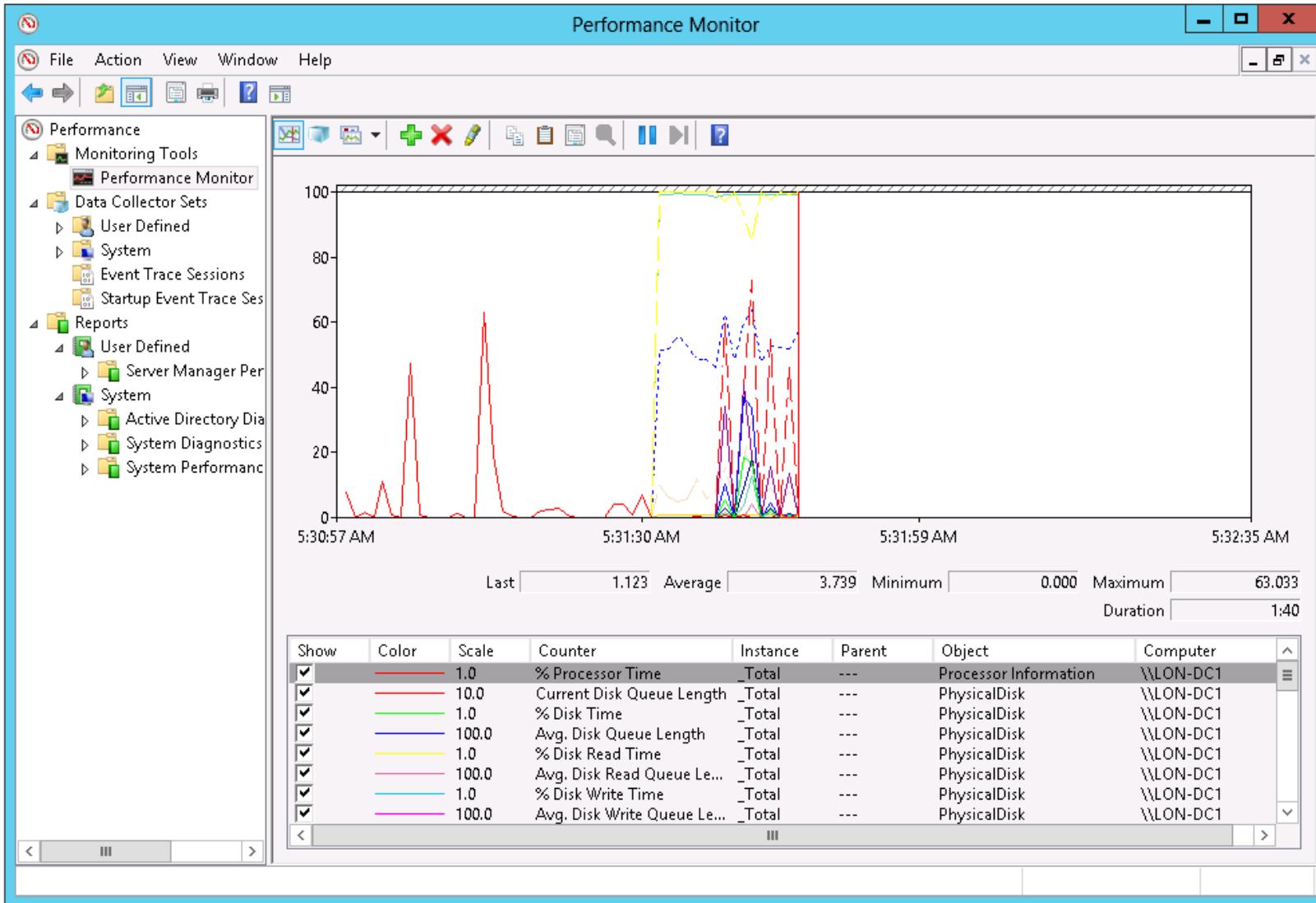
The screenshot shows the Windows Task Manager interface. At the top, there's a menu bar with File, Options, and View. Below the menu is a tab bar with Processes (selected), Performance, Users, Details, and Services. The main area is a table with columns for Name, Status, CPU, and Memory. The table lists various processes categorized into Apps, Background processes, and Windows processes. Most processes are shown with 0% CPU usage and low memory consumption.

| Name                                 | Status | CPU | Memory  |
|--------------------------------------|--------|-----|---------|
| Apps (1)                             |        |     |         |
| Task Manager                         |        | 0%  | 7.2 MB  |
| Background processes (8)             |        |     |         |
| Distributed File System Replicati... |        | 0%  | 6.7 MB  |
| Domain Name System (DNS) Se...       |        | 0%  | 79.3 MB |
| Microsoft Distributed Transacti...   |        | 0%  | 2.3 MB  |
| Microsoft.ActiveDirectory.WebS...    |        | 0%  | 9.3 MB  |
| Spooler SubSystem App                |        | 0%  | 1.9 MB  |
| Virtual Disk Service                 |        | 0%  | 1.6 MB  |
| Windows NT Distributed File Sy...    |        | 0%  | 0.9 MB  |
| Windows NT Intersite Messagin...     |        | 0%  | 0.9 MB  |
| Windows processes (22)               |        |     |         |
| Client Server Runtime Process        |        | 0%  | 1.0 MB  |
| Client Server Runtime Process        |        | 0%  | 0.9 MB  |
| Desktop Window Manager               |        | 0%  | 16.3 MB |
| Host Process for Windows Tasks       |        | 0%  | 1.2 MB  |

At the bottom left is a "Fewer details" button, and at the bottom right is an "End task" button.

# Overview of Performance Monitor

Performance Monitor enables you to view current performance statistics or to view historical data  
Data Collector Sets have gathered



# Overview of Performance Monitor

## **Primary Processor Counters:**

- Processor > % Processor Time
- Processor > Interrupts/sec
- System > Processor Queue Length

## **Primary Disk Counters:**

- Physical Disk > % Disk Time
- Physical Disk > Avg. Disk Queue Length

## **Primary Network Counters:**

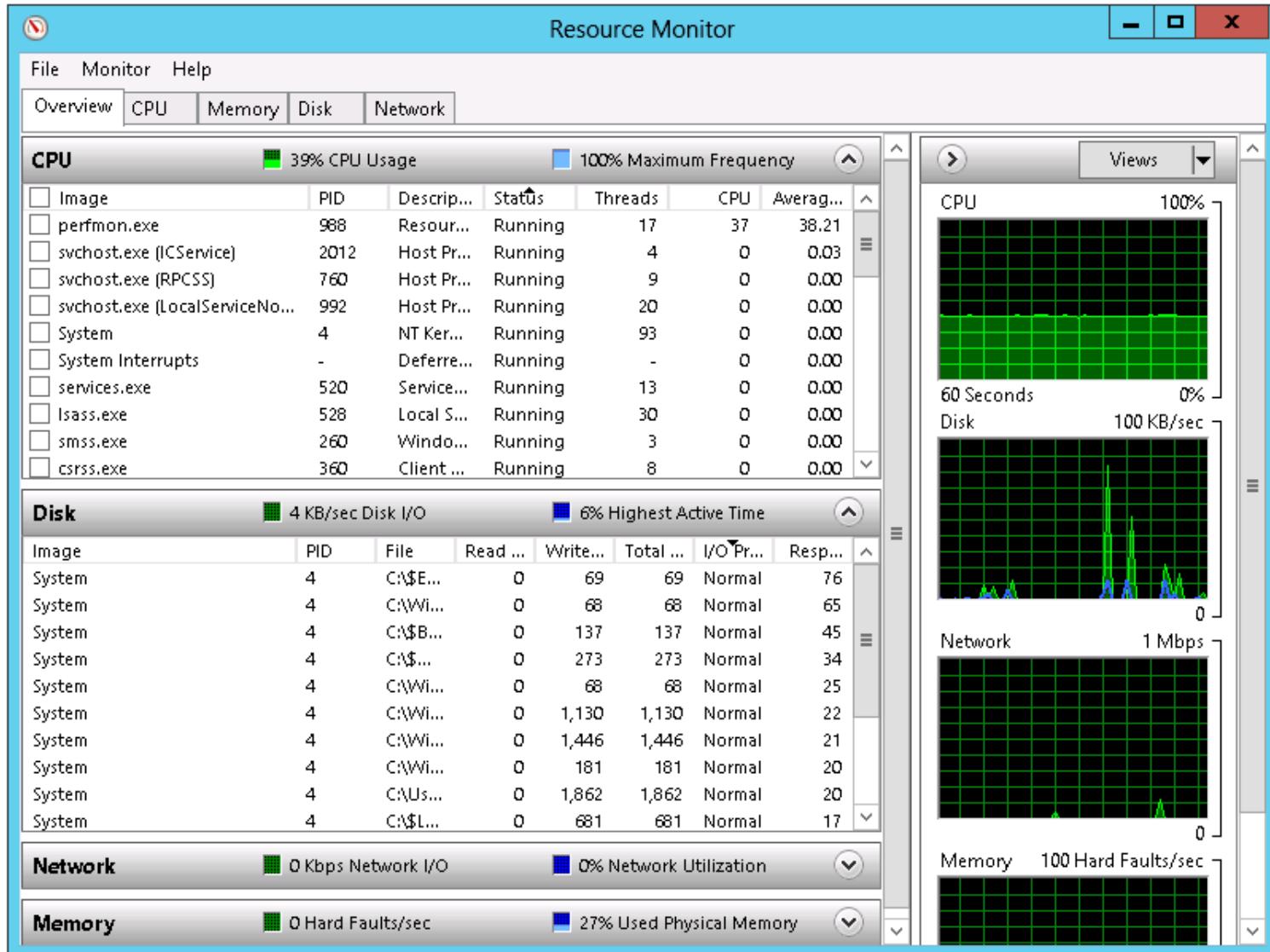
- Network Interface > Current Bandwidth
- Network Interface > Output Queue Length
- Network Interface > Bytes Total/sec

## **Primary Memory Counter:**

- The Memory > Pages/sec counter

# Overview of Resource Monitor

Resource Monitor provides an in-depth look at the real-time performance of your server

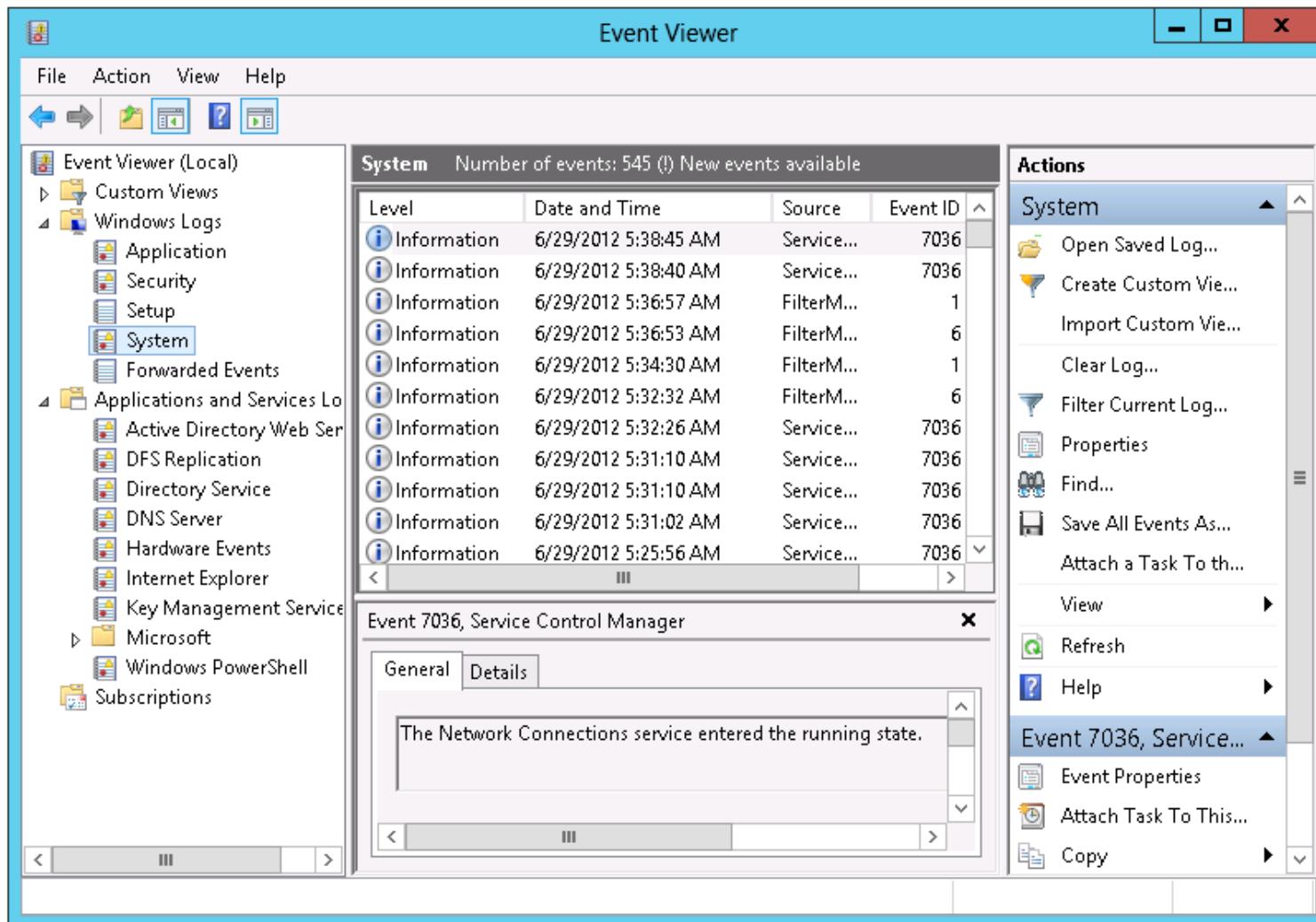


# Overview of Reliability Monitor

- Monitors hardware and software issues
- Provides Stability Index number (from 1 to 10)
  - 1 represents lowest stability
  - 10 represents highest stability
- Reliability monitor window components include:
  - Historical reports on stability index
  - Reliability details
  - Action to be performed: saving historical data, starting Problem Reports console, checking online for a solution to specific problem

# Overview of Event Viewer

Event Viewer provides categorized lists of essential Windows log events, and log groupings for individual installed applications and specific Windows component categories



# Overview of Event Viewer

- Event Viewer provides the ability to
  - View multiple logs
  - Create customized views
  - Configure tasks scheduled to run in response to events
  - Create and manage event subscriptions
- Event Viewer has many built-in logs such as
  - Application log
  - Security log
  - Setup log
  - System log
  - Forwarded events

# Monitoring a Server With Server Manager

## Server Manager console:

- Installed by default on Windows Server 2012, can be installed on Windows 8
- Supports monitoring of Windows Server operating systems
- Provides a centralized monitoring dashboard
- Analyzes or troubleshoots different types of issues
- Identifies critical events
- Monitors the status of Best Practices Analyzer tool

# Lesson 2: Using Performance Monitor

- Performance Baselines, Trends, and Capacity Planning
- What Are Data Collector Sets?
- Demonstration: Capturing Counter Data with a Data Collector Set
- What Are Alerts?
- Demonstration: Configuring an Alert
- Demonstration: Viewing Reports in Performance Monitor
- Monitoring Network Infrastructure Services
- Considerations for Monitoring Virtual Machines

# Performance Baselines, Trends, and Capacity Planning

- By calculating performance baselines for your server environment, you can more accurately interpret real-time monitoring information
- By establishing a baseline, you can:
  - Interpret performance trends
  - Perform capacity planning
  - Identify bottlenecks
- Analyze performance trends to predict when existing capacity is likely to be exhausted
- Plan the capacity for the key hardware components: processor, disk, memory and network

# What Are Data Collector Sets?

- Data collector sets enable you to gather performance-related and other system statistics for analysis
- Data collector sets can contain the following types of data collectors:
  - Performance counters
  - Event trace data
  - System configuration information

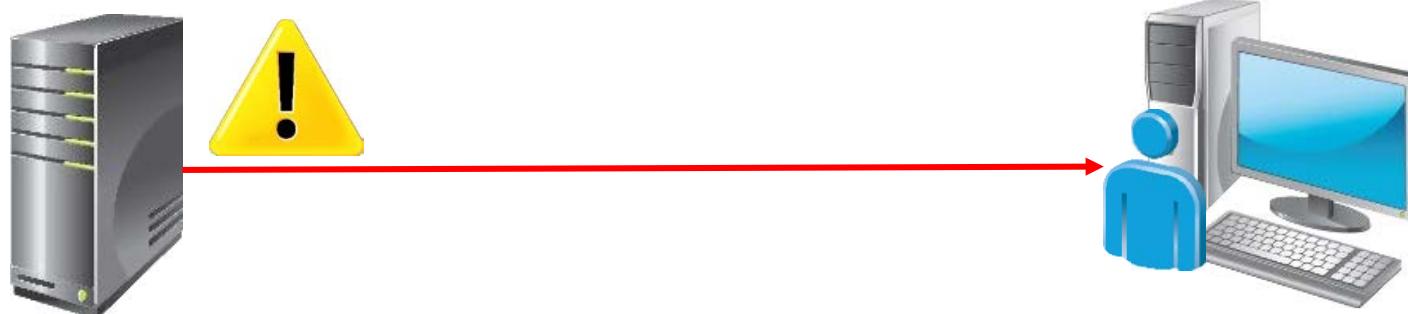
# Demonstration: Capturing Counter Data with a Data Collector Set

In this demonstration, you will see how to:

- Create a data collector set
- Create a disk load on the server
- Analyze the resulting data in a report

# What Are Alerts?

- An alert notifies the administrator of events that have occurred or performance thresholds that have been reached
- When creating an alert, configure the following settings:
  - Alert when
  - Alert Action
  - Alert Task



# Demonstration: Configuring an Alert

In this demonstration, you will see how to:

- Create a data collector set with an alert counter
- Generate a server load that exceeds the configured threshold
- Examine the event log for the resulting event

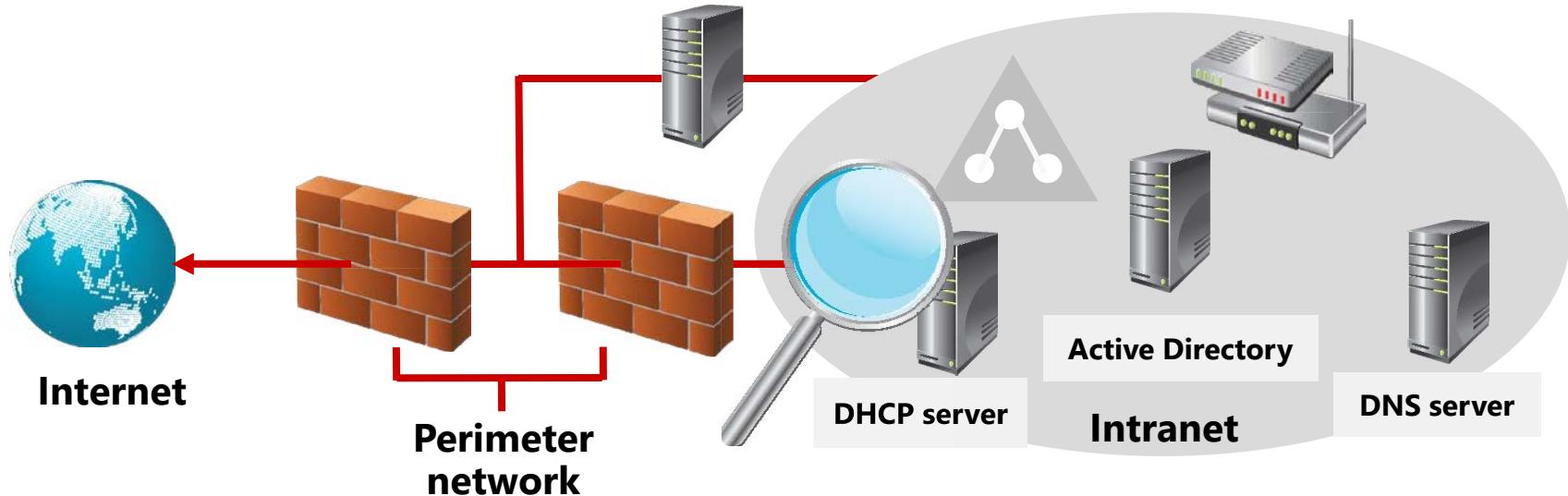
# Demonstration: Viewing Reports in Performance Monitor

In this demonstration, you will see how to view a performance report

# Monitoring Network Infrastructure Services

Monitoring is essential for:

- Optimizing network infrastructure server performance
- Troubleshooting servers



# Considerations for Monitoring Virtual Machines

Considerations for monitoring virtual machines:

- Virtual machines must be assigned sufficient resources for their workload
- If multiple virtual machines run on a host, ensure the host has enough resources
- Resources are shared, so performance of one virtual machine can affect the performance of others
- You must remember to monitor the resource utilization on the host as well as the guests

# Lesson 3: Monitoring Event Logs

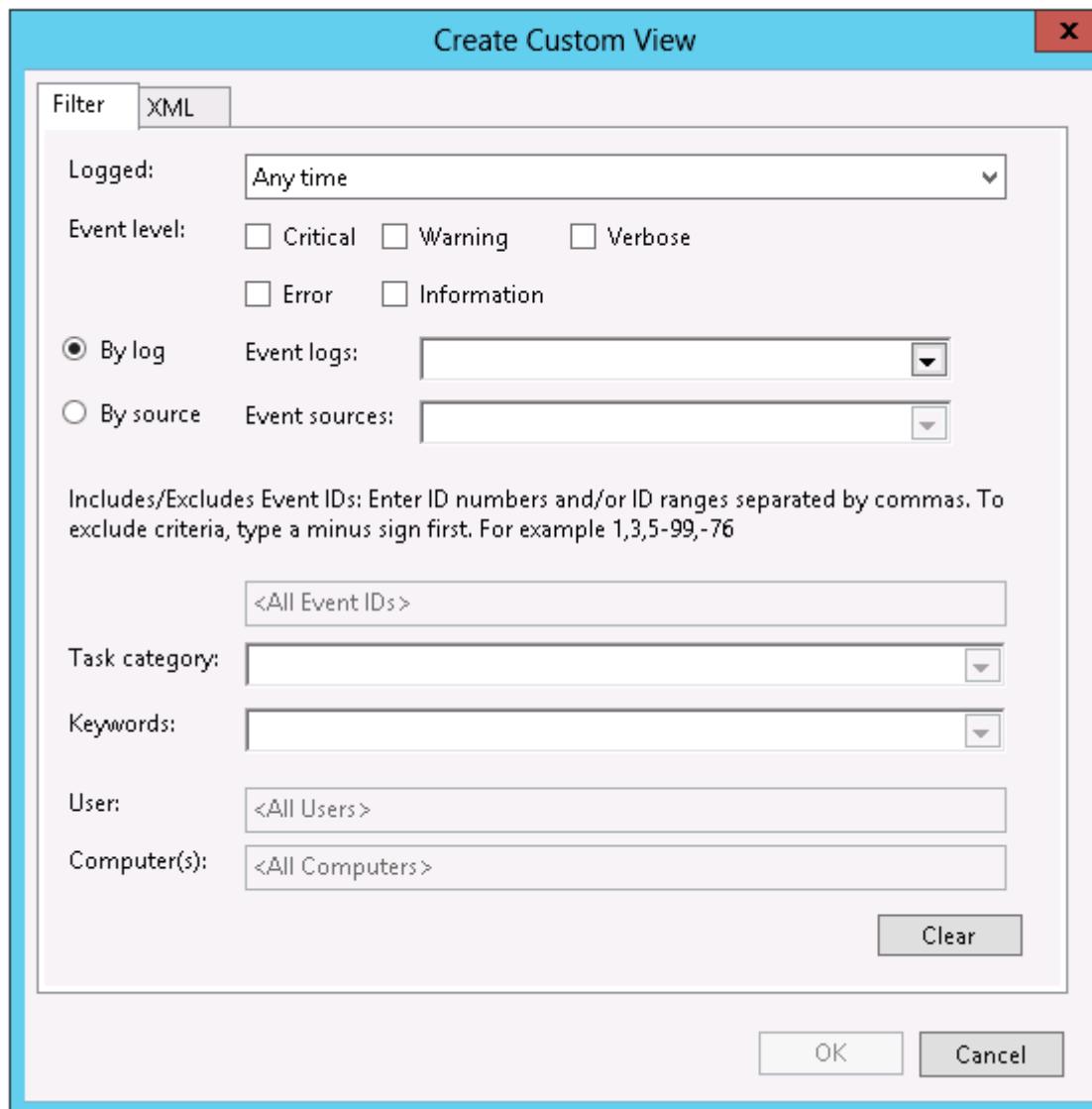
- Using Server Manager to View Event Logs
- What Is a Custom View?
- Demonstration: Creating a Custom View
- What Are Event Subscriptions?
- Demonstration: Configuring an Event Subscription

# Using Server Manager to View Event Logs

- Server Manager provides a centralized location for event logs from remote servers
- Event logging
  - Enabled by default
  - Categorized by technology: AD DS, DNS, Remote Access
- Customized views
  - Create queries for specific types of events that need to be displayed
  - Configure event data that needs to be displayed

# What Is a Custom View?

Custom views allow you to query and sort just the events that you want to analyze



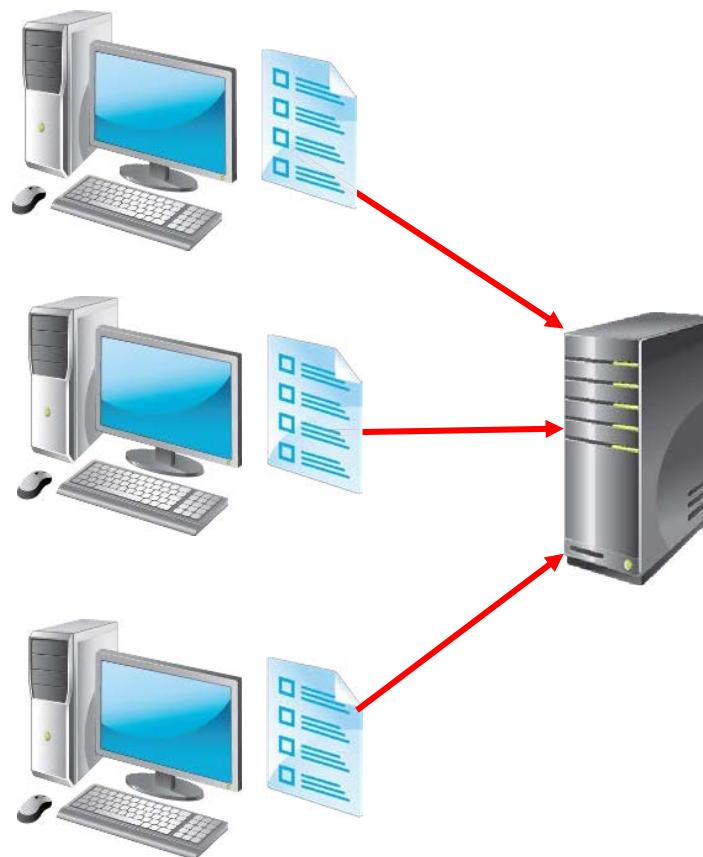
# Demonstration: Creating a Custom View

In this demonstration, you will see how to:

- View Server Roles custom views
- Create a custom view

# What Are Event Subscriptions?

Event subscriptions allow you to collect event logs from multiple servers, and then store them locally



# Demonstration: Configuring an Event Subscription

In this demonstration, you will see how to:

- Configure the source computer
- Configure the collector computer
- Create and view the subscribed log

# Lab: Monitoring Windows Server 2012

- Exercise 1: Establishing a Performance Baseline
- Exercise 2: Identifying the Source of a Performance Problem
- Exercise 3: Viewing and Configuring Centralized Event Logs

## Logon Information

**Virtual Machines:** 20411D-LON-DC1,  
20411D-LON-SVR1

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

Estimated Time: 60 minutes

# Lab Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, England. An IT office and data center are in London to support the London location and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure.

Because the organization has deployed new servers, it is important to establish a performance baseline with a typical load for these new servers. You have been asked to work on this project.

## Lab Scenario

Additionally, to make the process of monitoring and troubleshooting easier, you decide to perform centralized monitoring of event logs.

# Lab Review

During the lab, you collected data in a data collector set. What is the advantage of collecting data in this way?

# Module Review and Takeaways

- Review Question(s)
- Tools
- Best Practices

# Course Evaluation



# Microsoft® Official Course



## Module 1

### Implementing Advanced Network Services

**Microsoft®**

# Module Overview

- Configuring Advanced DHCP Features
- Configuring Advanced DNS Settings
- Implementing IPAM
- Managing IP Address Spaces with IPAM

# Lesson 1: Configuring Advanced DHCP Features

- DHCP Components Overview
- Configuring DHCP Interaction with DNS
- Configuring Advanced DHCP Scope Designs
- DHCP Integration with IPv6
- What Is DHCP Name Protection?
- What Is DHCP Failover?
- Demonstration: Configuring DHCP Failover

# DHCP Components Overview

DHCP components consist of:

- The DHCP server service
- DHCP options
- DHCP console
- DHCP scopes
- DHCP database

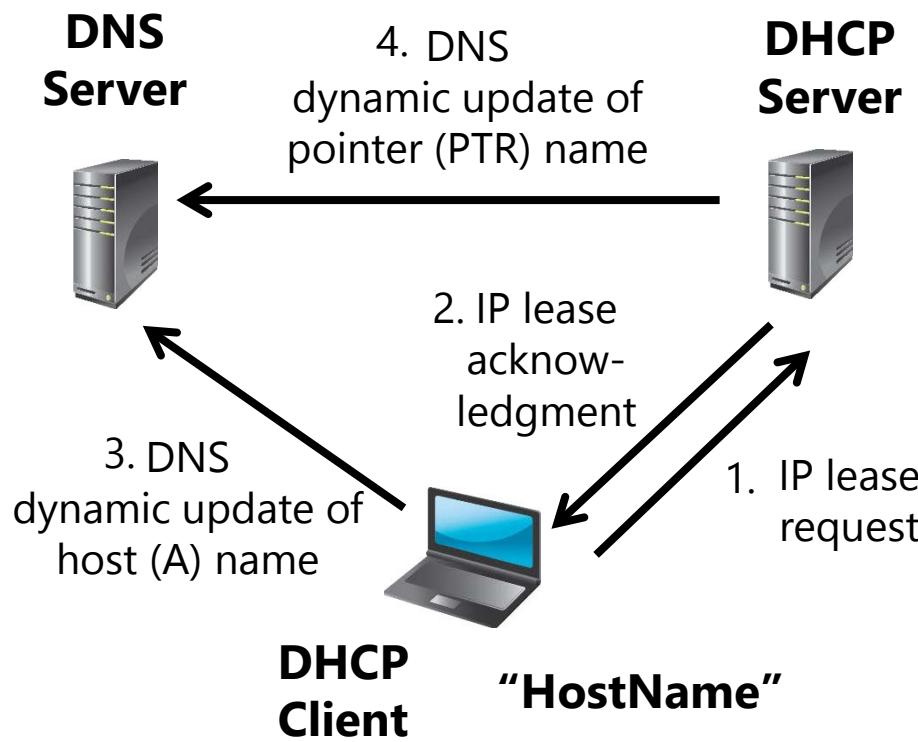
When you use DHCP:

- Clients request IP configuration through a broadcast
- IP addresses are leased to clients for a configurable period, and are regularly renewed
- DHCP servers must be authorized in AD DS

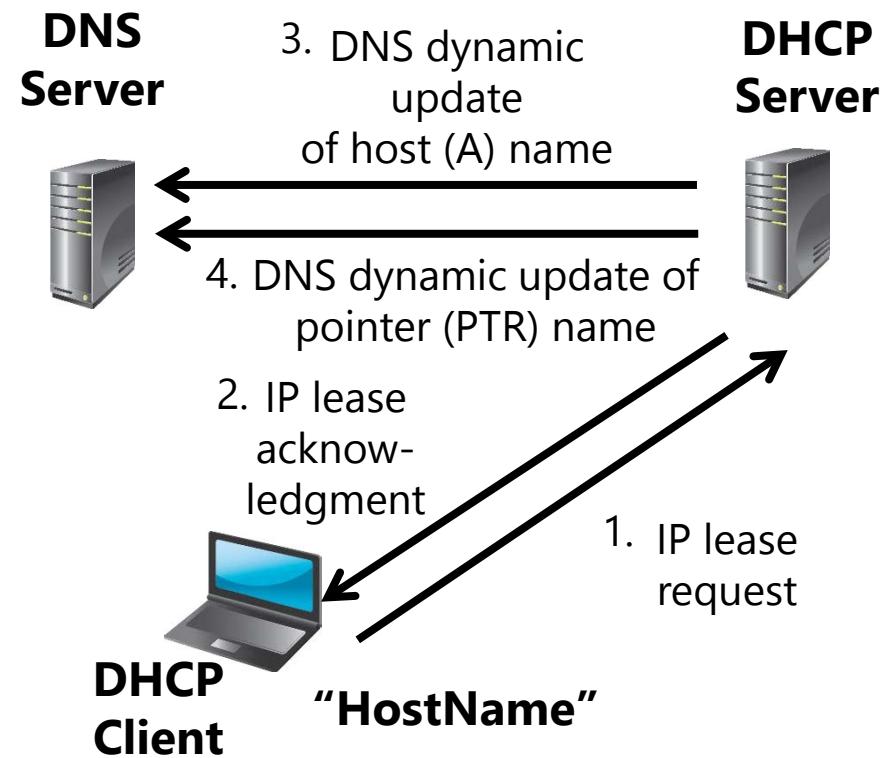
# Configuring DHCP Interaction with DNS

Configuring option 081 allows the DHCP server to register both A and PTR resource records for the client

Normal option 081 behavior



Modified option 081 behavior



# Configuring Advanced DHCP Scope Designs

## Superscopes

- Support multiple VLANs on a single physical network
- Can ease transitioning to new IP Scheme
- Require router support between VLANs

## Multicast

- Uses the Class D 224.0.0.0/3
- Used for applications that need simultaneous communication with multiple clients
- Use in addition to the Network IP Address

# DHCP Integration with IPv6

DHCPv6 supports stateful and stateless configurations

DHCPv6 also supports scopes that you can configure with the following properties:

- Name and description
- Preference
- Valid and Preferred lifetimes
- Prefix
- Exclusions
- DHCP options

# What Is DHCP Name Protection?

## DHCP Name Protection:

- Prevents Windows operating systems from having their DNS name registrations overwritten by non-Windows operating systems that have the same name
- Uses a DHCID resource record to track the machines that originally requested the DNS names
- Is configurable at the network protocol level and at the scope level

# What Is DHCP Failover?

## DHCP failover:

- Enables two DHCP servers to provide IP addresses and optional configurations to the same subnets or scopes
- Requires failover relationships to have unique names
- Supports the hot standby mode and the load sharing mode

## When you use DHCP failover:

- The MCLT determines when a failover partner assumes control of the subnet or scope
- The auto state switchover interval determines when a failover partner is considered to be down
- Message authentication can validate the failover messages
- Firewall rules are auto-configured during DHCP installation

# Demonstration: Configuring DHCP Failover

- In this demonstration, you will see how to configure a DHCP failover relationship

# Lesson 2: Configuring Advanced DNS Settings

- Managing DNS Services
- Optimizing DNS Name Resolution
- What Is the GlobalNames Zone?
- Options for Implementing DNS Security
- How DNSSEC Works
- New DNSSEC Features for Windows Server 2012
- Demonstration: Configuring DNSSEC

# Managing DNS Services

To manage DNS services:

- Delegate DNS administration through membership in the DNS Admins group
- View DNS logs in Event Viewer
- Enable DNS debug logging in the DNS server properties
- Enable aging and scavenging to remove stale records

Backup methods for the DNS database depend on how the database is deployed:

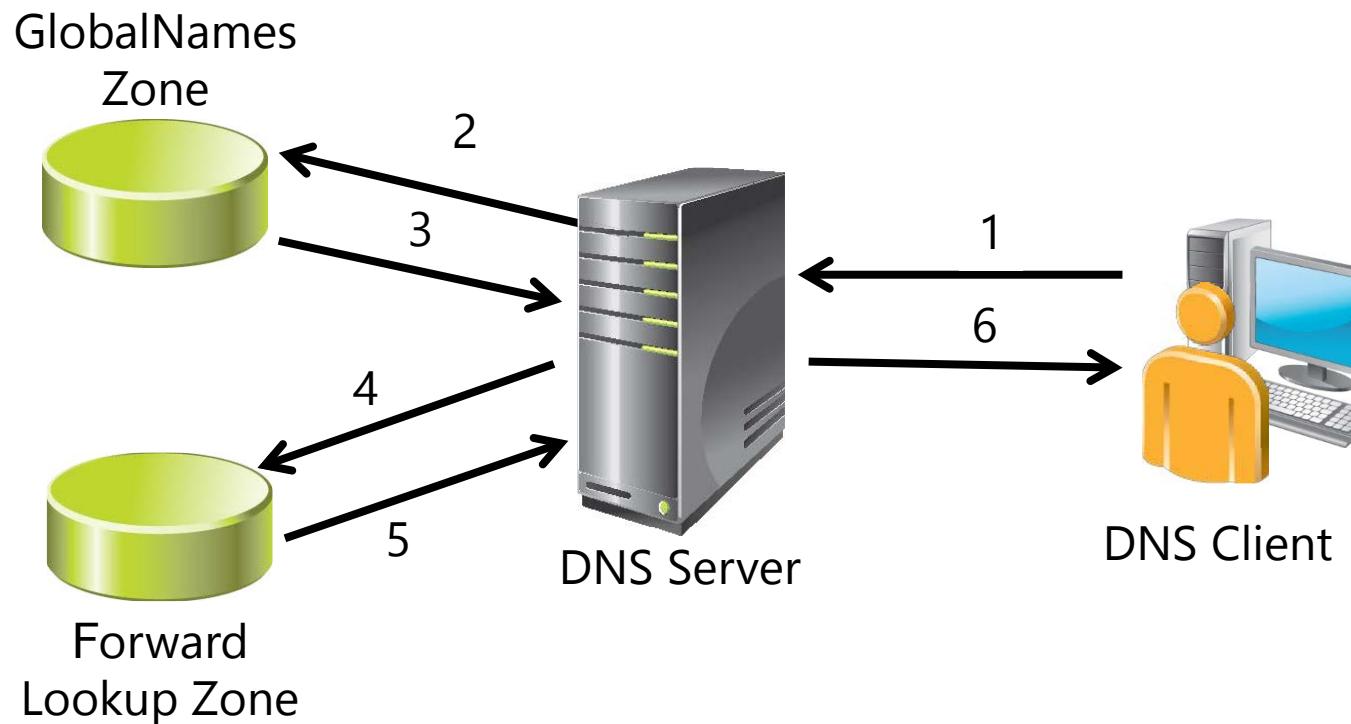
- Back up Active Directory-integrated zones through system state backups, by using `dnscmd`, or by using Windows PowerShell
- Non-integrated primary zone are single files that you can copy or back up

# Optimizing DNS Name Resolution

| Option                 | Description                                                                                                               |
|------------------------|---------------------------------------------------------------------------------------------------------------------------|
| Forwarding             | Forwards DNS requests that cannot be resolved locally to other specific DNS servers                                       |
| Conditional forwarding | Forwards queries for specific DNS suffixes to specific DNS servers                                                        |
| Stub zones             | A regularly replicated copy of certain resource records that identify authoritative DNS servers for specific DNS domains  |
| Netmask ordering       | Responds with addresses of hosts that are close in proximity based in IP address information of the client to DNS queries |

# What Is the GlobalNames Zone?

The GlobalNames zone allows single label names to be resolved in multiple DNS domain environments



# Options for Implementing DNS Security

| Option            | Description                                                                                         |
|-------------------|-----------------------------------------------------------------------------------------------------|
| DNS cache locking | Prevents entries in the cache from being overwritten until a percentage of the TTL has expired      |
| DNS socket pool   | Randomizes the source port for issuing DNS queries<br><br>Enabled by default in Windows Server 2012 |
| DNSSEC            | Enables cryptographically signing DNS records so that client computers can validate responses       |

# How DNSSEC Works

DNSSEC functions as follows:

- If a zone has been digitally signed, a query response will contain digital signatures
- DNSSEC uses trust anchors, which are special zones that store public keys associated with digital signatures
- Resolvers use trust anchors to retrieve public keys and build trust chains
- DNSSEC requires trust anchors to be configured on all DNS servers participating in DNSSEC
- DNSSEC uses the NRPT, which contains rules that control the requesting client computer behavior for sending queries and handling responses

# New DNSSEC Features for Windows Server 2012

DNSSEC enhancements for Windows Server 2012 include:

- Simplified DNSSEC implementation
- A DNSSEC Zone Signing Wizard that steps you through the process of signing and configuring signing parameters for zones
- The following new resource records:
  - DNSKEY
  - DS
  - RRSIG
  - NSEC

# Demonstration: Configuring DNSSEC

- In this demonstration, you will see how to configure DNSSEC

# Lesson 3: Implementing IPAM

- What Is IPAM?
- IPAM Overview
- Requirements for IPAM Implementation
- Demonstration: Implementing IPAM
- Virtual Address Space Management in IPAM
- IPAM RBAC

# What Is IPAM?

IPAM facilitates IP management in organizations with complex networks by enabling administration and monitoring of DHCP and DNS

| IP administration area | Description                                                                                                        |
|------------------------|--------------------------------------------------------------------------------------------------------------------|
| Planning               | Reduces the time and expense of the planning process when changes occur in the network                             |
| Managing               | Provides a single point of management and assists in optimizing utilization and capacity planning for DHCP and DNS |
| Tracking               | Enables tracking and forecasting of IP address utilization                                                         |
| Auditing               | Assists with compliance requirements and provides reporting for forensics and change management                    |

# IPAM Overview

IPAM architecture consists of:

- Four main modules:
  - IPAM discovery
  - IPAM address space management
  - Multiserver management and monitoring
  - Operational auditing and IP address tracking
- A server component and a client component
- You can deploy IPAM in the following topologies:
  - Distributed
  - Centralized
  - Hybrid
- Provisioned either manually or through GPO

# Requirements for IPAM Implementation

| Prerequisites                                                                                                                                                                                                                                                                                                                                                                                        | Hardware and software requirements                                                                                                                                      |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• IPAM server must belong to the domain</li><li>• IPAM server cannot be a domain controller</li><li>• IPv6 must be enabled in order to manage IPv6</li><li>• Log on with a domain account</li><li>• You must be in the correct IPAM local security group</li><li>• Logging account logon events must be enabled for IP address tracking and auditing</li></ul> | <ul style="list-style-type: none"><li>• CPU – dual-core 2.0 GHz or higher</li><li>• Windows Server 2012</li><li>• 4 GB of RAM</li><li>• 80 GB free disk space</li></ul> |

# Demonstration: Implementing IPAM

- In this demonstration, you will see how to install and configure IPAM management

# Virtual Address Space Management in IPAM

IPAM ▶ VIRTUALIZED IP ADDRESS SPACE ▶ IPv4 ▶

Manage Tools

OVERVIEW SERVER INVEN... IP ADDRESS SP... IP Address Bl... IP Address In... IP Address R...

VIRTUALIZED I...

MONITOR AN... DNS and DH... DHCP Scopes DNS Zone M... Server Groups

IPv4 Provider IP Ad... Customer IP A... IPv6 Provider IP Ad...

**IPv4**  
IPv4 | 3 total  
Current view: IP Address Spaces  
Filter

+ Add criteria

| Utilization | Name                     | Type of IP address space  | Access Scope | Percentage Utilized | Owner                             | Description |
|-------------|--------------------------|---------------------------|--------------|---------------------|-----------------------------------|-------------|
| Under       | Security Department      | Customer IP Address Space | \Global      | 0.00                | Security Department Network       |             |
| Under       | Default IP Address Space | Provider IP Address Space | \Global      | 0.00                | Default Provider IP Address Space |             |
| Under       | AdatumHQ                 | Provider IP Address Space | \Global      | 0.00                | Adatum HQ Datacenter              |             |

**Details View**  
Security Department

Configuration Details Event Catalog

Description:  
Security Department Network

|                           |                           |                            |          |
|---------------------------|---------------------------|----------------------------|----------|
| Name:                     | Security Department       | Utilization:               | Under    |
| Type of IP address space: | Customer IP Address Space | Percentage Utilized:       | 0.00     |
| Owner:                    |                           | Provider IP address space: | AdatumHQ |
| Access Scope:             | \Global                   | Is Inherited Access Scope: | Yes      |
| Isolation Method:         | NVGRE                     |                            |          |

# IPAM RBAC

Server Manager ▶ IPAM ▶ ACCESS CONTROL ▶ Roles

Manage Tools View Help

IP ADDRESS SPACE

- IP Address Blocks
- IP Address Inventory
- IP Address Range Groups

VIRTUALIZED IP ADDRESS SPACE

MONITOR AND MANAGE

- DNS and DHCP Servers
- DHCP Scopes
- DNS Zone Monitoring
- Server Groups

EVENT CATALOG

ACCESS CONTROL

Roles

Access Scopes

Access Policies

Roles | 8 total

Filter

TASKS

Add User Role...

Export...

| Name                                      | Built-in Role |
|-------------------------------------------|---------------|
| DNS Record Administrator Role             | Yes           |
| IP Address Record Administrator Role      | Yes           |
| IPAM Administrator Role                   | Yes           |
| IPAM ASM Administrator Role               | Yes           |
| IPAM DHCP Administrator Role              | Yes           |
| IPAM DHCP Reservations Administrator Role | Yes           |
| IPAM DHCP Scope Administrator Role        | Yes           |
| IPAM MSM Administrator Role               | Yes           |



# Lesson 4: Managing IP Address Spaces with IPAM

- Using IPAM to Manage IP Addressing
- Adding Address Spaces to IPAM
- Importing and Updating Address Spaces
- Finding, Allocating, and Reclaiming IP Addresses
- Maintaining IP Address Inventory in IPAM
- Demonstration: Using IPAM to Manage IP Addressing
- IPAM Monitoring
- Demonstration: Using IPAM Monitoring

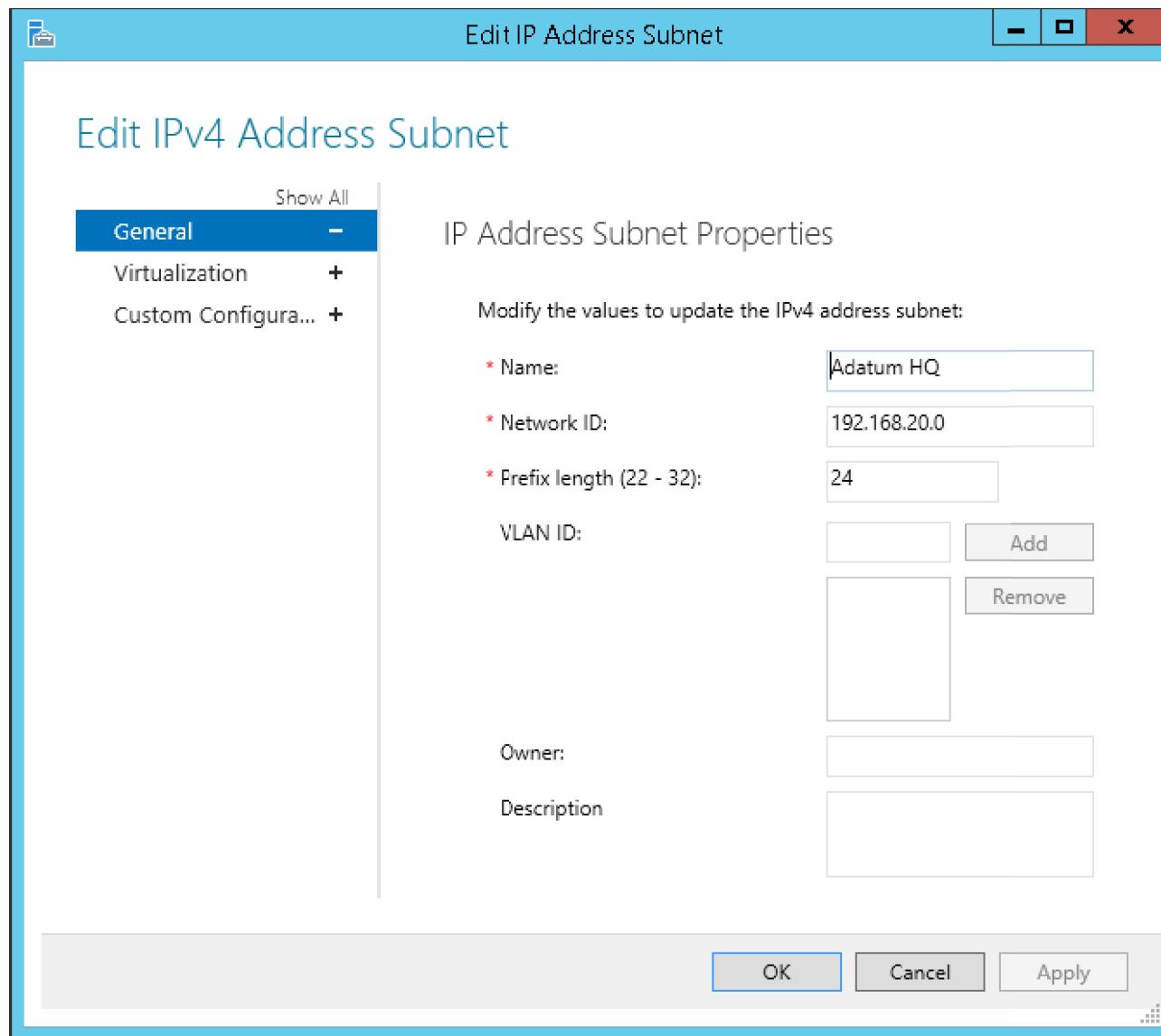
# Using IPAM to Manage IP Addressing

You can view and manage the IP address space using the following views:

- IP address blocks
- IP address ranges
- IP addresses
- IP inventory
- IP address range groups
- You can monitor the IP address space using the following views:
  - DNS and DHCP servers
  - DHCP scopes
  - DNS zone monitoring
  - Server groups



# Adding Address Spaces to IPAM



# Importing and Updating Address Spaces

- Use a text file to import individual IP addresses
- The mandatory fields for IP address import are:
  - IP Address
  - Managed by Service
  - Service Instance
  - Device Type
  - IP Address State
  - Assignment Type
- Use a text file to import or update IP address ranges
- The mandatory fields for IP address block import are:
  - Network
  - Start IP address
  - End IP address
  - RIR

# Finding, Allocating, and Reclaiming IP Addresses

Reclaim IP Addresses

Select IP addresses to reclaim

Delete DNS resource records    Delete DHCP reservation

Select IP addresses to reclaim from the identified IP address range

Selected IP address ranges:

| Network         | Percentage Utilized | Reclaim Last Run | Start IP Address | End IP Address | Managed by Service | Service Instance | Assigned Addresses | Utilized Addresses |
|-----------------|---------------------|------------------|------------------|----------------|--------------------|------------------|--------------------|--------------------|
| 192.168.30.0/24 | 1.57                |                  | 192.168.30.1     | 192.168.30.254 | IPAM               | localhost        | 254                | 4                  |

Summary

Select IP addresses to be reclaimed:

|                          | Expiry Status | Expiry Date | IP Address   | MAC Address | Managed by Service | Service Instance | Device Name | Device Type | IP Address State |  |
|--------------------------|---------------|-------------|--------------|-------------|--------------------|------------------|-------------|-------------|------------------|--|
| <input type="checkbox"/> | Not expired   |             | 192.168.30.1 |             | IPAM               | localhost        |             | Host        | In-Use           |  |
| <input type="checkbox"/> | Not expired   |             | 192.168.30.2 |             | IPAM               | localhost        |             | Host        | In-Use           |  |
| <input type="checkbox"/> | Not expired   |             | 192.168.30.3 |             | IPAM               | localhost        |             | Host        | In-Use           |  |
| <input type="checkbox"/> | Not expired   |             | 192.168.30.4 |             | IPAM               | localhost        |             | Host        | In-Use           |  |

Select all   Unselect all

Reclaim   Cancel



# Maintaining IP Address Inventory in IPAM

IPv4

IPv4 | 1 total

Current view: IP Addresses ▾

Filter

Duplicate Expiry Status IP Address MAC Address Managed by Service Service Instance Access Scope IP Range Virtualized

| No | Expiry Status | IP Address   | MAC Address | Managed by Service | Service Instance | Access Scope | IP Range                    | Virtualized |
|----|---------------|--------------|-------------|--------------------|------------------|--------------|-----------------------------|-------------|
| 1  | Not expired   | 192.168.30.1 |             | IPAM               | localhost        | \Global      | 192.168.30.1-192.168.30.254 | No          |

Details View  
192.168.30.1

Configuration Details Event Catalog

Edit IP Address...  Create DHCP Reservation  Create DNS Host Record  Create DNS PTR Record  Delete DHCP Reservation  Delete DNS Host Record  Delete DNS PTR Record  Delete



# Demonstration: Using IPAM to Manage IP Addressing

- In this demonstration, you will see how to use IPAM to manage IP addressing

# IPAM Monitoring

With IPAM, you can:

- Monitor IP address space utilization
- Monitor DNS and DHCP health
- Configure many DHCP properties and values from the IPAM console
- Use the event catalog to view a centralized repository for all configuration changes

# Demonstration: Using IPAM Monitoring

- In this demonstration, you will see how to use IPAM to monitoring

# Lab: Implementing Advanced Network Services

- Exercise 1: Configuring Advanced DHCP Settings
- Exercise 2: Configuring Advanced DNS Settings
- Exercise 3: Configuring IPAM

## Logon Information

Virtual machines: 20412D-LON-DC1,  
20412D-LON-SVR1,  
20412D-LON-SVR2,  
20412D-LON-CL1

User Name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 70 minutes

# Lab Scenario

A. Datum Corporation has grown rapidly over the last few years. The company has deployed several new branch offices, and it has increased significantly the number of users in the organization. Additionally, it has expanded the number of partner organizations and customers that access A. Datum websites and applications. Because of this expansion, the network infrastructure complexity has increased, and the organization now needs to be much more aware of network-level security.

# Lab Scenario

- As one of the senior network administrators at A. Datum, you are responsible for implementing some of the advanced networking features in Windows Server 2012 R2 to manage the networking infrastructure. You need to implement new features in DHCP and DNS, with the primary goal of providing higher levels of availability while increasing the security of these services. You also need to implement IPAM so that you can simplify and centralize the IP address usage and configuration management in an increasingly complex network.

# Lab Review

- Will client computers immediately stop communicating on the network if there is no functioning DHCP server?
- What is the default size of the DNS socket pool?
- What value does the DNS cache lock use to determine when to update an IP address in the DNS cache?

# Module Review and Takeaways

- Review Question
- Real-world Issues and Scenarios
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 2 Implementing Advanced File Services

**Microsoft®**

# Module Overview

- Configuring iSCSI Storage
- Configuring BranchCache
- Optimizing Storage Usage

# Lesson 1: Configuring iSCSI Storage

- What Is iSCSI?
- iSCSI Target Server and iSCSI Initiator
- Implementing High Availability for iSCSI
- iSCSI Security Options
- Demonstration: Configuring an iSCSI Target
- Demonstration: Connecting to the iSCSI Storage
- Considerations for Implementing iSCSI Storage

# What Is iSCSI?

iSCSI transmits SCSI commands over IP networks

| Component        | Description                                                                              |
|------------------|------------------------------------------------------------------------------------------|
| IP network       | Provides high performance and redundancy                                                 |
| iSCSI targets    | Run on the storage device and enable access to the disks                                 |
| iSCSI initiators | A software component or host adapter on the server that provides access to iSCSI targets |
| IQN              | A globally unique identifier used to address initiators and targets on an iSCSI network  |



TCP/IP protocol



Storage Array

iSCSI Target Server

iSCSI client that runs the iSCSI Initiator

# iSCSI Target Server and iSCSI Initiator

## The iSCSI target server

- Is available as a role service in Windows Server 2012
- Provides the following features:
  - Network/diskless boot
  - Server application storage
  - Heterogeneous storage
  - Lab environments
- Windows Server 2012 R2 features include:
  - Virtual disks
  - Manageability
  - Scalability limits
  - Local mount functionality
- Support for .vhdx
- Improved manageability
- Improved scalability
- Local mount functionality deprecated

# iSCSI Target Server and iSCSI Initiator

## The iSCSI initiator

- Runs as a service in the operating system
- Is installed by default on Windows 8 and Windows Server 2012
- iSCSI targets can be discovered using multiple methods that include:
  - SendTargets
  - iSNS
  - Manually configured targets
  - HBA discovery

# Implementing High Availability for iSCSI

Two technologies for implementing iSCSI for high availability are:

- MCS, in the event of a failure, all outstanding iSCSI commands are reassigned to another connection automatically
- MPIO, if you have multiple network interface cards in your iSCSI initiator and iSCSI target server, you can use MPIO to provide failover redundancy in the event of network outages

# iSCSI Security Options

Mitigate security risks to iSCSI by the following best practices:

- Segregate the iSCSI SAN channel
- Secure management consoles
- Disable unneeded services
- Use CHAP authentication
- Use IPsec authentication
- Use IPsec encryption

# Demonstration: Configuring an iSCSI Target

In this demonstration, you will see how to:

- Add the iSCSI target server role service
- Create two iSCSI virtual disks and an iSCSI target

# Demonstration: Connecting to the iSCSI Storage

In this demonstration, you will see how to:

- Connect to the iSCSI target
- Verify the presence of the iSCSI drive

# Considerations for Implementing iSCSI Storage

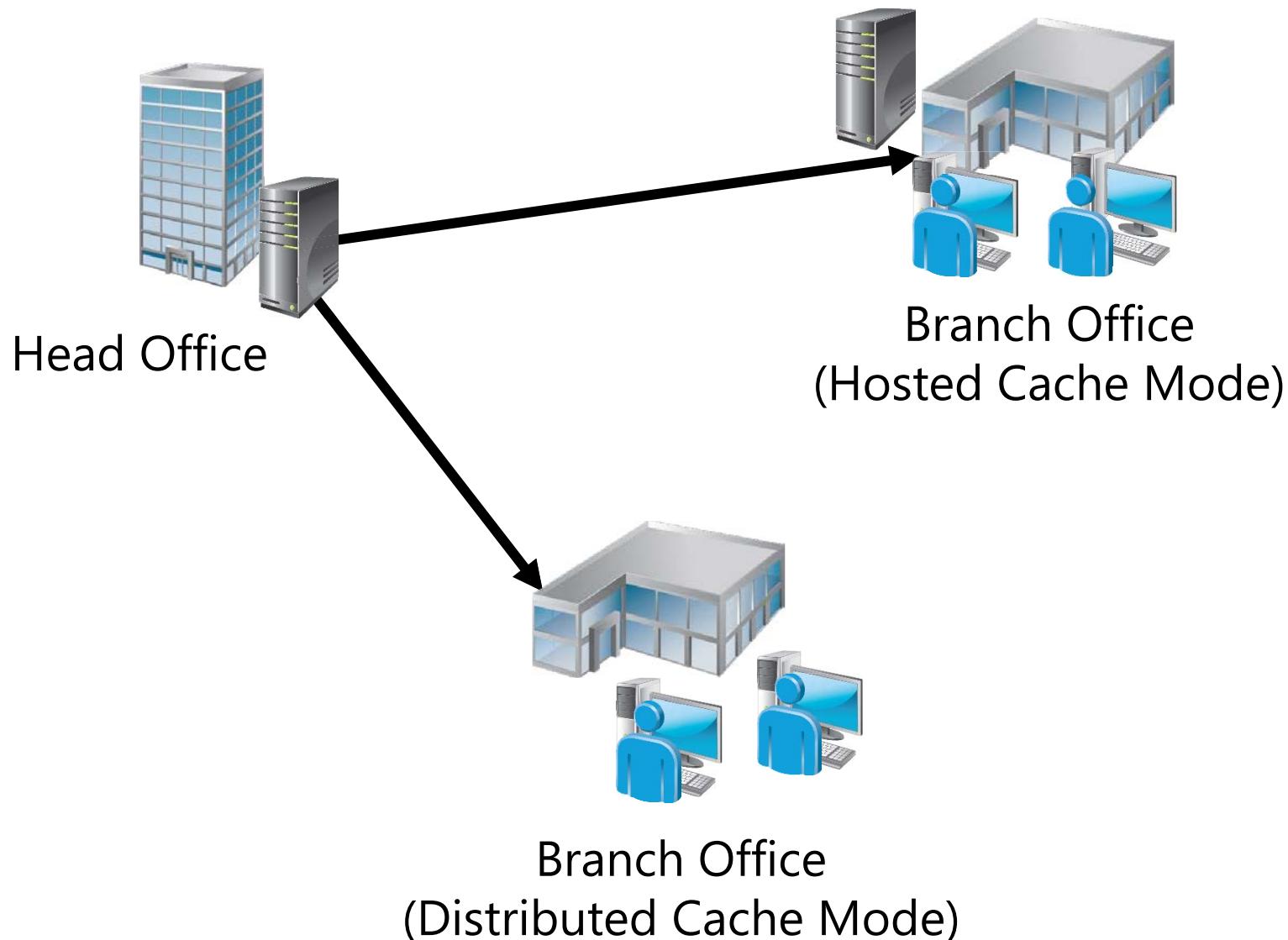
Consider the following when designing your iSCSI storage solution:

- Deploy the solution on fast networks
- Design a highly available network infrastructure for your iSCSI storage solution
- Design an appropriate security strategy for the iSCSI storage solution
- Follow the vendor-specific best practices for different types of deployments
- The iSCSI storage solution team must contain IT administrators from different areas of specialization
- Design application-specific iSCSI storage solutions together with application-specific administrators, such as Exchange Server and SQL Server administrators

# Lesson 2: Configuring BranchCache

- How BranchCache Works
- BranchCache Requirements
- Configuring BranchCache Server Settings
- Configuring BranchCache Client Settings
- Demonstration: Configuring BranchCache
- Monitoring BranchCache

# How BranchCache Works



# BranchCache Requirements

| Requirements for using BranchCache                                                                                                                                                                                                                                     | Requirements for the modes                                                                                                                                                                                                                                                                               |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Install the BranchCache feature or the BranchCache for Network Files feature on the server that is hosting the content</li><li>• Configure client computers by using either Group Policy or the <b>netsh</b> command</li></ul> | <ul style="list-style-type: none"><li>• In distributed cache mode, the content cache at a branch office is distributed between client computers</li><li>• In hosted cache mode, the content cache at the branch office is hosted on one or more server computers that are hosted cache servers</li></ul> |
| <ul style="list-style-type: none"><li>• Content versions:<ul style="list-style-type: none"><li>• V1 uses fixed file segment sizes</li><li>• V2 uses smaller, variable size segments</li></ul></li></ul>                                                                |                                                                                                                                                                                                                                                                                                          |

# Configuring BranchCache Server Settings



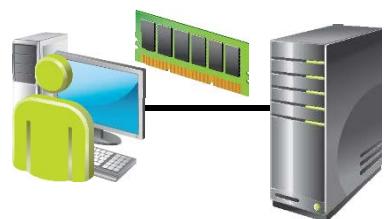
## Configuring the Web Server

Install the BranchCache feature



## Configuring the File Server

1. Install BranchCache for Network Files role service
2. Enable BranchCache on the server
3. Enable BranchCache on file shares



## Configuring the Hosted Cache Server

Add the BranchCache feature to the Windows Server 2012 server

# Configuring BranchCache Client Settings

To enable and configure BranchCache, do the following:

1. Enable BranchCache
2. Enable distributed cache mode or hosted cache mode
3. Configure the client firewall

You can modify BranchCache settings and perform additional configuration tasks, such as:

- Setting the cache size
- Setting the location of the hosted cache server
- Clearing the cache
- Creating and replicating a shared key for using in a server cluster

# Demonstration: Configuring BranchCache

In this demonstration, you will see how to:

- Add BranchCache for the Network Files role service
- Configure BranchCache in Local Group Policy Editor
- Enable BranchCache for a file share

# Monitoring BranchCache

The BranchCache monitoring tools include:

- Get-BCStatus Windows Powershell cmdlet
- Netsh branchcache shows status command
- Event Viewer
- Performance monitor counters

# Lesson 3: Optimizing Storage Usage

- What Is FSRM?
- What Is File Classification Management?
- What Are File Classification Properties?
- What Is a File Classification Rule?
- Demonstration: How to Configure Classification Management
- Considerations for Using File Classification Options for Storage Optimization in Windows Server 2012
- Options for Storage Optimization
- Demonstration: Configuring Data Deduplication
- Storage Space Enhancements

# What Is FSRM?

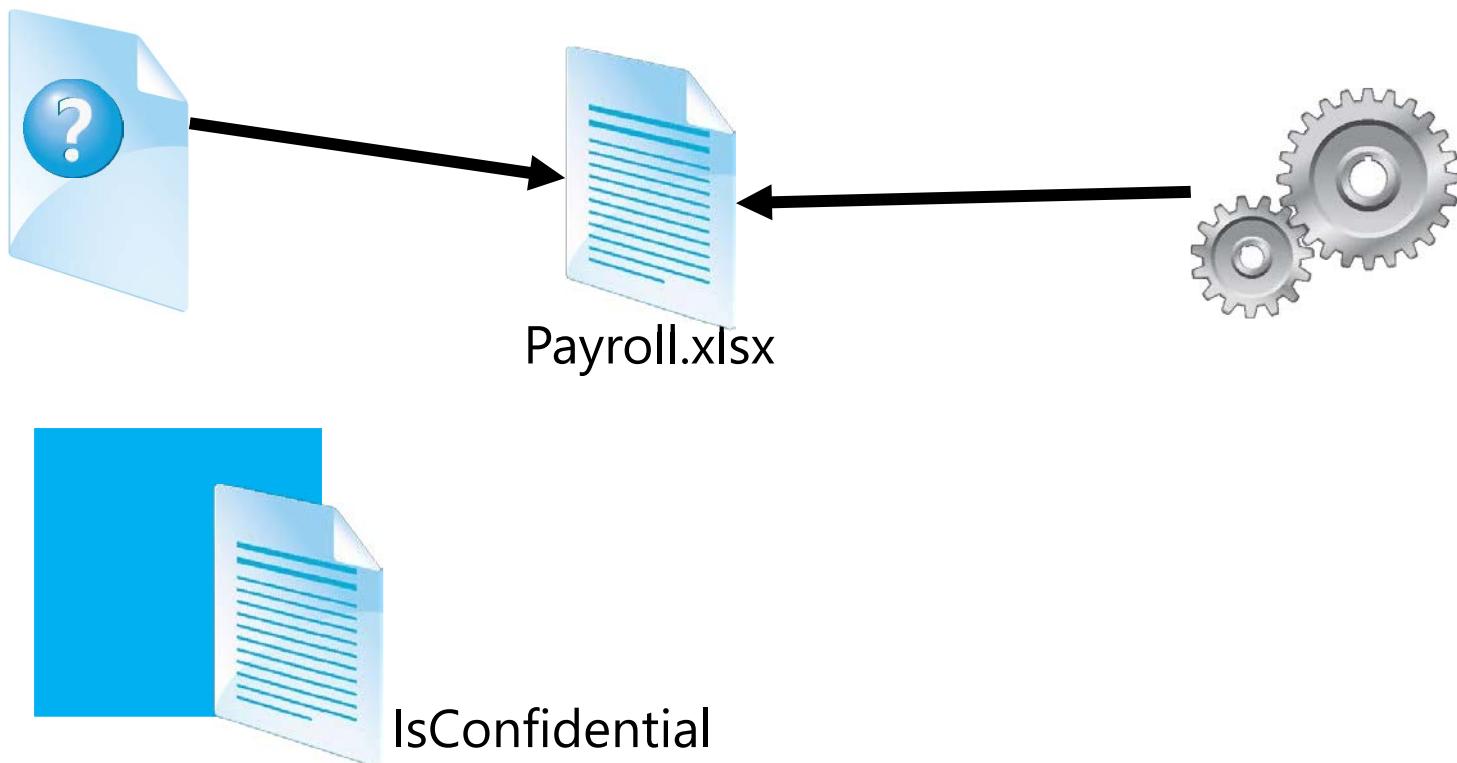
You can use the FSRM to manage and classify data that is stored on file servers

| FSRM features                                                                                                                                                                                                 | New FSRM features                                                                                                                                                                           |
|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• File classification infrastructure</li><li>• File management tasks</li><li>• Quota management</li><li>• File screening management</li><li>• Storage reports</li></ul> | <ul style="list-style-type: none"><li>• DAC</li><li>• Manual classification</li><li>• Access-denied assistance</li><li>• File management tasks</li><li>• Automatic classification</li></ul> |

# What Is File Classification Management?

- Classification management allows you to use an automated mechanism to create and assign classification properties to files

## Classification Rule



# What Are File Classification Properties?

Classification properties are configurable values that can be assigned to files

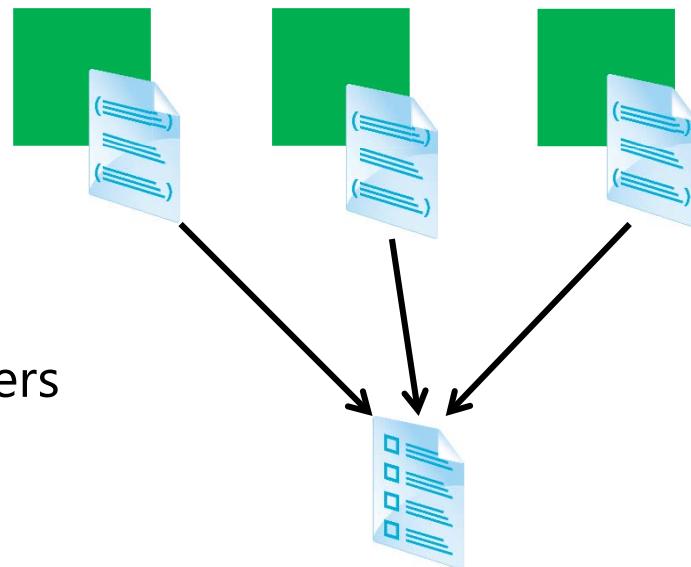
- Classification properties can be any of the following:
  - Yes/No
  - Date/Time
  - Number
  - Multiple choice list
  - Ordered list
  - String
  - Multi-string

# What Is a File Classification Rule?

A rule applies classification properties to files based on information about the file

A classification rule contains the following information:

- Rule enabled/disabled
- Rule scope
- Classification mechanism
- Property to assign
- Additional classification parameters



# Demonstration: How to Configure Classification Management

In this demonstration, you will see how to:

- Create a classification property
- Create a classification rule
- Modify the classification schedule

# Considerations for Using File Classification Options for Storage Optimization in Windows Server 2012

When using file classification, consider the following:

- How classification properties are stored
- Movement can affect a file classification's properties
- The classification management process exists only in Windows Server 2008 R2 and newer
- Classification rules can conflict
- Classification management cannot classify certain files

# Options for Storage Optimization

The following options are available for storage optimization:

- File access auditing allows for auditing of files for regulatory compliance, forensic analysis, monitoring, and troubleshooting access issues
- NFS data stores allows a Windows-based computer to act as an NFS server and share files in heterogeneous environments
- Data deduplication allows more data to be stored using less space by replacing redundant copies of files with a reference to a single copy

# Demonstration: Configuring Data Deduplication

In this demonstration, you will see how to:

- Add the Data Deduplication role service
- Enable data deduplication
- Test data deduplication

# Storage Space Enhancements

- Tiered storage uses a virtual disk that consists of at least one SSD and one hard disk drive
- Two tiers are created:
  - Faster Tier (all the SSDs)
  - Standard Tier (all the hard disk drives)
- Heavily accessed files are automatically moved to the faster tier
- Parallelized repair allows data to be rebuilt after a disk failure
- The virtual disk may be fixed or thin provisioned
- Thin provisioning and trim is enabled by default

# Lab A: Implementing Advanced File Services

- Exercise 1: Configuring iSCSI Storage
- Exercise 2: Configuring the File Classification Infrastructure

## Logon Information

|                   |                                                                                          |
|-------------------|------------------------------------------------------------------------------------------|
| Virtual machines: | 20412D-LON-DC1<br>20412D-LON-SVR1<br>20412D-LON-SVR2<br>20412D-LON-CL1<br>20412D-LON-CL2 |
| User name:        | <b>Adatum\Administrator</b>                                                              |
| Password:         | <b>Pa\$\$w0rd</b>                                                                        |

Estimated Time: 75 minutes

# Lab Scenario

As the A. Datum Corporation has expanded, the requirements for managing storage and shared file access have also expanded. Although the cost of storage has decreased significantly over recent years, the amount of data produced by the A. Datum business groups has increased even faster. The organization is considering alternate ways to decrease the cost of storing data on the network, and is considering options for optimizing data access in the new branch offices. The organization would also like to ensure that data that is stored on the shared folders is limited to company data, and that it does not include unapproved file types.

As a senior server administrator at A. Datum, you are responsible for implementing the new file storage technologies for the organization. You will implement iSCSI storage to provide a less complicated option for deploying large amounts of storage.

# Lab Review

- Why would you implement MPIO together with iSCSI? What problems would you solve with this approach?
- Why must you have the iSCSI initiator component?
- Why would you configure file classification for documents located in a folder such as a Corporate Documentation folder?

# Lab B: Implementing BranchCache

- Exercise 1: Configuring the Main Office Servers for BranchCache
- Exercise 2: Configuring the Branch Office Servers for BranchCache
- Exercise 3: Configuring Client Computers for BranchCache
- Exercise 4: Monitoring BranchCache

## Logon Information

|                   |                                                                       |
|-------------------|-----------------------------------------------------------------------|
| Virtual machines: | 20412D-LON-DC1<br>20412D-LON-SVR2<br>20412D-LON-CL1<br>20412D-LON-CL2 |
| User name:        | <b>Adatum\Administrator</b>                                           |
| Password:         | <b>Pa\$\$w0rd</b>                                                     |

Estimated Time: 40 Minutes

## Lab Scenario

The A. Datum Corporation has deployed a new branch office, which has a single server. To optimize file access in branch offices, you must configure BranchCache. To reduce WAN use out to the branch office, you must configure BranchCache to cache data retrieved from the head office. You will also implement FSRM to assist in optimizing file storage.

# Lab Review

- When would you consider implementing BranchCache into your own organization?

# Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools
- Best Practice

# Microsoft® Official Course



## Module 3

### Implementing Dynamic Access Control

**Microsoft®**

# Module Overview

- Overview of DAC
- Implementing DAC Components
- Implementing DAC for Access Control
- Implementing Access Denied Assistance
- Implementing and Managing Work Folders

# Lesson 1: Overview of DAC

- Limitations of Current Access Management Methods
- What Is DAC?
- What Is the Claim?
- What Are Resource Properties?
- Accessing Resources with DAC
- Requirements for DAC Implementation

# Limitations of Current Access Management Methods

- NTFS file system permissions and ACLs provide access control that is based on a user's SID or group membership SID
- AD RMS provides greater protection for documents by controlling how applications use them, and also works with user or group SID
- NTFS file system permissions cannot use AND between conditions
- In NTFS file system permissions, you cannot build your own conditions for access control

# What Is DAC?

- DAC in Windows Server 2012 is a new access control mechanism for file system resources
- DAC uses claims in the authentication token, resource properties on the resource, and conditional expressions within permission and auditing entries
- DAC is designed for four scenarios:
  - Central access policy for managing access to files
  - Auditing for compliance and analysis
  - Protecting sensitive information
  - Access-denied remediation

# What Is the Claim?

- A claim is something that AD DS states about a specific object
- In the DAC infrastructure, claims are defined by using specific attributes from a user or device
- In Windows Server 2012, the authorization mechanism is extended to support conditional expressions that includes claims
- In Windows Server 2012, you can create:
  - User claims
  - Device claims
- You can deploy claims between trusted forests

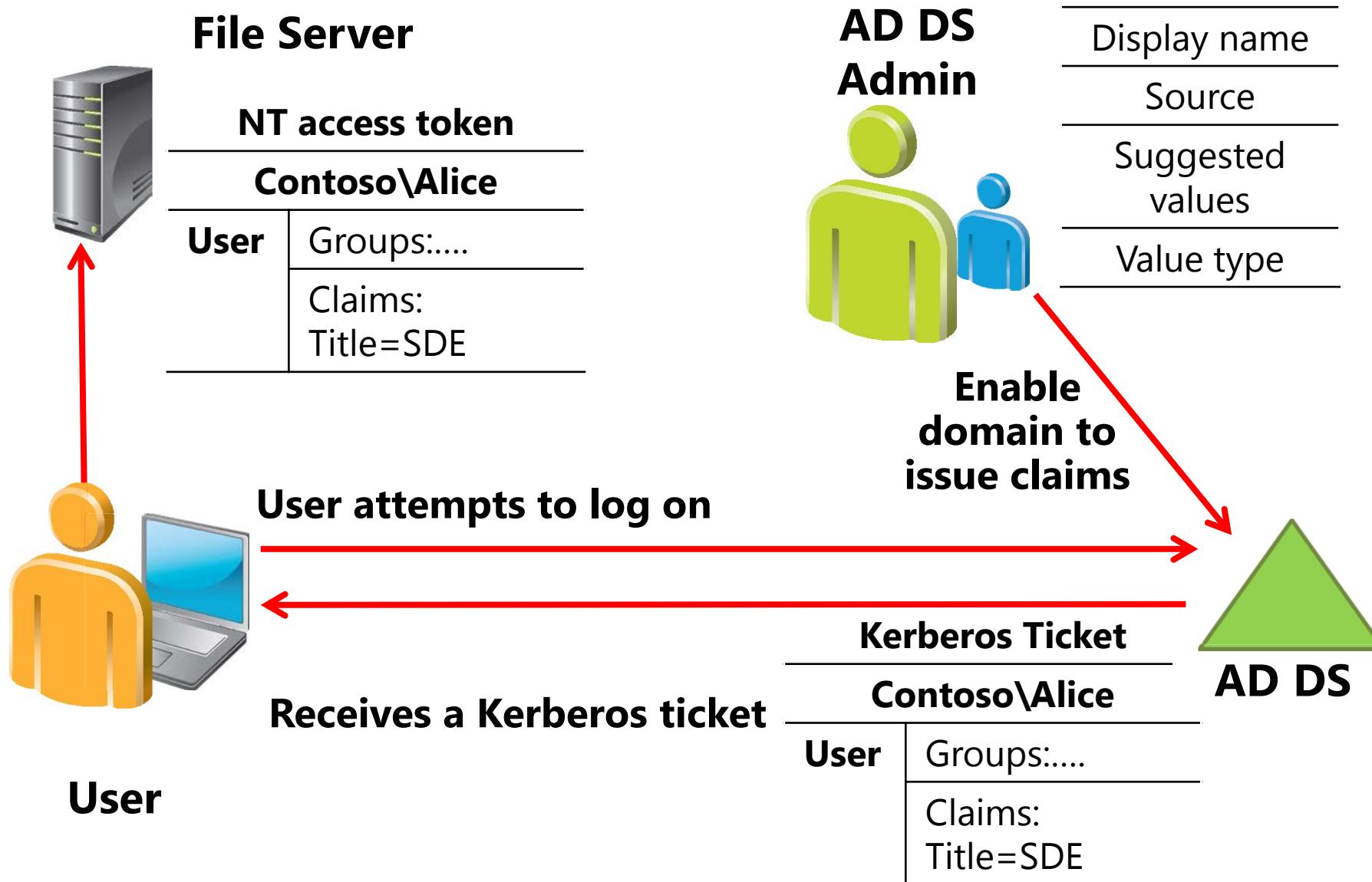
# User and Device Claims

- Pre-2012 Access Control approach:
  - Restricted to making policies where decisions are based on the user's group memberships
  - Shadow groups are often created to reflect existing attributes as groups
  - Groups that have rules around who can be members of which types of groups
  - Not able to transform groups across AD trust boundaries
  - Not able to control access based on characteristics of user's device
- Windows Server 2012 considerations:
  - AD DS user/computer attributes are included in the security token
  - Claims can be used directly in file server permissions
  - Claims are consistently issued to all users in a forest
  - Claims can be transformed across trust boundaries
  - Enables newer types of policies that were not possible before

# What Are Resource Properties?

- Resource properties define attributes of the resource that you want to use
- Resource properties are grouped in resource property lists
- When creating a resource property, you can specify the property type and the allowed or suggested values

# Accessing Resources with DAC



# Kerberos and a New Token

- DAC leverages Windows Kerberos
  - Windows 8 Kerberos extensions
  - Compound ID – binds a user to the device to be authorized as one principal
- DC issues groups and claims
  - DC enumerates user claims
  - Claims delivered in Kerberos Privilege Account Certificate
- NT Token has the following sections:
  - User & Device data
  - Claims and Groups
  - Tokens have same size

| 2012 Token   |              |
|--------------|--------------|
| User Account |              |
| User         | Groups       |
|              | Claims       |
| Device       | Groups       |
|              | Claims       |
|              | (other data) |

| Pre-2012 Token |  |
|----------------|--|
| User Account   |  |
| User Groups    |  |
| (other data)   |  |

# Requirements for DAC Implementation

To implement DAC, you need to have:

- Windows Server 2012 or newer with the FSRM
- Update AD DS schema, or at least one Windows Server 2012 domain controller
- Windows 8 or newer on clients to use device claims
- Enabled support for DAC in AD DS (default domain controllers GPO)

## Lesson 2: Implementing DAC Components

- Creating and Managing Claims
- Creating and Managing Resource Properties and Resource Property Lists
- Creating and Managing Access Control Rules
- Creating and Managing Access Policies
- Demonstration: Configuring Claims, Resource Properties, and Rules
- Implementing and Managing File Classifications
- Demonstration: Configuring Classification Rules

# Creating and Managing Claims

- Use the ADAC to create attribute-based claims
- Use the Active Directory module for Windows PowerShell to create certificate-based claims
- Claims are stored within the configuration partition in AD DS
- Attributes are used to source values for claims
- Make sure that you configure attributes for your computer and user accounts in AD DS with the information that is correct for the respective user or computer

# Creating and Managing Resource Properties and Resource Property Lists

- Resource properties describe resources that you protect with DAC
- Several resource properties are already predefined in Windows Server 2012
- All predefined resource properties are disabled
- When creating a new resource property, you have to set its name and value type
- In Windows Server 2012 R2, you also can create reference resource properties
- Resource properties are grouped in resource property lists

# Creating and Managing Access Control Rules

- A central access rule contains one or multiple criteria that the Windows operating system uses when evaluating access
- You create and configure central access rules in the Active Directory Administrative Center
- To create a new central access rule, you should:
  - Provide a name and description for the rule
  - Configure the target resources
  - Configure permissions

# Conditional Expression Example

User



AD DS



File  
Server



**User claims**  
`User.Department = Finance`  
`User.Clearance = High`

**Device claims**  
`Device.Department = Finance`  
`Device.Managed = True`

**Resource properties**  
`Resource.Department = Finance`  
`Resource.Impact = High`



**Access Rule**

Applies to: `@File.Impact = High`

`Allow | Read, Write | if (@User.Department = @File.Department) AND  
(@Device.Managed = True)`

# Creating and Managing Access Policies

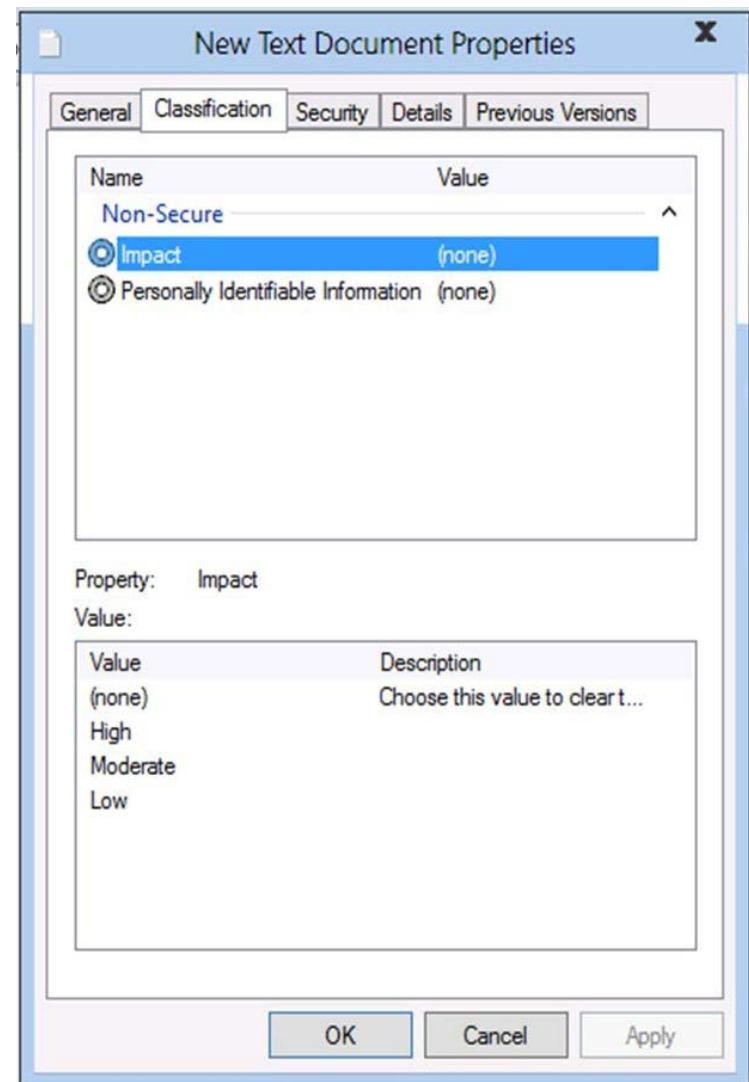
- Central access policies enable you to manage and deploy consistent authorization throughout an organization
- The main component of a central access policy is a central access rule
- Central access policies act as a security net that an organization applies across its servers
- Group Policy is used to deploy a central access policy
- Manually apply the policies to all Windows Server 2012 file servers, and configure folder security settings.

# Demonstration: Configuring Claims, Resource Properties, and Rules

In this demonstration, you will learn how to configure claims, resource properties, and access rules

# Implementing and Managing File Classifications

- Resource property definitions are defined in AD DS
- Resource property definitions can be used during file classifications
- File classifications can be run automatically



# Demonstration: Configuring Classification Rules

In this demonstration, you will learn how to classify files by using a file classification mechanism

# Lesson 3: Implementing DAC for Access Control

- Planning Central Access Policies for File Servers
- Demonstration: Creating and Deploying Central Access Policies
- How Does Access Check Work When DAC Is in Use
- Managing and Monitoring DAC
- Demonstration: Evaluating and Managing DAC

# Planning Central Access Policies for File Servers

When planning deployment of central access policies, you should:

- Identify the resources that you want to protect
- Define the authorization policies
- Translate the authorization policies that you require into expressions
- Identify attributes for access filtering

# Demonstration: Creating and Deploying Central Access Policies

In this demonstration, your instructor will show you how to create and deploy central access policy

# How Does Access Check Work When DAC Is in Use

Share  
security descriptor  
Share permissions



File/Folder  
security descriptor

Central access policy  
reference

NTFS file system  
permissions



AD DS  
(cached in local registry)

Cached central access policy definition

Cached central access rule

Cached central access rule

Cached central access rule

Access control decision is calculated by using following checks:

1. Access check – Share permissions if applicable
2. Access check – File permissions
3. Access check – Every matching central access rule in central access policy

# Managing and Monitoring DAC

- DAC allows you to test a central access policy update by staging it
- Windows Server 2012 staging:
  - Is implemented by deploying proposed permissions
  - Compares the proposed permissions against the current permissions
  - Causes audit-log events to appear in the security log on the file server

**Current Central Access policy for high impact data**

**Applies to: @File.Impact = High**

**Allow | Full Control | if @User.Company=Contoso**

**Staging policy**

**Applies to: @File.Impact = High**

**Allow | Full Control | if (@User.Company=Contoso) AND  
(@User.Clearance =High)**

# Sample Staging Event (4818)

Proposed Central Access Policy does not grant the same access permissions as the current Central Access Policy

Subject:

Security ID: CONTOSODOM\alice  
Account Name: alice  
Account Domain: CONTOSODOM

Object:

Object Server: Security  
Object Type: File  
Object Name: C:\FileShare\Finance\FinanceReports\FinanceReport.xls

Current Central Access Policy results:

Access Reasons: READ\_CONTROL: Granted by Ownership  
ReadAttributes: Granted by D:(A;ID;FA;;;BA)

Proposed Central Access Policy results that differ from the current Central Access Policy results:

Access Reasons: READ\_CONTROL: NOT Granted by CAR "HBI Rule"  
ReadAttributes: NOT Granted by CAR "HBI Rule"

# Demonstration: Evaluating and Managing DAC

In this demonstration, you will learn how to evaluate and manage DAC

# Lesson 4: Implementing Access Denied Assistance

- What Is Access Denied Assistance?
- Configuring Access Denied Assistance
- Demonstration: Implementing Access Denied Assistance

# What Is Access Denied Assistance?

On file server:

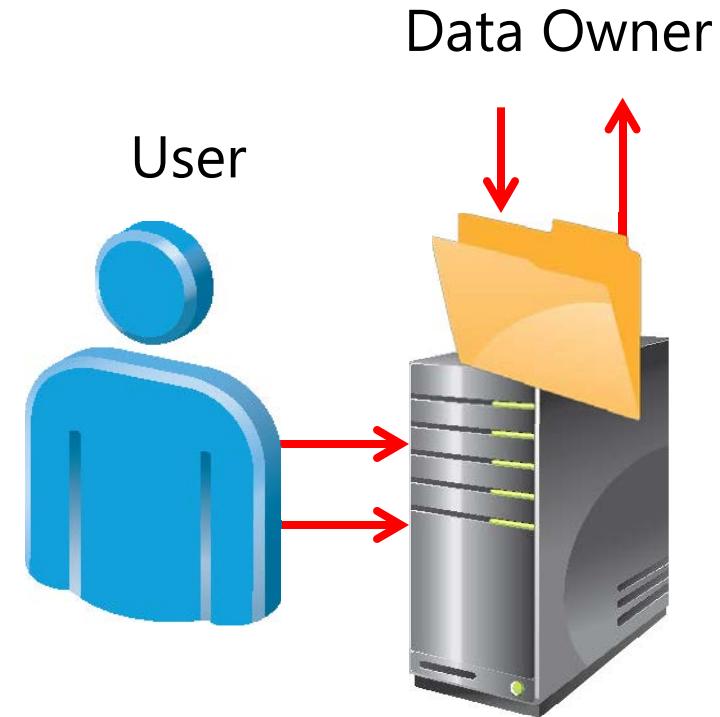
- Specify troubleshooting text for access denied
- Specify owner's email for share or folder

Access attempt:

- User is denied access, sees troubleshooting text or device-state troubleshooting
- User can request access via email

Data owner or help desk:

- Owner receives user's request
- Use effective permissions UI to decide appropriate actions
- Can forward request to IT admin



# Configuring Access Denied Assistance

- When implementing Access Denied Assistance:
  - Define messages that users will receive when they attempt to access resources
  - Determine whether users should be able to send a request for access
  - Determine recipients for the access-request email messages
  - Consider target operating systems
- Use Group Policy to enable and configure Access Denied Assistance
- Decide about the method for remediation

# Demonstration: Implementing Access Denied Assistance

In this demonstration, your instructor will show you how to configure and implement Access Denied Assistance

# Lesson 5: Implementing and Managing Work Folders

- What Are Work Folders?
- Configuring Work Folders
- Demonstration: Implementing Work Folders

# What Are Work Folders?

- Work Folders enable users to access business data securely at any location and on any device
- Work Folders are managed by administrators
- Currently supported on Windows 8.1 devices, and support also is planned for iOS-based devices

# Configuring Work Folders

To use Work Folders, you should:

- Have at least one Windows Server 2012 R2 file server
- Have at least one Windows Server 2012 R2 domain controller
- Install Work Folders functionality on file server
- Provision a share where users' data will be stored
- Run New Sync Share Wizard to create Work Folders structure
- Configure clients to use Work Folders by using Group Policy or manually

# Demonstration: Implementing Work Folders

In this demonstration, you will learn how to implement Work Folders

# Lab: Implementing Secure Data Access

- Exercise 1: Preparing for DAC Deployment
- Exercise 2: Implementing DAC
- Exercise 3: Validating and Remediating DAC
- Exercise 4: Implementing Work Folders

## Logon Information

Virtual machines: 20412D-LON-DC1, 20412D-LON-SVR1  
20412D-LON-SVR2, 20412D-LON-CL1, 20412D-LON-CL2

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 110 minutes

# Lab Scenario

You are working as an administrator at A. Datum Corporation. The company has a wide and complex file server infrastructure. It manages access control to folder shares by using NTFS file system ACLs, but in some cases, that approach does not provide the desired results.

Most of the files that departments use are stored in shared folders dedicated to specific departments, but confidential documents sometimes appear in other shared folders. Only members of the Research team should be able to access Research team folders, and only Executive department managers should be able to access highly confidential documents.

# Lab Scenario

The Security department also is concerned that managers are accessing files by using their home computers, which might not be highly secure. Therefore, you must create a plan for securing documents regardless of where they are located, and you must ensure that documents can be accessed only from authorized computers. Authorized computers for managers are members of the security group ManagersWks.

The Support department reports that a high number of calls are generated by users who cannot access resources. You must implement a feature that helps users understand error messages better and will enable them to request access automatically.

# Lab Scenario

Many users use personal devices such as tablets and laptops to work from home and while at work. You have to provide them with an efficient way to synchronize business data on all the devices that they use.

# Lab Review

- How do file classifications enhance DAC usage?
- Can you implement DAC without central access policy?

# Module Review and Takeaways

- Review Questions
- Tools
- Best Practices
- Common Issue and Troubleshooting Tip

# Microsoft® Official Course



## Module 4

### Implementing Distributed Active Directory® Domain Services Deployments

# Module Overview

- Overview of Distributed AD DS Deployments
- Deploying a Distributed AD DS Environment
- Configuring AD DS Trusts

# Lesson 1: Overview of Distributed AD DS Deployments

- Discussion: AD DS Components Overview
- Overview of Domain and Forest Boundaries in an AD DS Structure
- Why Implement Multiple Domains?
- Why Implement Multiple Forests?
- Integrating On-Premises AD DS with Cloud Services
- Implementing Windows Azure AD
- DNS Requirements for Complex AD DS Environments

# Discussion: AD DS Components Overview

- What is an AD DS domain?
- What is an AD DS tree?
- What is an AD DS forest?
- What is a trust relationship?
- What is the global catalog?

# Overview of Domain and Forest Boundaries in an AD DS Structure

| <b>AD DS object</b> | <b>Boundary type</b>                |
|---------------------|-------------------------------------|
| Domain              | Domain partition replication        |
|                     | Administrative permissions          |
|                     | Group Policy application            |
|                     | Auditing                            |
|                     | Password and account policies       |
|                     | Domain DNS zone replication         |
| Forest              | Security boundary                   |
|                     | Schema partition replication        |
|                     | Configuration partition replication |
|                     | Global catalog replication          |
|                     | Forest DNS zone replication         |

# Why Implement Multiple Domains?

Organizations may choose to deploy multiple domains to meet:

- Domain replication requirements
- DNS namespace requirements
- Distributed administration requirements
- Forest administrative group security requirements
- Resource domain requirements

# Why Implement Multiple Forests?

Organizations may choose to deploy multiple forests to meet:

- Security isolation requirements
- Incompatible schema requirements
- Multinational requirements
- Extranet security requirements
- Business merger or divestiture requirements

# Integrating On-Premises AD DS with Cloud Services

- Windows Azure AD:
  - Is a shared environment
  - Updating and upgrading is maintained by Microsoft
  - Can synchronize with on-premises AD DS
  - Does not support AD DS integrated applications
- AD in Windows Azure:
  - Is a private environment
  - Updating and upgrading is the responsibility of the customer
  - Can be part of on-premises AD DS
  - Supports AD DS-aware applications

# Implementing Windows Azure AD

The screenshot shows the Windows Azure portal interface. The left sidebar lists various service categories: ALL ITEMS, WEB SITES, VIRTUAL MACHINES, MOBILE SERVICES, CLOUD SERVICES, SQL DATABASES, STORAGE, NETWORKS, SQL REPORTING, ADD-ONS, SERVICE BUS, and MEDIA SERVICES. The ACTIVE DIRECTORY category is highlighted with a red border and contains a sub-item labeled '1'. The main content area is titled 'active directory' and includes tabs for 'DIRECTORY' and 'ACCESS CONTROL NAMESPACES'. A central message reads: 'You haven't created a directory. Create one to use organizational accounts or to integrate apps with Windows Azure AD.' Below this message is a red-bordered button labeled 'CREATE YOUR DIRECTORY'. At the bottom of the page are 'NEW', 'CREATE', and help/question icons.

Subscriptions keith@keithmayer.com

ALL ITEMS

WEB SITES

VIRTUAL MACHINES

MOBILE SERVICES

CLOUD SERVICES

SQL DATABASES

STORAGE

NETWORKS

SQL REPORTING

ADD-ONS

SERVICE BUS

MEDIA SERVICES

ACTIVE DIRECTORY 1

RECOVERY SERVICES

SETTINGS

active directory

DIRECTORY ACCESS CONTROL NAMESPACES

You haven't created a directory. Create one to use organizational accounts or to integrate apps with Windows Azure AD.

CREATE YOUR DIRECTORY

NEW

CREATE

# DNS Requirements for Complex AD DS Environments

When implementing DNS in a complex AD DS environment, you should:

- Verify the DNS client configuration
- Verify and monitor DNS name resolution
- Optimize DNS name resolution between multiple namespaces
- Use AD DS integrated DNS zones
- Consider deploying a GlobalNames zone
- Design interoperability for DNS in Windows Azure and on-premise

## Lesson 2: Deploying a Distributed AD DS Environment

- Demonstration: Installing a Domain Controller in a New Domain in an Existing Forest
- AD DS Domain Functional Levels
- AD DS Forest Functional Levels
- Upgrading a Previous Version of AD DS to Windows Server 2012 R2
- Migrating to Windows Server 2012 R2 AD DS from a Previous Version

# Demonstration: Installing a Domain Controller in a New Domain in an Existing Forest

In this demonstration, you will see how to:

- Configure an AD DS domain controller
- Access the AD DS domain controller

# AD DS Domain Functional Levels

New functionality requires that domain controllers are running a particular version of Windows

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows Server 2012 R2
- Cannot raise functional level while domain controllers are running previous Windows Server versions
- Cannot add domain controllers running previous Windows Server versions after raising functional level

# AD DS Forest Functional Levels

## Windows Server 2003:

- Forest trusts
- Domain rename
- Linked-value replication
- Support for RODCs
- Improved KCC
- Conversion of inetOrgPerson objects to user objects
- Deactivation and redefinition of attributes and object classes

## Windows Server 2008:

- No new features; sets minimum level for all new domains

## Windows Server 2008 R2:

- Active Directory Recycle Bin

## Windows Server 2012:

- No new features; sets minimum level for all new domains

## Windows Server 2012 R2:

- No new features; sets minimum level for all new domains

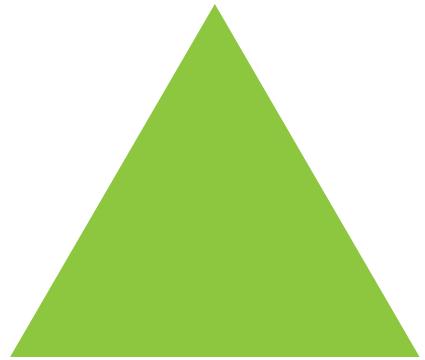
# Upgrading a Previous Version of AD DS to Windows Server 2012 R2

## Options to upgrade AD DS to Windows Server 2012 R2:

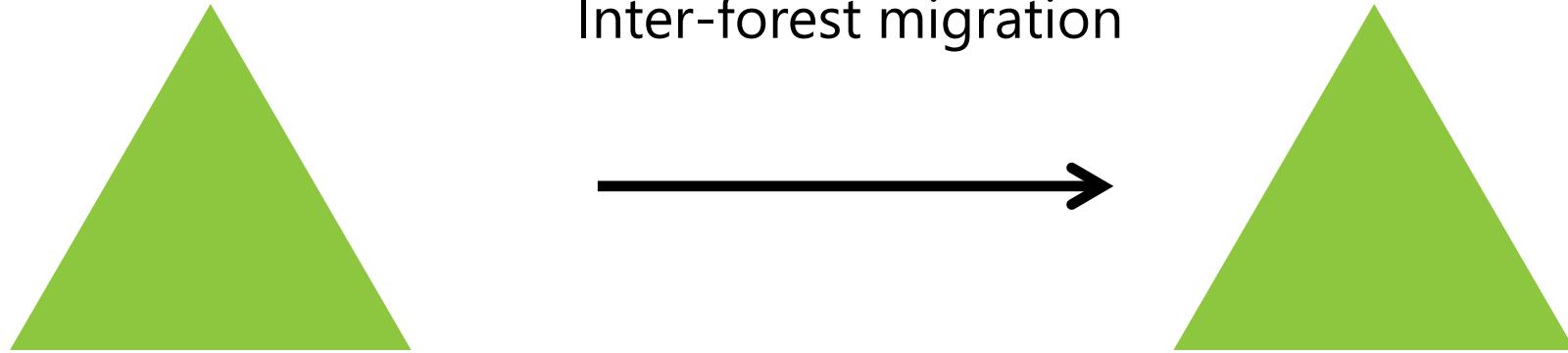
- In-place upgrade (from Windows Server 2008, Windows Server 2008 R2 or Windows 2012)
  - Only domain controllers running Windows Server 2008 x64, Windows Server 2008 R2, or Windows 2012 can be upgraded
- Introduce a new Windows Server 2012 R2 server into the domain and promote it to be a domain controller
  - This option is recommended
- Both options require that the schema is at the Windows Server 2012 R2 level
  - The Active Directory Domain Services Installation Wizard will upgrade the schema automatically when run with appropriate permissions
  - ADPrep is available

# Migrating to Windows Server 2012 R2 AD DS from a Previous Version

fabrikam.net



Adatum.com



Security Principals that are migrated:

- User accounts
- Managed service accounts
- Computer accounts
- Groups

Accounts get new SIDs, but resource access is maintained by using SID History

# Migrating to Windows Server 2012 R2 AD DS from a Previous Version

fabrikam.net

Adatum.com

|                   |                                               |
|-------------------|-----------------------------------------------|
| Department        | IT                                            |
| distinguishedName | CN=April Reagan,OU=IT,DC=fabrikam,DC=net      |
| givenName         | April                                         |
| name              | April Reagan                                  |
| objectSID         | S-1-5-21-322346712-1256085132-1900709958-1375 |

|                   |                                                          |
|-------------------|----------------------------------------------------------|
| Department        | IT                                                       |
| distinguishedName | CN=April Reagan,OU=IT,DC=Adatum,DC=com                   |
| givenName         | April                                                    |
| name              | April Reagan                                             |
| objectSID         | <b>NEW</b> S-1-5-21-433457823-2367196243-2011810069-2486 |
| sIDHistory        | S-1-5-21-322346712-1256085132-1900709958-1375            |

Security Principals that are migrated:

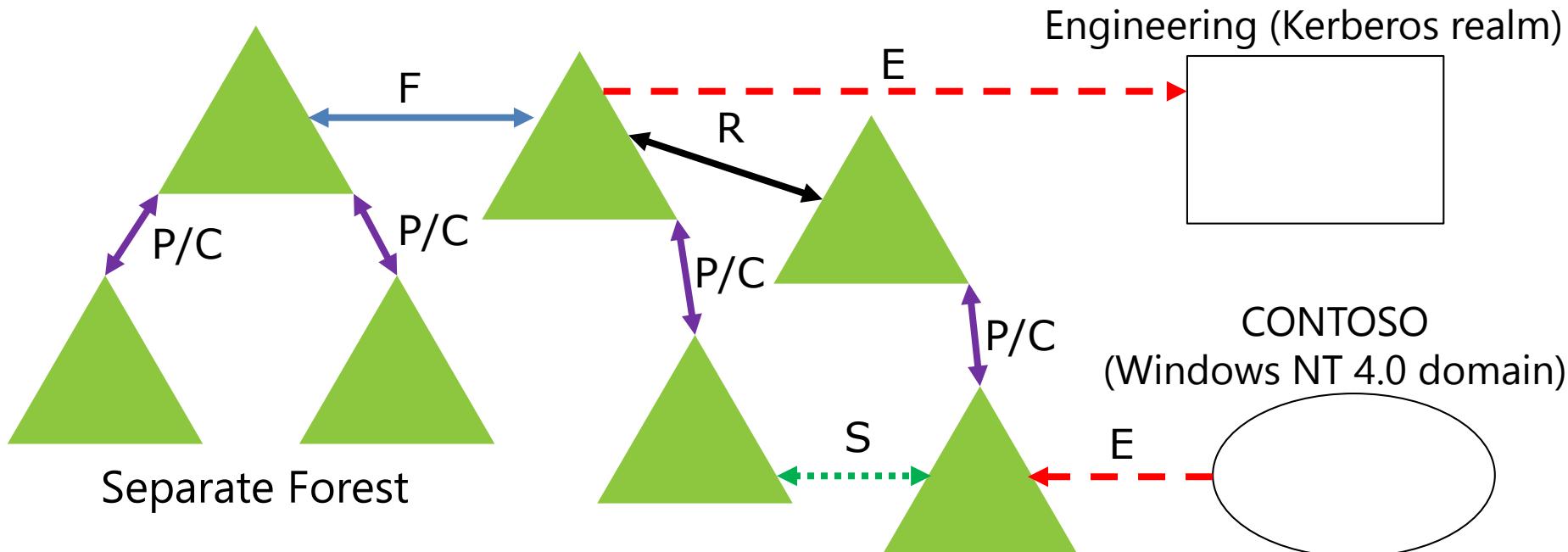
- User accounts
- Managed service accounts
- Computer accounts
- Groups

Accounts get new SIDs, but resource access is maintained by using SID History

# Lesson 3: Configuring AD DS Trusts

- Overview of Different AD DS Trust Types
- How Trusts Work Within a Forest
- How Trusts Work Between Forests
- Configuring Advanced AD DS Trust Settings
- Demonstration: Configuring a Forest Trust

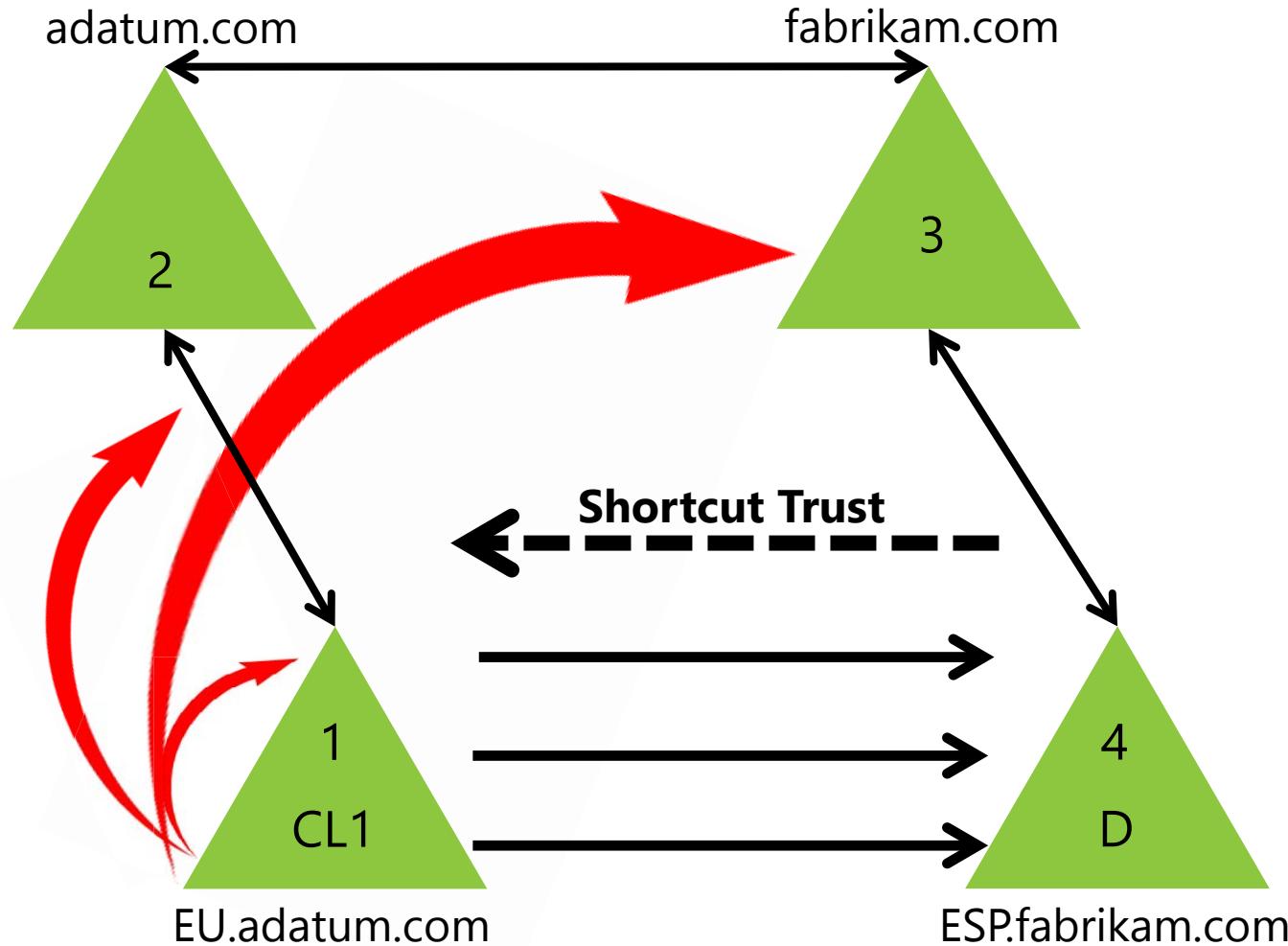
# Overview of Different AD DS Trust Types



| Trust type                              | Transitive? | Color        |
|-----------------------------------------|-------------|--------------|
| P/C - Parent-child                      | Yes         | Purple       |
| R - Tree root                           | Yes         | Black        |
| E - External (domain or Kerberos realm) | No          | Red/Dashed   |
| S - Shortcut                            | Yes         | Green/Dotted |
| F - Forest (complete or selective)      | Yes         | Blue         |



# How Trusts Work Within a Forest



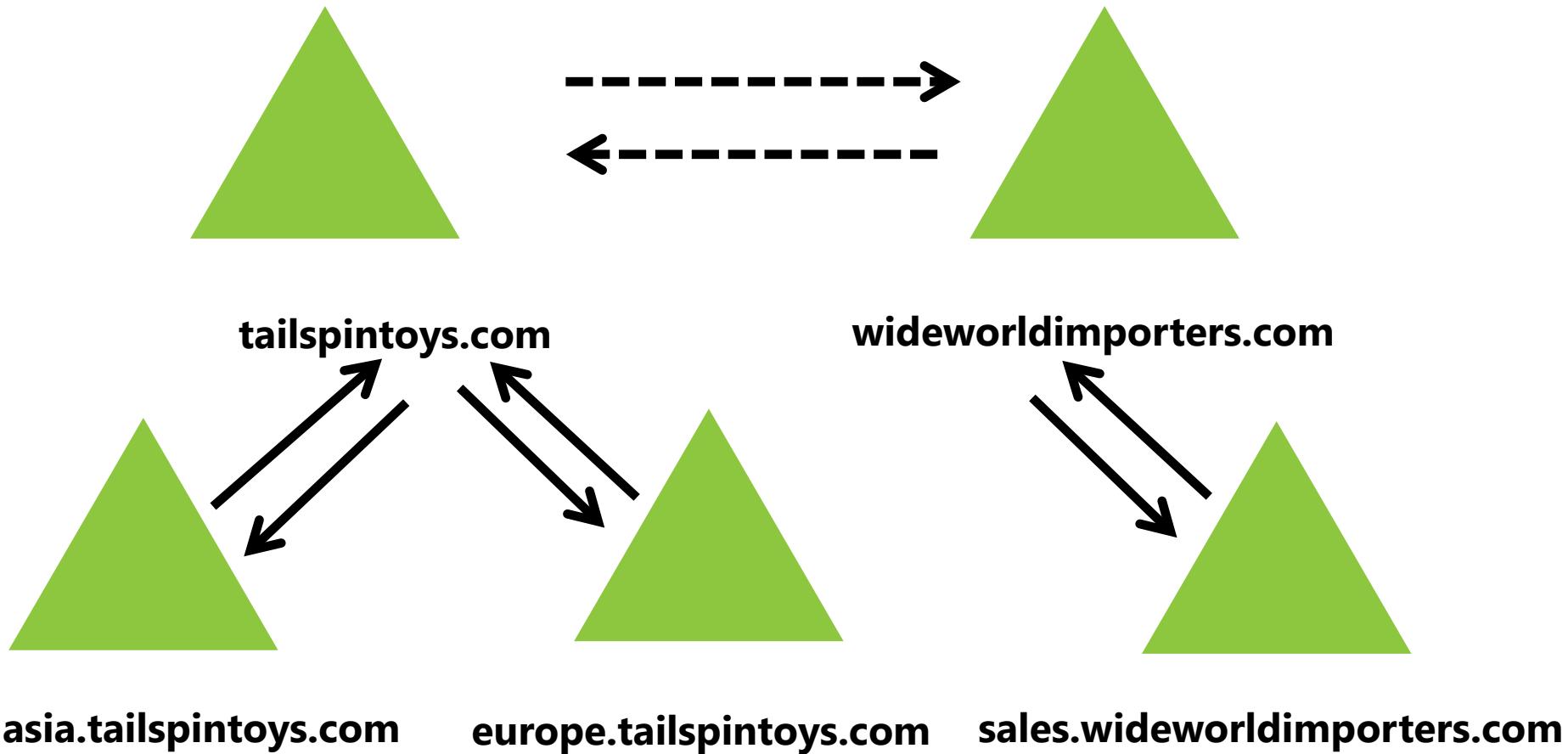
Client computer CL1 requests access to a file on File server D



# How Trusts Work Between Forests

## What Is a Forest Trust?

A forest trust is a one-way or two-way trust relationship between the forest root domains of two forests



# Configuring Advanced AD DS Trust Settings

Security considerations in forest trusts:

- SID filtering
- Selective authentication
- Name suffix routing

An incorrectly configured trust can allow unauthorized access to resources

# Demonstration: Configuring a Forest Trust

In this demonstration, you will see how to:

- Configure DNS Name Resolution by using a conditional forwarder
- Configure a two-way selective forest trust

# Lab: Implementing Distributed AD DS Deployments

- Exercise 1: Implementing Child Domains in AD DS
- Exercise 2: Implementing Forest Trusts

## Logon Information

Virtual Machines 20412D-LON-DC1,  
20412D-TOR-DC1,  
20412D-LON-SVR2,  
20412D-TREY-DC1

User Name: Adatum\Administrator  
Password: Pa\$\$w0rd

Estimated Time: 45 minutes

# Lab Scenario

A. Datum Corporation has deployed a single AD DS domain with all the domain controllers located in its London datacenter. As the company has grown and added branch offices with large numbers of users, it is becoming increasingly apparent that the current AD DS environment does not meet company requirements. The network team is concerned about the amount of AD DS-related network traffic that is crossing WAN links, which are becoming highly utilized.

The company has also become increasingly integrated with partner organizations, some of which need access to shared resources and applications that are located on the A. Datum internal network. The security department at A. Datum wants to ensure that the access for these external users is as secure as possible.

# Lab Scenario

As one of the senior network administrators at A. Datum, you are responsible for implementing an AD DS infrastructure that will meet the company requirements. You are responsible for planning an AD DS domain and forest deployment that will provide optimal services for both internal and external users, while addressing the security requirements at A. Datum.

# Lab Review

- Why did you configure a delegated subdomain record in DNS on LON-DC1 before adding the child domain na.adatum.com?
- What are the alternatives to creating a delegated subdomain record in the previous question?
- When you create a forest trust, why would you create a selective trust instead of a complete trust?

# Module Review and Takeaways

- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 5

### Implementing Active Directory Domain Services Sites and Replication

**Microsoft®**

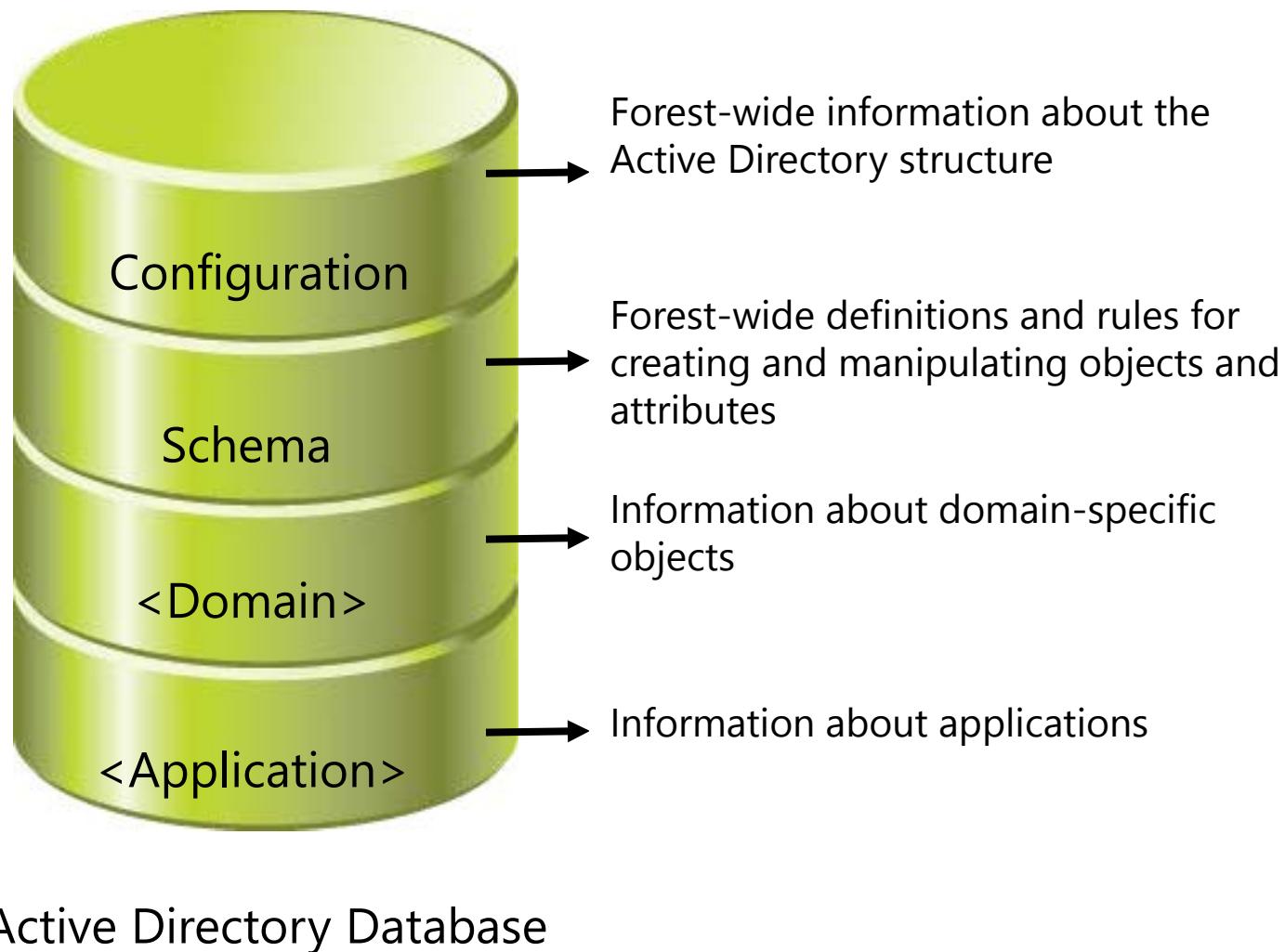
# Module Overview

- AD DS Replication Overview
- Configuring AD DS Sites
- Configuring and Monitoring AD DS Replication

# Lesson 1: AD DS Replication Overview

- What Are AD DS Partitions?
- Characteristics of AD DS Replication
- How AD DS Replication Works Within a Site
- Resolving Replication Conflicts
- How Replication Topology Is Generated
- How RODC Replication Works
- How SYSVOL Replication Works

# What Are AD DS Partitions?

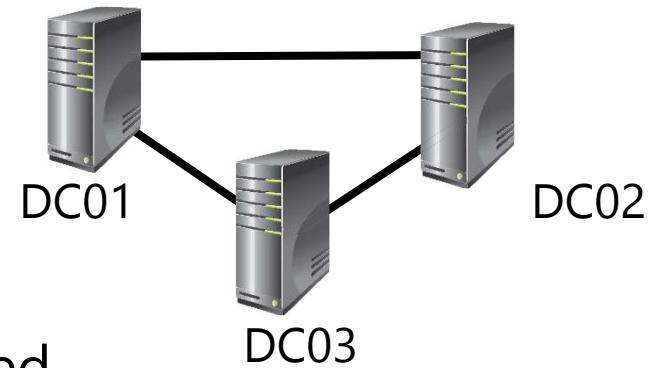


# Characteristics of AD DS Replication

- Multi-master replication ensures:
  - Accuracy (integrity)
  - Consistency (convergence)
  - Performance (keeping replication traffic to a reasonable level)
- Key characteristics of Active Directory replication include:
  - Multi-master replication
  - Pull replication
  - Store-and-forward
  - Partitions
  - Automatic generation of an efficient, robust replication topology
  - Attribute-level and multivalue replication
  - Distinct control of intrasite and intersite replication
  - Collision detection and remediation

# How AD DS Replication Works Within a Site

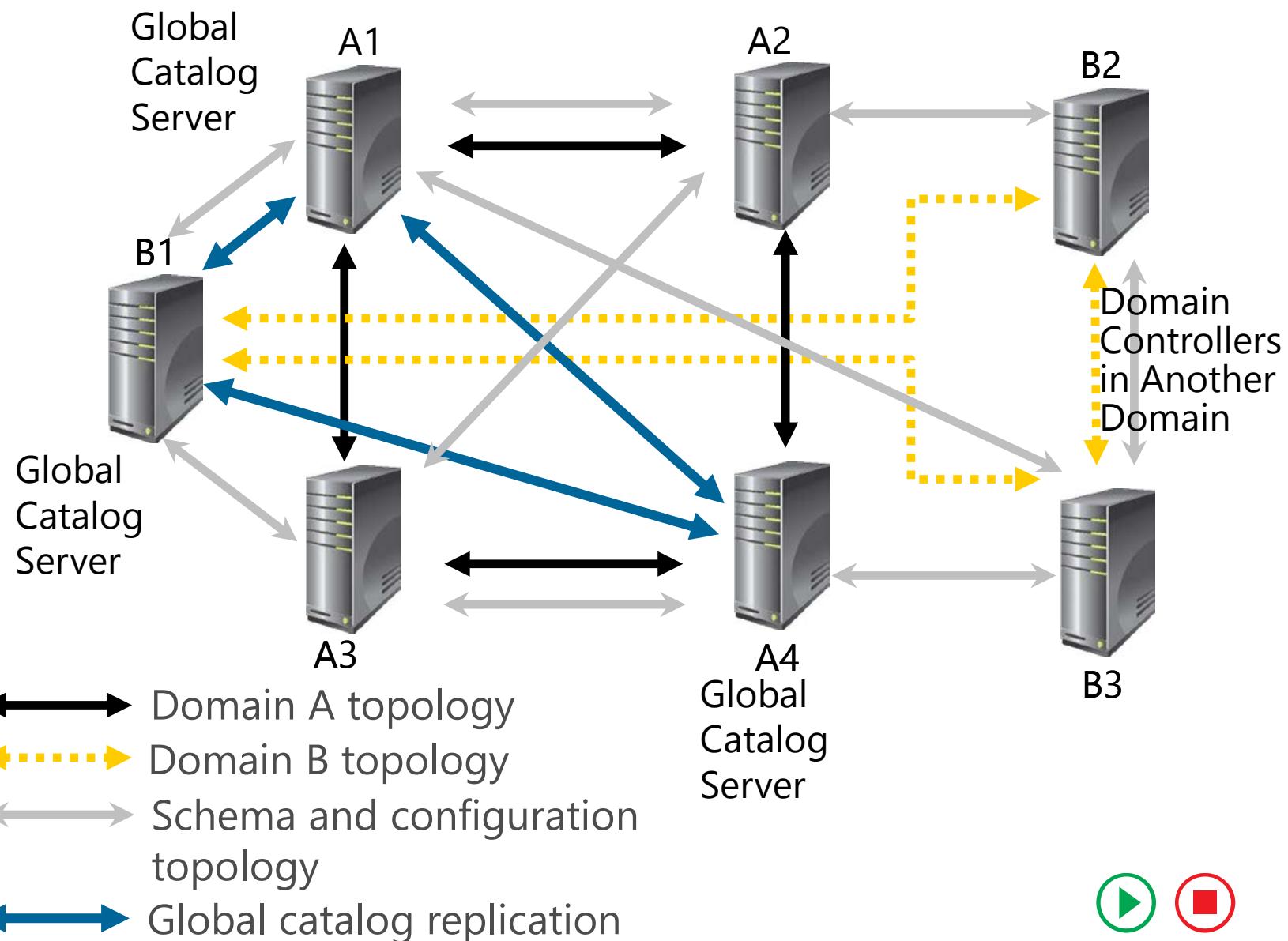
- Intrasite replication uses:
  - Connection objects for inbound replication to a domain controller
  - KCC to automatically create topology
    - Efficient (maximum three-hop) and robust (two-way) topology
  - Notifications in which the domain controller tells its downstream partners that a change is available
  - Polling, in which the domain controller checks with its upstream partners for changes
    - Downstream domain controller directory replication agent replicates changes
    - Changes to all partitions held by both domain controllers are replicated



# Resolving Replication Conflicts

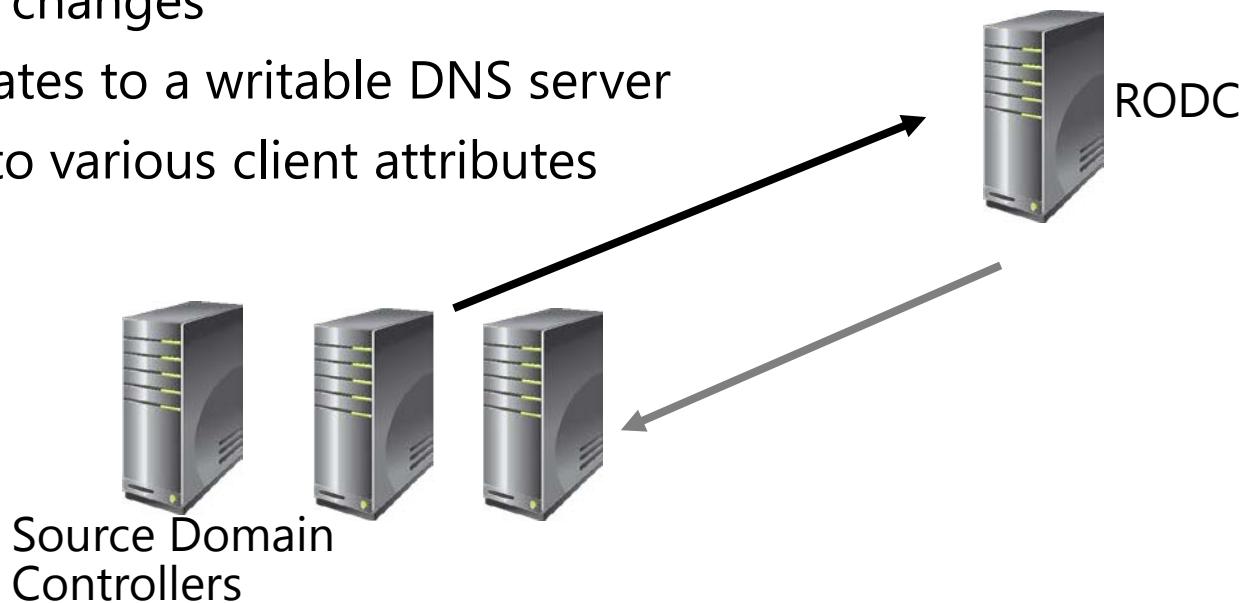
- In multi-master replication models, replication conflicts arise when:
  - The same attribute is changed on two domain controllers simultaneously
  - An object is moved or added to a deleted container on another domain controller
  - Two objects with the same relative distinguished name are added to the same container on two different domain controllers
- To resolve replication conflicts, AD DS uses:
  - Version number
  - Time stamp
  - Server GUID

# How the Replication Topology Is Generated



# How RODC Replication Works

- When an RODC is implemented:
  - The KCC detects that it is an RODC and creates one-way-only connection objects (black) from one or more source domain controllers
  - Write referrals are sent to the source domain controllers from the RODC (gray)
- An RODC performs Replicate Single Object inbound replication during:
  - Password changes
  - DNS updates to a writable DNS server
  - Updates to various client attributes



# How SYSVOL Replication Works

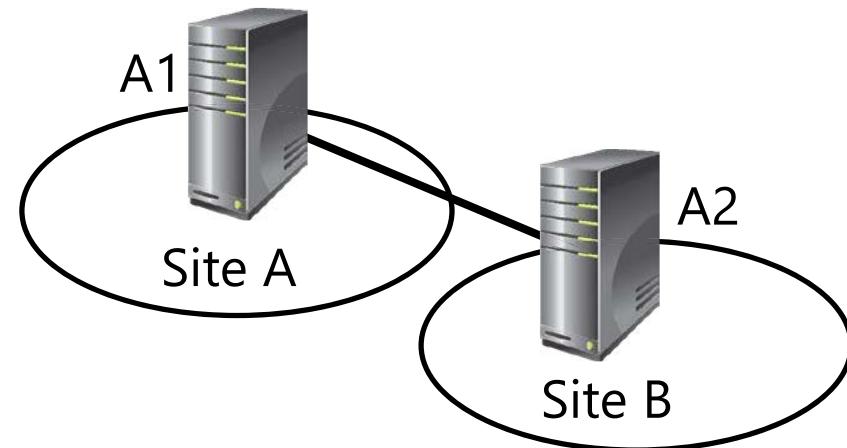
- SYSVOL contains logon scripts, Group Policy templates, and GPOs with their content
- SYSVOL replication can take place using:
  - FRS, which is primarily used in Windows Server 2003 and older domain structures
  - DFS Replication, which is used in Windows Server 2008 and newer domains
- To migrate SYSVOL replication from the FRS to DFS Replication:
  - The domain functional level must be at least Windows Server 2008
  - Use the Dfsrmig.exe tool to perform the migration

# Lesson 2: Configuring AD DS Sites

- What Are AD DS Sites?
- Why Implement Additional Sites?
- Demonstration: Configuring AD DS Sites
- How Replication Works Between Sites
- What Is the Intersite Topology Generator?
- Optimizing Domain Controller Coverage in Multiple Site Scenarios
- How Client Computers Locate Domain Controllers Within Sites

# What Are AD DS Sites?

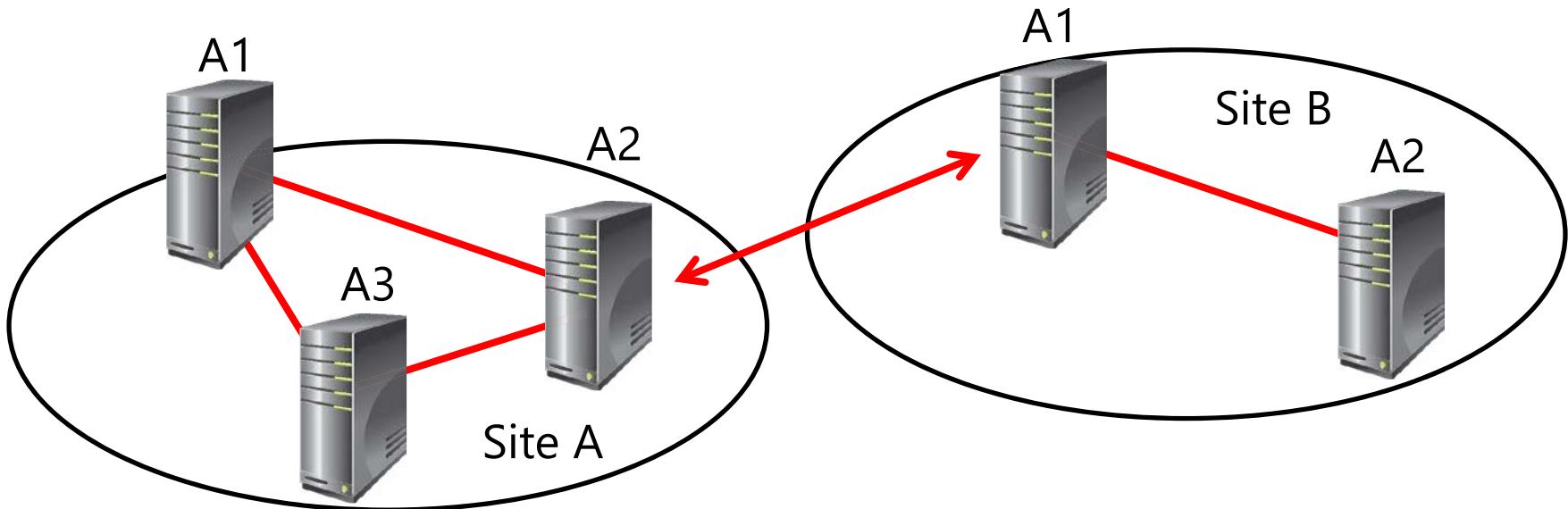
- Sites identify network locations with fast, reliable network connections
- Sites are associated with subnet objects
- Sites are used to manage:
  - Replication when domain controllers separated by slow, expensive links
  - Service localization:
    - Domain controller authentication (LDAP and Kerberos)
    - Active Directory-aware (site-aware) services or applications



# Why Implement Additional Sites?

Create additional sites when:

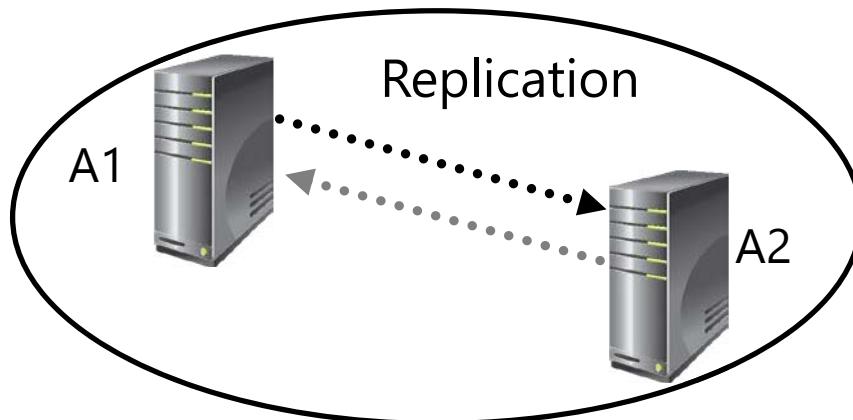
- A part of the network is separated by a slow link
- A part of the network has enough users to warrant hosting domain controllers or other services in that location
- You want to control service localization
- You want to control replication between domain controllers



# Demonstration: Configuring AD DS Sites

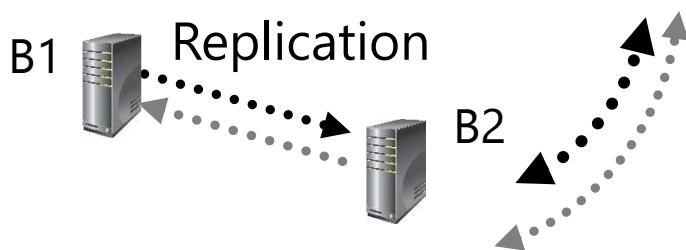
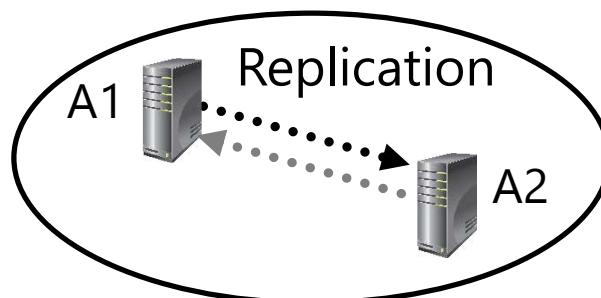
In this demonstration, you will see how to configure AD DS sites

# How Replication Works Between Sites



## Replication within sites:

- Assumes fast, inexpensive, and highly reliable network links
- Does not compress traffic
- Uses a change notification mechanism

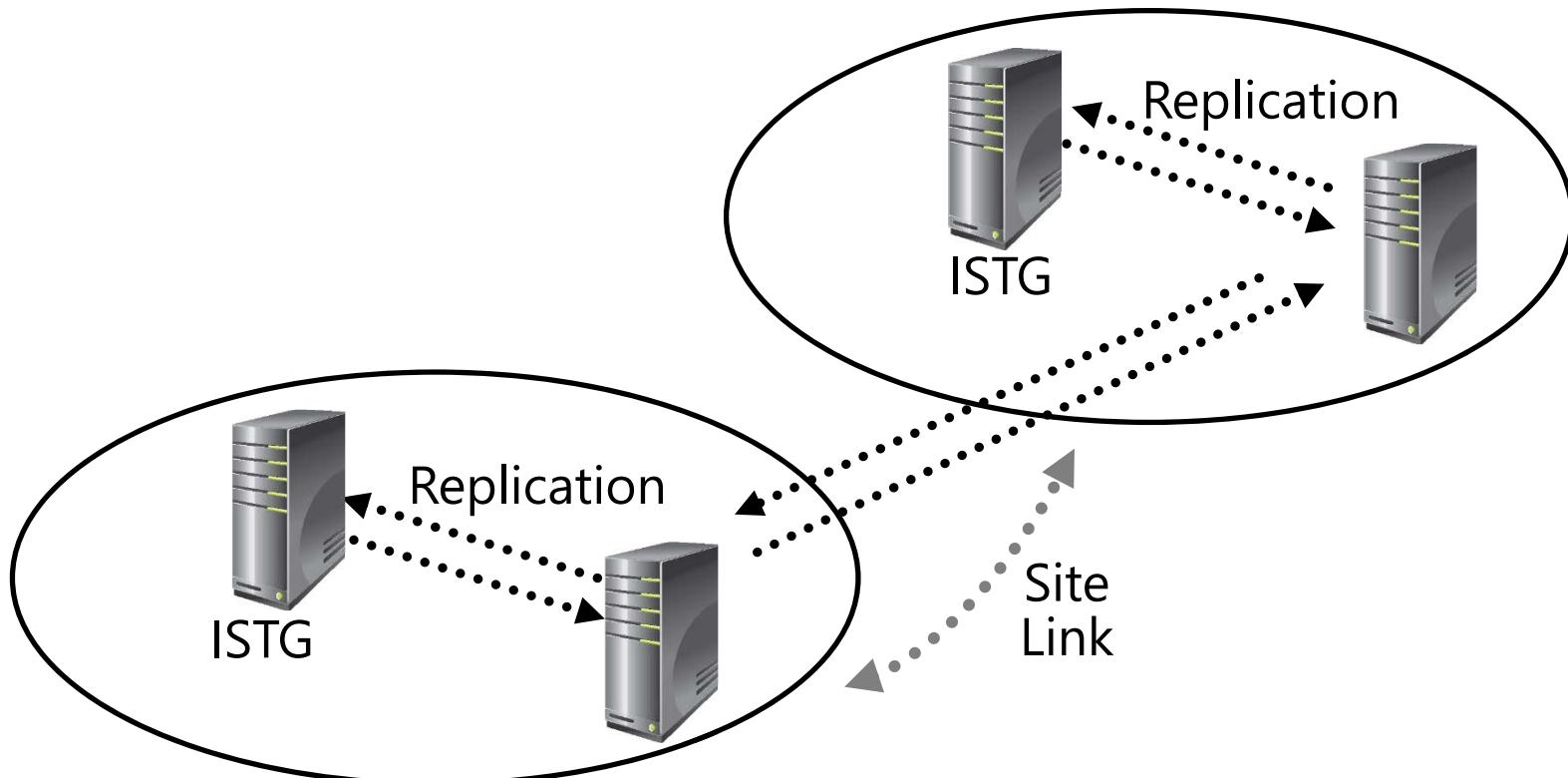


## Replication between sites:

- Assumes higher cost, limited bandwidth, and unreliable network links
- Has the ability to compress replication
- Occurs on a configured schedule
- Can be configured for immediate and urgent replications

# What Is the Intersite Topology Generator?

ISTG defines the replication between AD DS sites on a network



# Optimizing Domain Controller Coverage in Multiple Site Scenarios

- Domain controllers register SRV records as follows:
  - `_tcp.adatum.com`: All domain controllers in the domain
  - `_tcp.sitename._sites.adatum.com`: All services in a specific site
- Clients query DNS to locate services in specific sites

The screenshot displays the Windows Server Management Console with the DNS snap-in open. The left pane shows a hierarchical tree of DNS objects under the node 'LON-SVR2'. The tree includes 'Global Logs', 'Forward Lookup Zones' (containing '\_msdcs.Adatum.com' and 'Adatum.com'), 'Reverse Lookup Zones', 'Trust Points', and 'Conditional Forwarders'. The 'Adatum.com' zone has sub-zones for '\_msdcs' and '\_sites', which further contains 'LondonHQ' and 'Toronto' sub-zones, each with its own '\_tcp' and '\_udp' sub-zones. The 'DomainDnsZones' and 'ForestDnsZones' nodes are also visible. The right pane is a table titled 'Name' showing three Service Location (SRV) records:

| Name      | Type                   | Data                                |
|-----------|------------------------|-------------------------------------|
| _gc       | Service Location (SRV) | [0][100][3268] lon-svr2.adatum.com. |
| _kerberos | Service Location (SRV) | [0][100][88] lon-svr2.adatum.com.   |
| _ldap     | Service Location (SRV) | [0][100][389] lon-svr2.adatum.com.  |

# How Client Computers Locate Domain Controllers Within Sites

The process for locating a domain controller occurs as follows:

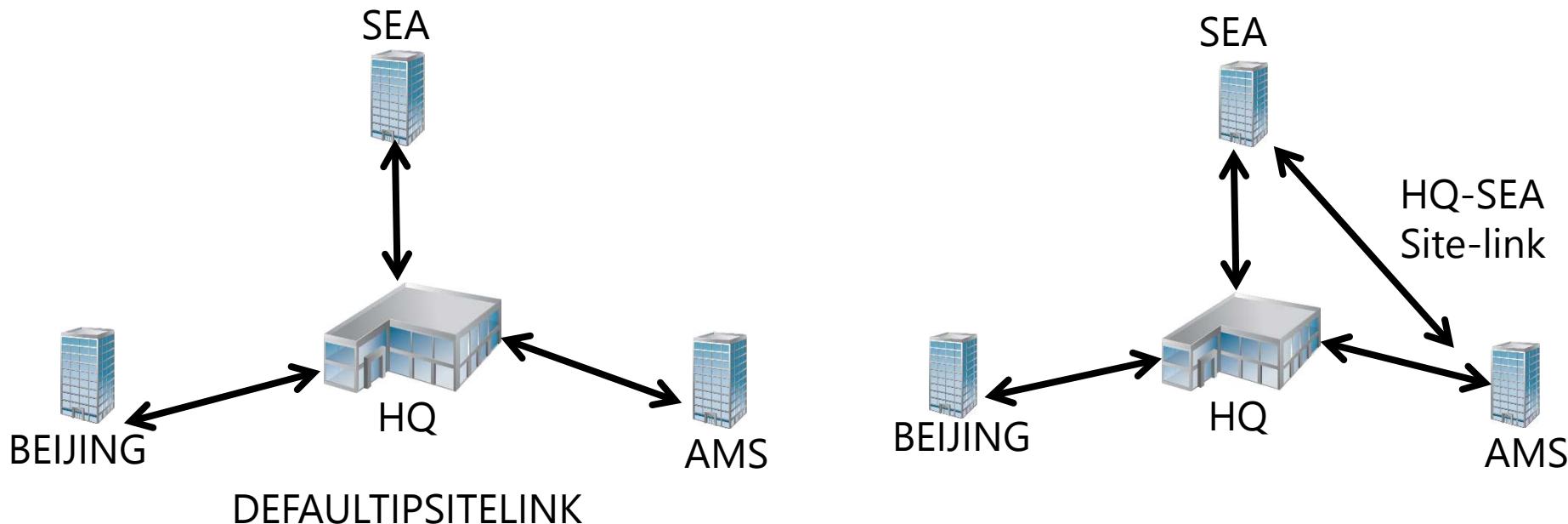
1. New client queries for all domain controllers in the domain
2. Client attempts LDAP ping to find all domain controllers
3. First domain controller responds
4. Client queries for all domain controllers in the site
5. Client attempts LDAP ping to find all domain controllers in the site
6. Client stores domain controller and site name for further use
7. Domain controller is used for the full logon process, including authentication, building the token, and building the list of GPOs to apply
  - Domain controller offline? Client queries for domain controllers in registry stored site
  - Client moved to another site? Domain controller refers client to another site

# Lesson 3: Configuring and Monitoring AD DS Replication

- What Are AD DS Site Links?
- What Is Site-Link Bridging?
- What Is Universal Group Membership Caching?
- Managing Intersite Replication
- Demonstration: Configuring AD DS Intersite Replication
- Best Practices When Deploying RODCs to Support Remote Sites
- Demonstration: Configuring Password Replication Policies
- Tools for Monitoring and Managing Replication

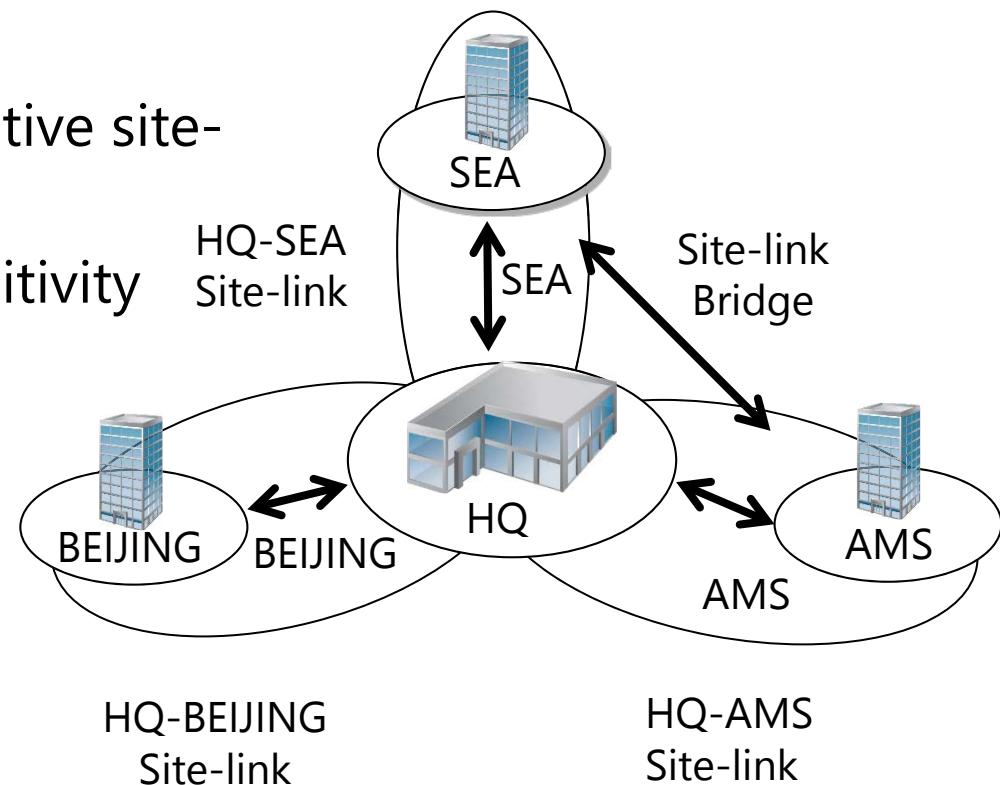
# What Are AD DS Site Links?

- Site-links contain sites:
  - Within a Site-link, a connection object can be created between any two domain controllers
  - The default Site-link, DEFAULTIPSITELINK, is not always appropriate given your network topology



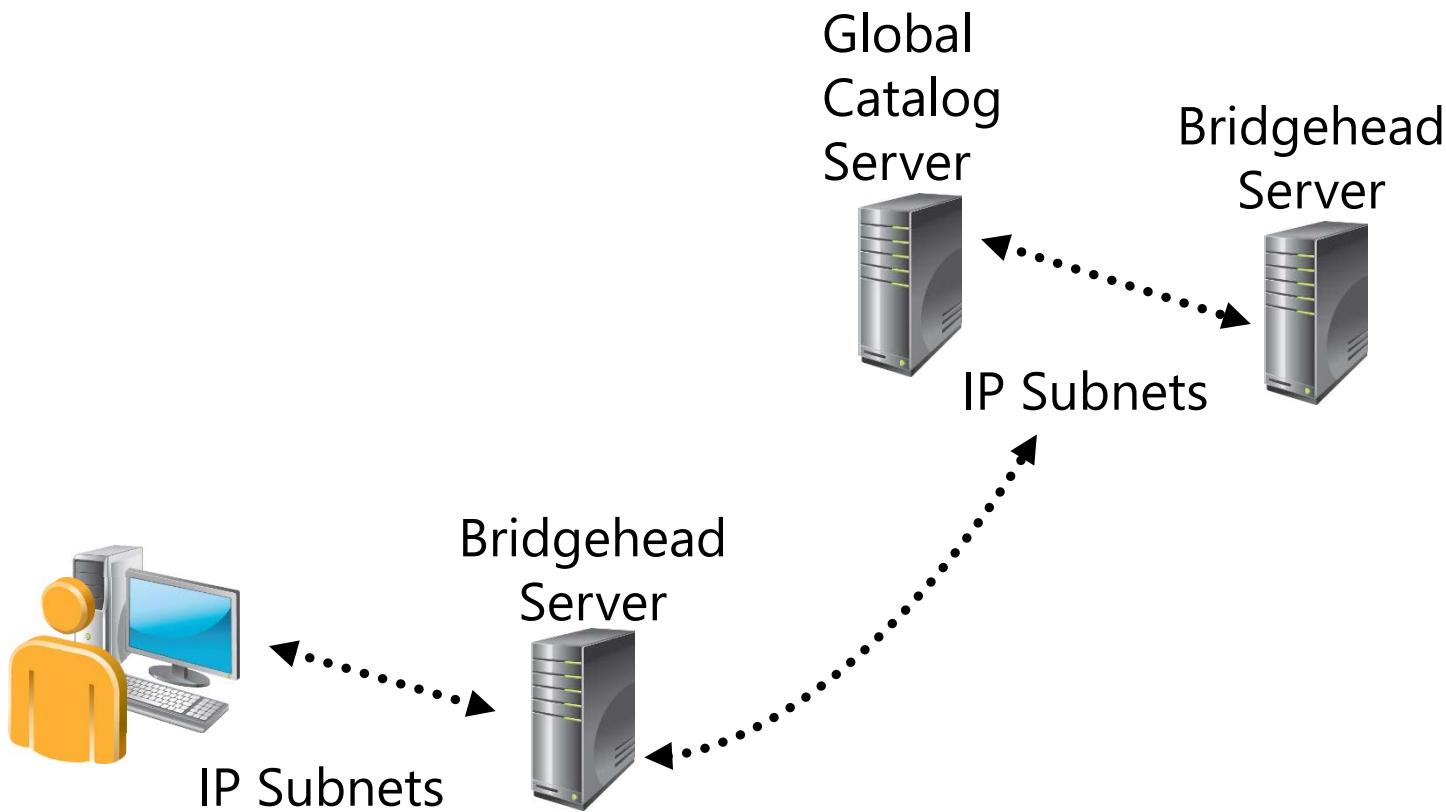
# What Is Site-Link Bridging?

- By default, automatic site-link bridging:
  - Enables ISTG to create connection objects between site-links
  - Allows disabling of transitivity in the properties of the IP transport
- Site-link bridges:
  - Enable you to create transitive site-links manually
  - Are useful only when transitivity is disabled



# What Is Universal Group Membership Caching?

Universal group membership caching enables domain controllers in a site with no global catalog servers to cache universal group membership



# Managing Intersite Replication

- Site-link costs:
  - Replication uses the connections with the lowest cost
- Replication:
  - Polling: Downstream bridgehead polls upstream partners
    - Default is 3 hours
    - Minimum is 15 minutes
    - Recommended is 15 minutes
  - Replication schedules:
    - 24 hours a day
    - Can be scheduled

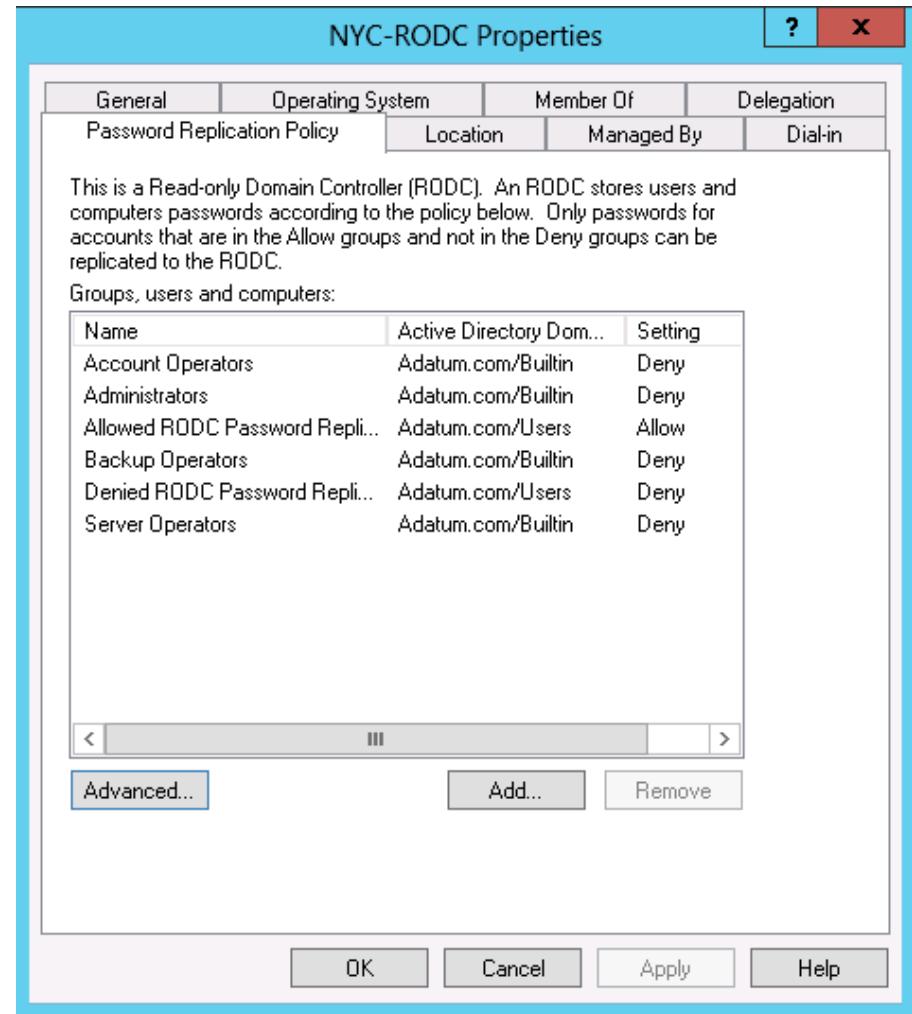
# Demonstration: Configuring AD DS Intersite Replication

In this demonstration, you will see how to configure AD DS intersite replication

# Best Practices When Deploying RODCs to Support Remote Sites

Password replication policies are:

- Used to determine which users' credentials should be cached on the RODC
- Determined by the Allowed List and the Denied List



# Demonstration: Configuring Password Replication Policies

In this demonstration, you will see how to configure password replication policies

# Tools for Monitoring and Managing Replication

- **Readmin.exe examples:**

- repadmin /showrepl Lon-dc1.adatum.com
- repadmin /showconn Lon-dc1 adatum.com
- repadmin /showobjmeta Lon-dc1 "cn=Linda Miller,ou=..."
- repadmin /kcc

- **Dcdiag.exe /test:*testName*:**

- FrsEvent or DFSREvent
- Intersite
- KccEvent
- Replications
- Topology

- Monitor replication with Operations Manager

- Windows PowerShell

# Lab: Implementing AD DS Sites and Replication

- Exercise 1: Modifying the Default Site
- Exercise 2: Creating Additional Sites and Subnets
- Exercise 3: Configuring AD DS Replication
- Exercise 4: Monitoring and Troubleshooting AD DS Replication

Logon Information

Virtual machines: 20412D-LON-DC1

20412D-TOR-DC1

User Name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 45 minutes

# Lab Scenario

A. Datum Corporation has deployed a single AD DS domain, with all the domain controllers located in the London data center. As the company has grown and added branch offices with large numbers of users, it has become apparent that the current AD DS environment does not meet the company requirements. Users in some branch offices report that it can take a long time for them to sign in on their computers. Access to network resources such as the company's Microsoft Exchange® 2013 servers and the Microsoft SharePoint® servers can be slow, and they fail sporadically. As one of the senior network administrators, you are responsible for planning and implementing an AD DS infrastructure that will help address the business requirements for the organization. You are responsible for configuring AD DS sites and replication to optimize the user experience and network utilization within the organization.

# Lab Review

- You decide to add a new domain controller to the LondonHQ site named LON-DC2. How can you ensure that LON-DC2 is used to pass all replication traffic to the Toronto site?
- You have added the new domain controller named LON-DC2 to the LondonHQ site. Which AD DS partitions will be modified as a result?
- In the lab, you created a separate site-link for the Toronto and TestSite sites. What might you also have to do to ensure that LondonHQ does not create a connection object directly with the TestSite site automatically?

# Module Review and Takeaways

- Review Questions
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 6 Implementing AD CS

**Microsoft®**

# Module Overview

- Using Certificates in a Business Environment
- PKI Overview
- Deploying CAs
- Deploying and Managing Certificate Templates
- Implementing Certificate Distribution and Revocation
- Managing Certificate Recovery

# Lesson 1: Using Certificates in a Business Environment

- Using Certificates for SSL
- Using Certificates for Digital Signatures
- Demonstration: Signing a Document Digitally
- Using Certificates for Content Encryption
- Using Certificates for Authentication

# Using Certificates for SSL

- The purpose of securing a connection with SSL is to protect data during communication
- For SSL, a certificate must be installed on the server
- Be aware of trust issues
- The SSL works in the following steps:
  1. The user types an HTTPS URL
  2. The web server sends its SSL certificate
  3. The client performs a check of the server certificate
  4. The client generates a symmetric encryption key
  5. The client encrypts this key with the server's public key
  6. The server uses its private key to decrypt the encrypted symmetric key
- Make sure that you configure the SSL certificate properly

# Using Certificates for Digital Signatures

- Digital signatures ensure:
  - Content is not modified during transport
  - The identity of the author is verifiable
- Digital signatures work in the following steps:
  1. When an author digitally signs a document or a message, the operating system on his or her machine creates a message cryptographic digest
  2. The cryptographic digest is then encrypted by using author's private key and added to the end of the document or message
  3. The recipient uses the author's public key to decrypt the cryptographic digest and compare it to the cryptographic digest created on the recipient's machine
- Users need to have a certificate based on a User template to use digital signatures

# Demonstration: Signing a Document Digitally

In this demonstration, your instructor will show you how to digitally sign a document in Microsoft Word

# Using Certificates for Content Encryption

- Encryption protects data from unauthorized access
- EFS uses certificates for file encryption

Header

File encryption key:  
Encrypted with the file owner's public key

File encryption key:  
Encrypted with the public key of Recovery agent 1

File encryption key:  
Encrypted with the public key of Recovery agent 2 (optional)

•  
•  
•  
•

Encrypted Data

Data Recovery Fields

# Using Certificates for Authentication

You can use certificates for user and device authentication, and in network and application access scenarios such as:

- L2TP/IPsec VPN
- EAP-TLS
- Protected Extensible Authentication Protocol
- NAP with IPsec
- Outlook Web App
- Mobile device authentication

## Lesson 2: PKI Overview

- What Is PKI?
- Components of a PKI Solution
- What Are CAs?
- Overview of the AD CS Server Role in Windows Server 2012
- New Features of AD CS in Windows Server 2012
- Public vs. Private CAs
- What Is a Cross-Certification Hierarchy?

# What Is PKI?

## PKI :

- Is a standard approach to security-based tools, technologies, processes, and services that are used to enhance the security of communications, applications, and business transactions
- Relies on the exchange of digital certificates between users and trusted resources

## PKI provides:

- Confidentiality
- Integrity
- Authenticity
- Nonrepudiation

# Components of a PKI Solution



CA



Digital Certificates



Certificate Templates



CRLs and Online Responders



Public Key–Enabled Applications and Services



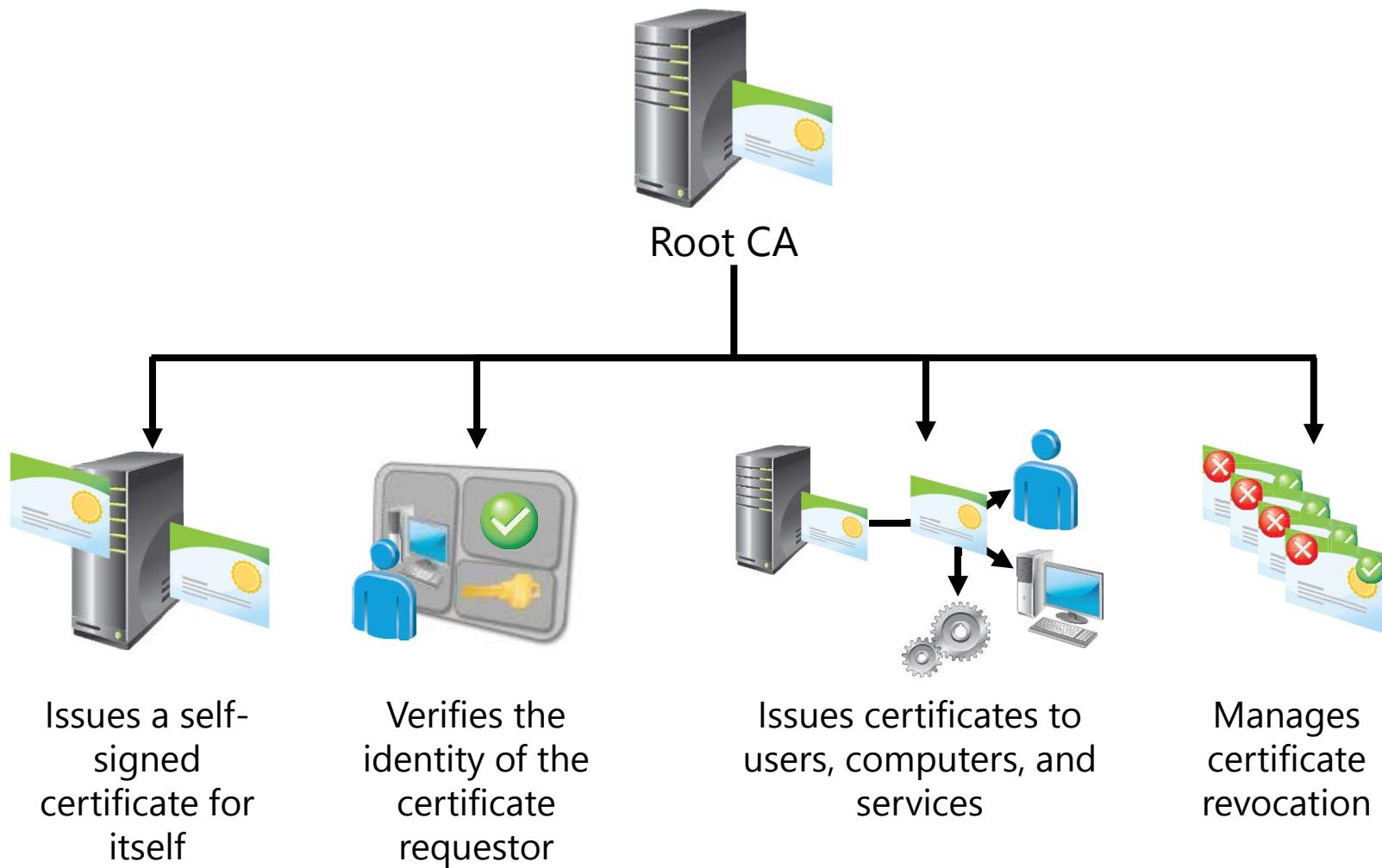
Certificates and CA Management Tools



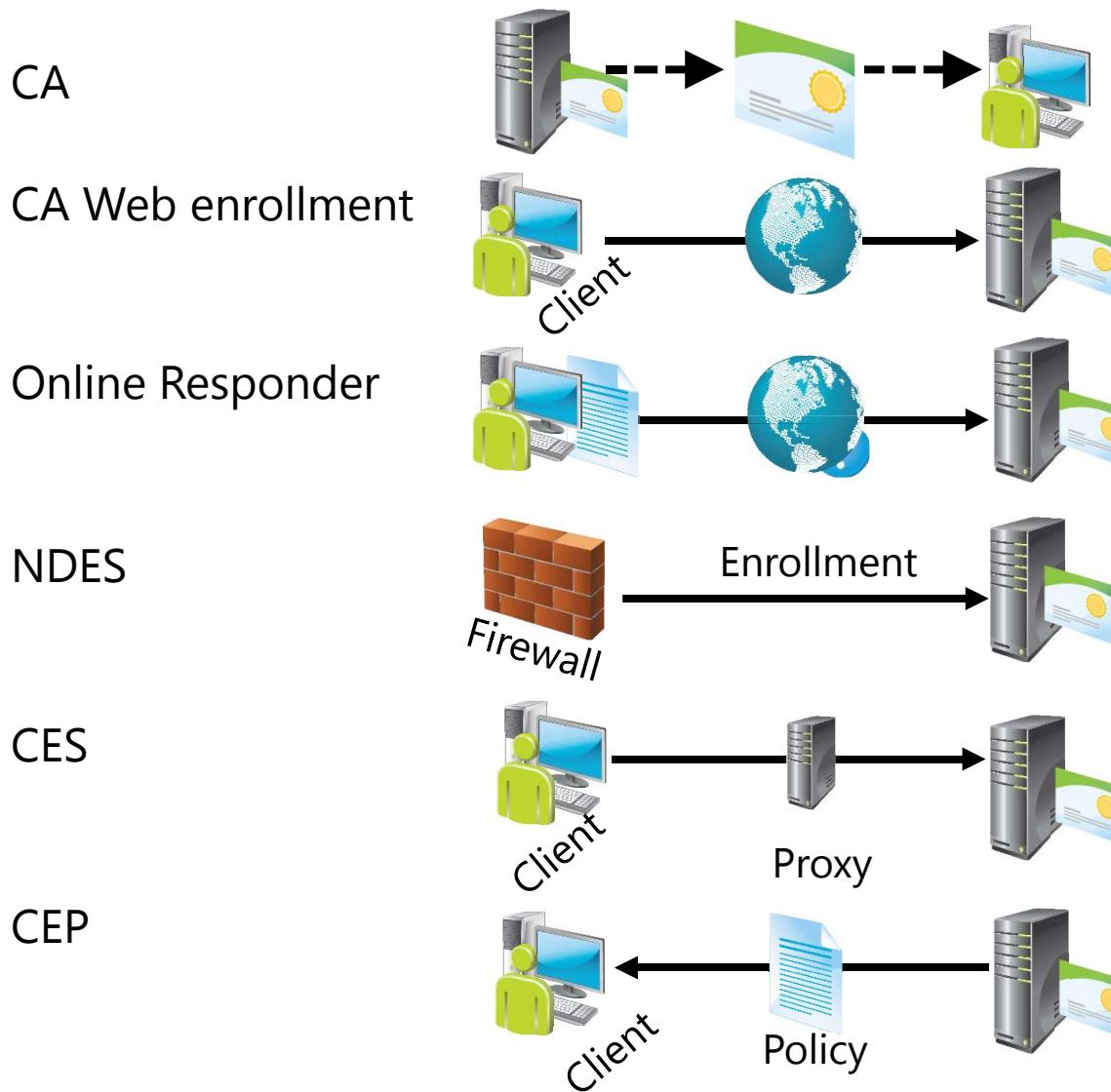
AIA and CDPs



# What Are CAs?



# Overview of the AD CS Server Role in Windows Server 2012



# New Features of AD CS in Windows Server 2012

- All AD CS role services run on all versions of Windows Server
- Full integration with Server Manager
- Manageable through Windows PowerShell
- New certificate template version (v4)
- Support for automatic renewal of certificates for non-domain joined computers
- Enforcement of certificate renewal with the same key
- Additional security for certificate requests
- Support for Virtual Smart Cards

# Public vs. Private CAs

## Internal private CAs:

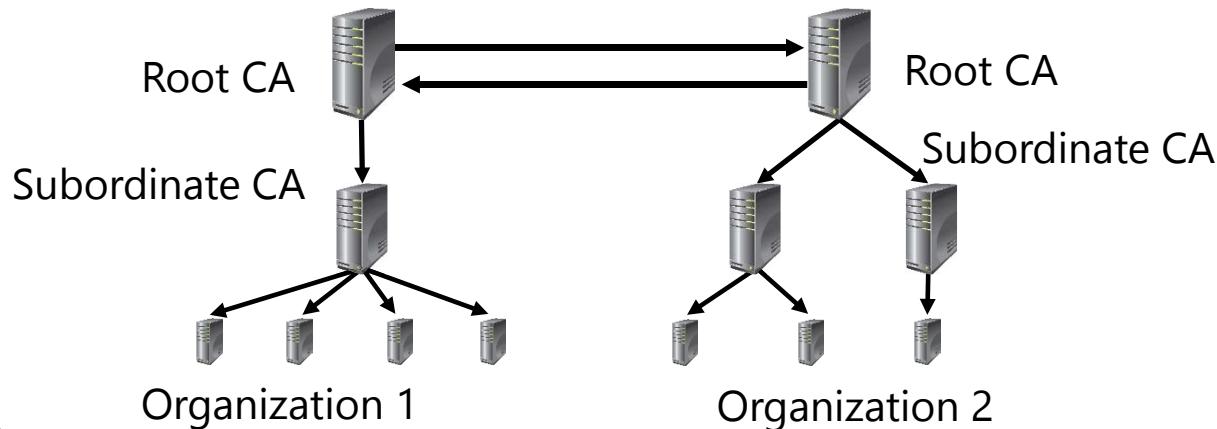
- Require greater administration than external public CAs
- Cost less than external public CAs, and provide greater control over certificate management
- Are not trusted by external clients by default
- Offer advantages such as customized templates and autoenrollment

## External public CAs:

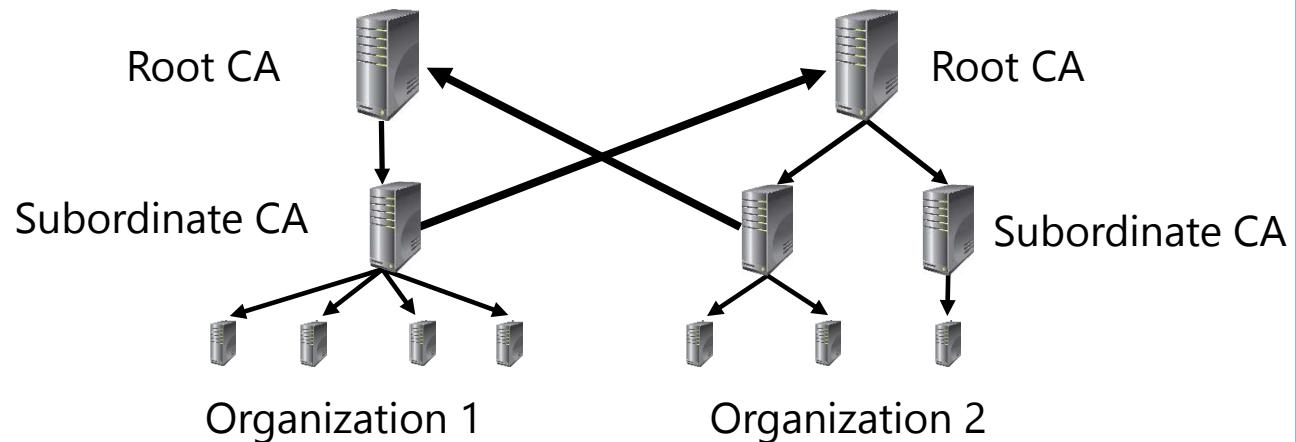
- Are trusted by many external clients
- Have slower certificate procurement

# What Is a Cross-Certification Hierarchy?

Cross-Certification at the Root CA Level



Cross-Certification Subordinate CA to Root CA

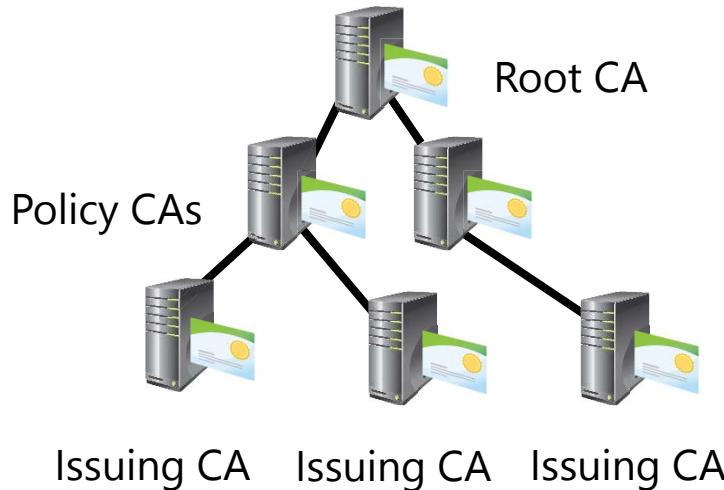


# Lesson 3: Deploying CAs

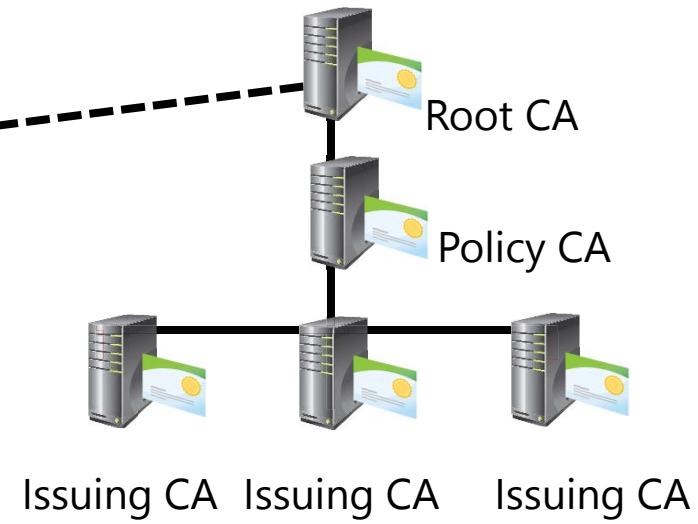
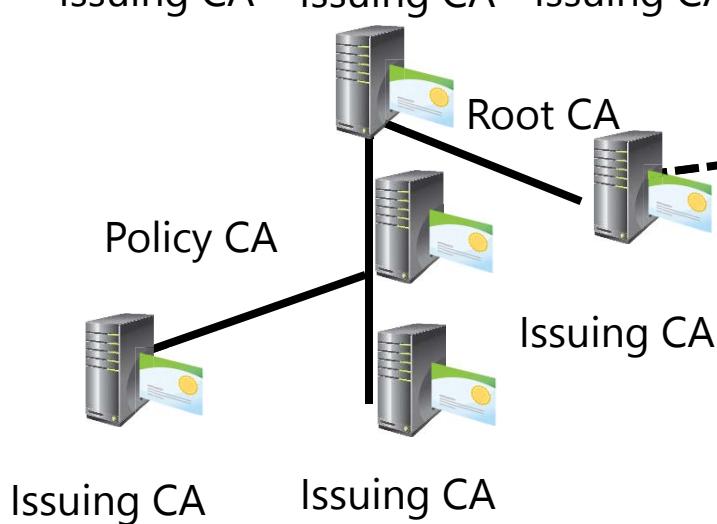
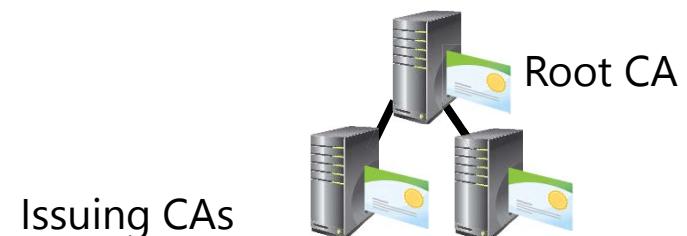
- Options for Implementing CA Hierarchies
- Stand-Alone vs. Enterprise CAs
- Considerations for Deploying a Root CA
- Demonstration: Deploying a Root CA
- Considerations for Deploying a Subordinate CA
- How to Use the CAPolicy.inf File for Installation
- Configuring CA Administration and Security
- Configuring CA Policy and Exit Modules
- Demonstration: Configuring CA Properties
- CA Backup and Recovery

# Options for Implementing CA Hierarchies

Policy CA Usage



Two-Tier Hierarchy



Cross-Certification Trust

# Stand-Alone vs. Enterprise CAs

| Stand-alone CAs                                                                    | Enterprise CAs                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|    | <p>Must be used if any CA (root/intermediate/policy) is offline, because a stand-alone CA is not joined to an AD DS domain</p>  |
|    | <p>Users provide identifying information and specify type of certificate</p>                                                    |
|   | <p>Does not require certificate templates</p>                                                                                   |
|  | <p>All certificate requests are kept pending until administrator approval</p>                                                 |

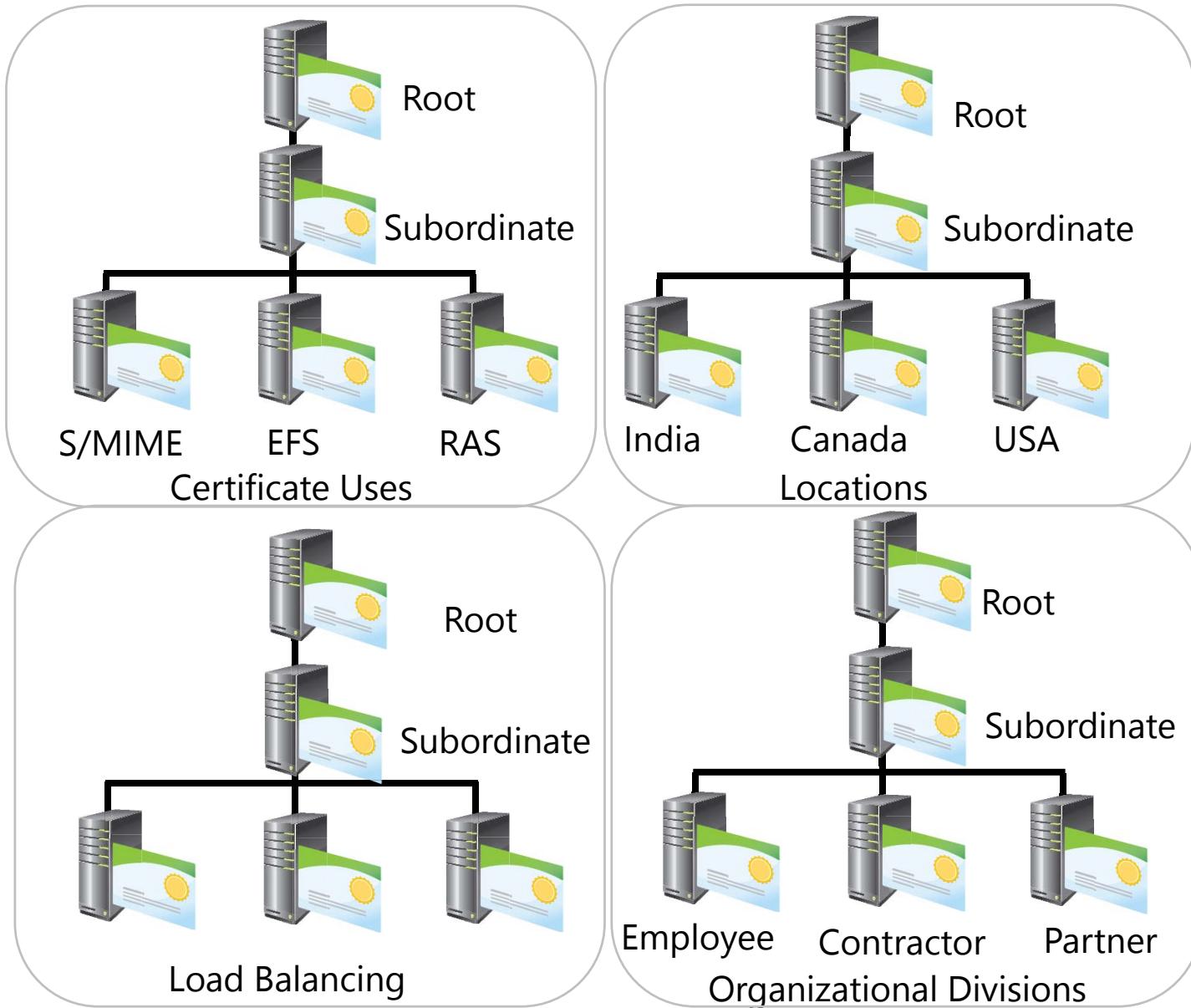
# Considerations for Deploying a Root CA

- Computer name and domain membership cannot change
- When you plan private key configuration, consider the following:
  - CSP
  - Key character length with a default of 2,048
  - The hash algorithm that is used to sign certificates issued by a CA
- When you plan a root CA, consider the following:
  - Name and configuration
  - Certificate database and log location
  - Validity period

# Demonstration: Deploying a Root CA

In this demonstration, you will see how to deploy an enterprise root CA

# Considerations for Deploying a Subordinate CA



# How to Use the CAPolicy.inf File for Installation

The CAPolicy.inf file is stored in the `%Windir%` folder of the root or subordinate CA, and defines the following:

- CPS
- Object Identifier
- CRL publication intervals
- CA renewal settings
- Key size
- Certificate validity period
- CDP and AIA paths

# Configuring CA Administration and Security

- You can establish role-based administration for the CA hierarchy by defining the following roles:
  - CA administrator
  - Certificate manager
  - Backup operator
  - Auditor
  - Enrollees
- You can assign the following permissions on the CA level:
  - Read
  - Issue and Manage Certificates
  - Manage CA
  - Request Certificates
- Certificate managers can be restricted to a template

# Configuring CA Policy and Exit Modules

- The policy module determines the action that is performed after the certificate request is received
- The exit module determines what happens with a certificate after it is issued
- Each CA is configured with default policy and exit modules
- The FIM CM 2010 deploys custom policy and exit modules
- The exit module can send email or publish a certificate to a file system
- You have to use certutil to specify these settings, as they are not available in the CA administrator console

# Demonstration: Configuring CA Properties

In this demonstration, your instructor will show you how to configure CA properties

# CA Backup and Recovery

- To back up a CA, follow this procedure:
  1. Record the names of the certificate templates
  2. Back up a CA in the CA admin console
  3. Export the registry subkey
  4. Uninstall the CA role (optional, only if you move CA)
  5. Confirm the `%SystemRoot%` folder locations
  6. Remove the old CA from the domain (optional, only if you move CA)
- To restore, follow this procedure:
  1. Install AD CS
  2. Use the existing private key
  3. Restore the registry file
  4. Restore the CA database and settings
  5. Restore the certificate templates

# Lab A: Deploying and Configuring a CA Hierarchy

- Exercise 1: Deploying a Stand-Alone Root CA
- Exercise 2: Deploying an Enterprise Subordinate CA

## Logon Information

|                   |                                                                        |
|-------------------|------------------------------------------------------------------------|
| Virtual machines: | 20412D-LON-DC1<br>20412D-LON-SVR1<br>20412D-LON-SVR2<br>20412D-LON-CA1 |
| User name:        | <b>Adatum\Administrator</b>                                            |
| Password:         | <b>Pa\$\$w0rd</b>                                                      |

Estimated Time: 50 minutes

## Lab Scenario

As A. Datum Corporation has expanded, its security requirements have also increased. The security department is particularly interested in enabling secure access to critical websites, and in providing additional security for features. To address these and other security requirements, A. Datum has decided to implement a PKI using the AD CS role in Windows Server 2012.

As one of the senior network administrators at A. Datum, you are responsible for implementing the AD CS deployment.

# Lab Review

- Why is it not recommended to install just an enterprise root CA?

# Lesson 4: Deploying and Managing Certificate Templates

- What Are Certificate and Certificate Templates?
- Certificate Template Versions in Windows Server 2012
- Configuring Certificate Template Permissions
- Configuring Certificate Template Settings
- Options for Updating a Certificate Template
- Demonstration: Modifying and Enabling a Certificate Template

# What Are Certificate and Certificate Templates?

A certificate contains information about users, devices, usage, validity, and a key pair

A certificate template defines:

- The format and contents of a certificate
- The process for creating and submitting a valid certificate request
- The security principals that are allowed to read, enroll, or use autoenrollment for a certificate that will be based on the template
- The permissions required to modify a certificate template

# Certificate Template Versions in Windows Server 2012

## Version 1:

- Introduced in Windows 2000 Server, provides for backward compatibility in newer versions
- Creates by default when a CA is installed
- Cannot be modified (except for permissions) or removed, but can be duplicated to become version 2 or 3 templates, which can then be modified

## Version 2:

- Default template introduced with Windows Server 2003
- Allows customization of most settings in the template
- Several preconfigured templates are provided when a CA is installed

## Version 3:

- Supports advanced Suite B cryptographic settings
- Includes advanced options for encryption, digital signatures, key exchange, and hashing
- Only supports Windows Server 2008 and Windows Server 2008 R2 servers
- Only supports Windows Vista and Windows 7 client computers

## Version 4:

- Available only for Windows Server 2012 and Windows 8 clients
- Supports both CSPs and KSPs
- Supports renewal with the same key

# Configuring Certificate Template Permissions

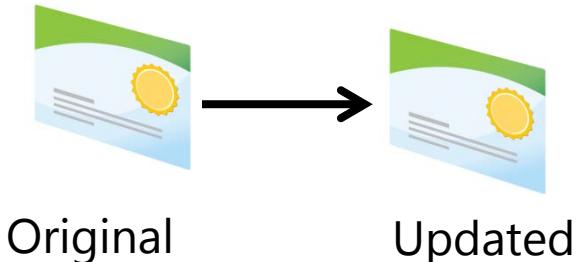
| Permissions  | Description                                                                                               |
|--------------|-----------------------------------------------------------------------------------------------------------|
| Full Control | Allows a designated user, group, or computer to modify all attributes—including ownership and permissions |
| Read         | Allows a designated user, group, or computer to read the certificate in AD DS when enrolling              |
| Write        | Allows a designated user, group, or computer to modify all attributes except permissions                  |
| Enroll       | Allows a designated user, group, or computer to enroll for the certificate template                       |
| Autoenroll   | Allows a designated user, group, or computer to receive a certificate through the autoenrollment process  |

# Configuring Certificate Template Settings

For each certificate template, you can customize several settings, such as validity time, purpose, CSP, private key exportability, and issuance requirements

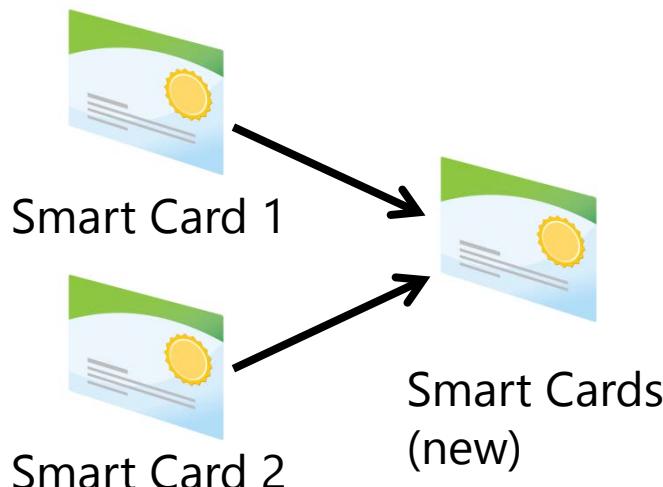
| Category  | Single purpose examples                                                                                                | Multiple purpose examples                                                                                |
|-----------|------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------|
| Users     | <ul style="list-style-type: none"><li>• Basic EFS</li><li>• Authenticated session</li><li>• Smart card logon</li></ul> | <ul style="list-style-type: none"><li>• Administrator</li><li>• User</li><li>• Smart card user</li></ul> |
| Computers | <ul style="list-style-type: none"><li>• Web server</li><li>• IPsec</li></ul>                                           | <ul style="list-style-type: none"><li>• Computer</li><li>• Domain controller</li></ul>                   |

# Options for Updating a Certificate Template



## Modifying

Modify the original certificate template to incorporate the new settings



## Superseding

Replace one or more certificate templates with an updated certificate template

# Demonstration: Modifying and Enabling a Certificate Template

In this demonstration, you will see how to modify and enable a certificate template

# Lesson 5: Implementing Certificate Distribution and Revocation

- Options for Certificate Enrollment
- How Does Autoenrollment Work?
- Enrollment Agent Overview
- Demonstration: Configuring the Restricted Enrollment Agent
- What Is NDES?
- How Does Certificate Revocation Work?
- Considerations for Publishing AIAs and CDPs
- What Is an Online Responder?
- Demonstration: Configuring an Online Responder

# Options for Certificate Enrollment

| Method            | Use                                                                                                                                                                                             |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Autoenrollment    | <ul style="list-style-type: none"><li>• To automate the request, retrieval, and storage of certificates for domain-based computers</li></ul>                                                    |
| Manual enrollment | <ul style="list-style-type: none"><li>• To request certificates by using the Certificates Templates console or Certreq.exe when the requestor cannot communicate directly with the CA</li></ul> |
| CA Web enrollment | <ul style="list-style-type: none"><li>• To request certificates from a website that is located on a CA</li><li>• To issue certificates when autoenrollment is not available</li></ul>           |
| Enroll on behalf  | <ul style="list-style-type: none"><li>• To provide IT staff with the right to request certificates on behalf of another user (Enrollment Agent)</li></ul>                                       |

# How Does Autoenrollment Work?



Certificate template

A certificate template is configured to Allow, Enroll, and Autoenroll permissions for users who receive the certificates



CA

The CA is configured to issue the template



Group Policy Object

An Active Directory Group Policy Object should be created to enable autoenrollment. The GPO should be linked to the appropriate site, domain, or organizational unit



Client machine

The client machine receives the certificates during the next Group Policy refresh interval

# Enrollment Agent Overview

An Enrollment Agent is a user who has the appropriate certificate assigned and has the ability to request certificates on behalf of other users or computers

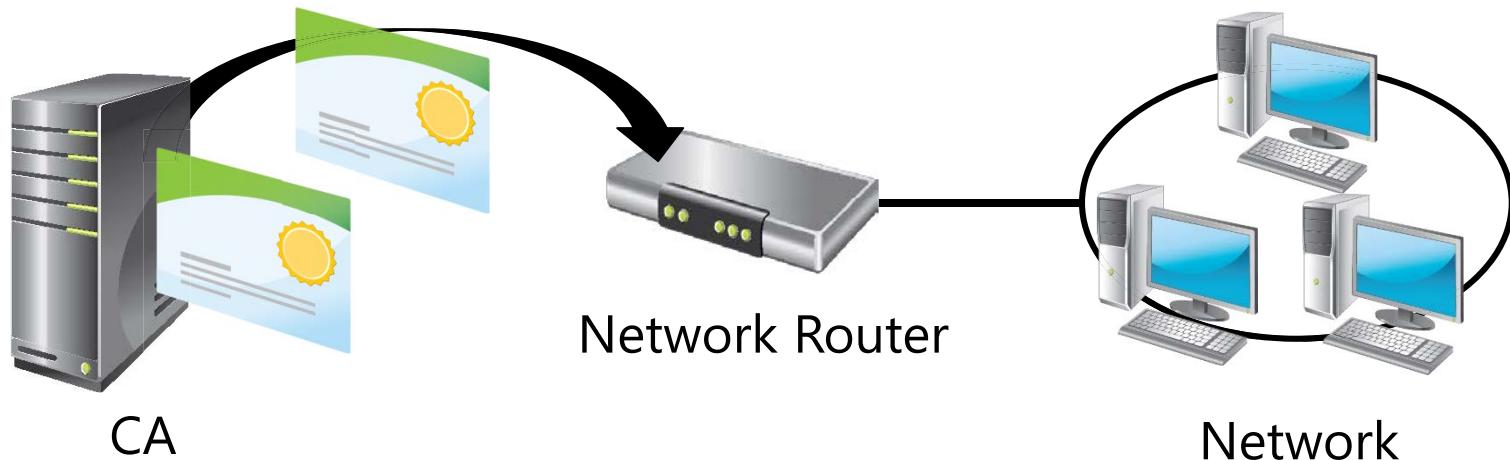
The restricted Enrollment Agent has limited permissions:

- Limits permissions of the Enrollment Agent:
  - For specific group of users
  - For specific certificate templates
- Requires Windows Server 2008 Enterprise edition or Windows Server 2012 CA

# Demonstration: Configuring the Restricted Enrollment Agent

In this demonstration, you will see how to configure the Restricted Enrollment Agent

# What Is NDES?



## NDES:

- Uses SCEP to communicate with network devices
- Functions as an AD CS role service
- Requires IIS

# How Does Certificate Revocation Work?

1. Certificate is revoked
2. Certificate revocation is published



3. Client computer verifies certificate validity and revocation



# Considerations for Publishing AIAs and CDPs

Publish the root certificate CA and URL

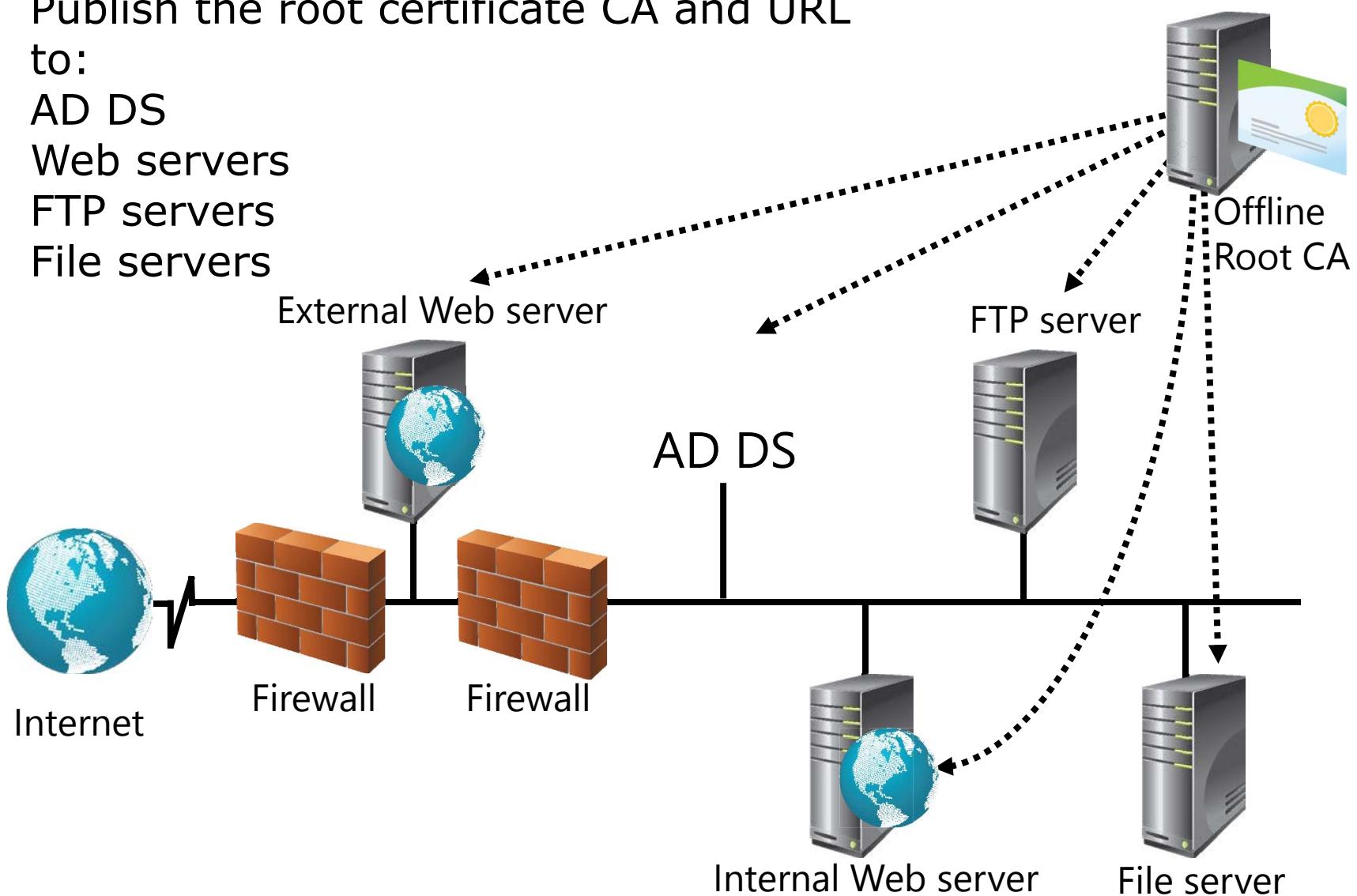
to:

AD DS

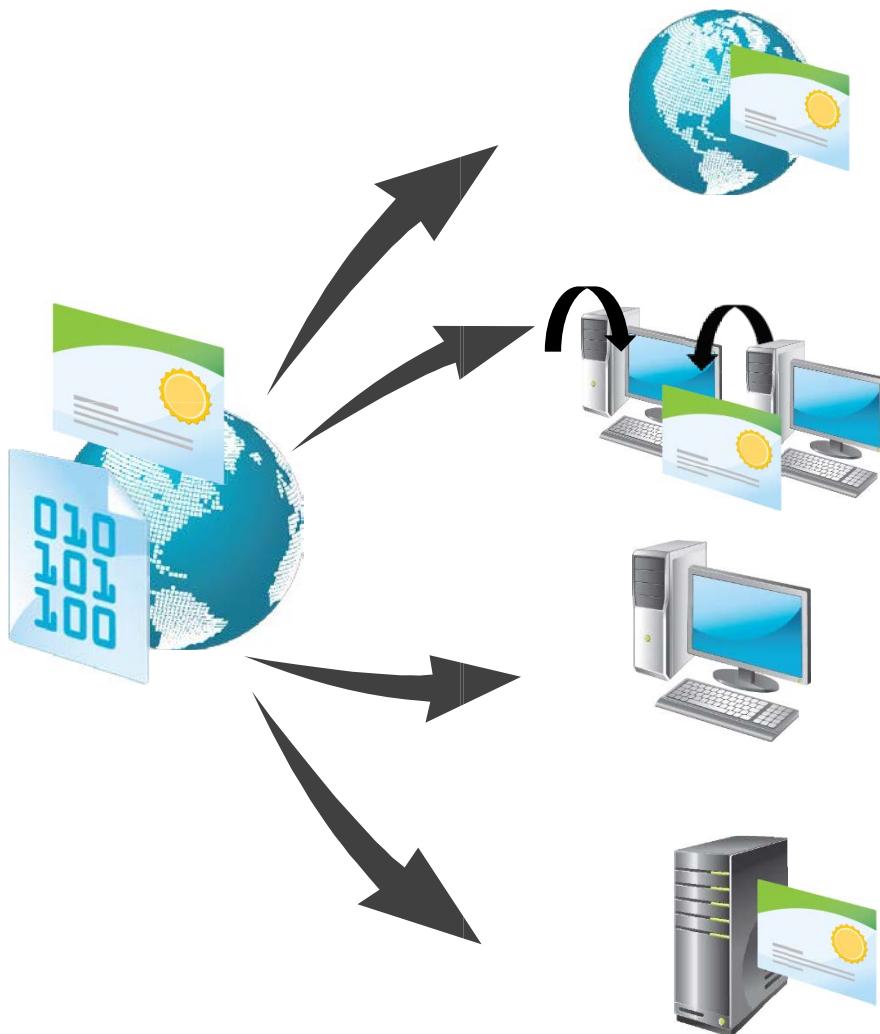
Web servers

FTP servers

File servers



# What Is an Online Responder?



Uses OCSP validation and revocation checking using HTTP

Receives and responds dynamically to individual requests

Supports only Windows Server 2008, Windows Vista, and newer Windows operating systems

Functions as a responder to multiple CAs

# Demonstration: Configuring an Online Responder

In this demonstration, you will see how to configure an Online Responder

# Lesson 6: Managing Certificate Recovery

- Overview of Key Archival and Recovery
- Configuring Automatic Key Archival
- Demonstration: Configuring a CA for Key Archival
- Recovering a Lost Key
- Demonstration: Recovering a Lost Private Key

# Overview of Key Archival and Recovery

- Private keys can get lost when:
  - A user profile is deleted
  - An operating system is reinstalled
  - A disk is corrupted
  - A computer is lost or stolen
- It is critical that you archive private keys for certificates that are used for encryption
- The KRA is needed for key recovery
- Key archival must be configured on the CA and on the certificate template
- Key recovery is a two-phase process:
  1. Key retrieval
  2. Key recovery
- The KRA certificate must be protected

# Configuring Automatic Key Archival

Steps to configure automatic key archival:



Configure and issue the KRA certificate template



Designate a person as the KRA, and enroll for the certificate



Enable key archival on the CA



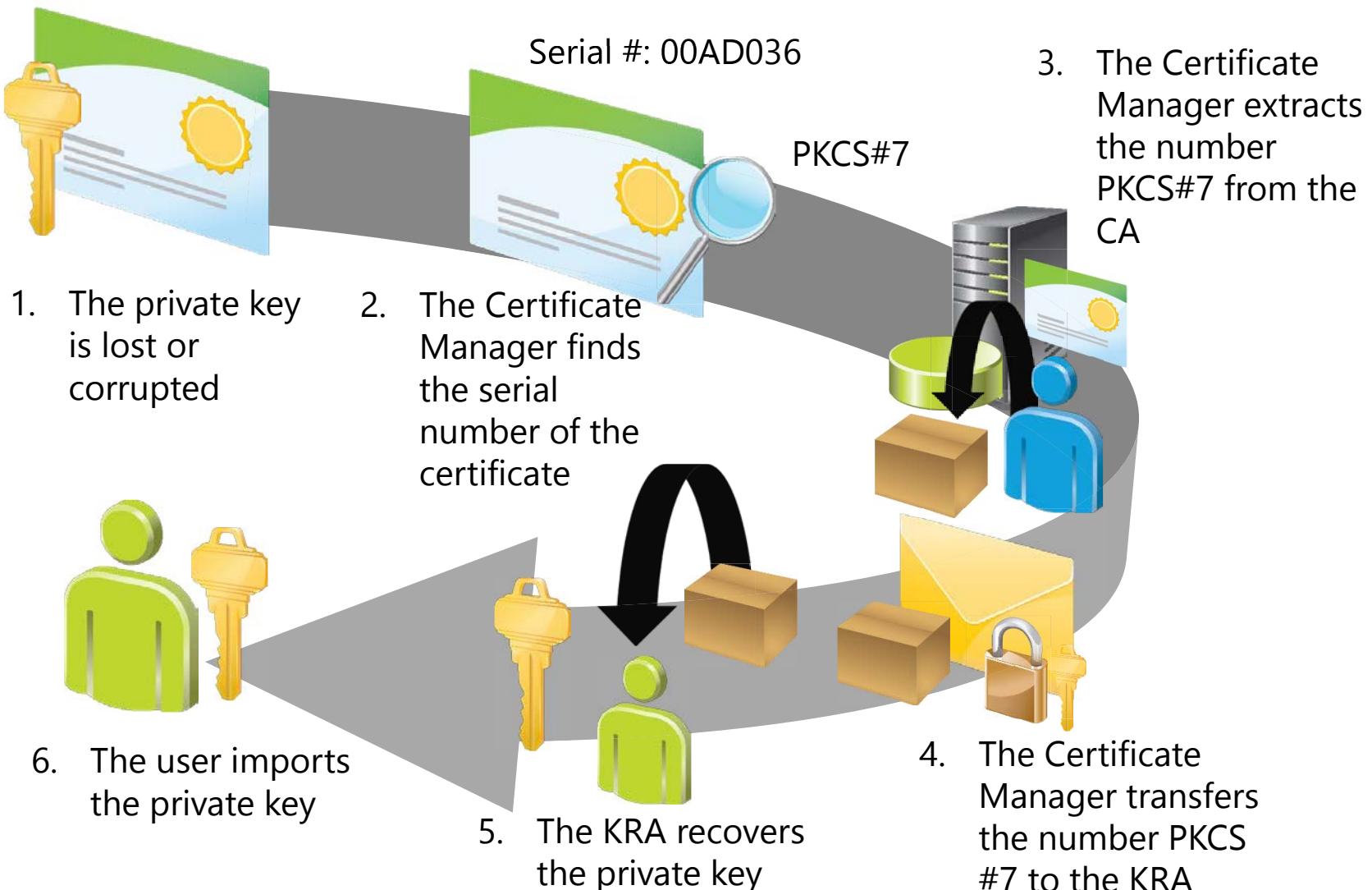
Modify and enable certificate templates for key archival



# Demonstration: Configuring a CA for Key Archival

In this demonstration, you will see how to configure a CA for key archival

# Recovering a Lost Key



# Demonstration: Recovering a Lost Private Key

In this demonstration, you will see how to recover a lost private key

# Lab B: Deploying and Managing Certificates

- Exercise 1: Configuring Certificate Templates
- Exercise 2: Configuring Certificate Enrollment
- Exercise 3: Configuring Certificate Revocation
- Exercise 4: Configuring Key Recovery

## Logon Information

Virtual machines:

20412D-LON-DC1

20412D-LON-SVR1

20412D-LON-SVR2

20412D-LON-CA1

20412D-LON-CL1

User name:

**Adatum\Administrator**

Password:

**Pa\$\$w0rd**

Estimated Time: 75 minutes

# Lab Scenario

As A. Datum Corporation has expanded, its security requirements have also increased. The security department is particularly interested in enabling secure access to critical websites, and in providing additional security for features such as drive encryption, smart cards, and the Windows 7 and Windows 8 DirectAccess feature. To address these and other security requirements, A. Datum has decided to implement a PKI using the AD CS role in Windows Server 2012.

As one of the senior network administrators at A. Datum, you are responsible for implementing the AD CS deployment. You will deploy the CA hierarchy, develop the procedures and process for managing certificate templates, and deploy and revoke certificates.

# Lab Review

- What is the main benefit of OCSP over CRL?
- What must you do to recover private keys?

# Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 7

### Implementing Active Directory Rights Management Services

**Microsoft®**

# Module Overview

- AD RMS Overview
- Deploying and Managing an AD RMS Infrastructure
- Configuring AD RMS Content Protection
- Configuring External Access to AD RMS

# Lesson 1: AD RMS Overview

- What Is AD RMS?
- Usage Scenarios for AD RMS
- Overview of the AD RMS Components
- AD RMS Certificates and Licenses
- How AD RMS Works

# What Is AD RMS?

- Information protection technology
- Designed to reduce information leakage
- Integrated with Windows operating systems, Microsoft Office, Exchange Server, and SharePoint Server
- Based on Symmetric and Public Key Cryptography
- Protects data at rest, in transit, and in use

# Usage Scenarios for AD RMS

- Prevent the transmission of sensitive information
- Comply with privacy regulations
- Can be used with encryption to protect data in transit and at rest

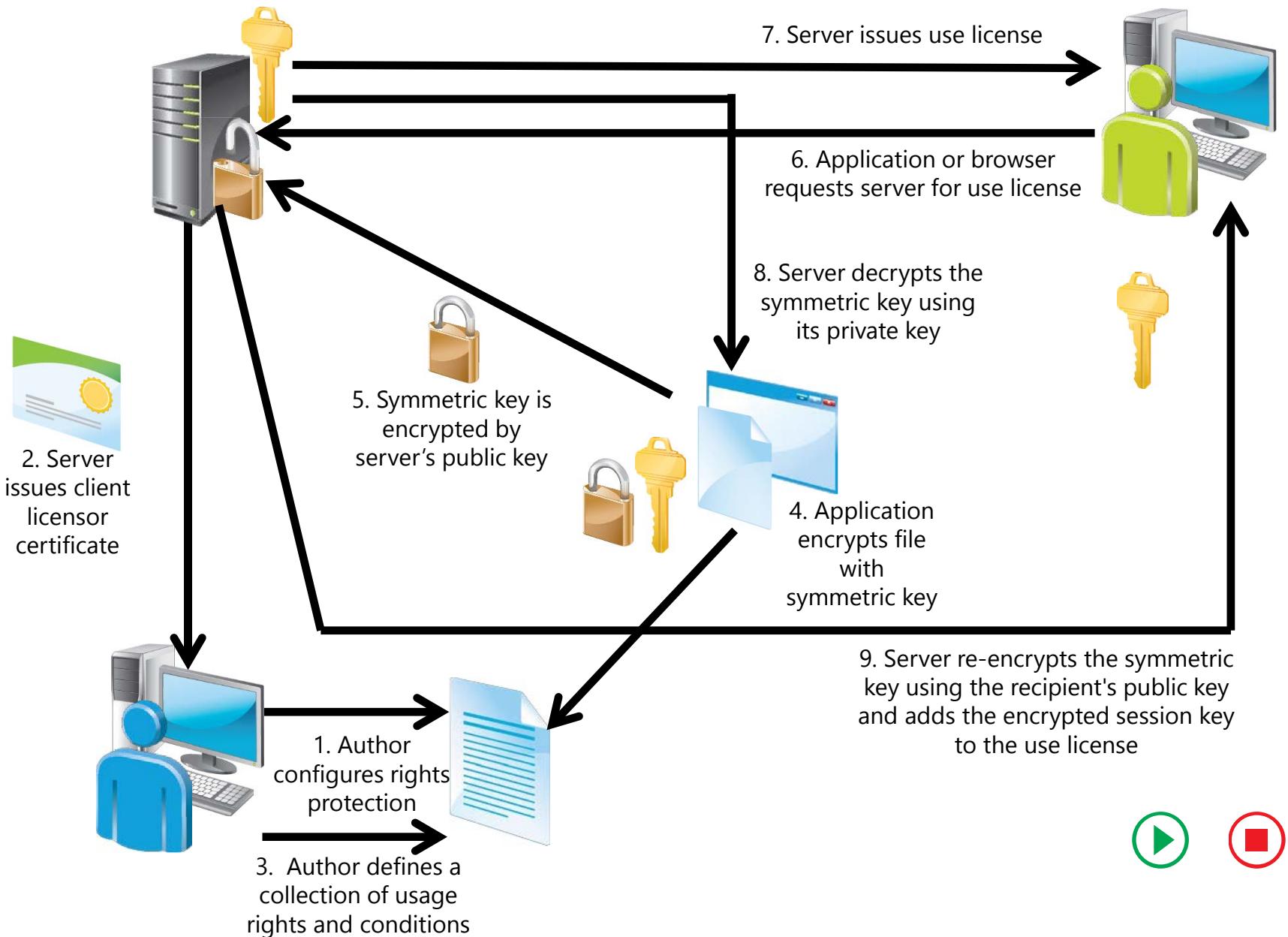
# Overview of the AD RMS Components

- AD RMS cluster
- AD RMS server
  - Licenses AD RMS-protected content
  - Certifies identity of trusted users and devices
- AD RMS client
  - Built into Windows Vista, Windows 7, and Windows 8
  - Interacts with AD RMS-enabled applications
- AD RMS-enabled applications
  - Allows publication and consumption of AD RMS-protected content
  - Includes Microsoft Office, Exchange Server, and SharePoint Server
  - Can be created using AD RMS SDKs.

# AD RMS Certificates and Licenses

- AD RMS certificate and licenses include:
  - Server licensor certificate
  - AD RMS machine certificate
  - Rights Account Certificate
  - Client licensor certificate
  - Publishing license
  - End-user license

# How AD RMS Works



# Lesson 2: Deploying and Managing an AD RMS Infrastructure

- AD RMS Deployment Scenarios
- Configuring the AD RMS Cluster
- Demonstration: Installing the First Server of an AD RMS Cluster
- AD RMS Client Requirements
- Implementing an AD RMS Backup and Recovery Strategy
- Decommissioning and Removing AD RMS

# AD RMS Deployment Scenarios

- Deployment scenarios for AD RMS are:
  - AD RMS in a single forest
  - AD RMS in multiple forests
  - AD RMS used on an extranet
  - AD RMS integrated with AD FS

# Configuring the AD RMS Cluster

AD RMS configuration includes configuring of following:

- New or join existing cluster
- Configuration database location
- Service account
- Cryptographic mode
- Cluster key storage
- Cluster key password
- Cluster website
- Cluster address
- Server certificate
- Licensor certificate
- SCP registration

# Demonstration: Installing the First Server of an AD RMS Cluster

In this demonstration, you will see how to install the first server of an AD RSM cluster

# AD RMS Client Requirements

- Client included in Windows Vista and newer operating systems
- Client included in Windows Server 2008 and newer operating systems
- Client available for download for previous versions of Windows operating systems, and Mac OS X
- AD RMS–enabled applications include Office 2007, Office 2010, and Office 2013
- Exchange Server 2007, Exchange Server 2010, and Exchange Server 2013 support AD RMS
- AD RMS clients needs RMS CAL

# Implementing an AD RMS Backup and Recovery Strategy

- Back up private key and certificates
- Ensure that the AD RMS database is backed up regularly
- Export templates to back them up
- Run the AD RMS server as a virtual machine, and perform full server backup

# Decommissioning and Removing AD RMS

- Decommission an AD RMS cluster prior to removing it
  - Decommissioning provides a key that decrypts previously published AD RMS content
  - Leave server in decommissioned state until all AD RMS-protected content is migrated
- Export the server licensor certificate prior to uninstalling the AD RMS role

# Lesson 3: Configuring AD RMS Content Protection

- What Are Rights Policy Templates?
- Demonstration: Creating a Rights policy Template
- Providing Rights policy Templates for Offline Use
- What Are Exclusion Policies?
- Demonstration: Creating an Exclusion Policy to Exclude an Application
- AD RMS Super Users Group
- AD RMS Integration with Dynamic Access Control

# What Are Rights Policy Templates?

- Allow authors to apply standard forms of protection across the organization
- Different applications allow different forms of rights
- Can configure rights related to viewing, editing, and printing documents
- Can configure content expiration rights
- Can configure content revocation

# Demonstration: Creating a Rights policy Template

In this demonstration, you will see how to create a rights policy template that allows users to view a document, but not to perform other actions

# Providing Rights policy Templates for Offline Use

- Ensure that templates are published to a shared folder
- Enable the AD RMS Rights Policy Template Management (Automated) Scheduled Task
- Edit the registry key and specify the shared folder location

# What Are Exclusion Policies?

Allows you to:

- Block specific users from accessing AD RMS-protected content by blocking their RAC
- Block specific applications from creating or consuming AD RMS-protected content
- Block specific versions of the AD RMS client

# Demonstration: Creating an Exclusion Policy to Exclude an Application

In this demonstration, you will see how to exclude the Microsoft PowerPoint application from AD RMS

# AD RMS Super Users Group

- Super users group members are granted full owner rights in all use licenses that are issued by the AD RMS cluster on which the super users group is configured.
- Super users group:
  - Is not configured by default
  - Can be used as data recovery mechanism for AD RMS-protected content
    - Can recover content that has expired
    - Can recover content if the template is deleted
    - Can recover content without requiring author credentials
  - Must be an Active Directory group with an assigned email address.

# AD RMS Integration with Dynamic Access Control

- DAC applies encryption by using AD RMS
- DAC protects documents even if inadvertently saved, sent, or processed incorrectly
- DAC extends AD RMS to the file server

# Lesson 4: Configuring External Access to AD RMS

- Options for Enabling External Users with AD RMS Access
- Implementing Trusted User Domain
- Implementing TPD
- Sharing AD RMS–Protected Documents by Using a Microsoft Account
- Considerations for Implementing External User Access to AD RMS
- Windows Azure AD Rights Management

# Options for Enabling External Users with AD RMS Access

- Trusted User Domains
  - Exchange protected content between two organizations
- Trusted Publishing Domains
  - Consolidate AD RMS architecture
- Federation Trust
  - One AD RMS infrastructure is accessible to AD FS partners
- Windows Live ID
  - Allow stand alone users access to AD RMS content
- Microsoft Federation Gateway
  - Allow an AD RMS cluster to work with Microsoft Federation Gateway without requiring a direct Federation Trust

# Implementing Trusted User Domain

- Allows AD RMS to service requests to users with RACs from different AD RMS clusters
- TUDs:
  - Support exclusions to individual users and groups
  - Can be one-way or bidirectional
- Must export TUD from partner before importing TUD locally

# Implementing TPD

- Allows a local AD RMS deployment to issue EULs to content protected by a partner AD RMS cluster
- Involves importing the SLC of the partner AD RMS cluster
- No limit to the number of supported TPDs

# Sharing AD RMS–Protected Documents by Using a Microsoft Account

- Provide RACs to users who are not part of an organization
- Users with Microsoft Accounts can consume AD RMS–protected content
- Users with Microsoft Accounts cannot publish AD RMS–protected content

# Considerations for Implementing External User Access to AD RMS

- Use Windows Live ID to issue RACs to users who are not part of organizations, and who need to consume content
- Use TUD for RACs issued by a different AD RMS cluster
- Use TPD to allow local RACs to access remotely published AD RMS content
- Use Federation Trust between organizations that have a federated relationship
- Use Microsoft Federation Gateway when no direct federated relationship exists

# Windows Azure AD Rights Management

- Windows Azure Rights Management is IRM-based cloud service protection
- Windows Azure Right Management is available in Office 365 Enterprise E3 and Office 365 ProPlus
- Windows Azure AD Rights Management provides:
  - IRM integration with Microsoft Office
  - Exchange Online IRM integration
  - SharePoint Online IRM integration

# Lab: Implementing AD RMS

- Exercise 1: Installing and AD RMS
- Exercise 2: Configuring AD RMS Templates
- Exercise 3: Implementing the AD RMS Trust Policies
- Exercise 4: Verifying AD RMS on a Client

## Logon Information

Virtual machines: 20412D-LON-DC1, 20412D-LON-SVR1,  
20412D-LON-CL1, 20412D-TREY-DC1,  
20412D-TREY-CL1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 60 minutes

# Lab Scenario

Because of the highly confidential nature of the research that is performed at A. Datum Corporation, the security team at A. Datum wants to implement additional security for certain documents that the Research department creates. The security team is concerned that anyone with Read access to the documents can modify and distribute the documents in any way that they choose. The security team would like to provide an extra level of protection that stays with the document even if it is moved around the network or outside the network.

## Lab Scenario

As one of the senior network administrators at A. Datum, you need to plan and implement an AD RMS solution that will provide the level of protection requested by the security team. The AD RMS solution must provide many different options that can be adapted for a wide variety of business and security requirements.

# Lab Review

- What considerations should you make and steps you can take when you use the AD RMS role?

# Module Review and Takeaways

- Review Questions
- Tools
- Real-world Issues and Scenarios
- Best Practice

# Microsoft® Official Course



## Module 8

### Implementing and Administering AD FS

**Microsoft®**

# Module Overview

- Overview of AD FS
- Deploying AD FS
- Implementing AD FS for a Single Organization
- Deploying AD FS in a Business-to-Business Federation Scenario
- Extending AD FS to External Clients

# Lesson 1: Overview of AD FS

- What Is Identity Federation?
- What Is Claims-Based Identity?
- Web Services Overview
- What Is AD FS?
- How AD FS Enables SSO in a Single Organization
- How AD FS Enables SSO in a Business-to-Business Federation
- How AD FS Enables SSO with Online Services
- What Is New in Windows Server 2012 R2

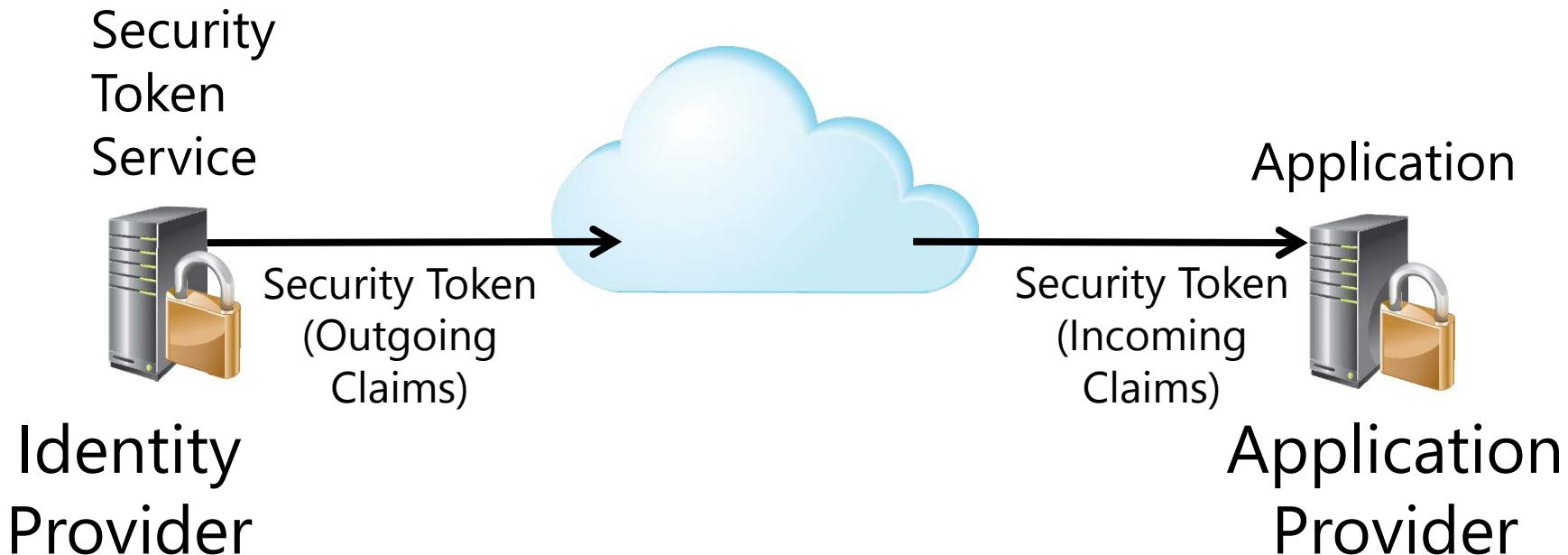
# What Is Identity Federation?

## Identity federation:

- Enables identification, authentication, and authorization across organizational and platform boundaries
- Requires a federated trust relationship between two organizations or entities
- Enables organizations to retain control over who can access resources
- Enables organizations to retain control of their user and group accounts

# What Is Claims-Based Identity?

- Claims provide information about users
- Information is provided by the user's identity provider, and is accepted by the application provider



# Web Services Overview

Web services are a standardized set of specifications used to build applications and services

Web services typically:

- Transmit data as XML
- Use SOAP to define the XML message format
- Use WSDL to define valid SOAP messages
- Use UDDI to describe available web services

SAML is a standard for exchanging identity claims

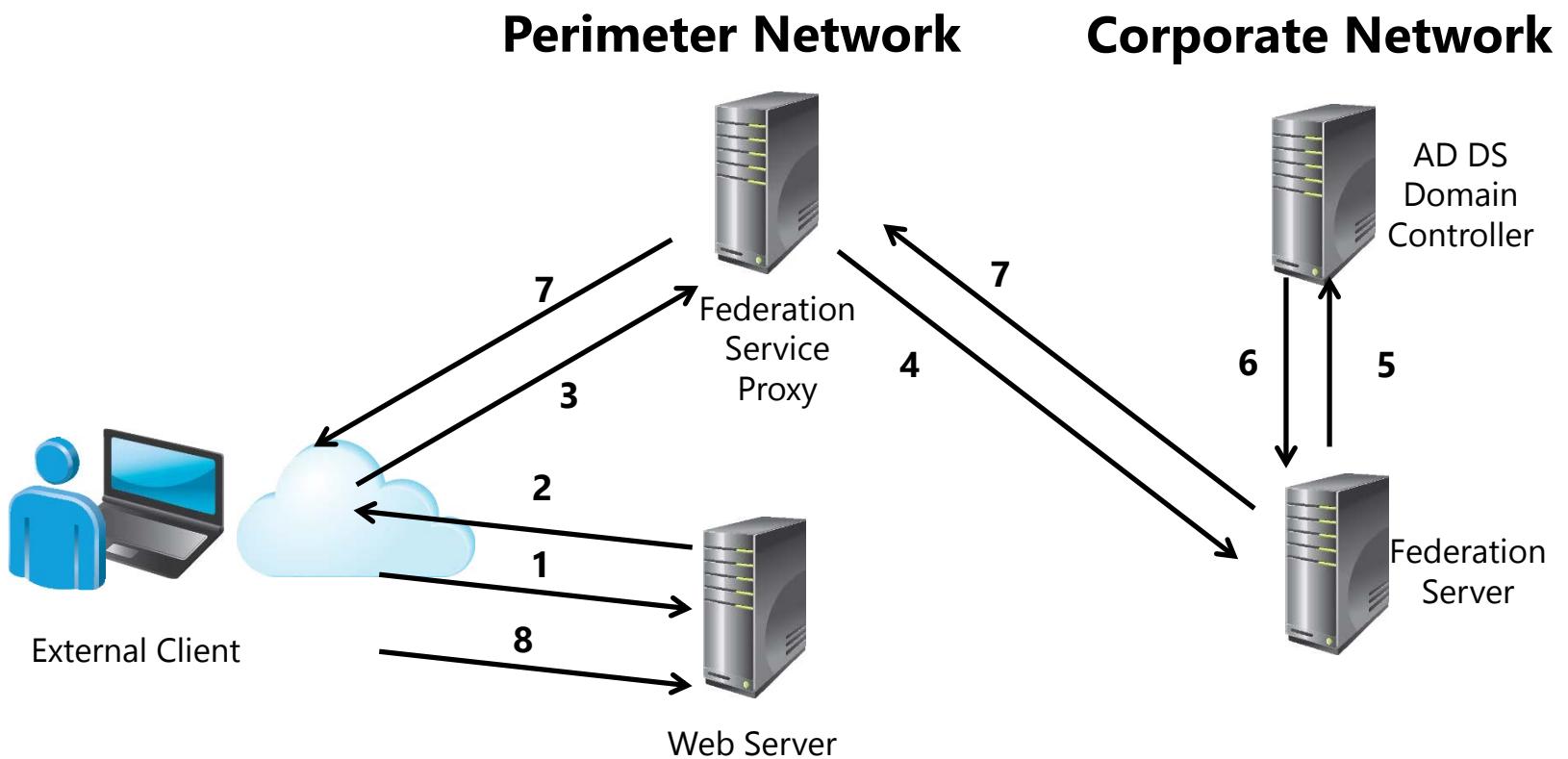
# What Is AD FS?

AD FS is the Microsoft identity federation product that can use claim-based authentication

AD FS has the following features:

- SSO for web-based applications
- Interoperability with web services on multiple platforms
- Support for many clients, such as web browsers, mobile devices, and applications
- Extensibility to support customized claims from third-party applications
- Delegation of account management to the user's organization
- Integration with DAC
- Windows PowerShell cmdlets for administration

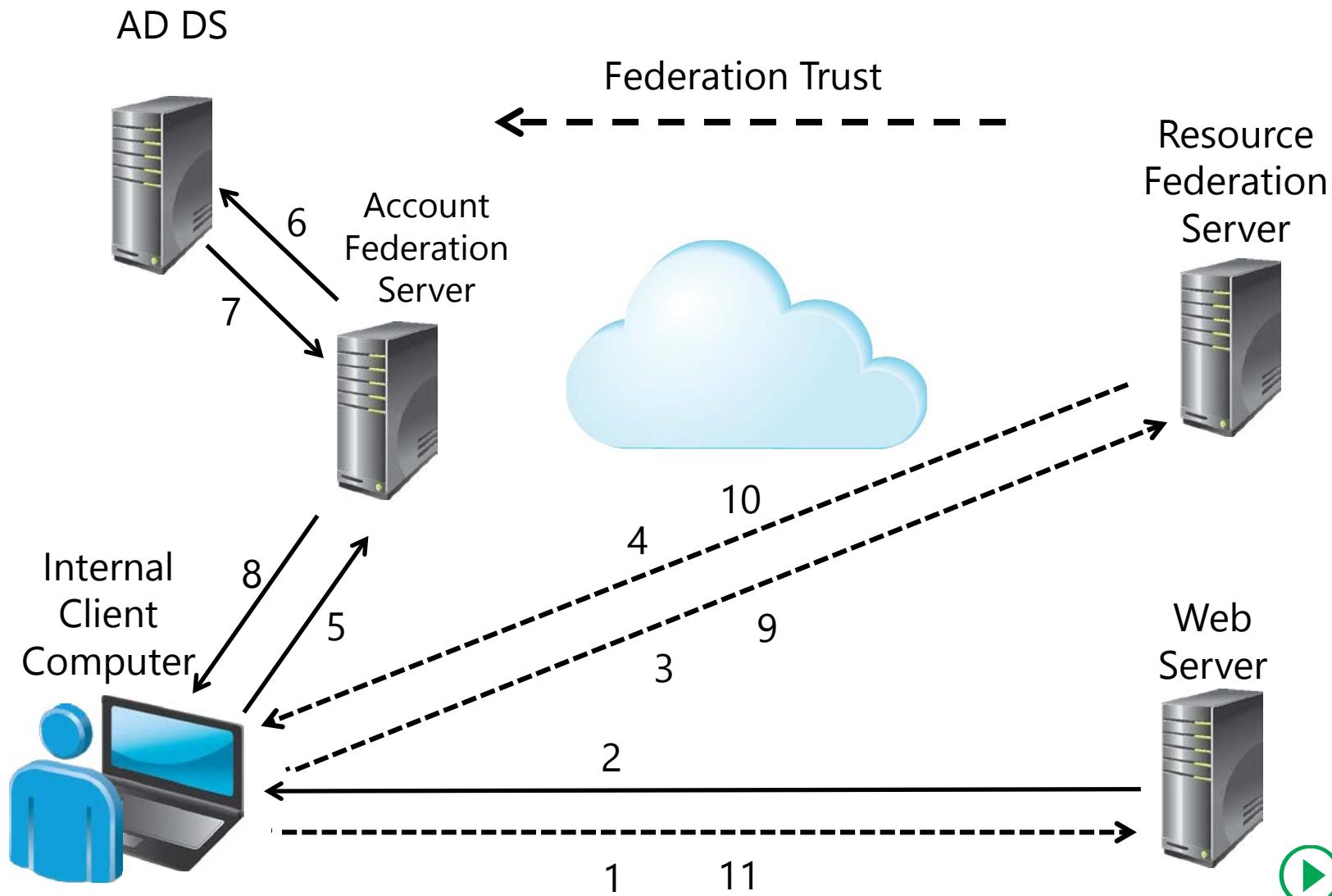
# How AD FS Enables SSO in a Single Organization



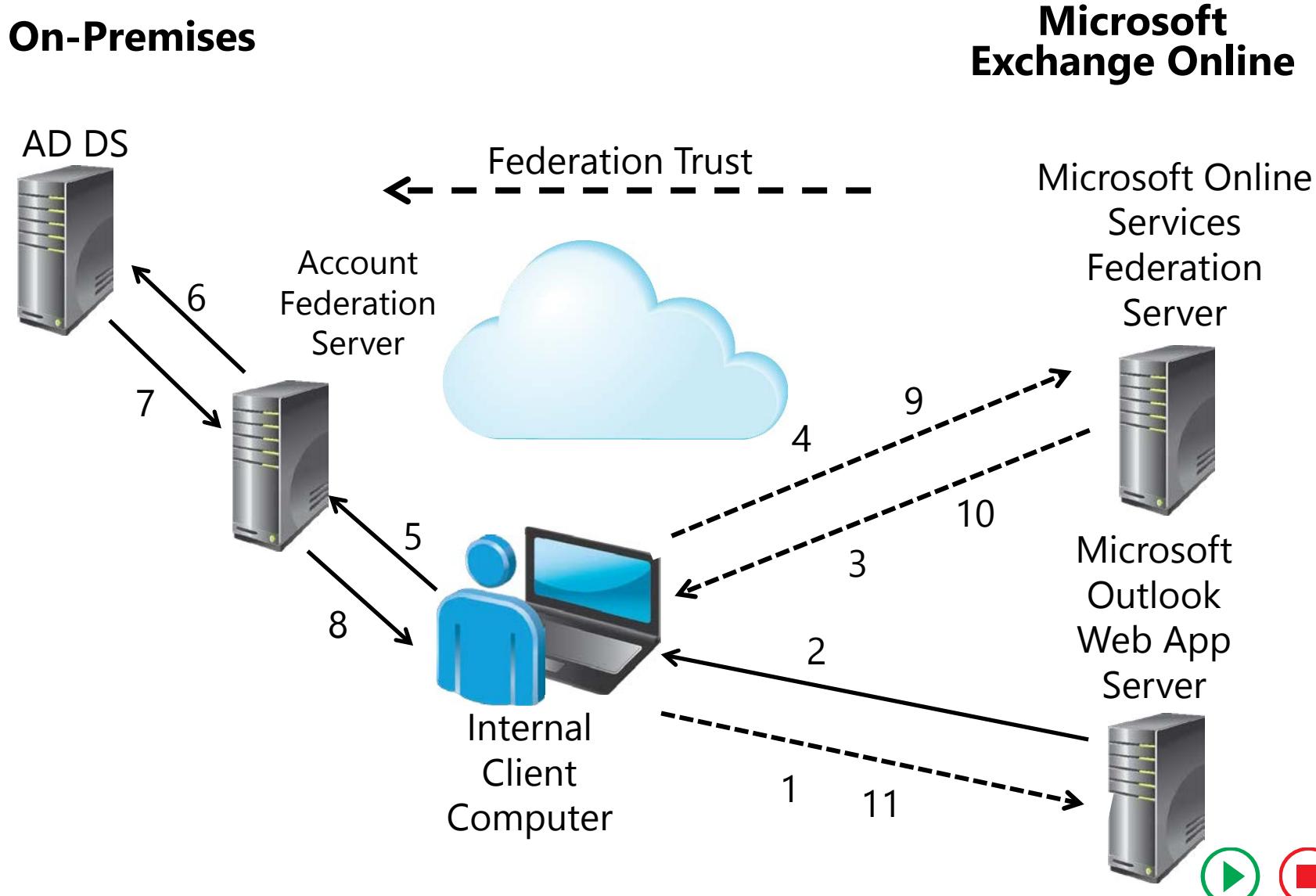
# How AD FS Enables SSO in a Business-to-Business Federation

Trey Research

A. Datum



# How AD FS Enables SSO with Online Services



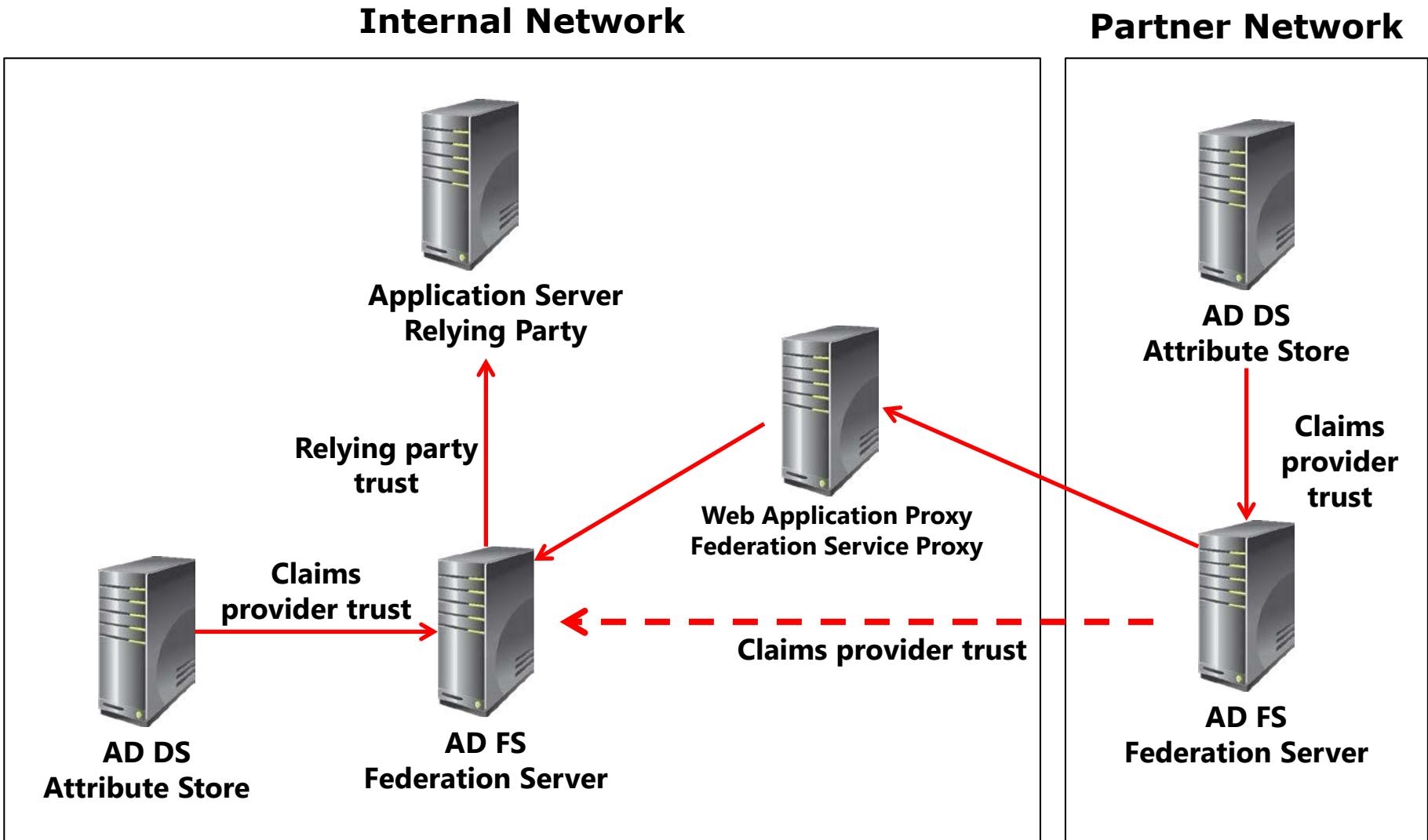
# What Is New in Windows Server 2012 R2

- Installation:
  - No IIS 8.5 required
  - Can install on domain controllers
- Enhanced authentication:
  - Authentication policies with scope
  - Multifactor authentication
- New claims types:
  - Mostly device and certificate related
- Web Application Proxy:
  - Provides secure remote access to web-based applications
  - Replaces AD FS proxy

# Lesson 2: Deploying AD FS

- AD FS Components
- AD FS Prerequisites
- PKI and Certificate Requirements
- Federation Server Roles
- Demonstration: Installing the AD FS Server Role

# AD FS Components



# AD FS Prerequisites

Successful AD FS deployment includes the following critical infrastructure:

- TCP/IP network connectivity
- AD DS
- Attribute stores
- DNS
- Compatible operating systems

Installation changes in Windows Server 2012 R2:

- IIS is not required
- No AD FS stand-alone server option

# PKI and Certificate Requirements

## Certificates used by AD FS:

- Service communication certificates
- Token-signing certificates
- Token-decrypting certificates

When choosing certificates, ensure that the service communication certificate is trusted by all federation partners and clients

If you use an internal CA then users must have access to certificate revocation information

# Federation Server Roles

Claims provider federation server:

- Authenticates internal users
- Issues signed tokens containing user claims

Relying party federation server:

- Consumes tokens from the claims provider
- Issues tokens for application access

Federation server proxy:

- Is deployed in a perimeter network
- Provides a layer of security for internal federation servers

# Demonstration: Installing the AD FS Server Role

- In this demonstration, you will see how to install and configure the AD FS server role

# Lesson 3: Implementing AD FS for a Single Organization

- What Are AD FS Claims?
- What Are AD FS Claim Rules?
- What Is a Claims-Provider Trust?
- What Is a Relying-Party Trust?
- Demonstration: Configuring Claims Provider and Relying Party Trusts
- What Are Authentication Policies?
- What Is Multifactor Authentication?

# What Are AD FS Claims?

Claims provide information about users from the claims provider to the relying party

AD FS:

- Provides a default set of built-in claims
- Enables the creation of custom claims
- Requires that each claim have a unique URI

Claims can be:

- Retrieved from an attribute store
- Calculated based on retrieved values
- Transformed into alternate values

# What Are AD FS Claim Rules?

- Claim rules define how claims are sent and consumed by AD FS servers
- Claims provider rules are acceptance transform rules
- Relying party rules can be:
  - Issuance transform rules
  - Issuance authorization rules
  - Delegation authorization rules
- AD FS servers provide default claim rules, templates, and a syntax for creating custom claim rules

# What Is a Claims-Provider Trust?

Claims provider trusts:

- Are configured on the relying party federation server
- Identify the claims provider
- Configure the claim rules for the claims provider

In a single-organization scenario, a claims provider trust called Active Directory defines how AD DS user credentials are processed

Additional claims provider trusts can be configured by:

- Importing the federation metadata
- Importing a configuration file
- Configuring the trust manually

# What Is a Relying-Party Trust?

Relying party trusts:

- Are configured on the claims provider federation server
- Identify the relying party
- Configure the claim rules for the relying party

In a single-organization scenario, a relying party trust defines the connection to internal applications

Additional relying party trusts can be configured by:

- Importing the federation metadata
- Importing a configuration file
- Manually configuring the trust

# Demonstration: Configuring Claims Provider and Relying Party Trusts

- In this demonstration, you will see how to:
  - Configure a claims provider trust
  - Configure a certificate for a web-based app
  - Configure a WIF application for AD FS
  - Configure a relying party trust

# What Are Authentication Policies?

Authentication methods can be configured for the intranet or extranet

- Windows authentication
- Forms authentication
- Certificate authentication

# What Is Multifactor Authentication?

Multifactor authentication requires an additional factor for authentication

- Certificate authentication or third-party vendors

Multifactor authentication can apply to:

- Specific users or groups
- Registered or unregistered devices
- Intranet or extranet

Windows Azure Multi-Factor Authentication uses the following:

- Phone calls
- Text messages
- Mobile App

# Lab A: Implementing AD FS

- Exercise 1: Installing and Configuring AD FS
- Exercise 2: Configuring an Internal Application for AD FS

## Logon Information

Virtual machines: 20412D-LON-DC1,  
20412D-LON-SVR1, 20412D-LON-CL1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 30 minutes

# Lab Scenario

A. Datum Corporation has set up a variety of business relationships with other companies and customers. Some of these partner companies and customers must access business applications that are running on the A. Datum network. The business groups at A. Datum want to provide a maximum level of functionality and access to these companies. The Security and Operations departments want to ensure that the partners and customers can access only the resources to which they require access, and that implementing the solution does not increase the workload for the Operations team significantly. A. Datum also is working on migrating some parts of its network infrastructure to Microsoft Online Services, including Windows Azure and Office 365.

## Lab Scenario

To meet these business requirements, A. Datum plans to implement AD FS. In the initial deployment, the company plans to use AD FS to implement SSO for internal users who access an application on a Web server.

As one of the senior network administrators at A. Datum, it is your responsibility to implement the AD FS solution. As a proof-of-concept, you plan to deploy a sample claims-aware application, and you will configure AD FS to enable internal users to access the application.

# Lab Review

- Why was it important to configure adfs.adatum.com to use as a host name for the AD FS service?
- How can you test whether AD FS is functioning properly?

# Lesson 4: Deploying AD FS in a Business-to-Business Federation Scenario

- Configuring an Account Partner
- Configuring a Resource Partner
- Configuring Claims Rules for Business-to-Business Scenarios
- How Home Realm Discovery Works
- Demonstration: Configuring Claim Rules

# Configuring an Account Partner

An account partner is a claims provider in a business to business federation scenario

To configure an account partner:

1. Implement the physical topology
2. Add an attribute store
3. Configure a relying party trust
4. Add a claim description
5. Prepare client computers for federation

# Configuring a Resource Partner

A resource partner is a relying party in a business-to-business federation scenario

To configure an relying partner:

1. Implement the physical topology
2. Add an attribute store
3. Configure a claims provider trust
4. Create claim rule sets for the claims provider trust

# Configuring Claims Rules for Business-to-Business Scenarios

Business to business scenarios may require more complex claims rules

You can create claims rules by using the following templates:

- Send LDAP Attributes as Claims
- Send Group Membership as a Claim
- Pass Through or Filter an Incoming Claim
- Transform an Incoming Claim
- Permit or Deny Users Based on an Incoming Claim

You can also create custom rules by using the AD FS claim rule language

# How Home Realm Discovery Works

Home realm discovery identifies the AD FS server responsible for providing claims about a user

There are two methods for home realm discovery:

- Prompt users during their first authentication
- Include a WHR string in the application URL

SAML applications can use a preconfigured profile for home realm discovery

# Demonstration: Configuring Claim Rules

- In this demonstration, you will see how to configure claim rules

# Lesson 5: Extending AD FS to External Clients

- What Is Web Application Proxy?
- Publishing an Application in Web Application Proxy
- Web Application Proxy and AD FS
- Demonstration: Installing and Configuring Web Application Proxy
- What Is Workplace Join?
- The Workplace Join Process
- Performing a Workplace Join

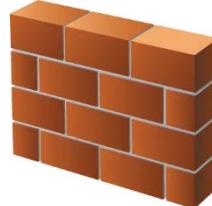
# What Is Web Application Proxy?

## Web Application Proxy:

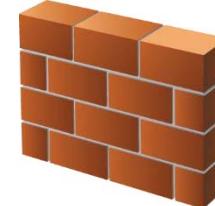
- Increases security for web-based applications and AD FS
- Is placed in a perimeter network
- Drops invalid requests
- Is independent of the web server software being used
- Is new in Windows Server 2012 R2



**Intranet Application**



**Web Application Proxy**



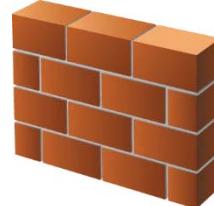
**Internet**

# Publishing an Application in Web Application Proxy

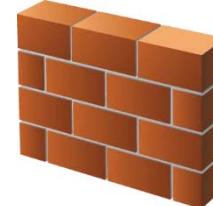
- Preauthentication options:
  - Pass-through
  - AD FS
- URLs:
  - External
  - Backend server
- Certificates



**Intranet Application**



**Web Application Proxy**



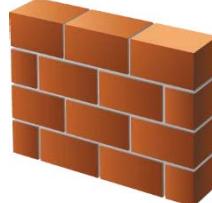
**Internet**

# Web Application Proxy and AD FS

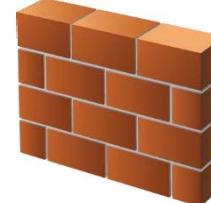
- Web Application Proxy includes federation service proxy functionality
- The same certificate is used on the AD FS server and Web Application Proxy
- Split DNS allows the same name to resolve to different IP addresses



**AD FS Server**  
**adfs.adatum.com**  
**172.16.0.21**



**Web Application Proxy**  
**adfs.adatum.com**  
**10.10.0.100**



**Internet**

# Demonstration: Installing and Configuring Web Application Proxy

- In this demonstration, you will see how to:
  - Install Web Application Proxy
  - Export the certificate from the AD FS server
  - Import the certificate to the Web Application Proxy server
  - Configure Web Application Proxy

# What Is Workplace Join?

## Workplace Join:

- Creates an object in AD DS for non-domain joined devices
- Works with Windows 8.1 and iOS devices
- Can control access to claims-aware applications
- Enables SSO for application access

## Enabling Workplace Join

1. `Enable-AdfsDeviceRegistration –PrepareActiveDirectory`
2. `Enable-AdfsDeviceRegistration`
3. Enable Device Authentication in AD FS

# The Workplace Join Process

To perform a Workplace Join the service communication certificate for AD FS must be trusted by devices

Devices running Windows:

- Require a UPN for authentication
- Access by using [enterpriseregistration.upndomainname.com](http://enterpriseregistration.upndomainname.com)

Devices running iOS use Safari to install a configuration profile

A certificate is placed on the device for authentication

# Performing a Workplace Join

```
Administrator: Windows PowerShell
PS C:\> Initialize-ADDeviceRegistration -ServiceAccountName Adatum\ADFS$
This command will prepare Active Directory to host Device Registration Service
in the current forest.
Do you want to continue with this operation?
[Y] Yes [A] Yes to All [N] No [L] No to All [S] Suspend [?] Help
(default is "Y"):y
WARNING: The Active Directory forest has been prepared for Device Registration.
To use the AD FS Device Registration Service, run the Enable-AdfsDeviceRegistration cmdlet on each node in your AD FS farm.

Message	Context	Status
-----	-----	-----
The configuration compl...	DeploymentSucceeded	Success

PS C:\> Enable-AdfsDeviceRegistration

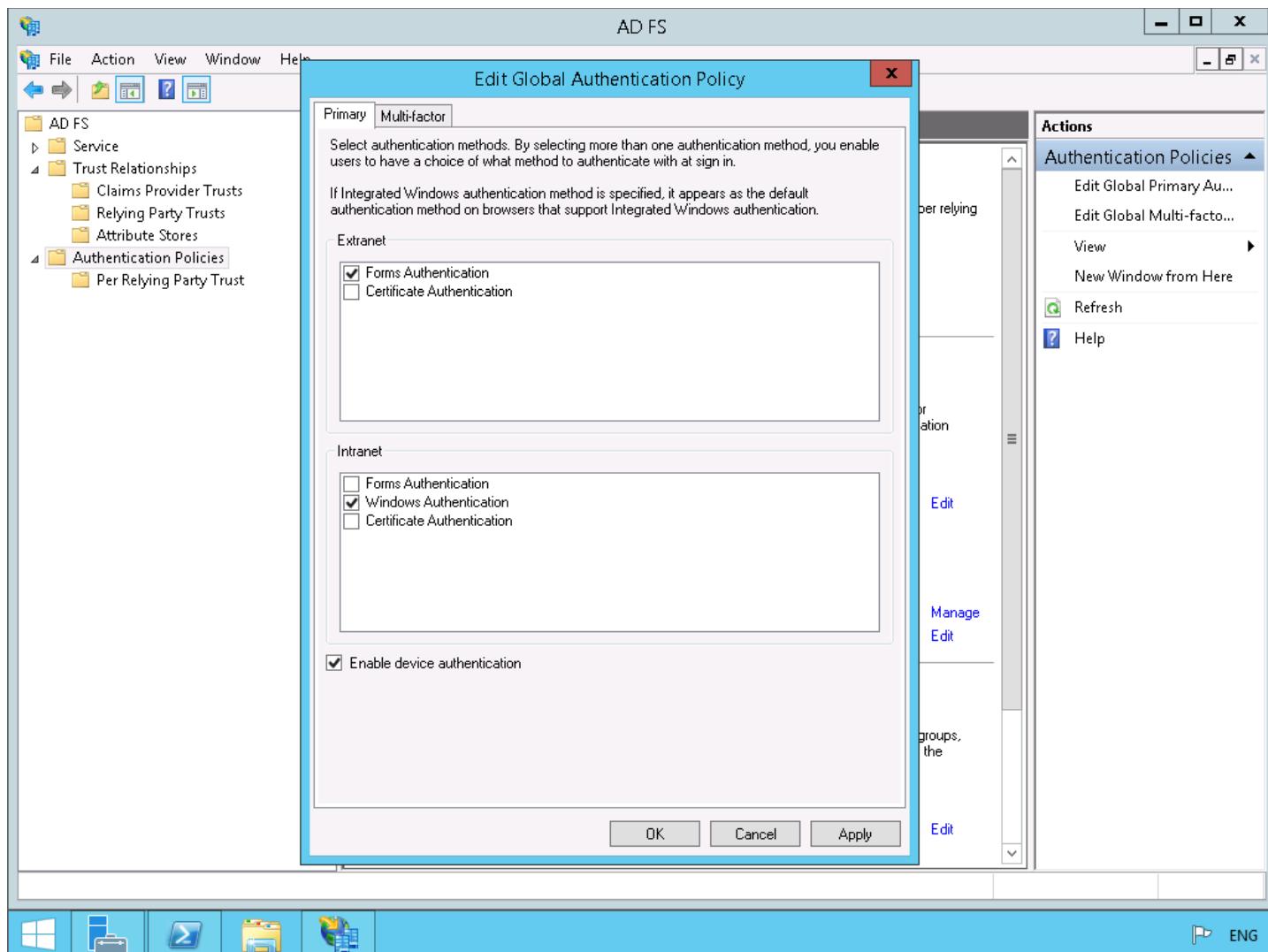
Message	Context	Status
-----	-----	-----
The configuration compl...	DeploymentSucceeded	Success

PS C:\> -
```

Enable Device Registration



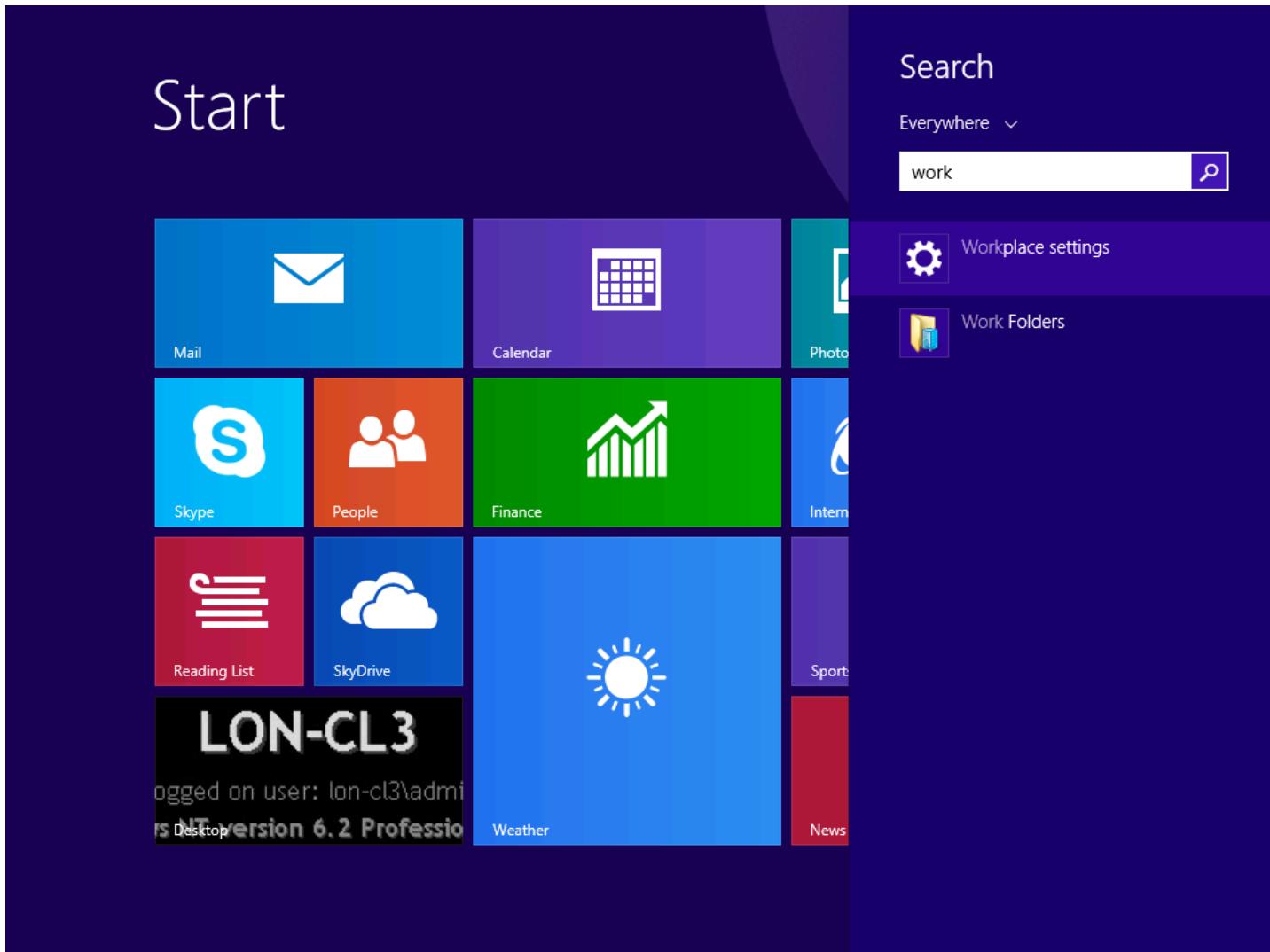
# Performing a Workplace Join



Enable device authentication in AD FS



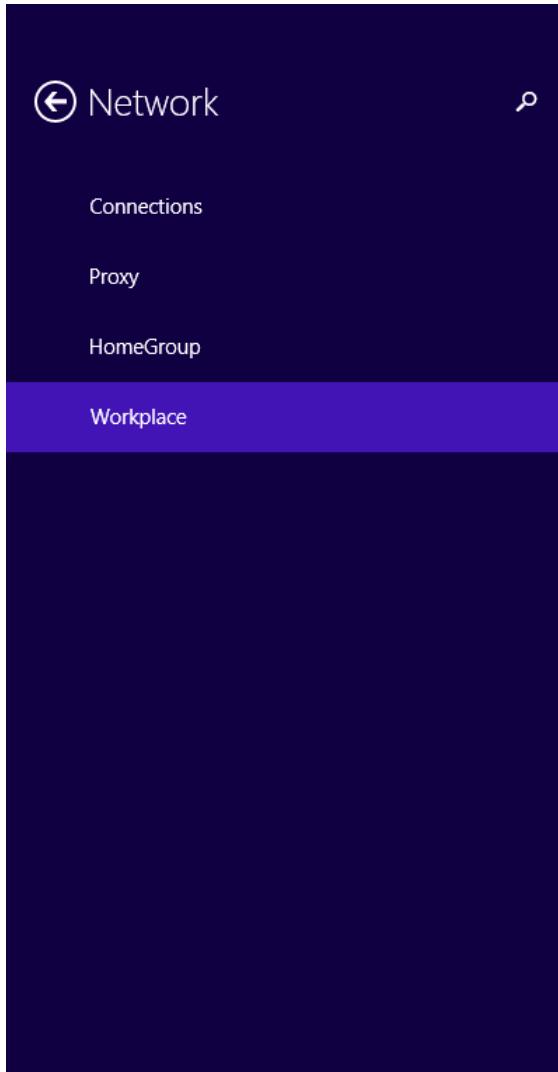
# Performing a Workplace Join



Go to Workplace settings on the client



# Performing a Workplace Join



## Workplace

Enter your user ID to get workplace access or turn on device management

Join your workplace network so that you can use network resources like internal websites and business apps

[Join](#)

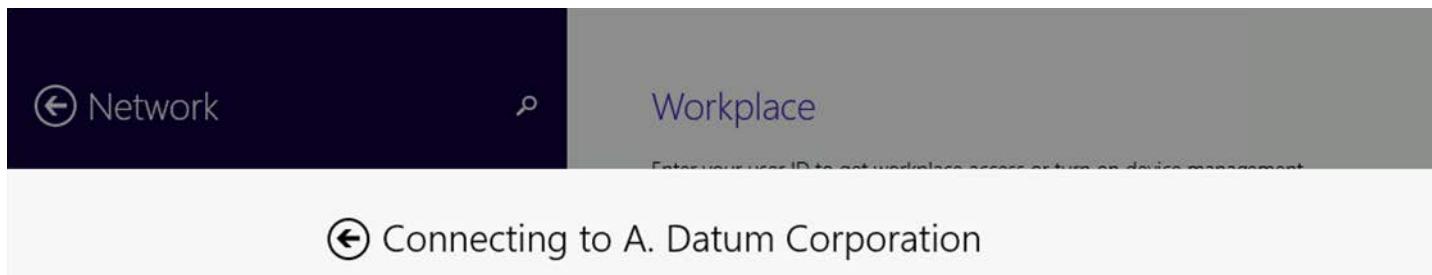
With device management turned on, your IT admin can set up apps and services for you

[Turn on](#)

Enter the email address/UPN



# Performing a Workplace Join



A. Datum Corporation

Sign in with your organizational account

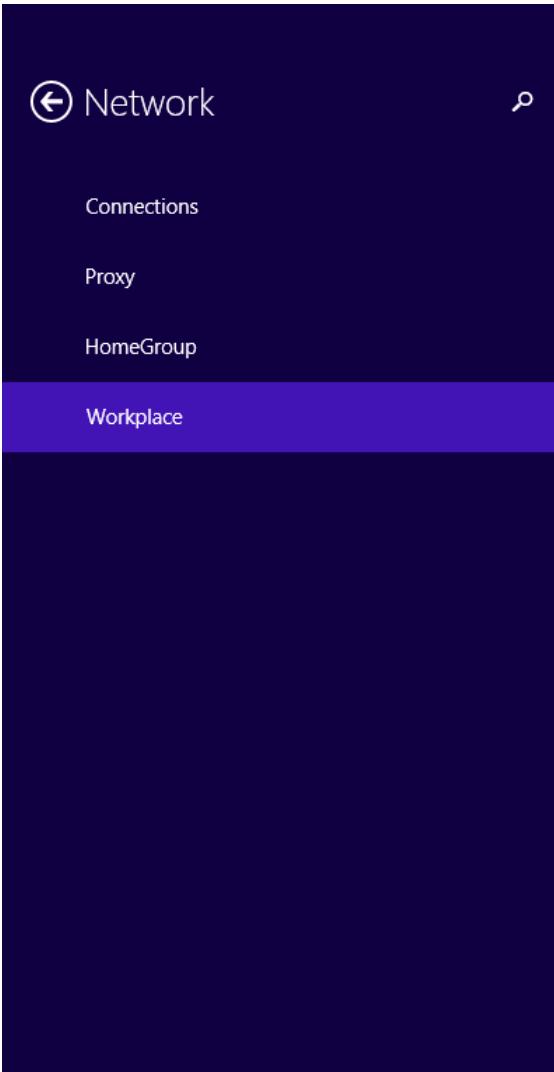
  

Sign in

© 2013 Microsoft



# Performing a Workplace Join



## Workplace

Enter your user ID to get workplace access or turn on device management

brad@adatum.com

Join your workplace network so that you can use network resources like internal websites and business apps

Join



Connecting to workplace

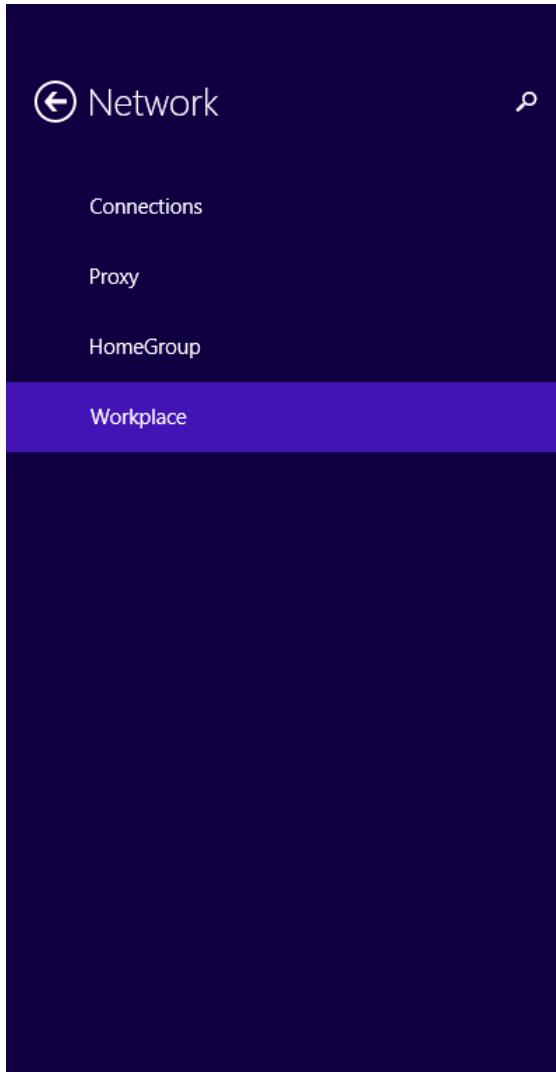
With device management turned on, your IT admin can set up apps and services for you

Turn on

Wait a few moments while connecting



# Performing a Workplace Join



Workplace

Enter your user ID to get workplace access or turn on device management

brad@adatum.com

This device has joined your workplace network

Leave

With device management turned on, your IT admin can set up apps and services for you

Turn on

Workplace join completed successfully



# Performing a Workplace Join

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is open, showing the following structure:

- Active Directory...
- Overview
- Adatum (local)** (selected)
- RegisteredDevices (selected)
- Dynamic Access Control
- Global Search

The main content area displays a table titled "RegisteredDevices (1)". The table has columns: Name, Type, and Description. One row is listed:

| Name                                 | Type           | Description |
|--------------------------------------|----------------|-------------|
| d39bab35-abcd-43bd-9e05-36e05-36e... | msDS-Device... |             |

A context menu is open for the selected row, listing options: Delete, Move..., Properties. Below the table, a summary box shows:

Object class: msDS-Device      Modified: 2/19/2014 8:31 PM  
Description:

Summary

At the bottom, a Windows PowerShell history bar is visible with several icons.

An object is created in AD DS for the device



# Performing a Workplace Join

The screenshot shows the Active Directory Administrative Center interface. The left navigation pane is titled "Active Directory" and includes links for Overview, Adatum (local), RegisteredDevices, Dynamic Access Control, and Global Search. The main content area is titled "d39bab35-abcd-43bd-9e05-36edc02f5771". The "Extensions" tab is selected, displaying the "Attribute Editor" tab. The "Attributes" table lists several attributes and their values:

| Attribute             | Value                                   |
|-----------------------|-----------------------------------------|
| adminDescription      | <not set>                               |
| adminDisplayName      | <not set>                               |
| altSecurityIdentities | X509:<SHA1-TP-PUBKEY>EA2288E9BEE2       |
| cn                    | d39bab35-abcd-43bd-9e05-36edc02f5771    |
| description           | <not set>                               |
| displayName           | LON-CL3                                 |
| displayNamePrintable  | <not set>                               |
| distinguishedName     | CN=d39bab35-abcd-43bd-9e05-36edc02f5771 |
| dsASignature          | <not set>                               |
| dsCorePropagationD... | 0x0 = ( )                               |
| extensionName         | <not set>                               |
| flags                 | <not set>                               |
| ISMORoleOwner         | <not set>                               |
| instanceType          | 0x4 = (WRITE )                          |

The right pane displays a "Tasks" list for the object "d39bab35-abcd-43bd-9e05-36edc02f5771" under "RegisteredDevices". The tasks include Delete, Move..., Properties, and a context menu item for "d39bab35-abcd-43bd-9e05-36edc02f5771". Below the tasks is a "New" link and a "Search under this node" field.

Properties of the registered device

ENG

# Performing a Workplace Join

The screenshot shows a web browser window with the URL <https://lon-svr1.adatum.com/AdatumTestApp/>. The page displays two sections of claims:

**Values from IIIdentity**

|                      |                  |
|----------------------|------------------|
| IsAuthenticated:True | Name:Brad Sutton |
|----------------------|------------------|

**Claims from IClaimsIdentity**

| Claim Type                                                                    | Claim Value                                                                   | Type     |
|-------------------------------------------------------------------------------|-------------------------------------------------------------------------------|----------|
| http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname    | ADATUM\Brad                                                                   | string   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn                     | Brad@adatum.com                                                               | string   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn                     | brad@adatum.com                                                               | string   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name                    | Brad Sutton                                                                   | string   |
| http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name                    | ADATUM\Brad                                                                   | string   |
| http://schemas.microsoft.com/2012/01/devicecontext/claims/displayname         | LON-CL3                                                                       | string   |
| http://schemas.microsoft.com/2012/01/devicecontext/claims/ostype              | Windows                                                                       | string   |
| http://schemas.microsoft.com/2012/01/devicecontext/claims/osversion           | 6.3.9600.0                                                                    | string   |
| http://schemas.microsoft.com/2012/01/devicecontext/claims/ismanaged           | false                                                                         | boolean  |
| http://schemas.microsoft.com/2012/01/devicecontext/claims/isregistereduser    | true                                                                          | boolean  |
| http://schemas.microsoft.com/2012/01/devicecontext/claims/identifier          | 2733927a-bf38-45e8-ba92-b80142a8e6af                                          | string   |
| http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod  | http://schemas.microsoft.com/ws/2008/06/identity/authenticationmethod/windows | string   |
| http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant | 2014-02-20T04:54:20.144Z                                                      | dateTime |

Claims presented to an application



ENG

# Lab B: Implementing AD FS for External Partners and Users

- Exercise 1: Configuring AD FS for a Federated Business Partner
- Exercise 2: Configuring Web Application Proxy

## Logon Information

Virtual machines: 20412D-LON-DC1, 20412D-LON-SVR1,  
20412D-LON-SVR2, 20412D-TREY-DC1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 45 minutes

# Lab Scenario

A. Datum Corporation has set up a variety of business relationships with other companies and customers. Some of these partner companies and customers must access business applications that are running on the A. Datum network. The business groups at A. Datum want to provide a maximum level of functionality and access to these companies. The Security and Operations departments want to ensure that the partners and customers can access only the resources to which they require access, and that implementing the solution does not increase the workload for the Operations team significantly. A. Datum also plans to migrate some parts of its network infrastructure to Microsoft Online Services, including Windows Azure and Office 365.

# Lab Scenario

Now that you have deployed AD FS for internal users, the next step is to enable access to the same application for external partner organizations and for external users. A. Datum Corporation has entered into a partnership with Trey Research. You need to ensure that Trey Research users can access the internal application. You also need to ensure that A. Datum Corporation users working outside the office can access the application.

As one of the senior network administrators at A. Datum, it is your responsibility to implement the AD FS solution. As a proof-of-concept, you are deploying a sample claims-aware application, and configuring AD FS to enable both Trey Research users and external A. Datum Corporation users to access the same application.

# Lab Review

- Why does using certificate from a trusted provider on the Internet negate the need to configure certificate trusts between organizations?
- Could you have created authorization rules in Adatum.com and achieved the same result if you had instead created authorization rules in TreyResearch.net?

# Module Review and Takeaways

- Review Questions

# Microsoft® Official Course



Module 9

Implementing Network Load  
Balancing

**Microsoft®**

# Module Overview

- Overview of NLB
- Configuring an NLB Cluster
- Planning an NLB Implementation

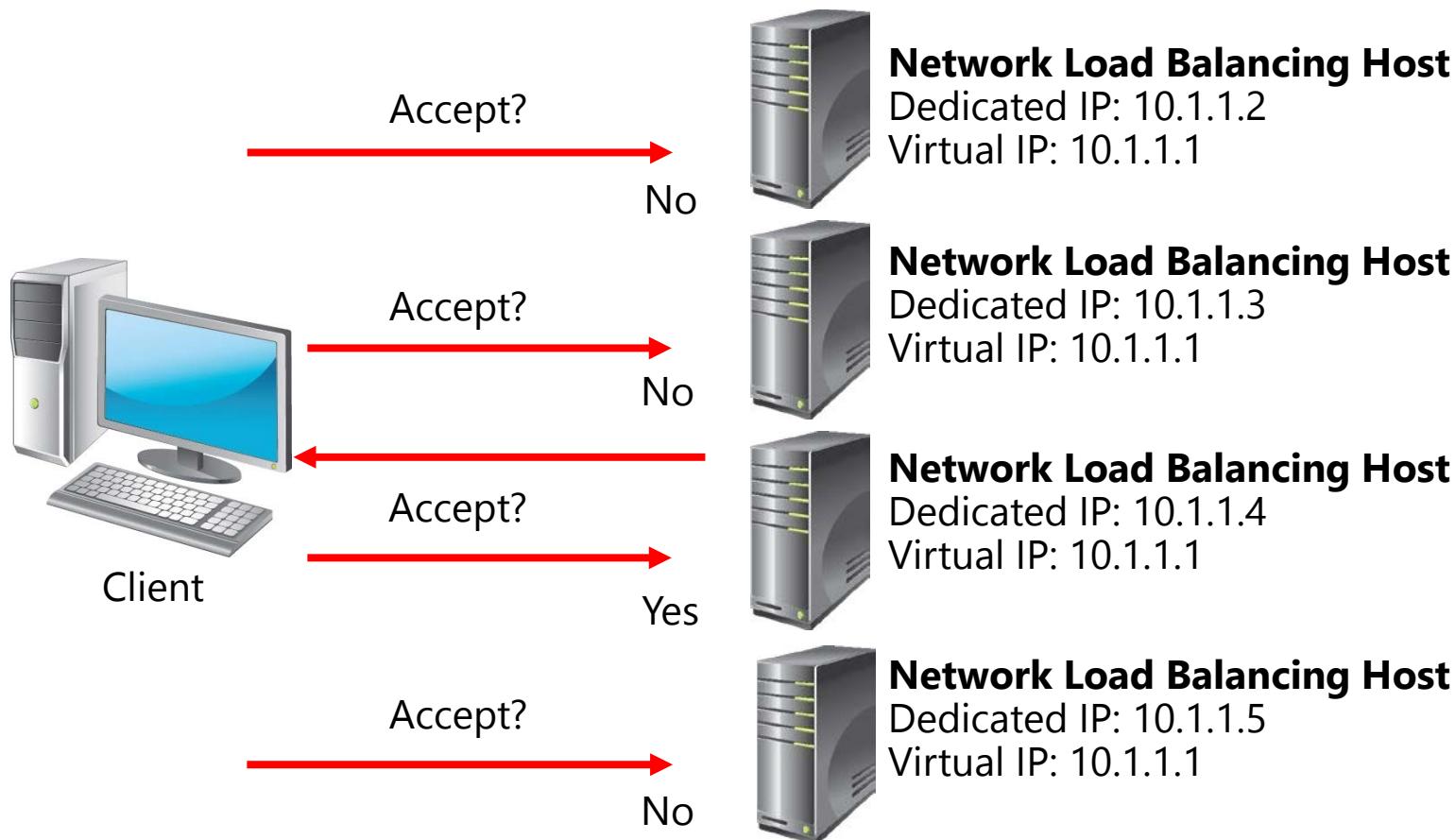
# Lesson 1: Overview of NLB

- What Is NLB?
- How NLB Works
- How NLB Works with Server Failures and Recovery
- NLB Features in Windows Server 2012 and Windows Server 2012 R2

# What Is NLB?

- Scalable high-availability technology
- Balances traffic based on node utilization
  - New traffic will be directed to the node that is being utilized the least
  - You can configure NLB to preference some nodes over others
- Used with stateless applications such as:
  - Web tiers of multi-tier applications
- Not used with stateful applications such as:
  - Traditional file servers
  - Database servers

# How NLB Works



# How NLB Works with Server Failures and Recovery

NLB cluster heartbeats are transmitted every second between nodes in a cluster

Convergence occurs when:

- A node misses five consecutive heartbeats, at which time it is automatically removed from an NLB cluster
- A node that was member of a cluster returns to functionality
- An administrator adds or removes a node manually

# NLB Features in Windows Server 2012 and Windows Server 2012 R2

Use 35 new NLB Windows PowerShell cmdlets to manage all aspects of NLB configuration

- Use `NlbCluster` noun to manage the cluster
- Use `NlbClusterNode` noun to manage individual nodes

## Lesson 2: Configuring an NLB Cluster

- Deployment Requirements for NLB
- Demonstration: Deploying NLB
- Configuration Options for NLB
- Demonstration: Configuring NLB Affinity and Port Rules
- Network Considerations for NLB

# Deployment Requirements for NLB

- All hosts must be on the same subnet
- All adapters must be configured as either unicast or multicast
- Only TCP/IP protocol can be used on adapters
- All adapters used with NLB must be configured with static IP address

# Demonstration: Deploying NLB

In this demonstration, you will see how to create a Windows Server 2012 R2 NLB cluster

# Configuration Options for NLB

Port rules determine how traffic is directed to cluster nodes depending on TCP or UDP port

- Multiple hosts
- Single host
- Disable port range

Affinity settings determine how reconnection occurs

- None
- Single
- Class C

# Demonstration: Configuring NLB Affinity and Port Rules

In this demonstration, you will see how to:

- Configure affinity for NLB cluster nodes
- Configure NLB port rules

# Network Considerations for NLB

## Unicast mode

- Suitable for clusters that have multiple network adapters

## Multicast mode

- Suitable for NLB clusters that have single network adapters
- Network devices must support multicast MAC addresses

## IGMP multicast

- Improves switch performance
- Requires a network switch that supports this functionality

# Lesson 3: Planning an NLB Implementation

- Designing Applications and Storage Support for NLB
- Considerations for Deploying an NLB Cluster on Virtual Machines
- Considerations for Securing NLB
- Considerations for Scaling NLB
- Considerations for Upgrading NLB Clusters

# Designing Applications and Storage Support for NLB

- Each node in an NLB cluster needs to have the same configuration
- Each node needs access to the same consistent application data
- Use IIS shared configuration to ensure that web application configuration is consistent across NLB nodes
- Use CSVs to host shared application and configuration data for NLB applications

# Considerations for Deploying an NLB Cluster on Virtual Machines

- Configure virtual machines with multiple network adapters
- Configure one network adapter on each node member to use a shared private network switch
- Configure the NLB cluster to use unicast mode and enable MAC address spoofing on Hyper-V host
- Use the shared private network switch for cluster communication
- When NLB nodes span multiple sites, use network virtualization to separate the cluster network

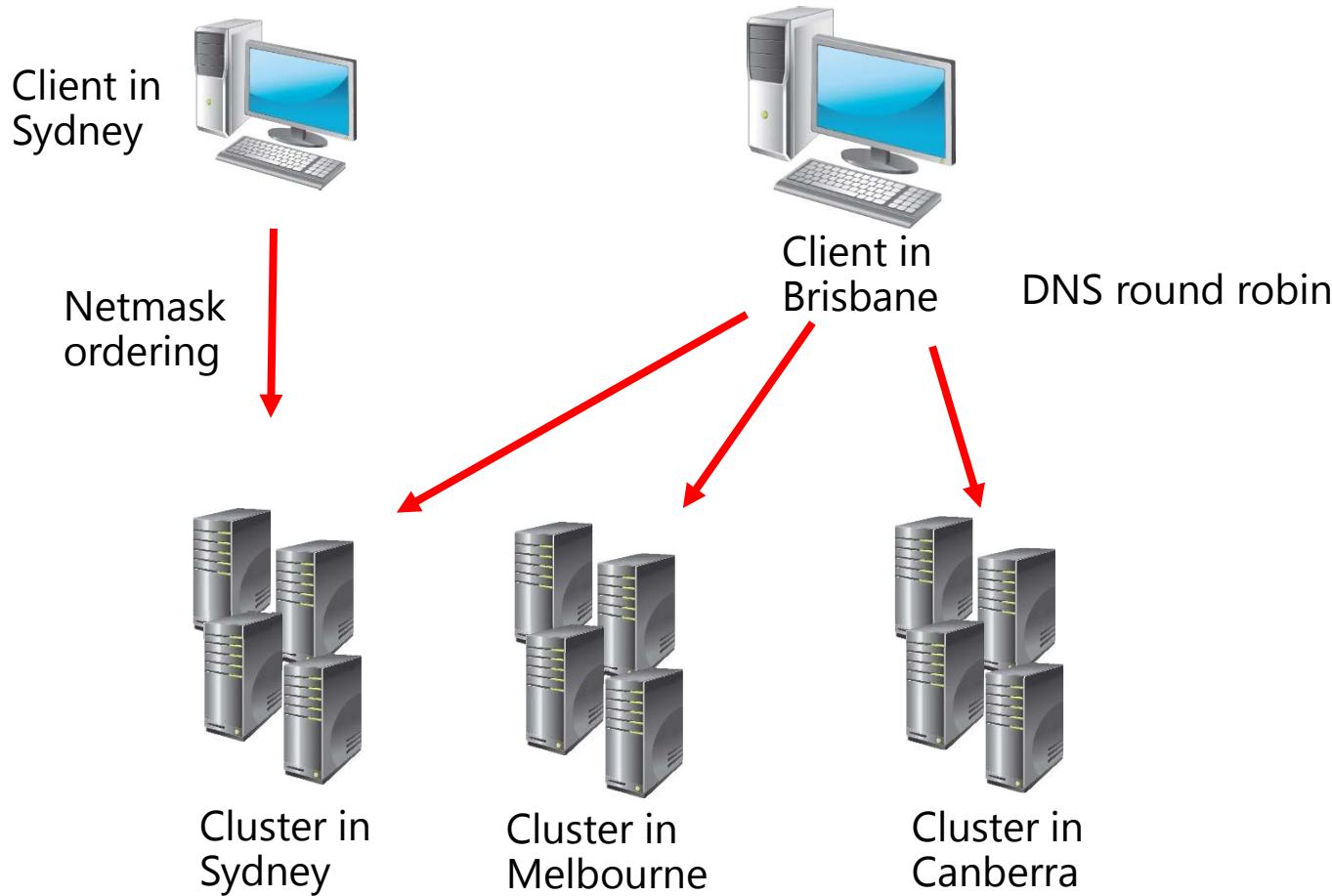
# Considerations for Securing NLB

- Use NLB cluster port rules to discard traffic not related to cluster applications
- Use firewall rules on cluster nodes to drop traffic not related to cluster applications or node management
- Configure applications to respond only to traffic that is addressed to the cluster
- Use SANs to create certificates that support the application name and node names
- Implement principle of least privilege to ensure that only authorized users have appropriate permissions on nodes

# Considerations for Scaling NLB

NLB clusters can have up to 32 nodes

Use DNS round robin to distribute traffic between NLB clusters



# Considerations for Upgrading NLB Clusters

NLB clusters can run with different operating systems

- Windows Server 2012 R2 NLB clusters can interoperate with:
  - Windows Server 2003 & Windows Server 2003 R2
  - Windows Server 2008 & Windows Server 2008 R2
  - Windows Server 2012
- Piecemeal upgrade:
  - Add Windows Server 2012 R2 cluster nodes
  - Remove nodes running earlier operating systems
- Upgrade clusters:
  1. Remove node from NLB cluster
  2. Upgrade to Windows Server 2012 R2
  3. Rejoin node to NLB cluster

# Lab: Implementing NLB

- Exercise 1: Implementing an NLB Cluster
- Exercise 2: Configuring and Managing the NLB Cluster
- Exercise 3: Validating High Availability for the NLB Cluster

## Logon Information

Virtual machines: 20412D-LON-DC1

20412D-LON-SVR1

20412D-LON-SVR2

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 45 minutes

# Lab Scenario

A. Datum Corporation is an engineering and manufacturing company. The organization is based in London, England, and is quickly expanding into Australia. As the company expands, the need for scalable web applications has increased. To address this need, you will develop a pilot program to test the deployment of NLB on hosts running the Windows Server 2012 operating system.

Because you intend to automate the process of deploying Windows NLB clusters, you will use Windows PowerShell to perform many of the cluster setup and configuration tasks. You also will configure port rules and affinity, which will allow you to deploy multiple load balanced web applications on the same Windows NLB clusters.

# Lab Review

- How many additional nodes can you add to the LON-NLB cluster?
- What steps would you take to ensure that LON-SVR1 always manages requests for web traffic on port 5678, given the port rules established by the end of this exercise?
- What is the difference between a Stop and a Drainstop command?

# Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios

# Microsoft® Official Course



## Module 10

### Implementing Failover Clustering

**Microsoft®**

# Module Overview

- Overview of Failover Clustering
- Implementing a Failover Cluster
- Configuring Highly Available Applications and Services on a Failover Cluster
- Maintaining a Failover Cluster
- Implementing a Multisite Failover Cluster

# Lesson 1: Overview of Failover Clustering

- What Is High Availability?
- Failover Clustering Improvements in Windows Server 2012
- Failover Clustering Improvements in Windows Server 2012 R2
- Failover Cluster Components
- What Are CSVs?
- New CSV Features in Windows Server 2012 R2
- What Are Failover and Failback?
- What Is Quorum?
- Quorum Modes in Windows Server 2012 Failover Clustering
- How Quorum Works in Windows Server 2012 R2 Failover Clustering
- Failover Cluster Networks
- Failover Cluster Storage

# What Is High Availability?

- Availability is a level of service expressed as a percentage of time
- Highly-available services or systems are available more than 99 percent of the time
- High availability requirements differ based on how availability is measured
- Planned outages typically are not included when calculating availability

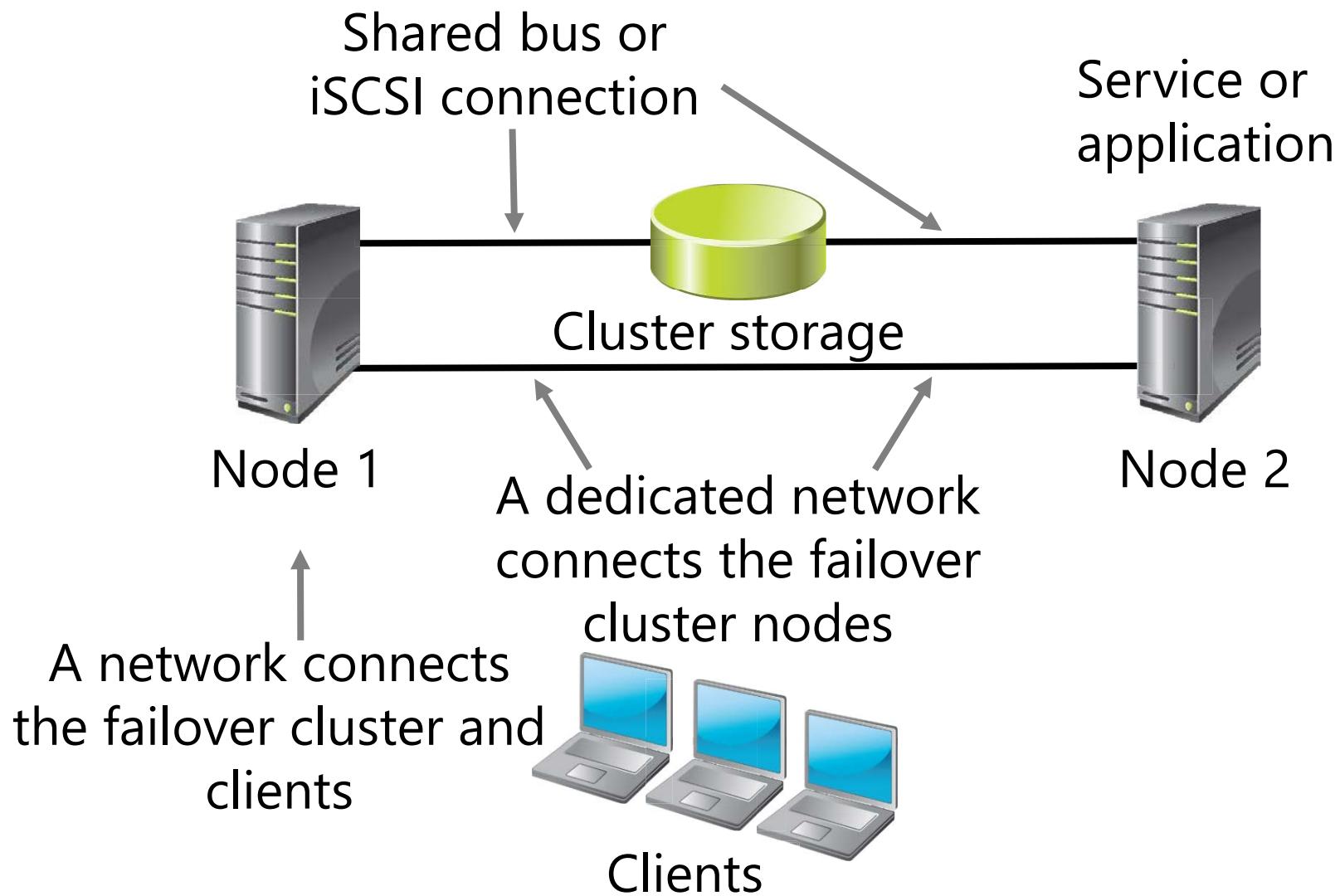
# Failover Clustering Improvements in Windows Server 2012

| Failover clustering improvements in Windows Server 2012                                                                                                                                                                | Removed and deprecated failover clustering features in Windows Server 2012                                                                                                                                       |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <ul style="list-style-type: none"><li>• Increased scalability</li><li>• Improved CSVs</li><li>• Cluster-aware updating</li><li>• Active Directory integration improvements</li><li>• Management improvements</li></ul> | <ul style="list-style-type: none"><li>• Cluster.exe command-line tool</li><li>• Cluster Automation Server (MSClus) COM interface</li><li>• Add-ClusterPrintServerRole cmdlet</li><li>• Printer cluster</li></ul> |

# Failover Clustering Improvements in Windows Server 2012 R2

- Significant new features of failover clustering in Windows Server 2012 R2 include:
  - Quorum changes and dynamic witness
  - Force quorum resiliency
  - Tie breaker for 50% node split
  - Global Update Manager mode
  - Cluster node health detection
  - AD DS-detached cluster

# Failover Cluster Components



# What Are CSVs?

The benefits of CSVs include:

- Fewer LUNs required
- Better use of disk space
- Resources in a single logical location
- No special hardware required
- Increased resiliency

To implement CSV:

1. Create and format volumes on shared storage
2. Add the disks to failover cluster storage
3. Add the storage to the CSV

# New CSV Features in Windows Server 2012 R2

- CSVs in Windows Server 2012 R2 provide the following enhancements and new functionalities:
  - Optimized CSV placement policies
  - Increased CSV resiliency
  - CSV cache allocation
  - CSV diagnosis
  - CSV interoperability

# What Are Failover and Failback?

- During failover, the clustered instance and all associated resources are moved from one node to another
- Failover occurs when:
  - The node that currently hosts the instance becomes inactive for any reason
  - One of the resources within the instance fails
  - An administrator forces a failover
- Cluster service can fallback after the offline node becomes active again

# What Is Quorum?

- In failover clusters, quorum defines the consensus that enough cluster members are available to provide services
- Quorum:
  - Is based on votes in Windows Server 2012
  - Enables nodes, file shares, or a shared disk to have a vote, depending on the quorum mode
  - Enables the failover cluster to remain online when sufficient votes are available

# Quorum Modes in Windows Server 2012 Failover Clustering

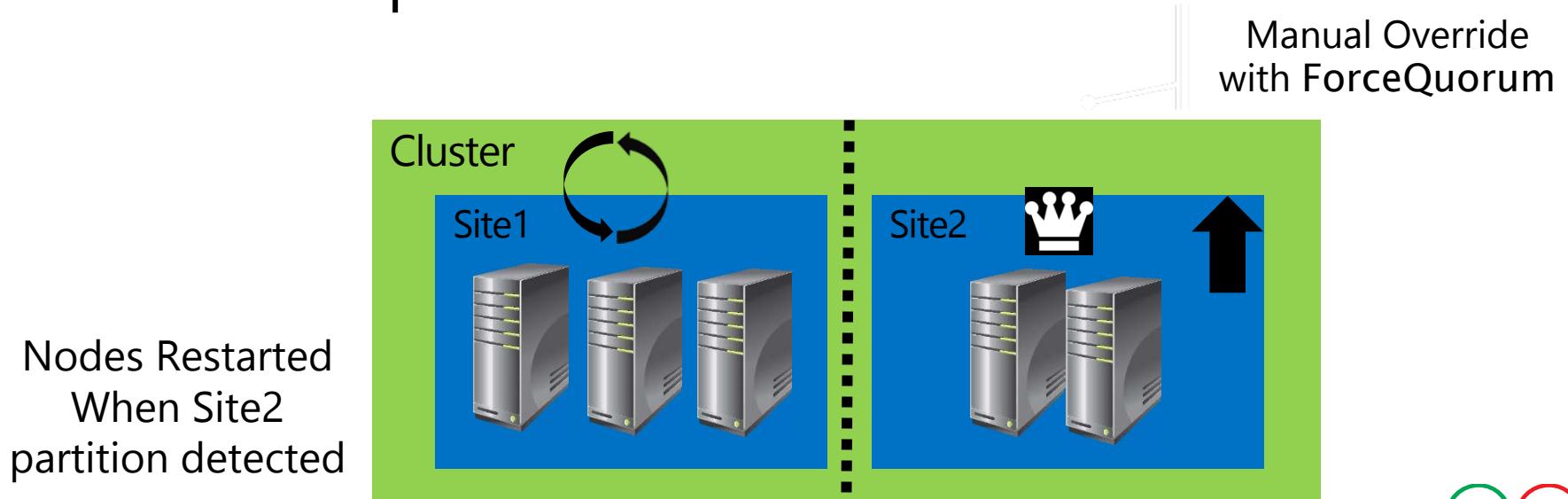
| Quorum mode                    | What has the vote?                                            | When is quorum maintained?                                       |
|--------------------------------|---------------------------------------------------------------|------------------------------------------------------------------|
| • Node Majority                | Only nodes in the cluster have a vote                         | Quorum is maintained when more than half of the nodes are online |
| • Node and Disk Majority       | The nodes in the cluster and a disk witness have a vote       | Quorum is maintained when more than half of the votes are online |
| • Node and File Share Majority | The nodes in the cluster and a file share witness have a vote | Quorum is maintained when more than half of the votes are online |
| • No Majority: Disk Only       | Only the quorum-shared disk has a vote                        | Quorum is maintained when the shared disk is online              |

# How Quorum Works in Windows Server 2012 R2 Failover Clustering

- The legacy concept of quorum mode is removed
- Dynamic quorum automatically adjusts votes to maintain cluster functionality
- You can define which nodes have a quorum vote
  - Configurable for 1 vote or 0 votes
- Always configure a witness disk with Windows Server 2012 R2
  - Clustering will determine when it is best to use it
- Witness vote dynamically/automatically adjusted based on cluster membership with dynamic quorum
  - Odd node votes (3) + no witness vote (0) = 3
  - Even node votes (2) + witness vote (1) = 3

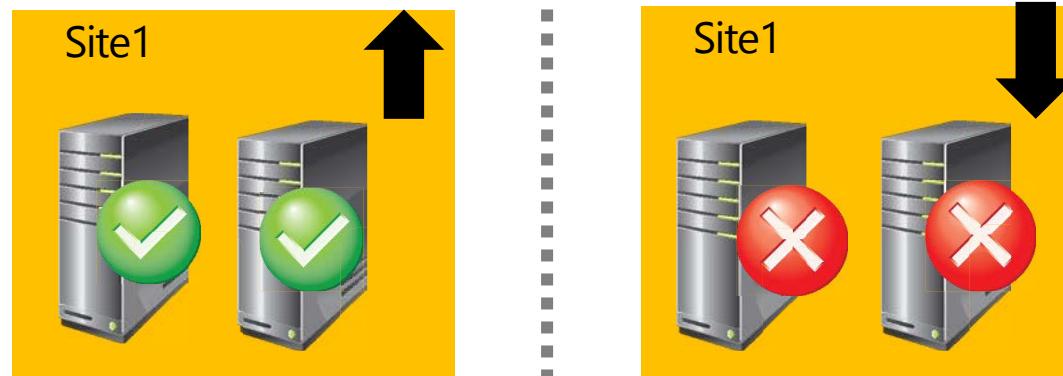
# Force Quorum Resiliency in Windows Server 2012 R2

- The cluster detects partitions after a manual ForceQuorum
- ForceQuorum partition is deemed authoritative
- Partitioned nodes restarted and rejoined
- Cluster brought back into a single view of membership



# Quorum Tie Breaker in Windows Server 2012 R2

- Cluster will survive simultaneous 50% loss of votes
- Balanced multi-site clusters with complete site partition
- One site automatically elected to win
- Winning site can be controlled with the `LowerQuorumPriorityNodeID` cluster common property
- Nodes in the other site drop out of the cluster



# Failover Cluster Networks

| Network                      | Description                                                                                                                                                                                                                                                           |
|------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| • Public network             | Clients use this network to connect to the clustered service                                                                                                                                                                                                          |
| • Private network            | Nodes use this network to communicate with each other                                                                                                                                                                                                                 |
| • Public-and-private network | Required to communicate with external storage systems                                                                                                                                                                                                                 |
|                              | <ul style="list-style-type: none"><li>• One network can support both client and node communications</li><li>• Multiple network cards are recommended to provide enhanced performance and redundancy</li><li>• iSCSI storage should have a dedicated network</li></ul> |

# Failover Cluster Storage

- Failover clusters require shared storage to provide consistent data to a virtual server after failover
- Shared storage options include:
  - Serial attached SCSI
  - iSCSI
  - Fibre channel
  - Shared VHDX (2012 R2)
- You can also implement clustered storage spaces to achieve high availability at the storage level



# Lesson 2: Implementing a Failover Cluster

- Preparing for Failover Cluster Implementation
- Hardware Requirements for Failover Cluster Implementation
- Network Requirements for Failover Cluster Implementation
- Infrastructure Requirements for Failover Cluster
- Software Requirements for Failover Cluster Implementation
- Demonstration: Validating and Configuring a Failover Cluster
- Migrating and Upgrading Failover Clusters

# Preparing for Failover Cluster Implementation

Use failover clustering when:

- High availability is required
- Scalability is not required
- The application is stateful
- Client or protocol automatically reconnects to the application
- Application uses IP-based protocols

# Hardware Requirements for Failover Cluster Implementation

The hardware requirements for a failover implementation include:

- Server hardware components must have the Certified for Windows Server 2012 logo
- Server nodes should all have the same configuration and contain the same or similar components
- All tests in the Validate a Configuration Wizard must pass

# Network Requirements for Failover Cluster Implementation

The network requirements for a failover implementation include:

- The network hardware components must have the Certified for Windows Server 2012 logo
- The server should be connected to multiple networks for communication redundancy, or to a single network with redundant hardware, to remove single points of failure
- The network adapters should be identical and have the same IP protocol versions, speed, duplex, and flow control capabilities

# Infrastructure Requirements for Failover Cluster

- The infrastructure requirements for a failover cluster implementation include:
  - The nodes in the cluster must use DNS for name resolution
  - All servers in the cluster must be in the same Active Directory domain
  - The user account that creates the cluster must have administrator rights and permissions on all servers, and the Create Computer Objects permission in the domain
- Failover cluster infrastructure recommendations include:
  - The same roles should be installed on each cluster node
  - The AD DS role should not be installed on any of the cluster nodes

# Software Requirements for Failover Cluster Implementation

The software requirements for a failover cluster implementation include:

- All nodes must run the same edition of Windows Server 2012 or 2012 R2, which can be any of the following:
  - Windows Server 2012 or 2012 R2 Standard, Full or Server Core installation
  - Windows Server 2012 or 2012 R2 Datacenter, Full or Server Core installation
- All nodes must run the same processor architecture (x64-based)
- All nodes should have the same service pack and updates

# Demonstration: Validating and Configuring a Failover Cluster

In this demonstration, you will see how to validate and configure a cluster

# Migrating and Upgrading Failover Clusters

You can migrate clustered roles from one cluster to another, and you can perform migration by:

- Migrating clustered roles to a new cluster with new servers
- Performing in-place migration with only two nodes

The Cluster Migration Wizard migrates roles, but not data or folders

# Lesson 3: Configuring Highly Available Applications and Services on a Failover Cluster

- Identifying Cluster Resources and Services
- The Process for Clustering Server Roles
- Demonstration: Clustering a File Server Role
- Failover Cluster Management Tasks
- Managing Cluster Nodes
- Configuring Application Failover Settings

# Identifying Cluster Resources and Services

- Clustered services:
  - Are services or applications that are made highly available by installing them on a failover cluster
  - Are active on one node, but can be moved to another node
- Resources:
  - Are the components that make up a clustered service
  - Are moved to another node when one node fails
  - Can only run on one node at a time
  - Include components such as shared disks, names, and IP addresses

# The Process for Clustering Server Roles

1. Install the failover clustering feature
2. Verify the configuration and create a cluster
3. Install the role on all cluster nodes, using Server Manager
4. Create a clustered application by using the Failover Cluster Management snap-in
5. Configure the application
6. Test the failover

# Demonstration: Clustering a File Server Role

In this demonstration, you will see how to cluster a file server role

# Failover Cluster Management Tasks

The most common management tasks include:

- Managing nodes
- Managing networks
- Managing permissions
- Configuring cluster quorum settings
- Migrating services and applications to a cluster
- Configuring new services and applications
- Removing the cluster

# Managing Cluster Nodes

To manage cluster nodes, you can:

- Add nodes after you create a cluster
- Pause nodes, which prevents resources from running on that node
- Evict nodes from a cluster, which removes the node from the cluster configuration

All of these actions are available in the Failover Cluster Management Actions pane

# Configuring Application Failover Settings

The considerations for using preferred owners include:

- Preferred owners are set on the clustered application
- Multiple preferred owners can be set in an ordered list
- Setting preferred owners gives control over:
  - The order in which an application will select a node to run on
  - The applications that can be run on the same nodes in an Active/Active configuration

The options to modify failover and fallback settings include:

- Setting the number of times the cluster service will restart a clustered application in a set period of time
- Setting or preventing failback of the clustered application to the preferred node when it becomes available

# Lesson 4: Maintaining a Failover Cluster

- Monitoring Failover Clusters
- Backing Up and Restoring Failover Cluster Configuration
- Maintaining and Troubleshooting Failover Clusters
- What Is CAU?
- Demonstration: Configuring CAU

# Monitoring Failover Clusters

Some of the tools you can use to monitor clusters include:

- Event Viewer
- Tracerpt.exe
- Performance and Reliability Monitor snap-in
- MHTML-formatted cluster configuration reports
- Validate a Configuration Wizard

# Backing Up and Restoring Failover Cluster Configuration

When backing up failover clusters, keep in mind that:

- Windows Server backup is an optional Windows Server 2012 feature
- Backup and restore operations involve the VSS
- Third-party tools are also available to perform backups and restores
- You must perform system-state backups

Two types of restore are:

- A non-authoritative restore completely restores a single node in the cluster
- An authoritative restore restores the entire cluster configuration to a point in time

# Maintaining and Troubleshooting Failover Clusters

Failover cluster troubleshooting techniques include:

- Reviewing events in logs, such as: cluster, hardware and storage
- Using the Validate a Configuration Wizard
- Defining a process for troubleshooting failover clusters
- Reviewing storage configuration
- Checking for group and resource failures

# What Is CAU?

- CAU:
  - Automated feature specific to Windows Server 2012
  - Updates nodes in a cluster with minimal or zero downtime
- Benefits:
  - Cluster updating is completely automatic
  - Can be scheduled
  - No downtime
- CAU can work in two modes:
  - Remote-updating mode
  - Self-updating mode

# Demonstration: Configuring CAU

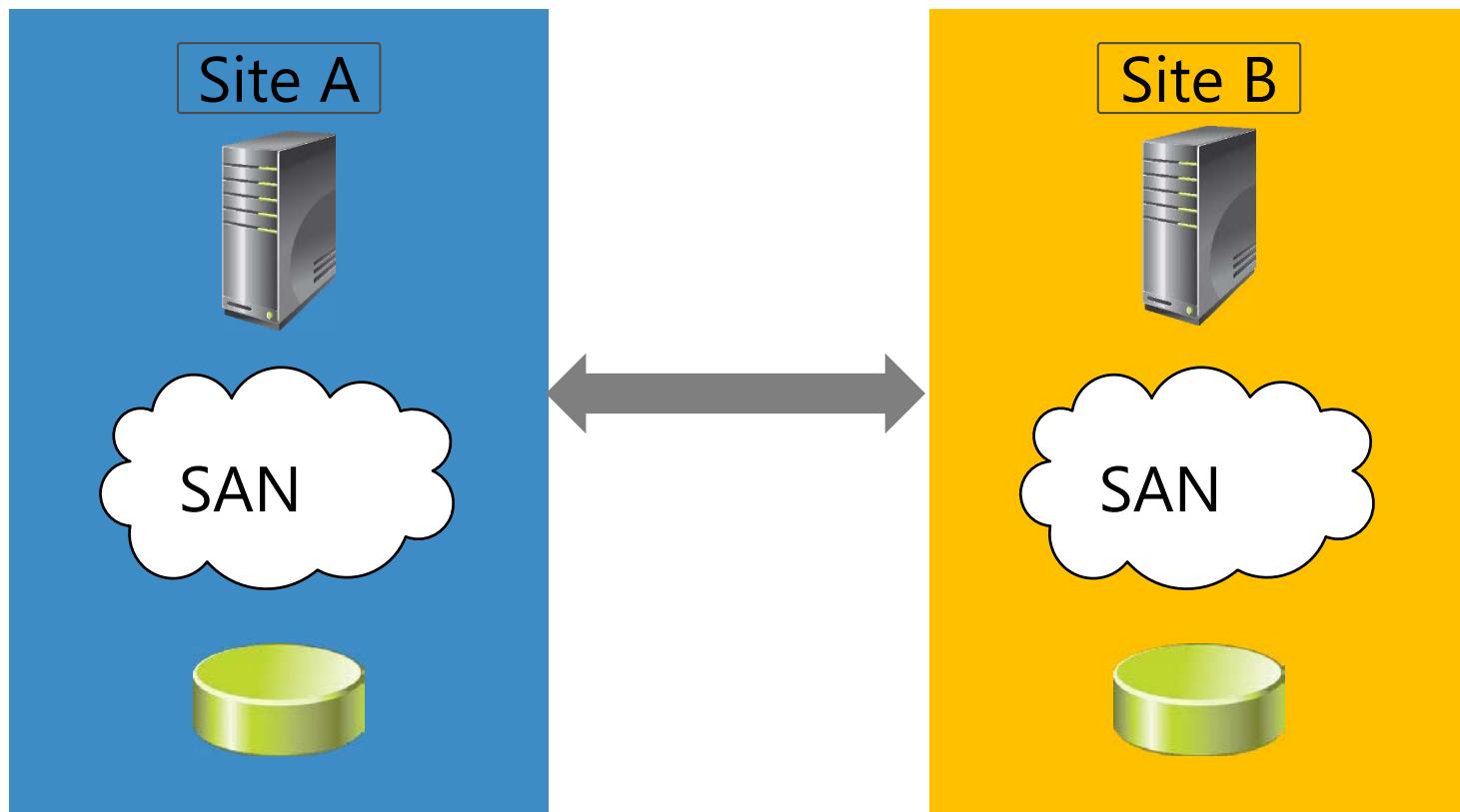
In this demonstration, you will see how to configure CAU

# Lesson 5: Implementing a Multisite Failover Cluster

- What Is a Multisite Cluster?
- Prerequisites for Implementing a Multisite Failover Cluster
- Synchronous and Asynchronous Replication
- Selecting a Quorum Mode for Multisite Clusters
- Process for Configuring a Multisite Failover Cluster
- Challenges with Implementing a Multisite Cluster
- Multisite Failover and Failback Considerations

# What Is a Multisite Cluster?

A multisite cluster is a cluster that has been extended so that different nodes in the same cluster reside in separate physical locations



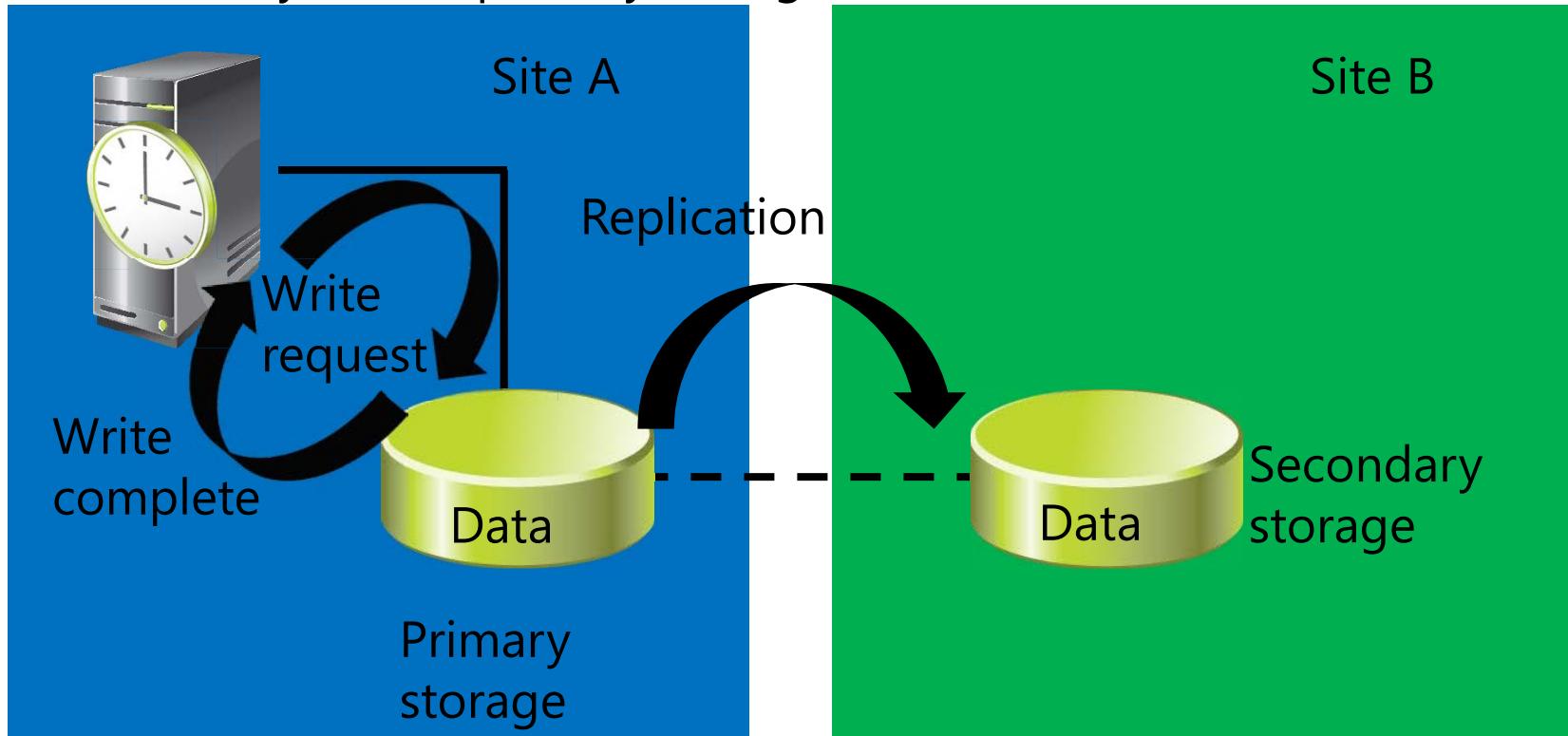
# Prerequisites for Implementing a Multisite Failover Cluster

To implement a multisite failover cluster, you must provide the following:

- ✓ Additional hardware to support enough nodes on each site
- ✓ Same operating systems and service packs on each node
- ✓ At least one low-latency and reliable network connection between sites
- ✓ Storage replication mechanism
- ✓ A storage infrastructure services on each site

# Synchronous and Asynchronous Replication

- In synchronous replication, the host receives a “write complete” response from the primary storage after the data is written successfully to both storage locations
- In asynchronous replication, the host receives a “write complete” response from the primary storage after the data is written successfully on the primary storage



# Selecting a Quorum Mode for Multisite Clusters

When designing automatic failover for geographically dispersed clusters:

- Use Node Majority or Node Majority with File Share quorum for Windows Server 2012 and older
- Use Dynamic Quorum for Windows Server 2012 R2
- Use three locations to allow automatic failover of a single virtual server:
  - All three locations must be linked directly to each other
  - One location is only a file-share witness

# Process for Configuring a Multisite Failover Cluster

High level steps for implementing a multisite failover cluster:

1. Ensure that enough nodes are available
2. Ensure that network connections between sites is reliable
3. Provide a storage replication mechanism
4. Provide key infrastructure services on both sites
5. Validate cluster configuration
6. Configure the clustered role and quorum
7. Configure and validate failover and fallback

# Challenges with Implementing a Multisite Cluster

| Challenge                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|--------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Requires a separate or third-party data replication solution | <ul style="list-style-type: none"><li>• Hardware (block level) storage-based replication</li><li>• Software (file system level) host-based replication</li><li>• Application-based replication, such as Exchange 2007 Cluster Continuous Replication</li></ul>                                                                                                                                                                                                            |
| Can be either synchronous or asynchronous replication        | <ul style="list-style-type: none"><li>• Synchronous. No acknowledgement of data changes made in Site A until the data is successfully written to Site B</li><li>• Asynchronous. Data changes made in Site A will eventually be written to the storage in Site B</li></ul>                                                                                                                                                                                                 |
|                                                              | <ul style="list-style-type: none"><li>• Inter-node communications are time sensitive; you might need to configure these thresholds to meet the higher WAN latency</li><li>• DNS replication might impact client reconnect times when failover is based on hostname</li><li>• Active Directory replication latency might affect application data availability</li><li>• Some applications might require all of the nodes to be in the same Active Directory site</li></ul> |

# Multisite Failover and Failback Considerations

- When implementing multisite clusters in a disaster recovery scenario, you should consider the following:
  - Failover time
  - Services for failover
  - Quorum maintenance
  - Storage connection
  - Published services and name resolution
  - Client connectivity
  - Failback procedure

# Lab: Implementing Failover Clustering

- Exercise 1: Configuring a Failover Cluster
- Exercise 2: Deploying and Configuring a Highly Available File Server
- Exercise 3: Validate the Deployment of the Highly Available File Server
- Exercise 4: Configuring CAU on the Failover Cluster

## Logon Information

|                   |                                                                         |
|-------------------|-------------------------------------------------------------------------|
| Virtual machines: | 20412D-LON-DC1<br>20412D-LON-SVR1<br>20412D-LON-SVR3<br>20412D-LON-SVR4 |
| User name:        | <b>Adatum\Administrator</b>                                             |
| Password:         | <b>Pa\$\$w0rd</b>                                                       |

Estimated Time: 60 minutes

# Lab Scenario

As A. Datum's business grows, it is becoming increasingly important that many of the applications and services on the network are available at all times. A. Datum has many services and applications that must be available to internal and external users who work in different time zones around the world. Many of these applications cannot be made redundant by using Network Load Balancing (NLB). Therefore, you have to use a different technology to make these applications highly available.

As one of the senior network administrators at A. Datum, you are responsible for implementing failover clustering on the Windows Server 2012 R2 servers to provide high availability for network services and applications. You are also responsible for planning the failover cluster configuration, and for deploying applications and services on the failover cluster.

# Lab Review

- What information do you have to collect as you plan a failover cluster implementation and choose the quorum mode?
- After running the Validate a Configuration Wizard, how can you resolve the network communication single point of failure?
- In what situations might it be important to enable fallback of a clustered application only during a specific time?

# Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



Module 11

Implementing Failover Clustering  
with Hyper-V

**Microsoft®**

# Module Overview

- Overview of Integrating Hyper-V with Failover Clustering
- Implementing Hyper-V Virtual Machines on Failover Clusters
- Implementing Hyper-V Virtual Machine Movement

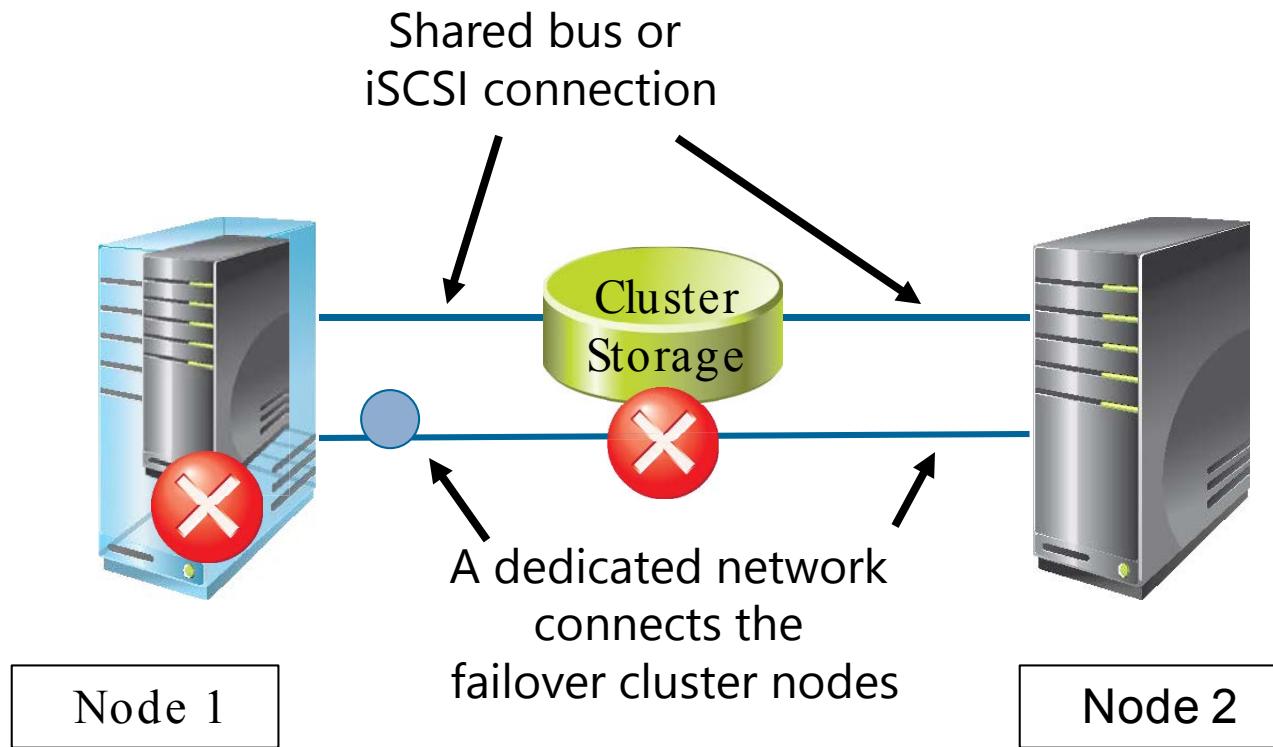
# Lesson 1: Overview of Integrating Hyper-V with Failover Clustering

- Options for Making Applications and Services Highly Available
- How Does a Failover Cluster Work with Hyper-V Nodes?
- What's New in Failover Clustering for Hyper-V in Windows Server 2012?
- What's New in Failover Clustering for Hyper-V in Windows Server 2012 R2?
- Best Practices for Implementing High Availability in a Virtual Environment

# Options for Making Applications and Services Highly Available

| High availability options | Description                                                                                                                                                                                                                                           |
|---------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Host clustering           | <ul style="list-style-type: none"><li>• Virtual machines are highly available</li><li>• Does not require virtual machine operating system or application to be cluster aware</li></ul>                                                                |
| Guest clustering          | <ul style="list-style-type: none"><li>• Virtual machines are failover cluster nodes</li><li>• Virtual machine applications must be cluster aware</li><li>• Requires iSCSI or virtual Fibre Channel interface for shared storage connections</li></ul> |
| NLB                       | <ul style="list-style-type: none"><li>• Virtual machines are NLB cluster nodes</li><li>• Use for web-based applications</li></ul>                                                                                                                     |

# How Does a Failover Cluster Work with Hyper-V Nodes?



# What's New in Failover Clustering for Hyper-V in Windows Server 2012?

The Failover Clustering improvements for Hyper-V in Windows Server 2012 include:

- Support for up to 8,000 virtual machines per cluster
- Multi-select virtual machines for Live Migration
- Virtual machine priority attribute
- CSV improvements
- Virtual machine application monitoring
- Storage of virtual machines on highly available SMB file share

# What's New in Failover Clustering for Hyper-V in Windows Server 2012 R2?

- Windows Server 2012 R2 provides new features for virtual machine clustering, which include:
  - Shared virtual hard disk
  - Virtual machine drain on shutdown
  - Network health detection

# Best Practices for Implementing High Availability in a Virtual Environment

- Use Windows Server 2012 R2 as the Hyper-V host
- Plan for failover scenarios
- Plan the network design for failover clustering
- Plan the shared storage for failover clustering
- Use the recommended failover cluster quorum mode
- Deploy standardized Hyper-V hosts
- Develop standard management practices

## Lesson 2: Implementing Hyper-V Virtual Machines on Failover Clusters

- Components of Hyper-V Clusters
- Implementing Failover Clustering for Hyper-V Virtual Machines
- Configuring CSV
- Configuring a Shared Virtual Hard Disk
- Using Scale-Out File Servers Over SMB 3 for Virtual Machines
- Considerations for Implementing Hyper-V Clusters
- Demonstration: Implementing Virtual Machines on Clusters (optional)
- Maintaining and Monitoring Virtual Machines in Clusters

# Components of Hyper-V Clusters

Hyper-V cluster components:

- Cluster nodes, must be physical computers
- Cluster networks
- Virtual networks
- Storage for virtual machines
- Virtual machines

# Implementing Failover Clustering for Hyper-V Virtual Machines

1. Install and configure Windows Server 2012
2. Configure shared storage
3. Install the Hyper-V and failover clustering features
4. Validate the cluster configuration
5. Create the cluster
6. Create a virtual machine on one of the cluster nodes
7. Make the virtual machine highly available, for existing virtual machine
8. Test virtual machine failover

# Configuring CSV

## CSV benefits:

- Fewer LUNs required
- Better use of disk space
- Virtual machine files are in a single logical location
- No special hardware required
- Increased resiliency

## To implement CSV:

1. Create and format volumes on shared storage
2. Add the disks to failover cluster storage
3. Add the storage to the CSV

# Configuring a Shared Virtual Hard Disk

- A failover cluster runs inside virtual machines
- A shared virtual disk is used as shared storage if:
  - Virtual machines do not need access to iSCSI or failover clustering SAN
  - Presented as a virtual serial attached SCSI disk
  - Used only for data
- Requirements for a shared virtual disk:
  - Virtual hard disk must be in VHDX format
  - Connected by using virtual SCSI adapter
  - Stored on a Scale-Out File Server or CSV
- Supported operating system in a virtual machine:
  - Windows Server 2012 or Windows Server 2012 R2

# Shared Virtual Disk vs. Other Shared Storage Technologies

## Comparing guest clustering options

| Capability                                    | Shared VHDX                                                     | Virtual Fibre Channel     | iSCSI     |
|-----------------------------------------------|-----------------------------------------------------------------|---------------------------|-----------|
| Supported storage                             | Storage Spaces, serial attached SCSI, Fibre Channel, iSCSI, SMB | Fibre Channel SAN         | iSCSI SAN |
| How storage is exposed in the virtual machine | Virtual serial attached SCSI                                    | Virtual Fibre Channel LUN | iSCSI LUN |
| Flows through the Hyper-V virtual switch      | No                                                              | No                        | Yes       |
| Storage configured at the Hyper-V host        | Yes                                                             | Yes                       | No        |
| Provides low latency and low CPU use          | Yes (RDMA or Fibre Channel)                                     | Yes (Fibre Channel)       | No        |
| Requires specific hardware                    | No                                                              | Yes                       | No        |
| Expose storage architecture                   | No                                                              | Yes                       | Yes       |

# Using Scale-Out File Servers Over SMB 3 for Virtual Machines

- In Windows Server 2012 or newer, you can store virtual machine files on an SMB 3.0 file share
- File servers should run Windows Server 2012 R2
- File server cluster should run in Scale-Out File Server mode
- Hyper-V Manager can be used to create or move virtual machine files to an SMB file share

# Considerations for Implementing Hyper-V Clusters

1. Identify the applications that require high availability
2. Identify the application components that must be highly available
3. Identify the application characteristics
4. Identify the total capacity requirements
5. To create the Windows Server 2012 Hyper-V design:
  - Verify basic requirements
  - Configure a dedicated network adapter for the private virtual network
  - Use similar host hardware
  - Verify network configuration

## Demonstration: Implementing Virtual Machines on Clusters (optional)

In this demonstration, you will see how to implement highly available virtual machines with failover clustering

# Maintaining and Monitoring Virtual Machines in Clusters

- In Windows Server 2012 failover clustering, you can implement the following technologies for virtual machine maintenance and monitoring:
  - Service and virtual machine health monitoring
  - Network health detection, for Windows Server 2012 R2 only
  - Virtual machine drain on shutdown, for Windows Server 2012 R2 only

# Lesson 3: Implementing Hyper-V Virtual Machine Movement

- Virtual Machine Migration Options
- How Does Virtual Machine and Storage Migration Work?
- Using ODX Capable Storage for Virtual Machines
- How Does Live Migration Work?
- How Does Hyper-V Replica Work?
- New Features of Hyper-V Replica in Windows Server 2012 R2
- Demonstration: Implementing Hyper-V Replica (optional)

# Virtual Machine Migration Options

Available options for moving virtual machines are:

- Virtual Machine and Storage Migration
- Quick Migration
- Live Migration
- Hyper-V Replica
- Export or import of a virtual machine

# How Does Virtual Machine and Storage Migration Work?

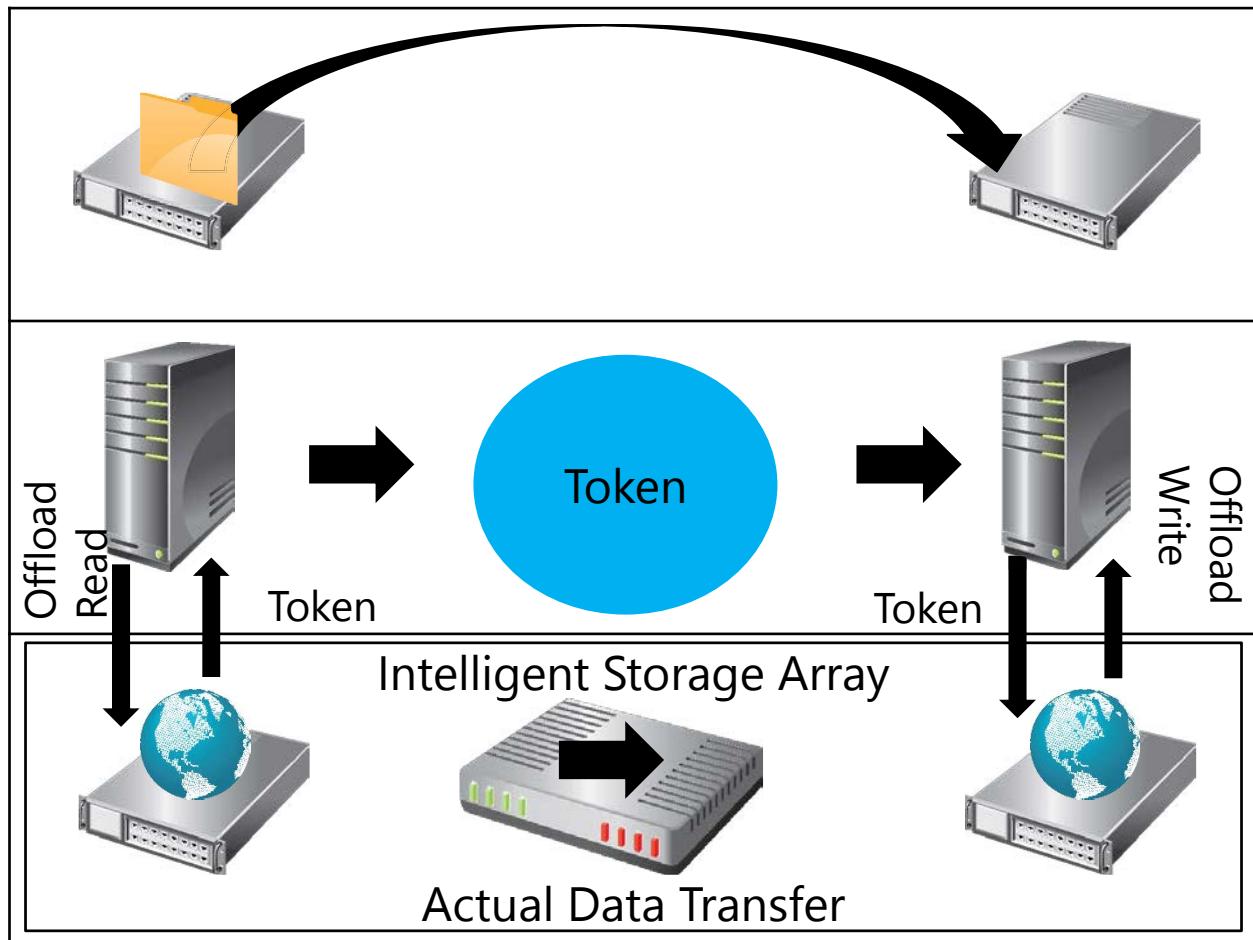
Virtual Machine and Storage Migration technology enables you to move a virtual machine and its storage to another location without downtime

- During migration, the virtual machine hard disk is copied from one location to another
- Changes are written to both the source and destination drive
- You can move virtual machine storage to the same host, another host, or an SMB share
- Storage and virtual machine configuration can be in different locations

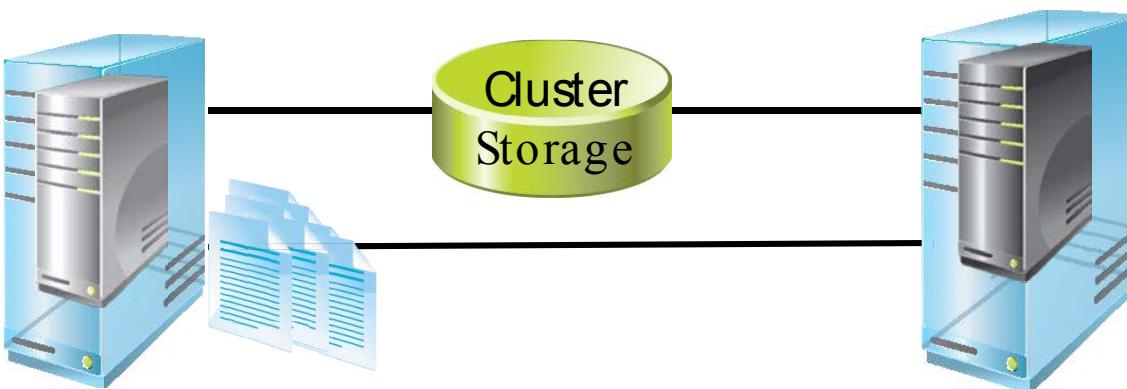
# Using ODX Capable Storage for Virtual Machines

When using ODX-capable storage you achieve following benefits:

- Increase data transfer
- Minimize latency
- Minimize host's resource usage while copying and migrating data



# How Live Migration Works?



Node 1

Node 2

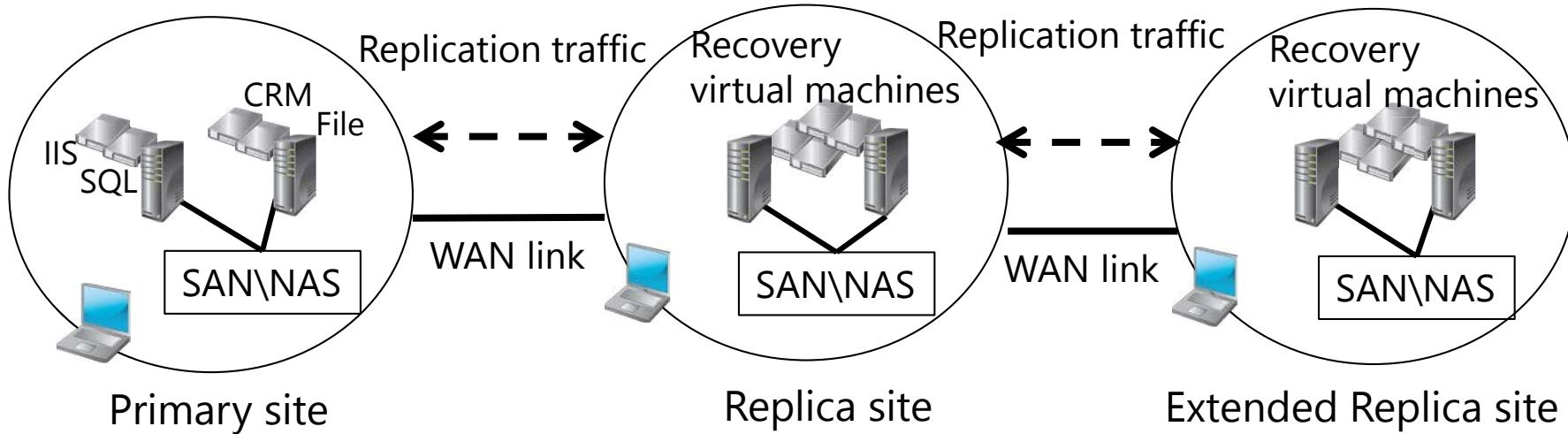


# How Does Hyper-V Replica Work?

Hyper-V Replica in Windows Server 2012 enables you to replicate a single virtual machine over a WAN or LAN network to another host

Hyper-V Replica components include:

- Replication engine
- Change tracking
- Network module
- Hyper-V Replica Broker role



# How to Configure Hyper-V Replica?

To configure Hyper-V Replica, you should:

1. Configure authentication options
2. Configure ports
3. Select replica servers
4. Select location for replica files
5. Enable replication on virtual machine

# New Features of Hyper-V Replica in Windows Server 2012 R2

Hyper-V Replica in Windows Server 2012 R2 is enhanced with the following features:

- The ability to change the replication frequency:
  - The available intervals are 30 seconds, 5 minutes, and 15 minutes
- Extended replication:
  - You can extend Hyper-V Replica to include a third host

# Demonstration: Implementing Hyper-V Replica (optional)

In this demonstration, you will see how to implement Hyper-V Replica

# Lab: Implementing Failover Clustering with Hyper-V

- Exercise 1: Configuring Hyper-V Replicas
  - Exercise 2: Configuring a Failover Cluster for Hyper-V
  - Exercise 3: Configuring a Highly Available Virtual Machine
- Logon Information

Virtual machines:

20412D-LON-DC1-B

20412D-LON-SVR1-B

20412D-LON-HOST1

20412D-LON-HOST2

**Adatum\administrator**

**Pa\$\$w0rd**

User name:

Password:

Estimated Time: 75 minutes

# Lab Scenario

The initial deployment of virtual machines on Hyper-V has been successful for A. Datum. As a next step in the deployment, A. Datum is considering ways to ensure that the services and applications deployed on the virtual machines are highly available. As part of the implementation of high availability for most network services and applications, A. Datum also is considering options for making the virtual machines that run on Hyper-V highly available.

As one of the senior network administrators at A. Datum, you are responsible for integrating Hyper-V with failover clustering to ensure that the virtual machines deployed on Hyper-V are highly available. You are responsible for planning the virtual machine and storage configuration, and for implementing the virtual machines as highly available services on the failover cluster. You also are considering other techniques, such as Hyper-V Replica, for ensuring high availability for virtual machines.

# Lab Review

- How can you extend Hyper-V Replica in Windows Server 2012 R2?
- What is the difference between Live Migration and Storage Migration?

# Module Review and Takeaways

- Review Question
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips

# Microsoft® Official Course



## Module 12

### Implementing Business Continuity and Disaster Recovery

**Microsoft®**

# Module Overview

- Data Protection Overview
- Implementing Windows Server Backup
- Implementing Server and Data Recovery

# Lesson 1: Data Protection Overview

- Identifying Recovery Requirements
- What Are Service Level Agreements?
- Overview of Enterprise Data Protection Strategies
- Mitigation Strategies
- Best Practices When Implementing a Data Protection Strategy

# Identifying Recovery Requirements

Identify your data protection options by:

1. Defining organization critical resources
2. Identifying risks associated with those critical resources
3. Identifying the time needed to complete the recovery
4. Developing a protection strategy

# What Are Service Level Agreements?

SLAs define responsibilities of the service provider

SLA components include:

- Hours of operation
- Service availability
- RPO and RTO
- Retention objectives
- System performance

# Overview of Enterprise Data Protection Strategies

You need strategies for recovering:

- Data
- Services
- Servers
- Sites
- Offsite backups

# Mitigation Strategies

| Problem                                                                                      | Mitigation strategy                                                                                                   |
|----------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------|
| The media where a copy of the backup data is stored becomes corrupted                        | Have at least two copies of your backup data                                                                          |
| An administrator has accidentally deleted an OU that contains many user and computer objects | Protect OUs from accidental deletion, especially after migrations                                                     |
| A server in a branch office where important files are located has failed                     | Use DFS Replication to replicate files from branch offices to central data centers                                    |
| The virtualization infrastructure where business servers are located is unavailable          | Avoid deploying all critical servers, such as domain controllers, on the same virtual infrastructure                  |
| A major outage in a data center has occurred                                                 | Deploy a secondary data center that will contain replicas of most of the critical servers in your primary data center |

# Best Practices When Implementing a Data Protection Strategy

To implement a data protection strategy , you should:

- Perform a risk assessment plan
- Discuss the risks you evaluated with your business managers, and create a data protection strategy and disaster mitigation strategy
- Ensure that each organization has its own data protection plan
- Document all steps that should be performed in a recovery scenario
- Test your recovery plan on regular basis, in an isolated, non-production environment.
- Evaluate your data protection strategy on a regular basis, and update your data protection strategy depending on your evaluation outcome

# Lesson 2: Implementing Windows Server Backup

- Planning a Backup Strategy
- What Is Windows Server Backup?
- Backup Types
- Backup Technologies
- Planning Backup Capacity
- Planning Backup Security
- Demonstration: Configuring a Scheduled Backup
- What Is Windows Azure Backup?
- Considerations for an Enterprise Backup Solution
- What Is Data Protection Manager?

# Planning a Backup Strategy

When planning your backup strategy, ensure that you:

- Determine the critical resources
- Verify your backups
- Confirm that backups are secure
- Ensure that compliance and regulatory responsibilities are met

# What Is Windows Server Backup?

You can use Windows Server Backup to:

- Back up full server (all volumes)
- Back up selected volumes
- Back up selected items
- Perform a bare-metal recovery
- Perform a system state
- Back up individual files and folders
- Exclude selected files or file types during backup
- Select from more storage locations for the backup

# Backup Types

- A full backup is a block-level replica of all blocks on all the server's volumes
- An incremental backup is a copy of only those blocks that have changed since the last full or incremental backup

# Backup Technologies

- The VSS backup technology solves data consistency issues by creating shadow copies
- You can also use streaming backups for older applications that are not VSS-aware
- Hyper-V replica provides you with a disaster recovery option by replicating a consistent copy of a virtual machine to another server or site.

# Planning Backup Capacity

When planning for backup capacity, consider the following:

- Space requirements for a full backup
- Space requirements for an incremental backup
- Amount of time required to back up
- Backup frequency
- Backup retention

# Planning Backup Security

When planning your backup security, consider the following:

- Backups contain all organizational data
- Access to backup media means access to all data
- Windows Server Backup does not encrypt backups
- Keep backup media in a secure location

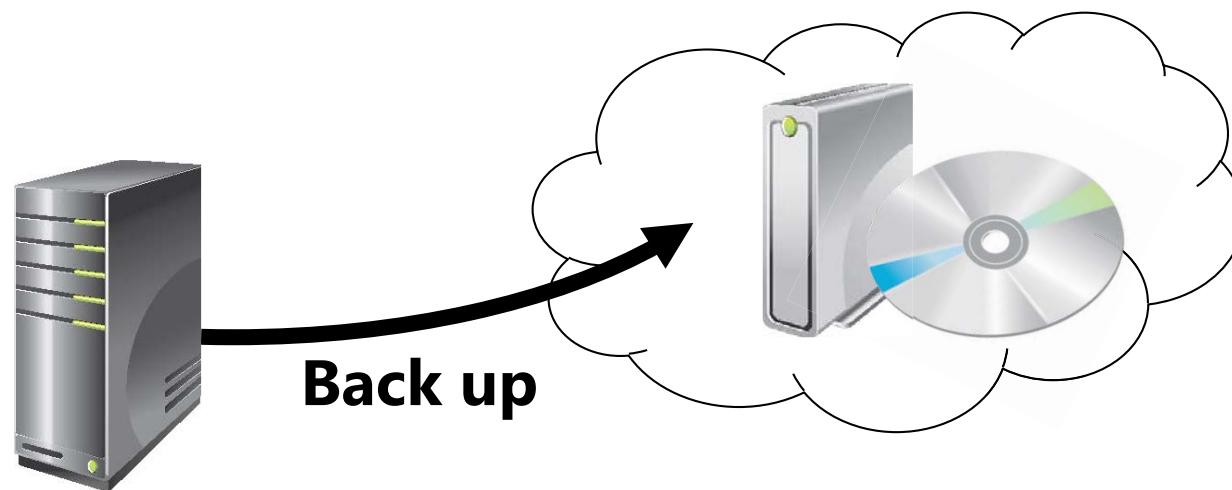
# Demonstration: Configuring a Scheduled Backup

In this demonstration, you will see how to configure Windows Server Backup to perform a scheduled backup of specific folders that includes a filter to exclude specific file types

# What Is Windows Azure Backup?

Windows Azure Backup features include:

- Simple configuration and management
- Block-level incremental backups
- Data compression, encryption, and throttling
- Data integrity verified in the cloud
- Configurable retention policies for storing data in the cloud



# Considerations for an Enterprise Backup Solution

Considerations for an enterprise backup solution are:

- What is the theoretical RPO of the product?
- How quick is RTO recovery?
- Does the solution provide centralized backup?
- Is the solution supported by vendors?
- What is the recovery point capacity?

# What Is Data Protection Manager?

DPM:

- Allows you to centralize backups
- Offers 15-minute snapshots of servers and clients
- Can store backup data on SANs and export to tape
- Can back up remote sites
- Can be used as part of a backup-to-cloud strategy
- Supports Microsoft products

# Lesson 3: Implementing Server and Data Recovery

- Options for Server Recovery
- Options for Server Restore with Windows RE
- Options for Data Recovery
- Demonstration: Using Windows Server Backup to Restore a Folder
- Restoring with Windows Azure Backup

# Options for Server Recovery

The options for server recovery include:

- Files and folders
- Applications and data
- Volumes
- Operating system
- Full server
- System state
- BCDEdit allows you to edit the BCD Store to modify boot options
- Safe mode boots computer with minimal services and drivers
- Last Known Good configuration is the most recent set of driver and registry settings from a successful startup

# Options for Server Restore with Windows RE

- Windows RE allows you to recover server images or volumes from local disk or network share

You can enter Windows RE when:

- You boot from install media
- You press F8
- Successive boot failures or unexpected shutdowns occur

# Options for Data Recovery

The four options for recovering data include:

- Allowing users to recover their own data
- Recovering data to an alternate location
- Recovering data to the original location
- Performing a full volume recovery

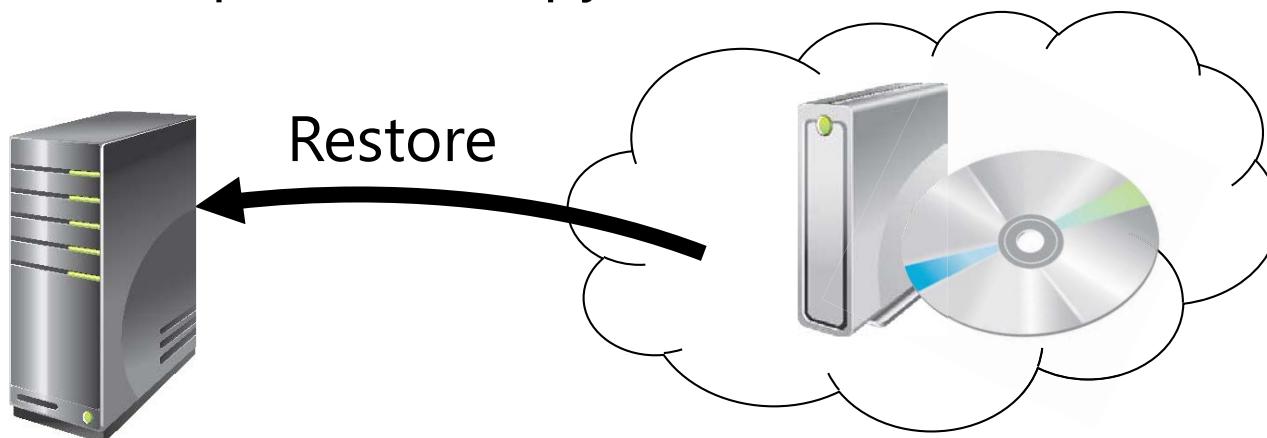
# Demonstration: Using Windows Server Backup to Restore a Folder

In this demonstration, you will see how to use the Recovery Wizard to restore a folder

# Restoring with Windows Azure Backup

When restoring files by using Windows Azure Online Backup, perform the following steps:

1. Select the server
2. Locate the files you want to recover from backup
3. Choose the restore location
4. Select an option for copy creation



# Lab: Implementing Windows Server Backup and Restore

- Exercise 1: Backing Up Data on a Windows Server 2012 R2 Server
- Exercise 2: Restoring Files Using Windows Server Backup

Logon Information

Virtual machines: 20412D-LON-DC1,  
20412D-LON-SVR1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

Estimated Time: 60 minutes

## Lab Scenario

Much of the data that is stored on the A. Datum Corporation's network is extremely valuable to the organization. Losing this data would be a significant loss to the organization. Additionally, many of the servers that are running on the network provide extremely valuable services for the organization, which means that losing these servers for a significant time would also result in losses to the organization. Because of the significance of the data and services, it is critical that they can be restored in the event of disaster.

## Lab Scenario

A. Datum is considering backing up critical data to a cloud-based service. A. Datum also is considering this as an option for small branch offices that do not have a full datacenter infrastructure.

As one of the senior network administrators at A. Datum, you are responsible for planning and implementing a data-protection solution that will ensure that critical data and services can be recovered in the event of any type of failure. You need to implement a backup-and-restore process that can recover lost data and services.

# Lab Review

- You are concerned about business-critical data that is located on your company's servers. You want to perform backups every day, but not during business hours. What should you do?
- Users report that they can no longer access data that is located on the server. You connect to the server, and you realize that the shared folder where users were accessing data is missing. What should you do?

# Module Review and Takeaways

- Review Questions
- Real-world Issues and Scenarios
- Tools
- Best Practice
- Common Issues and Troubleshooting Tips

# Course Evaluation



# Lab: Deploying and Managing Windows Server 2012

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, England. A. Datum has recently deployed a Windows Server 2012 infrastructure with Windows 8.1 clients.

You have been working for A. Datum for several years as a desktop support specialist and have recently accepted a promotion to the server support team.

The marketing department has purchased a new web-based application. You need to install and configure the servers in the data center for this application. One server has a GUI interface, and the other server is configured as Server Core.

## Objectives

After completing this lab, you should be able to:

- Deploy Windows Server 2012.
- Configure Windows Server 2012 Server Core.
- Manage servers by using Server Manager.
- Manage servers with Windows PowerShell.

## Lab Setup

Estimated Time: 75 minutes

|                  |                                                                           |
|------------------|---------------------------------------------------------------------------|
|                  |                                                                           |
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR3</b><br><b>20410D-LON-CORE</b> |
| User name        | <b>Adatum\Administrator</b>                                               |
| Password         | <b>Pa\$\$w0rd</b>                                                         |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20410D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20410D-LON-CORE**. Do not sign in until directed to do so.

## Exercise 1: Deploying Windows Server 2012

### Scenario

The first Windows Server 2012 server that you are installing for the Marketing department will host a SQL Server 2012 database engine instance. You want to configure the server so that it will have the full GUI, as this will allow the application vendor to run support tools directly on the server, rather than requiring a remote connection.

The first server you will install for the new marketing app is for a SQL Server 2012 database. This server will have the full GUI to allow the application vendor to run support tools directly on the server.

The main tasks for this exercise are as follows:

1. Install the Windows Server 2012 R2 server.
2. Change the server name.
3. Change the date and time.
4. Configure the network.
5. Add the server to the domain.

#### ► Task 1: Install the Windows Server 2012 R2 server

1. In the Hyper-V Manager console, open the settings for 20410D-LON-SVR3.
2. Configure the DVD drive to use the Windows Server 2012 R2 image file named **Windows2012R2RTM.iso**. This file is located at **D:\Program Files\Microsoft Learning\20410\Drives**.
3. Start **20410D-LON-SVR3**. In the Windows Setup Wizard, on the **Windows Server 2012 R2** page, verify the following settings, click **Next**, and then click **Install Now**:
  - Language to install: **English (United States)**
  - Time and currency format: **English (United States)**
  - Keyboard or input method: **US**
4. Click to install the **Windows Server 2012 R2 Datacenter Evaluation (Server with a GUI)** operating system.
5. Accept the license terms, click **Next**, and then click **Custom: Install Windows only (advanced)**.
6. Install Windows Server 2012 on **Drive 0**.

 **Note:** Depending on the speed of the equipment, the installation takes approximately 20 minutes. The virtual machine will restart several times during this process.

7. Enter the password **Pa\$\$w0rd** in both the **Password** and **Reenter password** boxes, and then click **Finish** to complete the installation.

#### ► Task 2: Change the server name

1. Sign in to LON-SVR3 as **Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, on the Local Server node, click the randomly generated name next to **Computer name**.
3. In the **System Properties** dialog box, on the **Computer Name** tab, click **Change**.
4. In the **Computer name** box, type **LON-SVR3**, and then click **OK**.

5. Click **OK** again, and then click **Close**.
6. Restart the computer.

► **Task 3: Change the date and time**

1. Sign in to server LON-SVR3 as **Administrator** with the password **Pa\$\$w0rd**.
2. On the taskbar, click the time display, and then click **Change date and time settings**.
3. Click **Change Time Zone**, and set the time zone to your current time zone.
4. Click **Change Date and Time**, and verify that the date and time that display in the Date and Time Settings dialog box match those in your classroom.
5. Close the Date and Time dialog box.

► **Task 4: Configure the network**

1. On LON-SVR3, click **Local Server**.
2. Next to Ethernet, click **IPv4 address assigned by DHCP, IPv6 Enabled**.
3. In the **Network Connections** dialog box, right-click **Ethernet**, and then click **Properties**.
4. Click **Internet Protocol Version 4 (TCP/IPv4)**, and then click **Properties**.
5. Enter the following IP address information, and then click **OK**:
  - IP address: **172.16.0.101**
  - Subnet Mask: **255.255.0.0**
  - Default Gateway: **172.16.0.1**
  - Preferred DNS server: **172.16.0.10**
6. Close all dialog boxes.

► **Task 5: Add the server to the domain**

1. On LON-SVR3, in the Server Manager console, click **Local Server**.
2. Next to Workgroup, click **WORKGROUP**.
3. On the **Computer Name** tab, click **Change**.
4. Click the **Domain** option, and in the **Domain** box, enter **adatum.com**, and then click **OK**.
5. Enter the following account details:
  - Username: **Administrator**
  - Password: **Pa\$\$w0rd**
6. In the **Computer Name/Domain Changes** dialog box, click **OK**.
7. Restart the computer to apply the changes.
8. In the **System Properties** dialog box, click **Close**.
9. After LON-SVR3 restarts, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

**Results:** After completing this exercise, you should have deployed Windows Server 2012 on LON-SVR3. You also should have configured LON-SVR3, including name change, date and time, and networking.

## Exercise 2: Configuring Windows Server 2012 Server Core

### Scenario

The web-based tier of the marketing application is a .NET application. To minimize the operating system footprint and reduce the need to apply software updates, you have chosen to host the IIS component on a computer that is running the Server Core installation option of the Windows Server 2012 operating system.

To enable this, you need to configure a computer that is running Windows Server 2012 with the Server Core installation option.

The main tasks for this exercise are as follows:

1. Set computer name.
2. Change the computer's date and time.
3. Configure the network.
4. Add the server to the domain.

#### ► Task 1: Set computer name

1. Sign in to LON-CORE as **Administrator** with the password **Pa\$\$w0rd**.
2. On LON-CORE, type **sconfig.cmd**.
3. Click option **2** to select **Computer Name**.
4. Set the computer name as **LON-CORE**.
5. In the **Restart** dialog box, click **Yes** to restart the computer.
6. After the computer restarts, sign in to server LON-CORE using the **Administrator** account with the password **Pa\$\$w0rd**.
7. At the command prompt, type **hostname**, and then press Enter to verify the computer's name.

#### ► Task 2: Change the computer's date and time

1. Ensure you are signed in to server LON-CORE as **Administrator** with the password **Pa\$\$w0rd**.
2. At the command prompt, type **sconfig.cmd**.
3. To select **Date and Time**, type **9**.
4. Click **Change time zone**, and then set the time zone to the same time zone that your classroom uses.
5. In the **Date and Time** dialog box, click **Change Date and Time**, and verify that the date and time match those in your location.
6. Exit sconfig.cmd.

#### ► Task 3: Configure the network

1. Ensure that you are signed in to server LON-CORE using the account **Administrator** and the password **Pa\$\$w0rd**.
2. At the command prompt, type **sconfig.cmd**, and then press Enter.
3. To configure Network Settings, type **8**.
4. Type the number of the network adapter that you want to configure.
5. Type **1** to set the Network Adapter Address.
6. Click **static IP address configuration**, and then enter the address **172.16.0.111**.

7. At the Enter subnet mask prompt, type **255.255.0.0**.
8. At the Enter default gateway prompt, type **172.16.0.1**.
9. Type **2** to configure the DNS server address.
10. Set the preferred DNS server to **172.16.0.10**.
11. Do not configure an alternate DNS server address.
12. Exit sconfig.cmd.
13. Verify network connectivity to lon-dc1.adatum.com by using the PING tool.

#### ► Task 4: Add the server to the domain

1. Ensure that you are signed in to server LON-CORE using the account **Administrator** with the password **Pa\$\$w0rd**.
2. At the command prompt, type **sconfig.cmd**, and then press Enter.
3. Type **1** to switch to **configure Domain/Workgroup**.
4. Type **D** to join a domain.
5. At the **Name of domain to join** prompt, type **adatum.com**.
6. At the **Specify an authorized domain\user** prompt, type **Adatum\Administrator**.
7. At the **Type the password associated with the domain user** prompt, type **Pa\$\$w0rd**.
8. At the prompt, click **No**.
9. Restart the server.
10. Sign in to server LON-CORE with the **Adatum\Administrator** account using the password **Pa\$\$w0rd**.

**Results:** After you complete this exercise, you should have configured a Windows Server 2012 Server Core deployment and verified the server's name.

## Exercise 3: Managing Servers

### Scenario

After deploying the servers LON-SVR3 and LON-CORE for hosting the Marketing application, you need to install appropriate server roles and features to support the application. With this in mind, you will install the Windows Server Backup feature on both LON-SVR3 and LON-CORE. You will install the Web Server role on LON-CORE.

You also need to configure the World Wide Web Publishing service on LON-CORE.

The main tasks for this exercise are as follows:

1. Create a server group.
2. Deploy features and roles to both servers.
3. Review services and change a service setting.

► **Task 1: Create a server group**

1. Sign in to LON-DC1 with the **Administrator** account and the password **Pa\$\$w0rd**.
2. In the Server Manager console, click **Dashboard**, and then click **Create a server group**.
3. Click the **Active Directory** tab, and then click **Find Now**.
4. In the **Server group name** box, type **LAB-1**.
5. Add **LON-CORE** and **LON-SVR3** to the server group.
6. Click **LAB-1**. Select both **LON-CORE** and **LON-SVR3**.
7. Scroll down, and under the **Performance** section, select both **LON-CORE** and **LON-SVR3**.
8. Right-click **LON-CORE**, and then click **Start Performance Counters**.

► **Task 2: Deploy features and roles to both servers**

1. In Server Manager on LON-DC1, click the **LAB-1** server group, right-click **LON-CORE**, and then click **Add Roles and Features**.
2. In the Add Roles and Features Wizard, click **Next**, click **Role-based or feature-based installation**, and then click **Next**.
3. Verify that **LON-CORE.A datum.com** is selected, and then click **Next**.
4. Select the **Web Server (IIS)** Server role.
5. Select the **Windows Server Backup** feature.
6. Add the **Windows Authentication** role service, and then click **Next**.
7. Select the **Restart the destination server automatically if required** check box, and then click **Install**.
8. Click **Close**.
9. Right-click **LON-SVR3**, click **Add Roles and Features**, and then click **Next**.
10. In the Add Roles and Features Wizard, click **Role-based or feature-based installation**, and then click **Next**.
11. Verify that **LON-SVR3.A datum.com** is selected, and then click **Next** twice.
12. Click **Windows Server Backup**, and then click **Next**.
13. Select the **Restart the destination server automatically if required** check box, click **Install**, and then click **Close**.
14. In Server Manager, click the **IIS** node, and verify that LON-CORE is listed.

► **Task 3: Review services and change a service setting**

1. Sign in to LON-CORE with the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.
2. In the Command Prompt window, execute the following commands:

```
netsh.exe advfirewall firewall set rule group="remote desktop" new enable=yes
netsh.exe advfirewall firewall set rule group="remote event log management" new
enable=yes
```

3. Sign in to LON-DC1 with the **Adatum\Administrator** account.
4. In Server Manager, click **LAB-1**, right-click **LON-CORE**, and then click **Computer Management**.

5. Expand **Services and Applications**, and then click **Services**.
6. Verify that the **Startup type** of the **World Wide Web Publishing** service is set to **Automatic**.
7. Verify that the service is configured to use the **Local System account**.
8. Configure the following service recovery settings:
  - First failure: **Restart the Service**
  - Second failure: **Restart the Service**
  - Subsequent failures: **Restart the Computer**.
  - Reset fail count after: **1 days**
  - Reset service after: **1 minute**
9. Configure the Restart Computer option to **2 minutes**, and then close the **World Wide Web Publishing Services Properties** dialog box.
10. Close the Computer Management console.

**Results:** After you complete this exercise, you should have created a server group, deployed roles and features, and configured the properties of a service.

## Exercise 4: Using Windows PowerShell to Manage Servers

### Scenario

The marketing application vendor has indicated that the company can provide some Windows PowerShell scripts to configure the web server that is hosting the application. You need to verify that remote administration is functional before you run the scripts.

The main tasks for this exercise are as follows:

1. Use Windows PowerShell to connect remotely to servers and view information.
2. Use Windows PowerShell to remotely install new features.

#### ► Task 1: Use Windows PowerShell to connect remotely to servers and view information

1. Sign in to LON-DC1 with the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.
2. On LON-DC1, in Server Manager, click the **LAB-1** server group.
3. Right-click **LON-CORE**, and then click **Windows PowerShell**.
4. Type **Import-Module ServerManager**.
5. Type **Get-WindowsFeature**, and review roles and features.
6. Use the following command to review the running services on LON-CORE:

```
Get-service | where-object {$_ .status -eq "Running"}
```

7. Type **get-process** to view a list of processes on LON-CORE.
8. Review the IP addresses assigned to the server by typing the following command:

```
Get-NetIPAddress | Format-table
```

9. Review the most recent 10 items in the security log by typing the following command:

```
Get-EventLog Security -Newest 10
```

10. Close Windows PowerShell.

► **Task 2: Use Windows PowerShell to remotely install new features**

1. On LON-DC1, on the taskbar, click the Windows PowerShell icon.
2. Type the following command to verify that the **XPS Viewer** feature has not been installed on LON-SVR3:

```
Get-WindowsFeature -ComputerName LON-SVR3
```

3. To deploy the XPS Viewer feature on LON-SVR3, type the following command, and then press Enter:

```
Install-WindowsFeature XPS-Viewer -ComputerName LON-SVR3
```

4. Type the following command to verify that the XPS Viewer feature has been deployed on LON-SVR3:

```
Get-WindowsFeature -ComputerName LON-SVR3
```

5. In the Server Manager console, in the **Tools** drop-down menu, click **Windows PowerShell ISE**.
6. In the Untitled1.ps1 script pane, type the following:

```
Import-Module ServerManager
Install-WindowsFeature WINS -ComputerName LON-SVR3
Install-WindowsFeature WINS -ComputerName LON-CORE
```

7. Save the script as InstallWins.ps1 in a new folder named **Scripts**.
8. Press the F5 key to execute InstallWins.ps1.

**Results:** After you complete this exercise, you should have used Windows PowerShell to perform a remote installation of features on multiple servers.

### Lab Review Questions

**Question:** What IP address range do the computers in the lab use?

**Question:** Why must you set the DNS server address prior to joining the domain?

**Question:** Besides **sconfig.cmd**, what other tool can you use to rename a computer running the Server Core operating system?

► **Prepare for the next module**

After you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, switch to the **Hyper-V Manager** console.
2. In the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-CORE** and **20410D-LON-SVR3**.

# Lab: Installing Domain Controllers

## Scenario

Your manager has asked you to install a new domain controller in the datacenter to improve sign-in performance and to create a new domain controller for a branch office by using IFM.

## Objectives

After performing this lab, you should be able to:

- Install a domain controller.
- Install a domain controller by using IFM.

## Lab Setup

Estimated Time: 50 minutes

| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b><br><b>20410D-LON-RTR</b><br><b>20410D-LON-SVR2</b> |
|------------------|----------------------------------------------------------------------------------------------------|
| User name        | <b>Adatum\Administrator</b>                                                                        |
| Password         | <b>Pa\$\$w0rd</b>                                                                                  |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**.  
Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20410D-LON-SVR1**, **20410D-LON-RTR**, and **20410D-LON-SVR2**.

## Exercise 1: Installing a Domain Controller

### Scenario

Users are experiencing slow sign-ins in London during peak use times. The server team has determined that the domain controllers are overwhelmed when many users authenticate simultaneously. To improve sign-in performance, you will add a new domain controller in the London data center.

The main tasks for this exercise are as follows:

1. Add an Active Directory Domain Services (AD DS) role to a member server.
2. Configure a server as a domain controller.
3. Configure a server as a global catalog server.

► **Task 1: Add an Active Directory Domain Services (AD DS) role to a member server**

1. On LON-DC1, in Server Manager, add **LON-SVR1** to the server list.
2. Add the **Active Directory Domain Services** server role to **LON-SVR1**. Add all required features as prompted.

Installation will take several minutes.

3. When the installation completes, click **Close** to close the Add Roles and Features Wizard.

► **Task 2: Configure a server as a domain controller**

- On LON-DC1, use Server Manager to promote LON-SVR1 to a domain controller, and choose the following options:
  - Add a domain controller to the existing Adatum.com domain
  - Use the credentials **Adatum\Administrator** with the password **Pa\$\$w0rd**
  - For Domain Controller Options, install the **Domain Name System**, but remove the selection to install the global catalog
  - The DSRM password is **Pa\$\$w0rd**
  - For all other options, use the default options

► **Task 3: Configure a server as a global catalog server**

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Use Active Directory Sites and Services to make LON-SVR1 a global catalog server.

**Results:** After completing this exercise, you will have explored Server Manager and promoted a member server to be a domain controller.

## Exercise 2: Installing a Domain Controller by Using IFM

### Scenario

Your manager has assigned you to manage one of the new branch offices that are being configured. A faster network connection will be installed in a few weeks. Until then, network connectivity will be very slow.

The branch office requires a domain controller to support local sign-ins. To avoid problems with the slow network connection, you will use IFM to install the domain controller in the branch office.

The main tasks for this exercise are as follows:

1. Use the ntdsutil tool to generate IFM.
2. Add the AD DS role to the member server.
3. Use IFM to configure a member server as a new domain controller.

► **Task 1: Use the ntdsutil tool to generate IFM**

1. On LON-DC1, open an administrative command-line interface, and then use **ntdsutil** to create an IFM backup of both the AD DS database and the SYSVOL folder. The commands to create the backup are as follows:

```
Ntdsutil
Activate instance ntds
Ifm
Create sysvol full c:\ifm
```

2. Wait for the IFM command to complete, and then close the command prompt.

► **Task 2: Add the AD DS role to the member server**

1. Switch to **LON-SVR2**, and sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open a command prompt, and then map the drive letter **K:** to **\LON-DC1\C\$\IFM**.
3. Use Server Manager to install the AD DS server role on LON-SVR2.

► **Task 3: Use IFM to configure a member server as a new domain controller**

1. On LON-SVR2, at the command prompt, copy the IFM backup from **K:** to **C:\ifm**.
2. On LON-SVR2, use Server Manager with the following options to perform the post-deployment configuration of AD DS:
  - o Add a domain controller to the existing Adatum.com domain
  - o Use **Adatum\Administrator** with the password **Pa\$\$w0rd** for credentials
  - o Use **Pa\$\$w0rd** for the DSRM password
  - o Use the IFM media to configure and install AD DS. Use the location **C:\IFM** for the IFM media
  - o Accept all other defaults
3. Restart LON-SVR2 to complete the AD DS installation.

**Results:** After completing this exercise, you will have installed an additional domain controller for the branch office by using IFM.

### Lab Review Questions

**Question:** Why did you use Server Manager and not **dcpromo** when you promoted a server to be a domain controller?

**Question:** What are the three operations masters found in each domain?

**Question:** What are the two operations masters that are present in a forest?

**Question:** What is the benefit of performing an IFM install of a domain controller?

### ► Prepare for the next module

When you have completed the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-SVR1**, **20410D-LON-RTR**, and **20410D-LON-SVR2**.

# Lab: Managing Active Directory Domain Services Objects

## Scenario

You have been working for A. Datum Corporation as a desktop support specialist and have visited desktop computers to troubleshoot app and network problems. You have recently accepted a promotion to the server support team. One of your first assignments is to configure the infrastructure service for a new branch office.

To begin deployment of the new branch office, you are preparing AD DS objects. As part of this preparation, you need to create an OU for the branch office and delegate permission to manage it. Then you need to create users and groups for the new branch office. Finally, you need to reset the secure channel for a computer account that has lost connectivity to the domain in the branch office.

## Objectives

After completing this lab, you should be able to:

- Delegate administration for a branch office.
- Create and configure user accounts in AD DS.
- Manage computer objects in AD DS.

## Lab Setup

Estimated Time: 70 minutes

| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-CL1</b> |
|------------------|------------------------------------------------|
| User name        | <b>Adatum\Administrator</b>                    |
| Password         | <b>Pa\$\$w0rd</b>                              |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**.  
Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20410D-LON-CL1**.

## Exercise 1: Delegating Administration for a Branch Office

### Scenario

A. Datum delegates management of each branch office to a specific group. This allows an employee who works onsite to be configured as an administrator when required. Each branch office has a branch administrators group that can perform full administration within the branch office OU. There is also a branch office help desk group that is able to manage users in the branch office OU, but not other objects. You need to create these groups for the new branch office and delegate permissions to the groups.

The main tasks for this exercise are as follows:

1. Delegate administration for Branch Administrators.
2. Delegate a user administrator for the Branch Office Help Desk.
3. Add a member to the Branch Administrators.
4. Add a member to the Branch Help Desk group.

#### ► Task 1: Delegate administration for Branch Administrators

1. On LON-DC1, open Active Directory Users and Computers, and then in the Adatum.com domain, create a new OU named **Branch Office 1**.
2. Create the following global security groups in the **Branch Office 1** OU:
  - o **Branch 1 Help Desk**
  - o **Branch 1 Administrators**
  - o **Branch 1 Users**
3. Move **Holly Dickson** from the **IT** OU to the **Branch Office 1** OU.
4. Move the following users to the **Branch Office 1** OU:
  - o **Development\Bart Duncan**
  - o **Managers\Ed Meadows**
  - o **Marketing\Connie Vrettos**
  - o **Research\Barbara Zighetti**
  - o **Sales\Arlene Huff**
5. Move the LON-CL1 computer to the **Branch Office 1** OU, and then restart the LON-CL1 computer.
6. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
7. On LON-DC1, in Active Directory Users and Computers, use the Delegate Control Wizard to delegate administration of the **Branch Office 1** OU to the **Branch 1 Administrators** security group by delegating the following common and custom tasks:
  - a. Delegate the following common tasks:
    - **Create, delete, and manage user accounts**
    - **Reset user passwords and force password change at next logon**
    - **Read all user information**
    - **Create, delete and manage groups**
    - **Modify the membership of a group**
    - **Manage Group Policy links**

- b. Delegate the following custom tasks:

- **Create and delete computer objects in the current OU**
- **Full control of computer objects in the current OU**

► **Task 2: Delegate a user administrator for the Branch Office Help Desk**

1. On LON-DC1, in Active Directory Users and Computers, use the Delegate Control Wizard to delegate administration of the **Branch Office 1** OU to the **Branch 1 Help Desk** security group.
2. Delegate the following common tasks:
  - **Reset user passwords and force password change at next logon**
  - **Read all user information**
  - **Modify the membership of a group**

► **Task 3: Add a member to the Branch Administrators**

1. On LON-DC1, add **Holly Dickson** to the **Branch 1 Administrators** global group.
2. Add the **Branch 1 Administrators** global group to the **Server Operators** domain local group.
3. Sign out from LON-DC1.
4. Sign in as **Adatum\Holly** with the password **Pa\$\$w0rd**.

You can sign in locally at a domain controller because Holly belongs indirectly to the Server Operators domain local group.

5. In Server Manager, open **Active Directory Users and Computers**.

Confirm Holly's current credentials in the **User Account Control** dialog box.

6. Attempt to delete **Sales\Aaren Ekelund**.

You are unsuccessful, because Holly lacks the required permissions.

7. Try to delete **Branch Office 1\Ed Meadows**.

You are successful, because Holly has the required permissions.

► **Task 4: Add a member to the Branch Help Desk group**

1. On LON-DC1, add **Bart Duncan** to the **Branch 1 Help Desk** global group.
2. Close Active Directory Users and Computers, and then close Server Manager.
3. Open Server Manager, and then open **Active Directory Users and Computers**.
4. In the **User Account Control** dialog box, specify **Adatum\Administrator** and **Pa\$\$w0rd** as the required credentials.

To modify the Server Operators membership list, you must have permissions beyond those available to the Branch 1 Administrators group.

5. Add the **Branch 1 Help Desk** global group to the **Server Operators** domain local group.

6. Sign out from LON-DC1.

7. Sign in as **Adatum\Bart** with the password **Pa\$\$w0rd**.

You can sign in locally at a domain controller because Bart belongs indirectly to the Server Operators domain local group.

8. Open Server Manager, and then open **Active Directory Users and Computers**. Confirm your current credentials in the **User Account Control** dialog box.

9. Try to delete **Branch Office 1\Connie Vrettos**.  
You are unsuccessful, because Bart lacks the required permissions.
10. Reset Connie's password to **Pa\$\$w0rd**.
11. After confirming the password reset is successful, sign out from LON-DC1.
12. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

**Results:** After completing this exercise, you will have successfully created an OU, and delegated administration of it to the appropriate group.

## Exercise 2: Creating and Configuring User Accounts in AD DS

### Scenario

You have a list of new users for the branch office, and you need to create user accounts for them.

The main tasks for this exercise are as follows:

1. Create a user template for the branch office.
2. Configure the template settings.
3. Create a new user for the branch office, based on the template.
4. Sign in as a user to test account settings.

#### ► Task 1: Create a user template for the branch office

1. On LON-DC1, create a folder called **C:\branch1-userdata**, and then share it.
2. Modify the shared folder permissions so that the **Everyone** group has **Full Control Allow** permissions.
3. In Server Manager, open **Active Directory Users and Computers**, and then create a new user with the following properties in the **Branch Office 1** OU:
  - o Full name: **\_Branch\_template**
  - o User logon name: **\_Branch\_template**
  - o Password: **Pa\$\$w0rd**
  - o **Account is disabled**

#### ► Task 2: Configure the template settings

- On LON-DC1, modify the following properties of the **\_Branch\_template** account:
  - o City: **Slough**
  - o Group: **Branch 1 Users**
  - o Home folder: **\\\\lon-dc1\\branch1-userdata\\%username%**

#### ► Task 3: Create a new user for the branch office, based on the template

1. On LON-DC1, copy the **\_Branch\_template** user account, and then configure the following properties:
  - o First name: **Ed**
  - o Last name: **Meadows**

- Password: **Pa\$\$w0rd**
  - **User must change password at next logon** is cleared
  - **Account is disabled** is cleared
2. Verify that the following properties have been copied during account creation:
    - City: **Slough**
    - Home folder path: **\\\lon-dc1\branch1-userdata\Ed**
    - Group: **Branch 1 Users**
  3. Sign out from LON-DC1.

► **Task 4: Sign in as a user to test account settings**

1. Switch to LON-CL1 and sign off.
2. Sign in to LON-CL1 as **Adatum\Ed** with the password **Pa\$\$w0rd**.  
You are able to sign in successfully.
3. Verify that you have a drive mapping for drive Z to Ed's home folder on LON-DC1.
4. Sign out of LON-CL1.

**Results:** After completing this exercise, you will have successfully created and tested a user account created from a template.

## Exercise 3: Managing Computer Objects in AD DS

### Scenario

A workstation has lost its connectivity to the domain and cannot authenticate users properly. When users attempt to access resources from this workstation, access is denied. You need to reset the computer account to recreate the trust relationship between the client and the domain.

The main tasks for this exercise are as follows:

1. Reset a computer account.
2. Observe the behavior when a client logs on.
3. Rejoin the domain to reconnect the computer account.

► **Task 1: Reset a computer account**

1. On LON-DC1, sign in as **Adatum\Holly** with the password **Pa\$\$w0rd**.
2. Open **Active Directory Users and Computers**.
3. Confirm your credentials in the **User Account Control** dialog box.
4. Navigate to **Branch Office 1**.
5. Reset the **LON-CL1** computer account.

► **Task 2: Observe the behavior when a client logs on**

1. Switch to LON-CL1, and attempt to sign in as **Adatum\Ed** with the password **Pa\$\$w0rd**.

A message appears stating that **The trust relationship between this workstation and the primary domain failed.**

2. Click **OK** to acknowledge the message.

► **Task 3: Rejoin the domain to reconnect the computer account**

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open the Control Panel, switch to **Large icons** view, and then open **System**.
3. View the **Advanced system settings**, and then click the **Computer Name** tab.
4. In the **System Properties** dialog box, use the **Network ID** button to rejoin the computer to the domain.
5. Complete the wizard using the following settings:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
  - Would you like to use the LON-CL1 computer name: **Yes**
  - Do you want to enable a domain user account on this computer: **No**
6. When prompted, restart the computer.
7. Sign in as **Adatum\Ed** with the password of **Pa\$\$w0rd**.

You are successful because the computer had been successfully rejoined.

**Results:** After completing this exercise, you will have successfully reset a trust relationship.

### Lab Review Questions

**Question:** What are the options for modifying the attributes of new and existing users?

**Question:** What types of objects can be members of global groups?

**Question:** What types of objects can be members of domain-local groups?

**Question:** Which two credentials are necessary for any computer to join a domain?

► **Prepare for the next module**

When you have completed the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the Virtual Machines list, right-click **20410D-LON-CL1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-DC1**.

# Lab: Automating AD DS Administration by Using Windows PowerShell

## Scenario

You have been working for A. Datum Corporation for several years as a desktop support specialist. In this role, you visited desktop computers to troubleshoot app and network problems. You have recently accepted a promotion to the server support team. One of your first assignments is configuring the infrastructure service for a new branch office.

As part of configuring a new branch office, you need to create user and group accounts. Creating multiple users with graphical tools is inefficient, so, you will use Windows PowerShell.

## Objectives

After completing this lab, you should be able to:

- Create user accounts and groups by using Windows PowerShell.
- Use Windows PowerShell to create user accounts in bulk.
- Use Windows PowerShell to modify user accounts in bulk.

## Lab Setup

Estimated Time: 45 minutes

|                  |                                                |
|------------------|------------------------------------------------|
|                  |                                                |
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-CL1</b> |
| User name        | <b>Adatum\Administrator</b>                    |
| Password         | <b>Pa\$\$w0rd</b>                              |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**.  
Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 and 3 for **20410D-LON-CL1**. Do not sign in to LON-CL1 until directed to do so.

## Exercise 1: Creating User Accounts and Groups by Using Windows PowerShell

### Scenario

A. Datum Corporation has a number of scripts that it has previously used to create user accounts by using command-line tools. However, an enterprise-wide mandate specifies that all future scripting will be done by using Windows PowerShell. As the first step in creating scripts, you need to identify the syntax required to manage AD DS objects in Windows PowerShell.

The main tasks for this exercise are as follows:

1. Create a user account by using Windows PowerShell.
2. Create a group by using Windows PowerShell.

#### ► Task 1: Create a user account by using Windows PowerShell

1. On LON-DC1, open a Windows PowerShell Command Prompt window.
2. At the Windows PowerShell prompt, create a new OU named **LondonBranch** by typing the following command:

```
New-ADOrganizationalUnit LondonBranch
```

3. Create a new user account for **Ty Carlson** in the LondonBranch OU by using the following command:

```
New-ADUser -Name Ty -DisplayName "Ty Carlson" -GivenName Ty -Surname Carlson -Path
"ou=LondonBranch,dc=adatum,dc=com"
```

4. Change the blank password for the new account to **Pa\$\$w0rd**, by using the following command:

```
Set-ADAccountPassword Ty
```

5. Enable the new user account by using the following command:

```
Enable-ADAccount Ty
```

6. On LON-CL1, sign in as **Ty** with the password **Pa\$\$w0rd**.

7. Verify that the sign-in is successful, and then sign out of LON-CL1.

#### ► Task 2: Create a group by using Windows PowerShell

1. On LON-DC1, at the Windows PowerShell prompt, create a new global security group for users in the London branch office, by using the following command:

```
New-ADGroup LondonBranchUsers -Path "ou=LondonBranch,dc=adatum,dc=com" -GroupScope
Global -GroupCategory Security
```

2. At the Windows PowerShell prompt, add **Ty** as a member of LondonBranchUsers, by using the following command:

```
Add-ADGroupMember LondonBranchUsers -Members Ty
```

3. At the Windows PowerShell prompt, confirm that Ty is now a member of LondonBranchUsers, by using the following command:

```
Get-ADGroupMember LondonBranchUsers
```

**Results:** After completing this exercise, you will have created user accounts and groups by using Windows PowerShell.

## Exercise 2: Using Windows PowerShell to Create User Accounts in Bulk

### Scenario

You have a .csv file that contains a large list of new users for the branch office. It is inefficient to create these users individually with graphical tools, so you will use a Windows PowerShell script instead. A colleague that has experience with scripting has given you a script that she created. You need to modify the script to match the format of your .csv file.

The main tasks for this exercise are as follows:

1. Prepare the .csv file.
2. Prepare the script.
3. Run the script.

#### ► Task 1: Prepare the .csv file

1. On LON-DC1, read the contents in **E:\Labfiles\Mod04\LabUsers.ps1** to identify the header requirements for the .csv file.
2. Edit the contents in **E:\Labfiles\Mod04\LabUsers.csv**, and then add the appropriate header.

#### ► Task 2: Prepare the script

1. On LON-DC1, use Windows PowerShell Integrated Scripting Environment (ISE) to modify the variables in **LabUsers.ps1**:
  - o \$csvfile: **E:\Labfiles\Mod04\LabUsers.csv**
  - o \$OU: "**ou=LondonBranch,dc=adatum,dc=com**"
2. Save the modified **LabUsers.ps1**.
3. Review the contents of the script.

#### ► Task 3: Run the script

1. On LON-DC1, open a Windows PowerShell command prompt, and then run **E:\Labfiles\Mod04\LabUsers.ps1**.
2. At the Windows PowerShell prompt, use the following command to verify that the users were created:

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com"
```

3. On LON-CL1, sign in as **Luka** with the password **Pa\$\$w0rd**.

**Results:** After completing this exercise, you will have used Windows PowerShell to create user accounts in bulk.

## Exercise 3: Using Windows PowerShell to Modify User Accounts in Bulk

### Scenario

You have received a request to update all user accounts in the new branch office OU with the correct address of the new building. Additionally, you have been asked to ensure that all of the new user accounts in the branch office are configured to force users to change their passwords the next time they sign in.

The main tasks for this exercise are as follows:

1. Force all user accounts in LondonBranch to change their passwords at next sign in.
2. Configure the address for user accounts in LondonBranch.

#### ► Task 1: Force all user accounts in LondonBranch to change their passwords at next sign in

1. On LON-DC1, open a Windows PowerShell Command Prompt window.
2. At the Windows PowerShell prompt, create a query for user accounts in the LondonBranch OU by using the following command:

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com" | Format-Wide
DistinguishedName
```

3. At the Windows PowerShell prompt, modify the previous command to force all users to change their password the next time they sign in by using the following command:

```
Get-ADUser -Filter * -SearchBase "ou=LondonBranch,dc=adatum,dc=com" | Set-ADUser
-ChangePasswordAtLogon $true
```

#### ► Task 2: Configure the address for user accounts in LondonBranch

1. On LON-DC1, open the **Active Directory Administrative Center**.
2. Open the properties for all user accounts in LondonBranch.
3. Set the address for multiple users as follows:
  - o Street: **Branch Office**
  - o City: **London**
  - o Country/Region: **United Kingdom**

**Results:** After completing this exercise, you will have modified user accounts in bulk.

### Lab Review Questions

**Question:** By default, are new user accounts enabled or disabled when you create them by using the **New-ADUser** cmdlet?

**Question:** What file extension do Windows PowerShell scripts use?

## ► Prepare for the next module

When you finish the lab, revert all virtual machines to their initial state by performing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the Virtual Machines list, right-click **20410D-LON-CL1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-DC1**.

# Lab: Implementing IPv4

## Scenario

You have recently accepted a promotion to the server support team. One of your first assignments is configuring the infrastructure service for a new branch office.

After a security review, your manager has asked you to calculate new subnets for the branch office to support segmenting network traffic. You also need to troubleshoot a connectivity problem on a server in the branch office.

## Objectives

After completing this lab, you should be able to:

- Identify appropriate subnets for a given set of requirements.
- Troubleshoot IPv4 connectivity issues.

## Lab Setup

Estimated Time: 45 minutes

|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
|                  |                                                                          |
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-RTR</b><br><b>20410D-LON-SVR2</b> |
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

- On the host computer, start **Hyper-V Manager**.
- In Microsoft Hyper-V® Manager, click **20410D-LON-DC1**, and then, in the Actions pane, click **Start**.
- In the Actions pane, click **Connect**. Wait until the virtual machine starts.
- Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
- Repeat steps 2 through 4 for **20410D-LON-RTR** and **20410D-LON-SVR2**.

## Exercise 1: Identifying Appropriate Subnets

### Scenario

The new branch office is configured with a single subnet. After a security review, all branch office network configurations are being modified to place servers on a separate subnet from the client computers. You need to calculate the new subnet mask and the default gateways for the subnets in your branch.

The current network for your branch office is 192.168.98.0/24. This network needs to be subdivided into three subnets that meet the following requirements:

- One subnet with at least 100 IP addresses for clients.
- One subnet with at least 10 IP addresses for servers.
- One subnet with at least 40 IP addresses for future expansion.

The main tasks for this exercise are as follows:

1. Calculate the bits required to support the hosts on each subnet.
2. Calculate subnet masks and network IDs.

**► Task 1: Calculate the bits required to support the hosts on each subnet**

1. How many bits are required to support 100 hosts on the client subnet?
2. How many bits are required to support 10 hosts on the server subnet?
3. How many bits are required to support 40 hosts on the future expansion subnet?
4. If all subnets are the same size, can they be accommodated?
5. Which feature allows a single network to be divided into subnets of varying sizes?
6. How many host bits will you use for each subnet? Use the simplest allocation possible, which is one large subnet and two equal-sized smaller subnets.

**► Task 2: Calculate subnet masks and network IDs**

1. Given the number of host bits allocated, what is the subnet mask that you will use for the client subnet? Calculate the subnet mask in binary and decimal.
  - o The client subnet is using 7 bits for the host ID. Therefore, you can use 25 bits for the subnet mask.

| Binary | Decimal |
|--------|---------|
|        |         |

2. Given the number of host bits allocated, what is the subnet mask that you will use for the server subnet? Calculate the subnet mask in binary and decimal.
  - o The server subnet is using 6 bits for the host ID. Therefore, you will use 26 bits for the subnet mask.

| Binary | Decimal |
|--------|---------|
|        |         |

3. Given the number of host bits allocated, what is the subnet mask that you can use for the future expansion subnet? Calculate the subnet mask in binary and decimal.
  - o The future expansion subnet is using 6 bits for the host ID. Therefore, you will use 26 bits for the subnet mask.

| Binary | Decimal |
|--------|---------|
|        |         |

4. For the client subnet, define the network ID, first available host, last available host, and broadcast address. Assume that the client subnet is the first subnet allocated from the available address pool. Calculate the binary and decimal versions of each address.

| Description | Binary | Decimal |
|-------------|--------|---------|
| Network ID  |        |         |
| First host  |        |         |
| Last host   |        |         |
| Broadcast   |        |         |

5. For the server subnet, define the network ID, first available host, last available host, and broadcast address. Assume that the server subnet is the second subnet allocated from the available address pool. Calculate the binary and decimal versions of each address.

| Description | Binary | Decimal |
|-------------|--------|---------|
| Network ID  |        |         |
| First host  |        |         |
| Last host   |        |         |
| Broadcast   |        |         |

6. For the future allocation subnet, define the network ID, first available host, last available host, and broadcast address. Assume that the future allocation subnet is the third subnet allocated from the available address pool. Calculate the binary and decimal versions of each address.

| Description | Binary | Decimal |
|-------------|--------|---------|
| Network ID  |        |         |
| First host  |        |         |
| Last host   |        |         |
| Broadcast   |        |         |

**Results:** After completing this exercise, you should have identified a configuration of subnet that will meet the requirements of the lab scenario.

## Exercise 2: Troubleshooting IPv4

### Scenario

A server in the branch office is unable to communicate with the domain controller in the head office. You need to resolve the network connectivity problem.

The main tasks for this exercise are as follows:

1. Prepare for troubleshooting.
2. Troubleshoot IPv4 connectivity between LON-SVR2 and LON-DC1.

#### ► Task 1: Prepare for troubleshooting

1. On LON-SVR2, open **Windows PowerShell**.
2. In the Windows PowerShell window, run the following cmdlet:

```
Test-NetConnection LON-DC1
```

3. Verify that you receive a reply that contains **PingSucceeded:True** from **LON-DC1**.
4. Open a File Explorer window, and browse to **\LON-DC1\E\$\Labfiles\Mod05**.
5. From File Explorer, run the **Break2.ps1** script by using Windows PowerShell.

This script creates the problem that you will troubleshoot and repair in the next task.

6. Close File Explorer.

#### ► Task 2: Troubleshoot IPv4 connectivity between LON-SVR2 and LON-DC1

1. Use your knowledge of IPv4 to troubleshoot and repair the connectivity problem between LON-SVR2 and LON-DC1. Consider using the following tools:
  - **Test-NetConnection**
  - **Test-NetConnection -TraceRoute**
  - **Get-NetRoute**
  - **New-NetRoute**
2. When you have repaired the problem, run the **Test-NetConnection LON-DC1** cmdlet from LON-SVR2 to confirm that the problem is resolved.

**Results:** After completing this lab, you should have resolved an IPv4 connectivity problem.

### Lab Review Questions

**Question:** Why is variable-length subnetting required in this lab?

**Question:** Which Windows PowerShell cmdlet can you use to view the local routing table of a computer instead of using **route print**?

### ► Prepare for the next module

After you finish the lab, revert the virtual machines back to their initial state by completing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, in the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-RTR** and **20410D-LON-SVR2**.

# Lab: Implementing DHCP

## Scenario

A. Datum Corporation has an IT office and data center in London, which supports the London location and other locations as well. A. Datum has recently deployed a Windows 2012 Server infrastructure with Windows 8 clients.

You have recently accepted a promotion to the server support team. One of your first assignments is to configure the infrastructure service for a new branch office. As part of this assignment, you need to configure a DHCP server that will provide IP addresses and configuration to client computers. Servers are configured with static IP addresses and do not use DHCP.

## Objectives

After completing this lab, you should be able to:

- Implement DHCP
- Implement a DHCP relay agent (optional)

## Lab Setup

Estimated Time: 60 minutes

| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b><br><b>20410D-LON-RTR</b><br><b>20410D-LON-CL1</b><br><b>20410D-LON-CL2</b> |
|------------------|----------------------------------------------------------------------------------------------------------------------------|
| User name        | <b>Adatum\Administrator</b>                                                                                                |
| Password         | <b>Pa\$\$w0rd</b>                                                                                                          |

For this lab, you will use the available virtual machine environment. Before beginning the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20410D-LON-SVR1** and **20410D-LON-CL1**.
6. For the optional Exercise 2, you should repeat steps 2 through 4 for **20410D-LON-RTR** and **20410D-LON-CL2**.

## Exercise 1: Implementing DHCP

### Scenario

As part of configuring the infrastructure for the new branch office, you need to configure a DHCP server that will provide IP addresses and configuration to client computers. Servers are configured with static IP addresses and usually do not use DHCP for obtaining IP addresses.

One of the client computers in the branch office needs to access an accounting app in the head office. The network team uses firewalls based on IP addresses to restrict access to this app. The network team has requested that you assign a static IP address to this client computer. Rather than configuring a static IP address on the client computer manually, you decide to create a reservation in DHCP for the client computer.

The main tasks for this exercise are as follows:

1. Install the Dynamic Host Configuration Protocol (DHCP) server role.
2. Configure the DHCP scope and options.
3. Configure the client to use DHCP, and then test the configuration.
4. Configure a lease as a reservation.

#### ► Task 1: Install the Dynamic Host Configuration Protocol (DHCP) server role

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open Server Manager, and then install the **DHCP Server** role.
3. In the Add Roles and Features Wizard, accept all defaults.

#### ► Task 2: Configure the DHCP scope and options

1. In Server Manager, open the DHCP console.
2. Authorize the **lon-svr1.adatum.com** server in AD DS.
3. In DHCP, in the navigation pane, browse to **IPv4**, right-click **IPv4**, and then click **New Scope**.
4. Create a new scope with the following properties:
  - Name: **Branch Office**
  - IP Address Range: **172.16.0.100-172.16.0.200**
  - Length: **16**
  - Subnet Mask: **255.255.0.0**
  - Exclusions: **172.16.0.190-172.16.0.200**
  - Configure options **Router 172.16.0.1**
  - For all other settings use default values
5. Activate the scope.

► **Task 3: Configure the client to use DHCP, and then test the configuration**

1. Sign in to **20410D-LON-CL1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Reconfigure the Ethernet Connection using the following information:
  - o **Configure Internet Protocol Version 4 (TCP/IPv4)**
  - o **Obtain an IP address automatically**
  - o **Obtain DNS server address automatically**
3. Open the Command Prompt window, and then initiate the DHCP process using the **ipconfig /renew** command.
4. To test the configuration, verify that LON-CL1 has received an IP address from the DHCP scope by typing **ipconfig /all** in the Command Prompt window.

This command returns information such as IP address, subnet mask, and DHCP enabled status, which should be **Yes**.

► **Task 4: Configure a lease as a reservation**

1. To display the physical address of the network adapter, in the Command Prompt window, run the following command:

```
ipconfig /all
```

2. Switch to **LON-SVR1**.
3. Open the DHCP console.
4. In the DHCP console, in the navigation pane, browse to **Scope [172.16.0.0] Branch Office**, right-click **Reservations**, and then click **New Reservation**.
5. Create a new reservation for **LON-CL1** using the physical address of the **LON-CL1** network adapter, and the IP address **172.16.0.155**.
6. On LON-CL1, use the **ipconfig** command to renew and then verify the IP address.

**Results:** After completing this exercise, you should have implemented DHCP, configured DHCP scope and options, and configured a DHCP reservation.

► **Prepare for the optional exercise**

If you are going to complete the optional lab, revert the 20410D-LON-CL1 and 20410D-LON-SVR1 virtual machines by performing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-CL1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 1 through 3 for **20410D-LON-SVR1**.
5. Start **20410D-LON-SVR1**.

## Exercise 2: Implementing a DHCP Relay Agent (Optional Exercise)

### Scenario

To avoid configuring an addition DHCP server on the subnet, your manager has asked you to configure a DHCP relay agent for another subnet in your branch office.

The main tasks for this exercise are as follows:

1. Install a DHCP relay agent.
2. Configure a DHCP relay agent.
3. Test the DHCP relay agent with a client.

#### ► Task 1: Install a DHCP relay agent

1. Sign in to LON-RTR as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, open **Routing and Remote Access**.
3. Add the DHCP relay agent to the router on LON-RTR by performing the following steps:
  - a. In the navigation pane, expand **LON-RTR (local)**, expand **IPv4**, right-click **General**, and then click **New Routing Protocol**.
  - b. In the **Routing protocols** list, click **DHCP Relay Agent**, and then click **OK**.

#### ► Task 2: Configure a DHCP relay agent

1. Open Routing and Remote Access.
2. Configure the DHCP relay agent by performing the following steps:
  - a. In the navigation pane, right-click **DHCP Relay Agent**, and then click **New Interface**.
  - b. In the **New Interface for DHCP Relay Agent** dialog box, click **Ethernet 2**, and then click **OK**.
  - c. In the **DHCP Relay Agent Properties – Ethernet 2 Properties** dialog box, click **OK**.
  - d. Right-click **DHCP Relay Agent**, and then click **Properties**.
  - e. In the **DHCP Relay Agent Properties** dialog box, in the **Server address** box, type **172.16.0.11**, click **Add**, and then click **OK**.
3. Close Routing and Remote Access.

### ► Task 3: Test the DHCP relay agent with a client

To test how a client receives an IP address from the DHCP relay agent in another subnet, you need to create another DHCP scope.

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Run Windows PowerShell as Administrator, and then type the following cmdlets:

```
Add-WindowsFeature -IncludeManagementTools dhcp
netsh dhcp add securitygroups
Restart-service dhcpserver
Add-DhcpServerInDC LON-SVR1 172.16.0.11
Add-DhcpServerv4Scope -Name "Branch Office 2" -StartRange 10.10.0.100 -EndRange
10.10.0.200 -SubnetMask 255.255.0.0
Add-DhcpServerv4ExclusionRange -ScopeID 10.10.0.0 -StartRange 10.10.0.190 -EndRange
10.10.0.200
Set-DhcpServerv4OptionValue -Router 10.10.0.1
Set-DhcpServerv4Scope -ScopeID 10.10.0.0 -State Active
```

3. To test the client, switch to **LON-CL2**.
4. Open the Network and Sharing Center window, and then configure the **Ethernet, Internet Protocol Version 4 (TCP/IPv4)** properties with the following settings:
  - **Obtain IP address automatically**
  - **Obtain DNS server address automatically**
5. Open the Command Prompt window.
6. In the Command Prompt window, at a command prompt, type the following command:

```
Ipconfig /renew
```

7. Verify that IP address and DNS server settings on LON-CL2 are obtained from DHCP Server scope installed on **LON-SVR1**.

The IP address should be in the following range: **10.10.0.100/16** to **10.10.0.200/16**.

**Results:** After completing this exercise, you should have implemented a DHCP relay agent.

### Lab Review Questions

**Question:** What purpose does the DHCP scope have?

**Question:** How should you configure a computer to receive an IP address from the DHCP server?

**Question:** Why do you need MAC address for a DHCP server reservation?

**Question:** What information do you need to configure on a DHCP relay agent?

## ► Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-SVR1**, **20410D-LON-RTR**, and **20410D-LON-CL2**.

# Lab: Implementing DNS

## Scenario

Your manager has asked you to configure the domain controller in the branch office as a DNS server. You also have been asked to create some new host records to support a new app that is being installed.

Finally, you need to configure forwarding on the DNS server in the branch office to support Internet name resolution.

## Objectives

After completing this lab, you should be able to:

- Install and configure DNS.
- Create host records in DNS.
- Manage the DNS server cache.

## Lab Setup

Estimated Time: 60 minutes

|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
|                  |                                                                          |
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b><br><b>20410D-LON-CL1</b> |
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

For this lab, you will use the available virtual machine environment. Before beginning the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20410D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20410D-LON-SVR1** and **20410D-LON-CL1**.

## Exercise 1: Installing and Configuring DNS

### Scenario

Contoso is a partner organization that is working closely with users in the new branch office. To support name resolution between A Datum's branch office and Contoso, you decide to enable DNS forwarding between the two DNS domains.

As part of configuring the infrastructure for the new branch office, you must configure a DNS server that provides name resolution for the branch office. This includes the forwarding for Contoso.com.

The DNS server in the branch office will be a domain controller. The Active Directory integrated zones required to support logons will be replicated automatically to the branch office.

The main tasks for this exercise are as follows:

1. Configure LON-SVR1 as a domain controller without installing the Domain Name System (DNS) server role.
2. Review configuration settings on the existing DNS server to confirm root hints.
3. Add the DNS server role for the branch office on the domain controller.
4. Verify replication of the Adatum.com Active Directory–integrated zone.
5. Create and configure Contoso.com zone on LON-DC1.
6. Use Windows PowerShell commands to test non-local resolution.
7. Configure Internet name resolution to forward to the head office.
8. Use Windows PowerShell to confirm name resolution.

► **Task 1: Configure LON-SVR1 as a domain controller without installing the Domain Name System (DNS) server role**

1. Use **Add roles and features** in Server Manager to add the **Active Directory Domain Services** role to LON-SVR1.
2. After the role is added, promote LON-SVR1 to domain controller.
3. Choose to add LON-SVR1 as an additional domain controller in the **Adatum.com** domain.
4. Choose to not install the DNS server by clearing the **DNS** check box, which is selected by default.

► **Task 2: Review configuration settings on the existing DNS server to confirm root hints**

1. In DNS Manager on LON-DC1, open the **Properties** dialog box for LON-DC1.
2. Review root hints and forwarder configuration.

► **Task 3: Add the DNS server role for the branch office on the domain controller**

- Use Server Manager to add the DNS Server role to LON-SVR1.

► **Task 4: Verify replication of the Adatum.com Active Directory–integrated zone**

1. On LON-SVR1, open the **DNS Manager** console.
2. Expand **Forward Lookup Zones**, and verify that both the **Adatum.com** and **\_msdcs.Adatum.com** zones are replicated.

 **Note:** If you do not see these zones, open Active Directory Sites and Services, force replication between **LON-DC1** and **LON-SVR1**, and then repeat steps 1 and 2.

► **Task 5: Create and configure Contoso.com zone on LON-DC1**

1. On the LON-DC1 virtual machine, open the **DNS Manager** console.
2. Create a new **Forward Lookup Zone** with the following parameters:
  - Zone type: **Primary Zone**
  - Store the zone in Active Directory: **No** (clear the check box)

- Zone name: **contoso.com**
  - All other values: defaults
3. Create a new host record named **www.contoso.com** with an IP Address of **172.16.0.100**.

► **Task 6: Use Windows PowerShell commands to test non-local resolution**

1. On LON-SVR1, make **127.0.0.1** the **preferred DNS server** for LON-SVR1 using the following Windows PowerShell cmdlet, where **X** is the Interface Index number, which you can find in the **Get-DnsClient** cmdlet:

```
Set-DnsClientServerAddress -InterfaceIndex X -ServerAddress 127.0.0.1
```

2. In a Windows PowerShell window on LON-SVR1, try to resolve **www.contoso.com** by using the **Resolve-DNSName** cmdlet.

You should receive an error message in red text. This is expected.

3. Perform an **nslookup** command within Windows PowerShell for the www.contoso.com address. This command should also fail.
4. Leave the Windows PowerShell window open.

► **Task 7: Configure Internet name resolution to forward to the head office**

1. Type the following cmdlet, and then press Enter:

```
Set-DnsServerForwarder -IPAddress '172.16.0.10' -PassThru
```

2. Type the following two cmdlets, and then press Enter after each one:

```
Stop-Service DNS
```

```
Start-Service DNS
```

► **Task 8: Use Windows PowerShell to confirm name resolution**

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In Windows PowerShell, type the following cmdlet, and then press Enter:

```
nslookup www.contoso.com
```

You should get a non-authoritative reply and an IP address.

**Results:** After completing this exercise, you should have installed and configured DNS on 20410D-LON-SVR1.

## Exercise 2: Creating Host Records in DNS

### Scenario

Several new web-based apps are being implemented in the A. Datum head office. For each app, you must configure a host record in DNS. You have been asked to create the new host records for these apps.

The main tasks for this exercise are as follows:

1. Configure a client to use LON-SVR1 as a DNS server.
2. Create several host records for web apps in the Adatum.com domain.
3. Verify replication of new records to LON-SVR1.
4. Use the ping command to locate new records from LON-CL1.

#### ► Task 1: Configure a client to use LON-SVR1 as a DNS server

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open **Control Panel**.
3. Open the **Properties** dialog box for the **Ethernet** adapter.
4. Configure the **preferred DNS server** to be **172.16.0.11**.

#### ► Task 2: Create several host records for web apps in the Adatum.com domain

1. On LON-DC1, open **DNS Manager**.
2. Go to the **Adatum.com** forward lookup zone.
3. Create a new record named **www** with the IP address **172.16.0.200**.
4. Create a new record named **ftp** with IP address **172.16.0.201**.

#### ► Task 3: Verify replication of new records to LON-SVR1

1. On LON-SVR1, open **DNS Manager**.
2. Go to the **Adatum.com** forward lookup zone.
3. Ensure that records **www** and **ftp** display.

 **Note:** If the **www** and **ftp** resource records do not display within several minutes, refresh the Adatum.com zone.

#### ► Task 4: Use the ping command to locate new records from LON-CL1

1. On LON-CL1, open a Command Prompt window.
2. Ping **www.adatum.com**. Ensure that ping resolves this name to **172.16.0.200**.
3. Ping **ftp.adatum.com**, and ensure that it resolves to **172.16.0.201**.

**Results:** After completing this exercise, you should have configured DNS records.

## Exercise 3: Managing the DNS Server Cache

### Scenario

After you changed some host records in zones configured on LON-DC1, you noticed that clients that use LON-SVR1 as their DNS server were still receiving old IP addresses during the name-resolving process. You want to determine which component is caching this data.

The main tasks for this exercise are as follows:

1. Use the ping command to locate an Internet record from LON-CL1.
2. Update an Internet record to point to the LON-DC1 IP address.
3. Examine the content of the DNS cache.
4. Clear the cache, and retry the ping command.

#### ► Task 1: Use the ping command to locate an Internet record from LON-CL1

1. On LON-CL1, in the Command Prompt window, use **ping** to locate **www.contoso.com**.
2. Ensure that the name resolves to an IP address, and then document the IP address.

#### ► Task 2: Update an Internet record to point to the LON-DC1 IP address

1. On LON-DC1, open the **DNS Manager** console.
2. Go to the **contoso.com** forward lookup zone.
3. Change the IP address for the record **www** to **172.16.0.10**.
4. From LON-CL1, ping **www.contoso.com**.

Note that this record is still resolved with the old IP.

#### ► Task 3: Examine the content of the DNS cache

1. On LON-SVR1, in the DNS Manager console, enable **Advanced View**.
2. Browse the content of the **Cached Lookups** container for the **com** namespace, and note the IP address for **www** record.
3. On LON-CL1, at a command prompt, type the following:

```
ipconfig /displaydns
```

4. Examine the cached content and notice the IP address for the **www** record.

#### ► Task 4: Clear the cache, and retry the ping command

1. Clear the cache on the LON-SVR1 DNS server, by using the **Clear-DNSServerCache** cmdlet.
2. Retry the ping to **www.contoso.com** on LON-CL1.

The result still returns the old IP address.

3. Clear the client resolver cache on LON-CL1 by typing the following in the Command Prompt window at a command prompt:

```
ipconfig /flushdns
```

4. On LON-CL1, retry ping to **www.contoso.com**.

The result should work.

**Results:** After completing this exercise, you should have examined the DNS server cache.

### Lab Review Questions

**Question:** Can you install the DNS server role on a server that is not a domain controller? If yes, are there any limitations?

**Question:** What is the most common way to carry out Internet name resolution on a local DNS?

**Question:** How can you browse the content of the DNS resolver cache on a DNS server?

### ► Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state.

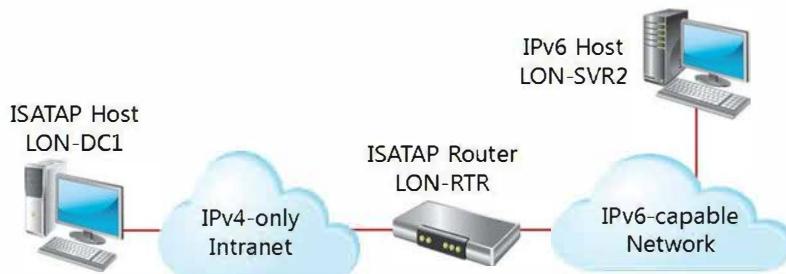
1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-SVR1** and **20410D-LON-CL1**.

# Lab: Implementing IPv6

## Scenario

The IT manager at A. Datum Corporation has been briefed by several program and application vendors about newly added support for IPv6 in their products. A. Datum Corporation does not have IPv6 support currently. However, the IT manager wants you to configure a test lab that uses IPv6. As part of the test lab configuration, you also need to configure ISATAP to allow communication between an IPv4 network and an IPv6 network.

This is the layout of the completed test environment.



**FIGURE 8.1: END RESULT OF THE LAB**

## Objectives

After completing this lab, you should be able to:

- Configure an IPv6 network.
- Configure an ISATAP router.

## Lab Setup

Estimated Time: 45 minutes

|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
|                  |                                                                          |
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-RTR</b><br><b>20410D-LON-SVR2</b> |
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

- On the host computer, start **Hyper-V Manager**.
- In Hyper-V® Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Start**.
- In the Actions pane, click **Connect**.

Wait until the virtual machine starts.

4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20410D-LON-RTR** and **20410D-LON-SVR2**.

## Exercise 1: Configuring an IPv6 Network

### Scenario

For the first step in configuring the test lab, you need to configure LON-DC1 as an IPv4-only node, and LON-SVR2 as an IPv6-only node. You also need to configure LON-RTR to support IPv6 routing by adding a network to an interface on the IPv6 network, and by enabling router advertisements. The router advertisements allow the IPv6 clients on the IPv6 network to obtain the correct IPv6 network automatically through stateless configuration.

The main tasks for this exercise are as follows:

1. Verify IPv4 routing.
2. Disable IPv6 on LON-DC1.
3. Disable IPv4 on LON-SVR2.
4. Configure an IPv6 network on LON-RTR.
5. Verify IPv6 on LON-SVR2.

#### ► Task 1: Verify IPv4 routing

1. On LON-SVR2, open a **Windows PowerShell** prompt.
2. Ping **LON-DC1** to verify that IPv4 is routing through LON-RTR.
3. Use the **ipconfig** command to verify that LON-SVR2 has only a link-local IPv6 address that cannot be routed.
4. Use the **Get-NetIPAddress** cmdlet to view the network configuration and link-local IPv6 address on the **Ethernet** adapter.

#### ► Task 2: Disable IPv6 on LON-DC1

1. On LON-DC1, in Server Manager, click **Local Server**, and then select **172.16.0.10, IPv6 enabled** to open the **Network Connections** dialog box.
2. In the **Network Connections** dialog box, open the **Ethernet Properties** dialog box, and then disable IPv6 for **Ethernet** adapter to make LON-DC1 an IPv4-only host.

#### ► Task 3: Disable IPv4 on LON-SVR2

1. On LON-SVR2, in Server Manager, click **Local Server**, and then select **10.10.0.11, IPv6 enabled** to open the **Network Connections** dialog box.
2. In **Network Connections** dialog box, open the **Ethernet Properties** dialog box, and then disable IPv4 for **Ethernet**, to make LON-SVR2 an IPv6-only host.

### ► Task 4: Configure an IPv6 network on LON-RTR

1. On LON-RTR, open Windows PowerShell.
2. Configure a network address that will be used on the IPv6 network by using the following Windows PowerShell **New-NetRoute** cmdlet to add an IPv6 network on **Ethernet 2** to the local routing table:

```
New-NetRoute -InterfaceAlias "Ethernet 2" -DestinationPrefix 2001:db8:0:1::/64
-Publish Yes
```

3. Allow clients to obtain the IPv6 network address automatically from LON-RTR by using the following **Set-NetIPInterface** cmdlet to enable router advertisements on Ethernet 2:

```
Set-NetIPInterface -InterfaceAlias "Ethernet 2" -AddressFamily IPv6 -Advertising
Enabled
```

4. Use **ipconfig** to verify that Ethernet 2 has an IPv6 address on the **2001:db8:0:1::/64** network.

This address is used for communication on the IPv6-only network.

### ► Task 5: Verify IPv6 on LON-SVR2

- On LON-SVR2, use **ipconfig** to verify that the Ethernet has an IPv6 address on the 2001:db8:0:1::/64 network.

The network address was obtained from the router through stateless configuration.

**Results:** After completing the exercise, you will have configured an IPv6-only network.

## Exercise 2: Configuring an ISATAP Router

### Scenario

After configuring the infrastructure for an IPv4-only network and an IPv6-only network, you need to configure LON-RTR as an ISATAP router to support communication between the IPv4-only nodes and the IPv6-only nodes.

To configure LON-RTR as an ISATAP router, you need to enable the IPv4 interface as the ISATAP router. Then you configure an IPv6 network on the ISATAP interface and enable advertising of the network route that includes that network. ISATAP clients will obtain the IPv6 network automatically from the advertisements.

To enable ISATAP automatically on clients, you need to create an ISATAP host record in DNS. Clients that can resolve this name automatically become ISATAP clients. To allow clients to resolve this name, you must remove ISATAP from the global query block list on the DNS server.

The main tasks for this exercise are as follows:

1. Add an ISATAP host record to DNS.
2. Enable the ISATAP router on LON-RTR.
3. Remove ISATAP from the Global Query Block List.
4. Enable LON-DC1 as an ISATAP client.
5. Test connectivity.

► **Task 1: Add an ISATAP host record to DNS**

1. On LON-DC1, in Server Manager, open the DNS tool.
2. Add an **ISATAP** host record in the Adatum.com domain that resolves to **172.16.0.1**. ISATAP clients resolve this host name to find the ISATAP router.

► **Task 2: Enable the ISATAP router on LON-RTR**

1. On LON-RTR, configure the IP address of the Ethernet adapter as the ISATAP router. Use the following **Set-NetIsatapConfiguration** cmdlet to enable ISATAP:

```
Set-NetIsatapConfiguration -Router 172.16.0.1
```

2. Use the following **Get-NetIPAddress** cmdlet to identify the interface index of the ISATAP interface with 172.16.0.1 in the link-local address:

```
Get-NetIPAddress | Format-Table InterfaceAlias,InterfaceIndex,IPv6Address
```

|                                  |  |
|----------------------------------|--|
| Record the interface index here: |  |
|----------------------------------|--|

3. Use the **Get-NetIPInterface** cmdlet to verify the following on the ISATAP interface:

- Forwarding is enabled
- Advertising is disabled

```
Get-NetIPInterface -InterfaceIndex IndexYouRecorded -PolicyStore ActiveStore | Format-List
```

4. The ISATAP interface for an ISATAP router must have forwarding enabled and advertising enabled. Use the following **Set-NetIPInterface** cmdlet to enable router advertisements on the ISATAP interface:

```
Set-NetIPInterface -InterfaceIndex IndexYouRecorded -Advertising Enabled
```

5. Create a new IPv6 network that will be used for the ISATAP network. Use the following **New-NetRoute** cmdlet to configure a network route for the ISATAP interface:

```
New-NetRoute -InterfaceIndex IndexYouRecorded -DestinationPrefix 2001:db8:0:2::/64 -Publish Yes
```

6. Use the following **Get-NetIPAddress** cmdlet to verify that the ISATAP interface has an IPv6 address on the 2001:db8:0:2::/64 network:

```
Get-NetIPAddress -InterfaceIndex IndexYouRecorded
```

► **Task 3: Remove ISATAP from the Global Query Block List**

1. On LON-DC1, in Windows PowerShell, run the following command:

```
dnscmd /config /globalqueryblocklist wpad
```

2. Restart the DNS service.

3. Ping **isatap.adatum.com** to verify it can be resolved.

The name should resolve, and you should receive four replies from 172.16.0.1.

► **Task 4: Enable LON-DC1 as an ISATAP client**

1. On LON-DC1, use the following **Set-NetIsatapConfiguration** cmdlet to enable ISATAP:

```
Set-NetIsatapConfiguration -State Enabled
```

2. Use **ipconfig** to verify that the Tunnel adapter for ISATAP has an IPv6 address on the 2001:db8:0:2/64 network.

Notice that this address includes the IPv4 address of LON-DC1.

► **Task 5: Test connectivity**

1. On LON-SVR2, use the following **ping** command to test connectivity to the ISATAP address for LON-DC1:

```
ping 2001:db8:0:2:0:5efe:172.16.0.10
```

2. Use the Server Manager to modify the properties of TCP/IPv6 on the Ethernet, and add **2001:db8:0:2:0:5efe:172.16.0.10** as the preferred DNS server.

3. Use the **ping** command to test connectivity to **LON-DC1**.

A ping from LON-DC1 to LON-SVR2 does not respond because the firewall configuration on LON-SVR2 blocks ping requests.

**Results:** After completing this exercise, you will have configured an ISATAP router on LON-RTR to allow communication between an IPv6-only network and an IPv4-only network.

### Lab Review Questions

**Question:** Did you configure IPv6 statically or dynamically in this lab?

**Question:** Why did you not need to configure LON-DC1 with the IPv4 address of the ISATAP router?

► **Prepare for the next module**

After you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-RTR** and **20410D-LON-SVR2**.

# Lab: Implementing Local Storage

## Scenario

Your manager has asked to add disk space to a file server. After creating volumes, your manager has also asked you to resize those volumes based on updated information he has been given. Finally, you need to make data storage redundant by creating a three-way mirrored virtual disk.

## Objectives

After completing this lab, you should be able to:

- Install and configure a new disk.
- Resize volumes.
- Configure a redundant storage space.

## Lab Setup

Estimated Time: 45 minutes

|                  |                                                 |
|------------------|-------------------------------------------------|
|                  |                                                 |
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b> |
| User name        | <b>Adatum\Administrator</b>                     |
| Password         | <b>Pa\$\$w0rd</b>                               |

For this lab, you will use the available virtual machine environment. Before beginning the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20410D-LON-SVR1**.

## Exercise 1: Installing and Configuring a New Disk

### Scenario

The file server in your branch office is low on disk space. You need to add a new disk to the server and create volumes based on specifications provided by your manager.

The main tasks for this exercise are as follows:

1. Initialize a new disk.
2. Create and format two simple volumes on the disk.
3. Verify the drive letter in a File Explorer window.

► **Task 1: Initialize a new disk**

1. Sign in to **LON-SVR1** with the username **Adatum\Administrator** and the password **Pa\$\$w0rd**.
2. In Server Manager, open **Computer Management**, and then access **Disk Management**.
3. Initialize **Disk2**, and then configure it to use **GPT (GUID Partition Table)**.

► **Task 2: Create and format two simple volumes on the disk**

1. In the Computer Management console, on Disk 2, create a **Simple Volume** with the following attributes:
  - o Volume size: **4000 MB**
  - o Drive Letter: **F**
  - o File system: **NTFS**
  - o Volume label: **Volume1**
2. In the Computer Management console, on Disk 2, create a **Simple Volume** with the following attributes:
  - o Volume size: **5000 MB**
  - o Drive Letter: **G**
  - o File system: **ReFS**
  - o Volume label: **Volume2**

► **Task 3: Verify the drive letter in a File Explorer window**

1. Use File Explorer to make sure you can access the following volumes:
  - o **Volume1 (F:)**
  - o **Volume2 (G:)**
2. On Volume2 (G:), create a folder named **Folder1**.

**Results:** After completing this exercise, you should have initialized a new disk, created two simple volumes, and then formatted them. Additionally, you should have verified that the drive letters you assigned are available in File Explorer.

## Exercise 2: Resizing Volumes

### Scenario

After installing the new disk in your file server, your manager contacts you to indicate that the information he gave you was incorrect. He now needs you to resize the volumes, without losing any data.

The main tasks for this exercise are as follows:

1. Shrink Volume1.
2. Extend Volume2.

► **Task 1: Shrink Volume1**

- Use Disk Management to shrink **Volume1 (F:)** to **3000 MB**.

► **Task 2: Extend Volume2**

1. Use Disk Management to extend **Volume2 (G:)** by **1000 MB**.
2. Use File Explorer to verify that the folder **Folder1** is still on drive **G**.

**Results:** After completing this exercise, you should have made one volume smaller and extended another.

## Exercise 3: Configuring a Redundant Storage Space

### Scenario

Your server does not have a hardware-based RAID card, but you have been asked to configure redundant storage. To support this feature, you need to create a storage pool.

After creating the storage pool, you need to create a redundant virtual disk. Because the data is critical, the request for redundant storage specifies that you must use a three-way mirrored volume. Shortly after the volume is in use, a disk fails, and you have to replace it by adding another disk to the storage pool.

The main tasks for this exercise are as follows:

1. Create a storage pool from five disks that are attached to the server.
2. Create a three-way mirrored virtual disk.
3. Copy a file to the volume, and verify that it is visible in File Explorer.
4. Remove a physical drive.
5. Verify that the write.exe file is still accessible.
6. Add a new disk to the storage pool and remove a broken disk.

► **Task 1: Create a storage pool from five disks that are attached to the server**

1. On LON-SVR1, open **Server Manager**.
2. In the left pane, click **File and Storage Services**, and then in the Servers pane, click **Storage Pools**.
3. Create a storage pool with the following settings:
  - Name: **StoragePool1**
  - Physical disks:
    - **PhysicalDisk3**
    - **PhysicalDisk4**
    - **PhysicalDisk5**
    - **PhysicalDisk6**
    - **PhysicalDisk7**

► **Task 2: Create a three-way mirrored virtual disk**

1. On LON-SVR1, in Server Manager, in the VIRTUAL DISKS pane, create a virtual disk with the following settings:
  - Storage pool: **StoragePool1**
  - Name: **Mirrored Disk**
  - Storage Layout: **Mirror**

- Resiliency settings: **Three-way mirror**
  - Provisioning type: **Thin**
  - Virtual disk size: **10 GB**
2. In the New Volume Wizard, create a volume with the following settings:
- Virtual disk: **Mirrored Disk**
  - Drive letter: **H**
  - File system: **ReFS**
  - Volume label: **Mirrored Volume**
- **Task 3: Copy a file to the volume, and verify that it is visible in File Explorer**
1. Open a Command Prompt window.
  2. Type the following command:

```
Copy C:\windows\system32\write.exe H:\
```
  3. Open File Explorer from the taskbar, and then access **Mirrored Volume (H:)**. You should see write.exe in the file list.
- **Task 4: Remove a physical drive**
- On the host computer, in Hyper-V Manager, in the Virtual Machines pane, change the **20410D-LON-SVR1** settings to the following:
    - Remove the hard drive that begins with **20410D-LON-SVR1-Disk5**.
- **Task 5: Verify that the write.exe file is still accessible**
1. Switch to LON-SVR1.
  2. Open File Explorer, and then browse to **H:\write.exe** to ensure access to the file is still available.
  3. In Server Manager, in the STORAGE POOLS pane, on the menu bar, click the **Refresh “Storage Pools”** button.  
Notice the warning that is visible next to **Mirrored Disk**.
  4. Open the **Mirrored Disk Properties** dialog box, and then access the Health pane.  
Notice that the Health Status indicates a Warning. The Operational Status should indicate **Incomplete, Unknown, or Degraded**.
- **Task 6: Add a new disk to the storage pool and remove a broken disk**
1. On LON-SVR1, in Server Manager, in the STORAGE POOLS pane, on the menu bar, click the **Refresh “Storage Pools”** button.
  2. In the STORAGE POOLS pane, right-click **StoragePool1**, click **Add Physical Disk**, and then click **PhysicalDisk8 (LON-SVR1)**.
  3. Open Windows PowerShell, and then run the following commands to remove the disconnected disk:
    - a. **Get-PhysicalDisk**  
Note the **FriendlyName** for the disk that shows an **OperationalStatus of Lost Communication**.
    - b. **\$Disk = Get-PhysicalDisk -FriendlyName diskname**  
Replace *diskname* with the name of the disk that you noted previously.

- c. **Remove-PhysicalDisk -PhysicalDisks \$disk -StoragePoolFriendlyName StoragePool1**
4. If you get a warning that the disk cannot be removed, wait five minutes, and then run the last command again. It can take some time for the mirrored disk to resynchronize after a disk is removed and another is added. If you cannot remove the disk after five minutes, restart LON-SVR1, sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**, and then repeat step 3.
  5. In Server Manager, refresh the storage pools view to see the warnings disappear.

**Results:** After completing this exercise, you should have created a storage pool and added five disks to it. Additionally, you should have created a three-way mirrored, thinly provisioned virtual disk from the storage pool; copied a file to the new volume; and then verified that it is accessible. Next, after removing a physical drive, you should have verified that the virtual disk was still available and that you could access it. Finally, you should have added another physical disk to the storage pool.

### Lab Review Questions

**Question:** At a minimum, how many disks must you add to a storage pool to create a three-way mirrored virtual disk?

**Question:** You have a USB-attached disk, four SAS disks, and one SATA disk that are attached to a Windows Server 2012 server. You want to provide a single volume to your users that they can use for file storage. What would you use?

### ► Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-SVR1**.

# Lab: Implementing File and Print Services

## Scenario

Your manager has recently asked you to configure file and print services for the branch office. This requires you to configure a new shared folder that will have subfolders for multiple departments, configure shadow copies on the file servers, and configure a printer pool.

Additionally, many users want to be able to work on their data files while they are out of the office and working on devices such as on Windows RT-based tablets. You must ensure that these users are able to access their work-related data files from other locations when offline.

## Objectives

After performing this lab you should be able to:

- Create and configure a file share.
- Configure shadow copies.
- Enable and configure Work Folders.
- Create and configure a printer pool.

## Lab Setup

Estimated Time: 60 minutes

| Virtual machines | <b>20410D-LON-CL1</b><br><b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b> |
|------------------|--------------------------------------------------------------------------|
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**.  
Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20410D-LON-SVR1**.
6. Repeat steps 2 and 3 for **20410D-LON-CL1**. Do not sign in to LON-CL1 until directed to do so.

## Exercise 1: Creating and Configuring a File Share

### Scenario

Your manager has asked you to create a new shared folder, which all departments will use. There will be a single file share, with separate folders, for each department. To ensure that users see only the folders and files to which they have access, you need to set the file permissions on the departmental folders and enable access-based enumeration on the share.

There have been problems in other branch offices with multiple versions of files when offline files were used for shared data structures. To avoid these conflicts, you need to disable Offline Files for this share.

The main tasks for this exercise are as follows:

1. Create the folder structure for the new share.
2. Configure file permissions on the folder structure.
3. Create the shared folder.
4. Test access to the shared folder.
5. Enable access-based enumeration.
6. Test access to the share.
7. Disable offline files for the share.

#### ► Task 1: Create the folder structure for the new share

- On LON-SVR1, open File Explorer and create the following folders:
  - **E:\Data**
  - **E:\Data\Development**
  - **E:\Data\Marketing**

#### ► Task 2: Configure file permissions on the folder structure

1. In File Explorer, block the file permissions inheritance for **E:\Data\Development** and **E:\Data\Marketing**, and when prompted, convert inherited permissions into explicit permissions.
2. In File Explorer, remove permissions for **LON-SVR1\Users** on **E:\Data\Development** and **E:\Data\Marketing**.
3. In File Explorer, add the following file permissions for the folder structure.

| Folder              | Permissions                |
|---------------------|----------------------------|
| E:\Data             | No change                  |
| E:\Data\Development | Modify: Adatum\Development |
| E:\Data\Marketing   | Modify: Adatum\Marketing   |

#### ► Task 3: Create the shared folder

1. In File Explorer, share the **E:\Data** folder.
2. Assign the following permissions to the shared folder:
  - Change: **Adatum\Authenticated Users**

► **Task 4: Test access to the shared folder**

1. Sign in to LON-CL1 as **Adatum\Bernard** with the password **Pa\$\$w0rd**.

Notice that Bernard is a member of the Development group.

2. Open File Explorer.
3. Navigate to **\LON-SVR1\Data**.
4. Attempt to open the **Development** and **Marketing** folders.

Bernard should have access to the Development folder. However, although Bernard can still see the Marketing folder, he does not have access to its contents.

5. Sign out of LON-CL1.

► **Task 5: Enable access-based enumeration**

1. Switch to LON-SVR1.
2. Open Server Manager.
3. Click **File and Storage Services**.
4. Click **Shares**.
5. Open the **Properties** dialog box for the **Data** share, and then on the **Settings** page, enable **Access-based enumeration**.

► **Task 6: Test access to the share**

1. Sign in to LON-CL1 as **Adatum\Bernard** with the password **Pa\$\$w0rd**.

2. Open File Explorer, and then navigate to **\LON-SVR1\Data**.

Bernard can now view only the Development folder, the folder for which he has permissions.

3. Open the **Development** folder to confirm access.
4. Sign out of LON-CL1.

► **Task 7: Disable offline files for the share**

1. Switch to LON-SVR1.
2. Open File Explorer.
3. Navigate to drive **E**.
4. Open the **Properties** dialog box for the Data folder, and then disable offline file caching.

**Results:** After completing this exercise, you will have created a new shared folder for use by multiple departments.

## Exercise 2: Configuring Shadow Copies

### Scenario

A. Datum Corporation stores daily backups offsite for disaster recovery. Every morning, the backup from the previous night is taken offsite. To recover a file from backup, the backup tapes need to be shipped back onsite so the overall time to recover a file from backup can be a day or more.

Your manager has asked you to enable shadow copies on the file server so you can restore recently modified or deleted files without using a backup tape. Because the data in this branch office changes frequently, you are going to create a shadow copy once per hour.

The main tasks for this exercise are as follows:

1. Configure shadow copies for the file share.
2. Create multiple shadow copies of a file.
3. Recover a deleted file from a shadow copy.

#### ► Task 1: Configure shadow copies for the file share

1. On LON-SVR1.
2. Open File Explorer.
3. Navigate to drive E, right-click **Allfiles (E:)**, and then click **Configure Shadow Copies**.
4. Enable **Shadow Copies** for drive E.
5. Configure the settings to schedule hourly shadow copies for drive E.

#### ► Task 2: Create multiple shadow copies of a file

1. On LON-SVR1, switch to **File Explorer**, and then navigate to **E:\Data\Development**.
2. Create a new text file named **Report.txt**.
3. Switch back to the **Allfiles (E:) Properties** dialog box. It should be opened on the **Shadow Copies** tab. Click **Create Now**.

#### ► Task 3: Recover a deleted file from a shadow copy

1. On LON-SVR1, switch back to File Explorer.
2. Delete the **Report.txt** file.
3. Open the **Properties** dialog box for **E:\Data\Development**, and then click the **Previous Versions** tab.
4. Open the most recent version of the **Development** folder, and then copy the **Report.txt** file.
5. Paste the file back into the **Development** folder.
6. Close File Explorer and all open windows.

**Results:** After completing this exercise, you will have enabled shadow copies on the file server.

## Exercise 3: Enabling and Configuring Work Folders

### Scenario

You must enable and configure Work Folders to support the requirements of your users. Domain users have their own Windows 8.1 and Windows RT 8.1 tablet devices and want access to their work data from anywhere. When they return to work, they want to be able to synchronize these data files. You will use Group Policy to force the Work Folders settings to users and test the settings.

The main tasks for this exercise are as follows:

1. Install the Work Folders role service.
2. Create a sync share on the file server.
3. Automate settings for users by using Group Policy.
4. Test synchronization.

#### ► Task 1: Install the Work Folders role service

- On LON-SVR1, use Windows PowerShell to run the following command to install the **Work Folders** role service:

**Add-WindowsFeature FS-SyncShareService**

Note that the name of the feature is case-sensitive.

#### ► Task 2: Create a sync share on the file server

1. On LON-SVR1, use Windows PowerShell to run the following command to create the sync share named **Corp**:

**New-SyncShare Corp –path C:\CorpData –User "Adatum\Domain Users"**

2. Open Server Manager, and then view the Work Folders to ensure the sync share was created.

#### ► Task 3: Automate settings for users by using Group Policy

1. On LON-DC1, create a GPO named **Work Folders**, and then link it to the **Adatum.com** domain.
2. Edit the **Work Folders** GPO, as follows:

- Navigate to **User Configuration\Policies\Administrative Templates\Windows Components\Work Folders**.
- Enable the **Specify Work Folders** settings policy, and then specify the Work Folders URL as **http://lon-svr1.Adatum.com**.
- Select **Force automatic setup** to force automatic setup.

3. Close all open windows.

#### ► Task 4: Test synchronization

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Use File Explorer to navigate to **C:\Labfiles\Mod10**, and then double-click **WorkFolders.bat**.  
This adds a registry entry to allow unsecured connections to the work folders.
3. Sign out of LON-CL1.
4. Sign in to LON-CL1 as **Adatum\Administrator**.

5. In File Explorer, open Work Folders, and then create a new text document named **TestFile2**.
6. Switch to LON-SVR1, and then use File Explorer to open **C:\CorpData\Administrator**.  
Ensure the new text file you created exists.

**Results:** After completing this exercise, you will have installed the Work Folders role service, created a sync share, and created a GPO to deliver the settings to the users automatically. Additionally, you will have tested the settings.

## Exercise 4: Creating and Configuring a Printer Pool

### Scenario

Your manager has asked you to create a new shared printer for your branch office. However, instead of creating the shared printer on the local server in the branch office, he has asked you to create the shared printer in the head office and use Branch Office Direct Printing. This allows people in the head office to manage the printer, but prevents print jobs from traversing WAN links.

To ensure high availability of this printer, you need to format it as a pooled printer. Two physical print devices of the same model have been installed in the branch office for this purpose.

The main tasks for this exercise are as follows:

1. Install the Print and Document Services server role.
2. Install a printer.
3. Configure printer pooling.
4. Install a printer on a client computer.

#### ► Task 1: Install the Print and Document Services server role

1. On LON-SVR1, open **Server Manager**.
2. Install the Print and Document Services role, and then accept the default settings.

#### ► Task 2: Install a printer

1. On LON-SVR1, use the Print Management console to install a printer with following parameters:
  - o IP Address: **172.16.0.200**
  - o Driver: **Microsoft XPS Class Driver**
  - o Name: **Branch Office Printer**
2. Share the printer.
3. List the printer in AD DS.
4. Enable Branch Office Direct Printing.

### ► Task 3: Configure printer pooling

1. On LON-SVR1, in the Print Management console, create a new port with the following configuration:
  - o Type: **Standard TCP/IP port**
  - o IP Address: **172.16.0.201**
  - o Connection: **Generic Network Card**
2. Open the **Branch Office Printer Properties** dialog box, and then on the **Ports** tab, enable printer pooling.
3. Select port **172.16.0.201** as the second port.

### ► Task 4: Install a printer on a client computer

- On LON-CL1, add a printer by selecting the **Branch Office Printer on LON-SVR1** printer.

**Results:** After completing this exercise, you will have installed the Print and Document Services server role and installed a printer with printer pooling.

### Lab Review Questions

**Question:** How does implementing access-based enumeration benefit the users of the Data shared folder in this lab?

**Question:** Is there another way you could recover the file in the shadow copy exercise? What benefit do shadow copies provide in comparison?

**Question:** In Exercise 3, how could you configure Branch Office Direct Printing if you were in a remote location and did not have access to the Windows Server 2012 GUI for the print server?

### ► Prepare for the next module

After you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-SVR1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-CL1** and **20410D-LON-DC1**.

# Lab: Implementing Group Policy

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, England. An IT office and a data center are located in London to support the London location and other locations. A. Datum has recently deployed a Windows Server 2012 infrastructure with Windows 8 clients.

In your role as a member of the server support team, you help to deploy and configure new servers and services into the existing infrastructure based on the instructions given to you by your IT manager.

Your manager has asked you to create a central store for ADMX files to ensure that everyone can edit GPOs that have been created with customized ADMX files. You also need to create a starter GPO that includes Internet Explorer settings, and then configure a GPO that applies GPO settings for the Marketing department and the IT department.

## Objectives

After completing this lab, you should be able to:

- Configure a central store.
- Create GPOs.

## Lab Setup

Estimated Time: 45 minutes

| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-CL1</b> |
|------------------|------------------------------------------------|
| User name        | <b>Adatum\Administrator</b>                    |
| Password         | <b>Pa\$\$w0rd</b>                              |

## Lab Setup Instructions

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

- On the host computer, start **Hyper-V Manager**.
- In Hyper-V® Manager, click **20410D-LON-DC1**. In the Actions pane, click **Start**.
- In the Actions pane, click **Connect**. Wait until the virtual machine starts.
- Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
- Repeat steps 2 and 3 for **20410D-LON-CL1**. Do not sign in until directed to do so.

## Exercise 1: Configuring a central store

### Scenario

A. Datum recently implemented a customized ADMX template to configure a program. A colleague obtained the ADMX files from the vendor before creating the GPO with the configurations settings. The settings were applied to the program as expected.

After implementation, you noticed that you are unable to modify the program's settings in the GPO from any location other than the workstation that was used originally by your colleague. To resolve this issue, your manager has asked you to create a central store for administrative templates. After you create the central store, your colleague will copy the vendor ADMX template from the workstation into the central store.

The main tasks for this exercise are as follows:

1. View the location of administrative templates in a GPO.
2. Create a central store.
3. Copy administrative templates to the central store.
4. Verify the administrative template location in GPMC.

#### ► Task 1: View the location of administrative templates in a GPO

1. Sign in to LON-DC1 as **Administrator** with the password **Pa\$\$w0rd**.
2. Start the Group Policy Management Console.
3. In the **Group Policy Object** folder, open the **Default Domain Policy**, and then view the location of the administrative templates.

#### ► Task 2: Create a central store

1. Open File Explorer, and then browse to **C:\Windows\SYSVOL\sysvol\Adatum.com\Policies**.
2. Create a folder to use for the central store, with the name **PolicyDefinitions**.

#### ► Task 3: Copy administrative templates to the central store

- Copy the contents of the default PolicyDefinitions folder located at **C:\Windows\PolicyDefinitions** to the new PolicyDefinitions folder located at **C:\Windows\SYSVOL\sysvol\Adatum.com\Policies**.

#### ► Task 4: Verify the administrative template location in GPMC

1. In the Group Policy Management Editor window, verify that the ADMX files in the **Administrative Templates** folder have been retrieved from the central store.
2. Close the Group Policy Management Editor window.

**Results:** After completing this exercise, you should have configured a central store.

## Exercise 2: Creating GPOs

### Scenario

After a recent meeting of the IT Policy committee, management has decided that A. Datum will use Group Policy to restrict user access to the General page of Internet Explorer.

Your manager has asked you to create a starter GPO that can be used for all departments, with default restriction settings for Internet Explorer. You then need to create the GPOs that will deliver the settings for members of all departments except for the IT department.

The main tasks for this exercise are as follows:

1. Create a Windows Internet Explorer Restriction default starter GPO.
2. Configure the Internet Explorer Restriction starter GPO.
3. Create an Internet Explorer Restrictions GPO from the Internet Explorer Restrictions starter GPO.
4. Test the GPO for Domain Users.
5. Use security filtering to exempt the IT Department from the Internet Explorer Restrictions policy.
6. Test the GPO app for IT department users.
7. Test the Application of the GPO for other domain users.

#### ► Task 1: Create a Windows Internet Explorer Restriction default starter GPO

1. Open the GPMC, and then create a starter GPO named **Internet Explorer Restrictions**.
2. Type a comment that states **This GPO disables the General page in Internet Options**.

#### ► Task 2: Configure the Internet Explorer Restriction starter GPO

1. Configure the starter GPO to disable the **General** page of Internet Options, and then name it **Internet Explorer Restrictions**.

**Hint:** To select all the content, click in the details pane, and then press CTRL+A.

2. Close the Group Policy Management Editor window.

#### ► Task 3: Create an Internet Explorer Restrictions GPO from the Internet Explorer Restrictions starter GPO

- Create a new GPO named **IE Restrictions** that is based on the Internet Explorer Restrictions starter GPO, and then link it to the **Adatum.com** domain.

#### ► Task 4: Test the GPO for Domain Users

1. Sign in to LON-CL1 as **Adatum\Brad** with the password **Pa\$\$w0rd**.
2. Open Control Panel.
3. Attempt to change your home page.
4. Open **Internet Options** to verify that the **General** tab has been restricted.
5. Sign out from LON-CL1.

#### ► Task 5: Use security filtering to exempt the IT Department from the Internet Explorer Restrictions policy

1. On LON-DC1, open the GPMC.
2. Configure security filtering on the **Internet Explorer Restrictions** policy to deny access to the IT department.

► **Task 6: Test the GPO app for IT department users**

1. Switch to LON-CL1.
2. Sign in to LON-CL1 as **Brad** with the password **Pa\$\$w0rd**.
3. Open Control Panel.
4. Attempt to change your home page. Verify that the **Internet Properties** dialog box opens to the **General** tab, and all settings are available.
5. Sign out from LON-CL1.

► **Task 7: Test the Application of the GPO for other domain users**

1. Sign in to LON-CL1 as **Boris** with the password **Pa\$\$w0rd**.
2. Open Control Panel.
3. Attempt to change your home page.
4. Open **Internet Options** to verify that the **General** tab has been restricted.
5. Sign out from LON-CL1.

**Results:** After completing this lab, you should have created a GPO.

### Lab Review Questions

**Question:** What is the difference between ADMX and ADML files?

**Question:** The Sales Managers group should be exempted from the desktop lockdown policy that is being applied to the entire Sales OU. All sales user accounts and sales groups reside in the Sales OU. How would you exempt the Sales Managers group?

**Question:** What Windows command can you use to force the immediate refresh of all GPOs on a client computer?

► **Prepare for the next module**

After you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-CL1**.

# Lab A: Increasing Security for Server Resources

## Scenario

Your manager has given you some security-related settings that need to be implemented on all member servers. You also need to implement file system auditing for a file share used by the Marketing department. Finally, you need to implement auditing for domain logons.

## Objectives

After completing this lab, you should be able to:

- Use Group Policy to secure member servers.
- Audit who is accessing specific files.
- Audit domain logons.

## Lab Setup

Estimated Time: 50 minutes

| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b><br><b>20410D-LON-SVR2</b><br><b>20410D-LON-CL1</b> |
|------------------|----------------------------------------------------------------------------------------------------|
| User name        | <b>Adatum\Administrator</b>                                                                        |
| Password         | <b>Pa\$\$w0rd</b>                                                                                  |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**.  
Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20410D-LON-SVR1** and **20410D-LON-SVR2**.
6. Repeat steps 2 and 3 for **20410D-LON-CL1**. Do not sign in to LON-CL1 until directed to do so.

## Exercise 1: Using Group Policy to Secure Member Servers

### Scenario

A. Datum Corporation uses the Computer Administrators group to provide administrators with permissions to administer member servers. As part of the installation process for a new server, the Computer Administrators group from the domain is added to the local Administrators group on the new server. Recently, this important step was missed when configuring several new member servers.

To ensure that the Computer Administrators group is always given permission to manage member servers, your manager has asked you to create a GPO that sets the membership of the local Administrators group on member servers to include Computer Server Administrators. This GPO also needs to enable Admin Approval Mode for UAC.

The main tasks for this exercise are as follows:

1. Create a Member Servers organizational unit (OU) and move servers into it.
2. Create a Server Administrators group.
3. Create a Member Server Security Settings Group Policy Object (GPO) and link it to the Member Servers OU.
4. Configure group membership for local administrators to include Server Administrators and Domain Admins.
5. Verify that Computer Administrators has been added to the local Administrators group.
6. Modify the Member Server Security Settings GPO to remove Users from Allow Log On Locally.
7. Modify the Member Server Security Settings GPO to enable User Account Control: Admin Approval Mode for the Built-in Administrator account.
8. Verify that a nonadministrative user cannot sign in to a member server.

► **Task 1: Create a Member Servers organizational unit (OU) and move servers into it**

1. On LON-DC1, open **Active Directory Users and Computers**.
2. Create a new OU named **Member Servers OU**.
3. Move servers **LON-SVR1** and **LON-SVR2** to **Member Servers OU**.

► **Task 2: Create a Server Administrators group**

- On LON-DC1, in **Member Servers OU**, create a new global security group called **Server Administrators**.

► **Task 3: Create a Member Server Security Settings Group Policy Object (GPO) and link it to the Member Servers OU**

1. On LON-DC1, open the Group Policy Management Console.
2. In the Group Policy Management Console, in the Group Policy Objects container, create a new GPO with a name **Member Server Security Settings**.
3. In the Group Policy Management Console, link the **Member Server Security Settings** to **Member Servers OU**.

► **Task 4: Configure group membership for local administrators to include Server Administrators and Domain Admins**

1. On LON-DC1, for the Default Domain Policy, open the Group Policy Management Editor window.
2. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Restricted Groups**.
3. Add the **Server Administrators** and **Domain Admins** groups to the **Administrators** group.
4. Close the Group Policy Management Editor window.

► **Task 5: Verify that Computer Administrators has been added to the local Administrators group**

1. Switch to LON-SVR1.
2. Open Windows PowerShell®, and at the Windows PowerShell prompt, type following command:

```
Gpupdate /force
```

3. Open **Server Manager**, open the Computer Management console, and then expand **Local Users and Groups**.
4. Confirm that the **Administrators** group contains both **ADATUM\Domain Admins** and **ADATUM\Server Administrators** as members.
5. Close the Computer Management console.

► **Task 6: Modify the Member Server Security Settings GPO to remove Users from Allow Log On Locally**

1. On LON-DC1, in the Group Policy Management Console, edit the **Member Server Security Settings** GPO.
2. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\User Rights Assignment**.
3. Configure **Allow log on locally** for **Domain Admins** and **Administrators** security groups.

► **Task 7: Modify the Member Server Security Settings GPO to enable User Account Control: Admin Approval Mode for the Built-in Administrator account**

1. On LON-DC1, in the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options**.
2. Enable **User Account Control: Admin Approval Mode for the Built-in Administrator account**.
3. Close the Group Policy Management Editor window.

► **Task 8: Verify that a nonadministrative user cannot sign in to a member server**

1. Switch to LON-SVR1.
2. Open a Windows PowerShell window, and at the Windows PowerShell prompt, type following command:

```
Gpupdate /force
```

3. Sign out from LON-SVR1.
4. Try to sign in to LON-SVR1 as **Adatum\Adam** with the password **Pa\$\$w0rd**.

Verify that you cannot sign in to LON-SVR1.

5. To prepare for the next exercise, sign out of LON-SVR1, and then sign back in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

**Results:** After completing this exercise, you will have used Group Policy to secure member servers.

## Exercise 2: Auditing File System Access

### Scenario

The manager of the Marketing department has concerns that there is no way to track who is accessing files that are on the departmental file share. Your manager has explained that only users with permissions are allowed to access the files. However, the manager of the Marketing department wants to try recording who is accessing specific files.

Your manager has asked you to enable auditing for the file system that is on the Marketing department file share, and to review the results with the manager of the Marketing department.

The main tasks for this exercise are as follows:

1. Modify the Member Server Security Settings GPO to enable object access auditing.
2. Create and share a folder.
3. Enable auditing on the Marketing folder for Domain Users.
4. Create a new file in the file share from LON-CL1.
5. View the results in the security log on the domain controller.

### ► Task 1: Modify the Member Server Security Settings GPO to enable object access auditing

1. Switch to LON-DC1.
2. In the Group Policy Management Console, edit the **Member Server Security Settings** GPO.
3. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy**.
4. Enable **Audit object access** with both **Success** and **Failure** settings.
5. Sign out of LON-DC1.

### ► Task 2: Create and share a folder

1. Switch to LON-SVR1.
2. On LON-SVR1, on drive C, create a new folder with the name **Marketing**.
3. Configure the Marketing folder with Read/Write sharing permissions for user **Adam**.

### ► Task 3: Enable auditing on the Marketing folder for Domain Users

1. On LON-SVR1, in the Local Disk (C:) window, configure auditing on the **Marketing** folder, with the following settings:
  - o Select a principal: **Domain Users**
  - o Type: **All**
  - o Permission: **Read & execute, List folder content, Read, Write**
  - o Leave other settings with their default values

2. Refresh Group Policy by typing the following command at the Windows PowerShell prompt:

```
gpupdate /force
```

► **Task 4: Create a new file in the file share from LON-CL1**

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open the Command Prompt window, and then type the following command:

```
gpupdate /force
```

3. Close the Command Prompt window.
4. Sign out from LON-CL1, and then sign in again as **Adatum\Adam** with the password **Pa\$\$w0rd**.
5. Open the **Marketing** folder on LON-SVR1, by using the following Universal Naming Convention (UNC) path: **\LON-SVR1\Marketing**.
6. Create a text document with a name **Employees**.
7. Sign out from LON-CL1.

► **Task 5: View the results in the security log on the domain controller**

1. Switch to LON-SVR1, and then start **Event Viewer**.
2. In the Event Viewer window, expand **Windows Logs**, and then open **Security**.
3. Verify that following event and information is displayed:
  - Source: **Microsoft Windows Security Auditing**
  - Event ID: **4663**
  - Task category: **File System**
  - An attempt was made to access an object

**Results:** After completing this exercise, you will have enabled file system access auditing.

## Exercise 3: Auditing Domain Logons

### Scenario

After a security review, the IT policy committee has decided to begin tracking all user logons to the domain. Your manager has asked you to enable auditing of domain logons and verify that they are working.

The main tasks for this exercise are as follows:

1. Modify the Default Domain Policy GPO.
2. Run **gpupdate**.
3. Sign in to LON-CL1 with an incorrect password.
4. Review event logs on LON-DC1.
5. Sign in to LON-CL1 with the correct password.
6. Review event logs on LON-DC1.

► **Task 1: Modify the Default Domain Policy GPO**

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-DC1, start **Server Manager**, and then from Server Manager, start **GPMC**.
3. On LON-DC1, in the Group Policy Management Console, edit the **Default Domain Policy** GPO.
4. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Audit Policy**.
5. Enable **Audit account logon events** with both **Success** and **Failure** settings.
6. Update Group Policy by using the **gpupdate /force** command.

► **Task 2: Run gpupdate**

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open the Command Prompt window, and then type the following command:

```
gpupdate /force
```

3. Close the Command Prompt window, and then sign out from LON-CL1.

► **Task 3: Sign in to LON-CL1 with an incorrect password**

- Sign in to LON-CL1 as **Adatum\Adam** with the password **password**.

This password is intentionally incorrect to generate a security-log entry that shows that an unsuccessful sign-in attempt has been made.

► **Task 4: Review event logs on LON-DC1**

1. On LON-DC1, start **Event Viewer**.
2. In the Event Viewer window, expand **Windows Logs**, and then click **Security**.
3. Review the event logs for the following message: "Event ID 4771 Kerberos pre-authentication failed. Account Information: Security ID: ADATUM\Adam".

► **Task 5: Sign in to LON-CL1 with the correct password**

1. Sign in to LON-CL1 as **Adatum\Adam** with the password **Pa\$\$w0rd**.

This password is correct, and you should be able to sign in successfully as **Adam**.

2. Sign out of LON-CL1.

► **Task 6: Review event logs on LON-DC1**

1. On LON-DC1, start **Event Viewer**.
2. In the Event Viewer window, expand **Windows Logs**, and then click **Security**.
3. Review the event logs for the following message: "Event ID 4624 An account was successfully logged on. New Logon: Security ID: ADATUM\Adam".

**Results:** After completing this exercise, you will have enabled domain logon auditing.

### Lab Review Questions

**Question:** What happens if you configure the Computer Administrators group, but not the Domain Admins group, to be a member of the Local Administrators group on all of a domain's computers?

**Question:** Why do you need to restrict local logon to some computers?

**Question:** What happens when an unauthorized user tries to access a folder that has auditing enabled for both successful and unsuccessful access attempts?

**Question:** What happens when you configure auditing for domain logons for both successful and unsuccessful logon attempts?

#### ► Prepare for the next lab

- To prepare for the next lab, leave the virtual machines running.

## Lab B: Configuring AppLocker and Windows Firewall

### Scenario

Your manager has asked you to implement AppLocker to restrict nonstandard applications from running. He also has asked you to create new Windows Firewall rules for any member servers running web-based applications.

### Objectives

After completing this lab, you should be able to:

- Configure AppLocker Policies.
- Configure Windows Firewall.

### Lab Setup

Estimated Time: 60 minutes

|                  |                                                                          |
|------------------|--------------------------------------------------------------------------|
|                  |                                                                          |
| Virtual machines | <b>20410D-LON-DC1</b><br><b>20410D-LON-SVR1</b><br><b>20410D-LON-CL1</b> |
| User name        | <b>Adatum\Administrator</b>                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                        |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In Hyper-V Manager, click **20410D-LON-DC1**, and then in the Actions pane, click **Connect**.  
Wait until the virtual machine starts.
3. If needed, sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
4. Repeat steps 2 and 3 for **20410D-LON-SVR1** and **20410D-LON-CL1**.

### Exercise 1: Configuring AppLocker Policies

#### Scenario

Your manager has asked you to configure new AppLocker policies to control the use of applications on user desktops. The new configuration should allow applications to be run only from approved locations. All users must be able to run applications from C:\Windows and C:\Program Files.

You also need to add an exception to run a custom-developed application that resides in a nonstandard location.

The first stage of the implementation records from which locations applications are being run now. The second stage of implementation prevents unauthorized applications from running.

The main tasks for this exercise are as follows:

1. Create an OU for client computers.
2. Move LON-CL1 to the Client Computers OU.
3. Create a Software Control GPO and link it to the Client Computers OU.
4. Run gpupdate.
5. Run app1.bat in the C:\CustomApp folder.
6. View AppLocker events in an event log.
7. Create a rule that allows software to run from a specific location.
8. Modify the Software Control GPO to enforce rules.
9. Verify that an application can still be run.
10. Verify that an application cannot be run.

► **Task 1: Create an OU for client computers**

1. Switch to LON-DC1.
2. Open Active Directory Users and Computers.
3. Create new OU called **Client Computers**.

► **Task 2: Move LON-CL1 to the Client Computers OU**

- On LON-DC1, in Active Directory Users and Computers, move **LON-CL1** to the **Client Computers** OU.

► **Task 3: Create a Software Control GPO and link it to the Client Computers OU**

1. On LON-DC1, open the Group Policy Management Console.
2. In the Group Policy Management Console, in the Group Policy Objects container, create a new GPO named **Software Control**.
3. For the Software Control GPO, open the Group Policy Management Editor window.
4. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker**.
5. Create default rules for the following:
  - **Executable Rules**
  - **Windows Installer Rules**
  - **Script Rules**
  - **Packaged app Rules**
6. Configure rule enforcement with the Audit only option for the following:
  - **Executable Rules**
  - **Windows Installer Rules**
  - **Script Rules**
  - **Packaged app Rules**
7. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings**.

8. Click **System Services**, and then double-click **Application Identity**.
9. In the **Application Identity Properties** dialog box, click **Define this policy setting**.
10. Under **Select service startup mode**, click **Automatic**, and then click **OK**.
11. Close the Group Policy Management Editor window.
12. In the Group Policy Management Console, link the **Software Control** GPO to the **Client Computers** OU.

► **Task 4: Run gpupdate**

1. Switch to LON-CL1.
2. Open the Command Prompt window, and then type the following command:

```
gpupdate /force
```

3. Close the Command Prompt window, and then restart LON-CL1.

► **Task 5: Run app1.bat in the C:\CustomApp folder**

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. At the command prompt, type the following command, and then press Enter:

```
gpresult /R
```

Review the result of the command, and ensure that Software Control is displayed under Computer Settings, Applied Group Policy Objects.

3. If Software Control is not displayed, restart LON-CL1, and then repeat steps 1 and 2.
4. At the command prompt, type the following command, and then press Enter:

```
C:\CustomApp\app1.bat
```

► **Task 6: View AppLocker events in an event log**

1. On LON-CL1, start **Event Viewer**.
2. In the Event Viewer window, browse to **Application and Services Logs\Microsoft\Windows\AppLocker**, and then review the events.
3. Click **MSI and Scripts**, and then review event log 8005 that contains the following text:  
**%OSDRIVE%\CUSTOMAPP\APP1.BAT was allowed to run.**

If no events are displayed, ensure that the Application Identity service has started, and then try again.

► **Task 7: Create a rule that allows software to run from a specific location**

1. On LON-DC1, edit the **Software Control** GPO.
2. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker**.
3. Create a new script rule with the following configuration:
  - o Permissions: **Allow**
  - o Conditions: **Path**
  - o Path: **%OSDRIVE%\CustomApp\app1.bat**
  - o Name and Description: **Custom Application Rule**

► **Task 8: Modify the Software Control GPO to enforce rules**

1. Use the **Enforce rules** option to configure rule enforcement for the following:
  - **Executable Rules**
  - **Windows Installer Rules**
  - **Script Rules**
  - **Packaged app Rules**
2. Close the Group Policy Management Editor window.

► **Task 9: Verify that an application can still be run**

1. Switch to LON-CL1.
2. Open the Command Prompt window, and then type the following command:

```
gpupdate /force
```

3. Close the Command Prompt window, and then restart LON-CL1.
4. Sign in to LON-CL1 as **Adatum\Tony** with the password **Pa\$\$w0rd**.
5. Open the Command Prompt window, and then verify that you can run the **app1.bat** application, which is located in the C:\CustomApp folder.

► **Task 10: Verify that an application cannot be run**

1. On LON-CL1, from the CustomApp folder, copy **app1.bat** to the **Documents** folder.
2. Verify that application cannot be run from the **Documents** folder, and that the following message appears: "This program is blocked by Group Policy. For more information, contact your system administrator."

**Results:** After completing this exercise, you will have configured AppLocker policies for all users whose computer accounts are located in the Client Computers OU. The policies you configured should allow these users to run applications that are located in the folders C:\Windows and C:\Program Files, and run the custom-developed application app1.bat in the C:\CustomApp folder.

## Exercise 2: Configuring Windows Firewall

### Scenario

Your manager has asked you to configure Windows Firewall rules for a set of new application servers. These application servers have a web-based program that is listening on a nonstandard port. You need to configure Windows Firewall to allow network communication through this port. You will use security filtering to ensure that the new Windows Firewall rules apply only to the application servers.

The main tasks for this exercise are as follows:

1. Create a group named Application Servers.
2. Add LON-SVR1 as a group member.
3. Create a new Application Servers GPO.
4. Link the Application Servers GPO to the Member Servers OU.
5. Use security filtering to limit the Application Server GPO to members of Application Server group.

6. Run gpupdate on LON-SVR1.
7. View the firewall rules on LON-SVR1.

► **Task 1: Create a group named Application Servers**

- On LON-DC1, in Active Directory Users and Computers, in the Member Servers OU, create a new global security group named **Application Servers**.

► **Task 2: Add LON-SVR1 as a group member**

- In Active Directory Users and Computers, in the Member Servers OU, open **Application Servers Properties**, and then add **LON-SVR1** as a group member.

► **Task 3: Create a new Application Servers GPO**

1. On LON-DC1, open the Group Policy Management Console.
2. In the Group Policy Management Console, in the Group Policy Objects container, create a new GPO named **Application Servers GPO**.
3. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security - LDAP://CN={GUID}**.
4. Configure an inbound rule with the following settings:
  - Rule Type: **Custom**
  - Protocol type: **TCP**
  - Local port: Specific Ports - **8080**
  - Scope: **Any IP address**
  - Action: **Allow the connection**
  - Profile: **Domain** (clear both the **Private** and **Public** check boxes)
  - Name: **Application Server Department Firewall Rule**
5. Close the Group Policy Management Editor window.

► **Task 4: Link the Application Servers GPO to the Member Servers OU**

- In the Group Policy Management Console, link the **Application Servers GPO** to the **Member Servers OU**.

► **Task 5: Use security filtering to limit the Application Server GPO to members of Application Server group**

1. On LON-DC1, open the Group Policy Management Console.
2. Expand the **Member Servers OU**, and then click **Application Servers GPO**.
3. In the right-hand pane, under **Security Filtering**, remove **Authenticated Users**, and then configure **Application Servers GPO** to apply only to the Application Servers security group.

► **Task 6: Run gpupdate on LON-SVR1**

1. Switch to LON-SVR1.
2. Open the Command Prompt window, and then type the following command:

```
gpupdate /force
```

3. Close the Command Prompt window.
4. Restart LON-SVR1, and then sign back in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

► **Task 7: View the firewall rules on LON-SVR1**

1. Switch to LON-SVR1.
2. Start Windows Firewall with Advanced Security.
3. In the Windows Firewall with Advanced Security window, in **Inbound rules**, verify that the **Application Server Department Firewall Rule** that you created earlier by using Group Policy is configured.
4. Verify that you cannot edit the **Application Server Department Firewall Rule**, because it is configured through Group Policy.

**Results:** After completing this exercise, you will have used Group Policy to configure Windows Firewall with Advanced Security to create rules for application servers.

### Lab Review Questions

**Question:** You configured an AppLocker rule that prevents users from running software in a specified file path. How can you prevent users from moving the folder containing the software so that they can circumvent the rule and still run it?

**Question:** You want to introduce a new application that needs to use specific ports. What information do you need to configure Windows Firewall with Advanced Security, and from what source can you get it?

► **Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state by performing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20410D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20410D-LON-SVR1** and **20410D-LON-CL1**.

# Lab: Implementing Server Virtualization with Hyper-V

## Scenario

Your assignment is to configure the infrastructure service for a new branch office.

To use the server hardware that is available currently at branch offices more effectively, your manager has decided that all branch office servers will run as virtual machines. You must now configure a virtual network and a new virtual machine for these branch offices.

## Objectives

After performing this lab, you should be able to:

- Install the Hyper-V role onto a server.
- Configure virtual networking.
- Create and configure a virtual machine.
- Use virtual machine checkpoints.

## Lab Setup

Estimated Time: 70 minutes

|                 |                         |
|-----------------|-------------------------|
|                 |                         |
| Virtual machine | <b>20410D-LON-HOST1</b> |
| User name       | <b>Administrator</b>    |
| Password        | <b>Pa\$\$w0rd</b>       |

Before beginning the lab, you must complete the following steps:

1. Reboot the classroom computer and from the Windows Boot Manager, select **20410D-LON-HOST1**.
2. Sign in to LON-HOST1 with the **Administrator** account and the password **Pa\$\$w0rd**.

## Exercise 1: Installing the Hyper-V Role onto a Server

### Scenario

The first step in migrating to a virtualized environment for the branch office is installing the Hyper-V role on a new Windows Server 2012 server.

The main tasks for this exercise are as follows:

1. Install the Hyper-V role onto a server.
2. Complete the Hyper-V role installation, and verify the settings.

#### ► Task 1: Install the Hyper-V role onto a server

1. In Server Manager, click **Local Server**, and then configure the following network settings:
  - IP Address: **172.16.0.31**
  - Subnet mask: **255.255.0.0**
  - Default gateway: **172.16.0.1**
  - Preferred DNS server: **172.16.0.10**

2. Use the Add Roles and Features Wizard to add the Hyper-V role to LON-HOST1 with the following options:
  - o Do not create a virtual switch.
  - o Use the Default stores locations.
  - o Allow the server to restart automatically if required.
3. After a few minutes, the server restarts automatically. Ensure that you restart the machine from the boot menu as **20410D-LON-HOST1**. The computer will restart several times.

► **Task 2: Complete the Hyper-V role installation, and verify the settings**

1. Sign in to LON-HOST1 by using the account **Administrator** with the password **Pa\$\$word**.
2. When the installation of the Hyper-V tools completes, click **Close**.
3. Open the Hyper-V Manager console, and then click **LON-HOST1**.
4. Edit the Hyper-V settings of LON-HOST1, and then configure the following settings:
  - o Keyboard: **Use on the virtual machine**
  - o Virtual Hard Disks: **C:\Users\Public\Documents\Hyper-V\Virtual Hard Disks**

**Results:** After completing this exercise, you should have installed the Hyper-V role onto a physical server.

## Exercise 2: Configuring Virtual Networking

### Scenario

After installing the Hyper-V role on the new server, you need to configure the virtual network. You need to create a network that connects to the physical network *and* a private network that you can use only for communication between virtual machines. You will use the private network when you configure the virtual machines for high availability. You also need to configure a specific range of media access control (MAC) addresses for the virtual machines.

The main tasks for this exercise are as follows:

1. Configure the external network.
2. Create a private network.
3. Create an internal network.
4. Configure the MAC address range.

► **Task 1: Configure the external network**

1. Open the Hyper-V Manager console, and then click **LON-HOST1**.
2. Use the Virtual Switch Manager to create a new External virtual network switch with the following properties:
  - o Name: **Switch for External Adapter**
  - o External Network: Mapped to the host computer's physical network adapter. (This varies depending on the host computer.)

► **Task 2: Create a private network**

- In the Hyper-V Manager console use the Virtual Switch Manager to create a new virtual switch with the following properties:
  - Name: **Private Network**
  - Connection type: **Private network**

► **Task 3: Create an internal network**

- Use the Virtual Switch Manager to create a new virtual switch with the following properties:
  - Name: **Internal Network**
  - Connection type: **Internal network**

► **Task 4: Configure the MAC address range**

- Use the Virtual Switch Manager to configure the following MAC Address Range settings:
  - Minimum: **00-15-5D-0F-AB-A0**
  - Maximum: **00-15-5D-0F-AB-EF**

**Results:** After completing this exercise, you should have configured virtual switch options on a physically deployed Windows Server 2012 server that is running the Hyper-V role.

## Exercise 3: Creating and Configuring a Virtual Machine

### Scenario

You have been asked to deploy two virtual machines to LON-HOST1. You have copied a sysprepped virtual hard disk file that hosts a Windows Server 2012 installation.

To minimize disk space use at the cost of performance, you are going to create two differencing virtual hard disk files based on the sysprepped virtual hard disk. You then will use these differencing virtual hard disk files as the virtual hard disk files for the new virtual machines.

The main tasks for this exercise are as follows:

1. Create differencing virtual hard disks.
2. Create virtual machines.
3. Enable resource metering.

► **Task 1: Create differencing virtual hard disks**

1. Use File Explorer to create the following two folders:
  - **E:\Program Files\Microsoft Learning\Base\LON-GUEST1**
  - **E:\Program Files\Microsoft Learning\Base\LON-GUEST2**

 **Note:** The drive letter may depend upon the number of drives on the physical host computer.

2. In the Hyper-V Manager console, create a virtual hard disk with the following properties:
  - Disk Format: **VHD**
  - Disk Type: **Differencing**

- Name: **LON-GUEST1.vhd**
  - Location: **E:\Program Files\Microsoft Learning\Base\LON-GUEST1\**
  - Parent Location: **E:\Program Files\Microsoft Learning\Base\ Base14A-WS12R2.vhd**
3. Open Windows PowerShell, and then execute the following command:

```
New-VHD "E:\Program Files\Microsoft Learning\Base\LON-GUEST2\LON-GUEST2.vhd"
-ParentPath "E:\Program Files\Microsoft Learning\Base\ Base14A-WS12R2.vhd"
```

4. Inspect the disk at **E:\Program Files\Microsoft Learning\Base\LON-GUEST2\LON-GUEST2.vhd**.
5. Verify that **LON-GUEST2.vhd** is configured as a differencing virtual hard disk with **E:\Program Files\Microsoft Learning\Base\ Base14A-WS12R2.vhd** as a parent.

#### ► Task 2: Create virtual machines

1. On LON-HOST1, in the Hyper-V Manager console, in the Actions pane, click **New**, and then click **Virtual Machine**.
2. Create a virtual machine with the following properties:
  - Name: **LON-GUEST1**
  - Location: **E:\Program Files\Microsoft Learning\Base\LON-GUEST1\**
  - Generation: **Generation 1**
  - Memory: **1024 MB**
  - Use Dynamic Memory: **Yes**
  - Networking: **Private Network**
  - Connect Virtual Hard Disk: **E:\Program Files\Microsoft Learning\Base\LON-GUEST1\lon-guest1.vhd**

3. Open Windows PowerShell, and then execute the following command:

```
New-VM -Name LON-GUEST2 -MemoryStartupBytes 1024MB -VHDPath "E:\Program
Files\Microsoft Learning\Base\LON-GUEST2\LON-GUEST2.vhd" -SwitchName "Private
Network"
```

4. Use the Hyper-V Manager console to edit the settings of LON-GUEST2 by configuring the following:
- Automatic Start Action: **Nothing**
  - Automatic Stop Action: **Shut down the guest operating system**

#### ► Task 3: Enable resource metering

- At the Windows PowerShell prompt, enter the following commands:

```
Enable-VMResourceMetering LON-GUEST1
Enable-VMResourceMetering LON-GUEST2
```

**Results:** After completing this exercise, you should have deployed two separate virtual machines by using a sysprepped virtual hard disk file as a parent disk for two differencing virtual hard disks.

## Exercise 4: Using Virtual Machine Checkpoints

### Scenario

You are in the process of developing a strategy to mitigate the impact of incorrectly applied change requests. As a part of this strategy development, you are testing the speed and functionality of virtual machine checkpoints to roll back to a previously existing stable configuration.

In this exercise, you will deploy Windows Server 2012 in a virtual machine. You then will create a stable configuration for that virtual machine, and create a virtual machine checkpoint. Finally, you will modify the configuration, and roll back to the checkpoint.

The main tasks for this exercise are as follows:

1. Deploy Windows Server 2012 in a virtual machine.
2. Create a virtual machine checkpoint.
3. Modify the virtual machine.
4. Revert to the existing virtual machine checkpoint.
5. View resource metering data.

### ► Task 1: Deploy Windows Server 2012 in a virtual machine

1. Use the Hyper-V Manager console to start LON-GUEST1.
2. Open the Virtual Machine Connection Window, and perform the following steps to deploy Windows Server 2012 on the virtual machine:
  - o On the **Settings** page, click **Next** to accept the Region and Language settings.
  - o On the **Settings** page, click **I accept**.
  - o On the **Settings** page, enter the password **Pa\$\$w0rd** twice, and then click **Finish**.
3. Sign in to the virtual machine by using the account **Administrator** and the password **Pa\$\$w0rd**.
4. Reset the name of the virtual machine to **LON-GUEST1**, and then restart the virtual machine.

### ► Task 2: Create a virtual machine checkpoint

1. Sign in to the LON-GUEST1 virtual machine, and then verify that the name of the computer is set to **LON-GUEST1**.
2. Create a checkpoint of LON-GUEST1, and name the checkpoint **Before Change**.

### ► Task 3: Modify the virtual machine

1. Sign in to the LON-GUEST1 virtual machine, and use the Server Manager console to change the computer's name to **LON-Computer1**.
2. Reboot the virtual machine.
3. Sign in to the LON-GUEST1 virtual machine, and then verify that the server name is set to **LON-Computer1**.

### ► Task 4: Revert to the existing virtual machine checkpoint

1. Use the Virtual Machine Connection window to revert the virtual machine.
2. Verify that the **Computer Name** of the virtual machine now is set to **LON-GUEST1**.

### ► Task 5: View resource metering data

1. On LON-HOST1, issue the following command:

```
Measure-VM LON-GUEST1
```

2. Note the average central processing unit (CPU), average random access memory (RAM), and total disk use figures, and then close Windows PowerShell.

**Results:** After completing this exercise, you should have used virtual machine checkpoints to recover from a virtual machine misconfiguration.

### ► Revert the virtual machines

After you finish the lab, restart the computer in Windows Server 2012 by performing the following steps:

1. On the taskbar, click the **Windows PowerShell** icon.
2. In the Windows PowerShell window, enter the following command, and then press Enter:

```
Shutdown /r /t 5
```

3. From the Windows Boot Manager, select **Windows Server 2012**.

### Lab Review Questions

**Question:** What type of virtual network switch would you create if you want to allow the virtual machine to communicate with the LAN that is connected to the Hyper-V virtualization server?

**Question:** How can you ensure that no single virtual machine uses all of the available bandwidth that the Hyper-V virtualization server provides?

**Question:** What Dynamic Memory configuration task was not possible on previous versions of Hyper-V, but which you can now perform on a virtual machine that is hosted on the Hyper-V role on a Windows Server 2012 server?

# Lab: Configuring and Troubleshooting DNS

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, United Kingdom. An Information Technology office and a data center are located in London to support the head office and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure.

Management has asked you to add several new resource records to the DNS service that is installed on LON-DC1. Records include a new MX record for Exchange Server 2013 and a SRV record for a Microsoft Lync® Server 2013 deployment that is occurring.

A. Datum is working with a partner organization, Contoso, Ltd. You have been asked to configure internal name resolution between the two organizations. A small branch office has reported that name resolution performance is poor. The branch office contains a Windows Server 2012 server that performs several roles. However, there is no plan to implement an additional domain controller. You have been asked to install the DNS server role at the branch office and to create a secondary zone of Adatum.com. To maintain security, you have been instructed to configure the branch office server to be on the Notify list for Adatum.com zone transfers. You also should update all branch office clients to use the new name server in the branch office.

You should configure the new DNS server role to perform standard aging and scavenging, as necessary and as specified by corporate policy. After implementing the new server, you need to test and verify the configuration by using standard DNS troubleshooting tools.

## Objectives

After completing this lab, you will be able to:

- Configure DNS resource records.
- Configure DNS conditional forwarding.
- Install and configure DNS zones.
- Troubleshoot DNS.

## Lab Setup

Estimated Time: 60 minutes

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-CL1

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20411D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for 20411D-LON-SVR1 and 20411D-LON-CL1.

## Exercise 1: Configuring DNS Resource Records

### Scenario

You have been asked to add several new resource records to the DNS service on LON-DC1. Records include a new MX record for Exchange Server 2010, and an SRV record that is required for a Lync Server 2013 deployment that is taking place currently. You also have been asked to configure a reverse lookup zone for the domain.

The main tasks for this exercise are as follows:

1. Add the required mail exchanger (MX) record
2. Add the required Microsoft Lync Server records
3. Create the reverse lookup zone

#### ► Task 1: Add the required mail exchanger (MX) record

1. Switch to LON-DC1, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Open the DNS Manager.
3. Create a new host record with the following properties:
  - Zone: **Adatum.com**
  - Name: **Mail1**
  - IP address: **172.16.0.250**
4. In the **Adatum.com** zone, add a new record with the following information:
  - Type: **New Mail Exchanger (MX)**
  - Fully qualified domain name (FQDN) of mail server: **Mail1.Adatum.com**

#### ► Task 2: Add the required Microsoft Lync Server records

1. Create a new host record with the following properties:
  - Zone: **Adatum.com**
  - Name: **Lync-svr1**
  - IP address: **172.16.0.251**
2. In the **Adatum.com** zone, add a new record:
  - Type: **Service Location (SRV)**
  - Service: **\_sipinternalls**
  - Protocol: **\_tcp**
  - Port Number: **5061**
  - Host offering this service: **Lync-svr1.adatum.com**

#### ► Task 3: Create the reverse lookup zone

1. Create a new reverse lookup zone with the following properties:
  - Zone Type: **Primary zone**
  - Active Directory Zone Replication Scope: Default
  - Reverse Lookup Zone Name: **IPv4 Reverse Lookup Zone**

- Reverse Lookup Zone Name: **172.16**.
- Dynamic Update: Default

**Results:** After this exercise, you should have configured the required messaging service records and the reverse lookup zone.

## Exercise 2: Configuring DNS Conditional Forwarding

### Scenario

You have been asked to configure internal name resolution between A. Datum and its partner organization, Contoso.

The main tasks for this exercise are as follows:

1. Add the conditional forwarding record for Contoso.com

► **Task 1: Add the conditional forwarding record for Contoso.com**

- From the **Conditional Forwarders** node, configure conditional forwarding for Contoso.com:
  - a. In the **New Conditional Forwarder** dialog box, in the **DNS Domain** box, type **contoso.com**.
  - b. Click the **<Click here to add an IP Address or DNS Name>** box, type **131.107.1.2**, and then press Enter. Validation will fail because the server cannot be contacted.
  - c. Enable **Store this conditional forwarder in Active Directory, and replicate it as follows**.

**Results:** After this exercise, you should have configured conditional forwarding.

## Exercise 3: Installing and Configuring DNS Zones

### Scenario

A small branch office has reported that name resolution performance is poor. The branch office contains a Windows Server 2012 server that performs several roles. However, there is no plan to implement an additional domain controller.

You have been asked to install the DNS server role at the branch office, and then create a secondary zone of Adatum.com. To maintain security, you also have been instructed to configure the branch office server to be on the Notify list for Adatum.com zone transfers. You also should update all branch office clients to use the new name server in the branch office, and then configure the new DNS server role to perform standard aging and scavenging, as needed and specified by corporate policy.

The main tasks for this exercise are as follows:

1. Install the DNS server role on LON-SVR1
2. Create the required secondary zones on LON-SVR1
3. Enable and configure zone transfers
4. Configure Time to Live (TTL), aging, and scavenging
5. Configure clients to use the new name server

► **Task 1: Install the DNS server role on LON-SVR1**

1. Switch to LON-SVR1, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Use Server Manager to install the DNS Server role.

► **Task 2: Create the required secondary zones on LON-SVR1**

1. Open a Windows PowerShell Administrator console.
2. Type the following cmdlet to create the required secondary zone:

```
Add-DnsServerSecondaryZone -Name "Adatum.com" -ZoneFile "Adatum.com.dns" -MasterServers 172.16.0.10
```

► **Task 3: Enable and configure zone transfers**

1. Switch to LON-DC1.
2. Open Windows PowerShell, and then run the following cmdlet to configure zone transfers for the Adatum.com zone:

```
Set-DnsServerPrimaryZone -Name "adatum.com" -Notify NotifyServers -notifyservers "172.16.0.21" -SecondaryServers "172.16.0.21" -SecureSecondaries TransferToSecureServers
```

3. In DNS Manager, verify the changes to the Zone Transfers settings:
  - a. In the navigation pane, click **Adatum.com**, and then, on the toolbar, click **Refresh**.
  - b. Right-click **Adatum.com**, and then click **Properties**.
  - c. In the **Adatum.com Properties** dialog box, click the **Zone Transfers** tab.
  - d. Click **Notify**, verify that the server **172.16.0.21** appears, and then click **Cancel**.

► **Task 4: Configure Time to Live (TTL), aging, and scavenging**

1. On LON-DC1, open the Adatum.com zone properties.
2. On the **Start of Authority (SOA)** tab, configure the **Minimum (default) TTL** value to be **2** hours.
3. Right-click **LON-DC1**, and then select the **Set Aging/Scavenging for All Zones** option to configure aging and scavenging options.
4. Enable **Scavenge stale resource records**, and then use the default values.

► **Task 5: Configure clients to use the new name server**

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Use Network and Sharing Center to view the properties of **Ethernet**.
3. Reconfigure **Internet Protocol Version 4 (TCP/IPv4)** as follows:
  - Modify the Preferred DNS server: **172.16.0.21**.

**Results:** After this exercise, you should have installed and configured Domain Name System (DNS) on LON-SVR1.

## Exercise 4: Troubleshooting DNS

### Scenario

After implementing the new server, you need to test and verify the configuration by using standard DNS troubleshooting tools.

The main tasks for this exercise are as follows:

1. Test simple and recursive queries
2. Verify start of authority (SOA) resource records with Windows PowerShell
3. To prepare for the next module

#### ► Task 1: Test simple and recursive queries

1. On LON-DC1, in DNS Manager, open the **LON-DC1 Properties**.
2. On the **Monitoring** tab, perform a simple query against the DNS server. This is successful.
3. Perform simple and recursive queries against this and other DNS servers. The recursive test fails because there are no forwarders configured.
4. Stop the DNS service, and then repeat the previous tests. They fail because no DNS server is available.
5. Restart the DNS service, and then repeat the tests. The simple test is successful.
6. Close the **LON-DC1 Properties** dialog box.

#### ► Task 2: Verify start of authority (SOA) resource records with Windows PowerShell

1. Open Windows PowerShell on LON-DC1.
2. Type the following command, and then press Enter:

```
resolve-dnsname -name Adatum.com -type SOA
```

3. View the results, and then close the Windows PowerShell console.

#### ► Task 3: To prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for 20411D-LON-SVR1 and 20411D-LON-CL1.

**Results:** After this exercise, you should have tested and verified DNS.

**Question:** In the lab, you were required to deploy a secondary zone because you were not going to deploy any additional domain controllers. If this condition changed—that is, if LON-SVR1 was a domain controller—how would that change your implementation plan?

# Lab: Maintaining AD DS

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, United Kingdom. An IT office and data center in London support the head office and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure, and is making several organizational changes that require modifications to the AD DS infrastructure. A new location requires a secure method of providing onsite AD DS. A. Datum is opening a new branch office that does not yet have a secure data center, but does now require a domain controller. You need to deploy a domain controller for this office. In addition, you have been asked to extend the capabilities of Active Directory Recycle Bin to the entire organization. As part of an overall virtualization strategy, IT management also wants you to perform a proof of concept deployment of a domain controller using domain controller cloning.

## Objectives

After completing this lab, you will be able to:

- Install and configure an RODC.
- Configure and view Active Directory snapshots.
- Configure the Active Directory Recycle Bin.
- Use domain controller cloning to deploy a domain controller.

## Lab Setup

Estimated Time: 75 minutes

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

## Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20411D-LON-DC1**, and, in the **Actions** pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20411D-LON-SVR1**.

## Exercise 1: Installing and Configuring an RODC

### Scenario

A. Datum is adding a new branch office. You have been asked to configure an RODC to service logon requests at the branch office. You also need to configure password policies that ensure caching only of passwords for local users in the branch office.

The main tasks for this exercise are as follows:

1. Verify requirements for installing an RODC
2. Install an RODC
3. Configure a password replication policy

► Task 1: Verify requirements for installing an RODC

1. On LON-DC1, from Server Manager, open **Active Directory Users and Computers**.
2. In the properties of Adatum.com, verify that the forest functional level is at least Windows Server 2003.
3. On LON-SVR1, open **Server Manager**, and verify whether the computer is a domain member.
4. Use **System Properties** to place LON-SVR1 in a workgroup named **TEMPORARY**.
5. Restart LON-SVR1.
6. On LON-DC1, open **Active Directory Users and Computers**.
7. Delete the **LON-SVR1** computer account from the Computers container.
8. In the **Domain Controllers** OU, precreate an RODC account by using default settings, except for the following:
  - Computer name: **LON-SVR1**
  - Delegate to: **ADATUM\IT**
9. Close Active Directory Users and Computers.

► Task 2: Install an RODC

1. Sign in to LON-SVR1 as **Administrator** with the password **Pa\$\$w0rd**.
2. On LON-SVR1, add the **Active Directory Domain Services** role.
3. Complete the Active Directory Domain Services Installation Wizard by using default options except those listed below:
  - Domain: **Adatum.com**
  - Network credentials: **Adatum\April (a member of the IT group)**
  - Password for April: **Pa\$\$w0rd**
  - Directory Services restore mode password: **Pa\$\$w0rd**
  - Replicate from: **LON-DC1.Adatum.com**
4. When installation is complete, restart LON-SVR1.

► Task 3: Configure a password replication policy

#### Configure password replication groups

1. On LON-DC1, from Server Manager, open **Active Directory Users and Computers**.
2. In the Users container, view the membership of the **Allowed RODC Password Replication Group**, and verify that there are no current members.
3. In the **Domain Controllers** OU, open the properties of LON-SVR1.
4. On the **Password Replication Policy** tab, verify that the **Allowed RODC Password Replication Group** and **Denied RODC Password Replication Group** are listed.

### Create a group to manage password replication to the remote office RODC

1. On LON-DC1, in **Active Directory Users and Computers**, in the **Research** OU, create a new group named **Remote Office Users**.
2. Add **Aziz, Colin, Lukas, Louise**, and **LON-CL1** to the membership of **Remote Office Users**.

### Configure a Password Replication Policy for the remote office RODC

1. On LON-DC1, in **Active Directory Users and Computers**, click the **Domain Controllers** OU, and then open the properties of LON-SVR1.
2. On the **Password Replication Policy** tab, allow the **Remote Office Users** group to replicate passwords to LON-SVR1.

### Evaluate the resulting Password Replication Policy

1. On LON-DC1, in **Active Directory Users and Computers**, in the **Domain Controllers** OU, open the properties of LON-SVR1.
2. On the **Password Replication Policy** tab, click **Advanced**. On the **Resultant Policy** tab, add **Aziz**, and then confirm that Aziz's password can be cached.

### Monitor credential caching

1. Attempt to sign in to LON-SVR1 as **Aziz**. This sign-in will fail because Aziz does not have permission to sign in to the RODC, but authentication is performed and the credentials are now cached.
2. On LON-DC1, in **Active Directory Users and Computers**, in the **Domain Controllers** OU, open the properties of LON-SVR1.
3. On the **Password Replication Policy** tab, open the **Advanced** configuration.
4. On the **Policy Usage** tab, select the **Accounts that have been authenticated to this Read-only Domain Controller** option. Notice that Aziz's password has been cached.

### Prepopulate credential caching

1. On LON-DC1, in **Active Directory Users and Computers**, in the **Domain Controllers** OU, right-click **LON-SVR1**, and then click **Properties**.
2. On the **Password Replication Policy** tab, click **Advanced**.
3. On the **Policy Usage** tab, prepopulate the password for **Louise** and **LON-CL1**.
4. Read the list of cached passwords, and then confirm that Louise and LON-CL1 have been added.
5. Close all open windows on LON-DC1.

**Results:** After completing this exercise, you should have successfully installed and configured a read-only domain controller (RODC).

## Exercise 2: Configuring AD DS Snapshots

### Scenario

As part of the overall disaster recovery plan for A. Datum, you have been instructed to test the process for taking Active Directory snapshots and viewing them. If the process is successful, you will schedule them to occur on a regular basis to assist in the recovery of deleted or modified AD DS objects.

The main tasks for this exercise are as follows:

1. Create a snapshot of AD DS
2. Make a change to AD DS
3. Mount an Active Directory snapshot, and create a new instance
4. Explore a snapshot with Active Directory Users and Computers
5. Unmount an Active Directory snapshot

### ► Task 1: Create a snapshot of AD DS

 **Note:** The commands in the following step return a message indicating that the snapshot set was generated successfully. The GUID that displays is important for commands in later tasks. Make a note of the GUID or copy it to the **Clipboard**.

- On LON-DC1, open a command prompt window, and then type each of the following commands followed by Enter:

```
ntdsutil
snapshot
activate instance ntds
create
quit
Quit
```

### ► Task 2: Make a change to AD DS

1. On LON-DC1, open **Server Manager**.
2. From Server Manager, open **Active Directory Users and Computers**.
3. Delete Adam Barr's account from the **Marketing** OU.

### ► Task 3: Mount an Active Directory snapshot, and create a new instance

1. Open an administrative command prompt, and then type each of the following commands followed by Enter:

```
ntdsutil
snapshot
activate instance ntds
list all
```

The command returns a list of all snapshots.

2. Type each of the following commands followed by Enter:

```
mount guid
quit
Quit
```

Where *guid* is the GUID of the snapshot you created.

3. While many command executables can be run without any issue in Windows PowerShell, you cannot run the `dsmain.exe` command from Windows PowerShell. Ensure that you are in the command prompt as administrator to perform this step.  
Use the snapshot to start an instance of Active Directory by typing the following command, all on one line, and then press Enter:

```
dsamain /dbpath c:\$snap_datetime_volumec$\windows\ntds\ntds.dit /ldapport 50000
```

Note that *datetime* will be a unique value. There should be only one folder on your drive C with a name that begins with \$snap.

4. A message indicates that AD DS startup is complete. Leave Dsomain.exe running, and do not close the command prompt.

#### ► Task 4: Explore a snapshot with Active Directory Users and Computers

1. Switch to **Active Directory Users and Computers**. Right-click the root node of the snap-in, and then click **Change Domain Controller**. Type the directory server name and port **LON-DC1:50000**, and then press Enter. Click **OK**.
2. Locate the **Adam Barr** user account object in the **Marketing** OU. Note that Adam Barr's object is displayed because the snapshot was taken prior to deleting it.

#### ► Task 5: Unmount an Active Directory snapshot

1. In the command prompt, press Ctrl+C. to stop DSAMain.exe.
2. Type the following commands:

```
ntdsutil
snapshot
activate instance ntds
list all
unmount guid
list all
quit
Quit
```

Where *guid* is the GUID of the snapshot.

**Results:** After completing this exercise, you should have successfully configured Active Directory Domain Services (AD DS) snapshots.

## Exercise 3: Configuring the Active Directory Recycle Bin

### Scenario

As part of the Disaster Recovery plan for AD DS, you need to configure and test the Active Directory Recycle Bin to allow for object and container level recovery.

The main tasks for this exercise are as follows:

1. Enable the Active Directory Recycle Bin
2. Create and delete test users
3. Restore the deleted users
4. Prepare for the next module

#### ► Task 1: Enable the Active Directory Recycle Bin

1. On LON-DC1, from Server Manager, open **Active Directory Administrative Center**.
2. Enable the Recycle Bin.
3. Press F5 to refresh **Active Directory Administrative Center**.

► **Task 2: Create and delete test users**

1. In **Active Directory Administrative Center**, create the following users in the **Research** OU. Give each a password of **Pa\$\$w0rd**:
  - Test1
  - Test2
2. Delete the **Test1** and **Test2** accounts.

► **Task 3: Restore the deleted users**

1. In **Active Directory Administrative Center**, navigate to the **Deleted Objects** folder for the **Adatum** domain.
2. Restore **Test1** to its original location.
3. Restore **Test2** to the **IT** OU.
4. Confirm that **Test1** is now located in the **Research** OU and that **Test2** is in the **IT** OU.

► **Task 4: Prepare for the next module**

 **Note:** Do not perform if you are performing the optional exercise entitled "Cloning a Domain Controller". If you are performing the optional exercise, return here when done to finish the "To prepare for the next module" task as outlined below.

When you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20411D-LON-SVR1**.

**Results:** After completing this exercise, you should have successfully configured the Active Directory Recycle Bin.

## Exercise 4: Optional Exercise: Cloning a Domain Controller

### Scenario

IT management at A. Datum wants to be able to deploy new virtual domain controllers rapidly when necessary. They are considering using the domain controller clone in Windows Server 2012 R2. You must perform a domain controller cloning procedure as a proof of concept for your IT management team.

The main tasks for this exercise are as follows:

1. Check for domain controller clone prerequisites
2. Export the source domain controller
3. Perform domain controller cloning

► **Task 1: Check for domain controller clone prerequisites**

1. Switch to LON-DC1.
2. Add the domain controller **LON-DC1** to the Active Directory group **Cloneable Domain Controllers**.
3. Verify applications and services on LON-DC1 to support cloning.
4. Create a DCCloneConfig.xml file, and then configure the name of that cloned domain as **LON-DC3**.
5. Shut down LON-DC1.

► **Task 2: Export the source domain controller**

1. On the host computer, in Hyper-V Manager, export **LON-DC1**.
2. Start LON-DC1.

► **Task 3: Perform domain controller cloning**

1. Import a new virtual machine by using the exported files. Name the new virtual machine **20411D-LON-DC3**, and then select to **Copy the virtual machine (create a new unique ID)**.
2. In Hyper-V Manager, start LON-DC3.

► **Task 4: Revert and delete virtual machines**

- Revert the 20411D-LON-DC1 and delete the 20411D-LON-DC3 virtual machines from the host computer's Hyper-V Manager.

**Results:** After completing this exercise, you will have successfully cloned a domain controller.

# Lab: Managing User and Service Accounts

## Scenario

A. Datum is a global engineering and manufacturing company with their head office based in London, United Kingdom. An IT office and data center are located in London to support the London location and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

A. Datum has completed a security review for passwords and account lockout policies. You need to implement the recommendations contained in the report to control password complexity and length. You also need to configure appropriate account lockout settings. Part of your password policy configuration will include a specific password policy you need to assign to the Executive security group. This group requires a different password policy than the policy applied at the domain level.

You need to configure a new group managed service account to support a new Web-based program. Using a group managed service account will help maintain the password security requirements for the account.

## Objectives

After completing this lab, you will be able to:

- Configure password policy and account lockout settings.
- Create and associate a managed service account.

## Lab Setup

Estimated Time: 45 minutes

**Virtual machines:** 20411D-LON-DC1

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

- On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
- In Microsoft Hyper-V® Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
- In the Actions pane, click **Connect**. Wait until the virtual machine starts.
- Log on using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**

## Exercise 1: Configuring Password Policy and Account Lockout Settings

### Scenario

A. Datum has recently completed a security review for passwords and account lockout policies. You need to implement the recommendations contained in the report to control password complexity and length. You also need to configure appropriate account lockout settings. Part of your password policy configuration will include a specific password policy to be assigned to the Managers security group. This group requires a different password policy than the policy that has been applied at the domain level.

The report has recommended that you apply the following password settings to all accounts in the domain:

- Password history: **20 passwords**
- Maximum password age: **45 days**
- Minimum password age: **1 day**
- Password length: **10 characters**
- Complexity enabled: **Yes**
- Account Lockout duration: **30 minutes**
- Account lockout threshold: **5 attempts**
- Reset account lockout counter after: **15 minutes**

The report has also recommended that you apply a separate policy to users in the Managers group, due to the elevated privileges assigned to those user accounts. The policy applied to the Managers groups should contain the following settings:

- Password history: **20 passwords**
- Maximum password age: **20 days**
- Minimum password age: **1 day**
- Password length: **15 characters**
- Complexity enabled: **Yes**
- Account Lockout duration: **0 minutes (An administrator will have to unlock the account)**
- Account lockout threshold: **3 attempts**
- Reset account lockout counter after: **30 minutes**

The main tasks for this exercise are as follows:

1. Configure a domain-based password policy
2. Configure an account lockout policy
3. Configure and apply a fine-grained password policy

#### ► **Task 1: Configure a domain-based password policy**

1. On LON-DC1, open the Group Policy Management console.
2. Edit the Default Domain Policy, and configure the following Account Password Policy settings:
  - Password history: **20 passwords**
  - Maximum password age: **45 days**
  - Minimum password age: **1 day**
  - Password length: **10 characters**
  - Complexity enabled: **Yes**

### ► Task 2: Configure an account lockout policy

1. In the Group Policy Management Editor, configure the following Account Lockout Policy settings for the Default Domain Policy:
  - Account Lockout duration: **30 minutes**
  - Account lockout threshold: **5 attempts**
  - Reset account lockout counter after: **15 minutes**
2. Close the Group Policy Management Editor.
3. Close Group Policy Management.

### ► Task 3: Configure and apply a fine-grained password policy

1. On LON-DC1, open the Active Directory Administrative Center console.
2. Change the group scope for the **Managers** group to **Global**.

 **Note:** Make sure that you open the **Properties** page for the Managers group, and not the Managers OU.

3. In the Active Directory Administrative Center, configure a fine-grained password policy for the **Adatum\Managers** group with the following settings:
  - Name: **ManagersPSO**
  - Precedence: **10**
  - Password length: **15 characters**
  - Password history: **20 passwords**
  - Complexity enabled: **Yes**
  - Minimum password age: **1 day**
  - Maximum password age: **30 days**
  - Number of failed logon attempts allowed: **3 attempts**
  - Reset failed logon attempts count after: **30 minutes**
  - Until an administrator manually unlocks the account: selected
4. Close the Active Directory Administrative Center.

**Results:** After completing this exercise, you will have configured password policy and account lockout settings.

## Exercise 2: Creating and Associating a Managed Service Account

### Scenario

You need to configure a managed service account to support a new Web-based program that you will deploy to the DefaultAppPool Web service on LON-DC1. Using a managed service account will help maintain the password security requirements for the account.

The main tasks for this exercise are as follows:

1. Create and associate a managed service account
2. Install a group managed service account on LON-DC1
3. To prepare for the next module

► **Task 1: Create and associate a managed service account**

1. On LON-DC1, open the Active Directory Module for Windows PowerShell console.
2. Create the KDS root key by using the **Add-KdsRootKey** cmdlet. Make the effective time minus 10 hours, so the key will be effective immediately.
3. Create the new service account named **Webservice** for the host LON-DC1.
4. Associate the Webservice managed account with LON-DC1.
5. Verify the group managed service account was created by using the **Get-ADServiceAccount** cmdlet.

► **Task 2: Install a group managed service account on LON-DC1**

1. On LON-DC1, install the Webservice service account.
2. From the **Tools** menu in Server Manager, open Internet Information Services (IIS) Manager.
3. In the Internet Information Services (IIS) Manager console, if a window appears with a "Do you want to get started with Microsoft Web Platform to stay connected" message, click **Cancel**.
4. In the **DefaultAppPool Actions** pane, in the **Advanced Settings** dialog box, configure the DefaultAppPool to use the Webservice\$ account as the identity. Note that you can click the **ellipses** (...) by the Identity name to add the Webservice\$ account as a Custom Account.
5. Stop and then start the application pool.

► **Task 3: To prepare for the next module**

When you are finished with the lab, revert the virtual machines to their initial state.

**Results:** After completing this exercise, you will have created and associated a managed service account.

# Lab: Implementing a Group Policy Infrastructure

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, England. An IT office and a data center are located in London to support the London office and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure.

You have been asked to use Group Policy to implement standardized security settings to lock computer screens when users leave computers unattended for 10 minutes or more. You also have to configure a policy setting that will prevent access to certain programs on local workstations.

After some time, you have been made aware that a critical application fails when the screensaver starts, and an engineer has asked you to prevent the setting from applying to the team of Research engineers that uses the application every day. You also have been asked to configure conference room computers to use a 45-minute timeout.

After creating the policies, you need to evaluate the RSoPs for users in your environment to ensure that the Group Policy infrastructure is optimal and that all policies apply as intended.

## Objectives

After completing this lab, you will be able to:

- Create and configure GPOs.
- Manage Group Policy scope.
- Troubleshoot Group Policy application.
- Manage GPOs.

## Lab Setup

**Estimated Time:** 90 minutes

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-CL1

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, click **Administrative Tools**, and then double-click **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20411D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 and 3 for **20411D-LON-CL1**. Do not sign in to LON-CL1 until directed to do so.

## Exercise 1: Creating and Configuring GPOs

### Scenario

You have been asked to use Group Policy to implement standardized security settings to lock computer screens when users leave computers unattended for 10 minutes or more. You also have to configure a policy setting that will prevent users from running the Notepad application on local workstations.

The main tasks for this exercise are as follows:

1. Create and Edit a GPO
2. Link the GPO
3. View the Effects of the GPO's Settings

► **Task 1: Create and Edit a GPO**

1. On LON-DC1, from Server Manager, open the Group Policy Management Console.
2. Create a GPO named **ADATUM Standards** in the **Group Policy Objects** container.
3. Edit the **ADATUM Standards** policy, and then navigate to **User Configuration\Policies, Administrative Templates\System**.
4. Prevent users from running **Notepad.exe** by configuring the **Don't run specified Windows applications** policy setting.
5. Navigate to the **User Configuration\Policies\Administrative Templates\Control Panel\Personalization** folder, and then configure the **Screen saver timeout** policy to **600 seconds**.
6. Enable the **Password protect the screen saver** policy setting, and then close the Group Policy Management Editor window.

► **Task 2: Link the GPO**

- Link the **ADATUM Standards** GPO to the **Adatum.com** domain.

► **Task 3: View the Effects of the GPO's Settings**

1. Sign in to LON-CL1 as **Adatum\Pat** with the password **Pa\$\$w0rd**.
2. Attempt to change the screen saver wait time and resume settings. You are prevented from doing this by Group Policy.
3. Attempt to run **Notepad**. You are prevented from doing this by Group Policy.

**Results:** After this exercise, you should have created, edited, and linked the required GPOs.

## Exercise 2: Managing GPO Scope

### Scenario

After some time, you have been made aware that a critical application that the Research Engineering team uses is failing when the screen saver starts. You have been asked to prevent the GPO setting from applying to any member of the Engineering security group. You also have been asked to configure conference room computers to be exempt from corporate policy. However, they always must have a 45-minute screen saver timeout applied.

The main tasks for this exercise are as follows:

1. Create and Link the Required GPOs
2. Verify the Order of Precedence
3. Configure the Scope of a GPO with Security Filtering
4. Configure Loopback Processing

► **Task 1: Create and Link the Required GPOs**

1. On LON-DC1, open **Active Directory Users and Computers** and in the **Research** OU, create a sub-OU named **Engineers**, and then close Active Directory Users and Computers.
2. In the Group Policy Management Console, create a new GPO linked to the **Engineers** OU named **Engineering Application Override**.
3. Configure the **Screen saver timeout** policy setting to be **Disabled**, and then close the Group Policy Management Editor.

► **Task 2: Verify the Order of Precedence**

- In the Group Policy Management Console, select the **Engineers** OU, and then click the **Group Policy Inheritance** tab. Notice that the Engineering Application Override GPO has precedence over the ADATUM Standards GPO. The screen saver timeout policy setting you just configured in the Engineering Application Override GPO will apply after the setting in the ADATUM Standards GPO. Therefore, the new setting will overwrite the standards setting, and will *win*. Screen saver timeout will be disabled for users within the scope of the Engineering Application Override GPO.

► **Task 3: Configure the Scope of a GPO with Security Filtering**

1. On LON-DC1, open **Active Directory Users and Computers**. In the **Research\Engineers** OU, create a global security group named **GPO\_Engineering Application Override\_Apply**.
2. In the **Group Policy Management** Console, select the **Engineering Application Override** GPO. Notice that, in the Security Filtering section, the GPO applies by default to all authenticated users. Configure the GPO to apply only to the **GPO\_Engineering Application Override\_Apply** group.
3. In the **Users** folder, create a global security group named **GPO\_ADATUM Standards\_Exempt**.
4. In the Group Policy Management Console, select the **ADATUM Standards** GPO. Notice that in the Security Filtering section, the GPO applies by default to all authenticated users.
5. Configure the GPO delegation to deny Apply Group Policy permission to the **GPO\_ADATUM Standards\_Exempt** group.

► **Task 4: Configure Loopback Processing**

1. On LON-DC1, switch to **Active Directory Users and Computers**.
2. Create a new OU named **Kiosks**.
3. Under Kiosks, create a sub-OU named **Conference Rooms**.
4. Switch to the Group Policy Management Console.
5. Create a new GPO named **Conference Room Policies**, and then link it to the **Kiosks\Conference Rooms** OU.
6. Confirm that the **Conference Room Policies** GPO is scoped to **Authenticated Users**.

7. Edit the **Conference Room Policies** GPO, and then modify the **Screen Saver timeout** policy to launch the screen saver after **45 minutes**.
8. Modify the **Configure user Group Policy loopback processing mode** policy setting to use **Merge mode**.

**Results:** After this exercise, you should have configured the required scope of the GPOs.

## Exercise 3: Verifying GPO Application

### Scenario

After creating the required policies, you need to evaluate the RSOPs for the users in your environment to ensure that the Group Policy infrastructure is healthy, and that all policies apply as intended.

The main tasks for this exercise are as follows:

1. Perform RSOP Analysis
2. Analyze RSOP with GPResults
3. Evaluate GPO Results by Using the Group Policy Modeling Wizard
4. Review Policy Events and Determine GPO Infrastructure Status

#### ► Task 1: Perform RSOP Analysis

1. On LON-CL1, verify that you are still signed in as **Adatum\Pat**. If necessary, provide the password of **Pa\$\$w0rd**.
2. At an elevated command prompt, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Run the **gpupdate /force** command. After the command has completed, make a note of the current system time, which you will need to know for a task later in this lab:

Time:

4. Restart LON-CL1, and then wait for it to restart before proceeding with the next task.
5. On LON-DC1, switch to the **Group Policy Management** Console.
6. Use the **Group Policy Results Wizard** to run an RSOP report for **Pat** on **LON-CL1**.
7. Review Group Policy Summary results. Identify the time of the last policy refresh and the list of allowed and denied GPOs for both user and computer configuration. Identify the components that were used to process policy settings.
8. Click the **Details** tab. Review the settings that applied during user and computer policy application, and then identify the GPO from which the settings were obtained.
9. Click the **Policy Events** tab, and then locate the event that logs the policy refresh that you triggered with the GPUpdate command at the beginning of the task.
10. Click the **Summary** tab, right-click the page, and then choose **Save Report**. Save the report as an HTML file to your desktop, and then open the RSOP report.

#### ► Task 2: Analyze RSOP with GPResults

1. Sign in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. At a command prompt, run the **gpresult /r** command. RSOP summary results are displayed. The information is very similar to the **Summary** tab of the RSOP report that was produced by the Group Policy Results Wizard.

3. Type **gpresult /v**, and then press Enter. A more detailed RSoP report is produced. Notice that many of the Group Policy settings that were applied by the client are listed in this report.
4. Type **gpresult /z**, and then press Enter. The most detailed RSoP report is produced.
5. Type **gpresult /h:"%userprofile%\Desktop\RSOP.html"**, and then press Enter. An RSoP report is saved as an HTML file to your desktop.
6. Open the saved RSoP report from your desktop. Compare the report, its information, and its formatting with the RSoP report that you saved in the previous task.

► **Task 3: Evaluate GPO Results by Using the Group Policy Modeling Wizard**

1. Switch to LON-DC1.
2. Start the **Group Policy Modeling Wizard**.
3. Select **Adatum\Mike** as the user, and **LON-CL1** as the computer for modeling.
4. When prompted, select the **Loopback Processing** check box, and then click **Merge**. Even though the Conference Room Policies GPO specifies loopback processing, you must instruct the Group Policy Modeling Wizard to consider loopback processing in its simulation.
5. When prompted, on the **Alternate Active Directory Paths** page, choose the **Kiosks\Conference Rooms** location. You are simulating the effect of LON-CL1 as a conference room computer.
6. Accept all other options as defaults.
7. On the **Details** tab, scroll to and expand, if necessary, **User Details**, **Group Policy Objects**, and **Applied GPOs**.
8. Check whether the Conference Room Policies GPO applies to Mike as a User policy when he logs on to LON-CL1 if LON-CL1 is in the Conference Rooms OU.
9. Scroll to and expand, if necessary, **User Details**, **Policies**, **Administrative Templates**, and **Control Panel/Personalization**.
10. Confirm that the screen saver timeout is 2,700 seconds (45 minutes), the setting configured by the Conference Room Policies GPO that overrides the 10-minute standard configured by the ADATUM Standards GPO.

► **Task 4: Review Policy Events and Determine GPO Infrastructure Status**

1. On LON-CL1, you are signed in as **Adatum\Administrator**.
2. Open **Control Panel**, and then browse to the **Event Viewer**.
3. Locate and review Group Policy events in the **System** log.
4. Locate and review Group Policy events in the **Application** log. Review the events and identify the Group Policy events that have been entered in this log. Which events are related to Group Policy application and which are related to the activities you have been performing to manage Group Policy? Note that depending on how long the virtual machine has been running, you might not have any Group Policy events in the application log.
5. Browse to the **Group Policy Operational** log and locate the first event related to the Group Policy refresh you initiated in Exercise 1: Creating and Configuring GPOs, with the GPUpdate command. Review that event and the events that followed it.

**Results:** After this exercise, you should have used RSoP tools to verify the correct application of your GPOs.

## Exercise 4: Managing GPOs

### Scenario

You must back up all critical GPOs. You use the Group Policy Management backup feature to back up the **ADATUM Standard** GPO.

The main tasks for this exercise are as follows:

1. Perform a Backup of GPOs
2. Perform a Restore of GPOs
3. Troubleshooting GPOs
4. Preparing for the Next Module

#### ► Task 1: Perform a Backup of GPOs

1. Switch to LON-DC1, and in the Group Policy Management Console, in the navigation pane, click **Group Policy Objects**.
2. Back up the **ADATUM Standards** GPO to **C:\**.

#### ► Task 2: Perform a Restore of GPOs

- In the Group Policy Management Console, restore the previous backup of **ADATUM Standards**.

#### ► Task 3: Troubleshooting GPOs

1. Run the GPOTroubleshooting.ps1 Windows PowerShell script in the Allfiles directory (**E:\Labfiles\Mod04\**).
2. Verify that the **ADATUM Standards** GPO is not applying to Pat.
3. Troubleshoot and resolve the problem.

#### ► Task 4: Preparing for the Next Module

- When you have finished the lab, revert all virtual machines back to their initial state.

**Results:** After this exercise, you should have performed common management tasks on your GPOs.

**Question:** Which policy settings are already being deployed by using Group Policy in your organization?

**Question:** Many organizations rely heavily on security group filtering to scope GPOs, rather than linking GPOs to specific OUs. In these organizations, GPOs typically are linked very high in the Active Directory logical structure—to the domain itself or to a first-level OU. What advantages do you gain by using security group filtering rather than GPO links to manage a GPO's scope?

**Question:** Why might it be useful to create an exemption group—a group that is denied the Apply Group Policy permission—for every GPO that you create?

**Question:** Do you use loopback policy processing in your organization? In which scenarios and for which policy settings can loopback policy processing add value?

**Question:** In which situations have you used RSOP reports to troubleshoot Group Policy application in your organization?

**Question:** In which situations have you used, or might you anticipate using, Group Policy Modeling?

# Lab: Managing User Desktops with Group Policy

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, England. An IT office and a data center are located in London to support the London head office and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

A. Datum has been using logon scripts to provide users with drive mappings to file shares. The maintenance of these scripts is an ongoing problem because they are large and complex. Your manager has asked you to implement the drive mappings by using Group Policy preferences so that logon scripts can be removed.

Your manager has also asked you to place a shortcut to the Notepad application for all users that belong to the IT security group and to add a new Computer Administrators security group as a local Administrator on all servers.

A. Datum wants to be able to manage Office 2013 settings for all client computers. They have decided to use Administrative templates to do this.

## Objectives

After completing this lab, you will be able to:

- Implement settings by using Group Policy preferences.
- Configure Office 2013 settings using Administrative templates.
- Configure folder redirection.
- Deploy software by using Group Policy.

## Lab Setup

**Estimated Time:** 45 minutes

**Virtual Machines:** 20411D-LON-DC1, 20411D-LON-CL1

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, click **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Log in using the following credentials:
  - User name: Administrator
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for 20411D-LON-CL1.

## Exercise 1: Implementing Settings by Using Group Policy Preferences

### Scenario

A. Datum has been using logon scripts to provide users with drive mappings to file shares. The maintenance of these scripts is an ongoing problem because they are large and complex. Your manager has asked you to implement the drive mappings by using Group Policy preferences so that logon scripts can be removed. Your manager has also asked you to place a shortcut to the Notepad application for all users that belong to the IT security group.

The main tasks for this exercise are as follows:

1. Create a new GPO, and link it to the Branch Office 1 organizational unit (OU)
2. Edit the default Domain Policy with the required Group Policy preferences
3. Test the preferences

#### ► Task 1: Create a new GPO, and link it to the Branch Office 1 organizational unit (OU)

1. On LON-DC1, open File Explorer, and then create a folder and share it with specific people by using the following properties:
  - Path: C:\Branch1Share
  - name: Branch1
  - Permissions: Everyone, Read/Write
2. On LON-DC1, open **Active Directory Users and Computers**, and then create an OU in the **Adatum.com** domain called **Branch Office 1**.
3. Move user **Holly Dickson** from the **IT** OU to the **Branch Office 1** OU.
4. Move the **LON-CL1** computer to the **Branch Office 1** OU.
5. Open the Group Policy Management Console.
6. Create and link a new GPO named **Branch1** to the **Branch Office 1** OU.
7. Open the **Branch1** GPO for editing.
8. Edit the GPO to configure a mapped drive by using Group Policy preferences.
9. Map the S:\ drive to \\LON-dc1\Branch1.

#### ► Task 2: Edit the default Domain Policy with the required Group Policy preferences

1. Open the **Default Domain Policy** for editing.
2. Navigate to **User Configuration\Preferences\Windows Settings\Shortcuts**.
3. Create a new shortcut to the **Notepad.exe** program:
  - Name: **Notepad**
  - Action: **Create**
  - Location: **Desktop**
  - Target path: **C:\Windows\notepad.exe**
4. Target the preference for members of the **IT** security group.
5. Close all open windows.

► **Task 3: Test the preferences**

1. Switch to LON-CL1 and restart the computer.
2. Log in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Open the **Command Prompt** window, and then use the **gpupdate /force** command to refresh the Group Policy.
4. Log off of LON-CL1.
5. Log in to LON-CL1 as **Adatum\Holly** with the password **Pa\$\$w0rd**.
6. Verify that a drive is mapped to \\LON-DC1\Branch1.
7. Verify that the shortcut to Notepad is on Holly's desktop.
8. If the shortcut does not appear, repeat steps 2 through 5.
9. Log off of LON-CL1.

**Results:** After this exercise, you should have created the required scripts and preference settings successfully, and then assigned them by using Group Policy Objects (GPOs).

## **Exercise 2: Managing Microsoft Office 2013 by Using Administrative templates**

### **Scenario**

In order to manage the Office 2013 settings by using GPOs, you need to import the Office 2013 Administrative templates into a GPO. Then you need to verify that you can configure the settings and that the settings are being applied to target computers.

The main tasks for this exercise are as follows:

1. Import the Office 2013 Administrative templates
2. Configure Office 2013 settings
3. Verify that the settings have been applied

► **Task 1: Import the Office 2013 Administrative templates**

- On **LON-DC1**, copy the Office 2013 Administrative template files from the E:\Labfiles\Mod05\Office 2013 folder to the PolicyDefinitions folder.

► **Task 2: Configure Office 2013 settings**

1. On LON-DC1, create a new GPO named **Office 2013**.
2. Edit the **Office 2013** GPO by enabling the **Display Developer tab** in the ribbon setting.
3. Edit the **Office 2013** GPO by disabling the **Replace text as you type** setting.

► **Task 3: Verify that the settings have been applied**

1. Log in to LON-CL1 as Adatum\Holly.
2. Run **Microsoft Word** on LON-CL1.
3. Verify that the **Developer** tab is present and that Microsoft Word is not auto correcting misspelled words as you type.

**Results:** After this exercise, you should have successfully added the Microsoft® Office 2013 administrative template files to a GPO, customized Office 2013 settings, and validated the settings on a computer that is in the GPO scope.

## Exercise 3: Deploying Software by Using Group Policy

### Scenario

In order to provide employees with a standardized XML editor, you need to deploy Microsoft XML Notepad 2007 to all domain computers by using a GPO.

The main tasks for this exercise are as follows:

1. Deploy XML Notepad 2007 by using a new GPO
2. Verify that XML Notepad 2007 was successfully deployed on LON-CL1

► **Task 1: Deploy XML Notepad 2007 by using a new GPO**

1. On **LON-DC1**, create a new GPO named **Deploy XML Notepad**, and link it to the domain.
2. Edit the GPO and configure the computer assigned software deployment of **\LON-DC1-Mod05\xmlnotepad.msi**.

► **Task 2: Verify that XML Notepad 2007 was successfully deployed on LON-CL1**

1. Switch to LON-CL1, and then restart it.
2. Log in to **LON-CL1** after restarting, and then verify that **XML Notepad 2007** is installed.

**Results:** After this exercise, you should have successfully deployed XML Notepad 2007 to all domain-joined computers and verified the installation on LON-CL1.

## Exercise 4: Configuring Folder Redirection

### Scenario

In order to help minimize profile sizes, your manager has asked you to configure folder redirection for the branch office users. This will allow you to redirect several profile folders to each user's home drive.

The main tasks for this exercise are as follows:

1. Create a shared folder to store the redirected folders
2. Create a new GPO and link it to the Branch Office OU
3. Edit the folder redirection settings in the policy you created
4. Test the folder redirection settings
5. To prepare for the next module

► **Task 1: Create a shared folder to store the redirected folders**

- On LON-DC1, open **File Explorer**, and then create a folder and share it with **Specific people** by using the following properties:
  - Path: **C:\Branch1\Redirect**
  - Share name: **Branch1Redirect**
  - Permissions: **Everyone, Read/Write**

► **Task 2: Create a new GPO and link it to the Branch Office OU**

1. On LON-DC1, open Group Policy Management.
2. Create and link a new GPO named **Folder Redirection** to the **Branch Office 1** OU.

► **Task 3: Edit the folder redirection settings in the policy you created**

1. Open the **Folder Redirection** GPO for editing.
2. Under User Configuration, browse to Folder Redirection, and then configure the **Documents** folder properties to use the **Basic-Redirect everyone's folder to the same location** setting.
3. Ensure that the **Target folder** location is set to **Create a folder for each user under the root path**.
4. Specify the root path as **\LON-DC1\Branch1Redirect**.
5. Close all open windows on LON-DC1.

► **Task 4: Test the folder redirection settings**

1. Switch to LON-CL1.
2. Log in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Open the **Command Prompt** window, and then use the **gpupdate /force** command to refresh the Group Policy.
4. Log off, and then log in as **Adatum\Holly** with the password **Pa\$\$word**.
5. Browse to the desktop.
6. Right-click the desktop, and then use the **Personalize** menu to enable **User's Files** on the desktop.
7. From the Desktop, open the **Holly Dickson** folder.
8. Right-click **Documents**, and then click **Properties**.
9. In the **Document Properties** dialog box, note that the location of the folder is now the network share in a subfolder named for the user.
10. If the folder redirection is not evident, log off, and then log in as **Adatum\Holly** with the password **Pa\$\$word**. Repeat steps 7 to 9.
11. Log off of LON-CL1.

► **Task 5: To prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start Microsoft Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the Revert Virtual Machine dialog box, click **Revert**.
4. Repeat steps 2 and 3 for 20411D-LON-CL1.

**Results:** After this exercise, you should have successfully configured folder redirection to a shared folder on the LON-DC1 server.

**Question:** Which options can you use to separate a user's redirected folders to different servers?

**Question:** Can you name two methods you could use to assign a GPO to selected objects within an organizational unit (OU)?

**Question:** You have created Group Policy preferences to configure new power options. How can you ensure that they will be applied only to laptop computers?

# Lab: Installing and Configuring a Network Policy Server

## Scenario

A. Datum is a global engineering and manufacturing company with its head office in London, United Kingdom. An Information Technology (IT) office and data center located in London supports the London office and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

A. Datum is expanding its remote-access solution to the entire organization. This will require multiple VPN servers that are located at different points to provide connectivity for its employees. You are responsible for performing the tasks necessary to support these VPN connections.

## Objectives

After completing this lab, you will be able to:

- Install and configure NPS to support RADIUS.
- Configure and test a RADIUS client.

## Lab Setup

Estimated Time: 45 minutes

**Virtual Machines:** 20411D-LON-DC1, 20411D-LON-RTR, 20411D-LON-CL2

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20411D-LON-DC1**, and then, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Perform steps 2 through 4 for **20411D-LON-RTR** and **20411D-LON-CL2**.

## Exercise 1: Installing and Configuring NPS to Support RADIUS

### Scenario

You have been tasked with installing an NPS into the existing infrastructure to be used for RADIUS services. In this exercise, you will configure the RADIUS server with appropriate templates to help manage any future implementations. You also need to configure Accounting to log authentication information to a local text file on the server.

The main tasks for this exercise are as follows:

1. Install and Configure the Network Policy Server
2. Configure NPS Templates
3. Configure RADIUS Accounting

► **Task 1: Install and Configure the Network Policy Server**

1. Switch to LON-DC1.
2. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Using Server Manager, install the **Network Policy and Access Services** role by using default values to complete the installation wizard.
4. Open the **Network Policy Server** console, and then register the server in Active Directory.
5. Leave the Network Policy Server console open.

► **Task 2: Configure NPS Templates**

1. Create a new **Shared Secrets** template with the following properties:
  - Name: **Adatum Secret**
  - Shared secret: **Pa\$\$w0rd**
2. Create a new **RADIUS Clients** template with the following properties:
  - Friendly name: **LON-RTR**
  - Address (IP or DNS): **LON-RTR**
  - Shared Secret: Use **Adatum Secret** template
3. Leave the Network Policy Server console open.

► **Task 3: Configure RADIUS Accounting**

1. In the Network Policy Server console, launch the Accounting Configuration Wizard.
2. Choose the **Log to a text file on the local computer** option, and then use the default values to complete the wizard.
3. Leave the Network Policy Server console open.

**Results:** After this exercise, you should have enabled and configured Network Policy Server (NPS) to support Remote Authentication Dial-In User Service (RADIUS) in the required environment.

## **Exercise 2: Configuring and Testing a RADIUS Client**

### **Scenario**

You need to configure a server as a VPN server and a RADIUS client, including the client configuration, and then you need to modify the Network Policy settings.

The main tasks for this exercise are as follows:

1. Configure a RADIUS Client
2. Configure a Network Policy for RADIUS
3. Test the RADIUS Configuration
4. To Prepare for the Next Module

### ► Task 1: Configure a RADIUS Client

1. Create a RADIUS client by using the following property:
  - Template: **LON-RTR**
2. Leave the console open, and then switch to LON-RTR.
3. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
4. Open Routing and Remote Access, and **Disable Routing and Remote Access**.
5. Select **Configure and Enable Routing and Remote Access**.
6. Reconfigure LON-RTR as a VPN server:
  - **Ethernet 2** is the public interface
  - The VPN server allocates addresses from the pool: **172.16.0.100 > 172.16.0.110**
  - The server is configured with the option **Yes, set up this server to work with a RADIUS server**.
  - Primary RADIUS server: **LON-DC1**
  - Secret: **Pa\$\$w0rd**

The VPN service starts.

### ► Task 2: Configure a Network Policy for RADIUS

1. Switch to LON-DC1.
2. Switch to the Network Policy Server console.
3. Disable the two existing network policies. These will interfere with the processing of the policy that you are about to create.
4. Create a new Network Policy by using the following properties:
  - Policy name: **Adatum VPN Policy**
  - Type of network access server: **Remote Access Server(VPN-Dial up)**
  - Condition: **NAS Port Type = Virtual (VPN)**
  - Permission: **Access granted**
  - Authentication methods: default
  - Constraints: default
  - Settings: default

### ► Task 3: Test the RADIUS Configuration

1. Switch to LON-CL2 and sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Create a new VPN connection with the following properties:
  - Internet address to connect to: **10.10.0.1**
  - Destination name: **Adatum VPN**
  - Allow other people to use this connection: **true**

3. After you create the VPN, modify its settings by viewing the properties of the connection, and then selecting the **Security** tab. Use the following settings to reconfigure the VPN:
  - Type of VPN: **Point to Point Protocol (PPTP)**
  - Authentication: **Allow these protocols =Microsoft CHAP Version 2 (MS-CHAP v2)**
4. Test the VPN connection. Use the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**

#### ► Task 4: To Prepare for the Next Module

When you are finished with the lab, revert all virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start Microsoft Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-CL2**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20411D-LON-RTR** and **20411D-LON-DC1**.

**Results:** After this exercise, you should have deployed a VPN server, and then configured it as a RADIUS client.

**Question:** What does a RADIUS proxy provide?

**Question:** What is a RADIUS client, and what are some examples of RADIUS clients?

# Lab: Implementing Network Access Protection

## Scenario

A. Datum is a global engineering and manufacturing company with its head office in London, United Kingdom. An Information Technology (IT) office and data center in London support the head office and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

To help increase security and meet compliance requirements, A. Datum is required to extend their VPN solution to include NAP. You need to establish a way to verify and, if required, automatically bring client computers into compliance whenever they connect remotely by using the VPN connection. You will accomplish this goal by using NPS to create system health validation settings and network and health policies, and to configure NAP to verify and remediate client health.

## Objectives

After completing this lab, you will be able to:

- Configure NAP components.
- Configure VPN access.
- Configure the client settings to support NAP.

## Lab Setup

Estimated Time: 60 minutes

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-RTR, 20411D-LON-CL2

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, click **Administrative Tools**, and then double-click **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Perform steps 2 through 4 for **20411D-LON-CL2** and **20411D-LON-RTR**.

## Exercise 1: Configuring NAP Components

### Scenario

You should configure NAP components, such as certificate requirements, health and network policies, and connection-request policies as the first step in implementing compliance and security.

The main tasks for this exercise are as follows:

1. Configure Server and Client Certificate Requirements
2. Configure Health Policies

3. Configure Network Policies
4. Configure Connection Request Policies for VPN

► **Task 1: Configure Server and Client Certificate Requirements**

1. Switch to the LON-DC1 virtual server.
2. Open the **Certification Authority** tool.
3. In the Certificate Templates Console details pane, open the properties of the **Computer** certificate template.
4. On the **Security** tab, grant the **Authenticated Users** group the **Allow Enroll** permission.
5. Restart the Certification Authority.
6. Close the **Certification Authority** tool.

► **Task 2: Configure Health Policies**

1. Switch to the LON-RTR computer.
2. Create a management console by running **mmc.exe**.
3. Add the **Certificates** snap-in with the focus on the local computer account.
4. Navigate to the **Personal** certificate store and request a new certificate.
5. On the **Select Certificate Enrollment Policy** page, click **Active Directory Enrollment Policy**, and then click **Next**.
6. Enroll the **Computer** certificate that is listed.
7. Close the console, and do not save the console settings.
8. Using **Server Manager**, install the NPS Server with the following role services:
  - Network Policy Server
9. Open the Network Policy Server console.
10. Expand the **Network Access Protection** node to the **Windows Security Health Validator** node, and open the **Default Configuration**.
11. On the **Windows 8/Windows 7/Windows Vista** tab, clear all check boxes except **A firewall is enabled for all network connections**.
12. Create a health policy with the following settings:
  - Name: **Compliant**
  - Client SHV checks: **Client passes all SHV checks**
  - SHVs used in this health policy: **Windows Security Health Validator**
13. Create a health policy with the following settings:
  - Name: **Noncompliant**
  - Client SHV checks: **Client fails one or more SHV checks**
  - SHVs used in this health policy: **Windows Security Health Validator**

### ► Task 3: Configure Network Policies

1. Disable all existing network policies.
2. Configure a new network policy with the following settings:
  - Name: **Compliant-Full-Access**
  - Conditions: **Health Policies, Compliant**
  - Access permissions: **Access granted**
  - Settings: **NAP Enforcement, Allow full network access**
  - Authentication methods: **none**
  - Perform machine health check only: **Yes**
3. Configure a new network policy with the following settings:
  - Name: **Noncompliant-Restricted**
  - Conditions: **Health Policies, Noncompliant**
  - Access permissions: **Access granted**
  - Settings: **NAP Enforcement, Allow limited access** is selected, and **Enable auto-remediation of client computers** is not selected.
  - IP Filters: **IPv4 input filter**
    - Destination network: **172.16.0.10/255.255.255.255**
    - IPv4 output filter:
    - Source network: **172.16.0.10/255.255.255.255**
  - Authentication methods: **none**
  - Perform machine health check only: **Yes**

### ► Task 4: Configure Connection Request Policies for VPN

1. Disable existing connection request policies.
2. Create a new **Connection Request Policy** with the following settings:
  - Policy name: **VPN connections**
  - Type of network access server: **Remote Access Server (VPN-Dial up)**
  - Conditions, Tunnel type: **L2TP, SSTP, and PPTP**
  - Authenticate requests on this server: **Enabled**
  - On the **Specify Authentication Methods** page, perform the following:
3. Select **Override network policy authentication settings**.
4. Add **Microsoft: Protected EAP (PEAP)**.
5. Add **Microsoft: Secured password (EAP-MSCHAP v2)**.
6. Edit **Microsoft: Protected EAP (PEAP)** to ensure that **Enforce Network Access Protection** is enabled.

**Results:** After this exercise, you should have installed and configured the required Network Access Protection (NAP) components, created the health and network policies, and created the connection request policies.

## Exercise 2: Configuring Virtual Private Network Access

### Scenario

After configuring NAP, you will configure a VPN server, and then enable the PING protocol through the firewall for testing purposes.

The main tasks for this exercise are as follows:

1. Configure a VPN Server
2. Allow PING for Testing Purposes

#### ► Task 1: Configure a VPN Server

1. On LON-RTR, open **Routing and Remote Access**.
2. Disable Routing and Remote Access.
3. Select **Configure and Enable Routing and Remote Access**.
4. Use the following settings to complete configuration:
  - Select **Remote access (dial-up or VPN)**.
  - Select the **VPN** check box.
  - Select the interface named **Internet**, and clear the **Enable security on the selected interface by setting up static packet filters** check box.
  - Select **Ethernet** as the network selection.
  - Under **IP Address Assignment**, type **172.16.0.100** and **172.16.0.110** for the IP addresses respectively.
  - Complete the process by accepting defaults when you receive a prompt, and by clicking **OK** to confirm any messages.
5. In the Network Policy Server, click the **Connection Request Policies** node, and verify that the **Microsoft Routing and Remote Access Service Policy** is disabled. This was created automatically when Routing and Remote Access was enabled.
6. Close the Network Policy Server management console, and then close the Routing and Remote Access console.

#### ► Task 2: Allow PING for Testing Purposes

1. On LON-RTR, open **Windows Firewall with Advanced Security**.
2. Create an inbound rule with the following properties:
  - Type: **Custom**
  - All programs
  - Protocol type: Select **ICMPv4**, and then click **Customize**
  - Specific ICMP types: **Echo Request**
  - Default scope
  - Action: **Allow the connection**

- Default profile
  - Name: **ICMPv4 echo request**
3. Close the Windows Firewall with Advanced Security console.

**Results:** After this exercise, you should have created a VPN server and configured inbound communications.

## Exercise 3: Configuring the Client Settings to Support NAP

### Scenario

In this exercise, you will enable a client VPN to connect to the Adatum network. You then will enable and configure the required client-side NAP components.

The main tasks for this exercise are as follows:

1. Enable a Client NAP Enforcement Method
2. Establish a VPN Connection
3. To Prepare for the Next Module

#### ► Task 1: Enable a Client NAP Enforcement Method

1. Switch to the LON-CL2 computer.
2. Run the **NAP Client Configuration** tool (napclcfg.msc).
3. Under **Enforcement Clients**, enable the **EAP Quarantine Enforcement Client**.
4. Close the NAP Client Configuration tool.
5. Run **services.msc**, and then configure the **Network Access Protection Agent** service for automatic startup.
6. Start the service.
7. Close the services console.
8. Open the **Local Policy Editor** (gpedit.msc), and then enable the **Local Computer Policy/Computer Configuration/Administrative Templates/Windows Components/Security Center/Turn on Security Center (Domain PCs only)** setting.
9. Close the Local Group Policy Editor.

#### ► Task 2: Establish a VPN Connection

1. On LON-CL2, create a new VPN connection with the following properties:
  - Internet address to connect to: **10.10.0.1**
  - Destination name: **Adatum VPN**
  - Allow other people to use this connection: **Enable**
2. After you have created the VPN, modify its settings by viewing the properties of the connection, and then clicking the **Security** tab. Use the following settings to reconfigure the VPN:
  - Authentication type: **Microsoft: Protected EAP (PEAP) (encryption enabled)**
  - Properties of this authentication type:
    - Validate server certificate: **Disable**
    - Connect to these servers: **Disable**

- Authentication method: **Secured password (EAP-MSCHAP v2)**
  - Enable Fast Reconnect: **Disable**
  - Enforce Network Access Protection: **Enable**
3. Test the VPN connection:
    - In the **Network Connections** window, connect to the **Adatum VPN** connection
  4. At the command prompt, run **ipconfig /all** to verify that the **System Quarantine State is Not Restricted**.
  5. Ping **172.16.0.10**.
  6. Disconnect the Adatum VPN.
  7. Switch to LON-RTR.
  8. Open Network Policy Server.
  9. In the Default Configuration of the Windows Security Health Validator, enable the **Restrict access for clients that do not have all available security updates installed** option on the **Windows 8/Windows 7/Windows Vista** page.
  10. Switch back to LON-CL2, and then reconnect the VPN.
  11. Run the **ipconfig /all** command to verify that the **System Quarantine State is Restricted**.
  12. Disconnect the VPN.

### ► Task 3: To Prepare for the Next Module

When you are finished with the lab, revert all virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start Microsoft Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-CL2**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20411D-LON-RTR** and **20411D-LON-DC1**.

**Results:** After this exercise, you should have created a new VPN connection on LON-CL2, and have enabled and tested NAP on LON-CL2.

**Question:** The DHCP NAP enforcement method is the weakest enforcement method in Windows Server 2012. Why is it a less preferable enforcement method than other available methods?

**Question:** Could you use the remote access NAP solution alongside the IPsec NAP solution? What benefit would this scenario provide?

**Question:** Could you have used DHCP NAP enforcement for the client? Why or why not?

# Lab A: Implementing DirectAccess by Using the Getting Started Wizard

## Scenario

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

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

## Objectives

After completing this lab, you will be able to:

- Verify that the infrastructure is prepared for the DirectAccess deployment.
- Run the Getting Started Wizard.
- Validate the DirectAccess deployment.

## Lab Setup

Estimated Time: 30 minutes

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

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

**Virtual Machine(s):** 20411D-INET1

**User Name:** Administrator

**Password:** Pa\$\$w0rd

## Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20411D-LON-SVR1**, **20411D-LON-RTR**, and **20411D-LON-CL1**.
6. In Microsoft Hyper-V® Manager, click **20411D-INET1**, and, in the Actions pane, click **Start**.

7. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
8. Sign in using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$wOrd**

## Exercise 1: Verifying Readiness for a DirectAccess Deployment

### Scenario

Before you deploy DirectAccess, you need to ensure that the infrastructure is ready for the deployment.

The main tasks for this exercise are as follows:

1. Document the network configuration
  2. Verify the server readiness for DirectAccess
- Task 1: Document the network configuration

### Verify the IP Address on LON-DC1

1. Switch to LON-DC1.
2. Open Control Panel.
3. Open the **Ethernet Properties** dialog box.
4. Open the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
5. Document the current IP address, subnet mask, default gateway, and DNS configuration.

### Verify Network Configuration on LON-RTR

1. Switch to LON-RTR.
2. Open Server Manager, and then, from the Tools menu, open Routing and Remote Access.
3. In the Routing and Remote Access console, disable **Routing and Remote Access**. This step is necessary in order to disable the Routing and Remote Access that was preconfigured for this lab.
4. Open Control Panel.
5. Under the Network and Internet section, click **View network status and tasks**.
6. In the Network and Sharing Center window, click on **Change adapter settings**.
7. In the Network Connections window, verify that there are three network adapters: **Ethernet**, **Ethernet 2**, and **Internet**.
8. In the Network Connections window, disable, and then enable **Ethernet** adapter.
9. Repeat step 8 for **Internet** network connection.
10. Verify that **Ethernet** adapter is connected to the domain network **adatum.com**.
11. Open the **Ethernet Properties** dialog box.
12. Open the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
13. Verify that the IP address corresponds with the subnet used in the domain network. (The IP address should be **172.16.0.1**.)
14. Open the **Internet Properties** dialog box.

15. Open the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
16. Verify that IP address corresponds with the subnet used to simulate Internet connectivity. (The IP address should be **131.107.0.10**.)

 **Note:** If you notice that the Internet network adapter is connected to Adatum.com, disable Routing and Remote Access service (RRAS). This is because for DirectAccess, you will need at least one adapter to be on the external network.

### Verify Network Configuration on LON-CL1

1. Switch to LON-CL1.
2. Open Control Panel, click Network and Sharing Center and then click Change adapter settings.
3. Verify that the **Ethernet** adapter is connected to domain network **Adatum.com**.
4. Open the **Ethernet Properties** dialog box.
5. Open the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
6. Document the current IP address, subnet mask, default gateway, and DNS configuration.

### Verify Network Configuration on LON-SVR1

1. Switch to LON-SVR1.
2. Open **Control Panel**, and, under the Network and Internet section, select **View network status and tasks**, and then select **Change adapter settings**.
3. Verify that the **Ethernet** adapter is connected to domain network **Adatum.com**.
4. Open the **Ethernet Properties** dialog box.
5. Open the Internet Protocol Version 4 (TCP/IPv4) Properties dialog box.
6. Document the current IP address, subnet mask, default gateway, and DNS configuration.

### Verify Network Configuration on INET1

1. Switch to INET1.
2. Open Control Panel, then under the Network and Internet section, click **View network status and tasks** to open the Network Connections window.
3. Document the current IP address, subnet mask, and DNS configuration of the **Ethernet** adapter.

**Note:** The INET1 server role in this module is to simulate the Internet DNS server.

#### ► Task 2: Verify the server readiness for DirectAccess

1. On LON-DC1, open the Active Directory Users and Computers console, and create an OU with the name **DA\_Clients OU**. Inside that OU, create a Global Security group with the name **DA\_Clients**.
2. Add **LON-CL1** to the **DA\_Clients** security group.
3. Close the Active Directory Users and Computers console.

**Results:** After completing this exercise, you should have successfully verified the readiness for DirectAccess deployment.

## Exercise 2: Configuring DirectAccess

### Scenario

You have verified that the infrastructure is prepared for the DirectAccess deployment. A colleague has already installed the role on LON-RTR. You now need to configure DirectAccess on the DirectAccess server by using the Getting Started Wizard.

The main tasks for this exercise are as follows:

1. Configure DirectAccess by using the Getting Started Wizard

#### ► Task 1: Configure DirectAccess by using the Getting Started Wizard

1. Switch to LON-RTR.
2. In the Server Manager console, select **Remote Access Management**. Complete the Run the Getting Started Wizard in the Remote Access Management console with the following settings:
  - On the Configure Remote Access page, click Deploy DirectAccess only.
  - Verify that Edge is selected, and in the Type the public name or IPv4 address used by clients to connect to Remote Access server box, type 131.107.0.10.
  - On the **Remote Access Review** page, change remote clients to **DA\_Clients**.
  - Clear the Enable DirectAccess for mobile computers only check box.

**Results:** After completing this exercise, you should have successfully configured DirectAccess by using the Getting Started Wizard.

## Exercise 3: Validating the DirectAccess Deployment

### Scenario

Now that you have configured DirectAccess, you need to verify that DirectAccess is working. You will start by verifying the changes made by the Getting Started Wizard, and then you will verify that client computers can access the internal network by using DirectAccess.

The main tasks for this exercise are as follows:

1. Verify the GPO deployment
2. Test DirectAccess connectivity

#### ► Task 1: Verify the GPO deployment

1. Switch to LON-CL1.
2. When you configured the DirectAccess server, the wizard created two Group Policies and linked them to the domain. To apply them, restart LON-CL1, and then sign in as **Adatum\Administrator** by using the password **Pa\$\$wOrd**.
3. On LON-CL1, open the Command Prompt window, and then type **gpupdate /force** to force apply Group Policy.
4. At the command prompt, type **gpresult /R** to verify that the **DirectAccess Client Settings** GPO is applied to the Computer Settings.

**Note:** If the DirectAccess Client Settings GPO is not applied, restart LON-CL1, and then repeat Step 2 and Step 3 on LON-CL1.

5. Type the following command at the command prompt:

```
netsh name show effectivepolicy
```

and verify that following message displays DNS Effective Name Resolution Policy Table Settings

**Note:** DirectAccess settings are inactive when this computer is inside a corporate network.

6. Simulate moving the client computer **LON-CL1** out of the corporate network and to the Internet, by disabling the **Ethernet** network adapter and enabling the **Ethernet 2** network adapter, which is configured with following values:

- IP address: **131.107.0.20**
- Subnet mask: **255.255.0.0**
- Preferred DNS server: **131.107.0.100**

7. Close all open windows.

## ► Task 2: Test DirectAccess connectivity

### Verify Connectivity to the Internal Network Resources

1. Switch to LON-CL1.
2. On the taskbar, start **Internet Explorer**.
3. In the Address bar, type **http://lon-svr1.adatum.com**, and then press Enter. The default Internet Information Services (IIS) 8.0 web page for LON-SVR1 displays. **Note:** If the default Internet Information Services (IIS) 8.0 web page for LON-SVR1 doesn't appear, restart LON-CL1. After LON-CL1 restarts, sign in as **Adatum\Administrator** and repeat steps 2 and 3 again.
4. Leave the Windows Internet Explorer® window open.
5. On the Start screen, type **\LON-SVR1\Files**, and then press **Enter**. Note that you are able to access the folder content.
6. Close all open windows.
7. Move the mouse pointer to the lower-right corner of the screen, in the notification area, click **search**, and then, in the **search** box, type **cmd**.
8. At the command prompt, run the **ipconfig command**.

Notice the IP address for Tunnel adapter iphttpsinterface starts with **2002**. This is an IP-HTTPS address.

### Verify Connectivity to the DirectAccess Server

1. At the command prompt, type the following command:

```
Netsh name show effectivepolicy
```

Verify that **DNS Effective Name Resolution Policy Table Settings** presents two entries for **adatum.com** and **Directaccess-NLS.Adatum.com**.

2. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Get-DAClientExperienceConfiguration
```

Notice the DirectAccess client settings.

### Verify Client Connectivity on DirectAccess Server

1. Switch to LON-RTR.
2. In the **Remote Access Management** console pane, click **Remote Client Status**.  
Notice that Client is connected via **IP-HTTPS**. In the Connection Details pane, in the bottom-right of the screen, note the use of Kerberos for the Machine and the User.
3. Close all open windows.



**Note:** After completing the lab, do not revert the virtual machines.

**Results:** After completing this exercise, you should have successfully verified that client computers can access the internal network by using DirectAccess.

**Question:** Why did you create the DA\_Clients group?

**Question:** How will you configure IPv6 addresses for client computers running the Windows® 8 operating system to use DirectAccess?

# Lab B: Deploying an Advanced DirectAccess Solution

## Scenario

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

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

## Objectives

After completing this lab, you will be able to:

- Prepare the infrastructure for the advanced DirectAccess deployment.
- Implement the advanced DirectAccess infrastructure.
- Validate the DirectAccess deployment.

## Lab Setup

Estimated Time: 60 minutes

**Virtual Machine(s):** 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-RTR, 20411D-LON-CL1, 20411D-LON-CL3

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

**Virtual Machine(s):** 20411D-INET1

**User Name:** Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20411D-LON-SVR1**, **20411D-LON-RTR**, **20411D-LON-CL3**, and **20411D-LON-CL1**.
6. In Microsoft Hyper-V® Manager, click **20411D-INET1**, and, in the Actions pane, click **Start**.
7. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
8. Sign in using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**

## Exercise 1: Preparing the Environment for DirectAccess

### Scenario

As the first step in implementing the advanced DirectAccess solution, you need to prepare the network infrastructure. You will configure an internal network location server, and then configure and distribute the required certificates.

The main tasks for this exercise are as follows:

1. Configure the AD DS and DNS requirements
2. Configure CRL distribution
3. Configure client certificate distribution
4. Configure the network location server and DirectAccess server certificates

#### ► Task 1: Configure the AD DS and DNS requirements

##### Edit the Security Group for DirectAccess Client Computers

1. Switch to LON-DC1.
2. Open the Active Directory Users and Computers console, and then in the OU named **DA\_Clients OU**, modify the membership of the **DA\_Clients** group to include **LON-CL3** and **LON-CL1**.
3. Close the Active Directory Users and Computers console.

##### Create Required DNS Records

1. Open the DNS Manager console, and then create new host records with the following settings:
  - Name: **nls**; IP Address: **172.16.0.21**
  - Name: **crl**; IP Address: **172.16.0.1**
2. Close the DNS Manager console.

**Note:** The **NLS** record will be used by the client to determine the network location.

**Note:** The **CRL** record will be used by the internal clients to check the revocation status on the certificates that are used in DirectAccess.

##### Remove ISATAP from the DNS Global Query Block List

1. Open the Command Prompt window, type the following command, and then press Enter:

```
dnscmd /config /globalqueryblocklist wpad
```

Ensure that the **Command completed successfully** message appears.

2. Close the Command Prompt window.

##### Configure the DNS Suffix on LON-RTR

1. Switch to LON-RTR, and in the **Internet Properties** dialog box, open the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, open the **Advanced TCP/IP Settings** dialog box, and then add the **Adatum.com** DNS suffix.
2. Close the **Internet Properties** dialog box.

**Note:** The Internet client needs this suffix when resolving names for internal resources.

## ► Task 2: Configure CRL distribution

### Configure Certificate Requirements

**Note:** The following steps will be performed to prepare the CA with proper extensions for the CRL distribution point, which will be included in the future certificates that will be used by the CA.

1. Switch to LON-DC1, and then open the Certification Authority console.
2. Configure the **AdatumCA** certification authority with the following extension settings:
  - Add Location: **http://crl.adatum.com/crl/**
  - Variable: **CAName, CRLNameSuffix, DeltaCRLAllowed**
  - Location: type .crl at the end of the Location string
  - Select **Include in CRLs. Clients use this to find Delta CRL locations and Include in the CDP extension of issued certificates**
  - Do not restart Certificate Services.
  - Add Location: **\LON-RTR\crldist\$\  
Variable: CAName, CRLNameSuffix, DeltaCRLAllowed**
  - Location: type .crl at the end of the Location string.
  - Select **Publish CRLs to this location** and select **Publish Delta CRLs to this location**.
  - Restart Certificate Services.
  - Close the Certificate Authority console.

### Export Root Certificate

**Note:** In following steps, you will export the root certificate because it will be required in Labs C and D for configuring VPN and Web Application Proxy.

1. In Certification Authority, open the **Properties** of **AdatumCA**.
2. On the **General** tab, click **View Certificate**. In the Certificate window, click the **Details** tab, and then click **Copy to File** to start the **Certificate Export Wizard**.
3. Select the **DER encoded binary x.509 (.CER)** format for exporting the certificate, and then store the certificate in the **c:\Root.cer** file.
4. Close the Certification Authority console.

## ► Task 3: Configure client certificate distribution

### Configure Computer Certificate Autoenrollment

1. On LON-DC1, open the Group Policy Management console.
2. In the console tree, navigate to **Forest: Adatum.com, Domains, and Adatum.com**.
3. Edit the Default Domain Policy, and then in the console tree of the Group Policy Management Editor, navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**.
4. Under Automatic Certificate Request Settings, configure **Automatic Certificate Request** to issue the Computer certificate.
5. Close the Group Policy Management Editor and close the Group Policy Management console.

## ► Task 4: Configure the network location server and DirectAccess server certificates

### Request a Certificate for LON-SVR1

1. On LON-SVR1, open a command prompt, type the following command, and then press Enter:

```
gpupdate /force
```

2. At the command prompt, type the following command, and then press Enter:

```
mmc
```

3. Add the **Certificates** snap-in for **Local computer**.
4. In the console tree of the Certificates snap-in, navigate to **Certificates (Local Computer)\Personal\Certificates**, request a new certificate, and then under Request Certificates, configure the **Adatum Web Certificate** with the following setting:
  - Subject name: Under **Common name**, type **nls.adatum.com**.
5. In the details pane of the Certificates snap-in, verify that a new certificate with the name **nls.adatum.com** is enrolled with **Intended Purposes of Server Authentication**.
6. Close the console. When you are prompted to save settings, click **No**.

### Change the HTTPS Bindings

**Note:** In following steps you will configure the https bindings for the host name nls.adatum.com that will be used by the clients to determine their network location.

1. Open the Internet Information Services (IIS) Manager console.
2. In the console tree of the Internet Information Services (IIS) Manager, navigate to **LON-SVR1/Sites**, and then click **Default Web site**.
3. Configure Site Bindings by selecting **nls.adatum.com** as **SSL Certificate**.
4. Close the Internet Information Services (IIS) Manager console.

### Configure DirectAccess Server with the Appropriate Certificate

1. Switch to LON-RTR.
2. Open a command prompt, and then refresh group policy by typing **gpupdate /force**.
3. Open Microsoft Management Console by typing **mmc**, and then add the **Certificates** snap-in for **Local computer**.
4. In the **Certificates** snap-in, in the mmc console, request a new certificate with the following settings:
  - Certificate template: **Adatum Web Certificate**
  - Common name: **131.107.0.10**
  - Friendly name: **IP-HTTPS Certificate**
5. Close the console.

**Note:** Instead of issuing a certificate with the IP address in the subject name, in a real-world environment, you can use the FQDN of the Internet facing server that will be reachable by the external client.

## Create a CRL Distribution Point on LON-RTR

1. Switch to Server Manager.
2. In Internet **Information Services (IIS) Manager**, create a new virtual directory named **CRLD**, enable browsing for the **CRLD** directory, and then assign **c:\crldist** as a home directory.
3. Using the Internet Information Services (IIS) Manager configuration editor, locate the **Section** drop-down list, and then navigate to **system.webServer\security\RequestFiltering**.
4. In the middle pane of the console, locate the **allowDoubleEscaping** entry, change the value from **False** to **True**, and then apply the changes.
5. Close Internet Information Services (IIS) Manager.

**Note:** You need to modify the value of **allowDoubleEscaping** to allow clients to access CRL deltas that will have a plus sign (+) appended to the filename.

## Share and Secure the CRL Distribution Point

1. Open File Explorer.
2. In the details pane of File Explorer, configure the following permissions for **CRLDist\$** share name:
  - Grant Full Share and file permission to the LON-DC1 computer.

## Publish the CRL to LON-RTR

This step makes the CRL available on the edge server for Internet-based DirectAccess clients.

1. Switch to LON-DC1.
2. Start the **Certification Authority** console.
3. In the console tree, open **AdatumCA**, right-click **Revoked Certificates**, point to **All Tasks**, click **Publish**, and then choose the **New CRL** option.
4. On the taskbar, start the File Explorer.
5. In File Explorer, open the following location: **\LON-RTR\CRLDist\$**
6. In File Explorer, notice the **AdatumCA** files.
7. Close File Explorer.

**Results:** After completing this exercise, you will have prepared the environment for implementing advanced DirectAccess infrastructure.

## Exercise 2: Implementing the Advanced DirectAccess Infrastructure

### Scenario

Now that you have prepared the environment, you can modify the DirectAccess configuration to use the advanced infrastructure components.

The main tasks for this exercise are as follows:

1. Modify the DirectAccess deployment
2. Verify the server and GPO configuration

## ► Task 1: Modify the DirectAccess deployment

### Configure the Remote Access Role

1. On LON-RTR, open the **Server Manager** console.
2. In the **Server Manager** console, start the **Remote Access Management** console, click **DirectAccess and VPN**, and **complete the Remote Access Setup Wizard** by performing the following steps.
3. In the details pane of the Remote Access Management console, under step 1, click **Edit**, and then specify the following:
  - Select Groups: Verify that **DA\_Clients** (ADATUM\DA\_Clients) **group is listed**.
  - **Network Connectivity Assistant – Delete the current resource, and add following resource:** <https://nls.adatum.com>
4. In the details pane of the **Remote Access Management** console, under **step 2**, click **Edit**.
5. On the **Network Topology** page, verify that **Edge** is selected, and type **131.107.0.10**.
6. On the **Network Adapters** page, **clear** selection for **Use a self-signed certificate created automatically by DirectAccess**, and notice that there are two certificates named **131.107.0.10**, one that is self-signed and the second one that is issued by **Adatum.com**. Ensure that you choose the certificate **131.107.0.10** that is issued by AdatumCA and is used as a certificate to authenticate IP-HTTPS connections.
7. On the **Authentication** page, select **Use computer certificates**, click **Browse**, and then select **AdatumCA**.
8. Select Enable Windows 7 client computers to connect via DirectAccess, and then click **Finish**.
 

**Note:** You need to enable certificate authentication with certificates issued from a trusted CA to support Windows 7 clients.
9. In details pane of the Remote Access Management console, under **Step 3**, click **Edit**.
10. On the **Network Location Server** page, select **The network location server is deployed on a remote web server (recommended)**; in the Type in the URL of the network location server box, type <https://nls.adatum.com>, and then click **Validate**. Ensure that the URL is validated.
11. On the **DNS** page, ensure that **nls.adatum.com** is listed, and also add the following entry in the NRPT table: **crl.adatum.com**.
12. On the **Management** page, click **Finish**.
13. In details pane of the **Remote Access Management** console, display the settings for **Step 4**.
14. On the **DirectAccess Application Server Setup** page, review the settings, and then click **Finish**.
15. In the **details pane of the Remote Access Management console**, click **Finish**.
16. On the Remote Access Review page, click **Apply**.
17. In the **Applying Remote Access Setup Wizard Settings dialog box**, click **Close**.

## ► Task 2: Verify the server and GPO configuration

On the Start screen, open the command prompt, type the following commands, and then press Enter:

```
gpupdate /force
Ipconfig
```

Verify that LON-RTR has an IPv6 address for Tunnel adapter IP-HTTPS Interface starting with **2002**.

**Results:** After completing this exercise, you will have implemented the advanced DirectAccess infrastructure.

## Exercise 3: Validating the DirectAccess Deployment

### Scenario

With the advanced DirectAccess infrastructure in place, you now need to test the deployment. You will verify that both Windows 8 and Windows 7 clients can connect to the internal network by using DirectAccess.

The main tasks for this exercise are as follows:

1. Verify Windows 8 client connectivity
2. Verify Windows 7 client connectivity
3. Monitor client connectivity

#### ► Task 1: Verify Windows 8 client connectivity

##### Verify DirectAccess Group Policy Configuration Settings for Windows 8 Clients

1. Simulate moving the client computer **LON-CL1 back from the public network to the intranet network**, by disabling the **Ethernet 2** network adapter and enabling the **Ethernet** network adapter.
2. On LON-CL1, in the Command Prompt window, type the following commands, and then press Enter:

```
gpupdate /force
gpresult /R
```

**Note:** If an error message appears, restart LON-CL1, and perform step 2 again.

3. If you are still not able to connect, perform following steps:
  - On LON-CL1, open the Registry Editor window, navigate to **HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\DNSPolicyConfig**, and then notice the three entries starting with DA.
  - In the Registry Editor window, in the navigation pane, delete each of the entries starting with DA, and then close the Registry Editor window.

**Note:** These registry settings you just deleted are from the previous labs and they might cause problems for verifying Windows 8 client connectivity. This is why you are deleting them.

  - Restart **LON-CL1** and perform steps from 1 through 3 to verify connectivity to the default IIS 8.0 web page on LON-SVR1.
4. Verify that **DirectAccess Client Settings GPO** is displayed in the list of the Applied Group Policy Objects for the Computer Settings.

### Verify Client Computer Certificate Distribution

1. On LON-CL1, open the **Certificates** MMC.
2. Verify that a certificate with the name **LON-CL1.adatum.com** is present with **Intended Purposes of Client Authentication and Server Authentication**. If there is no certificate issued, restart LON-CL1. After LON-CL1 restarts, sign in as **Adatum\Administrator** and at the command prompt run the **gpupdate /force** command again.
3. Close the console without saving it.

## Verify IP Address Configuration

1. On LON-CL1, open Internet Explorer, and then navigate to <http://lon-svr1.adatum.com/>. The default Internet Information Services (IIS) 8.0 web page for LON-SVR1 appears.
2. In Internet Explorer, go to <https://nls.adatum.com/>. The default IIS 8.0 web page for LON-SVR1 appears.
3. Open File Explorer, type `\\\Lon-SVR1\Files`, and then press Enter. You should see a folder window with the contents of the **Files** folder.
4. Close all open windows.

## Move the Client Computer to the Internet Virtual Network

1. Switch to LON-CL1.
2. Simulate moving the client computer **LON-CL1** out of the corporate network, and to the Internet, by disabling the **Ethernet** network adapter and enabling **Ethernet 2** network adapter.
3. Close the Network Connections window.

## Verify Connectivity to the DirectAccess Server

1. On LON-CL1, open a command prompt, and type the following command:

```
ipconfig
```
2. Notice the IP address that starts with **2002**. This is an IP-HTTPS address.
3. If you notice that there is no IP address for **iphttpsinterface**, type the following commands, restart the computer, and then repeat steps 1 and 2:

```
Netsh interface teredo set state disabled
Netsh interface 6to4 set state disabled
```

**Note:** In this lab setup, IP-HTTPS connectivity on the firewall is enabled and other connectivity methods from the client, such as the Teredo or 6to4 tunneling protocol, are disabled. If you are planning to use the Teredo or 6to4 tunneling protocol in the production environment, you do not have to disable them.

4. At the command prompt, type the following command, and then press Enter:

```
Netsh name show effectivepolicy
```

Verify that **DNS Effective Name Resolution Policy Table Settings** is present in the three entries for **adatum.com**, **crl.adatum.com**, and **nls.adatum.com**.
5. At the command prompt, type the following command, and then press Enter:

```
powershell
```
6. At the Windows PowerShell command prompt, type the following command, and then press Enter:

```
Get-DAClientExperienceConfiguration
```

Notice the DirectAccess client settings.

## Verify Connectivity to the Internal Network Resources

1. On the taskbar, open Internet Explorer, and then go to <http://lon-svr1.adatum.com/>. You should see the default IIS 8.0 web page for LON-SVR1.
2. Open File Explorer, type `\\\LON-SVR1\Files`, and then press Enter.

3. You should see a folder window with the contents of the Files folder.
4. At the command prompt, type the following command:

```
ping lon-dc1.adatum.com
```

5. Verify that you are receiving replies from LON-DC1.adatum.com.
6. At the command prompt, type the following command, and then press Enter:

```
gpupdate /force
```

7. Close all open windows.
8. Switch to LON-RTR.
9. Start the **Remote Access Management** console and review the information on **Remote Client Status**.

Notice that LON-CL1 is connected via IP-HTTPS. In the Connection Details pane, in the bottom-right of the screen, note the use of Machine Certificate, and User Kerberos.

 **Note:** When establishing the infrastructure tunnel, NTLMv2 authentication is used to authenticate the computer account that connects to the DirectAccess server. When establishing the intranet tunnel, Kerberos authentication is used for authenticating the user.

10. Close all open windows.

## ► Task 2: Verify Windows 7 client connectivity

### Verify DirectAccess Group Policy Configuration Settings for Windows 7 Clients

1. Switch to LON-CL3.
2. Restart LON-CL3, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**. If a dialog box displays with information that Windows needs to be restarted for the second time, restart LON-CL3 again, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Open the Command Prompt window, type the following commands, and then press Enter:

```
gpupdate /force
gpresult /R
```

4. Verify that the **DirectAccess Client Settings GPO** is displayed in the list of the Applied Group Policy Objects for the Computer Settings.
5. If the policy is not being applied, run the **gpupdate /force** command again. If the policy is still not being applied, restart the computer. After the computer restarts, sign in as **Adatum\Administrator** and run the **Gpresult /R** command again.

### Verify Client Computer Certificate Distribution

1. On LON-CL3, open the **Certificates** MMC.
2. Verify that a certificate with the name **LON-CL3.adatum.com** is present with **Intended Purposes of Client Authentication and Server Authentication**.
3. Close the console window without saving it.

## Verify IP Address Configuration

1. On LON-CL3, open Internet Explorer, and then navigate to <http://lon-svr1.adatum.com/>. The default IIS 8.0 web page for LON-SVR1 appears.
2. In Internet Explorer, navigate to <https://nls.adatum.com/>. The default IIS 8.0 web page for LON-SVR1 appears.
3. Open File Explorer, type `\\\Lon-SVR1\Files`, and then press Enter. You should see a folder window with the contents of the **Files** folder.
4. Close all open windows.

## Move the Client Computer to the Internet Virtual Network

1. Switch to LON-CL3.
2. Simulate moving the client computer **LON-CL1** out of the corporate network, and to the Internet, by disabling **Internal** network adapter and enabling **Internet** network adapter.
3. Close the Network Connections window.

## Verify Connectivity to the DirectAccess Server

1. On LON-CL3, open a command prompt, and type the following command:

```
ipconfig
```
2. Notice the IP address that starts with **2002**. This is an IP-HTTPS address.  
**Note:** If you notice that there is no IP address for iphttpsinterface, type the following commands, and then repeat step 2:

```
Netsh interface teredo set state disabled
Netsh interface 6to4 set state disabled
```

Verify the IP address for Tunnel adapter iphttpsinterface which starts with 2002. This is an IP-HTTPS address.

3. At the command prompt, type the following command, and then press Enter:

```
Netsh name show effectivepolicy
```

Verify that **DNS Effective Name Resolution Policy Table Settings** is present in three entries for **adatum.com**, **crl.adatum.com**, and **nls.Adatum.com**.

## Verify Connectivity to the Internal Network Resources

1. On the taskbar, open Internet Explorer, and navigate to <http://lon-svr1.adatum.com/>. You should see the default IIS 8.0 web page for LON-SVR1.
2. Open File Explorer, type `\\\LON-SVR1\Files`, and then press Enter.
3. You should see a folder window with the contents of the Files folder.
4. At the command prompt, type the following command:

```
ping lon-dc1.adatum.com
```

5. Verify that you are receiving replies from LON-DC1.adatum.com, and notice that the IPv6 address of LON-DC1 is resolved. This is because DirectAccess configures a GPO with firewall settings that allow IPv6 ICMP echo replies and not IPv4 ICMP echo replies.

6. At the command prompt, type the following command, and then press Enter:

```
gpupdate /force
```

7. Close all open windows.
8. Switch to LON-RTR.
9. Start the **Remote Access Management** console and review the information on **Remote Client Status**.

Notice that LON-CL3 is connected via IP-HTTPS. If there is still information in central pane that LON-CL3 is connected with 6to4, from the **Task** pane click **Refresh** once again. 6to4 information should disappear because 6to4 was disabled in Step 4 of the previous section in this task.

10. Close all open windows.

#### ► **Task 3: Monitor client connectivity**

1. Switch to LON-RTR.
2. Open the Remote Access Management console, and then in the left pane, click **Dashboard**.
3. Review the information in the central pane, under DirectAccess and VPN Client Status.
4. In the left pane, click **Remote Client Status**, and then in the central pane, review the information under the Connected Clients list.
5. In the left pane, click **Reporting**, and then, in the central pane, click **Configure Accounting**.
6. In the Configure Accounting window, under Select Accounting Method, click **Use inbox accounting**, click **Apply**, and then click **Close**.
7. In the central pane, under Remote Access Reporting, review the options for monitoring historical data.



**Note:** After completing the lab, do not revert the virtual machines.

**Results:** After completing this exercise, you will have verified that both Windows 8 and Windows 7 clients can connect to the internal network by using DirectAccess.

**Question:** Why did you make the CRL available on the edge server?

**Question:** Why did you install a certificate on the client computer?

# Lab C: Implementing VPN

## Scenario

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

## Objectives

After completing this lab, you will be able to:

- Implement VPN.
- Validate the VPN deployment.

Estimated Time: 45 minutes

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

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

## Exercise 1: Implementing VPN

### Scenario

The first step in implementing VPN is to modify the remote access server configuration to provide VPN connectivity. You need to ensure that the clients can connect to the server by using IKEv2 and SSTP.

The main tasks for this exercise are as follows:

1. Review the default VPN configuration
2. Verify certificate requirements for IKEv2 and SSTP
3. Configure the remote access server

#### ► Task 1: Review the default VPN configuration

1. Switch to LON-RTR.
2. In the Remote Access Management console, from the Actions pane, select **Enable VPN**.
3. In the Routing and Remote Access console, verify that 128 ports exist for SSTP, IKEv2, PPTP, and L2TP. Modify the number of ports for each type of connection to **5**.
4. In the Routing and Remote Access console, verify that:
  - IPv4 Remote Access Server is selected.
  - SSL Certificate Binding Certificate 131.107.0.10 is selected.
  - EAP is selected as authentication protocol.
  - VPN server is configured to assign IPv4 addressing by using Dynamic Host Configuration Protocol (DHCP).
5. Close the Routing and Remote Access console.

► **Task 2: Verify certificate requirements for IKEv2 and SSTP**

1. Switch to LON-RTR.
2. On the Start screen, open an MMC console, and then add the **Certificates – Computer Account** snap-in.
3. In the Certificates console, verify that certificate 131.107.0.10 has Intended Purpose for Server Authentication (this is required for SSTP and IKEv2 VPN connectivity).
4. Close the console without saving changes.

► **Task 3: Configure the remote access server**

1. On LON-RTR, from Server Manager, open the Network Policy Server console.
2. In the Network Policy Server console, in the navigation pane, expand **Policies**, and then click **Network Policies**.
3. Disable existing network policies and create a new network policy with following settings:
  - Policy name: **VPN Policy**
  - Type of network access server: Remote Access Server(VPN-Dial up)
  - Windows Groups: IT
  - Specify Access Permission: Access granted
  - Configure Authentication Methods: Clear the Microsoft Encrypted Authentication (MS-CHAP) check box, add Microsoft Secured password (EAP-MSCHAP v2), and then Microsoft: Smart Card or other certificate.
4. Complete the wizard by accepting the default settings on the other pages of the wizard.

**Results:** After completing this exercise, you will have modified the remote access server configuration to provide VPN connectivity.

## Exercise 2: Validating the VPN Deployment

### Scenario

Now that you have deployed the VPN solution, you will verify that the clients that cannot connect using DirectAccess can connect using VPN. You also want to test the offline domain join feature in DirectAccess.

The main tasks for this exercise are as follows:

1. Remove the client computer from the domain
2. Verify that DirectAccess does not work
3. Configure a VPN connection and verify connectivity
4. Rejoin the computer to the domain by using DirectAccess offline domain join
5. Verify DirectAccess connectivity

► **Task 1: Remove the client computer from the domain**

1. Switch to LON-CL1.
2. Open Control Panel.

3. In Control Panel, remove LON-CL1 from the Adatum.com domain, and add LON-CL1 to a workgroup named WORKGROUP.
4. If prompted for username and password in the **Windows Security** dialog box, for username type **Administrator**, for password type **Pa\$\$w0rd**, and then click **OK**.
5. Restart **LON-CL1**.

► **Task 2: Verify that DirectAccess does not work**

1. When the LON-CL1 computer restarts, sign in with the user name **Admin** and password **Pa\$\$w0rd**.
2. Open **Internet Explorer**, in the Address bar, type **https://nls.adatum.com/**, and then press **Enter**. Notice that you are unable to open the website.
3. Leave the Internet Explorer window open.
4. On the taskbar, open **File Explorer**, type **\Lon-SVR1\Files**, and then press Enter. Notice that the Network Error message appears.
5. Close all open windows.

**Note:** The client is unable to open the resource by using DirectAccess because this feature is not available for workgroup computers.

► **Task 3: Configure a VPN connection and verify connectivity**

1. On LON-CL1, open the Control Panel.
2. In Control Panel, start the Set up a new connection or network wizard with following settings:
  - Choose a connection option: Connect to a workplace
  - How do you want to connect: Use my Internet connection (VPN)
  - Do you want to set up Internet connection before continuing: I'll set up an Internet connection later
  - Internet address: 131.107.0.10
  - Destination name: Adatum VPN, select the Allow other people to use this connection checkbox, and then clear the Remember my credentials checkbox.
  - Configure Adatum VPN connection to allow following protocol: Microsoft CHAP version 2 (MS-CHAP v2).
3. Open the Adatum VPN connection, and then sign in with user name **Adatum\Danielle** and password **Pa\$\$w0rd**.
4. Verify that you are now connected to Adatum by using the PPTP connection.

**Note:** To verify the type of connection, you can view the status of the connection in the Network Connections window in **Control Panel**. By default, the client will attempt to connect to the VPN server by using a secure connection such as L2TP with IPsec, IKEv2, or SSTP. In this case, however, because the client does not have a computer certificate or a preshared key, an L2TP or IKEv2 connection could not be established. An SSTP connection could not be established because this connection requires that the client trusts the certificate on the VPN server. Therefore, the only possible connection in this case is PPTP with the CHAP v2 authentication.

**Note:** If you are unable to connect, restart LON-CL1 and then perform step 9 again.

**Note:** In the following steps, you will import the certificate of AdatumCA in Trusted Root Certification Authorities so that the clients that trust the certificate on the VPN server establish a VPN connection by using the SSTP protocol.

5. Open File Explorer, open \\172.16.0.10\C\$, and then install the Root.cer certificate on LON-CL1 to Local Machine by choosing the Place all certificates in the Trusted Root Certification Authorities option.
6. On the Start screen, open a command prompt, open an MMC console, and then add the **Certificate - Local Computer** snap-in.
7. In the Certificates console, in the navigation pane, navigate to **Trusted Root Certification Authorities\Certificates** and then verify that the **AdatumCA** certificate exists.
8. Switch to the Network and Sharing Center, and then open the **Adatum VPN Properties** dialog box; on the **Security** tab, select **IKEv2** and **Use Extensible Authentication Protocol (EAP)**.
9. Disconnect the Adatum VPN and connect once again.
10. Open the Adatum VPN connection, and then sign in with user name **Adatum\Danielle** and password **Pa\$\$w0rd**.
11. Verify that now the connection is established by using the IKEv2 protocol.
12. Open the Adatum VPN Properties dialog box, and then on the Security tab, select Secure Socket Tunneling Protocol (SSTP) and Use Extensible Authentication Protocol (EAP).
13. Disconnect the Adatum VPN, connect again with the Adatum VPN connection, and then if the **Network sign-in** dialog box appears, sign in with the user name **Adatum\Danielle** and password **Pa\$\$w0rd**.
14. Verify that now the connection is established by using SSTP protocol.
15. Disconnect the **Adatum VPN** connection.

► **Task 4: Rejoin the computer to the domain by using DirectAccess offline domain join**  
 Provision Computer Account Data in Active Directory

1. Switch to LON-DC1.
2. Open Server Manager, and then, from the **Tools** menu, open the Group Policy Management console.
3. In the Group Policy Management console, open the DirectAccess Client Settings console, in the Details pane, select the entire Unique ID string, including the braces, right-click, and then click **Copy**. Record the Unique ID for the GPO. Copy the Unique ID to Notepad.
4. Minimize the Group Policy Management console.
5. Open the Windows PowerShell window, and then type the following commands:

```
Djoin.exe /provision /domain adatum.com /machine LON-CL1 /savefile client.txt
/policynames "DirectAccess Client Settings" /POLICYPATHS
"c:\windows\SYSVOL\sysvol\adatum.com\policies\[unique ID of Group Policy Object
copied in previous step]\Machine\Registry.pol" /reuse
```

6. At the Windows PowerShell command prompt, type the following command:

```
Copy .\client.txt C:\
```

Note: You are copying the Client.txt file to C:\ which will be accessed to the VPN client via the Internet. This allows the client computer to download the file and use the Djoin.exe command to run the file to perform an offline domain join.

## Add the Client Computer to the DA\_Clients Group

- At the Windows PowerShell command prompt, type the following command:

```
Add-ADGroupMember -Identity DA_Clients -Members LON-CL1$
```

 **Note:** No output or confirmation displays. You can use the Active Directory Administrative Center to confirm that the CLIENT computer account was added to the DA\_Clients group.

## Configure the Client by Using the Offline Domain Join File

- Switch to LON-CL1, and then connect to **LON-RTR** by using VPN SSTP connection you created in previous task. If the **Windows Security** dialog box appears, sign in with the username **Adatum\Danielle** and password **Pa\$\$w0rd**.
- Open the **File Explorer**, connect to address **\\"172.16.0.10\\c\$**, copy the **client.txt** file, on **LON-CL1**, create a folder named **Client File**, and then paste the file **client.txt** into the folder **Client File**.

 **Note:** You run djoin.exe from the **c:\\windows** folder because the client.txt file that contains the AD DS blob is located in the **c:\\windows** folder.

- On LON-CL1, start the **Command Prompt (Admin)**, in the Administrator: Command Prompt window, type the following commands, and then press Enter after each command:

```
copy "c:\\Client File\\client.txt" c:\\windows
Cd..
Djoin.exe /requestodj /loadfile client.txt /windowspath C:\\Windows /localos
```

- At the command prompt, type the following command, and then press Enter to restart **LON-CL1**:

```
Shutdown /t 0 /r /f
```

### ► Task 5: Verify DirectAccess connectivity

- When the computer restarts, sign in with the user name **Adatum\Administrator** and password **Pa\$\$w0rd**.
- On LON-CL1, open **Internet Explorer**, and in the Address bar, type **http://lon-svr1.adatum.com/**. The default IIS 8.0 web page for LON-SVR1 displays.
- In the Address bar, type **https://nls.adatum.com/**, and then press Enter. Notice that you are unable to open the website.
- Close Internet Explorer.
- On the taskbar, click **File Explorer**, and then open **\\\\LON-SVR1\\Files**. Notice that you can access the Network share.
- At the command prompt, type **ipconfig**, and then press Enter. Notice the IP address for Tunnel adapter iphttpsinterface that starts with **2002**. This is an IP-HTTPS address.
- Close all open windows.

 **Note:** After completing the lab, do not revert the virtual machines.

**Results:** After completing this exercise, you will have verified that the clients that cannot connect by using DirectAccess can now connect by using VPN.

**Question:** In the lab, you configured the VPN server to allocate an IP address configuration by using a static pool of addresses. Is there a way to automate IP configuration?

**Question:** Why was DirectAccess not working when we removed LON-CL1 from the Adatum.com domain?

# Lab D: Implementing Web Application Proxy

## Scenario

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

## Objectives

After completing this lab, you will be able to:

- Implement Web Application Proxy.
- Validate the Web Application Proxy deployment.

**Estimated Time:** 30 minutes

**Virtual Machine(s):** 20411D-LON-DC1, 20411D-LON-SVR1, **20411D-LON-SVR4**, 20411D-LON-RTR, 20411D-LON-CL1

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

**Virtual Machine(s):** 20411D-INET1

**User Name:** Administrator

**Password:** Pa\$\$w0rd

## Exercise 1: Implementing Web Application Proxy

### Scenario

You need to implement Web Application Proxy to enable external users to access applications at A. Datum. The initial deployment will be used as a proof-of-concept while the developers at A. Datum modify the internal applications to use claims-based authentication.

The main tasks for this exercise are as follows:

1. Install the Web Application Proxy role service
2. Configure access to an internal website

#### ► Task 1: Install the Web Application Proxy role service

1. Switch to LON-RTR.
2. Open Server Manager from the Start screen, and then on the **Dashboard** page, click **Add roles and features**.
3. In the Add Roles and Features Wizard, on the **Select server roles** page, expand **Remote Access**, and then select **Web Application Proxy**.

## ► Task 2: Configure access to an internal website

### Obtain Certificate for the ADFS1 Farm

- Open an MMC console, add the **Certificates - Computer account** snap-in, and then request a new certificate with the following settings:
  - Subject Name: Common Name adfs1.adatum.com
  - Alternative name: DNS adfs1.adatum.com, lon-svr1.adatum.com, enterpriseregistration.adatum.com.

### Configure Bindings for the Website on LON-SVR1

1. Switch to LON-SVR1.
2. In the console tree of Internet Information Services (IIS) Manager, navigate to **LON-SVR1/Sites**, and then click **Default Web site**.
3. Configure Site Bindings by entering **lon-svr1.adatum.com** as a host name, and then selecting **lon-svr1.adatum.com** as **SSL Certificate**.
4. Close the Internet Information Services (IIS) Manager console.

### Configure Web Application Proxy

1. Switch to LON-RTR.
2. From Server Manager, open the Remote Access Management console, and in the navigation pane, click **Web Application Proxy**, and then run the Web Application Proxy Configuration Wizard.
3. In the Web Application Proxy Configuration Wizard, for **Federation service name**, enter the FQDN of the federation service: **adfs1.adatum.com**.
4. In the User name and Password boxes, enter Administrator and Pa\$\$w0rd.
5. On the **AD FS Proxy Certificate** page, in the list of certificates currently installed on the Web Application Proxy server, select a certificate to be used by Web Application Proxy for AD FS proxy functionality, **adfs1.adatum.com**.
6. On the **Results** page, verify that the configuration was successful, and then close the wizard.
7. If you receive an error message, switch to **LON-SVR4**, and then ensure that all services that are configured to start automatically are started. If not, start the services manually. Repeat steps from 1 through 6.

**Note:** If you are not able to start **Device Registration Service**, switch to LON-SVR4 and in **Windows PowerShell** window, run the following cmdlets:

```
update-adfscertificate -CertificateType: Token-Signing -Urgent:$True
update-adfscertificate -CertificateType: Token-Decrypting -Urgent:$True
```

Restart LON-SVR4 and repeat steps from 1 to 6.

### Publish Internal Website

1. On the Web Application Proxy server, in the Remote Access Management console, in the navigation pane, start the Publish New Application Wizard.
2. On the Preauthentication page, select Pass-through.
3. In the **Name** box, enter a friendly name for the application, **LON-SVR1 Web**.
4. In the **External URL** box, enter the external URL for this application, **https://lon-svr1.adatum.com**.

5. In the **External certificate** list, select the certificate **adfs1.adatum.com**.
6. In the **Backend server URL** box, ensure that **https://lon-svr1.adatum.com** is listed. Note that this value is automatically entered when you enter the external URL.
7. On the **Confirmation** page, review the settings, and then click **Publish**.
8. On the **Results** page, ensure that the application published successfully, and then click **Close**.

### Configure Internal Website Authentication

1. Switch to **LON-SVR1**.
2. From Server Manager, open the Internet Information Services (IIS) Manager console.
3. In the Internet Information Services (IIS) Manager console, navigate to **Default Web Site**.
4. Configure Authentication for the Default Web Site with following settings:
  - Windows Authentication - Enabled.
  - Anonymous Authentication – Disabled.
5. Close the Internet Information Services (IIS) Manager console.

**Results:** After completing this exercise, you will have implemented Web Application Proxy.

## Exercise 2: Validating the Web Application Proxy Deployment

### Scenario

Now that you have deployed the Web Application Proxy role service, you need to verify that external users can access the internal application through the proxy.

The main tasks for this exercise are as follows:

1. Disable DirectAccess on client computer
2. Verify access to the internal website from the client computer
3. To prepare for the next module

#### ► Task 1: Disable DirectAccess on client computer

In this task, the LON-CL1 computer will be removed from the domain. Because DirectAccess works for domain members only, removing a computer from the domain will disable DirectAccess on LON-CL1. DirectAccess is disabled so that LON-CL1 connects to an internal website by using Web Application Proxy, and not by using DirectAccess.

1. Switch to LON-CL1.
2. Open Control Panel.
3. In Control Panel, remove LON-CL1 from the adatum.com domain, and add LON-CL1 to a workgroup named WORKGROUP.
4. If prompted for username and password in the Windows Security dialog box, for username type **Administrator**, for password type **Pa\$\$w0rd**, and then click **OK**.
5. Restart LON-CL1.

► **Task 2: Verify access to the internal website from the client computer**

1. Switch to LON-CL1, and sign in with the username **Admin** and password **Pa\$\$w0rd**.
2. On LON-CL1, open Internet Explorer, and then type the following address **https://lon-svr1.adatum.com**.
3. When prompted, in the **Internet Explorer** dialog box type **Adatum\Bill** for username and **Pa\$\$w0rd** for password, click **OK**, and then verify that the default IIS 8.0 web page for LON-SVR1 opens.
4. If you are unable to connect to **https://lon-svr1.adatum.com**, restart **LON-CL1** and then perform steps from 1 through 3.
5. If you are still not able to connect, perform following steps:
  - On LON-CL1, open the Registry Editor window, navigate to **HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\DNSPolicyConfig**, and then notice the three entries starting with DA.
  - In the Registry Editor window, in the navigation pane, delete each of the entries starting with DA, and then close the Registry Editor window.
  - **Note:** These registry settings you just deleted are from the previous labs and they might cause problems for Web Application Proxy. This is why you are deleting them.
  - Restart **LON-CL1** and perform steps from 1 through 3 to verify connectivity to the default IIS 8.0 web page on LON-SVR1.

► **Task 3: To prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start Microsoft **Hyper-V® Manager**.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20411D -LON-SVR1**, **20411D-LON-SVR4**, **20411D-LON-RTR**, **20411D-INET**, **20411D-LON-CL3**, and **20411D-LON-CL1**.

**Results:** After completing this exercise, you will have verified that external users are able to access the internal application through the Web Application Proxy.

**Question:** Where should we deploy the Web Application Proxy server?

**Question:** What is required for a client to be able to access a published application?

## Module Review and Takeaways



### Best Practices:

- Although DirectAccess was present in previous Windows 7 and Windows 2008 R2 editions, Windows 8 introduces new features for improved manageability, ease of deployment, and improved scale and performance.
- Monitoring of the environment is now much easier with Windows PowerShell, Windows Management Instrumentation (WMI), and GUI monitoring, along with Network Connectivity Assistant on the client side.
- One of the best enhancements is that DirectAccess can now access IPv4 servers on your network and your servers do not need to have IPv6 addresses to be exposed through DirectAccess, because your DirectAccess server acts as a proxy.
- For ease of deployment, you do not need to have IP addresses on the Internet-facing network. Therefore, this is a good scenario for proof-of-concept. However, if you are concerned about security and if you want to integrate with Network Access Protection (NAP), you still need two public addresses.
- Consider integrating DirectAccess with your existing Remote Access solution because Windows Server 2012 can implement DirectAccess server behind the NAT device, which is the most common remote access server solution for organizations.

### Common Issues and Troubleshooting Tips

| Common Issue                                                                                                                                   | Troubleshooting Tip |
|------------------------------------------------------------------------------------------------------------------------------------------------|---------------------|
| You have configured DirectAccess, but users are complaining about connectivity issues. You want to troubleshoot those issues more efficiently. |                     |
| The DirectAccess client tries to connect to the DirectAccess server by using IPv6 and IPsec with no success.                                   |                     |

### Review Question(s)

**Question:** What remote access solutions can you deploy by using Windows Server 2012 R2?

**Question:** What are the main benefits of using DirectAccess for providing remote connectivity?

**Question:** How do you configure DirectAccess clients?

**Question:** How does the DirectAccess client determine if it is connected to the intranet or the Internet?

**Question:** What is the benefit of an NRPT?

**Question:** What type of remote access solutions you can provide by using VPN in Windows Server 2012?

**Question:** What type of applications you can publish by using Web Application Proxy in Windows Server 2012 R2?

# Lab A: Configuring Quotas and File Screening Using File Server Resource Manager

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, England. An IT office and data center in London support the London location and other locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

Each network client within the Adatum domain is provided with a server-based home folder that is used for storing personal documents or files that are works-in-progress. It has come to your attention that home folders are becoming quite large, and may contain file types such as MP3 files that are not approved under corporate policy. You decide to implement FSRM quotas and file screening to help address this issue.

## Objectives

After completing this lab, you will be able to:

- Configure FSRM quotas.
- Configure file screening and generate a storage report.

## Lab Setup

Estimated Time: 30 minutes

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, double-click **Administrative Tools**, and then double-click **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Perform steps 2 through 4 for **20411D-LON-SVR1**.

## Exercise 1: Configuring File Server Resource Manager Quotas

### Scenario

You are implementing FSRM quotas to control the size of home folders. Each home folder is limited to 100 MB. To ensure that administrators are made aware of home folders that are running out of space, an event is written to the event log when a user exceeds 85 percent of their storage quota so that it can be tracked by administrators.

The main tasks for this exercise are as follows:

1. Create a quota template
2. Configure a quota based on the quota template
3. Test that the quota is functional

► **Task 1: Create a quota template**

1. On LON-SVR1, from Server Manager, install the **File Server Resource Manager**.
2. In the File Server Resource Manager console, use the Quota Templates node to configure a template that sets a hard limit of 100 MB as the maximum folder size.
3. Configure the template to record an event in the Event Log when the folder reaches 85 percent capacity and 100 percent capacity.

► **Task 2: Configure a quota based on the quota template**

1. Use the File Server Resource Manager console and the Quotas node to create a quota on the **E:\Labfiles\Mod09\Users** folder by using the quota template that you created in Task 1.
2. Configure the quota to auto apply on existing and new subfolders.
3. Create an additional folder named **Max** in the **E:\Labfiles\Mod09\Users** folder, and ensure that the new folder is listed in the quotas list in File Server Resource Manager.

► **Task 3: Test that the quota is functional**

1. Open a Windows PowerShell window, and use the following commands to create a file in the **E:\Labfiles\Mod09\Users\Max** folder. Press Enter after each of the three commands:

```
E:
cd \Labfiles\Mod09\Users\Max fsutil file createnew file1.txt 89400000
```

2. Check the Event Viewer for an **Event ID of 12325**.
3. Test that the quota works by attempting to create a file that is **16,400,000 bytes**, and then press Enter:

```
fsutil file createnew file2.txt 16400000
```

4. Notice that the file cannot be created. The message returned from Windows references disk space, but the file creation fails because it would exceed the quota limit. Close the Windows PowerShell window.
5. Close all open windows on LON-SVR1.

**Results:** After completing this exercise, you should have configured a File Server Resource Manager (FSRM) quota.

## Exercise 2: Configuring File Screening and Storage Reports

### Scenario

Managers are concerned that large media files are being stored in home folders, a practice that violates corporate policy. Managers want to prevent media files such as video, audio, and graphics files from being saved. You need to implement file screening to prevent media files from being stored in home folders. However, you have also been made aware that several users store Microsoft Project files with the

extension .mpp in their home directories. You must ensure that the file screen you create does not restrict the storage of these files.

You have also been asked to provide a report to your manager documenting any attempts to save restricted media files on LON-SVR1.

The main tasks in this exercise are:

- Create a file group.
- Create a file screen template.
- Create a file screen.
- Test the file screen.
- Generate an on-demand storage report.

The main tasks for this exercise are as follows:

1. Create a file screen
2. Create a file group
3. Test the file screen
4. Generate an on-demand storage report
5. To prepare for the next lab

► **Task 1: Create a file screen**

1. On LON-SVR1, open File Server Resource Manager.
2. Create a **File Screen** based on the Block Audio and Video Files file screen template for the E:\Labfiles\Mod09\Users directory.

► **Task 2: Create a file group**

1. On LON-SVR1, open the **File Server Resource Manager Configuration Options** dialog box, and, on the **File Screen Audit** tab, enable the **Record file screening activity in auditing database** option.



**Note:** This step allows recording of file screening events. These recordings will supply data for a File Screen Audit report, which you will run later in this exercise.

2. Create a new File Group with the following properties:
  - File group name: **MPx Media Files**
  - Files to include: **\*.mp\***
  - Files to exclude **\*.mpp**
3. Modify the **Block Audio and Video Files** template to use only the **MPx Media Files** file group.

► **Task 3: Test the file screen**

1. On the taskbar, click the **File Explorer** shortcut.
2. Create a new text document in **E:\Labfiles\Mod09**, and then rename it as **musicfile.mp3**.
3. Copy **musicfile.mp3** into **E:\Labfiles\Mod09\Users**. You will be notified that the system was unable to copy the file.

► **Task 4: Generate an on-demand storage report**

1. Open the **File Server Resource Manager** console.
2. Right-click **Storage Reports Management**, select **Generate Reports Now**, and then provide the following parameters:
  - Generate only the **File Screening Audit** report
  - Report on **E:\Labfiles\Mod09\Users**
3. Review the generated reports in Internet Explorer.
4. Close all open windows on LON-SVR1.

► **Task 5: To prepare for the next lab**

When you finish the lab, do not shut down the virtual machines. You will need them for the next lab.

**Results:** After completing this exercise, you will have configured file screening and storage reports in FSRM.

**Question:** What criteria do you need to meet to use FSRM for managing a server's file structure?

**Question:** In what ways can classification management and file-management tasks decrease administrative overhead when dealing with a complex file and folder structure?

# Lab B: Implementing Distributed File System

## Scenario

A. Datum Corporation has deployed a new branch office. This office has a single server. To support the requirements of a branch staff, you must configure DFS. To avoid performing backups remotely, a departmental file share in the branch office will be replicated back to the head office for centralized backup, and branch data files will be replicated to the branch server to provide quicker access.

## Objectives

After completing this lab, you will be able to:

- Install the DFS role service.
- Configure a DFS namespace.
- Configure DFS Replication.

## Lab Setup

Estimated Time: 45 minutes

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-SVR4

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the virtual machines that are still running from the last lab and 20411D-LON-SVR4. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20411D-LON-SVR4**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**

## Exercise 1: Installing the DFS Role Service

### Scenario

To support the creation of a replicated namespace, your managers have asked you to perform the installation of the DFS server role for LON-SVR1 and LON-SVR4.

The main tasks for this exercise are as follows:

1. Install the DFS role service on LON-SVR1
2. Install the DFS role service on LON-SVR4

#### ► Task 1: Install the DFS role service on LON-SVR1

- On LON-SVR1, from Server Manager, under the File and Storage Management role, install the DFS Namespaces and DFS Replication role services.

#### ► Task 2: Install the DFS role service on LON-SVR4

- On LON-SVR4, in Server Manager, under the File and Storage Management role, install the DFS Namespaces and DFS Replication role services.

**Results:** After completing this exercise, you will have installed the Distributed File System (DFS) role service on LON-SVR1 and installed the DFS role service on LON-SVR4.

## Exercise 2: Configuring a DFS Namespace

### Scenario

You have been asked to configure a DFS namespace to support the newly requested file structure at Adatum.com. Management has requested that the new structure include a file share on LON-SVR4 called ResearchTemplates and a file share on LON-SVR1 called DataFiles. Your notes include:

- Namespace: \\Adatum.com\BranchDocs
- File shares to include:
  - \\LON-SVR4\ResearchTemplates
  - \\LON-SVR1\DataFiles

The main tasks for this exercise are as follows:

1. Create the BranchDocs namespace
2. Enable access-based enumeration for the BranchDocs namespace
3. Add the ResearchTemplates folder to the BranchDocs namespace
4. Add the DataFiles folder to the BranchDocs namespace
5. Verify the BranchDocs namespace

#### ► Task 1: Create the BranchDocs namespace

1. Switch to LON-SVR1 and then open Server Manager.
2. Open **DFS Management**.
3. Create a new namespace with the following properties:
  - Server: **LON-SVR1**
  - Name: **BranchDocs**
  - Namespace type: **Domain-based namespace**, and select **Enable Windows Server 2008 mode**
4. Under the Namespaces node, verify that the namespace has been created.

#### ► Task 2: Enable access-based enumeration for the BranchDocs namespace

- In DFS Management, in the \\Adatum.com\BranchDocs Properties dialog box, on the **Advanced** tab, select the **Enable access-based enumeration for this namespace** check box.

#### ► Task 3: Add the ResearchTemplates folder to the BranchDocs namespace

- Add a new folder to the BranchDocs namespace:
  - Folder name: **ResearchTemplates**
  - Add a folder target:
    - Path: \\LON-SVR4\ResearchTemplates
    - Create share

- Local path: **C:\BranchDocs\ResearchTemplates**
- Permissions: **All users have read and write permissions**

► **Task 4: Add the DataFiles folder to the BranchDocs namespace**

- Add a new folder to the **BranchDocs** namespace:
  - Folder name: **DataFiles**
  - Add a folder target:
    - Path: **\LON-SVR1\DataFiles**
    - Create share
    - Local path: **C:\BranchDocs\DataFiles**
    - Permissions: **All users have read and write permissions**

► **Task 5: Verify the BranchDocs namespace**

1. On LON-SVR1, open File Explorer, in the address bar, type **\Adatum.com\BranchDocs\**, and then press Enter.
2. Verify that both **ResearchTemplates** and **DataFiles** display, and then close the window.

**Results:** After completing this exercise, you will have configured a DFS namespace.

## Exercise 3: Configuring DFS Replication

### Scenario

You have been asked to ensure that the files contained in the new DFS namespace are replicated to both LON-SVR1 and LON-SVR4 to ensure data availability.

The main tasks for this exercise are as follows:

1. Create another folder target for DataFiles
2. Configure replication for the namespace
3. Verify DFS Replication
4. To prepare for the next module

► **Task 1: Create another folder target for DataFiles**

1. In DFS Management, expand **Adatum.com\BranchDocs**, and then click **DataFiles**.
2. In the details pane, notice that there is currently only one folder target.
3. Add a new folder target:
  - Path to target: **\LON-SVR4\DataFiles**
  - Create share
  - Local path: **C:\BranchDocs\DataFiles**
  - Permissions: **All users have read and write permissions**
  - Create folder
4. In the **Replication** dialog box, click **Yes**. The Replicate Folder Wizard starts.

► **Task 2: Configure replication for the namespace**

1. Complete the Replicate Folder Wizard:
  - Primary member: **LON-SVR1**
  - No topology
  - Use defaults elsewhere, and accept any messages.
2. Create a new replication topology for the namespace:
  - Type: **Full mesh**
  - Schedule and bandwidth: Use default settings
3. In the details pane, on the **Memberships** tab, verify that the replicated folder displays on both LON-SVR4 and LON-SVR1.

► **Task 3: Verify DFS Replication**

1. Switch to **LON-DC1**.
2. Map a network drive to **\\\Adatum.com\BranchDocs**.
3. Check the **BranchDocs properties DFS** tab to determine which server the volume is currently referring to.
4. Open the **Datafiles** folder, and create a new text document.
5. Add the text “**Hello World**”, and then save and close the file.
6. Switch to LON-SVR1, and force DFS Replication from LON-SVR1 to LON-SVR4.
7. Shut down **LON-SVR1**.
8. Switch to **LON-DC1**, and then attempt to open the **New Text Document** in the **Datafiles** folder.

► **Task 4: To prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start Microsoft Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat these steps for **20411D-LON-SVR1** and **20411D-LON-SVR4**.

**Results:** After completing this exercise, you will have configured DFS Replication.

**Question:** What are the requirements for deploying a namespace in Windows Server 2008 mode?

**Question:** What are the benefits of hosting a namespace on several namespace servers?

# Lab: Configuring Encryption and Advanced Auditing

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with a head office based in London, England. An IT office and data center are located in London to support the London location and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure.

You have been asked to configure the Windows Server 2012 environment to protect sensitive files, and to ensure that access to files on the network is audited appropriately. You also have been asked to configure auditing for the new server.

## Objectives

After completing this lab, you will be able to:

- Use BitLocker to secure data drives.
- Encrypt and recover files by using EFS management tools.
- Configure advanced auditing.

## Lab Setup

**Estimated Time:** 40 minutes

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-CL1, and 20411D-LON-SVR1

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, press the Windows key, click **Administrative Tools**, and then double-click **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20411D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Log in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Perform steps 2 through 4 for **20411D-LON-SVR1** and **20411D-LON-CL1**.

## Exercise 1: Using BitLocker® Drive Encryption to Secure Data Drives

The main tasks for this exercise are as follows:

1. Use Group Policy to Prepare the Server for Implementing BitLocker
2. Enable BitLocker for a Data Drive
3. Move the Data Drive to Another Server
4. Recover the Data

► Task 1: Use Group Policy to Prepare the Server for Implementing BitLocker

1. On LON-DC1, modify Group Policy by enabling the Choose how BitLocker-protected fixed drives can be recovered option. Ensure that the checkbox next to the Save BitLocker recovery information to AD DS for fixed data drives option is selected, click the Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives option, and then click OK.
2. On LON-SVR1, run the **gpupdate /force** command.
3. Restart LON-SVR1.

► Task 2: Enable BitLocker for a Data Drive

**Add the BitLocker Drive Encryption feature**

1. On LON-SVR1, add the BitLocker Drive Encryption feature and any required role services.
2. Restart LON-SVR1 to complete the process.

**Turn on BitLocker, and then validate that BitLocker is encrypting the data volume**

1. On LON-SVR1, turn on BitLocker for the F: volume, and then use the password option for unlocking the volume at startup.
2. For backing up the recovery key, save the recovery key locally to the E:\Labfiles\Mod10 folder.
3. Restart LON-SVR1 to complete the process.

After restarting, log in to LON-SVR1, and then run the **manage-bde -status** command to view the status of the F: volume. The F: volume should show "Protection On" as the protection status.

► Task 3: Move the Data Drive to Another Server

1. On LON-SVR1, remove the SCSI hard drive named 20411D-LON-SVR1-Encrypted.vhdx.
2. On LON-DC1, add D:\Program Files\Microsoft Learning\20411\Drives\20411D-LON-SVR1\20411D-LON-SVR1-Encrypted.vhdx as a SCSI hard drive.
3. Bring the added hard drive online on LON-DC1.

► Task 4: Recover the Data

1. On LON-DC1, double-click the F: drive from File Explorer.
2. In the BitLocker window, click **More options**.
3. Acquire the BitLocker recovery key from the LON-SVR1 computer object in Active Directory Users and Computers.
4. Type the BitLocker recovery key into the BitLocker window to unlock the drive.
5. In File Explorer, verify that the unlocked icon displays and that the hard drive is accessible.

**Results:** After completing this exercise, you will have configured Group Policy for BitLocker, enabled BitLocker on a data drive, moved the data drive to a different server, and then prepared for recovering data from the drive.

## Exercise 2: Encrypting and Recovering Files

### Scenario

Your organization wants to allow users to encrypt files with EFS. However, there are concerns about recoverability. To enhance the management of the certificates that are used for EFS, you will configure an

internal CA to issue certificates to users. You will also configure a recovery agent for EFS and verify that the recovery agent can recover files. The recovery consists of opening a file to validate that the recovery agent can view the contents. In a real-world scenario, most likely you would need to recover the file from a backup prior to the recovery agent accessing it. However, this step is not part of this lab.

The main tasks for this exercise are as follows:

1. Update the Recovery Agent Certificate for the Encrypting File System (EFS)
2. Update Group Policy on the Computers
3. Obtain a Certificate for EFS
4. Encrypt a File
5. Use the Recovery Agent to Open the File

► **Task 1: Update the Recovery Agent Certificate for the Encrypting File System (EFS)**

1. On LON-DC1, from Server Manager, open the Group Policy Management console.
2. Edit the **Default Domain Policy** that is linked to **Adatum.com**.
3. In the Group Policy Management Editor, browse to **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Encrypting File System**.
4. In the **Encrypting File System** folder, delete the existing **Administrator** certificate.
5. Create a new **Data Recovery Agent**.
6. Read the information about the new certificate, and then verify that it was issued by AdatumCA.

► **Task 2: Update Group Policy on the Computers**

1. On LON-DC1, at the Windows PowerShell command prompt, run **gpupdate /force**.
2. On LON-CL1, open a command prompt, and then run **gpupdate /force**.
3. Sign out of LON-CL1.

► **Task 3: Obtain a Certificate for EFS**

1. On LON-CL1, log in as **Adatum\Doug** with a password of **Pa\$\$w0rd**.
2. Run **mmc.exe** to open an empty MMC.
3. Add the **Certificates** snap-in to the MMC.
4. In the MMC, right-click **Personal**, and then request a new certificate.
5. Select a **Basic EFS** certificate.
6. Verify that the new certificate was issued by AdatumCA.
7. Close the console, and do not save the changes.

► **Task 4: Encrypt a File**

1. On LON-CL1, browse to **\LON-DC1\Mod10Share\Marketing**.
2. Open the properties of **DougFile**.
3. Enable encryption in the advanced attributes for only the **DougFile**.
4. Close File Explorer.
5. Sign out of LON-CL1.

► **Task 5: Use the Recovery Agent to Open the File**

1. On LON-DC1, browse to **E:\Labfiles\Mod10\Mod10Share\Marketing**.
2. Open **DougFile.txt**, modify the contents, and then save the file.

**Results:** After completing this exercise, you will have encrypted and recovered files.

## Exercise 3: Configuring Advanced Auditing

### Scenario

Your manager has asked you to track all access to file shares that are on LON-SVR1. You also need to be aware of any time a user accesses a file on a removable storage device that is attached to the server. You have decided to implement the appropriate object access settings by using Advanced Audit Policy Configuration.

The main tasks for this exercise are as follows:

1. Create a Group Policy Object (GPO) for Advanced Auditing
2. Verify Audit Entries
3. To Prepare for the Next Module

► **Task 1: Create a Group Policy Object (GPO) for Advanced Auditing**

1. On LON-DC1, from Server Manager, open **Active Directory Users and Computers**.
2. Create a new organizational unit (OU) in **Adatum.com** named **File Servers**.
3. Move **LON-SVR1** from the **Computers** container to the **File Servers** OU.
4. On LON-DC1, open Group Policy Management.
5. Create a new GPO named **File Audit**, and link it to the **File Servers** OU.
6. Edit the **File Audit** GPO, and then under Computer Configuration, browse to the **Advanced Audit Policy Configuration\Audit Policies\Object Access** node.
7. Configure both the **Audit Detailed File Share** and **Audit Removable Storage** settings to record Success and Failure events.
8. Restart LON-SVR1, and then log in as **Adatum\Administrator** with a password of **Pa\$\$w0rd**.

► **Task 2: Verify Audit Entries**

1. Log in to LON-CL1 as **Adatum\Allan** with a password of **Pa\$\$w0rd**.
2. Open File Explorer, and then navigate to **\LON-SVR1\Mod10**.
3. Open **testfile** in Notepad, and then close Notepad.
4. Switch to LON-SVR1.
5. Open **Event Viewer**, and then view the Audit Success events in the Security Log.
6. Double-click one of the log entries with a **Source of Microsoft Windows security auditing**, and a **Task Category of Detailed File Share**.
7. Click the **Details** tab, and then note the access that was performed.

### ► Task 3: To Prepare for the Next Module

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat these steps for **20411D-LON-SVR1** and **20411D-LON-CL1**.

**Results:** After completing this exercise, you will have configured advanced auditing.

**Question:** In Exercise 3, Task 1, why were you asked to generate a new data recovery agent certificate by using the AdatumCA CA?

**Question:** What are the benefits of placing servers in an OU and then applying audit policies to that OU?

**Question:** What is the reason for applying audit policies across the entire organization?

# Lab: Using Windows Deployment Services to Deploy Windows Server 2012

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, England. An IT office and data center are in London to support the head office and other branch locations. A. Datum has recently deployed a Windows Server 2012 R2 server and client infrastructure.

A. Datum is deploying servers to branch offices throughout the region for the Research department. Management selected you to automate this deployment. You suggest using Windows Deployment Services to deploy Windows Server 2012 R2 to the branch offices. Management has sent you some instructions by email regarding the deployment. You must read these instructions, and then install and configure Windows Deployment Services to support the deployment.

## Objectives

**After completing this lab, you will be able to:**

- Install and configure Windows Deployment Services.
- Create operating system images using Windows Deployment Services.
- Configure custom computer naming.
- Deploy images with Windows Deployment Services.

## Lab Setup

**Estimated Time:** 75 minutes

**Virtual Machines:** 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-SVR3

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Log on using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Perform steps 2 through 4 for **20411D-LON-SVR1**.
6. Do not start 20411D-LON-SVR3 until directed to do so.

## Exercise 1: Installing and Configuring Windows® Deployment Services

### Scenario

To assist with the process of configuring Windows Deployment Services, you have received an email with the appropriate configuration information.

## Branch Office Deployment Guide

- **Requirements Overview.** Configure Windows Deployment Services to aid in the deployment of branch office servers.
- **Additional Information.** Deployment method: Automated standard image deployments.
- **Configuration information:**
  - LON-SVR1 will host Windows Deployment Services.
  - Configure multicast transmission to use Auto-cast.
  - Configure automatic naming to identify branch servers.
  - Place branch servers in the Research OU.
  - Perform a Server Core installation.

The main tasks for this exercise are as follows:

1. Read the supporting documentation
2. Install the Windows Deployment Services role
3. Configure Windows Deployment Services
  - ▶ Task 1: Read the supporting documentation
    - Read the supporting documentation in the Exercise Scenario to determine the deployment details.
  - ▶ Task 2: Install the Windows Deployment Services role
    1. Switch to the **LON-SVR1** computer.
    2. Open **Server Manager**.
    3. Install the **Windows Deployment Services** server role with both role services.
    4. Close **Server Manager**.
  - ▶ Task 3: Configure Windows Deployment Services
    1. Open the **Windows Deployment Services** console.
    2. Right-click **LON-SVR1.Adatum.com**, and then click **Configure Server**.
    3. Use the following information to complete configuration:
      - a. Integrate Windows Deployment Services with AD DS.
      - b. On the **Remote Installation Folder Location** page, accept the defaults.
      - c. Accept the **System Volume Warning** message.
      - d. On the **PXE Server Initial Settings** page, select the **Respond to all client computers (known and unknown)** option.
      - e. When prompted, choose not to add images to the server.

**Results:** After completing this exercise, you will have installed and configured Windows Deployment Services to deploy the Windows Server 2012 operating system.

## Exercise 2: Creating Operating System Images with Windows Deployment Services

### Scenario

Windows Deployment Services is installed and configured successfully. You now must create various operating-system images to aid deployment.

The main tasks for this exercise are as follows:

1. Insert the Windows Server 2012 R2 installation media in LON-SVR1
2. Add a boot image
3. Add an install image

#### ► Task 1: Insert the Windows Server 2012 R2 installation media in LON-SVR1

1. On the host computer, open Hyper-V Manager.
2. Open the **Settings** page for 20411D-LON-SVR1.
3. Select the DVD Drive, and attach the .iso file located at **D:\Program Files\Microsoft Learning\20411\Drives\Windows2012R2.iso**.

#### ► Task 2: Add a boot image

1. Switch to LON-SVR1.
2. If necessary, open the **Windows Deployment Services** console.
3. Add a new boot image using the following information to complete the process:
  - On the **Image File** page, use the file name **D:\sources\boot.wim**.
  - Accept the defaults on the **Image Metadata** page.
  - Accept the defaults on the **Summary** page.
4. On the **Task Progress** page, click **Finish**.

#### ► Task 3: Add an install image

1. If necessary, open **Windows Deployment Services**.
2. Add a new **Image Group** with the image group name of **Windows Server 2012 R2**.
3. Use the Add Image Wizard to add a new install image to this group. Use the following information to complete the process:
  - a. On the **Image File** page, use the following file name: **D:\sources\install.wim**
  - b. On the **Available Images** page, clear all check boxes except **Windows Server 2012 R2 SERVERSTANDARDCORE**.
  - c. Accept the defaults on the **Summary** page.
  - d. On the **Task Progress** page, click **Finish**.

**Results:** After completing this exercise, you will create an operating system image with Windows Deployment Services.

## Exercise 3: Configuring Custom Computer Naming

### Scenario

To automate computer naming, you must configure the custom naming properties for Windows Deployment Services according to the requirements sent to you by management. This also involves configuring delegation on the Active Directory OU that will contain the computer accounts. Administrator approval is required, so you must also configure that.

The main tasks for this exercise are as follows:

1. Configure automatic naming
2. Configure administrator approval
3. Configure Active Directory® Domain Services (AD DS) permissions

#### ► Task 1: Configure automatic naming

1. In Windows Deployment Services, view the properties of **LON-SVR1.Adatum.com**.
2. On the **AD DS** tab, use the following information to configure automatic naming:
  - Format: **BRANCH-SVR-%02#**
  - Computer Account Location: **Research OU**

#### ► Task 2: Configure administrator approval

1. In Windows Deployment Services, view the properties of **LON-SVR1.Adatum.com**.
2. On the **PXE Response** tab, select **Require administrator approval for unknown computers**, and change the **PXE Response Delay** to **3 seconds**.
3. Open Windows PowerShell, and then type the following command to create a message for installers to view while awaiting admin approval:

```
WDSUTIL /Set-Server /AutoAddPolicy /Message:"The Adatum administrator is authorizing
this request. Please wait."
```

4. Close the Windows PowerShell command prompt window.

#### ► Task 3: Configure Active Directory® Domain Services (AD DS) permissions

1. Switch to LON-DC1, and open **Active Directory Users and Computers**.
2. Right-click the **Research** OU, and use the Delegation of Control Wizard to delegate to the **LON-SVR1** computer account the ability to create computer objects in the OU. Use the following information to help:
  - a. Tasks to delegate: **Create a custom task to delegate**
  - b. On the **Active Directory Object Type** page, click **Only the following objects in the folder**, and then select both the **Computer objects** and **Create selected objects in this folder** check boxes.
  - c. On the **Permissions** page, in the **Permissions list**, select the **Full Control** check box.

**Results:** After completing this exercise, you will have configured custom computer naming.

## Exercise 4: Deploying Images with Windows Deployment Services

### Scenario

You have provided instructions for a branch supervisor to initiate the installation process on the branch office server computer. The installation now will occur.

The main tasks for this exercise are as follows:

1. Configure a Windows Deployment Services server for multicast transmission
2. Configure the client for PXE booting
3. To prepare for the next module

#### ► Task 1: Configure a Windows Deployment Services server for multicast transmission

1. Switch to the LON-SVR1 computer.
2. Create a new multicast transmission using the following information:
  - Transmission name: **Windows Server 2012 Branch Servers**
  - Image group: **Windows Server 2012 R2**
  - Image: **Windows Server 2012 R2 SERVERSTANDARDCORE**
  - Multicast type: **Auto-cast**

#### ► Task 2: Configure the client for PXE booting

1. On the host computer, switch to **Hyper-V Manager**.
2. In the Virtual Machines list, right-click **20411D-LON-SVR3**, and then click **Settings**.
3. In the **Settings for 20411D-LON-SVR3** dialog box, click **BIOS**.
4. In the results pane, click **Legacy Network adapter**.
5. Use the arrows to move **Legacy Network adapter** to the top of the list, and then click **OK**.
6. In Hyper-V Manager, click **20411D-LON-SVR3**, and in the Actions pane, click Start.
7. In the **Actions** pane, click **Connect**.
8. When the computer reboots, note the PXE DHCP notice. When prompted, press the **F12** key for Network Boot.
  - **Question:** Does the admin approval message display?
9. Switch to the LON-SVR1 computer.
10. In Windows Deployment Services, click **Pending Devices**.
11. Right-click the **pending request**, and then click **Approve**.
12. In the **Pending Device** dialog box, click **OK**.
13. Switch to LON-SVR3.
  - **Question:** Which image is the default?
  - **Question:** Does setup start?
14. You do not have to continue setup.

► **Task 3: To prepare for the next module**

**When you finish the lab, revert the virtual machines to their initial state**

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat these steps for **20411D-LON-SVR3** and **20411D-LON-SVR1**.

**Results:** After completing this exercise, you will have deployed an image with Windows Deployment Services.

**Question:** How do You Use Windows Deployment Services in your organization?

**Question:** For what two categories of images do you need to use Windows Deployment Services to deploy an operating system to a computer over the network?

**Question:** How can you avoid name conflicts when deploying an operating system to multiple computers in the same transmission?

# Lab: Implementing Update Management

## Scenario

A. Datum is a global engineering and manufacturing company with a head office in London, United Kingdom. An IT office and a data center are located in London to support the London location and other branch office locations. A. Datum has recently deployed a Windows Server 2012 server and client infrastructure.

A. Datum has been manually applying updates to servers in a remote location. This has resulted in difficulty identifying which servers have updates applied and which do not. This is a potential security issue. You have been asked to automate the update process by extending A. Datum's WSUS deployment to include the branch office.

## Objectives

After completing this lab, you will be able to:

- Implement the WSUS server role.
- Configure update settings.
- Approve and deploy an update by using WSUS.

## Lab Setup

Estimated Time: 60 minutes

**Virtual machines:** 20411D-LON-DC1, 20411D-LON-SVR1, 20411D-LON-SVR4, 20411D-LON-CL1

**User name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, on the Start screen, click **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Log on using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Perform steps 2 through 4 for **20411D-LON-SVR1**, **20411D-LON-SVR4**, and **20411D-LON-CL1**.

## Exercise 1: Implementing the WSUS Server Role

### Scenario

Your organization already has a WSUS server called LON-SVR1, which is located in the head office. You need to install the WSUS server role on LON-SVR4 at a branch location. LON-SVR4 will use LON-SVR1 as the source for Windows Update downloads. The installation on LON-SRV4 will use the Windows Internal Database for the deployment.

The main tasks for this exercise are as follows:

1. Install the WSUS server role
2. Configure WSUS to synchronize with an upstream WSUS server

► **Task 1: Install the WSUS server role**

1. Log on to LON-SVR4 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. From Server Manager, install the Windows Server Update Services role with the WID Database and WSUS Services Role Services. Also, configure the updates location as **C:\WSUSUpdates**.
3. Open the Windows Server Update Services console and complete the installation when prompted.

► **Task 2: Configure WSUS to synchronize with an upstream WSUS server**

1. On LON-SVR4, complete the Windows Server Update Services Configuration Wizard, specifying the following settings:
  - Upstream Server: **LON-SVR1.Adatum.com**
  - No proxy server
  - Default languages
  - Manual sync schedule
  - Begin initial synchronization
2. In the Windows Server Update Services console, under Options, set Computers to **Use Group Policy or registry settings on computers**. You many need to wait until synchronization is complete before selecting this option.

**Results:** After completing this exercise, you should have implemented the WSUS server role.

## Exercise 2: Configuring Update Settings

### Scenario

You need to configure the Group Policy settings to deploy automatic WSUS settings to client computers. With the WSUS role configured on LON-SVR4, you must ensure that the Research Department has its own computer group in WSUS on LON-SVR4. You must also configure client computers in the Research organizational unit (OU) to use LON-SVR4 as their source for updates.

The main tasks for this exercise are as follows:

1. Configure WSUS groups
2. Configure Group Policy to deploy WSUS settings
3. Verify the application of Group Policy settings
4. Initialize Windows Update

► **Task 1: Configure WSUS groups**

1. On LON-SVR4, if necessary, open the Windows Server Update Services console.
2. Create a new computer group named **Research**.

► **Task 2: Configure Group Policy to deploy WSUS settings**

1. Switch to LON-DC1.
2. Open Group Policy Management.
3. Create and link a new GPO to the **Research** OU named **WSUS Research**.

4. Configure the following policy settings under the Windows Update node:
  - Configure Automatic Updates: **Auto download and schedule the install**
  - Microsoft Update service location: **http://LON-SVR4.Adatum.com:8530**
  - Intranet statistics server: **http://LON-SVR4.Adatum.com:8530**
  - Client-side targeting group: **Research**
5. Move LON-CL1 to the Research OU.

► **Task 3: Verify the application of Group Policy settings**

1. Switch to LON-CL1.
2. Restart LON-CL1.
3. On LON-CL1, log on as **Adatum\Administrator** with a password of **Pa\$\$w0rd**.
4. Open a command prompt by using the **Run as Administrator** option.
5. At the command prompt, run the following command:

```
Gpresult /r
```

6. In the output of the command, confirm that, under Computer Settings, **WSUS Research** is listed under **Applied Group Policy Objects**.

► **Task 4: Initialize Windows Update**

1. On LON-CL1, at the command prompt, type the following command, and then press Enter:
 

```
Wuauctl.exe /detectnow /reportnow
```
2. Switch to LON-SVR4.
3. In the Update Services console, expand **Computers**, then expand **All Computers**, and then click **Research**.
4. Verify that LON-CL1 appears in the Research Group. If it does not, then repeat steps 1-3. It may take several minutes for LON-CL1 to display.
5. Verify that updates are reported as needed. If updates are not reported, repeat steps 1-3. It may take 10-15 minutes for updates to register.

**Results:** After completing this exercise, you should have configured update settings for client computers.

## Exercise 3: Approving and Deploying an Update by Using WSUS

### Scenario

After you have configured the Windows Update settings, you can view, approve, and then deploy required updates. You have been asked to use LON-CL1 as a test case for the Research Department. You will approve, deploy, and verify an update on LON-CL1 to confirm the proper configuration of the WSUS environment.

The main tasks for this exercise are as follows:

1. Approve WSUS updates for the Research computer group
2. Deploy updates to LON-CL1

3. Verify update deployment to LON-CL1
4. To prepare for the next module

► **Task 1: Approve WSUS updates for the Research computer group**

1. On LON-SVR4, open the WSUS console.
2. Approve the **Update for Microsoft Office 2013 (KB2760267), 32-bit Edition** update for the Research group.

► **Task 2: Deploy updates to LON-CL1**

1. On LON-CL1, at the command prompt, type the following command, and then press Enter:

```
Wuauctl.exe /detectnow
```

2. Open Windows Update and then check for updates.
3. Click **Install** to install the approved update.

► **Task 3: Verify update deployment to LON-CL1**

1. On LON-CL1, open Event Viewer.
2. Navigate to Applications and Services Logs\ Microsoft\Windows, and view the events under WindowsUpdateClient / Operational.
3. Confirm that events are logged in relation to the update.

► **Task 4: To prepare for the next module**

When you finish the lab, revert all virtual machines back to their initial state. To do this, perform the following steps:

1. On the host computer, start Microsoft Hyper-V® Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 to 3 for **20411D-LON-SVR1**, **20411D-LON-SVR4**, and **20411D-LON-CL1**.

**Results:** After completing this exercise, you should have approved and deployed an update by using WSUS.

# Lab: Monitoring Windows Server 2012

## Scenario

A. Datum Corporation is a global engineering and manufacturing company with its head office in London, England. An IT office and data center are in London to support the London location and other locations. A. Datum recently deployed a Windows Server 2012 server and client infrastructure.

Because the organization has deployed new servers, it is important to establish a performance baseline with a typical load for these new servers. You have been asked to work on this project. Additionally, to make the process of monitoring and troubleshooting easier, you decide to perform centralized monitoring of event logs.

## Objectives

After completing this lab, you will be able to:

- Establish a performance baseline.
- Identify the source of a performance problem.
- View and configure centralized event logs.

## Lab Setup

**Estimated Time:** 60 minutes

**Virtual Machines:** 20411D-LON-DC1, 20411D-LON-SVR1

**User Name:** Adatum\Administrator

**Password:** Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Microsoft Hyper-V Manager, click **20411D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Administrator**
  - Password: **Pa\$\$w0rd**
  - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20411D-LON-SVR1**.

## Exercise 1: Establishing a Performance Baseline

### Scenario

In this exercise, you will use Performance Monitor on the server, and create a baseline by using typical performance counters.

The main tasks for this exercise are as follows:

1. Create and Start a Data Collector Set
2. Create a Typical Workload on the Server
3. Analyze the Collected Data

- Task 1: Create and Start a Data Collector Set
1. Switch to the LON-SVR1 computer.
  2. Open **Performance Monitor**.
  3. Create a new **User Defined** data collector set by using the following information to complete the process:
    - Name: **LON-SVR1 Performance**
    - Create: **Create manually (Advanced)**
    - Type of data: **Performance counter**
    - Select the following counters:
      - Memory, Pages/sec
      - Network Interface, Bytes Total/sec
      - PhysicalDisk, %Disk Time
      - PhysicalDisk, Avg. Disk Queue Length
      - Processor, %Processor Time
      - System, Processor Queue Length
    - Sample interval: **1 second**
    - Where to store data: default value
  4. Save and close the data collector set.
  5. In Performance Monitor, in the results pane, right-click **LON-SVR1 Performance**, and then click **Start**.

► Task 2: Create a Typical Workload on the Server

1. Open a command prompt, and then run the following commands by pressing Enter after each command:

```
Fsutil file createnew bigfile 104857600
Copy bigfile \\LON-dc1\c$
Copy \\LON-dc1\c$\bigfile bigfile2
Del bigfile*.*
Del \\LON-dc1\c$\bigfile*.*
```

2. Do not close the command prompt.

► Task 3: Analyze the Collected Data

1. Switch to Performance Monitor.
2. Stop the **LON-SVR1 Performance** data collector set.
3. In Performance Monitor, in the navigation pane, navigate to **Reports, User Defined, LON-SVR1, LON-SVR1\_DateTime-000001, and then review the report data**.
4. Record the values that are listed in the report for later analysis. Recorded values include:
  - Memory, Pages/sec
  - Network Interface, Bytes Total/sec
  - PhysicalDisk, %Disk Time
  - PhysicalDisk, Avg. Disk Queue Length

- Processor, %Processor Time
- System, Processor Queue Length

**Results:** After this exercise, you should have established a baseline for performance-comparison purposes.

## Exercise 2: Identifying the Source of a Performance Problem

### Scenario

In this exercise, you will simulate a load to represent the system in live usage, gather performance data by using your data collector set, and then determine the potential cause of the performance problem.

The main tasks for this exercise are as follows:

1. Create Additional Workload on the Server
2. Capture Performance Data by Using a Data Collector Set
3. Remove the Workload, and then Review the Performance Data

#### ► Task 1: Create Additional Workload on the Server

1. On LON-SVR1, switch to the command prompt.
2. Change to the **C:\Labfiles** folder.
3. On LON-SVR1, run **StressTool.exe 95**.

#### ► Task 2: Capture Performance Data by Using a Data Collector Set

1. Switch to Performance Monitor.
2. In Performance Monitor, navigate to **Data Collector Sets, User Defined**, and in the results pane start the **LON-SVR1 Performance data collector set**.
3. Wait one minute to allow the data capture to occur.

#### ► Task 3: Remove the Workload, and then Review the Performance Data

1. At the command prompt, press **Ctrl+ C**. Leave the command prompt running.
2. Switch to **Performance Monitor**.
3. Stop the **LON-SVR1 Performance** data collector set.
4. In Performance Monitor, in the navigation pane, navigate to **Reports, User Defined, LON-SVR1, LON-SVR1\_DateTime-000002, and then review the report data..**

Record the following values:

- a. Memory, Pages/sec
- b. Network Interface, Bytes Total/sec
- c. PhysicalDisk, %Disk Time
- d. PhysicalDisk, Avg. Disk Queue Length
- e. Processor, %Processor Time
- f. System, Processor Queue Length

**Question:** Compared with your previous report, which values have changed?

**Question:** What would you recommend?

**Results:** After this exercise, you should have used performance tools to identify a potential performance bottleneck.

## Exercise 3: Viewing and Configuring Centralized Event Logs

### Scenario

In this exercise, you will use LON-DC1 to collect event logs from LON-SVR1. Specifically, you will use this process to gather performance-related alerts from your network servers.

The main tasks for this exercise are as follows:

1. Configure Subscription Prerequisites
2. Create a Subscription
3. Configure a Performance Counter Alert
4. Introduce Additional Workload on the Server
5. Verify Results
6. To Prepare for the Next Module

#### ► Task 1: Configure Subscription Prerequisites

1. Switch to LON-SVR1.
2. At the command prompt, run **winrm quickconfig** to enable the administrative changes that are necessary on a source computer.
3. Add the **LON-DC1** computer to the local **Administrators** group.
4. Switch to LON-DC1.
5. At a command prompt, run **wecutil qc** to enable the administrative changes that are necessary on a collector computer.

#### ► Task 2: Create a Subscription

1. Open **Event Viewer**.
2. Create a new subscription with the following properties:
  - Computers: **LON-SVR1**
  - Name: **LON-SVR1 Events**
  - Collector **initiated**
  - Events: **Critical, Warning, Information, Verbose**, and **Error**
  - Logged: **Last 7 days**
  - Logs: **Applications and Services Logs > Microsoft > Windows > Diagnosis-PLA > Operational**

#### ► Task 3: Configure a Performance Counter Alert

1. Switch to LON-SVR1.
2. Open Performance Monitor.

3. Create a new **User Defined** data collector set by using the following information to complete the process:
  - Name: **LON-SVR1 Alert**
  - Create: **Create manually (Advanced)**
  - Type of data: **Performance counter Alert**
  - Select the following counters: **Processor, %Processor Time** above **10** percent
  - Sample interval: **1** second
  - Where to store data: default value
  - Alert Action: **Log an entry in the application event log**
4. Start the **LON-SVR1 Alert** data collector set.

► **Task 4: Introduce Additional Workload on the Server**

1. Switch to the command prompt.
2. Change to the C:\Labfiles folder, and then run **StressTool.exe 95**.
3. Wait one minute for the data capture to occur, and, at the command prompt, press Ctrl+ C, and then close the command prompt.

► **Task 5: Verify Results**

- Switch to LON-DC1, and then open **Forwarded Events**.

**Question:** In Performance Monitor, are there any performance-related alerts in the subscribed application log? Hint: They have an ID of 2031.

► **Task 6: To Prepare for the Next Module**

When you are finished with the lab, revert all virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start Microsoft Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machines** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20411D-LON-SVR1**.

**Results:** At the end of this exercise, you will have centralized event logs and examined these logs for performance-related events.

**Question:** During the lab, you collected data in a data collector set. What is the advantage of collecting data in this way?

# Lab: Implementing Advanced Network Services

## Scenario

A. Datum Corporation has grown rapidly over the last few years. The company has deployed several new branch offices, and it has increased significantly the number of users in the organization. Additionally, it has expanded the number of partner organizations and customers that access A. Datum websites and applications. Because of this expansion, the network infrastructure complexity has increased, and the organization now needs to be much more aware of network-level security.

As one of the senior network administrators at A. Datum, you are responsible for implementing some of the advanced networking features in Windows Server 2012 R2 to manage the networking infrastructure. You need to implement new features in DHCP and DNS, with the primary goal of providing higher levels of availability while increasing the security of these services. You also need to implement IPAM so that you can simplify and centralize the IP address usage and configuration management in an increasingly complex network.

## Objectives

In this lab, you will see how to:

- Configure advanced DHCP settings.
- Configure advanced DNS settings.
- Configure IP address management.

## Lab Setup

Estimated Time: 70 minutes

Virtual machines: 20412D-LON-DC1, 20412D-LON-SVR1,  
20412D-LON-SVR2, 20412D-LON-CL1

User Name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 to 4 for 20412D-LON-SVR1 and 20412D-LON-SVR2. Do not start 20412D-LON-CL1 until directed to do so.

## Exercise 1: Configuring Advanced DHCP Settings

### Scenario

With the expansion of the network, and the increased availability and security requirements at A. Datum Corporation, you need to implement additional DHCP features. Because of the recent business expansion, the main office DHCP scope is almost completely utilized, which means that you need to configure a superscope. Additionally, you need to configure DHCP Name Protection and DHCP failover.

The main tasks for this exercise are as follows:

1. Configure a superscope.
2. Configure DHCP name protection.
3. Configure and verify DHCP failover.

#### ► Task 1: Configure a superscope

1. On LON-DC1, configure a scope named **Scope1**, with a range of **192.168.0.50 – 192.168.0.100**, and with the following settings:
  - Subnet mask: **255.255.255.0**
  - Router: **192.168.0.1**
  - DNS Suffix: **Adatum.com**
  - Choose to activate the scope later.
2. Configure a second scope named **Scope2** with a range of **192.168.1.50 – 192.168.1.100**, and with the following settings:
  - Subnet mask: **255.255.255.0**
  - Router: **192.168.1.1**
  - DNS Suffix: **Adatum.com**
  - Choose to activate the scope later.
3. Create a superscope called **AdatumSuper** that has **Scope1** and **Scope2** as members.
4. Activate the **AdatumSuper** superscope.

#### ► Task 2: Configure DHCP name protection

- Switch to the DHCP console on LON-DC1, and enable **DHCP Name Protection** found on the DNS tab of the IPv4 node.

#### ► Task 3: Configure and verify DHCP failover

1. On LON-SVR1, start the DHCP console and observe the current state of DHCP. Note that the server is authorized, but that no scopes are configured.
2. On LON-DC1, in the DHCP console, launch the Configure Failover Wizard.
3. Configure failover replication with the following settings:
  - Partner server: **172.16.0.21**
  - Relationship Name: **Adatum**
  - Maximum Client Lead Time: **15 minutes**
  - Mode: **Load balance**

- Load Balance Percentage: **50%**
  - State Switchover Interval: **60 minutes**
  - Message authentication shared secret: **Pa\$\$w0rd**
4. Complete the Configure Failover Wizard.
  5. On LON-SVR1, refresh the IPv4 node. Notice that the IPv4 node is active, and that Scope Adatum is configured.
  6. Start **20412D-LON-CL1**, and sign in as **Adatum\Administrator**.
  7. Configure LON-CL1 to obtain an IP address from the DHCP server.
  8. Open a command prompt window, and record the IP address.
  9. Switch to LON-DC1, and stop the DHCP server service.
  10. Switch back to LON-CL1, and renew the IP address.
  11. On LON-DC1, in the Services console, start the DHCP server service.
  12. Close the Services console.

**Results:** After completing this exercise, you will have configured a superscope, configured DHCP Name Protection, and configured and verified DHCP failover.

## Exercise 2: Configuring Advanced DNS Settings

### Scenario

To increase the security level for the DNS zones at A. Datum, you need to configure DNS security settings such as DNSSEC, DNS socket pool, and cache locking. A. Datum has a business relationship with Contoso, Ltd., and will host the Contoso.com DNS zone. A. Datum clients use an application that accesses a server named **App1** in the Contoso.com zone by using its NetBIOS name. You need to ensure that these applications can resolve the names of the required servers correctly. You will employ a GlobalNames zone to achieve this.

The main tasks for this exercise are as follows:

1. Configure DNSSEC.
2. Configure the DNS socket pool.
3. Configure DNS cache locking.
4. Configure a GlobalNames zone.

### ► Task 1: Configure DNSSEC

1. On LON-DC1, start the DNS Manager.
2. Use the DNSSEC Zone Signing Wizard to sign the **Adatum.com** zone.
3. Choose to customize zone-signing parameters.
4. Ensure that DNS server **LON-DC1** is the Key Master.
5. Add the **Key Signing Key** by accepting the default values for the new key.
6. Add the **Zone Signing Key** by accepting the default values for the new key.
7. Choose to use **NSCE3** with the default values.

8. Choose to enable the distribution of trust anchors for this zone.
9. Accept the default values for **signing and polling**.
10. Verify that the DNSKEY resource records have been created in the **Trust Points zone**.
11. Minimize the DNS console.
12. Use the Group Policy Management Console, in the Default Domain Policy object, to configure the Name Resolution Policy Table.
13. Create a rule that enables DNSSEC for the Adatum.com suffix, and that requires DNS clients to verify that the name and address data were validated.

#### ► Task 2: Configure the DNS socket pool

1. On LON-DC1, start Windows PowerShell.
2. Run the following command to view the current size of the socket pool:

```
Get-DNSServer
```

3. Run the following command to change the socket pool size to 3,000:

```
dnscmd /config /socketpoolsize 3000
```

4. Restart the DNS service.
5. Run the following command to confirm the new socket pool size:

```
Get-DnsServer
```

#### ► Task 3: Configure DNS cache locking

1. Run the following command to view the current cache lock size:

```
Get-DnsServer
```

2. Run the following command to change the cache lock value to 75 percent:

```
Set-DnsServerCache -LockingPercent 75
```

3. Restart the DNS service.
4. Run the following command to confirm the new cache lock value:

```
Get-DnsServer
```

#### ► Task 4: Configure a GlobalNames zone

1. Create an Active Directory-integrated forward lookup zone named **Contoso.com**, by running the following command:

```
Add-DnsServerPrimaryZone -Name Contoso.com -ReplicationScope Forest
```

2. Run the following command to enable support for GlobalName zones:

```
Set-DnsServerGlobalNameZone -AlwaysQueryServer $true
```

3. Create an Active Directory-integrated forward lookup zone named **GlobalNames** by running the following command:

```
Add-DnsServerPrimaryZone -Name GlobalNames -ReplicationScope Forest
```

4. Open the DNS Manager console, and add a new host record to the Contoso.com domain named **App1** with the IP address of **192.168.1.200**.
5. In the GlobalNames zone, create a new alias named **App1** using the FQDN of **App1.Contoso.com**.
6. Close DNS Manager, and close the Windows PowerShell window.

**Results:** After completing this exercise, you will have configured DNSSEC, the DNS socket pool, DNS cache locking, and the GlobalName zone.

## Exercise 3: Configuring IPAM

### Scenario

- A. Datum Corporation is evaluating solutions for simplifying IP address management. Since you implemented Windows Server 2012, you have decided to implement IPAM.

The main tasks for this exercise are as follows:

1. Install the IPAM feature.
2. Configure IPAM-related GPOs.
3. Configure IP management server discovery.
4. Configure managed servers.
5. Configure and verify a new DHCP scope with IPAM.
6. Configure IP address blocks, record IP addresses, and create DHCP reservations and DNS records.
7. To prepare for the next module.

#### ► Task 1: Install the IPAM feature

- On LON-SVR2, install the **IP Address Management (IPAM) Server** feature by using the Add Roles and Features Wizard in Server Manager.

#### ► Task 2: Configure IPAM-related GPOs

1. On LON-SVR2, in the Server Manager, in the IPAM Overview pane, provision the IPAM server using Group Policy.
2. Enter **IPAM** as the GPO name prefix, and provision IPAM using the Provision IPAM Wizard.

#### ► Task 3: Configure IP management server discovery

1. In the IPAM Overview pane, configure server discovery for the Adatum domain.
2. In the IPAM Overview pane, start the server discovery process. Discovery may take five to 10 minutes to run. The yellow bar will indicate when discovery is complete.

#### ► Task 4: Configure managed servers

1. In the IPAM Overview pane, add the servers that you need to manage. Verify that IPAM access is currently blocked for both LON-DC1 and LON-SVR1.

2. Use Windows PowerShell to grant the IPAM server permission to manage by running the following command:

```
Invoke-IpamGpoProvisioning -Domain Adatum.com -GpoPrefixName IPAM -IpamServerFqdn LON-SVR2.adatum.com -DelegatedGpoUser Administrator
```

3. For both LON-DC1 and LON-SVR1, set the manageability status to **Managed**.
4. Switch to LON-DC1, and force the update of Group Policy using **gpupdate /force**.
5. Switch to LON-SVR1, and force the update of Group Policy by using **gpupdate /force**.
6. Return to LON-SVR2, and refresh the server access status for LON-DC1 and LON-SVR1 and the Server Manager console view. It may take up to 10 minutes for the status to change. If necessary, repeat both refresh tasks as needed until a green check mark displays next to LON-DC1 and the IPAM Access Status displays as **Unblocked**.
7. In the IPAM Overview pane, right click LON-SVR1 and **Retrieve All Server Data**.
8. In the IPAM Overview pane, right-click LON-DC1 and **Retrieve All Server Data**.

#### ► Task 5: Configure and verify a new DHCP scope with IPAM

1. On LON-SVR2, use IPAM to create a new DHCP scope with the following parameters:
  - Scope Name: **TestScope**
  - Scope start address: **10.0.0.50**
  - Scope end address: **10.0.0.100**
  - Subnet mask: **255.0.0.0**
  - Default gateway: **10.0.0.1**
2. Use IPAM to configure failover for the TestScope on LON-DC1 with the following parameters:
  - Partner server: **LON-SVR1.adatum.com**
  - Relationship name: **TestFailover**
  - Shared secret: **Pa\$\$w0rd**
  - Maximum client lead time: **15 minutes**
  - Mode: **Load balance**
  - Load balance percentage: **50%**
  - State Switchover Interval: **60 minutes**
3. On LON-DC1, verify the scope in the DHCP MMC.
4. On LON-SVR1, verify the scope in the DHCP MMC.

#### ► Task 6: Configure IP address blocks, record IP addresses, and create DHCP reservations and DNS records

1. On LON-SVR2, add an IP address block in the IPAM console with the following parameters:
  - Network ID: **172.16.0.0**
  - Prefix length: **16**
  - Description: **Head Office**

2. Add IP addresses for the network router by adding to the IP Address Inventory with the following parameters:
  - IP address: **172.16.0.1**
  - MAC address: **112233445566**
  - Device type: **Routers**
  - Description: **Head Office Router**
3. Use the IPAM console to create a DHCP reservation as follows:
  - IP address: **172.16.0.10**
  - MAC address: **223344556677**
  - Device type: **Host**
  - Client ID: **Associate MAC to Client ID checkbox**
  - Reservation server name: **LON-DC1.Adatum.com**
  - Reservation name: **Webserver**
  - Reservation type: **Both**
4. Use the IPAM console to create the DNS host record as follows:
  - Device name: **Webserver**
  - Forward lookup zone: **Adatum.com**
  - Forward lookup primary server: **LON-DC1.adatum.com**
  - **Automatically create DNS records for this IP address**
5. On LON-DC1, open the DHCP console and confirm that the reservation was created in the 172.16.0.0 scope.
6. On LON-DC1, open the DNS Manager console and confirm that the DNS host record was created.

► **Task 7: To prepare for the next module**

1. On the host computer, start the Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20412D-LON-SVR1**, **20412D-LON-SVR2**, and **20412D-LON-CL1**.

**Results:** After completing this exercise, you will have installed IPAM and configured IPAM with IPAM-related GPOs, IP management server discovery, managed servers, a new DHCP scope, IP address blocks, IP addresses, DHCP reservations, and DNS records.

**Question:** Will client computers immediately stop communicating on the network if there is no functioning DHCP server?

**Question:** What is the default size of the DNS socket pool?

**Question:** What value does the DNS cache lock use to determine when to update an IP address in the DNS cache?

# Lab A: Implementing Advanced File Services

## Scenario

As the A. Datum Corporation has expanded, the requirements for managing storage and shared file access have also expanded. Although the cost of storage has decreased significantly over recent years, the amount of data produced by the A. Datum business groups has increased even faster. The organization is considering alternate ways to decrease the cost of storing data on the network, and is considering options for optimizing data access in the new branch offices. The organization would also like to ensure that data that is stored on the shared folders is limited to company data, and that it does not include unapproved file types.

As a senior server administrator at A. Datum, you are responsible for implementing the new file storage technologies for the organization. You will implement iSCSI storage to provide a less complicated option for deploying large amounts of storage.

## Objectives

After completing this lab, the students will be able to:

- Configure iSCSI storage.
- Configure the File Classification Infrastructure.

## Lab Setup

Estimated Time: 75 minutes

|                  |                                                                                          |
|------------------|------------------------------------------------------------------------------------------|
| Virtual machines | 20412D-LON-DC1<br>20412D-LON-SVR1<br>20412D-LON-SVR2<br>20412D-LON-CL1<br>20412D-LON-CL2 |
| User name        | <b>Adatum\Administrator</b>                                                              |
| Password         | <b>Pa\$\$w0rd</b>                                                                        |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, open **Hyper-V Manager**.
2. In the Hyper-V Manager console, right-click **20412D-LON-SVR2**, and then click **Settings**.
3. In the **Settings for 20412D-LON-SVR2** window, in the left pane, ensure that the first network adapter is connected to Private Network, and change the second network adapter to also be connected to Private Network.

 **Note:** You can only perform the previous step if LON-SVR2 has not been started. If LON-SVR2 is already started, shut down LON-SVR2, and then perform these steps.

4. In the Hyper-V Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
5. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
6. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
7. On LON-DC1, right-click the **Start** button, and then click **Network Connections**.

8. Right-click **Ethernet 2** and click **Enable**.
9. Close the Network Connections dialog box.
10. Repeat steps four through six for 20412D-LON-SVR1 and 20412D-LON-SVR2.

## Exercise 1: Configuring iSCSI Storage

### Scenario

To decrease the cost and complexity of configuring centralized storage, A. Datum has decided to use iSCSI to provide storage. To get started, you will install and configure the iSCSI target, and then configure access to the target by configuring the iSCSI initiators.

The main tasks for this exercise are as follows:

1. Install the iSCSI target feature
2. Configure the iSCSI targets
3. Configure MPIO
4. Connect to and configure the iSCSI targets

#### ► Task 1: Install the iSCSI target feature

1. Sign in to LON-DC1 with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.
2. Open the Server Manager.
3. In the Add Roles and Features Wizard, install the following roles and features to the local server, and accept the default values:
  - **File And Storage Services (Installed)\File and iSCSI Services\iSCSI Target Server**

#### ► Task 2: Configure the iSCSI targets

1. On LON-DC1, in the Server Manager, in the navigation pane, click **File and Storage Services**, and then click **iSCSI**.
2. Create a virtual disk with the following settings:
  - Storage location: **C:**
  - Disk name: **iSCSIDisk1**
  - Size: **5 GB**
  - iSCSI target: **New**
  - Target name: **lon-dc1**
  - Access servers: **172.16.0.22** and **131.107.0.2**
3. On the **View results** page, wait until the creation completes, and then click **Close**.
4. Create a New iSCSI virtual disk with the following settings:
  - Storage location: **C:**
  - Disk name: **iSCSIDisk2**
  - Size: **5 GB**
  - iSCSI target: **lon-dc1**
5. Create a New iSCSI virtual disk with the following settings:
  - Storage location: **C:**
  - Disk name: **iSCSIDisk3**
  - Size: **5 GB**
  - iSCSI target: **lon-dc1**

### ► Task 3: Configure MPIO

1. Sign in to LON-SVR2 with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.
2. On LON-SVR2, from the Server Manager, open the Routing and Remote Access console.
3. Right-click **LON-SVR2**, and click **Disable Routing and Remote Access**. Close the Routing and Remote Access console.

 **Note:** Normally, you do not disable Routing and Remote Access (RRAS) before configuring MPIO. You do it here because of lab requirements.

4. In the Server Manager, start the Add Roles and Features Wizard and install the **Multipath I/O** feature.
5. In Server Manager, on the **Tools** menu, open **iSCSI Initiator**, and configure the following:
  - Enable the **iSCSI Initiator** service
  - **Quick Connect** to target: **LON-DC1**
6. In Server Manager, on the **Tools** menu, open **MPIO**, and then configure the following:
  - Enable **Add support for iSCSI devices on Discover Multi-paths**
7. After the computer restarts, sign in to LON-SVR2 with the user name **Adatum\Administrator** and password **Pa\$\$w0rd**.
8. In the Server Manager, on the **Tools** menu, click **MPIO**, and then verify that **Device Hardware ID MSFT2005iSCSIBusType\_0x9** is added to the list.

### ► Task 4: Connect to and configure the iSCSI targets

1. On LON-SVR2, in the Server Manager, on the **Tools** menu, open **iSCSI Initiator**.
2. In the **iSCSI Initiator Properties** dialog box, perform the following steps:
  - **Disconnect all Targets**.
  - **Connect and Enable multi-path**.
  - Set **Advanced** options as follows:
    - Local Adapter: **Microsoft iSCSI Initiator**
    - Initiator IP: **172.16.0.22**
    - Target Portal IP: **172.16.0.10 / 3260**
  - **Connect** to another target, **enable multi-path**, and configure the following **Advanced** settings:
    - Local Adapter: **Microsoft iSCSI Initiator**
    - Initiator IP: **131.107.0.2**
    - Target Portal IP: **131.107.0.1 / 3260**
3. In the **Targets** list, open **Devices for iqn.1991-05.com.microsoft:lon-dc1-lon-dc1-target**, access the MPIO information, and then verify that in **Load balance policy, Round Robin** is selected. Verify that two paths are listed by looking at the IP addresses of both network adapters.

**Results:** After completing this exercise, you will have configured and connected to iSCSI targets.

## Exercise 2: Configuring the File Classification Infrastructure

### Scenario

A. Datum has noticed that many users are copying corporate documentation to their mapped drives on the users' or departmental file servers. As a result, there are many different versions of the same documents on the network. To ensure that only the latest version of the documentation is available for most users, you need to configure a file classification system that will delete specific files from user folders.

The main tasks for this exercise are as follows:

1. Create a classification property for corporate documentation
2. Create a classification rule for corporate documentation
3. Create a classification rule that applies to a shared folder
4. Create a file management task to expire corporate documents
5. Verify that corporate documents are expired
6. Prepare for the next lab

#### ► Task 1: Create a classification property for corporate documentation

1. On LON-SVR1, from the Server Manager, start the File Server Resource Manager.
2. In File Server Resource Manager, under Classification Management, create a local property with the following settings:
  - Name: **Corporate Documentation**
  - Property Type: **Yes/No**
3. Leave the File Server Resource Manager console open.

#### ► Task 2: Create a classification rule for corporate documentation

1. In the File Server Resource Manager console, create a classification rule with following settings:
  - General tab, Rule name: **Corporate Documents Rule**, and ensure that the rule is enabled.
  - Scope tab: **E:\Labfiles\Corporate Documentation** folder
  - Classification tab:
    - Classification method: **Folder Classifier**
    - Property, Choose a property to assign to files: **Corporate Documentation**
    - Property, Specify a value: **Yes**
    - Evaluation type tab: **Re-evaluate existing property values** and **Aggregate the values**
2. Select both **Run the classification with all rules** and **Wait for classification to complete**.
3. Review the Automatic Classification report that displays in Internet Explorer®, and ensure that the report lists the same number of classified files as in the Corporate Documentation folder.
4. Close Internet Explorer, but leave the File Server Resource Manager console open.

#### ► Task 3: Create a classification rule that applies to a shared folder

1. In the File Server Resource Manager console, create a local property with following settings:
  - Name: **Expiration Date**
  - Property Type: **Date-Time**

2. In the File Server Resource Manager console, create a classification rule with the following settings:
  - General tab, Rule name: **Expiration Rule**, and ensure that the rule is enabled
  - Scope tab: **E:\Labfiles\Corporate Documentation**
  - Classification tab, Classification method: **Folder Classifier**
  - Property, Choose a property to assign to files: **Expiration Date**
  - Evaluation type tab: **Re-evaluate existing property values** and **Aggregate the values**
3. Select both **Run the classification with all rules** and **Wait for classification to complete**.
4. Review the Automatic classification report that appears in Internet Explorer, and ensure that report lists the same number of classified files as the Corporate Documentation folder.

Close Internet Explorer, but leave the File Server Resource Manager console open.

#### ► Task 4: Create a file management task to expire corporate documents

1. In the File Server Resource Manager, create a file management task with following settings:
  - General tab: Task name: **Expired Corporate Documents**, and ensure that the task is enabled
  - Scope tab: **E:\Labfiles\Corporate Documentation**
  - Action tab, Type: **File expiration** is selected,
  - Expiration directory: **E:\Labfiles\Expired**
  - Notification tab: **Event Log** and **Send warning to event log**
  - Condition tab: Days since the file was last modified: **1**

 **Note:** This value is for lab purposes only. In a real scenario, the value would be 365 days or more, depending on each company's policy

- Schedule tab: Weekly and Sunday
- Leave the File Server Resource Manager console open

#### ► Task 5: Verify that corporate documents are expired

1. In the File Server Resource Manager, click **Run File Management Task Now**, and then click **Wait for the task to complete**.
2. Review the file management task report that displays in Internet Explorer, and ensure that the report lists the same number of classified files as the Corporate Documentation folder.
3. Start the Event Viewer, and in the Event Viewer console, open the **Application** event log.
4. Review events with numbers **908** and **909**. Notice that 908 – FSRM started a file management job, and 909 – FSRM finished a file management job.
5. Close open Windows.

► **Task 6: Prepare for the next lab**

When you finish the lab, revert 20412D-LON-SVR1. To do this, complete the following steps.

1. On the host computer, start Hyper-V Manager.
2. On the **Virtual Machines** list, right-click **20412D-LON-SVR1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.

Keep all other virtual machines running for the next lab.

**Results:** After completing this exercise, you will have configured a File Classification Infrastructure so that the latest version of the documentation is always available to users.

**Question:** Why would you implement MPIO together with iSCSI? What problems would you solve with this approach?

**Question:** Why must you have the iSCSI initiator component?

**Question:** Why would you configure file classification for documents located in a folder such as a Corporate Documentation folder?

# Lab B: Implementing BranchCache

## Scenario

The A. Datum Corporation has deployed a new branch office, which has a single server. To optimize file access in branch offices, you must configure BranchCache. To reduce WAN use out to the branch office, you must configure BranchCache to cache data retrieved from the head office. You will also implement FSRM to assist in optimizing file storage.

## Objectives

After completing this lab, the students will be able to:

- Configure the main office servers for BranchCache.
- Configure the branch office servers for BranchCache.
- Configure client computers for BranchCache.
- Monitor BranchCache.

## Lab Setup

Estimated Time: 40 Minutes

|                  |                                                                 |
|------------------|-----------------------------------------------------------------|
| Virtual machines | 20412D-LON-DC1, 20412D-LON-SVR2, 20412D-LON-CL1, 20412D-LON-CL2 |
| User name        | <b>Adatum\Administrator</b>                                     |
| Password         | <b>Pa\$\$w0rd</b>                                               |

For this lab, you will continue to use the 20412D-LON-DC1 and 20412D-LON-SVR2 virtual machines that are still running from the last lab. You will also use 20412D-LON-CL1 and 20412D-LON-CL2, but do not start 20412D-LON-CL1 and 20412D-LON-CL2 until instructed to do so in the lab steps.

## Exercise 1: Configuring the Main Office Servers for BranchCache

### Scenario

Before you can configure the BranchCache feature for your branch offices, you must configure the network components.

The main tasks for this exercise are as follows:

1. Configure LON-DC1 to use Windows BranchCache
2. Simulate a slow link to the branch office
3. Enable a file share for BranchCache
4. Configure client firewall rules for BranchCache

#### ► Task 1: Configure LON-DC1 to use Windows BranchCache

1. Switch to LON-DC1.
2. Open the Server Manager, and install the **BranchCache for network files** role service.
3. Open the Local Group Policy Editor (**gpedit.msc**).
4. Navigate to and open **Computer Configuration/Administrative Templates/Network/Lanman Server/Hash Publication for BranchCache**.
5. Enable the BranchCache setting, and elect **Allow hash publication only for shared folders on which BranchCache is enabled**.

► **Task 2: Simulate a slow link to the branch office**

1. In the Local Group Policy Editor console, navigate to **Computer Configuration\Windows Settings\Policy-based QoS**.
2. Create a new policy with the following settings:
  - Name: **Limit to 100 Kbps**
  - Specify Outbound Throttle Rate: **100**
  - Accept default values on other wizard pages

► **Task 3: Enable a file share for BranchCache**

1. On LON-DC1, in the File Explorer window, create a new folder named **C:\Share**.
2. Share this folder with the following properties:
  - Share name: **Share**
  - Permissions: **default**
  - Caching: **Enable BranchCache**
3. Copy **C:\Windows\System32\mspaint.exe** to the **C:\Share** folder.
4. Close all the command prompt and File Explorer.

► **Task 4: Configure client firewall rules for BranchCache**

1. On LON-DC1, open the Group Policy Management console.
2. Navigate to **Forest: Adatum.com\Domains\Adatum.com\Default Domain Policy**, and open the policy for editing.
3. Navigate to **Computer Configuration\Policies\Windows Settings\Security Settings\Windows Firewall with Advanced Security\Windows Firewall with Advanced Security\Inbound Rules**.
4. Create a new inbound firewall rule with the following properties:
  - Rule type: **predefined**
  - Use **BranchCache – Content Retrieval (Uses HTTP)**
  - Action: **Allow**
5. Create a new inbound firewall rule with the following properties:
  - Rule type: **predefined**
  - Use **BranchCache – Peer Discovery (Uses WSD)**
  - Action: **Allow**
6. Close the Group Policy Management Editor and Group Policy Management console.
7. Update the group policy.

**Results:** At the end of this exercise, you will have deployed BranchCache, configured a slow link, and enabled BranchCache on a file share.

## Exercise 2: Configuring the Branch Office Servers for BranchCache

### Scenario

The next step you must perform is to configure a file server for the BranchCache feature. You will install and start the BranchCache feature.

The main tasks for this exercise are as follows:

1. Install the BranchCache for Network Files role and the BranchCache feature on LON-SVR2
2. Start the BranchCache host server

► **Task 1: Install the BranchCache for Network Files role and the BranchCache feature on LON-SVR2**

- On LON-SVR2 from Server Manager, add the **BranchCache for Network Files** role service and the **BranchCache** feature.

► **Task 2: Start the BranchCache host server**

1. On LON-SVR2, open Windows PowerShell, and run the following cmdlet:

```
Enable-BCHostedServer
-RegisterSCP
```

2. On LON-SVR1, in Windows PowerShell, run the following cmdlet:

```
Get-BCStatus
```

3. Ensure that Branch Cache is enabled and running. Note in the DataCache section, the current active cache size is zero.
4. Update group policy.

**Results:** At the end of this exercise, you will have enabled the BranchCache server in the branch office.

## Exercise 3: Configuring Client Computers for BranchCache

### Scenario

After configuring the network components, you must ensure that the client computers are configured correctly. This is a preparatory task for using BranchCache.

The main tasks for this exercise are as follows:

1. Configure client computers to use BranchCache in hosted cache mode

► **Task 1: Configure client computers to use BranchCache in hosted cache mode**

1. On LON-DC1, open the Server Manager, and then open Group Policy Management.
2. Create a new OU named **Branch**.
3. Create and link a new GPO named **BranchCache** to Branch OU.
4. Edit the **BranchCache** GPO.
5. In the Group Policy Management Editor, browse to **Computer Configuration\Policies\Administrative Templates\Network\BranchCache**, and configure the following:
  - Turn on BranchCache: **Enabled**
  - Enable Automatic Hosted Cache Discovery by Service Connection Point: **Enabled**
  - Configure BranchCache for network files: **Enabled**
  - Type the maximum round trip network latency (milliseconds) after which caching begins: **0**

6. Open the Server Manager, and then open **Active Directory Users and Computers**.
7. Move **LON-CL1** and **LON-CL2** from the Computers container to the Branch OU.
8. Start **20412D-LON-CL1**, sign in as Administrator.
9. At the command prompt, type **netsh branchcache show status all**, and then press Enter.
10. Verify that the BranchCache Status is **Running**. If the status is **Stopped**, restart the client computer.
11. Start the **20412D-LON-CL2**, sign in as Adatum\Administrator and open the command prompt window.
12. At the command prompt, type **netsh branchcache show status all**, and then press Enter.
13. Verify that the BranchCache status is **Running**. If the status is **Stopped**, restart the client computer.

**Results:** At the end of this exercise, you will have configured the client computers for BranchCache.

## Exercise 4: Monitoring BranchCache

### Scenario

Lastly, you must test and verify that the BranchCache feature is working as expected.

The main tasks for this exercise are as follows:

1. Configure Performance Monitor on LON-SVR2
2. Configure performance statistics on LON-CL1
3. Configure performance statistics on LON-CL2
4. Test BranchCache in the hosted cache mode
5. Prepare for the next module

#### ► Task 1: Configure Performance Monitor on LON-SVR2

1. On LON-SVR2, open the Performance Monitor.
2. In the Performance Monitor console, in the navigation pane, under **Monitoring Tools**, click **Performance Monitor**.
3. Remove existing counters, change to report view, and then add the **BranchCache** object counters to the report.

#### ► Task 2: Configure performance statistics on LON-CL1

1. Switch to LON-CL1, and open the Performance Monitor.
2. In the navigation pane of the Performance Monitor console, under **Monitoring Tools**, click **Performance Monitor**.
3. In Performance Monitor, remove existing counters, change to a report view, and then add the **BranchCache** object to the report.

#### ► Task 3: Configure performance statistics on LON-CL2

1. Switch to LON-CL2, and open the Performance Monitor.
2. In the Performance Monitor console, in the navigation pane, under **Monitoring Tools**, click **Performance Monitor**.
3. In the Performance Monitor, remove existing counters, change to a report view, and then add the **BranchCache** object to the report.

► **Task 4: Test BranchCache in the hosted cache mode**

1. Switch to LON-CL1.
2. Open **\LON-DC1.adatum.com\share**, and copy **mspaint.exe** to the local desktop. This could take several minutes because of the simulated slow link.
3. Read the performance statistics on LON-CL1. This file was retrieved from LON-DC1 (Retrieval: Bytes from Server). After the file was cached locally, it was passed up to the hosted cache. (Retrieval: Bytes Served).
4. Switch to LON-CL2.
5. Open **\LON-DC1.adatum.com\share**, and copy **mspaint.exe** to the local desktop. This should not take as long as the first file copy, because the file is cached.
6. Read the performance statistics on LON-CL2. This file was obtained from the hosted cache (Retrieval: Bytes from Cache).
7. Read the performance statistics on LON-SVR2. This server has offered cached data to clients (Hosted Cache: Client file segment offers made).
8. On LON-SVR2, in Windows PowerShell, run the following cmdlet:

```
Get-BCStatus
```



**Note:** In the DataCache section, the current active cache size is no longer zero, it is 6560896.

► **Task 5: Prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. On the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for **20412D-LON-SVR2**, **20412D-LON-CL1**, and **20412D-LON-CL2**.

**Results:** At the end of this exercise, you will have verified that BranchCache is working as expected.

**Question:** When would you consider implementing BranchCache into your own organization?

# Lab: Implementing Secure Data Access

## Scenario

You are working as an administrator at A. Datum Corporation. The company has a wide and complex file server infrastructure. It manages access control to folder shares by using NTFS file system ACLs, but in some cases, that approach does not provide the desired results.

Most of the files that departments use are stored in shared folders dedicated to specific departments, but confidential documents sometimes appear in other shared folders. Only members of the Research team should be able to access Research team folders, and only Executive department managers should be able to access highly confidential documents.

The Security department also is concerned that managers are accessing files by using their home computers, which might not be highly secure. Therefore, you must create a plan for securing documents regardless of where they are located, and you must ensure that documents can be accessed only from authorized computers. Authorized computers for managers are members of the security group ManagersWks.

The Support department reports that a high number of calls are generated by users who cannot access resources. You must implement a feature that helps users understand error messages better and will enable them to request access automatically.

Many users use personal devices such as tablets and laptops to work from home and while at work. You have to provide them with an efficient way to synchronize business data on all the devices that they use.

## Objectives

After completing this lab, you will be able to:

- Prepare for DAC deployment.
- Implement DAC.
- Validate and remediate DAC.
- Implement Work Folders.

## Lab Setup

Estimated Time: 90 minutes

Virtual machines: 20412D-LON-DC1,

20412D-LON-SVR1,

20412D-LON-SVR2,

20412D-LON-CL1,

20412D-LON-CL2

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following procedure:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.

4. Sign in by using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for 20412D-LON-SVR1 and 20412D-LON-SVR2.
6. Do not start or sign in to 20412D-LON-CL1 and 20412D-LON-CL2 machines until instructed by lab steps.

## Exercise 1: Preparing for DAC Deployment

### Scenario

To address the requirements from the lab scenario, you decide to implement DAC technology. The first step in implementing DAC is to configure the claims for the users and devices that access the files. In this exercise, you will review the default claims, and create new claims based on department and computer group attributes. You also will configure the Resource Property lists and the Resource Property definitions. You will do this and then use the resource properties to classify files.

The main tasks for this exercise are as follows:

- Prepare AD DS for DAC deployment.
- Configure user and device claims.
- Configure resource properties and resource property lists.
- Implement file classifications.
- Assign a property to the Research folder.

### ► Task 1: Prepare AD DS for DAC deployment

1. On LON-DC1, in Server Manager, open **Active Directory Domains and Trusts** console.
2. Raise the domain and forest functional level to Windows Server 2012.
3. On LON-DC1, in Server Manager, open **Active Directory Users and Computers**.
4. Create a new Organizational Unit named **DAC-Protected**.
5. Move the LON-SVR1 and LON-CL1 computer objects into the **DAC-Protected** OU.
6. On LON-DC1, from Server Manager, open the Group Policy Management Console.
7. Edit the **Default Domain Controllers Policy** GPO.
8. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **KDC**.
9. Enable the **KDC support for claims, compound authentication and Kerberos armoring** policy setting.
10. In the **Options** section, click **Always provide claims**.
11. On LON-DC1, refresh Group Policy.
12. Open Active Directory Users and Computers, and in the **Users** container, create a security group named **ManagersWKS**.
13. Add **LON-CL1** to the **ManagersWKS** group.
14. Verify that user Aidan Delaney is a member of **Managers** department, and that Allie Bellew is the member of the **Research** department. Department entries should be filled in for the appropriate Organization attribute in each user profile. After you verify these values, click **Cancel** and don't make any changes.

► **Task 2: Configure user and device claims**

1. On LON-DC1, open the **Active Directory Administrative Center**.
2. In the Active Directory Administrative Center, in the navigation pane, click **Dynamic Access Control**.
3. Open the Claim Types container, and then create a new claim type for users and computers by using the following settings:
  - Source Attribute: **department**
  - Display name: **Company Department**
  - Suggested values: **Managers, Research**
4. In the Active Directory Administrative Center, in the Tasks pane, click **New**, and then click **Claim Type**.
5. Create a new claim type for computers by using the following settings:
  - Source Attribute: **description**
  - Display name: **description**

► **Task 3: Configure resource properties and resource property lists**

1. In the Active Directory Administrative Center, click **Dynamic Access Control**, and then open the **Resource Properties** container.
2. Enable the **Department** and **Confidentiality** Resource properties.
3. Open Properties for the **Department** property.
4. Add **Research** as a suggested value.
5. Open the **Global Resource Property List**, ensure that **Department** and **Confidentiality** are included in the list, and then click **Cancel**.
6. Close the **Active Directory Administrative Center**.

► **Task 4: Implement file classifications**

1. On LON-SVR1, open the File Server Resource Manager.
2. Refresh **Classification Properties**, and then verify that **Confidentiality** and **Department** properties are listed.
3. Create a classification rule with following values:
  - Name: **Set Confidentiality**
  - Scope: **C:\Docs**
  - Classification method: **Content Classifier**
  - Property: **Confidentiality**
  - Value: **High**
  - Classification Parameters: **String “secret”**
  - Evaluation Type: **Re-evaluate existing property values**, and then click **Overwrite the existing value**
4. Run the classification rule.
5. Open a File Explorer window, browse to the **C:\Docs** folder, and then open the Properties window for files Doc1.txt, Doc2.txt, and Doc3.txt.
6. Verify values for Confidentiality. Doc1.txt and Doc2.txt should have confidentiality set to High.

► **Task 5: Assign a property to the Research folder**

1. On LON-SVR1, open File Explorer.
2. Browse to **C:\Research**, and open its properties.
3. On the **Classification** tab, set the **Department** value to **Research**.

**Results:** After completing this exercise, you will have prepared Active Directory® Domain Services (AD DS) for Dynamic Access Control (DAC) deployment, configured claims for users and devices, and configured resource properties to classify files.

## Exercise 2: Implementing DAC

### Scenario

The next step in implementing DAC is to configure the central access rules and policies that link claims and property definitions. You will configure rules for DAC to address the requirements from the lab scenario. After you configure DAC rules and policies, you will apply the policy to a file server.

The main tasks for this exercise are as follows:

1. Configure central access rules.
2. Configure central access policies.
3. Apply central access policies to a file server.

► **Task 1: Configure central access rules**

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. Click **Dynamic Access Control**, and then open the **Central Access Rules** container.
3. Create a new central access rule with the following values:
  - Name: **Department Match**
  - Target Resource: **use condition Resource-Department-Equals-Value-Research**
  - Current Permissions:
    - Remove **Administrators**
    - Add **Authenticated Users**,
    - Modify, with condition **User-Company Department-Equals-Resource-Department**
4. Create another central access rule with the following values:
  - Name: **Access Confidential Docs**
  - Target Resource: **use condition Resource-Confidentiality-Equals-Value-High**
  - Current Permissions:
    - Remove **Administrators**
    - Add **Authenticated Users**
    - Modify, and set the first condition to: **User-Company Department-Equals-Value-Managers**
    - Permissions: Set the second condition to: **Device-Group-Member of each-Value-ManagersWKS**

► **Task 2: Configure central access policies**

1. On LON-DC1, in the Active Directory Administrative Center, create a new central access policy with following values:
  - Name: **Protect confidential docs**
  - Rules included: **Access Confidential Docs**
2. Create another central access policy with following values:
  - Name: **Department Match**
  - Rules included: **Department Match**
3. Close the Active Directory Administrative Center.

► **Task 3: Apply central access policies to a file server**

4. On LON-DC1, from the **Server Manager**, open the **Group Policy Management** console.
5. Create new GPO named **DAC Policy**, and in the Adatum.com domain, link it to the **DAC-Protected OU**.
6. Edit the **DAC Policy**, browse to **Computer Configuration /Policies/Windows Settings/Security Settings/File System**, and then right-click **Central Access Policy**.
7. Click **Manage Central Access Policies**, click both **Department Match** and **Protect confidential docs**, click **Add**, and then click **OK**.
8. Close the Group Policy Management Editor and the Group Policy Management Console.
9. On LON-SVR1, use Windows PowerShell to refresh Group Policy on LON-SVR1.
10. Open File Explorer, and then browse to the **C:\Docs** folder.
11. Apply the **Protect confidential docs** central policy to the **C:\Docs** folder.
12. Browse to the **C:\Research** folder.
13. Apply the **Department Match** central policy to the **C:\Research** folder.

**Results:** After completing this exercise, you will have implemented DAC.

## Exercise 3: Validating and Remediating DAC

### Scenario

To ensure that the DAC settings are configured correctly, you will test various scenarios for users to access files. You will try approved users and devices, and unapproved users and devices. You also will validate the access-remediation configuration.

The main tasks for this exercise are as follows:

- Access file resources as an approved user.
- Access file resources as an unapproved user.
- Evaluate user access with DAC.
- Configure access-denied remediation.
- Request access remediation.

► **Task 1: Access file resources as an approved user**

1. Start LON-CL1 and LON-CL2 virtual machines.
2. Sign in to LON-CL1 as **Adatum\Allie** with the password **Pa\$\$w0rd**.
3. Try to open documents inside the **\LON-SVR1\Research** folder.
4. Sign out of LON-CL1.
5. Sign in to LON-CL1 as **Adatum\Aidan** with the password **Pa\$\$w0rd**.
6. Try to open files inside the **\LON-SVR1\Docs** folder.

 **Note:** Both attempts should succeed.

7. Sign out of LON-CL1.

► **Task 2: Access file resources as an unapproved user**

1. Sign in to LON-CL2 as **Adatum\Aidan** with the password **Pa\$\$w0rd**.
2. Open the **\LON-SVR1\Docs** folder. Try to open files Doc1.txt and Doc2.txt.
3. Sign out of LON-CL2.
4. Sign in to LON-CL2 as **Adatum\April** with the password **Pa\$\$word**.
5. Open **\LON-SVR1\Docs** folder, and then try to open Doc3.txt file. You should be able to open that document.
6. While still signed in as April, try to open the **\LON-SVR1\Research** folder. You should be unable to access the folder.
7. Sign out of LON-CL2.

► **Task 3: Evaluate user access with DAC**

1. On LON-SVR1, open the Properties for the **C:\Research** folder.
2. Open the Advanced options for **Security**, and then click **Effective Access**.
3. Click **select a user**, and in the Select User, Computer, Service Account, or Group window, type **April**, click **Check Names**, and then click **OK**.
4. Click **View effective access**, and then review the results. The user should not have access to this folder.
5. Click **Include a user claim**, and then in the drop-down list box, click **Company Department**.
6. In the **Value** text box, type **Research**, and then click **View Effective access**. The user should now have access.
7. Close all open windows.

► **Task 4: Configure access-denied remediation**

1. On LON-DC1, open the Group Policy Management Console, and then browse to **Group Policy objects**.
2. Edit the DAC Policy.
3. Under the Computer Configuration node, browse to **Policies\Administrative Templates\System**, and then click **Access-Denied Assistance**.
4. In the details pane, double-click **Customize Message for Access Denied errors**.
5. In the Customize Message for Access Denied errors window, click **Enabled**.

6. In the **Display the following message to users who are denied access** text box, type **You are denied access because of permission policy. Please request access.**
7. Select the **Enable users to request assistance** check box, and then click **OK**.
8. Double-click **Enable access-denied assistance on client for all file types**, enable it, and then click **OK**.
9. Close the Group Policy Management Editor and the Group Policy Management Console.
10. Switch to LON-SVR1, and then refresh Group Policy.

► **Task 5: Request access remediation**

1. Sign in to LON-CL1 as **Adatum\April** with the password **Pa\$\$w0rd**.
2. Try to access the **\LON-SVR1\Research** folder
3. Request assistance when prompted. Review the options for sending a message, and then click **Close**.
4. Sign out of LON-CL1.

**Results:** After completing this exercise, you will have validated DAC functionality.

## Exercise 4: Implementing Work Folders

### Scenario

To address the requirements for allowing employees to use their own devices to access and synchronize company data, you decide to implement Work Folders for a limited number of users.

The main tasks for this exercise are as follows:

- Install Work Folders functionality, configure SSL certificate, and create WFSync group
- Provision a share for Work Folders.
- Configure and implement Work Folders.
- Validate Work Folders functionality.
- Prepare for the next module.

► **Task 1: Install Work Folders functionality, configure SSL certificate, and create WFSync group**

1. Sign in to LON-SVR2 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Start Server Manager.
3. Add the **Work Folders** role service by using the Add Roles and Features Wizard.
4. Open **Internet Information Services (IIS) Manager** console.
5. Create a domain certificate for lon-svr2.adatum.com as follows:
  - a. Common name: **lon-svr2.adatum.com**
  - b. Organization: **Adatum**
  - c. Organizational unit: **IT**
  - d. City/locality: **Seattle**
  - e. State/province: **WA**
  - f. Country/region: **US**
6. Assign this certificate to the https protocol on the Default Web Site.

7. Open Active Directory Users and Computers console on LON-DC1.
8. Create security group WFSync in the Users container.
9. Add Aidan Delaney from Managers OU as a member of the WFSync group.

► **Task 2: Provision a share for Work Folders**

1. On LON-SVR2, in Server Manager, expand **File and Storage Services**, and then click **Shares**.
2. Start the New Share Wizard.
3. Select the **SMB Share – Quick** profile.
4. Name the share **WF-Share**.
5. Enable access-based enumeration.
6. Leave all other options on default values.

► **Task 3: Configure and implement Work Folders**

1. On LON-SVR2, in Server Manager, expand **File and Storage Services**, and then select **Work Folders**.
2. Start the New Sync Share Wizard.
3. Select the share that you created in previous step: WF-Share.
4. Use user alias for the structure for user folders.
5. Grant access to the WFSync user group.
6. Switch to LON-DC1.
7. Open Group Policy Management.
8. Create a new GPO and name it **Work Folders GPO**.
9. Open the Group Policy Management Editor for Work Folders GPO.
10. Expand **User Configuration / Policies / Administrative Templates / Windows Components**, and then click **Work Folders**.
11. Enable the Work Folders support and type <https://lon-svr2.adatum.com> as the Work Folders URL.
12. Link the Work Folders GPO to the domain.

► **Task 4: Validate Work Folders functionality**

1. Sign in to LON-CL1 as **Adatum\Aidan** with the password **Pa\$\$w0rd**.
2. Open Windows PowerShell, and then refresh Group Policy.
3. Open File Explorer, click **This PC** and then make sure that Work Folders are created.
4. Open the Work Folders applet from Control Panel and apply security policies.
5. Create a few text files in Work Folders.
6. Ensure that the files are synchronized.
7. Sign in to LON-CL2 as **Adatum\Aidan** with the password **Pa\$\$w0rd**.
8. Open Windows PowerShell, and then refresh Group Policy.
9. Open File Explorer, click **This PC** and then make sure that Work Folders are created.
10. Open the Work Folders applet from Control Panel, and apply security policies.
11. Ensure that the files that you created on LON-CL1 are present.

► **Task 5: Prepare for the next module**

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the Revert Virtual Machine dialog box, click **Revert**.
4. Repeat steps two and three for 20412D-LON-SVR1, 20412D-LON-SVR2, 20412D-LON-CL1, and 20412D-LON-CL2.

**Results:** After completing this exercise, you will have configured Work Folders.

**Question:** How do file classifications enhance DAC usage?

**Question:** Can you implement DAC without central access policy?

# Lab: Implementing Distributed AD DS Deployments

## Scenario

A. Datum Corporation has deployed a single AD DS domain with all the domain controllers located in its London datacenter. As the company has grown and added branch offices with large numbers of users, it is becoming increasingly apparent that the current AD DS environment does not meet company requirements. The network team is concerned about the amount of AD DS-related network traffic that is crossing WAN links, which are becoming highly utilized.

The company has also become increasingly integrated with partner organizations, some of which need access to shared resources and applications that are located on the A. Datum internal network. The security department at A. Datum wants to ensure that the access for these external users is as secure as possible.

As one of the senior network administrators at A. Datum, you are responsible for implementing an AD DS infrastructure that will meet the company requirements. You are responsible for planning an AD DS domain and forest deployment that will provide optimal services for both internal and external users, while addressing the security requirements at A. Datum.

## Objectives

After completing this lab, you will be able to:

- Implement child domains in AD DS.
- Implement forest trusts in AD DS.

## Lab Setup

Estimated Time: 45 minutes

Virtual machines: 20412D-LON-DC1, 20412D-TOR-DC1

20412D-LON-SVR2, 20412D-TREY-DC1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following procedure:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In the Hyper-V® Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for 20412D-LON-SVR2 and 20412D-TOR-DC1.
6. Start 20412D-TREY-DC1, and sign in as **Treyresearch\Administrator** with the password **Pa\$\$w0rd**.

## Exercise 1: Implementing Child Domains in AD DS

### Scenario

A. Datum has decided to deploy a new domain in the adatum.com forest for the North American region. The first domain controller will be deployed in Toronto, and the domain name will be na.adatum.com. You need to configure and install the new domain controller.

The main tasks for this exercise are as follows:

1. Install a domain controller in a child domain.
2. Verify the default trust configuration.

#### ► Task 1: Install a domain controller in a child domain

1. On TOR-DC1, use the Server Manager to install the AD DS binaries.
2. When the AD DS binaries have installed, use the Active Directory Domain Services Configuration Wizard to install and configure TOR-DC1 as an AD DS domain controller for a new child domain named **na.adatum.com**.
3. When prompted, use **Pa\$\$w0rd** as the **Directory Services Restore Mode (DSRM)** password.

#### ► Task 2: Verify the default trust configuration

Sign in to TOR-DC1 as **NA\Administrator** with the password **Pa\$\$w0rd**.

1. When the Server Manager opens, click **Local Server**. Verify that **Windows Firewall** shows **Domain: Off**. If it does not, then next to **Local Area Connection**, click **172.16.0.25, IPv6 enabled**. Right-click **Local Area Connection**, and then click **Disable**. Right-click **Local Area Connection**, and then click **Enable**. The Local Area Connection should now show **Adatum.com**.
2. From the Server Manager, launch the **Active Directory Domains and Trusts** management console, and verify the parent child trusts.

 **Note:** If you receive a message that the trust cannot be validated, or that the secure channel (SC) verification has failed, ensure that you have completed step 2, and then wait for at least 10 to 15 minutes. You can continue with the lab and come back later to verify this step.

**Results:** After completing this exercise, you will have implemented child domains in AD DS.

## Exercise 2: Implementing Forest Trusts

### Scenario

A. Datum is working on several high-priority projects with a partner organization named Trey Research. To simplify the process of enabling access to resources located in the two organizations, companies have deployed a WAN between London and Munich, where Trey Research is located. You now need to implement and validate a forest trust between the two forests, and configure the trust to allow access to only selected servers in London.

The main tasks for this exercise are as follows:

- Configure stub zones for DNS name resolution.
- Configure a forest trust with selective authentication.
- Configure a server for selective authentication.
- To prepare for the next module

#### ► Task 1: Configure stub zones for DNS name resolution

1. On LON-DC1 using the DNS management console, configure a DNS stub zone for **TreyResearch.net**.
2. Use **172.16.10.10** as the Master DNS server.
3. Close DNS Manager.
4. Sign in to TREY-DC1 as **TreyResearch\Administrator** with the password **Pa\$\$w0rd**.

5. Using the DNS management console, configure a DNS stub zone for adatum.com.
6. Use **172.16.0.10** as the Master DNS server.
7. Close DNS Manager.

► **Task 2: Configure a forest trust with selective authentication**

1. On LON-DC1, create a one-way outgoing trust between the treyresearch.net AD DS forest and the adatum.com forest. Configure the trust to use Selective authentication.
2. On LON-DC1, confirm and validate the trust from TreyResearch.net.
3. Close Active Directory Domains and Trusts.

► **Task 3: Configure a server for selective authentication**

1. On LON-DC1, from the Server Manager, open **Active Directory Users and Computers**.
2. On LON-SVR2, configure the members of **TreyResearch\IT** group with the **Allowed to authenticate** permission. If you are prompted for credentials, type **TreyResearch\administrator** with the password **Pa\$\$w0rd**.
3. On LON-SVR2, create a shared folder named **IT-Data**, and grant **Read and Write** access to members of the **TreyResearch\IT** group. If you are prompted for credentials, type **TreyResearch\administrator** with the password **Pa\$\$w0rd**.
4. Sign out of TREY-DC1.
5. Sign in to TREY-DC1 as **TreyResearch\Alice** with the password **Pa\$\$w0rd**, and verify that you can access the shared folder on LON-SVR2.

► **Task 4: To prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for 20412D-TOR-DC1, 20412D-TREY-DC1, and 20412D-LON-SVR2.

**Results:** After completing this exercise, you will have implemented forest trusts.

**Question:** Why did you configure a delegated subdomain record in DNS on LON-DC1 before adding the child domain na.adatum.com?

**Question:** What are the alternatives to creating a delegated subdomain record in the previous question?

**Question:** When you create a forest trust, why would you create a selective trust instead of a complete trust?

# Lab: Implementing AD DS Sites and Replication

## Scenario

A. Datum Corporation has deployed a single AD DS domain, with all the domain controllers located in the London data center. As the company has grown and added branch offices with large numbers of users, it has become apparent that the current AD DS environment does not meet the company requirements. Users in some branch offices report that it can take a long time for them to sign in on their computers. Access to network resources such as the company's Microsoft Exchange® 2013 servers and the Microsoft SharePoint® servers can be slow, and they fail sporadically.

As one of the senior network administrators, you are responsible for planning and implementing an AD DS infrastructure that will help address the business requirements for the organization. You are responsible for configuring AD DS sites and replication to optimize the user experience and network utilization within the organization.

## Objectives

After completing this lab, you will be able to:

- Modify the default site created in AD DS.
- Create and configure additional sites and subnets.
- Configure AD DS replication.
- Monitor and troubleshoot AD DS replication.

## Lab Setup

Estimated Time: 45 minutes

|                  |                                  |
|------------------|----------------------------------|
| Virtual machines | 20412D-LON-DC1<br>20412D-TOR-DC1 |
| User Name        | <b>Adatum\Administrator</b>      |
| Password         | <b>Pa\$\$w0rd</b>                |

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following procedure:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
  - User name: **Adatum\Administrator**
  - Password: **Pa\$\$w0rd**
5. Repeat steps two through four for 20412D-TOR-DC1.

## Exercise 1: Modifying the Default Site

### Scenario

A. Datum Corporation has decided to implement additional AD DS sites to optimize the network utilization for AD DS network traffic. Your first step in implementing the new environment is to install a new domain controller for the Toronto site. You then will reconfigure the default site and assign appropriate IP address subnets to the site.

Finally, you have been asked to change the name of the default site to LondonHQ and associate it with the IP subnet 172.16.0.0/24, which is the subnet range used for the London head office.

The main tasks for this exercise are as follows:

1. Install the Toronto domain controller
2. Rename the default site
3. Configure IP subnets associated with the default site

#### ► Task 1: Install the Toronto domain controller

1. On TOR-DC1, use Server Manager to install **Active Directory Domain Services**.
2. When the AD DS binaries have installed, use the Active Directory Domain Services Configuration Wizard to install and configure TOR-DC1 as an additional domain controller for Adatum.com.
3. After the server restarts, sign in as **Adatum\Administrator** with the password of **Pa\$\$w0rd**.

#### ► Task 2: Rename the default site

1. If necessary, on LON-DC1, open the Server Manager console.
2. Open Active Directory Sites and Services, and then rename the **Default-First-Site-Name** site to **LondonHQ**.
3. Verify that both LON-DC1 and TOR-DC1 are members of the **LondonHQ** site.

#### ► Task 3: Configure IP subnets associated with the default site

1. If necessary, on LON-DC1, open the Server Manager console, and then open Active Directory Sites and Services.
2. Create a new subnet with the following configuration:
  - Prefix: **172.16.0.0/24**
  - Site object: **LondonHQ**

**Results:** After completing this exercise, you will have reconfigured the default site and assigned IP address subnets to the site.

## Exercise 2: Creating Additional Sites and Subnets

### Scenario

The next step you take to implement the AD DS site design is to configure the new AD DS site. The first site that you need to implement is the Toronto site for the North American datacenter. The network team in Toronto would also like to dedicate a site called TestSite in the Toronto datacenter. You have been instructed that the Toronto IP subnet address is 172.16.1.0/24, and the test network IP subnet address is 172.16.100.0/24.

The main tasks for this exercise are as follows:

1. Create the AD DS sites for Toronto
2. Create IP subnets associated with the Toronto sites

#### ► Task 1: Create the AD DS sites for Toronto

1. If necessary, on LON-DC1, open the Server Manager console, and then open Active Directory Sites and Services.
2. Create a new site with the following configuration:
  - Name: **Toronto**
  - Site link object: **DEFAULTIPSITELINK**
3. Create another new site with the following configuration:
  - Name: **TestSite**
  - Site link object: **DEFAULTIPSITELINK**

#### ► Task 2: Create IP subnets associated with the Toronto sites

1. If necessary, on LON-DC1, open Active Directory Sites and Services.
2. Create a new subnet with the following configuration:
  - Prefix: **172.16.1.0/24**
  - Site object: **Toronto**
3. Create another new subnet with the following configuration:
  - Prefix: **172.16.100.0/24**
  - Site object: **TestSite**
4. In the navigation pane, click the **Subnets** folder. Verify in the details pane that the two subnets are created and associated with their appropriate site.

**Results:** After this exercise, you will have created two additional sites representing the IP subnet addresses located in Toronto.

## Exercise 3: Configuring AD DS Replication

### Scenario

Now that the AD DS sites have been configured for Toronto, your next step is to configure the site-links to manage replication between the sites, and then to move the TOR-DC1 domain controller to the Toronto site. Currently, all sites belong to DEFAULTIPSITELINK.

You need to modify site-linking so that LondonHQ and Toronto belong to one common site-link called LON-TOR. You should configure this link to replicate every hour. Additionally, you should link the TestSite site only to the Toronto site using a site-link named TOR-TEST. Replication should not be available from the Toronto site to the TestSite during the working hours of 9 a.m. to 3 p.m. You then will use tools to monitor replication between the sites.

The main tasks for this exercise are as follows:

1. Configure site-links between AD DS sites
2. Move TOR-DC1 to the Toronto site
3. Monitor AD DS site replication

► **Task 1: Configure site-links between AD DS sites**

1. If necessary, on LON-DC1, open Active Directory Sites and Services.
2. Create a new IP-based site-link with the following configuration:
  - Name: **TOR-TEST**
  - Sites: **Toronto, TestSite**
  - Modify the schedule to only allow replication from **Monday 9 AM to Friday 3 PM**
3. Rename DEFAULTIPSITELINK, and configure it with the following settings:
  - Name: **LON-TOR**
  - Sites: **LondonHQ, Toronto**
  - Replication: Every **60 minutes**

► **Task 2: Move TOR-DC1 to the Toronto site**

1. If necessary, on LON-DC1, open Active Directory Sites and Services.
2. Move **TOR-DC1** from the **LondonHQ** site to the **Toronto** site.
3. Verify that TOR-DC1 is located under the Servers node in the Toronto site.

► **Task 3: Monitor AD DS site replication**

1. On LON-DC1, on the taskbar, click the **Windows PowerShell** icon.
2. Use the following commands to monitor site replication:

```
Repadmin /kcc
```

This command recalculates the inbound replication topology for the server.

```
Repadmin /showrep1
```

Verify that the last replication with TOR-DC1 was successful.

```
Repadmin /bridgeheads
```

This command displays the bridgehead servers for the site topology.

```
Repadmin /replsummary
```

This command displays a summary of replication tasks. Verify that no errors appear.

```
DCDiag /test:replications
```

Verify that all connectivity and replication tests pass successfully.

3. Switch to TOR-DC1, and then repeat the commands to view information from the TOR-DC1 perspective.

**Results:** After this exercise, you will have configured site-links and monitored replication.

## Exercise 4: Monitoring and Troubleshooting AD DS Replication

### Scenario

After AD DS sites and replication are established, A. Datum experiences replication issues. You must use monitoring and troubleshooting tools to diagnose the issue and resolve it.

The main tasks for this exercise are as follows:

1. Produce an error
2. Monitor AD DS site replication
3. Troubleshoot AD DS replication
4. To prepare for the next module

#### ► Task 1: Produce an error

1. On LON-DC1, in Active Directory Sites and Services, replicate TOR-DC1 with LON-DC1 from the LondonHQ site.
  2. In Windows PowerShell, run:
- ```
Get-ADReplicationUpToDateNessVectorTable -Target "adatum.com"
```
3. Observe the results, and note the date/time of the most recent replication event.
 4. Go to TOR-DC1, and execute the following Windows PowerShell script:
- ```
\LON-DC1\E$\Mod05\Mod05Ex4.ps1
```

#### ► Task 2: Monitor AD DS site replication

1. On TOR-DC1, in Active Directory Sites and Services, replicate **LON-DC1** with **TOR-DC1** from the **Toronto** site. Acknowledge the error.
2. In Windows PowerShell, run the following cmdlets, and observe the results:

```
Get-ADReplicationUpToDateNessVectorTable -Target "adatum.com"
Get-AdReplicationSubnet -filter *
Get-AdReplicationSiteLink-filter *
```

#### ► Task 3: Troubleshoot AD DS replication

1. On TOR-DC1, in Windows PowerShell, determine the IP address settings for the computer, and then run the following cmdlet:
- ```
Get-DnsClient | Set-DnsClientServerAddress -ServerAddresses
("172.16.0.10","172.16.0.25")
```
- Ensure that the IP address settings are correct.
2. Go to **Active Directory Sites and Services**, and replicate **LON-DC1** with **TOR-DC1** from the **Toronto** site. Acknowledge the error.
 3. Attempt to go to the **DNS Console**. Close any error windows.
 4. In Windows PowerShell, investigate the DNS Server service with the Get-Service cmdlet. If it is not running, start the service with the Start-Service cmdlet.
 5. Go to **Active Directory Sites and Services**, and replicate **LON-DC1** with **TOR-DC1** from the **Toronto** site. You should not get an error. Review the objects to determine if any are missing.

6. From **TOR-DC1**, open the following script in **Windows PowerShell ISI**:

```
\LON-DC1\E$\Mod05\Mod05Ex4Fix.ps1
```

7. Run the **recreate Site Links** and **recreate subnets** sections of the script.
8. Return to **Active Directory Sites and Services**, and determine if anything is still missing.
9. Close all open windows, and sign off **LON-DC1** and **TOR-DC1**.

► **Task 4: To prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start Hyper-V Manager.
2. On the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for 20412D-TOR-DC1.

Question: You decide to add a new domain controller to the LondonHQ site named LON-DC2. How can you ensure that LON-DC2 is used to pass all replication traffic to the Toronto site?

Question: You have added the new domain controller named LON-DC2 to the LondonHQ site. Which AD DS partitions will be modified as a result?

Question: In the lab, you created a separate site-link for the Toronto and TestSite sites. What might you also have to do to ensure that LondonHQ does not create a connection object directly with the TestSite site automatically?

Lab A: Deploying and Configuring a CA Hierarchy

Scenario

As A. Datum Corporation has expanded, its security requirements have also increased. The security department is particularly interested in enabling secure access to critical websites, and in providing additional security for features. To address these and other security requirements, A. Datum has decided to implement a PKI using the AD CS role in Windows Server 2012.

As one of the senior network administrators at A. Datum, you are responsible for implementing the AD CS deployment.

Objectives

After completing this lab, you will be able to:

- Deploy a stand-alone root CA.
- Deploy an enterprise subordinate CA.

Lab Setup

Estimated Time: 50 minutes

Virtual machines	20412D-LON-DC1 20412D-LON-SVR1 20412D-LON-SVR2 20412D-LON-CA1
User name	Adatum\Administrator
Password	Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
 - User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
5. Repeat steps two and three for 20412D-LON-SVR1, 20412D-LON-SVR2, and 20412D-LON-CA1. Do not sign in until instructed to do so.

Exercise 1: Deploying a Stand-Alone Root CA

Scenario

A. Datum wants to start using certificates for various purposes. You need to install the appropriate CA infrastructure. Because they are using Windows Server 2012 AD DS, you decided to implement the AD CS role. When you were reviewing available designs, you decided to implement a stand-alone root CA. This CA will be taken offline after it issues a certificate for subordinate CA.

The main tasks for this exercise are as follows:

1. Install and configure Active Directory Certificate Services on LON-CA1
2. Creating a DNS host record for LON-CA1 and configure sharing

► **Task 1: Install and configure Active Directory Certificate Services on LON-CA1**

1. Sign in to LON-CA1 as **Administrator** with the password **Pa\$\$w0rd**.
2. Use the Add Roles and Features Wizard to install the **Active Directory Certificate Services** role.
3. After installation completes successfully, click the text **Configure Active Directory Certificate Services on the destination server**.
4. Configure the AD CS role as a stand-alone root CA. Name it **AdatumRootCA**.
5. Set the key length to **4096**, and then accept all other values as default.
6. On LON-CA1, open the **Certification Authority** console.
7. Open the **Properties** dialog box for **AdatumRootCA**.
8. Configure new locations for the CDP to be **http://lon-svr1.adatum.com/CertData/<CaName><CRLONameSuffix><DeltaCRLAllowed>.crl**.
9. Select the following options:
 - **Include in the CDP extension of issued certificates**
 - **Include in CRLs. Clients use this to find Delta CRL locations**
10. Configure new locations for AIA to be on **http://lon-svr1.adatum.com/CertData/<ServerDNSName>_<CaName><CertificateName>.crt**
11. Select the **Include in the AIA extension of issued certificates** check box.
12. Publish the CRL on LON-CA1.
13. Export the root CA certificate, and then copy the .cer file to **\\\lon-svr1\C\$**.
14. Copy the contents of folder **C:\Windows\System32\CertSrv\CertEnroll** to **\\\lon-svr1\C\$**.

► **Task 2: Creating a DNS host record for LON-CA1 and configure sharing**

1. On LON-DC1, open the DNS Manager console.
2. Create a host record for LON-CA1 in the Adatum.com forward lookup zone.
3. Use IP address **172.16.0.40** for the LON-CA1 host record.
4. On LON-CA1, from the Network and Sharing Center, turn on file and printer sharing on guest and public networks.

Results: After completing this exercise, you will have deployed a root stand-alone certification authority (CA).

Exercise 2: Deploying an Enterprise Subordinate CA

Scenario

After you deploy the stand-alone root CA, the next step is to deploy an enterprise subordinate CA. A. Datum wants to use an enterprise subordinate CA to utilize AD DS integration. In addition, because the root CA is stand-alone, you want to publish its certificate to all clients.

The main tasks for this exercise are as follows:

1. Install and configure AD CS on LON-SVR1
2. Install a subordinate CA certificate
3. Publish the root CA certificate through Group Policy
4. Prepare for the next lab

► Task 1: Install and configure AD CS on LON-SVR1

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Install the Active Directory Certificate Services role on LON-SVR1. Include the **Certification Authority** and **Certification Authority Web Enrollment** role services.
3. After installation is successful, click **Configure Active Directory Certificate Services on the destination server**.
4. Select the **Certification Authority** and **Certification Authority Web Enrollment** role services.
5. Configure LON-SVR1 to be an **Enterprise CA**.
6. Configure the CA Type to be a **Subordinate CA**.
7. For the CA Name, type **Adatum-IssuingCA**.
8. Save the request file to the local drive.

► Task 2: Install a subordinate CA certificate

1. On LON-SVR1, install the **C:\RootCA.cer** certificate to the Trusted Root Certification Authority store.
2. Navigate to **Local Disk (C:)**, and copy the **AdatumRootCA.crl** and **LON-CA1_AdatumRootCA.crt** files to **C:\inetpub\wwwroot\CertData**.
3. Copy the **LON-SVR1.Adatum.com_Adatum-LON-SVR1-CA.req** request file to **\\\LON-CA1\c\$**.
4. Switch to LON-CA1.
5. From the Certification Authority console on LON-CA1, submit a new certificate request by using the .req file that you copied in step 3.
6. Issue the certificate, and then export it to .p7b format with a complete chain. Save the file to **\\\lon-svr1\c\$\SubCA.p7b**.
7. Switch to LON-SVR1.
8. Install the subordinate CA certificate on LON-SVR1 by using the Certification Authority console.
9. Start the service.

► **Task 3: Publish the root CA certificate through Group Policy**

1. On LON-DC1, from the Server Manager, open the Group Policy Management Console.
2. Edit the Default Domain Policy.
3. Publish the **RootCA.cer** file from **\\\lon-svr1\C\$** to the Trusted Root Certification Authorities store, which is located in **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies**.

► **Task 4: Prepare for the next lab**

Keep all virtual machines running for the next lab. Do not revert any virtual machines.

Results: After completing this exercise, you will have deployed and configured an enterprise subordinate CA.

Question: Why is it not recommended to install just an enterprise root CA?

Lab B: Deploying and Managing Certificates

Scenario

As A. Datum Corporation has expanded, its security requirements have also increased. The security department is particularly interested in enabling secure access to critical websites, and in providing additional security for features such as drive encryption, smart cards, and the Windows 7 and Windows 8 DirectAccess feature. To address these and other security requirements, A. Datum has decided to implement a PKI using the AD CS role in Windows Server 2012.

As one of the senior network administrators at A. Datum, you are responsible for implementing the AD CS deployment. You will deploy the CA hierarchy, develop the procedures and process for managing certificate templates, and deploy and revoke certificates.

Objectives

After completing this lab, you will be able to:

- Configure certificate templates.
- Configure certificate enrollment.
- Configure certificate revocation.
- Configure and perform private key archival and recovery.

Lab Setup

Estimated Time: 75 minutes

Virtual machines	20412D-LON-DC1 20412D-LON-SVR1 20412D-LON-SVR2 20412D-LON-CA1 20412D-LON-CL1
User name	Adatum\Administrator
Password	Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. All virtual machines needed for this lab should be running from the previous lab.

Exercise 1: Configuring Certificate Templates

Scenario

After deploying the CA infrastructure, the next step is to deploy the certificate templates that are required in the organization. First, A. Datum wants to implement a new Web server certificate and implement smart card certificates for users. They also want to implement new certificates on the LON-SVR2 web server.

The main tasks for this exercise are as follows:

1. Create a new template based on the web server template
2. Create a new template for users that includes smart card logon
3. Configure the templates so that they can be issued
4. Update the web server certificate on the LON-SVR2 web server

► **Task 1: Create a new template based on the web server template**

1. On LON-SVR1, from the Certification Authority console, open the Certificate Templates console.
2. Duplicate the **Web Server** template.
3. Create a new template and name it **Adatum WebSrv**.
4. Configure validity for **3 years**.
5. Configure the private key as exportable.

► **Task 2: Create a new template for users that includes smart card logon**

1. In the Certificate Templates console, duplicate the **User** certificate template.
2. Name the new template **Adatum User**.
3. On the **Subject Name** tab, clear both the **Include e-mail name in subject name** and the **E-mail name** check boxes.
4. Add **Smart Card Logon** to the Application Policies of the new certificate template.
5. Configure this new template to supersede the **User** template.
6. Allow Authenticated Users to **Read**, **Enroll**, and **Autoenroll** for this certificate.
7. Close the Certificate Templates console.

► **Task 3: Configure the templates so that they can be issued**

- Configure LON-SVR1 to issue certificates based on the **Adatum User** and **Adatum WebSrv** templates.

► **Task 4: Update the web server certificate on the LON-SVR2 web server**

1. Sign in to LON-SVR2 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Refresh Group Policy, and restart the server if necessary.
3. From the Server Manager, open the **Internet Information Services (IIS) Manager**.
4. Enroll for a domain certificate using the following parameters:
 - Common name: **lon-svr2.adatum.com**
 - Organization: **Adatum**
 - Organizational Unit: **IT**
 - City/locality: **Seattle**
 - State/province: **WA**
 - Country/region: **US**
 - Friendly name: **lon-svr2**
5. Create HTTPS binding for the Default Web Site, and associate it with a new certificate.

Results: After completing this exercise, you will have created and published new certificate templates.

Exercise 2: Configuring Certificate Enrollment

Scenario

The next step in implementing the PKI at A. Datum is to configure certificate enrollment. A. Datum wants to enable different options for distributing the certificates. Users should be able to enroll automatically, and smart card users should get their smart cards from an Enrollment Agent. A. Datum has delegated Enrollment Agent rights for the Marketing department group to user Allie Bellew.

The main tasks for this exercise are as follows:

1. Configure autoenrollment for users
2. Verify autoenrollment
3. Configure the Enrollment Agent for smart card certificates

► Task 1: Configure autoenrollment for users

1. On LON-DC1, open Group Policy Management.
2. Edit the Default Domain Policy.
3. Navigate to **User Configuration/Policies/Windows Settings/Security Settings**, and then click to highlight **Public Key Policies**.
4. Enable the **Certificate Services Client – Auto-Enrollment** option, and enable **Renew expired certificates, update pending certificates, and remove revoked certificates** and **Update certificates that use certificate templates**.
5. Enable the **Certificate Services Client – Certificate Enrollment Policy**.
6. Close Group Policy Management Editor and the Group Policy Management console.

► Task 2: Verify autoenrollment

1. On LON-SVR1, open the Windows PowerShell and use **gpupdate /force** to refresh Group Policy.
2. Open an mmc.exe console and add the Certificates snap-in focused on the user account.
3. Verify that you have been issued a certificate based on the **Adatum Smart Card User** template.

► Task 3: Configure the Enrollment Agent for smart card certificates

1. On LON-SVR1, from the Certification Authority console, open the Certificate Templates console.
2. Allow **Allie Bellew** to enroll for an Enrollment Agent certificate.
3. Publish the Enrollment Agent certificate template.
4. Sign in to **LON-CL1** as **Allie**, and enroll for an Enrollment Agent certificate.
5. On LON-SVR1, open properties of **Adatum-IssuingCA**, and configure **Restricted Enrollment Agent** so that Allie can only issue certificates based on **Adatum User**, for security group **Marketing**.

Results: After completing this exercise, you will have configured and verified autoenrollment for users, and configured an Enrollment Agent for smart cards.

Exercise 3: Configuring Certificate Revocation

Scenario

As part of configuring the certificate infrastructure, A. Datum wants to configure revocation components on newly established CAs. You will configure CRL and Online Responder components.

The main tasks for this exercise are as follows:

1. Configure certified revocation list (CRL) distribution
2. Install and configure an Online Responder

► Task 1: Configure certified revocation list (CRL) distribution

1. On LON-SVR1, in the Certification Authority console, right-click **Revoked Certificates**, and then click **Properties**.
2. Set the CRL publication interval to **1 Days**, and set the **Delta CRL** publication interval to **1 Hours**.
3. Review CDP locations on **Adatum-IssuingCA**.

► Task 2: Install and configure an Online Responder

1. On LON-SVR1, use the Server Manager to add an Online Responder role service to the existing AD CS role.
2. When the message displays that installation succeeded, click **Configure Active Directory Certificate Services on the destination server**.
3. Configure the online responder.
4. On LON-SVR1, open the Certification Authority console.
5. Configure the new AIA distribution location on **Adatum-IssuingCA** to be **http://lon-svr1/ocsp**.
6. On **Adatum-IssuingCA**, publish the OCSP Response signing certificate template, and then allow **Authenticated** users to enroll.
7. Open the Online Responder Management console.
8. Add revocation configuration for **Adatum-IssuingCA**.
9. Enroll for an OCSP Response signing certificate.
10. Ensure that the revocation configuration status is **Working**.

Results: After completing this exercise, you will have configured certificate revocation settings.

Exercise 4: Configuring Key Recovery

Scenario

As a part of establishing a PKI, you want to configure and test procedures for the recovery of private keys. You want to assign a KRA certificate for an administrator, and configure CA and specific certificate templates to allow key archiving. In addition, you want to test a procedure for key recovery.

The main tasks for this exercise are as follows:

1. Configure the CA to issue KRA certificates
2. Acquire the KRA certificate
3. Configure the CA to allow key recovery
4. Configure a custom template for key archival
5. Verify key archival functionality
6. Prepare for the next module

► **Task 1: Configure the CA to issue KRA certificates**

1. On LON-SVR1, in the Certification Authority console, right-click the **Certificates Templates** folder, and then click **Manage**.
2. In the Certificates Templates console, open the **Key Recovery Agent certificate properties** dialog box.
3. On the **Issuance Requirements** tab, clear the **CA certificate manager approval** check box.
4. On the **Security** tab, notice that only Domain Admins and Enterprise Admins groups have the **Enroll** permission.
5. Right-click the **Certificates Templates** folder, and enable the **Key Recovery Agent** template.

► **Task 2: Acquire the KRA certificate**

1. Create an MMC console window that includes having the Certificates snap-in for the current user loaded.
2. Use the Certificate Enrollment Wizard to request a new certificate and to enroll the KRA certificate.
3. Refresh the console window, and view the KRA in the personal store.

► **Task 3: Configure the CA to allow key recovery**

1. On LON-SVR1, open the Certification Authority console.
2. On LON-SVR1, in the Certification Authority console, open the **Adatum-IssuingCA Properties** dialog box.
3. On the **Recovery Agents** tab, click **Archive the key**, and then add the certificate by using the **Key Recovery Agent Selection** dialog box.
4. Restart Certificate Services when prompted.

► **Task 4: Configure a custom template for key archival**

1. On LON-SVR1, open the Certificates Templates console.
2. Duplicate the User template, and name it **Archive User**.
3. On the **Request Handling** tab, set the option for the **Archive subject's encryption private key**. By using the archive key option, the KRA can obtain the private key from the certificate store.
4. Click the **Subject Name** tab, and then clear both the **E-mail name** and **Include e-mail name in subject name** check boxes.
5. Add the **Archive User template** as a new certificate template to issue.

► **Task 5: Verify key archival functionality**

1. Sign in to LON-CL1 as **Adatum\Aidan**, using the password **Pa\$\$w0rd**.
2. Create an MMC console window that includes the Certificates snap-in.
3. Request and enroll a new certificate based on the **Archive User** template.
4. From the personal store, locate the Archive User certificate.
5. Delete the certificate for Aidan to simulate a lost key.
6. Switch to LON-SVR1.
7. Open the Certification Authority console, expand **Adatum-IssuingCA**, and then click the **Issued Certificates** store.

8. In the Certificate Authority console, note the serial number of the certificate that has been issued for Aidan Delaney.
9. On LON-SVR1, open a command prompt, and then type the following command:

```
Certutil -getkey <serial number> outputblob
```

-  **Note:** Replace serial number with the serial number that you wrote down.

10. Verify that the **Outputblob** file now displays in the C:\Users\Administrator folder.
11. To convert the **Outputblob** file into an importable .pfx file, at the command prompt, type the following command:

```
Certutil-recoverkey outputblob aidan.pfx
```

12. Enter the password **Pa\$\$w0rd** for the certificate.
13. Verify the creation of the recovered key in the C:\Users\Administrator folder.
14. Switch to the LON-CL1 machine.
15. Open the Network and Sharing Center item in Control Panel, and then enable file and printer sharing for guest or public network profiles.
16. Switch back to LON-SVR1 and then copy and paste the **aidan.pfx** file to the root of drive C on LON-CL1.
17. Switch to LON-CL1, and import the **aidan.pfx** certificate.
18. Verify that the certificate displays in the Personal store.

► Task 6: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start Hyper-V Manager.
2. On the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for 20412D-LON-CL1, 20412D-LON-SVR1, 20412D-LON-CA1, and 20412D-LON-SVR2.

Results: After completing this exercise, you will have implemented key archival and tested private key recovery.

Question: What is the main benefit of OCSP over CRL?

Question: What must you do to recover private keys?

Lab: Implementing AD RMS

Scenario

Because of the highly confidential nature of the research that is performed at A. Datum Corporation, the security team at A. Datum wants to implement additional security for certain documents that the Research department creates. The security team is concerned that anyone with Read access to the documents can modify and distribute the documents in any way that they choose. The security team would like to provide an extra level of protection that stays with the document even if it is moved around the network or outside the network.

As one of the senior network administrators at A. Datum, you need to plan and implement an AD RMS solution that will provide the level of protection requested by the security team. The AD RMS solution must provide many different options that can be adapted for a wide variety of business and security requirements.

Objectives

- Install and configure AD RMS.
- Configure AD RMS Templates.
- Implement AD RMS Trust Policies.
- Verify AD RMS Deployment.

Lab Setup

Estimated Time: 60 minutes

Virtual machines: 20412D-LON-DC1, 20412D-LON-SVR1,
20412D-LON-CL1, 20412D-TREY-DC1,
20412D-TREY-CL1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
 - User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
5. Repeat step 2 for 20412D-LON-SVR1, 20412D-TREY-DC1, 20412D-LON-CL1, and 20412D-TREY-CL1. Do not sign in until directed to do so.

Exercise 1: Installing and Configuring Active Directory® Rights Management Services (AD RMS)

Scenario

The first step in deploying AD RMS at A. Datum is to deploy a single server in an AD RMS cluster. You will begin by configuring the appropriate DNS records and the AD RMS service account. Then you will install and configure the first AD RMS server. You will also enable the AD RMS Super Users group.

The main tasks for this exercise are as follows:

1. Configure DNS and configure an AD RMS service account.
2. Install and configure the AD RMS server role.
3. Configure the AD RMS Super Users group.

► Task 1: Configure DNS and configure an AD RMS service account

1. Sign in to LON-DC1 with the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.
2. Use the Active Directory Administrative Center to create an OU named **Service Accounts** in the adatum.com domain.
3. Create a new user account in the Service Accounts OU with the following properties:
 - First name: **ADRMSSVC**
 - User UPN logon: **ADRMSSVC**
 - Password: **Pa\$\$w0rd**
 - Confirm Password: **Pa\$\$w0rd**
 - Password never expires: **Enabled**
 - User cannot change password: **Enabled**
4. Create a new Global security group in the Users container named **ADRMS_SuperUsers**. Set the email address of this group as **ADRMS_SuperUsers@adatum.com**.
5. Create a new global security group in the Users container named **Executives**. Set the email address of this group as **executives@adatum.com**.
6. Add the user accounts **Aidan Delaney** and **Bill Malone** to the Executives group.
7. Use the DNS Manager console to create a host (A) resource record in the adatum.com zone with the following properties:
 - Name: **adrms**
 - IP Address: **172.16.0.21**

► Task 2: Install and configure the AD RMS server role

1. Sign in to LON-SVR1 with the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.
2. Use the Add Roles and Features Wizard to add the Active Directory Rights Management Services role to LON-SVR1 using the following option:
 - Role services: **Active Directory Rights Management Services**
3. From the AD RMS node in the **Server Manager**, click **More** to start post deployment configuration of AD RMS.

4. On the AD RMS Configuration Wizard, provide the following information:
 - **Create a new AD RMS root cluster**
 - **Use Windows Internal Database on this server**
 - Service account: **Adatum\ADRMSSVC**
 - Cryptographic Mode: **Cryptographic Mode 2**
 - Cluster Key Storage: **Use AD RMS centrally managed key storage**
 - Cluster Key Password: **Pa\$\$w0rd**
 - Cluster Web Site: **Default Web Site**
 - Connection Type: **Use an unencrypted connection**
 - Fully Qualified Domain Name: **http://adrms.adatum.com**
 - Port: **80**
 - Licenser Certificate: **Adatum AD RMS**
 - Register AD RMS Service Connection Point: **Register the SCP Now**
5. Use the Internet Information Services (IIS) Manager console to enable Anonymous Authentication on the **Default Web Site\wmcs** and the **Default Web Site\wmcs\licensing** virtual directories.
6. Sign out of LON-SVR1.



Note: You must sign out before you can manage AD RMS. This lab uses port 80 for convenience. In production environments, you would protect AD RMS using an encrypted connection.

► Task 3: Configure the AD RMS Super Users group

1. Sign in to LON-SVR1 with the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.
2. Open the Active Directory Rights Management Services console.
3. From the Active Directory Rights Management Services console, enable **Super Users**.
4. Set the **ADRMS_SuperUsers** group as the Super Users group.

Results: After completing this exercise, you should have installed and configured AD RMS.

Exercise 2: Configuring AD RMS Templates

Scenario

After you deploy the AD RMS server, you must configure the rights policy templates and exclusion policies for the organization. You will then deploy both components.

The main tasks for this exercise are as follows:

1. Configure a new rights policy template.
2. Configure the rights policy template distribution.
3. Configure an exclusion policy.

► Task 1: Configure a new rights policy template

- On LON-SVR1, use the Rights Policy Template node of the Active Directory Rights Management Services console to create a Distributed Rights Policy Template with the following properties:
 - Language: **English (United States)**
 - Name: **ReadOnly**
 - Description: **Read only access. No copy or print**
 - Users and rights: **executives@adatum.com**
 - Rights for Anyone: **View**
 - **Grant owner (author) full control right with no expiration**
 - Content Expiration: **7 days**
 - Use license expiration: **7 days**
 - Require a new use license: **every time content is consumed (disable client-side caching)**

► Task 2: Configure the rights policy template distribution

1. On LON-SVR1, open a Windows PowerShell prompt, and then issue the following commands, pressing Enter at the end of each line:

```
New-Item c:\rmstemplates -ItemType Directory
New-SmbShare -Name RMSTEMPLATES -Path c:\rmstemplates -FullAccess ADATUM\ADRMSSVC
New-Item c:\docshare -ItemType Directory
New-SmbShare -Name docshare -Path c:\docshare -FullAccess Everyone
```

2. In the Active Directory Rights Management Services console, set the Rights Policy Templates file location to **\LON-SVR1\RMSTEMPLATES**.
3. In File Explorer, view the c:\rmstemplates folder. Verify that the **ReadOnly.xml** template displays.

► Task 3: Configure an exclusion policy

1. In the Active Directory Rights Management Services console, enable Application exclusion.
2. In the **Exclude Application** dialog box, enter the following information:
 - Application File name: **Powerpnt.exe**
 - Minimum version: **14.0.0.0**
 - Maximum version: **16.0.0.0**

Results: After completing this exercise, you should have configured AD RMS templates.

Exercise 3: Implementing the AD RMS Trust Policies

Scenario

As part of the AD RMS deployment, you need to ensure that AD RMS functionality is extended to the Trey Research AD RMS deployment. You will configure the required trust policies, and then validate that you can share protected content between the two organizations.

The main tasks for this exercise are as follows:

1. Export the Trusted User Domains policy.
2. Export the Trusted Publishing Domains policy.
3. Import the Trusted User Domain policy from the partner domain.
4. Import the Trusted Publishing Domains policy from the partner domain.

► Task 1: Export the Trusted User Domains policy

1. On LON-SVR1, open a Windows PowerShell prompt, and then issue the following commands, pressing Enter at the end of each line:

```
New-Item c:\export -ItemType Directory  
New-SmbShare -Name Export -Path c:\export -FullAccess Everyone
```

2. Use the Active Directory Rights Management Services console to export the TUD policy to the **\LON-SVR1\export** share as **ADATUM-TUD.bin**.
3. Sign in to TREY-DC1 with the **TREYRESEARCH\Administrator** account and the password **Pa\$\$w0rd**.
4. On TREY-DC1, open the Active Directory Rights Management Services console.
5. Export the **Trusted User Domains** policy to the **\LON-SVR1\export** share as **TREYRESEARCH-TUD.bin**.
6. On TREY-DC1, open a Windows PowerShell prompt, issue the following command, and then press Enter:

```
Add-DnsServerConditionalForwarderZone -MasterServers 172.16.0.10 -Name adatum.com
```

► Task 2: Export the Trusted Publishing Domains policy

1. Switch to LON-SVR1.
2. Use the Active Directory Rights Management Services console to export the TPD policy to the **\LON-SVR1\export** share as **ADATUM-TPD.xml**. Protect this file by using the password **Pa\$\$w0rd**.
3. Switch to TREY-DC1.
4. Use the Active Directory Rights Management Services console to export the TPD policy to the **\LON-SVR1\export** share as **TREYRESEARCH-TPD.xml**.
5. Protect this file by using the password **Pa\$\$w0rd**.

► **Task 3: Import the Trusted User Domain policy from the partner domain**

1. Switch to LON-SVR1.
2. Import the TUD policy for Trey Research by importing the file **\LON-SVR1\export\treyresearch-tud.bin**. Use the display name **TreyResearch**.
3. Switch to TREY-DC1.
4. Import the TUD policy for Trey Research by importing the file **\LON-SVR1\export\adatum-tud.bin**. Use the display name **Adatum**.

► **Task 4: Import the Trusted Publishing Domains policy from the partner domain**

1. Switch to LON-SVR1.
2. Import the Trey Research TPD by importing the file **\LON-SVR1\export\TREYRESEARCH-TPD.xml**, using the password **Pa\$\$w0rd** and the display name **Trey Research**.
3. Switch to TREY-DC1.
4. Import the Adatum Trusted Publishing Domain by importing the file **\LON-SVR1\export\adatum-tpd.xml**, using the password **Pa\$\$w0rd**, and the display name **Adatum**.

Results: After completing this exercise, you should have implemented the AD RMS trust policies.

Exercise 4: Verifying AD RMS on a Client

Scenario

As a final step in the deployment, you will validate that the configuration is working correctly.

The main tasks for this exercise are as follows:

1. Create a rights-protected document.
2. Verify internal access to protected content.
3. Open the rights-protected document as an unauthorized user.
4. Open and edit the rights-protected document as an authorized user at Trey Research.
5. To prepare for the next module.

► Task 1: Create a rights-protected document

1. Sign in to LON-CL1 with the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.
2. Add **Aidan**, **Bill**, and **Carol** as local Remote Desktop Users in the **Systems** properties.
3. Sign out of LON-CL1.
4. Sign in to LON-CL1 with the **Adatum\Aidan** account and the password **Pa\$\$w0rd**.
5. Add the **http://adrms.adatum.com** URL to the Local intranet group on the Internet options **Security** tab using the **Advanced** button in Sites.

 **Note:** This above step is necessary for the Office program to find the proper AD RMS Cluster URL. It must be in the local intranet sites, and it must be done for each user.

6. Open **Word 2013**.
7. Create a document named **Executives Only**.
8. In the document, type the following text:

This document is for executives only, it should not be modified.

1. From the Permissions item, choose to restrict access. Grant **bill@adatum.com** permission to read the document.
2. Save the document in the share **\\\lon-svr1\docshare**.
3. Sign out of LON-CL1.

► Task 2: Verify internal access to protected content

1. Sign in to LON-CL1 with the **Adatum\Bill** account using the password **Pa\$\$w0rd**.
2. Add the **http://adrms.adatum.com** URL to the **Local intranet** group on the Internet options **Security** tab using the **Advanced** button in Sites.
3. In the **\\\lon-svr1\docshare** folder, open the **Executives Only** document.
4. When prompted, provide the credentials **Adatum\Bill** with the password of **Pa\$\$w0rd**.

5. Verify that you are unable to modify or save the document.
6. Select a line of text in the document.
7. Right-click the line of text. Verify that you cannot modify this text.
8. View the document permissions.
9. Sign out of LON-CL1.

► **Task 3: Open the rights-protected document as an unauthorized user**

1. Sign in to LON-CL1 as **Adatum\Carol** using the password **Pa\$\$w0rd**.
2. Add the **http://adrms.adatum.com** URL to the Local intranet group on Internet options **Security** tab using the **Advanced** button in Sites.
3. In the **\lon-svr1\docshare** folder, attempt to open the **Executives Only** document.
4. Verify that Carol does not have permission to open the document.
5. Sign out of LON-CL1.

► **Task 4: Open and edit the rights-protected document as an authorized user at Trey Research**

1. Sign in to LON-CL1 with the **Adatum\Aidan** account using the password **Pa\$\$w0rd**.
2. Open Word 2013.
3. Create a new document named **\LON-SVR1\docshare\TreyResearch-Confidential.docx**.
4. In the document, type the following text:

This document is for Trey Research only, it should not be modified.

1. Restrict the permission so that **april@treyresearch.net** is able to open the document.
2. Sign in to Trey-CL1 with the **TREYRESEARCH\Administrator** account and the password **Pa\$\$w0rd**.
3. Add April as local Remote Desktop Users in the **Systems** properties.
4. Sign out of Trey-CL1.
5. Sign in to TREY-CL1 as **TREYRESEARCH\April** with the password **Pa\$\$w0rd**.
6. Add the **http://adrms.treyresearch.net** URL to the Local intranet group in Internet options Security tab using the **Advanced** button in Sites.
7. Use File Explorer to navigate to **\LON-SVR1\docshare**.
8. Use the credentials **Adatum\Administrator** and **Pa\$\$w0rd** to connect.
9. Copy the **TreyReserch-Confidential.docx** document to the desktop.
10. Attempt to open the document. When prompted, enter the following credentials, select the **Remember my credentials** check box, and then click **OK**:
 - a. Username: **April**
 - b. Password: **Pa\$\$w0rd**
11. Verify that you can open the document, but that you cannot make modifications to it.
12. View the permissions that the **april@treyresearch.com** account has for the document.

► **Task 5: To prepare for the next module**

When you finish the lab, revert the virtual machines to their initial state. To do this, complete the following steps.

1. On the host computer, start Hyper-V Manager.
2. In the Virtual Machines list, right-click **20412C-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for 20412C-LON-SVR1, 20412C-TREY-DC1, 20412C-LON-CL1, and 20412C-TREY-CL1.

Results: After completing this exercise, you should have verified that the AD RMS deployment is successful.

Question: What considerations should you make and steps you can take when you use the AD RMS role?

Lab A: Implementing AD FS

Scenario

A. Datum Corporation has set up a variety of business relationships with other companies and customers. Some of these partner companies and customers must access business applications that are running on the A. Datum network. The business groups at A. Datum want to provide a maximum level of functionality and access to these companies. The Security and Operations departments want to ensure that the partners and customers can access only the resources to which they require access, and that implementing the solution does not increase the workload for the Operations team significantly. A. Datum also is working on migrating some parts of its network infrastructure to Microsoft Online Services, including Windows Azure and Office 365.

To meet these business requirements, A. Datum plans to implement AD FS. In the initial deployment, the company plans to use AD FS to implement SSO for internal users who access an application on a Web server.

As one of the senior network administrators at A. Datum, it is your responsibility to implement the AD FS solution. As a proof-of-concept, you plan to deploy a sample claims-aware application, and you will configure AD FS to enable internal users to access the application.

Objectives

After completing this lab, you will be able to:

- Install and configure AD FS.
- Configure an internal application for AD FS.

Lab Setup

Estimated Time: 30 minutes

Virtual machines: 20412D-LON-DC1,

20412D-LON-SVR1,

20412D-LON-CL1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20412D-LON-DC1**, and then in the Actions pane, click **Start**.
3. In the **Actions** pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
 - User name: Adatum\Administrator
 - Password: **Pa\$\$w0rd**
5. Repeat steps 2 and 3 for 20412D-LON-SVR1 and 20412D-LON-CL1.
 - a. Sign in to 20412D-LON-SVR1 as **Adatum\Administrator**.
 - b. Do not sign in to 20412D-LON-CL1.

Exercise 1: Installing and Configuring AD FS

Scenario

To start the AD FS implementation, you need to install AD FS on an A. Datum domain controller. During the initial deployment, you will configure it as the first server in a farm, with the option for later expansion. The certificate for AD FS already has been installed on LON-DC1.

The main tasks for this exercise are as follows:

1. Create a DNS record for AD FS.
2. Create a service account.
3. Install AD FS.
4. Configure AD FS.
5. Verify AD FS functionality.

► Task 1: Create a DNS record for AD FS

- On LON-DC1, use the DNS Manager to add a new host record for AD FS:
 - Forward lookup zone: **Adatum.com**
 - Name: **adfs**
 - IP address: **172.16.0.10**

► Task 2: Create a service account

1. On LON-DC1, open a Windows PowerShell prompt.
2. Create a new user account:
 - **New-ADUser –Name adfsService**
3. Set a password for adfsService:
 - **Set-ADAccountPassword adfsService**
 - Current password: none (press Enter)
 - **Desired password:** Pa\$\$w0rd
4. Enable the adfsService account:
 - **Enable-ADAccount adfsService**

► Task 3: Install AD FS

- On LON-DC1, in the Server Manager, add the Active Directory Federation Services role.

► Task 4: Configure AD FS

1. On LON-DC1, in the Server Manager notifications, click **Configure the federation services on this server.**
2. Use the following options to configure the AD FS server:
 - **Create the first federation server in a federation server farm**
 - Account for configuration: Adatum\Administrator
 - SSL Certificate: adfs.adatum.com

- Federation Service Display Name: **A. Datum Corporation**
 - Use an existing domain user account or group Managed Service Account:
 - Adatum\adfsService
 - **Password:** Pa\$\$w0rd
 - **Create a database on this server using Windows Internal Database**



Note: The adfs.adatum.com certificate was preconfigured for this task. In your own environment, you need to obtain this certificate.

► Task 5: Verify AD FS functionality

1. On LON-CL1, sign in as **Adatum\Brad** with the password **Pa\$\$w0rd**.
2. Use Internet Explorer to access **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**.
3. Verify that the file loads, and then close Internet Explorer.

Results: In this exercise, you installed and configured AD FS. You also verified that it is functioning by viewing the FederationMetaData.xml file contents.

Exercise 2: Configuring an Internal Application for AD FS

Scenario

The first scenario for implementing the proof-of-concept AD FS application is to ensure that internal users can use SSO to access the web application. You plan to configure the AD FS server and a web application to enable this scenario. You also want to verify that internal users can access the application.

The main tasks for this exercise are as follows:

1. Configure a certificate for the application.
2. Configure the Active Directory claims-provider trust.
3. Configure the application to trust incoming claims.
4. Configure a relying-party trust for the claims-aware application.
5. Configure claim rules for the relying-party trust.
6. Test access to the claims-aware application.
7. Configure Internet Explorer to pass local credentials to the application automatically.

► Task 1: Configure a certificate for the application

1. On LON-SVR1, open Internet Information Services (IIS) Manager, and then view the server certificates.
2. Create a new domain certificate with the following settings:
 - Common name: **lon-svr1.adatum.com**
 - Organization: **A. Datum**
 - Organizational unit: **IT**
 - City/locality: **London**
 - State/Province: **England**
 - Country/region: **GB**
 - Certification Authority: **AdatumCA**
 - Friendly name: **AdatumTestApp Certificate**
3. Add an https binding for the Default Web Site:
 - SSL certificate: **AdatumTestApp Certificate**

► Task 2: Configure the Active Directory claims-provider trust

1. On LON-DC1, in the Server Manager, open the AD FS Management tool.
2. Browse to the **Claims Provider Trusts**, and then edit the claim rules for **Active Directory**.
3. Add an acceptance transform rule with the following settings:
 - Claim rule template: **Send LDAP attributes as claims**
 - Name: **Outbound LDAP Attributes Rule**
 - Attribute store: **Active Directory**
 - Mapping of LDAP attributes:
 - E-Mail-Addresses: **E-Mail Address**
 - User-Principal-Name: **UPN**
 - Display-Name: **Name**

► **Task 3: Configure the application to trust incoming claims**

1. On LON-SVR1, in the Server Manager, open the Windows Identity Foundation Federation Utility tool.
2. Enter the following in the Federation Utility Wizard:
 - Application configuration location: **C:\inetpub\wwwroot\AdatumTestApp\web.config**
 - Application URI: **https://lon-svr1.adatum.com/AdatumTestApp/**
 - **Use an existing STS**
 - STS WS-Federation metadata document location:
https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml
 - **Disable certificate chain validation**
 - **No encryption**

► **Task 4: Configure a relying-party trust for the claims-aware application**

1. On LON-DC1, in the AD FS console, add a relying-party trust with the following settings:
 - **Import data about the relying party published online or on a local network**
 - Federation Metadata address: **https://lon-svr1.adatum.com/adatumtestapp/**
 - Display name: **A. Datum Test App**
 - **I do not want to configure multi-factor authentication settings for this relying party trust at this time**
 - **Permit all users to access this relying party**
2. Leave the Edit Claim Rules for A. Datum Test App window open for the next task.

► **Task 5: Configure claim rules for the relying-party trust**

1. On LON-DC1, in the Edit Claim Rules for A. Datum Test App window, add a rule on the **Issuance Transform Rules** tab.
2. Complete the Add Transform Claim Rule Wizard with the following settings:
 - Claim rule template: **Pass Through or Filter an Incoming Claim**
 - Claim rule name: **Pass through Windows account name**
 - Incoming claim type: **Windows account name**
 - **Pass through all claim values**
3. Create three more rules to pass through the **E-Mail Address**, **UPN**, and **Name** claim types.

► **Task 6: Test access to the claims-aware application**

1. On LON-CL1, use Internet Explorer to access **https://lon-svr1.adatum.com/AdatumTestApp/**.

 **Note:** It is critical to use the trailing slash in the URL for step 1.

2. Sign in as **Adatum\Brad** with the password **Pa\$\$w0rd**.
3. Review the claim information that the application displays.
4. Close Internet Explorer.

► **Task 7: Configure Internet Explorer to pass local credentials to the application automatically**

1. On LON-CL1, from the Start screen, open Internet Options.
2. On the **Security** tab, add the following sites to the **Local intranet** zone:
 - **https://adfs.adatum.com**
 - **https://lon-svr1.adatum.com**
3. Use Internet Explorer to access **https://lon-svr1.adatum.com/AdatumTestApp/**.

 **Note:** It is critical to use the trailing slash in the URL for step 3.

4. Notice that you were not prompted for credentials.
5. Review the claim information that the application displays.
6. Close Internet Explorer.

Results: After completing this exercise, you will have configured AD FS to support authentication for an application.

Question: Why was it important to configure adfs.adatum.com to use as a host name for the AD FS service?

Question: How can you test whether AD FS is functioning properly?

Lab B: Implementing AD FS for External Partners and Users

Scenario

A. Datum Corporation has set up a variety of business relationships with other companies and customers. Some of these partner companies and customers must access business applications that are running on the A. Datum network. The business groups at A. Datum want to provide a maximum level of functionality and access to these companies. The Security and Operations departments want to ensure that the partners and customers can access only the resources to which they require access, and that implementing the solution does not increase the workload for the Operations team significantly. A. Datum also plans to migrate some parts of its network infrastructure to Microsoft Online Services, including Windows Azure and Office 365.

Now that you have deployed AD FS for internal users, the next step is to enable access to the same application for external partner organizations and for external users. A. Datum Corporation has entered into a partnership with Trey Research. You need to ensure that Trey Research users can access the internal application. You also need to ensure that A. Datum Corporation users working outside the office can access the application.

As one of the senior network administrators at A. Datum, it is your responsibility to implement the AD FS solution. As a proof-of-concept, you are deploying a sample claims-aware application, and configuring AD FS to enable both Trey Research users and external A. Datum Corporation users to access the same application.

Objectives

After completing this lab, you will be able to:

- Configure AD FS for a federated partner.
- Configure Web Application Proxy for external users.

Lab Setup

Estimated Time: 45 minutes

20412D-LON-DC1

20412D-LON-SVR1

20412D-LON-SVR2

20412D-TREY-DC1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

- On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
- In Hyper-V Manager, click **20412D-LON-DC1**, and then in the Actions pane, click **Start**.
- In the Actions pane, click **Connect**. Wait until the virtual machine starts.
- Sign in by using the following credentials:
 - User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
- Repeat steps 2 through 4 for 20412D-LON-SVR1, 20412D-LON-SVR2, and 20412D-TREY-DC1.
 - For TREY-DC1, sign in as **TREYRESEARCH\Administrator** with the password **Pa\$\$w0rd**.

Exercise 1: Configuring AD FS for a Federated Business Partner

Scenario

The second deployment scenario is to enable Trey Research users to access the web application. You plan to configure the integration of AD FS at Trey Research with AD FS at A. Datum, and then verify that Trey Research users can access the application. You also want to confirm that you can configure access that is based on user groups. You must ensure that all users at A. Datum, and only users who are in the Production group at Trey Research, can access the application.

The main tasks for this exercise are as follows:

1. Configure DNS forwarding between TreyResearch.net and Adatum.com.
2. Configure certificate trusts between TreyResearch.net and Adatum.com.
3. Create a DNS record for AD FS in TreyResearch.net.
4. Create a certificate for AD FS.
5. Create a service account.
6. Install AD FS for TreyResearch.net.
7. Configure AD FS for TreyResearch.net.
8. Add a claims-provider trust for the TreyResearch.net AD FS server.
9. Configure a relying party trust in TreyResearch.net for the Adatum.com application.
10. Test access to the application.
11. Configure issuance authorization rules.
12. Test the application of issuance authorization rules.

► Task 1: Configure DNS forwarding between TreyResearch.net and Adatum.com

1. On LON-DC1, use the DNS Manager to create a new conditional forwarder with the following settings:
 - DNS Domain: **TreyResearch.net**
 - IP address of the master server: **172.16.10.10**
 - **Store this conditional forwarder in Active Directory and replicate it as follows: All DNS servers in this forest**
2. On TREY-DC1, use the DNS Manager to create a new conditional forwarder with the following settings:
 - DNS Domain: **Adatum.com**
 - IP address of the master server: **172.16.0.10**
 - **Store this conditional forwarder in Active Directory and replicate it as follows: All DNS servers in this forest**



Note: In a production environment, it is likely that you would use Internet DNS instead of conditional forwarders.

► **Task 2: Configure certificate trusts between TreyResearch.net and Adatum.com**

1. On LON-DC1, use File Explorer to copy **TREY-DC1.TreyResearch.net_TreyResearchCA.crt** from **\TREY-DC1\CertEnroll** to **C:**.
2. Open Group Policy Management, and then edit the **Default Domain Policy**.
3. In the Default Domain Policy, browse to **Computer Configuration\Policies\Windows Settings\Security Settings\Public Key Policies\Trusted Root Certification Authorities**.
4. Import **C:TREY-DC1.TreyResearch.net_TreyResearchCA.crt** as a trusted root CA.
5. On TREY-DC1, use File Explorer to browse to **\LON-DC1\CertEnroll**.
6. Right-click **LON-DC1.Adatum.com_AdatumCA.crt**, and then install the certificate into the **Trusted Root Certification Authority** store.
7. On LON-SVR1, run **Gpupdate**.
8. On LON-SVR2, run **Gpupdate**.



Note: If you obtain certificates from a trusted certification authority, you do not need to configure a certificate trust between the organizations.

► **Task 3: Create a DNS record for AD FS in TreyResearch.net**

- On TREY-DC1, use the DNS Manager to add a new host record for AD FS:
 - Forward lookup zone: **TreyResearch.net**
 - Name: **adfs**
 - IP address: **172.16.10.10**

► **Task 4: Create a certificate for AD FS**

1. On TREY-DC1, open Internet Information Services (IIS) Manager, and then view the server certificates.
2. Create a new domain certificate with the following settings:
 - Common name: **adfs.TreyResearch.net**
 - Organization: **Trey Research**
 - Organizational unit: **IT**
 - City/locality: **London**
 - State/Province: **England**
 - Country/region: **GB**
 - Certification Authority: **TreyResearchCA**
 - Friendly name: **adfs.TreyResearch.net**

► **Task 5: Create a service account**

1. On TREY-DC1, open a Windows PowerShell prompt.
2. Create a new user account:
 - **New-ADUser –Name adfsService**
3. Set a password for adfsService:
 - **Set-ADAccountPassword adfsService**
 - Current password: none (press Enter)
 - Desired password: **Pa\$\$w0rd**
4. Enable the adfsService account:
 - **Enable-ADAccount adfsService**

► **Task 6: Install AD FS for TreyResearch.net**

- On TREY-DC1, in the Server Manager, add the Active Directory Federation Services role.

► **Task 7: Configure AD FS for TreyResearch.net**

1. In the Server Manager notifications, click **Configure the federation services on this server**.
2. Use the following options to configure the AD FS server:
 - **Create the first federation server in a federation server farm**
 - Account for configuration: **TREYRESEARCH\Administrator**
 - SSL Certificate: **adfs.TreyResearch.net**
 - Federation Service Display Name: **Trey Research**
 - Use an existing domain user account or group Managed Service Account:
 - **TREYRESEARCH\adfsService**
 - Password: **Pa\$\$w0rd**
 - **Create a database on this server using Windows Internal Database**

► **Task 8: Add a claims-provider trust for the TreyResearch.net AD FS server**

1. On LON-DC1, use the AD FS management console to add a new claims provider trust with the following settings:
 - **Import data about the claims provider published online or on a local network**
 - Federation metadata address: **https://adfs.treyresearch.net**
 - Display name: **Trey Research**
 - **Open the Edit Claim Rules dialog for this claims provider trust when the wizard closes**
2. Create a claim rule for Trey Research by using the following settings:
 - Claim rule template: **Pass Through or Filter an Incoming Claim**
 - Claim rule name: **Pass through Windows account name**
 - Incoming claim type: **Windows account name**
 - **Pass through all claim values**

► **Task 9: Configure a relying party trust in TreyResearch.net for the Adatum.com application**

1. On TREY-DC1, use the AD FS management console to create a new relying-party trust with the following settings:
 - Import data about the relying party published online or on a local network
 - Federation metadata address: **adfs.adatum.com**
 - Display name: **A. Datum Corporation**
 - I do not want to configure multi-factor authentication settings for this relying party trust at this time
 - Permit all users to access this relying party
 - Open the Edit Claim Rules dialog box for the relying party trust when the wizard closes
2. Create a new transform claim rule with the following settings:
 - Claim rule template: **Pass Through or Filter an Incoming Claim**
 - Claim rule name: **Pass through Windows account name**
 - Incoming claim type: **Windows account name**
 - **Pass through all claim values**

► **Task 10: Test access to the application**

1. On TREY-DC1, use Internet Explorer to access **https://lon-svr1.adatum.com/adatumtestapp/**
2. Select the Trey Research home realm, and then sign in as **TreyResearch\April** with the password **Pa\$\$w0rd**.
3. Verify that you can access the application.
4. Close Internet Explorer, and then connect to the same website. Verify that you are not prompted for a home realm this time.

 **Note:** You are not prompted for a home realm on the second access. Once users have selected a home realm and have been authenticated by a realm authority, they are issued a _LSRealm cookie by the relying party's federation server. The default lifetime for the cookie is 30 days. Therefore, to sign in multiple times, you should delete that cookie after each logon attempt to return to a clean state.

► **Task 11: Configure issuance authorization rules**

1. On TREY-DC1, in the AD FS management console, remove the issuance authorization rule from the A. Datum Corporation relying party trust that permits access for all users.
2. Add an issuance authorization rule to the A. Datum Corporation relying party trust that allows all users that are members of the Production group:
 - Claim rule template: **Permit or Deny Users Based on an Incoming Claim**
 - Claim rule name: **Allow Production Members**
 - Incoming claim type: **Group**
 - Incoming claim value: **TreyResearch-Production**
 - **Permit access to users with the incoming claim**

3. Add a transform claim rule to the Active Directory claims provider trust to send group membership as a claim:
 - Claim rule template: **Send Group Membership as a Claim**
 - Claim rule name: **Production Group Claim**
 - User's group: **Production**
 - Outgoing claim type: **Group**
 - Outgoing claim value: **TreyResearch-Production**

► **Task 12: Test the application of issuance authorization rules**

1. On TREY-DC1, use Internet Explorer to access <https://lon-svr1.adatum.com/adatumtestapp/>
2. Sign in as **TreyResearch\April** with the password **Pa\$\$w0rd**.
3. Verify that you cannot access the application because April is not a member of the production group.
4. Close Internet Explorer, and then connect to the same website.
5. Sign in as **TreyResearch\Ben** with the password **Pa\$\$w0rd**.
6. Verify that you can access the application because April is a member of the production group.

Results: After completing this exercise, you will have configured access for a claims-aware application in a partner organization.

Exercise 2: Configuring Web Application Proxy

Scenario

The third scenario for implementing the proof-of-concept AD FS application is to increase security for AD FS authentication by implementing an AD FS proxy for the AD FS and a reverse proxy for the application. You will implement Web Application Proxy to fulfill both of these roles.

The main tasks for this exercise are as follows:

1. Install Web Application Proxy.
2. Add the adfs.adatum.com certificate to LON-SVR2.
3. Add the LON-SVR1.adatum.com certificate to LON-SVR2.
4. Configure Web Application Proxy.
5. Configure the test application in Web Application Proxy.
6. Test Web Application Proxy.
7. To prepare for the next module.

► Task 1: Install Web Application Proxy

- On LON-SVR2, in the Server Manager, add the **Remote Access** server role and the **Web Application Proxy** role service.

► Task 2: Add the adfs.adatum.com certificate to LON-SVR2

1. On LON-DC1, open the Microsoft Management Console, and then add the **Certificates** snap-in for the **Local Computer**.
2. From the **Personal** folder, export the **adfs.adatum.com** certificate:
 - **Yes**, export the private key
 - File format: Personal Information Exchange – PKCS #12 (.PFX)
 - Password: Pa\$\$w0rd
 - File name: **C:\adfs.pfx**
3. On LON-SVR2, open a Microsoft Management Console, and then add the **Certificates** snap-in for the **Local Computer**.
4. From the **Personal** folder, import the **adfs.adatum.com** certificate:
 - **File name:** \\LON-SVR2\c\$\adfs.pfx
 - Password: Pa\$\$w0rd
 - Mark this key as exportable
 - Certificate store: Personal

► **Task 3: Add the LON-SVR1.adatum.com certificate to LON-SVR2**

1. On LON-SVR1, open the Microsoft Management Console, and then add the **Certificates** snap-in for the **Local Computer**.
2. From the **Personal** folder, export the **adfs.adatum.com** certificate:
 - Yes, export the private key
 - File format: Personal Information Exchange – PKCS #12 (.PFX)
 - Password: Pa\$\$w0rd
 - File name: C:\lon-svr1.pfx
3. On LON-SVR2, open the Microsoft Management Console, and then add the **Certificates** snap-in for the **Local Computer**.
4. From the **Personal** folder, import the **adfs.adatum.com** certificate:
 - File name: \\LON-SVR1\c\$\lon-svr1.pfx
 - Password: Pa\$\$w0rd
 - **Mark this key as exportable**
 - Certificate store: **Personal**

► **Task 4: Configure Web Application Proxy**

1. In the Server Manager, click the **Notifications** icon, and then click **Open the Web Application Proxy Wizard**.
2. In the Web Application Proxy Wizard, provide the following configuration settings:
 - Federation service name: adfs.adatum.com
 - User name: Adatum\Administrator
 - Password: Pa\$\$w0rd
 - Certificate to be used by the AD FS proxy: **adfs.adatum.com**
3. Leave the Remote Access Management Console open for the next task.

► **Task 5: Configure the test application in Web Application Proxy**

- On LON-SVR2, in the Remote Access Management Console, publish a new application with the following settings:
 - Preauthentication: Active Directory Federation Services (AD FS)
 - Relying Party: A. Datum Test App
 - Name: A. Datum Test App
 - External URL: <http://lon-svr1.adatum.com/adatumtestapp/>
 - External certificate: lon-svr1.adatum.com
 - Back-end server URL: <https://lon-svr1.adatum.com/adatumtestapp/>

► Task 6: Test Web Application Proxy

1. On TREY-DC1, open Notepad as Administrator to add the following lines to **C:\Windows\System32\Drivers\etc\hosts**:
 - **172.16.0.22 adfs.adatum.com**
 - **172.16.0.22 lon-svr1.adatum.com**
2. Use Internet Explorer to access <https://lon-svr1.adatum.com/adatumtestapp/>.
3. Sign in as **TreyResearch\Ben** with the password **Pa\$\$w0rd**.



Note: You edit the hosts to force TREY-DC1 to access the application through Web Application Proxy. In a production environment, you would do this by using split DNS.

► Task 7: To prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start the Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 to revert **20412D-LON-SVR1**, **20412D-LON-SVR2**, **20412D-LON-CL1**, and **20412D-TREY-DC1**.

Results: After completing this exercise, you will have configured Web Application Proxy to secure access to AdatumTestApp from the Internet.

Question: Why does using certificate from a trusted provider on the Internet negate the need to configure certificate trusts between organizations?

Question: Could you have created authorization rules in Adatum.com and achieved the same result if you had instead created authorization rules in TreyResearch.net?

Lab: Implementing NLB

Scenario

A. Datum Corporation is an engineering and manufacturing company. The organization is based in London, England, and is quickly expanding into Australia. As the company expands, the need for scalable web applications has increased. To address this need, you will develop a pilot program to test the deployment of NLB on hosts running the Windows Server 2012 operating system.

Because you intend to automate the process of deploying Windows NLB clusters, you will use Windows PowerShell to perform many of the cluster setup and configuration tasks. You also will configure port rules and affinity, which will allow you to deploy multiple load balanced web applications on the same Windows NLB clusters.

Objectives

After completing this lab, the students will be able to:

- Implement an NLB cluster.
- Configure and manage an NLB cluster.
- Validate high availability for the NLB cluster.

Lab Setup

Estimated Time: 45 minutes

Virtual machines	20412D-LON-DC1 20412D-LON-SVR1 20412D-LON-SVR2
User name	Adatum\Administrator
Password	Pa\$\$w0rd

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
 - User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
5. Repeat steps two through four for 20412D-LON-SVR1 and 20412D-LON-SVR2.

Exercise 1: Implementing an NLB Cluster

Scenario

You eventually want to automate the process of deploying Windows Server 2012 NLB clusters. To accomplish this, you will use Windows PowerShell to perform the majority of the NLB cluster deployment tasks.

The main tasks for this exercise are as follows:

1. Verify website functionality for stand-alone servers
2. Install NLB
3. Create a new Windows Server 2012 NLB cluster
4. Add a second host to the cluster
5. Validate the NLB cluster

► Task 1: Verify website functionality for stand-alone servers

1. On LON-SVR1, navigate to the **c:\inetpub\wwwroot** folder.
2. Open **iis-85.png** in Microsoft Paint, and use the Paintbrush tool and the color red to mark the IIS logo in a distinctive manner.
3. Close File Explorer.
4. Switch to LON-DC1, and then open Windows Internet Explorer.
5. Navigate to **http://LON-SVR1**, and verify that the web page is marked in a distinctive manner with the color red.
6. Navigate to **http://LON-SVR2**, and verify that the website is not marked in a distinctive manner.
7. Close Internet Explorer.

► Task 2: Install NLB

1. On LON-SVR1, open Windows PowerShell ISE.
2. Type the following command, and then press Enter:

```
Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-WindowsFeature NLB,RSAT-NLB}
```

► Task 3: Create a new Windows Server 2012 NLB cluster

1. On LON-SVR1, in Windows PowerShell ISE, type the following command, and then press Enter:

```
New-NlbCluster -InterfaceName "Ethernet" -OperationMode Multicast -ClusterPrimaryIP 172.16.0.42 -ClusterName LON-NLB
```

2. In Windows PowerShell ISE, type the following command, and then press Enter:

```
Invoke-Command -Computername LON-DC1 -command {Add-DNSServerResourceRecordA -zonename adatum.com -name LON-NLB -IPv4Address 172.16.0.42}
```

► Task 4: Add a second host to the cluster

1. On LON-SVR1, in Windows PowerShell ISE, type the following command, and then press Enter:

```
Add-NlbClusterNode -InterfaceName "Ethernet" -NewNodeName "LON-SVR2" -NewNodeInterface "Ethernet"
```

► **Task 5: Validate the NLB cluster**

1. On LON-SVR1, open the Network Load Balancing Manager console, and verify that nodes LON-SVR1 and LON-SVR2 display with the status of **Converged**.
2. View the properties of the LON-NLB cluster, and verify the following:
 - The cluster is set to use the **Multicast** operations mode.
 - There is a single port rule named **All** that starts at port **0** and ends at port **65535** for both **TCP** and **UDP** protocols, and that it uses **Single** affinity.

Results: After completing this exercise, you will have successfully implemented an NLB cluster.

Exercise 2: Configuring and Managing the NLB Cluster

Scenario

You want to deploy multiple separate websites to the NLB cluster, and then differentiate these websites based on port address. To do this, you want to ensure that you are able to configure and validate port rules. You also want to experiment with affinity settings to ensure that requests are distributed evenly across hosts.

The main tasks for this exercise are as follows:

1. Configure port rules and affinity
2. Validate port rules
3. Manage host availability in the NLB cluster

► Task 1: Configure port rules and affinity

1. On LON-SVR2, open Windows PowerShell.
2. In Windows PowerShell, enter the following commands, and then press Enter after each command:

```
Cmd.exe  
  
Mkdir c:\porttest  
  
Xcopy /s c:\inetpub\wwwroot c:\porttest  
  
Exit  
  
New-Website -Name PortTest -PhysicalPath "C:\porttest" -Port 5678  
  
New-NetFirewallRule -DisplayName PortTest -Protocol TCP -LocalPort 5678
```

3. Open File Explorer, and then browse to and open **c:\porttest\iis-85.png** in Microsoft Paint.
4. Use the **Blue** paintbrush to mark the IIS logo in a distinctive manner.
5. Switch to LON-DC1.
6. Open Internet Explorer, and navigate to **http://LON-SVR2:5678**.
7. Verify that the IIS Start page with the image marked with blue displays.
8. Switch to LON-SVR1.
9. On LON-SVR1, open Network Load Balancing Manager, and view the cluster properties of LON-NLB.
10. Remove the **All port** rule.
11. Add a port rule with the following properties:
 - Port range: **80 to 80**
 - Protocols: **Both**
 - Filtering mode: **Multiple Host**
 - Affinity: **None**
12. Create a new port rule with the following properties:
 - Port range: **5678 to 5678**
 - Protocols: **Both**
 - Filtering mode: **Single Host**

13. Close the **LON-NLB(172.16.0.42)**.
14. Edit the host properties of LON-SVR1.
15. Configure the **Handling Priority** value of the port rule for port **5678** as **10**.

► **Task 2: Validate port rules**

1. Switch to LON-DC1.
2. Using Internet Explorer, navigate to **http://lon-nlb**, refresh the web page 20 times, and verify that web pages with and without the distinctive red marking display.
3. On LON-DC1, navigate to address **http://LON-NLB:5678**, refresh the web page 20 times, and verify that only the web page with the distinctive blue marking displays.

► **Task 3: Manage host availability in the NLB cluster**

1. Switch to LON-SVR1.
2. On LON-SVR1, use the Network Load Balancing Manager console to suspend LON-SVR1.
3. Verify that node LON-SVR1 displays as **Suspended**, and that node LON-SVR2 displays as **Converged**.
4. Resume and then start LON-SVR1.
5. Verify that both node LON-SVR1 and LON-SVR2 now display as **Converged**.

Results: After completing this exercise, you will have successfully configured and managed an NLB cluster.

Exercise 3: Validating High Availability for the NLB Cluster

Scenario

As part of preparing to deploy NLB in your organization's environment, you want to ensure that it is possible to perform maintenance tasks (such as reboot operations), without affecting the availability of the websites that are hosted on the cluster. To accomplish this, you will verify availability by rebooting one host while you attempt to access the clustered website. You will also explore the Drainstop functionality.

The main tasks for this exercise are as follows:

1. Validate website availability when the host is unavailable
2. Configure and validate Drainstop
3. Prepare for the next module

► Task 1: Validate website availability when the host is unavailable

1. Restart LON-SVR1.
2. Switch to LON-DC1.
3. On LON-DC1, open Internet Explorer, and navigate to **http://LON-NLB**.
4. Refresh the website 20 times. Verify that the website is available, but that it does not display the distinctive red mark on the IIS logo until LON-SVR1 has restarted.

► Task 2: Configure and validate Drainstop

1. On LON-SVR1, open the Network Load Balancing Manager console, and initiate a Drainstop on LON-SVR2.
2. On LON-DC1, navigate to **http://lon-nlb**, and verify that only the welcome page with the red IIS logo displays.

► Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state.

1. On the host computer, start the Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for 20412D-LON-SVR1 and 20412D-LON-SVR2.

Results: After completing this exercise, you will have successfully validated high availability for the NLB cluster.

Question: How many additional nodes can you add to the LON-NLB cluster?

Question: What steps would you take to ensure that LON-SVR1 always manages requests for web traffic on port 5678, given the port rules established by the end of this exercise?

Question: What is the difference between a Stop and a Drainstop command?

Lab: Implementing Failover Clustering

Scenario

As A. Datum's business grows, it is becoming increasingly important that many of the applications and services on the network are available at all times. A. Datum has many services and applications that must be available to internal and external users who work in different time zones around the world. Many of these applications cannot be made redundant by using Network Load Balancing (NLB). Therefore, you have to use a different technology to make these applications highly available.

As one of the senior network administrators at A. Datum, you are responsible for implementing failover clustering on the Windows Server 2012 R2 servers to provide high availability for network services and applications. You are also responsible for planning the failover cluster configuration, and for deploying applications and services on the failover cluster.

Objectives

After completing this lab, you will be able to:

- Configure a failover cluster.
- Deploy and configure a highly available file server.
- Validate the deployment of the highly available file server.
- Configure cluster-aware updating on the failover cluster.

Lab Setup

Estimated Time: 60 minutes

Virtual machines	20412D-LON-DC1 20412D-LON-SVR1 20412D-LON-SVR3 20412D-LON-SVR4
User name	Adatum\Administrator
Password	Pa\$\$w0rd

Lab Setup

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Microsoft Hyper-V® Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
 - User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
5. Repeat steps two through four for 20412D-LON-SVR1, 20412D-LON-SVR3, and 20412D-LON-SVR4.

Exercise 1: Configuring a Failover Cluster

Scenario

A. Datum has important applications and services that the company wants to make highly available. Some of these services cannot be made redundant by using NLB. Therefore, you decide to implement failover clustering. Because iSCSI storage is set up, you decide to use the iSCSI storage for failover clustering. First, you will implement the core components for failover clustering and validate the cluster, and then you will create the failover cluster.

The main tasks for this exercise are as follows:

1. Connect cluster nodes to the iSCSI targets
2. Install the failover clustering feature
3. Validate the servers for failover clustering
4. Create the failover cluster
5. Configuring CSV

► Task 1: Connect cluster nodes to the iSCSI targets

1. On LON-SVR3, start the **iSCSI Initiator**, and configure **Discover Portal** with the IP address **172.16.0.21**.
2. Connect to the discovered target in the **Targets** list.
3. Repeat steps one and two on LON-SVR4.
4. Open **Disk Management** on LON-SVR3.
5. Bring online and initialize the three new disks.
6. Make a simple volume on each disk, and format it with NTFS.
7. On LON-SVR4, open **Disk Management**, and bring online and initialize the three new disks.

► Task 2: Install the failover clustering feature

1. On LON-SVR3, install the Failover Clustering feature by using the Server Manager.
2. On LON-SVR4, install the Failover Clustering feature by using the Server Manager.

► Task 3: Validate the servers for failover clustering

1. On LON-SVR3, open the Failover Cluster Manager console.
2. Start the **Validate a Configuration Wizard**.
3. Use LON-SVR3 and LON-SVR4 as nodes for test.
4. Run all tests.
5. Review the report.

► Task 4: Create the failover cluster

1. On LON-SVR3, in the Failover Cluster Manager, start the **Create Cluster Wizard**.
2. Use LON-SVR3 and LON-SVR4 as cluster nodes.
3. Specify **Cluster1** as the **Cluster name**.
4. Specify the **IP address** as **172.16.0.125**.

► **Task 5: Configuring CSV**

1. On LON-SVR3, in the Failover Cluster Manager console, navigate to **Storage->Disks**.
2. Locate the disk that is assigned to **Available Storage**. If possible, use Cluster Disk 2.
3. Add this to **Cluster Shared Volumes**.

Results: After this exercise, you will have installed and configured the failover clustering feature.

Exercise 2: Deploying and Configuring a Highly Available File Server

Scenario

In A. Datum, File Services is one of the important services that must be highly available. After you have created a cluster infrastructure, you decide to configure a highly available file server and implement settings for failover and failback.

The main tasks for this exercise are as follows:

1. Add the File Server application to the failover cluster
2. Add a shared folder to a highly available file server
3. Configure failover and failback settings

► **Task 1: Add the File Server application to the failover cluster**

1. Add the File Server role service to LON-SVR4 by using the Server Manager console. LON-SVR3 already has File Server Role service installed.
2. On LON-SVR3, open the Failover Cluster Manager console.
3. In the **Storage** node, click **Disks**, and verify that three cluster disks are online.
4. Add **File Server** as a cluster role. Select the **File Server for general use** option.
5. Specify **AdatumFS** as **Client Access Name**.
6. Specify **172.16.0.130** as the **IP address** for the cluster role.
7. Select **Cluster Disk 3** as the storage disk for the AdatumFS role.
8. Complete the wizard.

► **Task 2: Add a shared folder to a highly available file server**

1. On LON-SVR4, open the Failover Cluster Manager.
2. Start the New Share Wizard, and add a new shared folder to the AdatumFS cluster role.
3. Specify the File share profile as **SMB Share – Quick**.
4. Accept the default values on the **Select the server and the path for this share** page.
5. Name the shared folder **Docs**.
6. Accept the default values on the **Configure share settings** and **Specify permissions to control access** pages.
7. Create the share at the end of wizard.

► **Task 3: Configure failover and failback settings**

1. On LON-SVR4, in the Failover Cluster Manager, open the **Properties** for the **AdatumFS** cluster role.
2. Enable failback between 4 and 5 hours.
3. Select both **LON-SVR3** and **LON-SVR4** as the preferred owners.
4. Move **LON-SVR4** to be first in the Preferred Owners list.

Results: After this exercise, you will have configured a highly available file server.

Exercise 3: Validate the Deployment of the Highly Available File Server

Scenario

In the process of implementing failover cluster, you want to perform failover and failback tests. Also, you want to change the disk witness in the quorum.

The main tasks for this exercise are as follows:

1. Validate the highly available file server deployment
2. Validate the failover and quorum configuration for the file server role

► **Task 1: Validate the highly available file server deployment**

1. On LON-DC1, open File Explorer, and attempt to access the **\AdatumFS** location. Make sure that you can access the **Docs** folder.
2. Create a test text document inside this folder.
3. On LON-SVR3, in the Failover Cluster Manager, move **AdatumFS** to the second node.
4. On LON-DC1, in File Explorer, verify that you can still access the **\AdatumFS** location.

► **Task 2: Validate the failover and quorum configuration for the file server role**

1. On LON-SVR3, determine the current owner of the **AdatumFS** role.
2. Stop the Cluster service on the node that is the current owner of the **AdatumFS** role.
3. Verify that **AdatumFS** has moved to another node, and that the **\AdatumFS** location is still available, by trying to access it from LON-DC1.
4. Start the Cluster service on the node in which you stopped it in step two.
5. Browse to the Disks node, and take the disk marked as **Disk Witness in Quorum** offline.
6. Verify that **AdatumFS** is still available, by trying to access it from LON-DC1.
7. Bring the disk witness online.
8. Open Cluster Quorum Settings.
9. Choose to perform advanced configuration.
10. Change the witness disk to Cluster Disk 3. Do not make any other changes.

Results: After this exercise, you will have tested the failover scenarios.

Exercise 4: Configuring CAU on the Failover Cluster

Scenario

In previous Windows Server versions, implementing updates to servers with critical service resulted in unwanted downtime. To enable seamless and zero-downtime cluster updating, you want to implement the CAU feature and test updates for cluster nodes.

The main tasks for this exercise are as follows:

1. Configure CAU
2. Update the failover cluster and configure self-updating
3. Prepare for the next module

► Task 1: Configure CAU

1. On LON-DC1, install the failover clustering feature by using the Server Manager console.
2. On LON-SVR3, open the Windows Firewall with Advanced Security window, and verify that the following two inbound rules are enabled:
 - **Inbound Rule for Remote Shutdown (RPC-EP-In)**
 - **Inbound Rule for Remote Shutdown (TCP-In)**
3. Repeat step two on LON-SVR4.
4. On LON-DC1, from Server Manager, open Cluster-Aware Updating.
5. Connect to **Cluster1**.
6. Preview the updates available for nodes in **Cluster1**. (Note: An Internet connection is required for this step.)

► Task 2: Update the failover cluster and configure self-updating

1. On LON-DC1, start the update process for **Cluster1**, by selecting **Apply updates to this cluster**.
2. Accept the default values in the update wizard.
3. Wait until the update process is completed. The process is finished when both nodes have a **Succeeded** value in the **Last Run status** column.
4. On LON-SVR3, open **Cluster- Aware Updating**, and then connect to **Cluster1**.
5. Select the **Configure cluster self-updating options** option.
6. Choose to add the CAU clustered role with the self-updating mode enabled in this cluster.
7. Configure self-updating to be performed **weekly**, on **Sundays at 4:00 AM**.
8. Close the wizard.

► Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state. To do this, perform the following steps:

1. On the host computer, start Hyper-V Manager.
2. On the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps two and three for 20412D-LON-SVR1, 20412D-LON-SVR3, and 20412D-LON-SVR4.

Results: After this exercise, you will have configured CAU.

Question: What information do you have to collect as you plan a failover cluster implementation and choose the quorum mode?

Question: After running the Validate a Configuration Wizard, how can you resolve the network communication single point of failure?

Question: In what situations might it be important to enable failback of a clustered application only during a specific time?

Lab: Implementing Failover Clustering with Hyper-V

Scenario

The initial deployment of virtual machines on Hyper-V has been successful for A. Datum. As a next step in the deployment, A. Datum is considering ways to ensure that the services and applications deployed on the virtual machines are highly available. As part of the implementation of high availability for most network services and applications, A. Datum also is considering options for making the virtual machines that run on Hyper-V highly available.

As one of the senior network administrators at A. Datum, you are responsible for integrating Hyper-V with failover clustering to ensure that the virtual machines deployed on Hyper-V are highly available. You are responsible for planning the virtual machine and storage configuration, and for implementing the virtual machines as highly available services on the failover cluster. You also are considering other techniques, such as Hyper-V Replica, for ensuring high availability for virtual machines.

Objectives

After completing this lab, you will be able to:

- Configure a Hyper-V Replica.
- Configure a failover cluster for Hyper-V.
- Configure a highly available virtual machine.

Lab Setup

Estimated Time: 75 minutes

Virtual machines	20412D-LON-DC1-B 20412D-LON-SVR1-B
Host machines	20412D-LON-HOST1 20412D-LON-HOST2
User name	Adatum\Administrator
Password	Pa\$\$w0rd

You should perform this lab with a partner. To perform this lab, you must start the host computers to Windows Server 2012 R2. Ensure that you and your partner have started different hosts—one should start the LON-HOST1, and the other should start the LON-HOST2. In addition, ensure that LON-DC1-B is imported on LON-HOST1, and LON-SVR1-B is imported on LON-HOST2, and that these virtual machines are started.

Exercise 1: Configuring Hyper-V Replicas

Scenario

Before you start with a cluster deployment, you have decided to evaluate the new technology in Hyper-V for replicating virtual machines between hosts. You want to be able to mount a copy of a virtual machine on to another host manually if the active copy or host fails.

The main tasks for this exercise are as follows:

1. Import LON-CORE virtual machine on LON-HOST1
2. Configure a replica on both host machines
3. Configure replication for LON-CORE virtual machine
4. Validate a planned failover to the replica site

► **Task 1: Import LON-CORE virtual machine on LON-HOST1**

1. On LON-HOST1, open the Hyper-V Manager, and import the 20412D-LON-CORE virtual machine.
2. Use path **E:\Program Files\Microsoft Learning\20412\Drives\20412D-LON-CORE**
3. Accept default values.

 **Note:** The drive letter might be different based upon the number of drives on the physical host machine.

► **Task 2: Configure a replica on both host machines**

1. On LON-HOST1 and LON-HOST2, configure each server to be a Hyper-V Replica server.
 - Use Kerberos (HTTP) for authentication.
 - Enable replication from any authenticated server.
 - Create and use the folder **E:\VMReplica** as a default location to store replica files.
2. Enable the firewall rule named **Hyper-V Replica HTTP Listener (TCP-In)** on both hosts.

► **Task 3: Configure replication for LON-CORE virtual machine**

1. On LON-HOST1, enable replication for the 20412D-LON-CORE virtual machine:
 - Use Kerberos (HTTP).
 - Set the replication frequency to 30 seconds.
 - Select to have only latest recovery point available.
 - Start replication immediately.
2. Wait for initial replication to finish, and ensure that the 20412D-LON-CORE virtual machine has appeared in Hyper-V Manager console on LON-HOST2.

► **Task 4: Validate a planned failover to the replica site**

1. On LON-HOST2, view replication health for 20412D-LON-CORE.
2. On LON-HOST1, perform the planned failover to LON-HOST2. Verify that 20412D-LON-CORE is running on LON-HOST2.
3. On LON-HOST1, remove replication for 20412D-LON-CORE.
4. On LON-HOST2, shut down 20412D-LON-CORE.

Results: After completing this exercise, you will have configured Hyper-V Replica.

Exercise 2: Configuring a Failover Cluster for Hyper-V

Scenario

A. Datum has several virtual machines that are hosting important services that must be highly available. Because these services are not cluster-aware, A. Datum has decided to implement a failover cluster on the Hyper-V host level. You plan to use iSCSI drives as storage for these virtual machines.

The main tasks for this exercise are as follows:

1. Connect to iSCSI target from both host machines
2. Configure failover clustering on both host machines
3. Configure disks for failover cluster

► Task 1: Connect to iSCSI target from both host machines

1. On LON-HOST1, start the **iSCSI initiator**.
2. Use the 172.16.0.21 address to discover and connect to the iSCSI target.
3. On LON-HOST2, start the **iSCSI initiator**.
4. Use the 172.16.0.21 address to discover and connect to the iSCSI target.
5. On LON-HOST2, open Disk Management, and initialize and bring online all iSCSI drives:
 - Format the first drive, and name it **ClusterDisk**.
 - Format the second drive, and name it **ClusterVMs**.
 - Format the third drive, and name it **Quorum**.
6. On LON-HOST1, open Disk Management, and bring all three iSCSI drives online.

► Task 2: Configure failover clustering on both host machines

1. On LON-HOST1 and LON-HOST2, install the Failover Clustering feature.
2. On LON-HOST1, create a failover cluster:
 - Add LON-HOST1 and LON-HOST2.
 - Name it **VMCluster**.
 - Assign the address **172.16.0.126**.
 - Clear the option to **Add all eligible storage to the cluster**.

► Task 3: Configure disks for failover cluster

1. In Failover Cluster Manager on LON-HOST1, add all three iSCSI disks to the cluster.
2. Verify that all three iSCSI disks appear available for cluster storage.
3. Add the disk with the volume name **ClusterVMs** to **Cluster Shared Volumes**.
4. From the **VMCluster.adatum.com** node, select **More Actions**, and then configure the Cluster Quorum Settings to use default configuration.

Results: After completing this exercise, the students will have the failover clustering infrastructure configured for Hyper-V.

Exercise 3: Configuring a Highly Available Virtual Machine

Scenario

After you have configured the Hyper-V failover cluster, you want to add virtual machines as highly available resources. In addition, you want to evaluate Live Migration and test Storage Migration.

The main tasks for this exercise are as follows:

1. Copy virtual machine storage to iSCSI target
2. Configure the virtual machine as highly available
3. Perform a Live Migration for the virtual machine
4. Perform a Storage Migration for the virtual machine
5. Prepare for the next module

► Task 1: Copy virtual machine storage to iSCSI target

1. Ensure that LON-HOST1 is the owner of the ClusterVMs disk. If it is not, move the ClusterVMs disk to LON-HOST1.
2. On LON-HOST1, open File Explorer, browse to **E:\Program Files\Microsoft Learning\20412\Drives\20412D-LON-CORE\Virtual Hard Disks**, and then copy the **20412D-LON-CORE.vhd** virtual hard disk file to the **C:\ClusterStorage\Volume1** location.

► Task 2: Configure the virtual machine as highly available

1. In the Failover Cluster Manager, click the **Roles** node, and then start the New Virtual Machine Wizard.
 - Select LON-HOST1 as the cluster node.
 - Name the computer as **TestClusterVM**.
 - Store the file at **C:\ClusterStorage\Volume1**.
 - Assign 1536 MB of RAM to the TestClusterVM.
 - Connect the machine to the existing virtual hard disk drive **20412D-LON-CORE.vhd**, located at **C:\ClusterStorage\Volume1**.
2. Open settings for TestClusterVM.
3. Enable the option for migration to computers with a different processor version.
4. From the Roles node, start the virtual machine.

► Task 3: Perform a Live Migration for the virtual machine

1. On LON-HOST2, in the Failover Cluster Manager, start **Live Migration** failover of **TestClusterVM** from LON-HOST1 to LON-HOST2.
2. Connect to **TestClusterVM**, and ensure that you can operate it.

► Task 4: Perform a Storage Migration for the virtual machine

1. On LON-HOST1, browse to **E:\Program Files\Microsoft Learning\20412\Drives** and create new folder on this location. Name the folder **LON-GUEST1**.
2. Browse to **E:\Program Files\Microsoft Learning\20412\Drives\20412D-LON-CORE\Virtual Hard Disks**, and then copy the **20412D-LON-CORE.vhd** virtual hard disk file to the **E:\Program Files\Microsoft Learning\20412\Drives\LON-GUEST1** location.

3. Create new virtual machine on LON-HOST1, with following settings:
 - Name: LON-GUEST1
 - Location: E:\Program Files\Microsoft Learning\20412\Drives\LON-GUEST1
 - Memory: 1024 MB
 - Network: External Network
 - Hard disk: E:\Program Files\Microsoft Learning\20412\Drives\LON-GUEST1\20412D-LON-CORE.vhd
4. On LON-HOST1, open the Hyper-V Manager, and start LON-GUEST1.
5. Perform a Move operation on LON-GUEST1. Move the virtual machine from its current location to C:\GUEST1.
6. Check whether the machine is operational during the move process.
7. When complete, shut down all running virtual machines.

► **Task 5: Prepare for the next module**

1. Restart LON-HOST1.
2. When you are prompted with the boot menu, select **Windows Server 2012**, and then press Enter.
3. Sign in to the host machine as directed by your instructor.
4. Repeat steps one through three on LON-HOST2.

Results: After completing this exercise, the students will have configured the virtual machine as highly available.

Question: How can you extend Hyper-V Replica in Windows Server 2012 R2?

Question: What is the difference between Live Migration and Storage Migration?

Lab: Implementing Windows Server Backup and Restore

Scenario

Much of the data that is stored on the A. Datum Corporation's network is extremely valuable to the organization. Losing this data would be a significant loss to the organization. Additionally, many of the servers that are running on the network provide extremely valuable services for the organization, which means that losing these servers for a significant time would also result in losses to the organization. Because of the significance of the data and services, it is critical that they can be restored in the event of disaster.

A. Datum is considering backing up critical data to a cloud-based service. A. Datum also is considering this as an option for small branch offices that do not have a full datacenter infrastructure.

As one of the senior network administrators at A. Datum, you are responsible for planning and implementing a data-protection solution that will ensure that critical data and services can be recovered in the event of any type of failure. You need to implement a backup-and-restore process that can recover lost data and services.

Objectives

- Back up data on a Windows Server 2012 server.
- Restore files by using Windows Server Backup.

Lab Setup

Estimated Time: 45 minutes

Virtual machines: 20412D-LON-DC1,

20412D-LON-SVR1

User name: **Adatum\Administrator**

Password: **Pa\$\$w0rd**

For this lab, you will use the available virtual machine environment. Before you begin the lab, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20412D-LON-DC1**, and in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in using the following credentials:
 - User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
5. Repeat steps 2 through 4 for **20412D-LON-SVR1**.

Exercise 1: Backing Up Data on a Windows Server 2012 R2 Server

Scenario

The LON-SVR1 server contains financial data that must be backed up on a regular basis. This data is critical to the organization. You decided to use Windows Server Backup to back up critical data. You will install this feature and configure scheduled backups.

The main tasks for this exercise are as follows:

1. Install Windows Server Backup.
2. Configure a scheduled backup.
3. Complete an on-demand backup.

► Task 1: Install Windows Server Backup

1. Switch to LON-SVR1.
2. From the Server Manager, install the Windows Server Backup feature. Accept the default values on the Add Roles and Features Wizard.

► Task 2: Configure a scheduled backup

1. On LON-SVR1, start Windows Server Backup.
2. Configure the backup schedule with the following options:
 - Backup Configuration: **Full server (recommended)**
 - Backup Time: **Once a day, 1:00 AM**
 - Destination Type: **Back up to a shared network folder**
 - Remote Shared Folder: \\LON-DC1\Backup.
 - Register Backup Schedule: Username: **Administrator**
 - Password: **Pa\$\$w0rd**

 **Note:** In a production environment, you will not store backup to a domain controller. You do it here for lab purposes only.

► Task 3: Complete an on-demand backup

1. On LON-SVR1, start Windows Server Backup.
2. Run the Backup Once Wizard to back up the **C:\Financial Data** folder to the remote folder **\LON-DC1\Backup**.

Results: After you complete this exercise, you will have configured the Windows Server Backup feature, scheduled a backup task, and completed an on-demand backup.

Exercise 2: Restoring Files Using Windows Server Backup

Scenario

To ensure that the financial data can be restored, you must validate the procedure for restoring the data to an alternate location.

The main tasks for this exercise are as follows:

1. Delete a file from the server.
2. Restore a file from backup.
3. Prepare for the next module.

► Task 1: Delete a file from the server

- On LON-SVR1, open Windows Explorer, and then delete the **C:\Financial Data** folder.

► Task 2: Restore a file from backup

1. In the Windows Server Backup MMC, run the Recovery Wizard, and specify the following information:
 - Getting Started: **A backup stored on another location**
 - Specify Location type: **Remote Shared Folder**
 - Specify Remote Folder: **\LON-DC1\Backup**
 - Select Backup Date: **Default value, Today**
 - Select Recovery Type: **Default value, Files and Folders**
 - Select Items to Recover: **LON-SVR1\Local disk (C):\Financial Data**
 - Specify Recovery Options: **Another Location (C:)**
2. Open drive **C**, and ensure that the **Financial Data** folder is restored.

► Task 3: Prepare for the next module

When you finish the lab, revert the virtual machines to their initial state.

1. On the host computer, start the Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20412D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for 20412D-LON-SVR1.

Results: After completing this exercise, you will have tested and validated the procedure for restoring a file from backup.

Question: You are concerned about business-critical data that is located on your company's servers. You want to perform backups every day, but not during business hours. What should you do?

Question: Users report that they can no longer access data that is located on the server. You connect to the server, and you realize that the shared folder where users were accessing data is missing. What should you do?

1: Deploying and Managing Windows Server 2012

Demonstration: Using DISM to Add Windows Features

In this demonstration, you see how to use the DISM command-line utility to:

- View a list of all Windows features and their current state
- Gather information about the Windows Server Backup feature
- Enable the Windows Server Backup feature

Emphasize that the feature names are case-sensitive when you use the DISM utility.

Preparation Steps

1. For this demonstration, start the 20410D-LON-DC1 virtual machine.
2. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

View a list of all Windows features and their current state

1. In Server Manager click the **Tools** menu, and then click **Windows Server Backup**.
In the details pane, notice that Windows Server Backup is not installed on the computer.
2. Close the wbadmin-[Windows Server Backup(Local)] window.

Gather information about the Windows Server Backup feature

1. Right-click the **Windows PowerShell** icon on the taskbar, and then click **Run as Administrator**.
2. Type the following command, and then press Enter:

DISM /online /get-features

3. Type the following command, and then press Enter:

DISM /online /get-featureinfo /featurename:WindowsServerBackup

Enable the Windows Server Backup feature

1. Type the following command, and then press Enter:

DISM /online /enable-feature /featurename:WindowsServerBackup

Note: The feature name is case-sensitive.

2. In Server Manager, click the **Tools** menu, and then click **Windows Server Backup**.
In the details pane, notice that Windows Server Backup is now available.
3. Close all open windows.

1: Deploying and Managing Windows Server 2012

Demonstration: Using Server Manager

In this demonstration, you will see how to:

- Add a feature by using the Add Roles and Features Wizard
- View role-related events
- Run the Best Practice Analyzer for a role
- List the tools available from Server Manager
- Restart Windows Server 2012

When you work through this demonstration, explain the purpose of each feature. Point out the following:

- Although the visual style differs, many wizards have the same content.
- When adding roles with Windows Server 2012, point out that any other necessary components will be added automatically.
- When viewing DNS events, describe what would appear in these dialog boxes in the event that a DNS server was unhealthy.
- Best Practices Analyzer only shows results if it has been run previously.
- Explain how to pin particular consoles to the Start screen or to the taskbar.
- Discuss other methods for shutting down the Windows Server 2012 server.

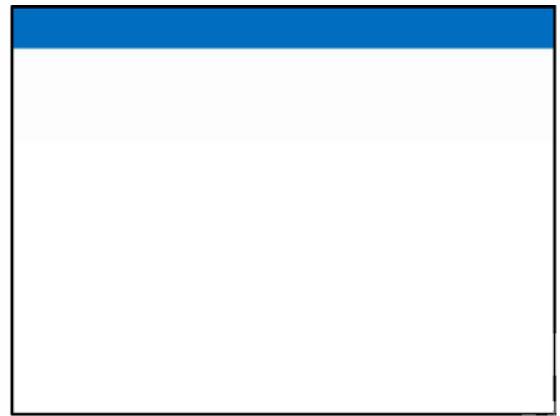
Preparation Steps

1. If necessary, start 20410D-LON-DC1.
2. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Add a feature by using the Add Roles and Features Wizard

1. In the Server Manager console, click **Manage**, and then click **Add Roles and Features**.
2. In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, select **Role-based or featured-based installation**, and then click **Next**.
4. On the Select destination server page, click **Select a server from the server pool**, verify that **LON-DC1.Adatum.com** is selected, and then click **Next**.
5. On the **Select server roles** page, select **Fax Server**.
6. In the **Add Roles and Features Wizard** dialog box that opens, click **Add Features**.
7. On the **Select server roles** page, click **Next**.
8. On the **Select features** page, select **BranchCache**, and then click **Next**.
9. On the **Fax Server** page, click **Next**.



10. On the **Print and Document Services** page, click **Next**.
11. On the **Select role services** page, click **Next**.
12. On the **Confirmation** page, select the **Restart the destination server automatically if required** check box, click **Yes**, and then click **Install**.
13. On the **Installation progress** page, click **Close**.
14. Click the flag icon next to **Server Manager Dashboard**, and review the messages.
You can close this console without terminating the task.

View role-related events

1. In the **Server Manager** console, click the **Dashboard** node.
2. In the Roles and Server Groups area, under **DNS**, click **Events**.
3. In the **DNS - Events Detail View** dialog box, change the time period to **12 hours** and the **Event Sources** to **All**, and then click **OK**.

Run the Best Practice Analyzer for a role

1. In the Roles and Server Groups area, under DNS, click **BPA results**.
2. In the **DNS - BPA Results Detail View** dialog box, click the **Severity Levels** drop-down menu, click **All**, and then click **OK**.

List the tools available in Server Manager

1. In the Server Manager console, click the **Tools** menu, and review the tools that are installed on **LON-DC1**.
2. Press the **Windows logo key** to open the Start menu.

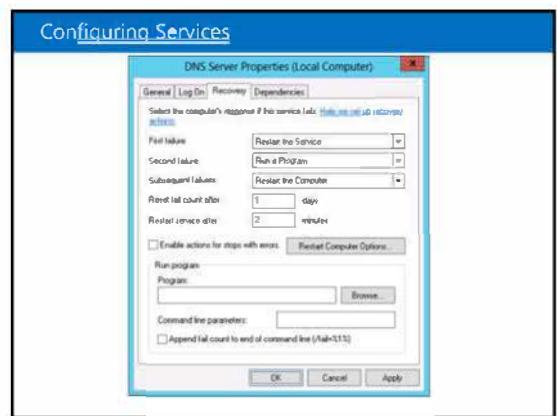
Sign out the currently signed-in user

1. In the Start screen, click **Administrator**, and then click **Sign Out**.
2. Sign back in to **LON-DC1** using the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.

Restart Windows Server 2012

1. On the taskbar, click the **Windows PowerShell** icon.
2. In the Windows PowerShell window, type the following command, and then press Enter:
Shutdown /r /t 5

1: Deploying and Managing Windows Server 2012



Discuss configuring service recovery, and why you should avoid having the service keep restarting.

Remind students to be careful with the option to restart the computer, because a service that keeps failing might trigger a cycle of restarting.

Discuss the benefits of managed service accounts over traditional service accounts. Ask students which method they currently use to manage service accounts.

The slide shows the properties of the DNS Server service, which is accessible from the Services console.

Question

What is the advantage of a managed service account compared to a traditional domain-based service account?

Answer

The advantage of a managed service account is that you do not have to manage passwords for it.

1: Deploying and Managing Windows Server 2012

Demonstration: Performing Remote Management

In this demonstration, you will see how to:

- Use Server Manager to manage a remote server
- Add the DNS Server role on a remote server
- Connect to and configure a remote server by using RDP

Point out how to search for an app from the Start screen by starting to type the name of the app.

Preparation Steps

1. Ensure that 20410D-LON-DC1 is running.
2. Start 20410D-LON-SVR1.
3. Start 20410D-LON-CL1.

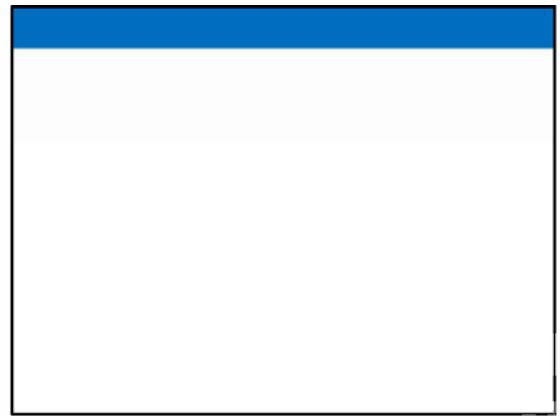
Demonstration Steps

Use Server Manager to manage a remote server

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In the Server Manager Dashboard detail pane, click **Add other servers to manage**.
3. In the Add Servers dialog box, in the Name box, type **LON-SVR1**, and then click **Find Now**.
4. Select **LON-SVR1**, click the arrow to move it into the **Selected** pane, and then click **OK**.

Add the DNS Server role on a remote server

1. In the Server Manager Dashboard detail pane, click **Add roles and features**.
2. On the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, click **LON-SVR1.Adatum.com** and click **Next**.
5. On the **Select server roles** page, select the **DNS Server** check box.
6. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **DNS Server** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**, and then click **Close**.



Connect to and configure a remote server by using RDP

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, click **Local Server**.
3. In the details pane, next to **Remote Desktop**, click **Disabled**.
4. In the **System Properties** dialog box, click **Allow remote connections to this computer**.
5. In the **Remote Desktop Connection** dialog box, click **OK**, and then click **OK**.
6. On LON-DC1, click the **Start** screen button in the lower-left corner.
7. Type **Remote**, and then click the **Remote Desktop Connection** icon.
8. In the **Remote Desktop Connection** dialog box, type **LON-SVR1**, and then click **Connect**.
9. Connect as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
10. Sign out from LON-SVR1.

1: Deploying and Managing Windows Server 2012

Demonstration: Using Windows PowerShell

In this demonstration, you will see how to use Windows PowerShell to:

- Display the running services and processes on a server
- Connect to a remote computer to display all services and their current status
- Invoke commands to multiple computers and display running processes

When you perform this demonstration, explain the information that is displayed after executing each command. Explain how you could modify the commands to display different information.

Mention that Windows PowerShell cmdlets are not case-sensitive.

Point out that you must exit the remote Windows PowerShell session or the invoke-command cmdlets will fail.

Preparation Steps

1. If necessary, start 20410D-LON-DC1.
2. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Start 20410D-LON-SVR1.
4. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Use Windows PowerShell to display the running services and processes on a server

1. On LON-DC1, on the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

Get-Service | where-object {\$_ .status -eq "Running"}

3. To view all the commands that are related to managing services, at the Windows PowerShell prompt, type the following command, and then press Enter:

Get-Command -Noun Service

4. To view a list of running processes on the server, at the Windows PowerShell prompt, type the following command, and then press Enter:

Get-Process

5. To view all the commands that are related to managing processes, at the Windows PowerShell prompt, type the following command, and then press Enter:

Get-Help Process



6. To view detailed information about the **Start-Process** cmdlet, at the Windows PowerShell prompt, type the following command, and then press Enter:

Get-Help -Full Start-Process

7. Close the Windows PowerShell window.
8. On the taskbar, right-click the **Windows PowerShell** icon, and then click **Run as Administrator**. Discuss with students why you might need to run a Windows PowerShell session using this option.

Use Windows PowerShell to connect to a remote computer and display all services and their current status

1. On LON-SVR1, click the **Windows PowerShell** icon on the taskbar to start Windows PowerShell.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

Enable-PSRemoting

3. Read the output, and respond to each of the ensuing prompts by pressing Enter (five times) to accept the default response of **Yes**.
4. Switch to **LON-DC1**, and then click the **Windows PowerShell** icon on the taskbar to start Windows PowerShell.
5. At a Windows PowerShell prompt, type the following commands, and press Enter after each one:

Enter-PSSession -Computername LON-SVR1

Get-Service

Exit-PSSession

6. View the resulting output.

Use Windows PowerShell to invoke commands to multiple computers and display running services

1. On LON-DC1, type the following command, and then press Enter:

Invoke-Command -computername LON-DC1, LON-SVR1 -Scriptblock {Get-Process}

2. Examine the output, and then close the Windows PowerShell window.

1: Deploying and Managing Windows Server 2012

Demonstration: Using Windows PowerShell ISE

In this demonstration, you will see how to:

- Use Windows PowerShell ISE to import the ServerManager module
- View the cmdlets made available in the ServerManager module
- Use the **Get-WindowsFeature** cmdlet from Windows PowerShell ISE
- Run a Windows PowerShell script from the scripting pane to create a universal group named Helpdesk and add members

Point out the autocomplete capability that occurs as you type cmdlets.

Point out that the script runs the following three commands:

- Imports the Active Directory module.
- Creates a universal group named Helpdesk.
- Populates the group based on the value of the Department field in the user properties.

Preparation Steps

1. If necessary, start 20410D-LON-DC1.
2. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Use Windows PowerShell ISE to import the ServerManager module

1. Ensure that you are signed in to LON-DC1 as Administrator.
2. In Server Manager, click **Tools**, and then click **Windows PowerShell ISE**.
3. At the prompt, type **Import-Module ServerManager**, and then press Enter.

This demonstrates the command-completion feature of the Windows PowerShell ISE.

View the cmdlets made available in the ServerManager module

- In the Commands pane, use the **Modules** drop-down menu to select the **ServerManager** module. Describe the function of the listed Windows PowerShell cmdlets.

Use the Get-WindowsFeature cmdlet from Windows PowerShell ISE

1. Click **Get-WindowsFeature**, and then click **Show Details**.
2. In the **ComputerName** field, type **LON-DC1**, and then click **Run**.

Run a Windows PowerShell script from the scripting pane to create a universal group named Helpdesk and add members

1. In Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. Expand **Adatum.com**, and then click the **IT** organizational unit (OU). Note that there is no group named Helpdesk.
3. Use File Explorer to go to **E:\Labfiles\Mod01**, right-click **CreateAndPopulateHelpdesk.ps1**, and then click **Edit**.

This opens a new instance of Windows PowerShell ISE and exposes the scripting pane.

4. View the script, and then click the green arrow on the toolbar to run the script.
5. Switch back to **Active Directory Users and Computers** and refresh the view of the IT OU. You should now see a group named Helpdesk.
6. Right-click the **Helpdesk** group and click **Properties**.
7. Click the **Members** tab.
8. Close all open windows.

You will see that the group is populated by the members of the IT department

2: Introduction to Active Directory Domain Services

Demonstration: Viewing the SRV Records in DNS

In this demonstration, you will see how to use DNS Manager to view SRV records

Demonstrate the SRV records in DNS briefly, or as appropriate for the level of student experience or interest.

After showing the sub-domains that start with an underscore, explain that domain controllers register several SRV records so that you can search them in multiple ways. Look for an SRV record in **_tcp.Default-First-Site-Name._sites.adatum.com** that is offering the Kerberos authentication service. Examine the record, and show that server LON-DC1.adatum.com is offering the Kerberos authentication service over TCP port 88, and that the server is answering for the site Default-First-Site-Name. This is the preferred domain controller to connect to because the domain controller is in the same AD DS site as the client computer.

Point out that, because domain controllers register SRV records in many different ways, you can find an alternative if the preferred domain controller is not available. Alternatively, you could go to C:\windows\system32\config, open netlogon.dns with Notepad, and show all of the SRV records that each domain controller will register in DNS.

Note that SRV records are registered in DNS by the Net Logon service that is running on each domain controller. If the SRV records are not entered in DNS correctly, you can trigger the domain controller to reregister those records by restarting the Net Logon service on that domain controller. This reregisters only the SRV records. If you want to reregister the host record information in DNS, you must run **ipconfig /registerdns** from the command prompt, just as you would for any other computer.

Preparation Steps

Start the 20410D-LON-DC1 virtual machine.

Demonstration Steps

View the SRV records by using DNS Manager

1. On LON-DC1, sign in with the user account **Adatum\Administrator** and the password **Pa\$\$w0rd**.
2. In Server Manager, click the **Tools** menu.

2: Introduction to Active Directory Domain Services



3. In the Tools list, click **DNS**.
4. In the DNS Manager window, in the tree menu, go to **LON-DC1\Forward Lookup Zones\adatum.com**. Show the following four DNS subzones:
 - _msdcs
 - _sites
 - _tcp
 - _udp
5. Expand **Forward Lookup Zones**, expand **adatum.com**, expand **_sites**, expand **Default-First-Site-Name**, expand **_tcp**, and then, in the right pane, show the following record:
_ldap Service Location (SRV) [0][100][389] lon-dc1.adatum.com.
6. If students have sufficient expertise and interest, open **c:\windows\system32\config**, and then open the **netlogon.dns** file in Notepad.

Show all the SRV records that this domain controller will register in DNS.

After you complete the demonstration, revert the virtual machine.

3: Managing Active Directory Domain Services Objects

In this demonstration, you will see how to:

- Use the Active Directory Administrative Center to manage user accounts
 - Delete a user account
 - Create a new user account
 - Move the user account
 - View the WINDOWS POWERSHELL HISTORY
- Use Windows PowerShell to manage user accounts
 - Find inactive user accounts
 - Find disabled user accounts
 - Delete disabled user accounts

Discussion Prompt

When you discuss the content that precedes the demonstration steps, students might be interested in discussing how to communicate a password change to users. Ask your students how they currently do this, and have them think about other methods. Possible solutions include sending a text to their cell phones, sending an email to an alternate address such as a Microsoft Live account, or making a telephone call.

Windows PowerShell

If appropriate, mention to your students that they also can use Windows PowerShell® commands to perform common user administration tasks, such as resetting a user's password, by using the **Set-ADAccountPassword** command.

For example, the following command resets Amy's password:

Set ADAccountPassword -identity 'cn=amy, ou=IT, dc=contoso, dc=com' -Reset -NewPassword (ConvertTo SecureString -AsPlainText "Pa\$\$w0rd2" -Force)

To unlock a user account by using Windows PowerShell, you can use the following command:

Unlock ADAccount -identity 'cn=amy strand, ou=IT, dc=contoso, dc=com'

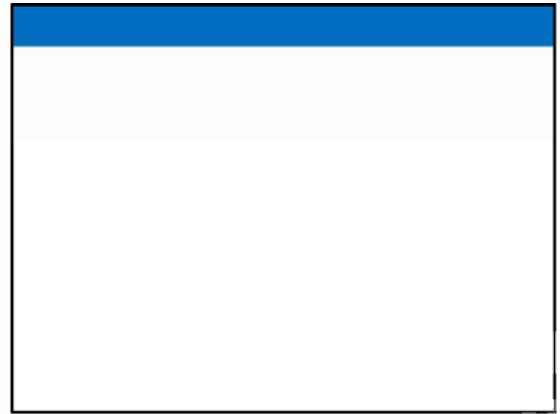
To disable or enable a user account by using Windows PowerShell, type the following cmdlets at a Windows PowerShell prompt:

Enable ADAccount -identity <name>

Disable ADAccount -identity <name>

Preparation Steps

Start the required virtual machine, 20410D-LON-DC1.



Demonstration Steps

Delete a user account

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-DC1, in Server Manager, click **Tools**.
3. Click **Active Directory Administrative Center**.
4. In the Active Directory Administrative Center, click **Adatum (local)**, and then double-click **Managers**.
5. In Managers, right-click **Ed Meadows**, and then click **Delete**.
6. In the **Delete Confirmation** dialog box, click **Yes**.

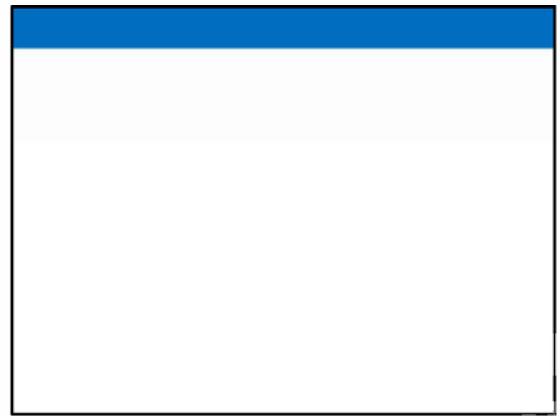
Create a new user account

1. In the Action pane, click **New**, and then click **User**.
2. In the **Create User** dialog box, in **Full name**, type **Ed Meadows**.
3. In **User UPN logon**, type **Ed**.
4. In **Password** and **Confirm password**, type **Pa\$\$w0rd**, and then click **OK**.

Move the user account

1. Right-click **Ed Meadows**, and then click **Move**.
2. Click the **IT** organizational unit (OU), and then click **OK**.
3. In the navigation pane, click **Adatum (local)**.
4. In the results pane, double-click **IT**.
5. Verify that Ed Meadow's account is listed.

3: Managing Active Directory Domain Services Objects



View the WINDOWS POWERSHELL HISTORY

1. If you have not already done so, maximize Active Directory Administrative Center.
2. At the bottom of the Active Directory Administrative Center window, click **WINDOWS POWERSHELL HISTORY** to expand the history section.
3. Discuss the following commands and switches:
 - a. The **Remove-ADObject** command and the switches used with it to delete Ed Meadows.
 - b. The **New-ADUser** command and the switches used with it to recreate Ed Meadows.
 - c. The additional commands used to configure the Ed Meadows account.
 - d. The **Move-ADObject** command and the switches used with it to move Ed Meadows.
4. Close the Active Directory Administrative Center.

Find users who have not signed in during the last 30 days

1. On the taskbar, click the **Windows PowerShell** icon.
2. To create a variable to specify the past 30 days, type the following command, and then press Enter:

\$logonDate = (get-date).AddDays(-30)
3. To find all the user accounts that have not signed in during the past 30 days, type the following command, and then press Enter:

Get-ADUser -Filter{LastLogon -le \$logonDate}

The results include nearly every account in the domain because most of the accounts have never signed in.

3: Managing Active Directory Domain Services Objects

Find and delete all disabled user accounts

1. To find all the disabled user accounts, type the following command, and then press Enter:

```
Get-ADUser -Filter{enabled -ne $True}
```

The results should list four accounts in the Sales OU and two system accounts in the Users container, Guest and krbtgt.

2. To delete the disabled user accounts in the Sales OU without being prompted for confirmation, type the following command, and then press Enter:

```
Get-ADUser -SearchBase "OU=Sales,DC=Adatum,DC=com" -Filter{enabled -ne $true} | Remove-adobject -Confirm:$False
```

If this command runs successfully, there is no output.

3. To verify that the disabled accounts have been deleted, type the following command, and then press Enter:

```
Get-ADUser -Filter{enabled -ne $True}
```

The results should list the two system accounts in the Users container, Guest and krbtgt.

Leave the virtual machine running for the next demonstration.

3: Managing Active Directory Domain Services Objects

Demonstration: Using Templates to Manage User Accounts

In this demonstration, you will see how to:

- Create a user template account
- Use Windows PowerShell to create a user from the user template
- Verify the properties of the new user account

Discussion Prompt

Discuss the reasons for using template accounts. Typically, you use template accounts to save the time needed to fill out the properties on the user accounts. Explain that using Windows PowerShell to create users from a template copies only the specified properties. The properties that cannot be copied include the Member Of property. If you want to include the group memberships from a template, then you need to use either Active Directory Users and Computers or the Active Directory Administrative Center.

Reference:

For a full list of the properties that can be copied from a template for a new user, refer to "Copy a User's Properties" at <http://go.microsoft.com/fwlink/?LinkId=331092>.

Preparation Steps

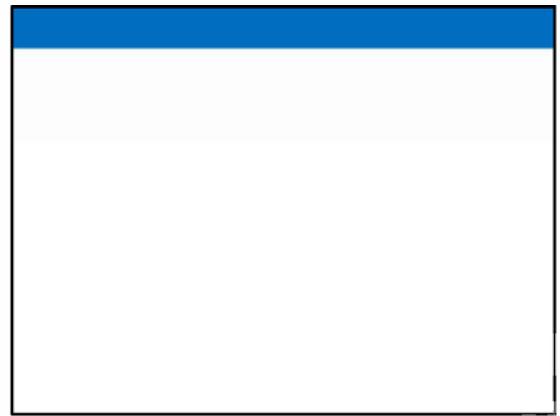
Ensure that the required virtual machine, 20410D-LON-DC1, is running.

Demonstration Steps

Create a template account

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. In the Active Directory Administrative Center, click **Adatum (local)**, and then double-click **Sales**.
3. In the Action pane, click **New**, and then click **User**.
4. In the **Create User** dialog box, in **First name**, type **_LondonSales**, in **Last name**, type **Template**.
5. In **User UPN logon**, type **_LondonSales**.
6. Select **Protect from accidental deletion**.
7. Under Organization, in **Department**, type **Sales**.
8. In **Company**, type **A. Datum**.

3: Managing Active Directory Domain Services Objects



9. In **City**, type **London**.
10. In **Description**, type **London Sales users**.
11. In the **Member of** section, click **Add**.
12. In **Enter the object names to select**, type **Sales**, and then click **OK**.
13. In the **Create User _LondonSales Template** dialog box, click **OK**.

Create a user from the **_LondonSales** template

1. In the Windows PowerShell window, create a variable (\$LondonSales) to hold the **_LondonSales** properties by using the following command, and then press Enter:

```
$LondonSales = Get-ADUser -Identity "_LondonSales" -Properties  
Department, Company, City
```

2. To create a new Sales user in the Sales OU, type the following command, and then press Enter:

```
New-ADUser -Name "Dan Park" -SamAccountName "Dan" -Path  
"OU=Sales,DC=Adatum,DC=com" -AccountPassword  
(ConvertTo-SecureString -AsPlainText "Pa$$w0rd" -Force) -GivenName  
"Dan" -Surname "Park" -DisplayName "Dan Park" -Enabled  
$True -UserPrincipalName "Dan@Adatum.com" -ChangePasswordAtLogon  
$true -Instance $LondonSales
```

Verify the User Properties

1. In the Windows PowerShell window, type the following command, and then press Enter:

```
Get-ADUser -Identity "Dan" -Properties *
```

2. Verify that the properties that you defined in the template were copied to the new user.

Leave the virtual machine running for the next demonstration.

3: Managing Active Directory Domain Services Objects

Demonstration: Managing Groups

In this demonstration, you will see how to:

- Create a new group
- Add members to the group
- Add a user to the group
- Change the group type and scope
- Modifying the group's Managed By property

Preparation Steps

The required virtual machine, 20410D-LON-DC1, should be running after the previous demonstration.

Demonstration Steps

Create a new group

1. On LON-DC1, switch to **Active Directory Administrative Center**.
2. Expand Adatum (Local), and then click **IT**.
3. In the Tasks list, under **IT**, point to **New**, and then click **Group**.
4. In the **Create Group** dialog box, in **Group name**, type **IT Managers**.

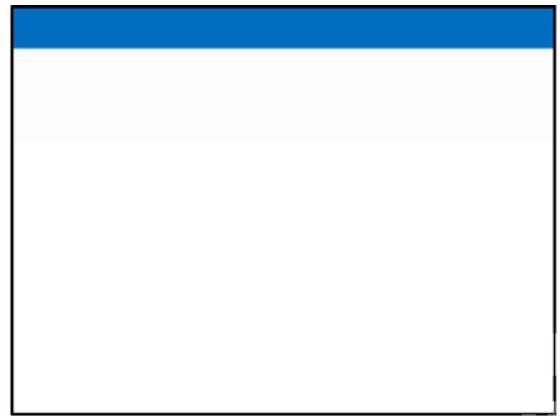
Add members to the group

1. Scroll down, and under **Members**, click **Add**.
2. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in **Enter the object names to select (examples)**, type **April; Don**.
3. Click **Check Names**, and then click **OK**.
4. In the **Create Group IT Managers** dialog box, click **OK**.

Add a user to the group

1. In the details pane, right-click **Ed Meadows**.
2. Click **Add to group**.
3. In the **Select Groups** dialog box, in **Enter the object names to select (examples)**, type **IT Managers**.
4. Click **Check Names**, and then click **OK**.

3: Managing Active Directory Domain Services Objects



Change the group type and scope

1. In the details pane, double-click **IT Managers**.
2. In the **IT Managers** dialog box, under **Group scope**, click **Universal**.
3. Under **Group type**, click **Distribution**, and then click **OK**.

Modify the group's Managed By property

1. In the details pane, double-click **IT Managers**.
2. In the details pane, under **Managed By**, click **Edit**.
3. In the **Select User, Contact or Groups** dialog box, in **Enter the object names to select (examples)**, type **Ed Meadows**, click **Check Names**, and then click **OK**.
4. Select **Manager can update membership list**, and then click **OK**.

Leave the virtual machine running for the next demonstration.

3: Managing Active Directory Domain Services Objects

Demonstration: Delegating Administrative Permissions

In this demonstration, you will see how to:

- Create an OU
- Move objects into an OU
- Delegate a standard task
- Delegate a custom task
- View AD DS permissions resulting from these delegations

Discussion Prompt

You can manage delegation of control in Active Directory Domain Services (AD DS) either manually or by using the Delegation of Control Wizard. If you have a complex permission scenario, you may need to configure the permissions manually, but it is usually easier to assign permissions in AD DS by using the Delegation of Control Wizard.

Preparation Steps

The required virtual machine, 20410D-LON-DC1, should be running after the previous demonstration.

Demonstration Steps

Create an OU

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. Expand the **Adatum.com** domain.
3. Right click **Adatum.com**, point to **New**, and then click **Organizational Unit**.
4. In the **New Object – Organizational Unit** dialog box, in **Name**, type **Executives**.

Note: Discuss the purpose of the **Protect Container From Accidental Deletion** setting.

5. In the **New Object – Organizational Unit** dialog box, click **OK**.

Move users into the Executives OU

1. Click the **Managers** OU.
2. Click **Carol Troup**, and then hold down Shift while clicking **Euan Garden**.
3. Right click **Euan Garden**, and then click **Move**.
4. In the **Move** dialog box, click **Executives**, and then click **OK**.

3: Managing Active Directory Domain Services Objects

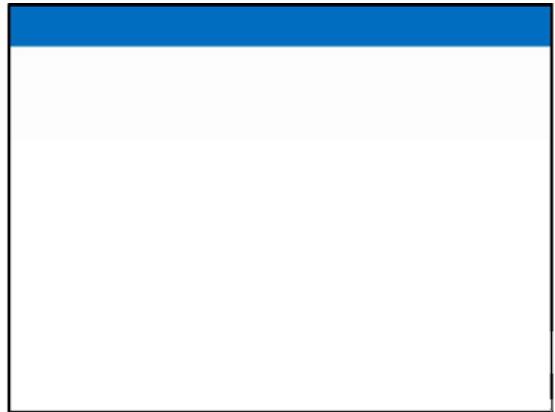
Delegate a standard task

1. In the navigation pane, right-click **Executives**, and then click **Delegate Control**.
2. In the Delegation of Control Wizard, click **Next**.
3. On the **Users or Groups** page, click **Add**.
4. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **IT**, and then click **OK**.
5. On the **Users or Groups** page, click **Next**.
6. On the **Tasks to Delegate** page, in the **Delegate the following common tasks** list, select the following options, and then click **Next**
 - o **Create, delete, and manage user accounts**,
 - o **Reset user passwords and force password change at next logon**,
 - o **Read all user information**
7. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

Delegate a custom task

1. In the navigation pane, right-click **Executives**, and then click **Delegate Control**.
2. In the Delegation of Control Wizard, click **Next**.
3. On the **Users or Groups** page, click **Add**.
4. In the **Select Users, Computers, or Groups** dialog box, in **Enter the object names to select (examples)**, type **IT**, and then click **OK**.
5. On the **Users or Groups** page, click **Next**.
6. On the **Tasks to Delegate** page, click **Create a custom task to delegate**, and then click **Next**.
7. On the **Active Directory Object Type** page, click **Only the following objects in the folder**.
8. In the list, select **Computer objects**.
9. Select **Create selected objects in this folder** and **Delete selected objects in this folder**, and then click **Next**.

3: Managing Active Directory Domain Services Objects



10. On the **Permissions** page, in the **Permissions** list, select **Full Control**, and then click **Next**.
11. On the **Completing the Delegation of Control Wizard** page, click **Finish**.

View AD DS permissions resulting from these delegations

1. On the **View** menu, click **Advanced Features**.
2. In the navigation pane, right-click **Executives**, and then click **Properties**.
3. In the **Executives Properties** dialog box, on the **Security** tab, click **Advanced**.

In the **Advanced Security Settings for Executives** dialog box, notice the Allow permissions that are assigned to IT (ADATUM\IT). These were created during the delegation process.

4. Click **Cancel** twice, and then close all open windows except Server Manager.

After you complete the demonstration, revert all virtual machines.

4: Automating Active Directory Domain Services Administration

Demonstration: Using Graphical Tools to Perform Bulk Operations

In this demonstration, you will see how to:

- Create a query for all users
- Configure the Company attribute for all users
- Verify that the Company attribute has been modified

Preparation Steps

Start the 20410D-LON-DC1 virtual machine.

Demonstration Steps

Create a query for all users

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
3. In the Active Directory Administrative Center, in the navigation pane, click **Global Search**.
4. At the far right of the Global Search pane, click the down arrow that is displayed inside a circle to display **Add criteria**.
5. Click **Add criteria**, select the **Object type is user/inetOrgPerson/computer/group/organization unit** check box, and then click **Add**.
6. Verify that the criteria that you added is **and The object type is: User**.
7. Click the **Search** button.

Configure the Company attribute for all users

1. Press **Ctrl+A** to select all of the user accounts, and then click **Properties**.
2. In the Multiple Users pane, in the Organization section, select the **Company** check box.
3. In the **Company** text box, type **A. Datum**, and then click **OK**.

Verify that the Company attribute has been modified

1. In the Global Search pane, click **Adam Barr**, and then click **Properties**.
2. In the Adam Barr window, verify that the Company is **A. Datum**.
3. Click **Cancel**.
4. Close the Active Directory Administrative Center.

Leave the virtual machine running after you complete the demonstration.

4: Automating Active Directory Domain Services Administration

Demonstration: Performing Bulk Operations with Windows PowerShell

In this demonstration, you will see how to:

- Configure a department for users
- Create an OU
- Run a script to create new user accounts
- Verify that new user accounts were created

Preparation Steps

For this demonstration, you need the 20410D-LON-DC1 virtual machine. It should be running after the previous demonstration.

Demonstration Steps

Configure a department for users

1. On LON-DC1, on the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

Get-ADUser -Filter * -SearchBase "ou=Research,dc=adatum,dc=com"

3. Type the following command, and then press Enter:

Get-ADUser -Filter * -SearchBase "ou=Research,dc=adatum,dc=com" | Set-ADUser -Department Research

4. Type the following command, and then press Enter:

Get-ADUser -Filter 'department -eq "Research"' | Format-Table DistinguishedName,Department

5. Type the following command, and then press Enter:

Get-ADUser -Filter 'department -eq "Research"' -Properties Department | Format-Table DistinguishedName,Department

Create an organizational unit (OU)

- At the Windows PowerShell prompt, type the following command, and then press Enter:

New-ADOrganizationalUnit LondonBranch -Path "dc=adatum,dc=com"

4: Automating Active Directory Domain Services Administration

Run a script to create new user accounts

1. On the taskbar, click the **File Explorer** icon.
2. In File Explorer, expand drive **E**, expand **Labfiles**, and then click **Mod04**.
3. Double-click **DemoUsers.csv**.
4. In the **How do you want to open this type of file (.csv)?** message, click **NotePad**.
5. In NotePad, review the contents of the .csv file, and then read the header row.
6. Close NotePad.
7. In File Explorer, right-click **DemoUsers.ps1**, and then click **Edit**.
8. In Windows PowerShell Integrated Scripting Environment (ISE), review the contents of the script.

Note that the script:

- Refers to the location of the .csv file.
 - Uses a **foreach** loop to process the .csv file contents.
 - Refers to the columns defined by the header in the .csv file.
9. Close Windows PowerShell ISE.
 10. At the Windows PowerShell prompt, type **cd E:\Labfiles\Mod04**, and then press Enter.
 11. Type **.\DemoUsers.ps1**, and then press Enter.
 12. Close Windows PowerShell.

Verify that new user accounts were created

1. In Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. In the Active Directory Administrative Center, in the navigation pane, go to **Adatum (local)>LondonBranch**.
3. Verify that the user accounts were created.

Note that the accounts are disabled, because no password was set during creation.
4. Close the Active Directory Administrative Center.

After you complete the demonstration, revert the virtual machine.

5: Implementing IPv4

Demonstration: How to Capture and Analyze Network Traffic by Using Microsoft Message Analyzer

In this demonstration, you will see how to:

- Start a new Capture/Trace in Microsoft Message Analyzer
- Capture packets from a ping request
- Analyze the captured network traffic
- Filter the network traffic

Mention to students that filtering is useful when you want to display only specific packets when troubleshooting a specific problem. For example, you could display only communication with a specific IP address. If students are interested, consider showing the contents of a few more packets, such as ARP packets.

Preparation Step

Start the virtual machines 20410D-LON-DC1, 20410D-LON-RTR, and 20410D-LON-SVR2.

Demonstration Steps

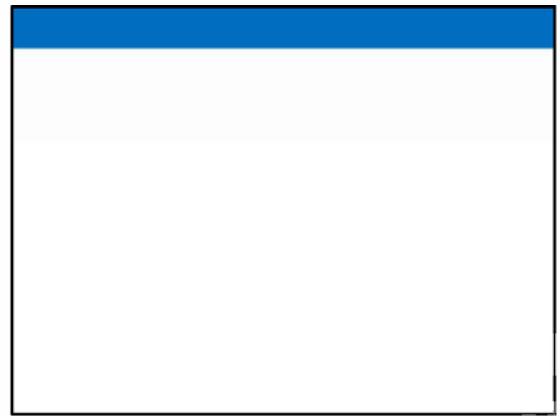
Start a new Capture/Trace in Microsoft Message Analyzer

1. Sign in to **LON-SVR2** as **Adatum\Administrator** with a password of **Pa\$\$w0rd**.
2. On the taskbar, click the **Windows PowerShell** icon.
3. At the Windows PowerShell prompt, type the following, and then press Enter:
ipconfig /flushdns
4. On the Start screen, click **Microsoft Message Analyzer**.
5. In the Microsoft Message Analyzer dialog box, click **Do not update items**, and then click **OK**.
6. In the navigation pane, click **Capture/Trace**, and then, in the **Trace Scenarios** section, click **Firewall**.

Capture packets from a ping request

1. In Microsoft Message Analyzer, on the toolbar, click **Start With**.
2. At the Windows PowerShell prompt, type the following, and then press Enter:
Test-NetConnection LON-DC1.adatum.com
3. In Microsoft Message Analyzer, on the toolbar, click **Stop**.

5: Implementing IPv4



Analyze the captured network traffic

1. In Microsoft Message Analyzer, in the results pane, under the Module column, select the first **ICMP** packet group.
2. In the results pane, click the plus sign '+' beside the selected packet group.
3. Show that the packet group includes both the **Echo Request** and the **Echo Reply** packets, due to the ping request that was executed when running the **Test-NetConnection** cmdlet.
4. View the source and destination IP addresses for each packet.

Filter the network traffic

1. On the Microsoft Message Analyzer toolbar, in the View Filter section, in the Filter box, type the following, and then click **Apply Filter**:
***DestinationAddress == 172.16.0.10**
2. Verify that only packets that match the filter are displayed.
3. Close **Microsoft Message Analyzer**.

6: Implementing Dynamic Host Configuration Protocol

Demonstration: Installing the DHCP Server Role

In this demonstration, you will see how to:

- Install the DHCP server role
- Authorize the DHCP server

Preparation Steps

Start the following virtual machines:

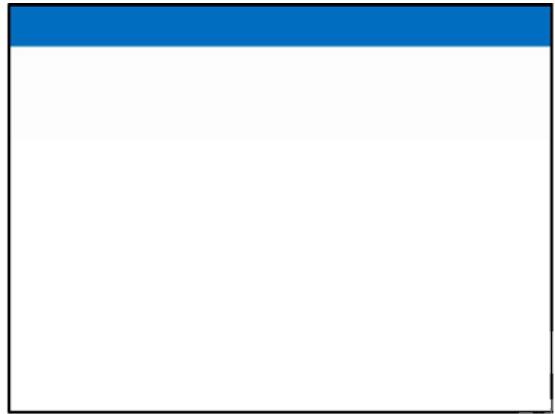
- 20410D LON DC1
- 20410D-LON-RTR
- 20410D LON SVR1
- 20410D-LON-SVR2

Demonstration Steps

Install the DHCP server role

1. Sign in to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, in the Manage drop-down menu, click **Add Roles and Features**.
3. In the Add Roles and Features Wizard, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On **Select destination server** page, click **Next**.
6. On **Select server roles** page, select the **DHCP Server** check box.
7. In Add Roles and Features Wizard, click **Add Features**, and then click **Next**.
8. On the **Select features** page, click **Next**.
9. On the **DHCP Server** page, click **Next**.
10. On the Confirm installation selections page, click **Install**.
11. On the **Installation progress** page, wait until the “Installation succeeded on lon-svr1.adatum.com” message appears, and then click **Close**.
12. Repeat steps 1 through 11 on LON-SVR2.

6: Implementing Dynamic Host Configuration Protocol



Authorize the DHCP Server

1. On LON-SVR1, on the Server Manager dashboard, click **Tools**, and then click **DHCP**.
2. In the DHCP console, expand **lon-svr1.adatum.com**.
3. Right-click **lon-svr1.adatum.com**, and then click **Authorize**.
4. In the DHCP console, right-click **lon-svr1.adatum.com**, and then click **Refresh**.

Notice that the icons next to IPv4 and IPv6 change color from red to green, which indicates that the DHCP server has been authorized in Active Directory® Domain Services (AD DS).

5. Repeat steps 1 through 3 on LON-SVR2, replacing the FQDN in step 4 with **lon-svr2.adatum.com**.

Note: Leave all virtual machines in their current state for the next demonstration.

6: Implementing Dynamic Host Configuration Protocol

Demonstration: Creating and Configuring a DHCP Scope

In this demonstration, you will see how to configure scope and scope options in DHCP.

Preparation Steps

You need the 20410D-LON-DC1, 20410D-LON-SVR1, 20410D-LON-RTR, and 20410D-LON-SVR2 virtual machines to complete this demonstration. They should be running after the previous demonstration.

Demonstration Steps

Configure scope and scope options in DHCP

1. On LON-SVR1, in DHCP, in the navigation pane, click **lon-svr1.adatum.com**, expand **IPv4**, right-click **IPv4**, and then click **New Scope**.
2. In the New Scope Wizard, click **Next**.
3. On the **Scope Name** page, in the **Name** box, type **Branch Office**, and then click **Next**.
4. On the **IP Address Range** page, complete the page using the following information, and then click **Next**:
 - a. Start IP address: **172.16.0.100**
 - b. End IP address: **172.16.0.200**
 - c. Length: **16**
 - d. Subnet mask: **255.255.0.0**
5. On the **Add Exclusions and Delay** page, complete the page using the following information:
 - Start IP address: **172.16.0.190**
 - End IP address: **172.16.0.200**
6. Click **Add**, and then click **Next**.
7. On the **Lease Duration** page, click **Next**.
8. On the **Configure DHCP Options** page, click **Next**.
9. On the **Router (Default Gateway)** page, in the IP address box, type **172.16.0.1**, click **Add**, and then click **Next**.

6: Implementing Dynamic Host Configuration Protocol

10. On the **Domain Name and DNS Servers** page, click **Next**.
11. On the **WINS Servers** page, click **Next**.
12. On the **Activate Scope** page, click **Next**.
13. On the **Completing the New Scope Wizard** page, click **Finish**.

Configure scope and scope options in DHCP with Windows PowerShell

1. Explain that you will use similar settings to those that you just applied to LON-SVR1, but you will alter the address range and default gateway for the 10.10.0.0 network, as appropriate.
2. On LON-SVR2, from the desktop, click the **PowerShell** icon on the taskbar.
3. In Windows PowerShell®, type the following cmdlets, and then press Enter after each one:

```
Add-DhcpServerv4Scope -Name "Branch Office 2" -StartRange 10.10.0.100 -EndRange 10.10.0.200 -SubnetMask 255.255.0.0
```

```
Add-DhcpServerv4ExclusionRange -ScopeID 10.10.0.0 -StartRange 10.10.0.190 -EndRange 10.10.0.200
```

```
Set-DhcpServerv4OptionValue -Router 10.10.0.1
```

```
Set-DhcpServerv4Scope -ScopeID 10.10.0.0 -State Active
```

4. In LON-SVR2 Server Manager, click the **Tools** drop-down menu, and then select **DHCP**.
5. In the DHCP Manager, expand **lon-svr2.adatum.com**, and then expand **IPv4**.
6. Examine the scope that you just created, pointing out the various entries that the Windows PowerShell cmdlets made. Explain that, if you were creating numerous Dynamic Host Configuration Protocol (DHCP) scopes, you could write a Windows PowerShell script by using the cmdlets listed with variables as substitutes for the various IP address that could be called when run.

7: Implementing DNS

Demonstration: Troubleshooting Name Resolution

In this demonstration, you will see how to:

- Use Windows PowerShell cmdlets to troubleshoot DNS
- Use command-line tools to troubleshoot DNS

Discuss troubleshooting techniques for DNS.

Note that the new cmdlets from Windows Server 2012 R2 that discuss signing keys and trusts were introduced in Windows Server 2012 R2 to facilitate enhanced DNSSEC functionality; however, further discussion of them is beyond the scope of this course. Explain that although these cmdlets are listed in the course to show the new cmdlets available in Windows Server 2012 R2, they are not used in the lab.

Preparation Steps

Start 20410D-LON-DC1 and 20410D-LON-CL1.

Demonstration Steps

Use Windows PowerShell cmdlets to troubleshoot DNS

1. Sign in to LON-DC1 and LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-CL1, at the lower-left of the **Start screen**, click the white **Down Arrow** icon.
3. In the **Apps** screen, scroll to the right, and in the **Windows System** category, click **Windows PowerShell**.
4. In **Windows PowerShell**, type the following cmdlets, and press Enter after each one:

Get-DnsClientServerAddress

Clear-DnsClientCache

Note that the DNS Server address assigned to Ethernet IPv4 is **172.16.0.10**. This is LON-DC1.

5. Explain the Interface Index number and how it is used to modify certain settings.
6. Note the entries labeled **Ethernet** in the InterfaceAlias column, and the entry labeled **IPv4** in the Address Family column. In the Interface Index column, note the Interface Index number that is in the same row as Ethernet and IPv4. Write this number here:

You will use this specific Interface Index number in a later step.

7. In Windows PowerShell, type the following cmdlet, and then press Enter:

Resolve-DnsName 1on-dc1

Note the address returned. Do not close Windows PowerShell.

7: Implementing DNS



8. Press **Windows key+X**, and then click **Control Panel**.
9. In **Control Panel**, click the **Network and Internet** hyperlink.
10. On the **Network and Internet** page, select and then click the **Network and Sharing Center** hyperlink.
11. On the **Network and Sharing Center** page, click the **Ethernet** hyperlink.
12. In the **Ethernet Status** window, click the **Details** button.
13. In the **Network Connections Details** pop-up window, write down the information shown in the following table.

IPv4 Address	
IPv4 Subnet Mask	
IPV4 Default Gateway	
IPv4 DNS Server	

You need to write down this information before you proceed to the next step, because you need to enter this information in a later step.

14. Click the **Close** button.
15. On the **Ethernet Status** page, click the **Properties** button.
16. In the **This connection uses the following items** section, scroll down, select **Internet Protocol Version 4 (TCP/IPv4)**, and then click the **Properties** button.
17. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select the **Obtain an IP address automatically** and **Obtain DNS server address automatically** option buttons, click **OK**, and then click **Close** twice.

7: Implementing DNS

18. Return to **Windows PowerShell**, type the following cmdlets, pressing Enter after each cmdlet, where X is the Interface Index number you wrote down in step 6:

Set-DnsClientServerAddress -InterfaceIndex X -ResetServerAddresses

Clear-DnsClientCache

Note that there is no IP address for IPv4.

19. In **Windows PowerShell**, type the following cmdlet, press Enter, and then note the message that is returned:

Resolve-DnsName 1on-dc1

20. In **Windows PowerShell**, type the following cmdlet, where X is the Interface Index number you wrote down in step 6, and then press Enter:

Set-DnsClientServerAddress -InterfaceIndex X -ServerAddress 172.16.0.10

21. In **Windows PowerShell**, type the following cmdlet, and then press Enter:

Get-DnsClientServerAddress

Note that there is now an address for IPv4.

22. In Windows PowerShell, type the following cmdlet, press Enter, and then note the address returned:

Resolve-DnsName 1on-dc1

23. Return to the **Network and Sharing Center**, and then click the **Ethernet** hyperlink.
24. On the **Ethernet Status** page, click the **Properties** button.
25. On the **Ethernet Properties** page, in the **This connection uses the following items** section, scroll down and select **Internet Protocol Version 4 (TCP/IPv4)**, and then click the **Properties** button.
26. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, select the **Use the following IP address** option button, enter the information that you wrote down in Step 13 into the same IP blocks you copied them from, click **OK**, and then click **Close** twice.

7: Implementing DNS

27. To demonstrate the output of the following cmdlets, in the Windows PowerShell window, type each of the following cmdlets, and press Enter after each one:

Get-DnsClientCache
Clear-DnsClientCache
Get-DnsClientCache
Get-DnsClientGlobalSetting
Register-DnsClient

28. Close **Windows PowerShell** and **Network and Sharing Center**.

Using Command Line tools to troubleshoot DNS

1. Go to the **Start screen** and, at the lower-left of the Start screen, click the white **Down Arrow** button.
2. In the **Apps screen**, scroll to the right, in the **Windows System** category, right-click **Command Prompt**, and then in the app bar, click **Run as Administrator**.
3. In the Command Prompt window, type the following, and then press Enter:

ipconfig /all

4. Review the output returned, and note the DNS server section.
5. Type **nslookup**, and then press Enter.

You should see the address of the DNS server from step 3 above returned.

Note the > prompt, which means that you are in the nslookup prompt.

6. Type **!on-cl1**, and then press Enter.
7. Type **exit**, and do not close any open Windows.
8. Switch to **LON-DC1**.
9. Go to the Start screen and then, at the lower-left of the **Start screen**, click the white **Down Arrow** icon.
10. On the Apps screen, scroll to the right, in the **Windows System** category, right-click **Command Prompt**, and then in the app bar, click **Run as Administrator**.

7: Implementing DNS

11. At the command prompt, type the following, and then press Enter:

dnscmd /?

Use the output to review some of the dsncmd options available. Do not spend much time here because the second DNS server has not been set up.

12. At the command prompt, type the following, and then press Enter:

ipconfig /displaydns

Note the output values displayed.

13. At the command prompt, type the following, and press Enter after each line:

ipconfig /flushdns

ipconfig /displaydns

Note that the output values are gone.

14. At the command prompt, type the following, and then press Enter:

ping LON-CL1

Note that while the ping replies are not successful (the client firewall is blocking ICMP packets), the ping command returned the fully qualified domain name (FQDN) of **LON-CL1**. Point out to the students that this is an indicator that DNS name resolution occurred even before the ping packet was generated.

15. At the command prompt, type the following, and then press Enter:

ipconfig /displaydns

Note that information on the LON-CL1 DNS resource record is displayed.

16. Close all open windows, and sign out from **20410D-LON-DC1** and **20410D-LON-CL1**.

7: Implementing DNS

Demonstration: Installing the DNS Server Role

In this demonstration, you will see how to:

- Install a second DNS server
- Create a forward lookup zone by using Windows PowerShell
- Configure forwarding



Preparation Steps

Start 20410D-LON-DC1 and 20410D-LON-SVR1.

Demonstration Steps

Install a second DNS server

1. Sign in to LON-DC1 and LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-SVR1, in the Server Manager console, in the Manage tab, click **Add roles and features**.
3. On the **Before you begin** page, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, ensure that **LON-SVR1.Adatum.com** is selected, and then click **Next**.
6. On the **Select server roles** page, click **DNS Server**.
7. In the Add Roles and Features Wizard window, click **Add Features**, and then click **Next**.
8. On the **Select Features** page, click **Next**.
9. On the **DNS Server** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**.
11. On the **Installation progress** page, when a message displays that installation succeeded, click **Close**.

Create a forward lookup zone by using Windows PowerShell

1. Switch to LON-DC1.
2. On the taskbar, select the **Windows PowerShell** icon.
3. In the Windows PowerShell window, type the following cmdlet, and then press Enter:

```
Add-DnsServerPrimaryZone -Name fabrikam.com -DynamicUpdate Secure  
-ReplicationScope Domain
```

(More notes on the next slide)

7: Implementing DNS

4. Switch to the DNS Console.

If the DNS console is not open, in Server Manager, click the **Tools** menu, and then click **DNS**.

5. In the console tree, expand **LON-DC1**, and then expand **Forward Lookup Zones**.

You should see the **fabrikam.com** zone.

6. Select and then right-click the **fabrikam.com** zone, and then click **Properties**.

7. On the General tab, confirm that **Replication** is set to **All DNS Servers in the Domain**, and that **Dynamic Updates** are set to **Secure only**.

8. On the **fabrikam.com Properties** page, click **Cancel**.

Configure forwarding

1. On LON-SVR1, open the **DNS Manager** console.

2. In the DNS Manager console, right-click **LON-SVR1**, click **Properties**, and then click the **Forwarders** tab.

3. In the **Forwarders** dialog box, click **Edit**.

4. In the **Edit Forwarders** page, type **172.16.0.10**, and then click **OK** twice.

Leave all virtual machines in their current state for the next demonstration.

7: Implementing DNS

Demonstration: Creating an Active Directory-Integrated Zone

In this demonstration, you will see how to:

- Promote a server as a domain controller
- Create an Active Directory-integrated zone
- Create a record
- Verify replication to a second DNS server

Preparation Steps

You need the 20410D-LON-DC1 and 20410D-LON-SVR1 virtual machines to complete this demonstration. They should already be running from the previous demonstration.

Demonstration Steps

Promote a server as a domain controller

1. On LON-SVR1, in the Server Manager console, click **Add roles and features**.
2. On the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **LON-SVR1.Adatum.com** is selected, and then click **Next**.
5. On the **Select server roles** page, click **Active Directory Domain Services**.
6. When the **Add Roles and Features Wizard** window appears, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Active Directory Domain Services** page, click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. On the **Installation progress** page, when the **Installation succeeded** message displays, click **Close**.
11. In the **Server Manager** console, on the Navigation page, click **AD DS**.
12. On the title bar where **Configuration required for Active Directory Domain Services at LON-SVR1** is visible, click **More**.
13. On the **All Server Task Details and Notifications** page, click **Promote this server to a domain controller**.

7: Implementing DNS



14. In the Active Directory Domain Services Configuration Wizard, on the **Deployment Configuration** page, ensure that **Add a domain controller to an existing domain** is selected, and then click **Next**.
 15. On the **Domain Controller Options** page, select the **Domain Name System (DNS) server** check box, and leave the **Global Catalog (GC)** check box selected.
 16. Type **Pa\$\$w0rd** in both text fields, and then click **Next**.
 17. On the **DNS Options** page, click **Next**.
 18. On the **Additional Options** page, click **Next**.
 19. On the **Paths** page, click **Next**.
 20. On the **Review Options** page, click **Next**.
 21. On the **Prerequisites Check** page, click **Install**.
 22. On the **You're about to be signed out** app bar, click **Close**.
- Note:** The server automatically restarts as part of the procedure.
23. After LON-SVR1 restarts, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Create an Active Directory–integrated zone

1. On LON-DC1, open **Server Manager**.
2. Click **Tools**, and then click **DNS**.
3. In the DNS Manager console, click and then right-click **LON-DC1**, and then select **New Zone**.
4. In the New Zone Wizard, click **Next**.
5. On the **Zone Type** page, click **Primary zone**, ensure that the **Store the zone in Active Directory** option is selected, and then click **Next**.

Note: Point out that this option determines that the zone is in AD DS.

7: Implementing DNS

6. On the **Active Directory Zone Replication Scope** page, review the available options, and then, without making any changes, click **Next**.
7. On the **Forward or Reverse Lookup Zone** page, select **Forward lookup zone**, and then click **Next**.
8. On the **Zone Name** page, in the **Zone name** field, type **Contoso.com**, and then click **Next**.
9. On the **Dynamic Update** page, review the available options, select the **Allow only secure dynamic updates** option, and then click **Next**.
10. On the **Completing the New Zone Wizard** page, click **Finish**.
11. In DNS Manager console, expand **Forward Lookup Zones**, click **Contoso.com**, and then review the records that are created automatically.

Create a record

1. In the DNS Manager console, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Contoso.com**.
2. Right-click **Contoso.com**, and then select **New Host (A or AAAA)**.
3. In the **New Host** window, in the **Name** field, type **www**, and in the IP address field, type **172.16.0.100**, click **Add Host**, and then click **OK**.
4. Click **Done**.

Verify replication to a second DNS server

1. On LON-SVR1, in the **Server Manager** console, click **Tools**, and then click **DNS**.
2. In the **DNS Manager** console, expand **LON-SVR1**, expand **Forward Lookup Zones**, and then click **Contoso.com**.
3. Verify that **www** resource record exists. It might take a couple of minutes for the record to appear, and you might have to refresh the console display.

8: Implementing IPv6

Demonstration: Configuring IPv6 Client Settings

In this demonstration, you will see how to:

- View IPv6 configuration by using **ipconfig** and **Get-NetIPAddress**
- Configure IPv6 on a domain controller and a server
- Verify IPv6 communication is functional

Preparation Steps

Start the 20410D-LON-DC1 and 20410D-LON-SVR1 virtual machines.

Demonstration Steps

View IPv6 configuration by using ipconfig and Get-NetIPAddress

1. Sign in to LON-DC1 and LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-DC1, on the taskbar, click the **Windows PowerShell®** icon.
3. At the Windows PowerShell prompt, type **ipconfig**, and then press Enter.
Notice that this returns a link-local IPv6 address.
4. At the Windows PowerShell prompt, type **Get-NetIPAddress**, and then press Enter.
Notice that the **Get-NetIPAddress** command returns a link-local IPv6 address.

Configure IPv6 on LON-DC1

1. On LON-DC1, in Server Manager, click **Local Server**.
2. In the local server's Properties pane, next to **Ethernet**, click **172.16.0.10, IPv6 enabled**.
3. In the **Network Connections** dialog box, right-click **Ethernet**, and then click **Properties**.
4. Click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
5. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Use the following IPv6 address**.
6. In the **IPv6 address** box, type **FD00:AAAA:BBBB:CCCC::A**.
7. In the **Subnet prefix length** box, type **64**.
8. In the **Preferred DNS server** box, type **::1**, and then click **OK**.
9. In the **Ethernet Properties** dialog box, click **Close**.
10. Close the **Network Connections** dialog box.

8: Implementing IPv6

Configure IPv6 on LON-SVR1

1. On LON-SVR1, in Server Manager, click **Local Server**.
2. In the local server's Properties pane, next to **Ethernet**, click **172.16.0.11, IPv6 enabled**.
3. In the **Network Connections** dialog box, right-click **Ethernet**, and then click **Properties**.
4. In the **Ethernet Properties** dialog box, click **Internet Protocol Version 6 (TCP/IPv6)**, and then click **Properties**.
5. In the **Internet Protocol Version 6 (TCP/IPv6) Properties** dialog box, click **Use the following IPv6 address**.
6. In the **IPv6 address** box, type **FD00:AAAA:BBBB:CCCC::15**.
7. In the **Subnet prefix length** box, type **64**.
8. In the **Preferred DNS server** box, type **FD00:AAAA:BBBB:CCCC::A**, and then click **OK**.
9. In the **Ethernet Properties** dialog box, click **Close**.
10. Close the **Network Connections** dialog box.

Verify that IPv6 communication is functional

1. On LON-SVR1, on the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type **ipconfig**, and then press Enter.
Notice that both the link-local IPv6 address and the IPv6 address that you have configured are displayed.
3. At a command prompt, type **ping -6 lon-dc1**, and then press Enter.
Verify that you receive four replies from **LON-DC1** IPv6 address.
4. Type **ping -4 lon-dc1**, and then press Enter.
Verify that you receive four replies from **LON-DC1** IPv4 address.
5. Type **Test-NetConnection FD00:AAAA:BBBB:CCCC::A**, and then press Enter.
Verify that you receive **Ping Succeeded: True** from **LON-DC1** IPv6 address.

Leave the virtual machines running after you complete the demonstration.

8: Implementing IPv6

Demonstration: Configuring DNS to Support IPv6

In this demonstration, you will see how to:

- Configure an IPv6 host (AAAA) resource record for an IPv6 address
- Verify name resolution for an IPv6 host (AAAA) resource record

Preparation Steps

You must have completed the previous demonstration in this module before you begin this demonstration. You need the 20410D-LON-DC1 and 20410D-LON-SVR1 virtual machines to complete this demonstration. They should be running after the previous demonstration.

Demonstration Steps

Configure an IPv6 host (AAAA) resource record

1. On LON-DC1, in Server Manager, click **Tools**, and then click **DNS**.
2. In DNS Manager, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Read the records listed for the zone, and notice that LON-DC1 and LON-SVR1 have registered their IPv6 addresses dynamically with the DNS server.
4. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
5. In the New Host window, in the **Name** box, type **WebApp**.
6. In the **IP address** box, type **FD00:AAAA:BBBB:CCCC::A**, and then click **Add Host**.
7. Click **OK** to clear the success message.
8. Click **Done** to close the New Host window.

Verify name resolution for an IPv6 host (AAAA) resource record

1. On LON-SVR1, if necessary, open a Windows PowerShell prompt.
2. At the Windows PowerShell prompt, type **ping WebApp.adatum.com**, and then press Enter.
Verify that you receive four replies from **WebApp.adatum.com** IPv6 address.
3. Type **Test-NetConnection WebApp.Adatum.com**, and then press Enter.
Verify that you receive **Ping Succeeded: True** from **WebApp.Adatum.com** IPv6 address.

After you complete the demonstration, revert all virtual machines.

9: Implementing Local Storage

Demonstration: Creating Mount Points and Links

In this demonstration, you will see how to:

- Create a mount point
- Create a directory junction for a folder
- Create a hard link for a file



Preparation Steps

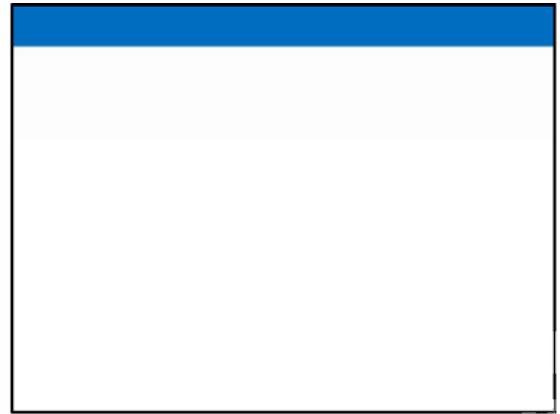
If necessary, start 20410D-LON-DC1 and 20410D-LON-SVR1.

Demonstration Steps

Create a mount point

1. Sign in to **LON-SVR1** with the username **Adatum\Administrator** and the password **Pa\$\$w0rd**.
2. In Server Manager, click the **Tools** menu, and then click **Computer Management**.
3. In the Computer Management console, under the Storage node, click **Disk Management**.
4. In the Disks pane, right-click **Disk2**, and then click **Online**.
5. Right-click **Disk2**, and then click **Initialize Disk**.
6. In the **Initialize Disk** dialog box, select the **Disk2** check box, click **GPT (GUID Partition Table)**, and then click **OK**.
7. In the Computer Management console, in Disk Management, right-click the black box to the right of Disk2, and then click **New Simple Volume**.
8. In the New Simple Volume Wizard, on the **Welcome to the New Simple Volume Wizard** page, click **Next**.
9. On the **Specify Volume Size** page, in the **Simple volume size in MB** field, type **4000**, and then click **Next**.
10. On **Assign Drive Letter or Path** page, click **Do not assign a drive letter or drive path**, and then click **Next**.
11. On the **Format Partition** page, from the **File system** drop-down list, click **NTFS**, in the **Volume label** text box, type **MountPoint**, and then click **Next**.
12. On the **Completing the New Simple Volume Wizard** page, click **Finish**.
13. Wait until the volume is created, right-click **MountPoint**, and then click **Change Drive Letter and Paths**.

9: Implementing Local Storage



14. In the **Change Drive Letter and Paths for MountPoint** dialog box, click **Add**.
15. On the **Assign Drive Letter or Path** page, click **Mount in the following empty NTFS folder**, and then click **Browse**.
16. In the **Browse for Drive Path** window, make sure that **C:** is selected, and then click **New Folder**.
17. In the **Browse for Drive Path** box, type **MountPointFolder**, and then click **OK**.
18. In the **Add drive Letter or Path** window, click **OK**.
19. On the taskbar, click the File Explorer icon, and then double-click **Local Disk (C:)**. You should see the **MountPoint** folder with a size of **4,095,996 KB** assigned to it. Point out the icon assigned to the mount point.

Create a directory junction for a folder

1. Right-click the **Start** button, and then click **Command Prompt**.
2. In the Command Prompt window, at the command prompt, type **cd **, and then press Enter.
3. Type **md CustomApp**, and then press Enter.
4. Type **copy C:\windows\system32\notepad.exe C:\CustomApp**, and then press Enter.
5. Type **mklink /j AppLink CustomApp**, and then press Enter.
6. In the File Explorer window, double-click the **AppLink** folder. Notice that because it is a link, the directory path in the address bar is not updated to **C:\CustomApp**.

Create a hard link for a file

1. At the command prompt, type **mklink /h C:\AppLink\Notepad2.exe C:\AppLink\Notepad.exe**, and then press Enter.
2. Switch to the File Explorer window, and then read the list of files. Notice that Notepad2.exe appears exactly the same as Notepad.exe. Both file names point to the same file.
3. Close all open Windows.

9: Implementing Local Storage

Demonstration: Managing Virtual Hard Disks

In this demonstration, you will see how to:

- Create a virtual hard disk
- Manage a virtual hard disk

Preparation Steps

If necessary, start 20410D-LON-DC1 and 20410D-LON-SVR1. Sign in to LON-SVR1 with the username **Adatum\Administrator** and the password **Pa\$\$w0rd**.

Demonstration Steps

Create a virtual hard disk

1. On LON-SVR1, if required, start **Server Manager**.
2. Click **Tools**, and then click **Computer Management**.
3. In Computer Management, click **Disk Management**.
4. Wait for the disks to display, right-click **Disk Management**, and then click **Create VHD**.
5. In the **Create and Attach Virtual Hard Disk** dialog box, click **Browse**.
6. Type **DiskF** as the **File name**, and then click **Save**.
7. In the **Create and Attach Virtual Hard Disk** dialog box, type **10** as the **Virtual hard disk size**.
8. Click **VHDX**, click **Dynamically expanding** and then click **OK**.
9. On the taskbar, click **File Explorer**.
10. Browse to **Documents**, and then verify that a .vhdx file named DiskF.vhdx was created.

Manage a virtual hard disk

1. In Disk Management, right-click **Disk 9**, click **Initialize disk**, and then click **OK**.
2. Right-click the unallocated space on Disk 9, and then click **New Simple Volume**.
3. On the **Welcome to the New Simple Volume Wizard** page, click **Next**.
4. On the **Specify Volume Size** page, click **Next**.
5. On the **Assign Drive Letter or Path** page, click **Next**.
6. On the **Format Partition** page, type **Data** as the **Volume label**, click **Next**, and then click **Finish**.
If the **Microsoft Windows** dialog box appears, click **Cancel**.
7. In File Manager, verify that the **Data (F:)** drive is listed.
8. Close all open windows.

9: Implementing Local Storage

Demonstration: Configuring Storage Spaces

In this demonstration, you will see how to:

- Create a storage pool
- Create a virtual disk and a volume

Preparation Steps

If necessary, start 20410D-LON-DC1 and 20410D-LON-SVR1.

Demonstration Steps

Create a storage pool

1. On LON-SVR1, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, in the left pane, click **File and Storage Services**, and in the Servers pane, click **Storage Pools**.
3. In the STORAGE POOLS pane, click **TASKS** and then in the **TASKS** drop-down list, click **New Storage Pool**.
4. In the New Storage Pool Wizard, on the **Before you begin** page, click **Next**.
5. On the **Specify a storage pool name and subsystem** page, in the **Name** box, type **StoragePool1**, and then click **Next**.
6. On the **Select physical disks for the storage pool** page, click all available physical disks, and then click **Next**.
7. On the **Confirm selections** page, click **Create**.
8. On the **View results** page, wait until task completes, and then click **Close**.

Create a virtual disk and a volume

1. Under Storage Pools, click **StoragePool1**.
2. In the VIRTUAL DISKS pane, click **TASKS**, and then in the **TASKS** drop-down list, click **New Virtual Disk**.
3. In the New Virtual Disk Wizard, on the **Before you begin** page, click **Next**.
4. On the **Select the storage pool** page, click **StoragePool1**, and then click **Next**.
5. On the **Specify the virtual disk name** page, in the **Name** box, type **Simple vDisk**, and then click **Next**.

9: Implementing Local Storage

6. On the **Select the storage layout** page, in the **Layout** list, select **Simple**, and then click **Next**.
7. On the **Specify the provisioning type** page, click **Thin**, and then click **Next**. You should mention that this configures thin provisioning for that volume.
8. On the **Specify the size of the virtual disk** page in the **Virtual disk size** box, type **2**, and then click **Next**.
9. On the **Confirm selections** page, click **Create**.
10. On the **View results** page, wait until the task completes. Make sure that the **Create a volume when this wizard closes** check box is selected, and then click **Close**.
11. In the New Volume Wizard, on the **Before you begin** page, click **Next**.
12. On the **Select the server and disk** page, under **Disk**, click **Simple vDisk** virtual disk, and then click **Next**.
13. On the **Specify the size of the volume** page, click **Next** to confirm the default selection.
14. On the **Assign to a drive letter or folder** page, click **Next** to confirm the default selection.
15. On the **Select file system settings** page, in the **File system** drop-down list, select **ReFS**, in the **Volume label** box, type **Simple Volume**, and then click **Next**.
16. On the **Confirm selections** page, click **Create**.
17. On the **Completion** page, wait until the task completes, and then click **Close**.

10: Implementing File and Print Services

Demonstration: Creating and Configuring a Shared Folder

In this demonstration, you will see how to:

- Create a shared folder
- Assign permissions for the shared folder
- Configure access-based enumeration
- Configure offline files

Preparation Steps

You need the virtual machines 20410D-LON-DC1 and 20410D-LON-SVR1 for this demonstration; start them now.

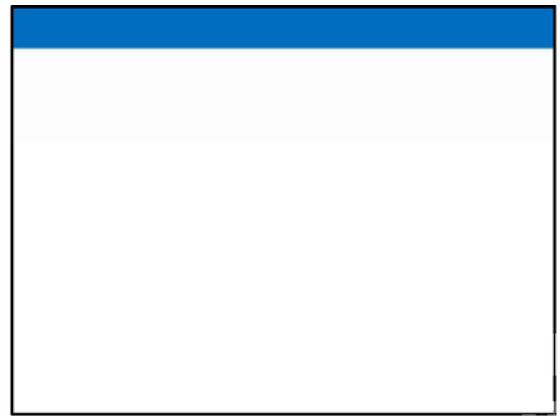
Demonstration Steps

Create a shared folder

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On the taskbar, click the **File Explorer** icon.
3. In File Explorer, in the navigation pane, expand **This PC**, and then click **Allfiles (E:)**.
4. On the menu toolbar, click **Home**, click **New folder**, type **Data**, and then press Enter.
5. Right-click the **Data** folder, and then click **Properties**.
6. In the **Data Properties** dialog box, click the **Sharing** tab, and then click **Advanced Sharing**.
7. In the **Advanced Sharing** dialog box, select **Share this folder**, and then click **Permissions**.

Assign permissions for the shared folder

1. In the **Permissions for Data** dialog box, click **Add**.
2. Type **Authenticated Users**, click **Check names**, and then click **OK**.
3. In the **Permissions for Data** dialog box, click **Authenticated Users**, and then under **Allow**, select **Change** permission.
4. Click **OK** to close the **Permissions for Data** dialog box.
5. Click **OK** to close the **Advanced Sharing** dialog box.
6. Click **Close** to close the **Data Properties** dialog box.

**Configure access-based enumeration**

1. On the taskbar, click the **Server Manager** icon.
2. In Server Manager, in the navigation pane, click **File and Storage Services**.
3. On the **File and Storage Services** page, in the navigation pane, click **Shares**. You may need to refresh the view to see the Shares.
4. In the Shares pane, right-click **Data**, and then click **Properties**.
5. In the **Data Properties** dialog box, click **Settings**, and then select **Enable access-based enumeration**.
6. Click **OK** to close the **Data Properties** dialog box.
7. Close Server Manager.

Configure Offline Files

1. In File Explorer, navigate to drive **E**, right-click the **Data** folder, and then click **Properties**.
2. In the **Data Properties** dialog box, click the **Sharing** tab, click **Advanced Sharing**, and then click **Caching**.
3. In the **Offline Settings** dialog box, select **No files or programs from the shared folder are available offline**, and then click **OK**.
4. Click **OK** to close the **Advanced Sharing** dialog box.
5. Click **Close** to close the **Data Properties** dialog box.

Leave all virtual machines in their current state for subsequent demonstrations.

10: Implementing File and Print Services

Demonstration: Restoring Data from a Shadow Copy

In this demonstration, you will see how to:

- Configure shadow copies
- Create a new file
- Create a shadow copy
- Modify the file
- Restore the previous version

Preparation Steps

You need the 20410D-LON-SVR1 and 20410D-LON-DC1 virtual machines to complete this demonstration. They should be running after the previous demonstration.

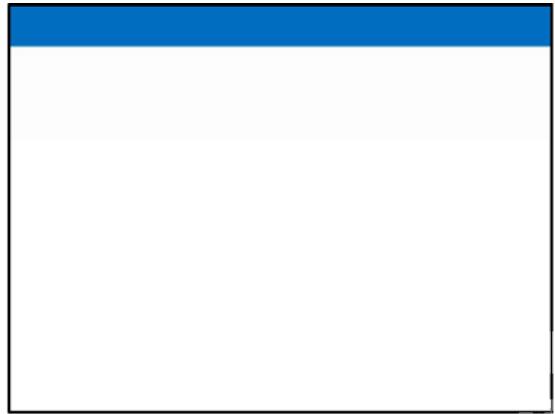
Demonstration Steps

Configure shadow copies

1. On LON-SVR1, on the taskbar, click the **File Explorer** icon.
2. In File Explorer, right-click **Local Disk (C:)**, and then click **Configure Shadow Copies**.
3. In the **Shadow Copies** dialog box, click **C:**, and then click **Enable**.
4. In the **Enable Shadow Copies** dialog box, click **Yes**.
5. Click **OK**.

Create a new file

1. In File Explorer, browse to drive C, and then click the **New folder** icon on the Quick Launch toolbar.
2. Name the new folder **Data**, and then press Enter.
3. Browse to the **Data** folder on drive C.
4. In the Data folder, right-click an empty space, point to **New**, and then click **Text Document**.
5. Name the new text document **TestFile**, and then press Enter.
6. Double-click **TestFile.txt** to open the document.
7. In Notepad, type **Version 1**.
8. Close Notepad, and then click **Save** to save the changes.



Create a shadow copy

1. In File Explorer, right-click **Local Disk (C:)**, and then click **Configure Shadow Copies**.
2. In the **Shadow Copies** dialog box, click **Create Now**.
3. When the shadow copy is complete, click **OK**.

Modify the file

1. In File Explorer, double-click **TestFile.txt**.
2. In Notepad, type **Version 2**.
3. Close Notepad, and then click **Save** to save the changes.

Restore the previous version

1. In File Explorer, in the Data folder, right-click **TestFile.txt**, and then click **Restore previous versions**.
2. In the **TestFile.txt Properties** dialog box, on the **Previous Versions** tab, click the most recent file version, and then click **Restore**.
3. In the **Are you sure you want to restore** message, click **Restore**.
4. Click **OK** to close the success message.
5. Click **OK** to close the **TestFile.txt Properties** dialog box.
6. Double-click **TestFile.txt** to open the document, and then verify that the previous version is restored.
7. Close all open windows.

Leave all virtual machines in their current state for subsequent demonstrations.

10: Implementing File and Print Services

In this demonstration, you will see how to:

- Install the Work Folders role service
- Create a sync share for work folders on a file server
- Configure Work Folder access on a Windows 8.1 client
- Create a file in the work folder
- Configure Work Folders to sync data on a second Windows 8.1 client

Explain that for the purposes of this demonstration, a registry entry was added to allow unsecured connections to work folders. Under normal circumstances, you are required to use Secure Sockets Layer (SSL) certificates to secure the connections between the client devices and the sync share.

Preparation Steps

You need the 20410D-LON-SVR1 and 20410D-LON-DC1 virtual machines to complete this demonstration. They should be running after the previous demonstration.

Start both the 20410D-LON-CL1 and the 20410D-LON-CL2 virtual machines.

Demonstration Steps

Install the Work Folders role service

1. On LON-SVR1, in Server Manager click **Add roles and features**.
2. In the Add Roles and Features Wizard, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, expand **File and Storage Services (2 of 12 installed)**, and then expand **File and iSCSI Services (1 of 11 installed)**.
6. Select **Work Folders**, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When the installation completes, click **Close**.

Create a sync share on a file server

1. In Server Manager, click **File and Storage Services**, and then click **Work Folders**.
2. In the details pane, click the **Tasks** drop-down arrow, and then click **New Sync Share**.
3. In the New Sync Share Wizard, click **Next**.

10: Implementing File and Print Services

4. On the **Select the server and path** page, ensure that **LON-SVR1** is selected, click **Select by file share**, and then click **Next**.

This procedure uses the shared folder Data which was created in the demonstration "Creating and Configuring a Shared Folder".
5. On the **Specify the structure for user folders** page, click **Next**.
6. On the **Enter the sync share name** page, type **WorkFolders**, and then click **Next**.
7. On the **Grant sync access to groups** page click **Add**.
8. In the **Select User or Group** dialog box, type **Domain Users**, click **OK**, and then click **Next**.
9. On the **Specify device policies** page click **Next**.
10. On the **Confirm selections** page, click **Create**, and then click **Close** when complete.

Configure Work Folder access on a Windows 8.1 client

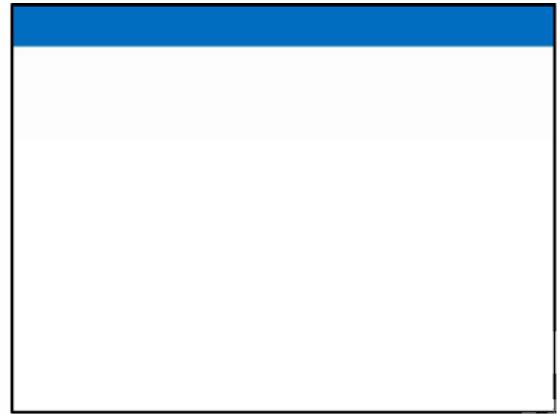
1. Sign in to **LON-CL1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On the **Start** screen, click **Desktop**.
3. On the taskbar, click the **File Explorer** icon.
4. Navigate to **C:\Labfiles\Mod10**, and then double-click **WorkFolders.bat**.

This batch file adds a registry entry that allows unsecured connections to work folders.
5. Close File Explorer.
6. In the lower-left corner of the screen, right-click **Start**, and then click **Control Panel**.
7. Click **System and Security**, and then click **Work Folders**.
8. In the **Work Folders** dialog box, click **Set up Work Folders**, and then click **Enter a Work Folders URL instead**.
9. On the **Enter a Work Folders URL** page, type **http://lon-svr1.adatum.com**, and then click **Next**.

Normally this requires a secure connection.

(More notes on the next slide)

10: Implementing File and Print Services



10. On the **Introducing Work Folders** page, click **Next**.
11. On the **Security policies** page, select the check box to accept the policies, and then click **Set up Work Folders**.
12. Close the **Work Folders** dialog box, and then on the taskbar, click the **File Explorer** icon.

Notice there is now a **Work Folders** folder under the **This PC** folder.

Create a file in the work folder

1. Double-click the **Work Folders** icon to open the folder.
2. Right-click a blank space in the details, click **New>Text Document**, and then press Enter.

Synchronize data on a second client computer

1. Sign in to **LON-CL2** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On the Start screen, click **Desktop**.
3. Right-click the **Start** charm, and then click **Network Connections**.
4. Right-click the **Ethernet 2** adapter, and then click **Enable**.
5. Close Network Connections.
6. Repeat steps 4 through 12 from the **Configure Work Folder access on a Windows 8.1 client** task.
7. Open the **Work Folders** folder, and then notice the file that you created is available from this computer.
8. Close all open windows.
9. On the host computer, open **Hyper-V manager**, and then locate 20410D-LON-CL2. Right-click the virtual machine, and then click **Revert**.

Leave all virtual machines in their current state for subsequent demonstrations.

10: Implementing File and Print Services

Demonstration: Creating Multiple Configurations for a Print Device

In this demonstration, you will see how to:

- Create a shared printer
- Create a second shared printer using the same port
- Increase printing priority for a high priority print queue

Preparation Steps

You need the 20410D-LON-SVR1 and 20410D-LON-DC1 virtual machines to complete this demonstration. They should be running after the previous demonstration.

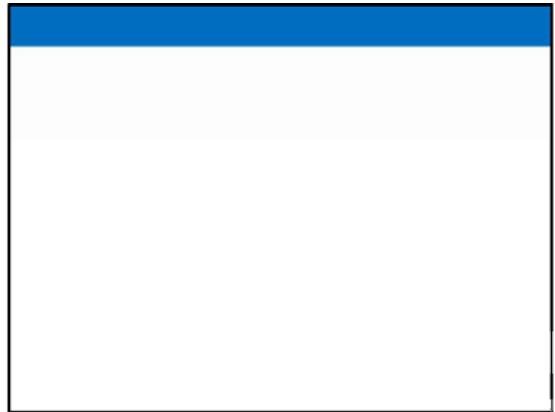
Demonstration Steps

Create a shared printer

1. On LON-SVR1, in the lower-left corner of the screen, click the **Start** button
2. In the **Start** box, type **Devices**, and then click **Devices and Printers**.
3. In the Devices and Printers window, click **Add a printer**.
4. In the Add Printer Wizard, on the **Select a Printer** page, click **The printer that I want isn't listed**.
5. Click **Add a local printer or network printer with manual settings**, and then click **Next**.
Other connections options are also available in this dialog box.
6. Click **Use an existing port**, ensure that **LPT1: (Printer Port)** is selected, and then click **Next**.
You can create other ports here manually, including TCP/IP, for network-connected printers.
7. Leave the driver choice as the default, and then click **Next**.
8. Change the printer name to **AllUsers**, and then click **Next** to finish the printer installation.
9. On the **Printer Sharing** page, ensure that the printer is shared, and then click **Next**.
10. Click **Finish** to close the Add Printer Wizard.

Create a second shared printer on the same port

1. In the Devices and Printers window, click **Add a printer**.
2. In the Add Printer Wizard, on the **Select a Printer** page, click **The printer that I want isn't listed**.



3. Click **Add a local printer or network printer with manual settings**, and then click **Next**.

4. On the **Choose a printer port** page, click **Next**.

This is the same port that you selected for the printer you created in the previous task.

5. On the **Install the printer driver** page, click **Next** to accept the default selection.

This is the same printer driver that you used for the printer you created in the previous task.

6. On the **Which version of the driver do you want to use** page, click **Next** to reuse the same printer driver.

7. On the **Type a printer name** page, in **Printer name**, type **Executives**, and then click **Next**.

8. On the **Printer Sharing** page, click **Next** to share the printer with the default settings.

9. On the **You've successfully added Executives** page, click **Finish**.

10. In the Devices and Printers window, review the list of devices.

Notice that only the Executives printer displays.

Increase printing priority for a high priority print queue

1. In the Devices and Printers window, right-click **Executives**, point to **Printer properties**, and then click **Executives**.

2. On the **Advanced tab**, in **Priority**, type **10**, and then click **OK**.

Now jobs that are submitted to the Executives printer have higher priority than those submitted to the AllUsers printer, and will be printed first.

After you complete the demonstration, revert all virtual machines.

11: Implementing Group Policy

Demonstration: Creating and Managing GPOs

In this demonstration, you will see how to:

- Create a GPO by using the GPMC
- Edit a GPO in the Group Policy Management Editor window
- Use Windows PowerShell to create a GPO

For a complete list of Group Policy cmdlets in Windows PowerShell, refer to “Group Policy Cmdlets in Windows PowerShell” at <http://go.microsoft.com/fwlink/?LinkId=266752>.

Preparation Steps

Start the 20410D-LON-DC1 virtual machine.

Demonstration Steps

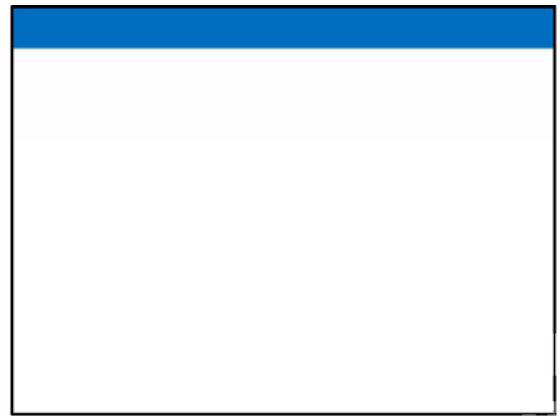
Create a GPO by using the GPMC

1. Sign in to **LON-DC1** as **Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. In the Group Policy Management Console (GPMC), expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click the **Group Policy Objects** folder, and then click **New**.
4. In the **New GPO** dialog box, in the **Name** field, type **Prohibit Windows Messenger**, and then click **OK**.

Edit a GPO in the Group Policy Management Editor window

1. Click the **Group Policy Objects** node, right-click the **Prohibit Windows Messenger** GPO, and then click **Edit**.
2. In the Group Policy Management Editor window, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, and then click **Windows Messenger**.
3. In the details pane, double-click the **Do not allow Windows Messenger to be run** setting.
4. Click **Enabled**, and then click **OK**.
5. Close the **Group Policy Management Editor** window.
6. Right-click the **Adatum.com** domain, and then click **Link an Existing GPO**.
7. In the **Select GPO** dialog box, click **Prohibit Windows Messenger**, and then click **OK**.
8. Minimize the GPMC.

11: Implementing Group Policy



Use Windows PowerShell® to create a GPO named Desktop Lockdown

1. On the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell prompt, type the following, and then press Enter:
New-GPO -Name "Desktop Lockdown"
3. Close Windows PowerShell.
4. Restore the GPMC from the taskbar.
5. Right-click the **Group Policy Objects** folder, and then click **Refresh** to refresh the view. You should see the new Desktop Lockdown GPO.
6. Minimize the GPMC.

Leave the virtual machine running for the next demonstration.

11: Implementing Group Policy

Demonstration: Using Group Policy Diagnostic Tools

In this demonstration, you will see how to:

- Use Gpupdate to refresh Group Policy
- Use the Gpresult command to output the results to an HTML file
- Use the Group Policy Modeling Wizard to test the policy

Stress that Resultant Set of Policy (RSoP) is the best troubleshooting tool for GPO issues. Students can use it to see what policies are delivering what settings to the user or computer.

Point out that in this demonstration, the Group Policy Modeling Wizard generates very little information because of the lack of policies and settings in place currently. The point of the exercise is to demonstrate the possibilities of the wizard itself, and not the contents of report that it generates.

Preparation Steps

Ensure that 20410D-LON-DC1 is running from the last demonstration.

Demonstration Steps

Use Gpupdate to refresh Group Policy

1. On LON-DC1, on the taskbar, click the **Windows PowerShell** icon.
2. In Windows PowerShell, at the command prompt, type the following, and then press Enter:

Gpupdate

Use the Gpresult cmdlet to output the results to an HTML file

1. At the Windows PowerShell command prompt, type the following, and then press Enter:

Gpresult /H c:\Gpresult.html

2. On the taskbar, click the **File Explorer** icon.
3. In the File Explorer window, expand **Computer**, and then click **Local Disk (C:)**.
4. Double-click the **Gpresult.html** file and review the results.
5. In the Gpresult.html file, scroll down to the User Details section, note that the "Do not allow Windows Messenger to be run" setting is Enabled, and then note that Winning GPO is the Prohibit Windows Messenger GPO.
6. Close the report.
7. Close File Explorer, and then close Windows PowerShell.

11: Implementing Group Policy

Use the Group Policy Modeling Wizard to test the policy

1. From the taskbar, restore the GPMC.
2. Right-click **Group Policy Modeling**, and then click **Group Policy Modeling Wizard**.
3. In the Group Policy Modeling Wizard, on the **Welcome** page, click **Next**.
4. On the **Domain Controller Selection** page, click **Next**.
5. On the **User and Computer Selection** page, in the User information section, click **Browse**.
6. Expand **Adatum**, click the **Managers** OU, click **OK**, and then click **Next**.
7. On the **Advanced Simulation Options** page, click **Next**.
8. On the **User Security Groups** page, click **Next**.
9. On the **WMI Filters for Users** page, click **Next**.
10. On the **Summary of Selections** page, click **Next**, and then click **Finish**.
11. Click the **Details** tab of the report, and then point out some of the results.

12: Securing Windows Servers by Using Group Policy Objects

Demonstration: Creating AppLocker Rules

In this demonstration, you will see how to:

- Create a GPO to enforce the default AppLocker Executable rules
- Apply the GPO to the domain
- Test the AppLocker rule

Preparation Steps

For this demonstration you need the virtual machines 20410D-LON-DC1 and 20410D-LON-CL1. They should be running after the previous lab.

Demonstration Steps

Create a GPO to enforce the default AppLocker Executable rules

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In GPMC, go to **Forest: Adatum.com\Domains\Adatum.com**.
3. Click **Group Policy Objects**, right-click **Group Policy Objects**, and then click **New**.
4. In the New GPO window, in **Name**, type **WordPad Restriction Policy**, and then click **OK**.
5. Right-click **WordPad Restriction Policy**, and then click **Edit**.
6. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings\Application Control Policies\AppLocker**.
7. Click **Executable Rules**, right-click **Executable Rules**, and then select **Create New Rule**.
8. On the **Before You Begin** page, click **Next**.
9. On the **Permissions** page, click **Deny**, and then click **Next**.
10. On the **Conditions** page, click **Publisher**, and then click **Next**.
11. On the **Publisher** page, click **Browse**, and then click **Computer**.
12. On the **Open** page, double-click **Local Disk (C:)**.
13. On the **Open** page, double-click **Program Files**, double-click **Windows NT**, double-click **Accessories**, click **wordpad.exe**, and then click **Open**.
14. Move the slider up to the **File name** position, and then click **Next**.
15. Click **Next** again, and then click **Create**.

12: Securing Windows Servers by Using Group Policy Objects

16. If prompted to create default rules, click **Yes**.
17. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings**.
18. Expand **Application Control Policies**, right-click **AppLocker**, and then select **Properties**.
19. On the **Enforcement** tab, under Executable rules, select the **Configured** check box, click **Enforce rules**, and then click **OK**.
20. In the Group Policy Management Editor window, go to **Computer Configuration\Policies\Windows Settings\Security Settings**.
21. Click **System Services**, and then double-click **Application Identity**.
22. In the **Application Identity Properties** dialog box, above **Select service startup mode**, click **Define this policy setting**, then click **Automatic**, and then click **OK**.
23. Close the Group Policy Management Editor window.

Apply the GPO to the domain

1. In the Group Policy Management Console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then expand **Group Policy Objects**.
2. In the Group Policy Management Console, right-click **Adatum.com**, and then click **Link an Existing GPO**.
3. In the Select GPO window, in the Group Policy Objects window, click **WordPad Restriction Policy**, and then click **OK**.
4. Close the Group Policy Management Console.
5. Switch to the **Start** screen, type **cmd**, and then press Enter.
6. In the Command Prompt window, type **gpupdate /force**, and then press Enter.
Wait for the policy to update.

12: Securing Windows Servers by Using Group Policy Objects

Test the AppLocker rule

1. Sign in to LON-CL1 as **Adatum\Alan** with the password **Pa\$\$w0rd**.
2. Point to the lower-right corner of the screen, and then click the **Search** charm when it appears.
3. In the **Search** box type **cmd**, and then press Enter.
4. In the Command Prompt window, type **gpupdate /force**, and then press Enter.
Wait for the policy to update.
5. In the lower-left corner of the screen, click the **Start** button.
6. In the **Search** box type **WordPad**, and then press Enter.

Notice that WordPad does not start.

Leave the virtual machines running after you complete the demonstration.

12: Securing Windows Servers by Using Group Policy Objects

Demonstration: Implementing Secured Network Traffic with Windows Firewall

In this demonstration, you will see how to:

- Check to see if ICMP v4 is blocked
- Enable ICMP v4 from LON-CL2 to LON-SVR2
- Create a connection security rule so that traffic is authenticated to the destination host
- Validate ICMP v4 after the connection security rule is in place

Mention the different options that are available when you are securing connections, including:

- Securing connections for all communication
- Securing connections for a single protocol
- Using certificates for authentication
- Using Kerberos for authentication
- Securing traffic to or from specific hosts only, or securing traffic for an entire domain

Also, mention the real-world situations where securing network traffic is valuable. These scenarios include an organization that has a security policy that prohibits communication between development computers and production computers, or a highly secure environment where compliance requires specific secure communications.

Preparation Steps

Start 20410D-LON-CL2, 20410D-LON-SVR2, and 20410D-LON-RTR.

Demonstration Steps

Check to see if ICMP v4 is blocked

1. Sign in to LON-CL2 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-CL2, click the **Desktop** tile, right-click the **Windows Start** menu, and then click **Command Prompt**.
3. At the command prompt, type **ping 10.10.0.11**, and then press Enter.

Notice that the ping times out.

12: Securing Windows Servers by Using Group Policy Objects

Enable ICMP v4 from LON-CL2 to LON-SVR2

1. Sign in to LON-SVR2 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On LON-SVR2, right-click the **Windows Start** menu, and then click **Control Panel**.
3. In Control Panel, click the **View by** drop-down menu, and then click **Small icons**.
4. Click **Windows Firewall**.
5. Click **Advanced settings**.
6. In the left-hand pane, click **Inbound Rules**.
7. In the right-hand pane, click **New Rule**.
8. On the New Inbound Rule Wizard, on the **Rule Type** page, click **Custom**, and then click **Next**.
9. On the **Program** page, click **Next**.
10. On the **Protocol and Ports** page, click the **Protocol type** drop-down menu, click **ICMPv4**, and then click **Next**.
11. In the **Which remote IP addresses does this rule apply to** section, click **These IP addresses**, and then click **Add**.
12. In the IP Address window, type **10.10.0.50** in the **This IP address or subnet** box, click **OK**, and then click **Next**.
13. On the **Action** page, click **Next** to accept the Allow the connection default action.
14. On the **Profile** page, click **Next** to accept the application of the rule for all profiles.
15. On the **Name** page, type **ICMPv4-Allow-From-10.10.0.50**, and then click **Finish**.
16. Switch to LON-CL2.
17. At the command prompt, type **ping 10.10.0.11**, and then press Enter.

Notice that the ping goes through successfully.

12: Securing Windows Servers by Using Group Policy Objects

Create a connection security rule

1. Switch to LON-SVR2.
2. In the Windows Firewall with Advanced Security window, in the left-hand pane, right-click **Connection Security Rules**, and then click **New Rule**.
3. On the **Rule Type** page, click **Next** to accept the default of **Isolation**.
4. On the **Requirements** page, click **Require authentication for inbound connections and request authentication for outbound connections**, and then click **Next**.
5. On the **Authentication Method** page, click **Advanced**, and then click **Customize**.
6. In the **Customize Advanced Authentication Method** dialog box, in the **First authentication** section, click **Add**.
7. In the **Add First Authentication Method** dialog box, click **Preshared key (not recommended)**, type **Pa\$\$w0rd** for the preshared key, and then click **OK**. Click **OK** again to close the dialog box.
8. On the **Authentication Method** page, click **Next**.
9. On the **Profile** page, click **Next**.
10. On the **Name** page, in **Name**, type **Require Inbound Authentication**, and then click **Finish**.
11. Repeat steps 2 through 10 on LON-CL2 before moving to the next demonstration section.

Validate ICMP v4

1. Switch to LON-CL2.
2. At the command prompt, type **ping 10.10.0.11**, and then press Enter.

Notice that the ping goes through successfully.

After you complete the demonstration, revert the virtual machines.

01: Configuring and Troubleshooting Domain Name System

Demonstration: Installing the DNS Server Role

In this demonstration, you will see how to install the DNS server role

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

You require the 20411D-LON-DC1, 20411D-LON-SVR1, and 20411D-LON-CL1 virtual machines. Ensure that you have started 20411D-LON-DC1 and that the sign-in screen appears before starting 20411D-LON-SVR1 and 20411D-LON-CL1.

Demonstration Steps

1. On 20411D-LON-SVR1, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. If necessary, on the taskbar, click **Server Manager**.
3. In Server Manager, in the navigation pane, click **Dashboard**, and then, in the details pane, click **Add roles and features**.
4. In the **Add Roles and Features Wizard** dialog box, click **Next**.
5. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, in the **Roles** list, select the **DNS Server** check box.
8. In the **Add Roles and Features Wizard** dialog box, click **Add Features**.
9. On the **Select server roles** page, click **Next**.
10. On the **Select features** page, click **Next**.
11. On the **DNS Server** page, click **Next**.
12. On the **Confirm installation selections** page, click **Install**.
13. After you have installed the role, click **Close**.

01: Configuring and Troubleshooting Domain Name System

Demonstration: Configuring the DNS Server Role

In this demonstration, you will see how to:

- Configure DNS server properties
- Configure conditional forwarding
- Clear the DNS cache

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

The required virtual machines, 20411D-LON-DC1, 20411D-LON-SVR1, and 20411D-LON-CL1, should be running after the preceding demonstration.

Demonstration Steps

Configure DNS server properties

1. Switch to LON-DC1.
2. If necessary, sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. In Server Manager, click **Tools**, and then click **DNS**.
4. In DNS Manager, expand **LON-DC1**, select and right-click **LON-DC1**, and then click **Properties**.
5. In the **LON-DC1 Properties** dialog box, click the **Forwarders** tab.
6. On the **Forwarders** tab, click **Edit**. You can configure forwarding by typing the forwarding server's IP address. Click **Cancel**.
7. Click the **Advanced** tab. You can configure options including securing the cache against pollution.
8. Click the **Root Hints** tab. You can see the configuration for the root hints servers here.
9. Click the **Debug Logging** tab, and then select the **Log packets for debugging** check box. You can configure debug logging options here.
10. Clear the **Log packets for debugging** check box, and then click the **Event Logging** tab.
11. Click **Errors and Warnings**.
12. Click the **Monitoring** tab. You can perform simple and recursive tests against the server by using the **Monitoring** tab. Select the **A simple query against this DNS server** check box, and then click **Test Now**.
13. Click the **Security** tab. You can define permissions on the DNS infrastructure here. Click **Cancel**.

01: Configuring and Troubleshooting Domain Name System

Configure conditional forwarding

1. In the navigation pane, click **Conditional Forwarders**.
2. Right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
3. In the **New Conditional Forwarder** dialog box, in the **DNS Domain** box, type **contoso.com**.
4. Click the **<Click here to add an IP Address or DNS Name>** box. Type **131.107.1.2**, and then press Enter. Validation will fail because this is an example configuration.
5. Click **OK**.

Clear the DNS cache

- In the navigation pane, right-click **LON-DC1**, and then click **Clear Cache**.

Use Windows PowerShell® to configure the DNS server role

1. On the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell command prompt, type **Get-DnsServer**, and then press Enter.
3. Observe the list of information that returns. You need to scroll up and down to read this information.
4. To see the same information one page at a time, you can pipe the output through the **more** function. Type **Get-DnsServer | more**, and then press Enter. Use the spacebar to advance one screen of text at a time or Enter to advance one line at a time. You can also pipe the output of the **Get-DnsServer** cmdlet to the **Export-Clixml** cmdlet, which generates an XML file of the configuration. You can use the XML file to back up or transfer DNS settings between computers.
5. Type **Get-DnsServer | Export-Clixml –path c:\DNSExport.xml**, and then press Enter.
6. Open File Explorer and the DNSExport.xml file. Point out some of the settings found there. Close the file and File Explorer.
7. Use the Windows PowerShell command-line interface to add a conditional forwarder. Type the following: **Add-DnsServerConditionalForwarderZone –Name Fabrikam.com -MasterServers**

01: Configuring and Troubleshooting Domain Name System

131.107.5.6, and then press Enter.

8. Return to the DNS console. In the navigation pane, click **Conditional Forwarders**.
9. Click the **Refresh** icon on the Tools ribbon. You should see both the **Contoso.com** and **Fabrikam.com** conditional forwarders items. In the console tree, select each item and verify the IP address settings.

01: Configuring and Troubleshooting Domain Name System

Demonstration: Creating Zones

In this demonstration, you will see how to:

- Create a reverse lookup zone
- Create a forward lookup zone

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

The required virtual machines, 20411D-LON-DC1, 20411D-LON-SVR1, and 20411D-LON-CL1, should be running after the preceding demonstration.

Demonstration Steps

Create a reverse lookup zone

1. On LON-DC1, in DNS Manager, in the navigation pane, click **Reverse Lookup Zones**.
2. Right-click **Reverse Lookup Zones**, and then click **New Zone**.
3. In the New Zone Wizard, click **Next**.
4. On the **Zone Type** page, click **Primary zone**, and then click **Next**.
5. On the **Active Directory Zone Replication Scope** page, click **Next**.
6. On the **Reverse Lookup Zone Name** page, click **IPv4 Reverse Lookup Zone**, and then click **Next**.
7. On the second **Reverse Lookup Zone Name** page, in the **Network ID** box, type **172.16.**, and then click **Next**.
8. On the **Dynamic Update** page, click **Next**.
9. On the **Completing the New Zone Wizard** page, click **Finish**.
10. Re-register LON-DC1 into the zone by doing the following:
 - a. Right-click the Windows® Start icon, and then select **Run**.
 - b. In the **Run** dialog box, in the Open text area, type **cmd** and then click **OK**.
 - c. At the command prompt, type **ipconfig /registerdns**, and then press Enter. Close the command prompt window.
 - d. Return to the DNS console, and under the Reverse Lookup Zones, select **16.172.in-**

01: Configuring and Troubleshooting Domain Name System

addr.arpa.

5. On the keyboard, press F5, and then verify that the Pointer (PTR) record for 172.16.0.10 appears.
5. **Create a forward lookup zone**
6. Switch to LON-SVR1.
7. Pause your pointer over the lower-left corner of the display, and then click **Start**.
8. On the Start screen, type **DNS**, and then, from the Search results, click the second **DNS** icon.
9. In DNS Manager, in the navigation pane, expand **LON-SVR1**, and then click **Forward Lookup Zones**.
10. Right-click **Forward Lookup Zones**, and then click **New Zone**.
11. In the New Zone Wizard, click **Next**.
12. On the **Zone Type** page, click **Secondary zone**, and then click **Next**.
13. On the **Zone Name** page, in the **Zone name** box, type **Adatum.com**, and then click **Next**.
14. On the **Master DNS Servers** page, in the **Master Servers** list, type **172.16.0.10**, and then press Enter.
15. Click **Next**, and on the **Completing the New Zone Wizard** page, click **Finish**.
16. **Create a forward lookup zone with Windows PowerShell**
17. Switch to LON-DC1.
18. On the taskbar, click the **Windows PowerShell** icon.
19. In the Windows PowerShell window, type **Add-DnsServerPrimaryZone –Name woodgrovebank.com –DynamicUpdate Secure –ReplicationScope Domain**, and then press Enter.

01: Configuring and Troubleshooting Domain Name System

4. Return to the DNS console. In the console tree, expand **LON-DC1**, and then expand and refresh **Forward Lookup Zones**. You should see the **woodgrovebank.com** zone.
5. Select and right-click the **woodgrovebank.com** zone, and then click **Properties**.
6. On the **General** tab, confirm that Replication is set to All DNS servers in this domain, and that Dynamic Updates are set to Secure only.
7. Click **Cancel** on the **woodgrovebank.com Properties** page.

01: Configuring and Troubleshooting Domain Name System

Demonstration: Configuring DNS Zone Transfers

In this demonstration, you will see how to:

- Enable DNS zone transfers
- Update the secondary zone from the master server
- Update the primary zone, and verify the change on the secondary zone

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

The required virtual machines, 20411D-LON-DC1, 20411D-LON-SVR1, and 20411D-LON-CL1, should be running after the preceding demonstration.

Demonstration Steps

Enable DNS zone transfers

1. Switch to LON-DC1.
2. In DNS Manager, in the navigation pane, expand **Forward Lookup Zones**.
3. Right-click **Adatum.com**, and then click **Properties**.
4. In the **Adatum.com Properties** dialog box, click the **Zone Transfers** tab.
5. Select the **Allow zone transfers** check box, and then click **Only to servers listed on the Name Servers tab**.
6. Click **Notify**, and then, in the **Notify** dialog box, click **Servers listed on the Name Servers tab**. Click **OK**.
7. Click the **Name Servers** tab, and then click **Add**.
8. In the **New Name Server Record** dialog box, in the **Server fully qualified domain name (FQDN)** box, type **LON-SVR1.Adatum.com**, and then click **Resolve**. Continue even if it gets a red X; it will be set after the OK. Click **OK**.
9. In the **Adatum.com Properties** dialog box, click **OK**.

To use Windows PowerShell for the same actions above:

1. Open the Windows PowerShell Administrator console on LON-DC1.
2. Type the following cmdlet, and then press Enter:
 - **Set-DnsServerPrimaryZone -Name "adatum.com" –Notify Notify -SecondaryServers**

01: Configuring and Troubleshooting Domain Name System

"172.16.0.21" –SecureSecondaries TransferToSecureServers

2. **Update the secondary zone from the master server**
3. Switch to LON-SVR1.
4. In DNS Manager, in the navigation pane, expand **Forward Lookup Zones**.
5. Refresh the display, right-click **Adatum.com**, and then click **Transfer from Master**. If successful, you will see the various Adatum.com DNS zone records, similar to the same zone in the DNS console of LON-DC1. You might need to perform this step a number of times before the zone transfers. Also, note that the transfer might occur automatically before you perform these steps manually.
6. **To use Windows PowerShell for the same actions above:**
7. Open the Windows PowerShell Administrator console on LON-SVR1.
8. Type the following cmdlet, and then press Enter:
9. **Add-DnsServerSecondaryZone -Name "Adatum.com" -ZoneFile "Adatum.com.dns" -MasterServers 172.16.0.10**
10. **Note:** The secondary zone "Adatum.com" was already created on LON-SVR1 in the previous demonstration. Attempting to create it in Windows PowerShell without first deleting it will result in a Windows PowerShell error.
11. **Update the primary zone, and then verify the change on the secondary zone**
12. Switch to LON-DC1.
13. In DNS Manager, right-click **Adatum.com**, and then click **New Alias (CNAME)**.
14. In the **New Resource Record** dialog box, in the **Alias name (uses parent domain if left blank)** box, type **intranet**.
15. In the **Fully qualified domain name (FQDN) for target host** box, type **LON-dc1.adatum.com**, and

01: Configuring and Troubleshooting Domain Name System



then click **OK**.

5. Switch to LON-SVR1.
6. In DNS Manager, click **Adatum.com**.
7. Right-click **Adatum.com**, and then click **Transfer from Master**. The record might take some time to appear. You might need to refresh the display.

01: Configuring and Troubleshooting Domain Name System

Demonstration: Managing DNS Records

In this demonstration, you will see how to:

- Configure TTL
- Enable and configure scavenging and aging

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

The required virtual machines, 20411D-LON-DC1, 20411D-LON-SVR1, and 20411D-LON-CL1, should already be running after the preceding demonstration.

Demonstration Steps

Configure TTL

1. Switch to LON-DC1.
2. In DNS Manager, right-click **Adatum.com**, and then click **Properties**.
3. In the **Adatum.com Properties** dialog box, click the **Start of Authority (SOA)** tab.
4. In the **Minimum (default) TTL** box, type **2**, and then click **OK**.

Enable and configure scavenging and aging

1. Right-click **LON-DC1**, and then click **Set Aging/Scavenging for All Zones**.
2. In the **Server Aging/Scavenging Properties** dialog box, select the **Scavenge stale resource records** check box, and then click **OK**.
3. In the **Server Aging/Scavenging Confirmation** dialog box, select the **Apply these settings to the existing Active Directory-integrated zones** check box, and then click **OK**.

To use Windows PowerShell for the same actions above:

1. Open the Windows PowerShell Administrator console on LON-DC1.
2. Type the following cmdlets, and then press Enter after each one:

```
Set-DnsServerScavenging -RefreshInterval 7.00:00:00 -Verbose -PassThru  
Set-DnsServerZoneAging adatum.com -Aging $true -PassThru -Verbose
```

01: Configuring and Troubleshooting Domain Name System

Demonstration: Testing the DNS Server Configuration

In this demonstration, you will see how to use Nslookup.exe to test the DNS server configuration

Revert all virtual machines.

Preparation Steps

The required virtual machines, 20411D-LON-DC1, 20411D-LON-SVR1, and 20411D-LON-CL1, should be running after the preceding demonstration.

Demonstration Steps

1. On LON-DC1, pause your pointer over the lower-left corner of the display, and then click the Windows icon.
2. On the Start screen, type **cmd**, and then press Enter.
3. In the Search results pane, click **Command Prompt**.
4. At the command prompt, type the following command, and then press Enter:

`nslookup -d2 LON-DC1.Adatum.com`

1. Review the information provided by Nslookup.

2: Maintaining Active Directory® Domain Services

Demonstration: Cloning Domain Controllers

- In this demonstration, you will see how to:
 - Prepare a source domain controller that is to be cloned
 - Export the source virtual machine
 - Create and start the cloned domain controller

Demonstrate to the students how to prepare a domain controller that will be a source domain controller for the cloning process, and then create a clone. Explain every step of the demonstration as instructed in the prior topics. After completing this demonstration, delete the LON-DC3 virtual machine, and then revert all virtual machines.

Preparation Steps

Note: If you are using the Online Labs for this instructor demonstration, then you cannot perform the demo as written, because it will not allow the export steps.

For this demonstration, you will use the available virtual machine environment. Before beginning the demonstration, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V® Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
 - User name: **Administrator**
 - Password: **Pa\$\$w0rd**
 - Domain: **Adatum**

Demonstration Steps

Prepare the source domain controller that you want to clone:

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. In Active Directory Administrative Center, double-click **Adatum (local)**, and then, in the details pane, double-click the **Domain Controllers** organizational unit (OU).
3. In the details pane, select **LON-DC1**, and then, in the Tasks panes, under the LON-DC1 section, click **Add to group**.

2: Maintaining Active Directory® Domain Services

4. In the **Select Groups** dialog box, in the **Enter the object names to select** box, type **Cloneable**, and then click **Check Names**.
5. Ensure that the group name is expanded to **Cloneable Domain Controllers**, and then click **OK**.
6. On LON-DC1, in the taskbar, click the **Windows PowerShell** icon.
7. At the Windows PowerShell® command prompt, type the following command, and then press Enter:

`Get-ADCCloningExcludedApplicationList`

8. Verify any critical applications in your production environment. You need to verify each application or use a domain controller that has fewer applications installed by default. For this demonstration, you will accept the risk.
9. At the Windows PowerShell command prompt, type the following command, and then press Enter:

`Get-ADCCloningExcludedApplicationList –GenerateXML`

10. Type the following command at the Windows PowerShell command prompt, and then press Enter to create the DCCloneConfig.xml file:

`New-ADCCloneConfigFile`

11. Type the following command at the Windows PowerShell command prompt, and then press Enter to shut down LON-DC1:

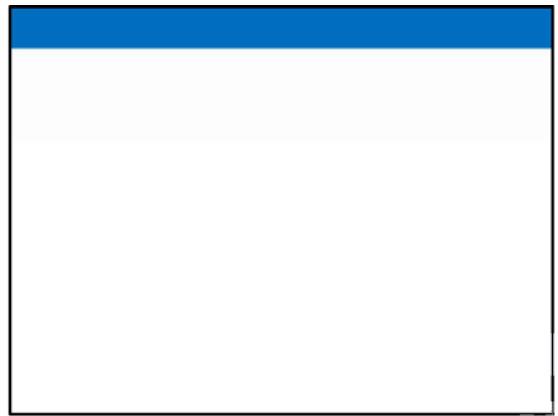
`Stop-Computer`

Export the source virtual machine

1. On the host computer, in Hyper-V Manager, in the details pane, select the **20411C-LON-DC1** virtual machine.
2. In the Actions pane, in the 20411C-LON-DC1 section, click **Export**.
3. In the **Export Virtual Machine** dialog box, select the location **D:\Program Files\Microsoft Learning\20411**, and then click **Export**. Note that the drive letter may be different on your host

(More notes on the next slide)

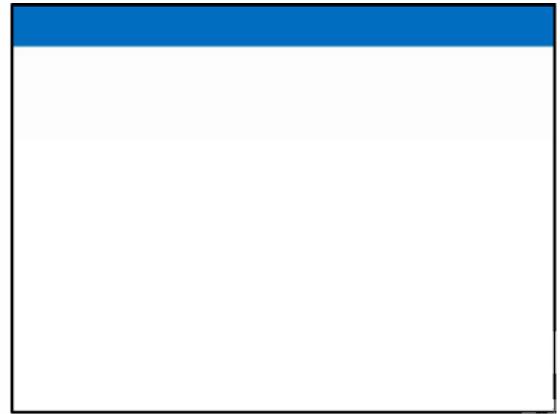
2: Maintaining Active Directory® Domain Services



4. Wait until the export is finished. This process will take approximately five minutes.
5. In the Actions pane, in the **20411-LON-DC1** section, click **Start**.

Create and start the cloned domain controller

1. In Hyper-V Manager, in the Actions pane, click **Import Virtual Machine**.
2. In the Import Virtual Machine Wizard, on the **Before You Begin** page, click **Next**.
3. On the **Locate Folder** page, click **Browse**, select the folder **D:\Program Files\Microsoft Learning\20411\20411C-LON-DC1**, click **Select Folder**, and then click **Next**. Note that the drive letter may be different on your host computer.
4. On the **Select Virtual Machine** page, select **20411C-LON-DC1**, and then click **Next**.
5. On the **Choose Import Type** page, click **Copy the virtual machine (create a new unique ID)**, and then click **Next**.
6. On the **Choose Folders for Virtual Machine Files** page, select the **store the virtual machine in a different location** check box. For each folder location, type the following path: **D:\Program Files\Microsoft Learning\20411**, and then click **Next**. Note that the drive letter may be different on your host computer.
7. On the **Choose Folders to Store Virtual Hard Disks** page, type the path **D:\Program Files\Microsoft Learning\20411**, and then click **Next**. Note that the drive letter may be different on your host computer.
8. On the **Completing Import Wizard** page, click **Finish**. This process will take about five minutes to complete.
9. In the Hyper-V Manager details pane, identify and select the newly imported virtual machine named **20411C-LON-DC1**, which has the State shown as Off, right-click **20411C-LON-DC1**, and then click **Rename**.
10. Type **20411C-LON-DC3** in the **name** box, and then press Enter.



11. In the Actions pane, in the 20411-LON-DC3 section, click **Start**, and then click **Connect**. This will show that the virtual machine is starting.
12. While the server is starting, note the “Domain Controller cloning is at x% completion” message.
13. Note that the cloning will take some time to complete. You may stop the **20411C-LON-DC3** virtual machine at any time.

2: Maintaining Active Directory® Domain Services

Demonstration: Configuring RODC Credential Caching

- In this demonstration, you will see how to:
 - Configure password replication groups
 - Create a group to manage password replication to the remote office RODC
 - Configure a password replication policy for the remote office
 - Evaluate the resulting password replication policy
 - Monitor credential caching

Preparation Steps

For this demonstration, you will use the available virtual machine environment. Before beginning the demonstration, you must complete the following steps:

1. On the host computer, click **Start**, point to **Administrative Tools**, and then click **Hyper-V Manager**.
2. In Hyper-V Manager, click **20411D-LON-DC1**, and, in the Actions pane, click **Start**.
3. In the Actions pane, click **Connect**. Wait until the virtual machine starts.
4. Sign in by using the following credentials:
 - User name: **Administrator**
 - Password: **Pa\$\$w0rd**
 - Domain: **Adatum**
5. Repeat steps 2 through 4 for **20411D-LON-SVR1**.

Demonstration Steps

Verify requirements for installing an RODC

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. In **Active Directory Users and Computers**, in the navigation pane, right-click the **Adatum.com** domain, and then click **Raise domain functional level**.
3. In the Raise domain functional level window, confirm that the **Current domain functional level** is set to **Windows Server 2008 R2**. The minimum level for RODC support is Windows Server 2003. Click **Cancel**.
4. Switch to LON-SVR1.
5. On LON-SVR1, in Server Manager, click **Local Server**, and then click **LON-SVR1** beside **Computer name**.

2: Maintaining Active Directory® Domain Services



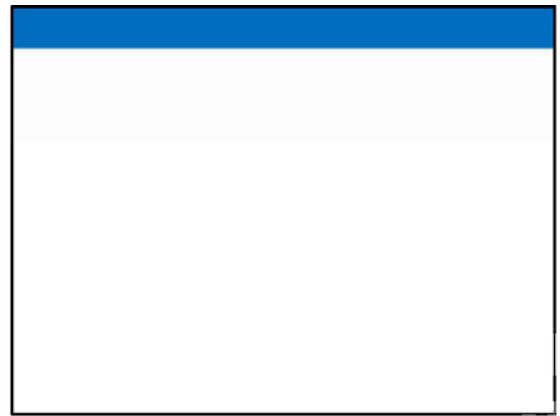
6. In the System Properties window, click **Change**.
7. In the Computer Name/Domain Changes window, click **Workgroup**, type **TEMPORARY** into the **Workgroup** field, and then click **OK**.
8. In the Computer Name/Domain Changes window, click **OK**.
9. Click **OK** twice to confirm the name change and pending server restart.
10. In the System Properties window, click **Close**.
11. In the Microsoft Windows window, click **Restart Now**.
12. Switch to LON-DC1.
13. On LON-DC1, in Active Directory Users and Computers, in the navigation pane, expand **Adatum.com**, and then click **Computers**.
14. Right-click **LON-SVR1**, and then click **Delete**.
15. Click **Yes** twice.
16. In Active Directory Users and Computers, right-click **Domain Controllers**, and then click **Create Read-only Domain Controller account**.
17. In the Active Directory Domain Services Installation Wizard window, click **Next**.
18. Click **Next** to accept the current credentials.
19. In the **Computer name** field, type **LON-SVR1**, and then click **Next**.
20. On the **Select a site** page, click **Next**.
21. On the **Additional Domain Controller Options** page, click **Next**.
22. On the **Delegation of RODC Installation and Administration** page, type **Adatum\IT** in the **Group or user** field, and then click **Next**.
23. On the **Summary** page, click **Next**.
24. Click **Finish** to complete the wizard.

25. Close Active Directory Users and Computers.

Install an RODC

1. Sign in to LON-SVR1 as **Administrator** with the password **Pa\$\$w0rd**.
2. On LON-SVR1, in Server Manager, click **Manage**, and then click **Add Roles and Features**.
3. In the Add Roles and Features Wizard, click **Next**.
4. Ensure that **Role-based or feature-based installation** is selected, and then click **Next**.
5. Select **LON-SVR1**, and then click **Next**.
6. On the **Select server roles** page, select the **Active Directory Domain Services** check box, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. Click **Next**, and then click **Install** to continue the installation.
9. When the installation completes, click **Close**.
10. In Server Manager, click the **Notifications** icon, and then click **Promote this server to a domain controller**.
11. In the Deployment Configuration window, beside Domain, type **adatum.com**, and then click **Select**.
12. In the Windows Security window, type **Adatum\April** for **User name** and **Pa\$\$w0rd** as the password, and then click **OK**.
13. In the Select a domain from the forest window, click **Adatum.com**, and then click **OK**.
14. In the Deployment Configuration window, click **Next**.
15. On the **Domain Controller Options** screen, note the yellow bar that says “A pre-created RODC account...” Close the yellow bar, and under **Type the Directory Services Restore Mode (DSRM) password**, type **Pa\$\$w0rd** in the **Password** and **Confirm password** fields, and then click **Next**.
16. On the **Additional Options** page, beside **Replicate from**, click the drop-down box, click **LON-** (More notes on the next slide)

2: Maintaining Active Directory® Domain Services



DC1.Adatum.com, and then click **Next**.

17. On the **Paths** page, click **Next**.
18. On the **Review Options** page, click **Next**.
19. On the **Prerequisites Check** page, click **Install**.
20. After the Active Directory Domain Services Wizard has completed, LON-SVR1 will restart.

Configure password replication groups

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the Active Directory Users and Computers window, click the **Users** container, double-click **Allowed RODC Password Replication Group**, click the **Members** tab, verify that there is nothing listed, and then Click **OK**.
3. In Active Directory Users and Computers, click the **Domain Controllers** OU, right-click **LON-SVR1**, and then click **Properties**.
4. Click the **Password Replication Policy** tab, confirm that **Allowed RODC Password Replication Group** and **Denied RODC Password Replication Group** are both listed, and then Click **OK**.

Create a group to manage password replication to the remote office RODC

1. On LON-DC1, in Active Directory Users and Computers, right-click the **Research** OU, click **New**, and then click **Group**.
2. In the New Object – Group window, type **Remote Office Users** in the **Group name** field, confirm that **Global** and **Security** are selected, and then click **OK**.
3. In Active Directory Users and Computers, click the **Research** OU, and then double-click the **Remote Office Users** group.
4. In the Remote Office Users Properties window, click the **Members** tab.



5. Click **Add**, type **Aziz; Colin; Lukas; Louise**, and then click **Check Names**.
6. Click **Object Types**, select **Computers**, and then click **OK**.
7. In the **Enter the object names to select** field, type **LON-CL1**, click **Check names**, and then click **OK**.
8. Click **OK** to close the Remote Office Users Properties window.

Configure a Password Replication Policy for the remote office RODC

1. On LON-DC1, in Active Directory Users and Computers, click the **Domain Controllers** OU, right-click **LON-SVR1**, and then click **Properties**.
2. In the LON-SVR1 Properties window, click the **Password Replication Policy** tab, and then click **Add**.
3. In the Add Groups, Users, and Computers window, select **Allow passwords for the account to replicate to this RODC**, and then click **OK**.
4. In the search window, in the **Enter the object names to select** field, type **Remote Office Users**, click **Check Names**, and then click **OK**.
5. In the LON-SVR1 Properties window, click **Apply**, and do not close the window.

Evaluate the resulting Password Replication Policy

1. On LON-DC1, in the LON-SVR1 Properties window, on the **Password Replication Policy** tab, click **Advanced**.
2. Click the **Resultant Policy** tab, click **Add**, type **Aziz**, click **Check Names**, and then click **OK**.
3. Confirm that the Resultant Setting for Aziz is **Allow**.
4. Click **Close**, and then click **OK** to close the **LON-SVR1 Properties** dialog box.

Monitor credential caching

1. Switch to LON-SVR1.

2: Maintaining Active Directory® Domain Services

2. Attempt to sign in as **Adatum\Aziz** with the password **Pa\$\$w0rd**. The sign-in will fail because Aziz does not have permission to sign in to LON-SVR1. However, the credentials for Aziz's account were processed and cached on LON-SVR1.
3. Switch to LON-DC1.
4. In Active Directory Users and Computers, click the **Domain Controllers** OU, double-click **LON-SVR1**, and then click the **Password Replication Policy** tab.
5. On the **Password Replication Policy** tab, click **Advanced**. Notice that Aziz's account's password has been stored on LON-SVR1.

Note: You may need to change the drop down to **Accounts that have been authenticated to this Read only domain controller**. This may be necessary if, due to the sign-in restrictions, the **Aziz** account did not yet store on **LON-SVR1**.

6. Click **Close**, and then click **OK**.

Prepopulate credential caching

1. On LON-DC1, in **Active Directory Users and Computers**, click the **Domain Controllers** OU, double-click **LON-SVR1**, and then click the **Password Replication Policy** tab.
2. On the **Password Replication Policy** tab, click **Advanced**, and then click **Prepopulate Passwords**.
3. Type **Louise; LON-CL1**, click **Check names**, click **OK**, and then click **Yes**.
4. Click **OK**, and confirm that Louise and LON-CL1 have both been added to the list of accounts with cached credentials.
5. Close all open windows.

2: Maintaining Active Directory® Domain Services

Demonstration: Managing AD DS by Using Management Tools

- In this demonstration, you will see how to:
 - Create objects in Active Directory Users and Computers
 - View object attributes in Active Directory Users and Computers
 - Navigate within Active Directory Administrative Center
 - Perform an administrative task in Active Directory Administrative Center
 - Use the Windows PowerShell Viewer in Active Directory Administrative Center
 - Manage AD DS objects with Windows PowerShell

Preparation Steps

You require the 20411D-LON-DC1 virtual machine. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Active Directory Users and Computers

View objects

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. In Active Directory Users and Computers, double-click the **Adatum.com** domain.
3. Double-click the **Computers** container to see the computer objects in the container.
4. Double-click the **Research** OU. Note the User and Group objects within the Research OU.

Refresh the view

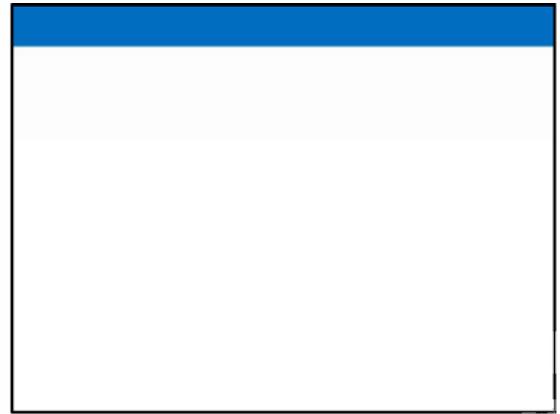
1. Right-click the **Adatum.com** domain, and then click **Refresh**.
2. In the toolbar, click the white and green **Refresh** icon.

Create objects

1. Right-click the **Computers** container, click **New**, and then click **Computer**.
2. In the **Computer name** field, type **LON-CL4**, and then click **OK**.

Configure object attributes

1. In Active Directory Users and Computers, click the **Computers** container.
2. Right-click **LON-CL4**, and then click **Properties**.
3. In the LON-CL4 Properties window, click the **Member Of** tab.
4. On the **Member Of** tab, click **Add**, type **Research**, and then click **OK**.



5. Click **OK** to close the LON-CL4 Properties window.

View all object attributes

1. In Active Directory Users and Computers, in the menu toolbar, click **View**, and then click **Advanced Features**.
2. Click the **Computers** container, right-click **LON-CL4**, and then click **Properties**.
3. Click the **Attribute Editor** tab, and then scroll through the **Attributes** list. Click **Cancel**.

Active Directory Administrative Center

Navigation

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. Click **Adatum (local)**, click **Dynamic Access Control**, and then click **Global Search**.
3. In the navigation pane, click the tab for **Tree View**.
4. Double-click **Adatum (local)** to expand the Adatum.com domain.

Perform administrative tasks

1. In Active Directory Administrative Center, click **Overview**.
2. In the Reset Password section, in the **User name** field, type **Adatum\Adam**.
3. In the **Password** and **Confirm password** fields, type **Pa\$\$w0rd**.
4. Clear the check box for **User must change password at next log on**, and then click **Apply**.
5. In the Global Search section, type **Rex** in the **Search** field, and then press Enter.

Use the Windows PowerShell History Viewer

1. In Active Directory Administrative Center, click the **Windows PowerShell History** toolbar at the bottom of the screen.

2: Maintaining Active Directory® Domain Services

2. View the details for the **Set-ADAccountPassword** cmdlet used to perform the most recent task.
3. On LON-DC1, close all open windows.

Windows PowerShell

Create a group

1. In Server Manager, click **Tools**, and then click **Active Directory Module for Windows PowerShell**.
2. At the Windows PowerShell prompt, type the following, and then press Enter:

```
New-ADGroup –Name "SalesManagers" –GroupCategory Security –GroupScope Global –DisplayName "Sales Managers" –Path "CN=Users,DC=Adatum,DC=com"
```
3. In Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
4. In Active Directory Administrative Center, double-click **Adatum (local)**, and then, in the details pane, scroll down, and double-click the **Users** container.
5. Confirm that the SalesManagers group is present in the Users container. You may need to press F5 on the keyboard to refresh the Users container.

Move an object to a new OU

1. Switch to the Windows PowerShell prompt.
2. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Move-ADObject "CN=SalesManagers,CN=Users,DC=Adatum,DC=com" –TargetPath "OU=Sales,DC=Adatum,DC=com"
```

3. Switch to **Active Directory Administrative Center**.
4. In Active Directory Administrative Center, double-click **Adatum (local)**, and then, in the details pane, scroll down and double-click the **Sales** OU.

Confirm that the **SalesManagers** group has been moved to the **Sales** OU.

2: Maintaining Active Directory® Domain Services

Demonstration: Performing AD DS Database Maintenance

In this demonstration, you will see how to:

- Stop AD DS
- Perform offline defragmentation of the AD DS database
- Check the integrity of the AD DS database
- Start AD DS

Preparation Steps

You require the 20411D-LON-DC1 virtual machine. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Stop AD DS

1. On LON-DC1, if necessary, on the taskbar, click the **Server Manager** shortcut.
2. In Server Manager, click **Tools**, and then click **Services**.
3. In the Services window, right-click **Active Directory Domain Services**, and then click **Stop**.
4. In the **Stop Other Services** dialog box, click **Yes**.

Perform an offline defragmentation of the AD DS database

1. On LON-DC1, on the taskbar, click the **Windows PowerShell** shortcut.
2. In the command window, type **ntdsutil**, and then press Enter.
3. At the **ntdsutil.exe:** prompt, type the following command, and then press Enter:

activate instance NTDS

4. At the **ntdsutil.exe:** prompt, type the following command, and then press Enter:

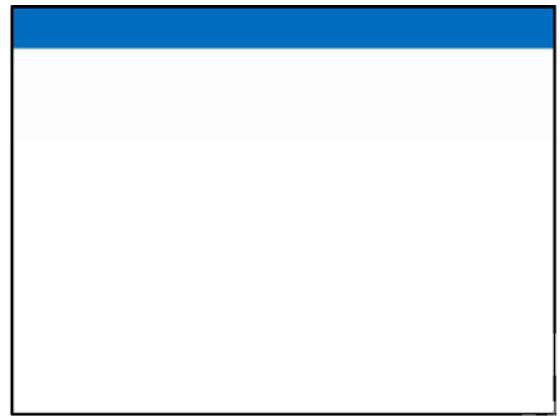
files

5. At the **file maintenance:** prompt, type the following command, and then press Enter:

compact to C:\

Check the integrity of the offline database

1. At the **file maintenance:** prompt, type the following command, and then press Enter:



Integrity

2. At the **file maintenance:** prompt, type the following command, and then press Enter:

quit

3. At the **ntdsutil.exe:** prompt, type the following command, and then press Enter:

Quit

4. Close the Windows PowerShell window.

Start AD DS

1. On the taskbar, click the **Server Manager** shortcut.
2. In Server Manager, click **Tools**, and then click **Services**.
3. In the Services window, right-click **Active Directory Domain Services**, and then click **Start**.
4. Confirm that the **Status** column for **Active Directory Domain Services** is listed as **Running**.
5. Close the **Services** console.

2: Maintaining Active Directory® Domain Services

Demonstration: Using the Active Directory Recycle Bin

In this demonstration, you will see how to:

- Enable the Active Directory Recycle Bin
- Create and then delete test accounts
- Restore deleted accounts

Preparation Steps

You require the 20411D-LON-DC1 virtual machine. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. Click **Adatum (local)**.
3. In the **Tasks** pane, click **Enable Recycle Bin**, click **OK** on the warning message box, and then click **OK** to refresh the **Active Directory Administrative Center** message.
4. Press F5 to refresh **Active Directory Administrative Center**.
5. In **Active Directory Administrative Center**, double-click the **Research OU**.
6. In the Task pane, click **New**, and then click **User**.
7. Enter the following information under **Account**, and then click **OK**:
 - Full name: **Test1**
 - User UPN logon: **Test1**
 - Password: **Pa\$\$w0rd**
 - Confirm password: **Pa\$\$w0rd**
8. Repeat the previous steps to create a second user, **Test2**.
9. Select both **Test1** and **Test2**. Right-click the selection, and then click **Delete**.
10. At the confirmation prompt, click **Yes**.
11. In **Active Directory Administrative Center**, click **Adatum (Local)**, and then double-click **Deleted Objects**.



12. Right-click **Test1**, and then click **Restore**.
13. Right-click **Test2**, and then click **Restore To**.
14. In the Restore To window, click the **IT OU**, and then click **OK**.
15. Navigate to the Research OU, confirm that Test1 is now located in the Research OU, and then navigate to the IT OU and confirm that Test2 is in the IT OU.
16. Close the Active Directory Administrative Center.

Revert Virtual Machines

When you finish the lab, revert the virtual machines to their initial state by completing the following steps:

1. On the host computer, start **Hyper-V Manager**.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20411D-LON-SVR1**.

3: Managing User and Service Accounts

Demonstration: Configuring PSOs

In this demonstration, you will see how to create a Password Settings Object for the ITAdmins group

Ask the students if they notice that they need to accomplish one more task before the PSO will become effective. They need to assign the group that contained users or user accounts to the ITAdmins group. Until that task is complete, there is no one to whom to assign the password settings.

Preparation Steps

Start 20411D-LON-DC1 and sign on as **adatum\administrator** with a password of **Pa\$\$w0rd**.

Demonstration Steps

1. On 20411D-LON-DC1, in Server Manager, from the **Tools** drop-down list, select **Active Directory Users and Computers**.
2. In the Active Directory Users and Computers console, expand the **adatum.com** node in the console tree. Highlight the following folders and organizational units (OUs), pointing out the various items in each: **Computers**, **Development**, **IT**, **Managers**, **Marketing**, **Research**, **Sales**, and **Users**. Make note of any groups in each OU, but do not examine the groups in the Users container.
3. Return to the Information Technology (IT) OU. Right-click **IT** and select **New**, and then select **Group**. In the New Object -Group console, type **ITAdmins**, and then click **OK**. Close **Active Directory Users and Computers**.
4. In Server Manager, from the **Tools** drop-down list, select **Group Policy Management**. In the Group Policy Management console, expand **Forest: Adatum.com**, and then expand **Domains**, **Adatum.com**.
5. Right-click **Default Domain Policy**, and then select **Edit**.
6. Maximize the **Group Policy Management Editor** window, and then expand the following: **Computer Configuration**, **Policies**, **Windows Settings**, **Security Settings**, **Account Policies**.
7. Select **Account Policies**, and then note the three nodes in the details pane: **Password Policy**, **Account Lockout Policy**, and **Kerberos Policy**.
8. Open each of these policies and go over the settings discussed in the topics pages on them, but do

3: Managing User and Service Accounts

1. not make any changes. When done, close the Group Policy Management Editor and Group Policy Management consoles.
2. In **Server Manager**, from the **Tools** drop-down list select **Active Directory Administrative Center**.
3. In the console tree on the left, click **Adatum (local)**. The top-level containers appear in the details pane.
4. In the details pane, scroll down and double-click the **System** container.
5. In the details pane, scroll down and double-click **Password Settings Container**.
6. In the **Tasks** area, on the right, click **New**, and then click **Password Settings**. Explore and explain the various components.
7. In the **Password Settings** area, in the top of the console, explain the purpose of the various elements while you fill out the following:
 - Name: **IT Administrators PSO**
 - Precedence: **1**
 - Enforce minimum password length (characters): **10**
 - Enforce maximum password age User must change the password after (days): **30**
 - Check the **Enforce account lockout policy** check box
 - Number of failed logon attempts allowed: **5**
 - Accept the defaults for all other values
8. In the **Directly Applies To** section, click **Add**.
9. In the Select Users or Groups popup window, in the **Enter the object names to select** text box, type **ITadmins**, and then click **Check Names**. The name should appear in all caps in the text box. Click **OK** twice.
10. Close all open windows.

3: Managing User and Service Accounts

Demonstration: Configuring Group Managed Service Accounts

In this demonstration, you will see how to:

- Create the KDS root key for the domain
- Create and associate a managed service account

Preparation Steps

Start the 20411D-LON-SVR1 virtual machine, and then log on as **Adatum\Administrator** with the password **Pa\$\$w0rd**. 20411D-LON-DC1 should be running from the preceding demonstration.

Demonstration Steps

Create the Key Distribution Services (KDS root key for the domain)

1. On LON-DC1, from Server Manager, open the Active Directory Module for Windows PowerShell® console.
2. At the prompt, type the following command, and then press Enter:
`Add-KDSRootKey -Effectivelmmediately`

Create and associate a managed service account

1. At the prompt, type the following command, and then press Enter:
`New-ADServiceAccount –Name SampleApp_SVR1 –DNSHostname LON-DC1.Adatum.com –PrincipalsAllowedToRetrieveManagedPassword LON-SVR1$`

1. At the prompt, type the following command, and then press Enter:
`Add-ADComputerServiceAccount –identity LON-SVR1 –ServiceAccount SampleApp_SVR1`

1. At the prompt, type the following command, and then press Enter:
`Get-ADServiceAccount -Filter *`

1. Verify that the **SampleApp_SVR1** service account is listed.

Install a managed service account

1. On LON-SVR1, from Server Manager, open the Active Directory Module for Windows PowerShell console.

2. At the prompt, type the following command, and then press Enter:

```
Install-ADServiceAccount -Identity SampleApp_SVR1
```

1. Click the **Server Manager** shortcut on the **Windows Taskbar**.
2. In Server Manager, on the **Menu** toolbar, click **Tools**, and then click **Services**.
3. In the Services console, right-click **Application Identity**, and then click **Properties**.

Note: The Application Identity service is used as an example. In a production environment, you would use the actual service that should be assigned the managed service account.

1. In the **Application Identity Properties (Local Computer)** dialog box, click the **Log On** tab.
2. On the **Log On** tab, click **This account**, and then type **Adatum\SampleApp_SVR1\$**.
3. Clear the password for both the **Password** and **Confirm password** boxes, and then click **OK**.
4. Click **OK** at all prompts.

Revert the Virtual Machines

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat steps 2 and 3 for **20411D-LON-SVR1**.

4: Implementing a Group Policy Infrastructure

Demonstration: How to Create a GPO and Configure GPO Settings

In this demonstration, you will see how to:

- Use the GPMC to create a new GPO
- Configure Group Policy settings

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

Start the 20411D-LON-DC1 virtual machine. Demonstration Steps

Use the Group Policy Management Console (GPMC) to create a new GPO

1. Switch to LON-DC1, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In **Server Manager**, click **Tools**, and then click **Group Policy Management**.
3. If necessary, expand **Forest: Adatum.com**, expand **Domains**, and then expand **Adatum.com**.
4. Select and then right-click the **Group Policy Objects** folder, and then click **New**.
5. In the **New GPO** dialog box, in the **Name** field, type **Desktop**, and then click **OK**.

Configure Group Policy settings

1. In Group Policy Management, expand the **Group Policy Objects** folder, right-click the **Desktop** policy, and then click **Edit**.
2. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Local Policies**, and then click **Security Options**.
3. In the details pane, double-click **Interactive logon: Do not display last user name**.
4. In the **Interactive logon: Do not display last user name Properties** dialog box, select the **Define this policy setting** check box, click **Enabled**, and then click **OK**.
5. Under the **Security Settings** node, click **System Services**.
6. In the details pane, double-click **Windows Installer**.
7. In the **Windows Installer Properties** dialog box, select the **Define this policy setting** check box, and then click **OK**.

4: Implementing a Group Policy Infrastructure

8. Under **User Configuration**, expand **Policies**, expand **Administrative Templates**, and then click **Start Menu and Taskbar**.
9. In the details pane, double-click **Remove Search link from Start Menu**.
10. In the **Remove Search link from Start Menu** dialog box, click **Enabled**, and then click **OK**.
11. Under the **Administrative Templates** folder, expand **Control Panel**, and then click **Display**.
12. In the details pane, double-click **Hide Settings tab**.
13. In the **Hide Settings tab** dialog box, click **Enabled**, and then click **OK**.
14. Close all open windows on LON-DC1.

4: Implementing a Group Policy Infrastructure

Demonstration: Linking GPOs

In this demonstration, you will see how to:

- Create and link GPOs to different locations
- Disable a GPO link
- Delete a GPO link

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

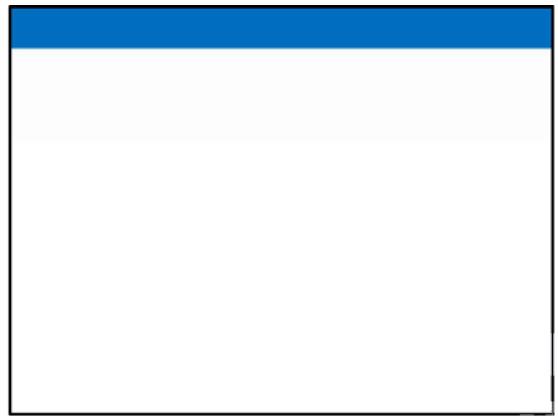
The required virtual machine, 20411D-LON-DC1, should be running already after the preceding demonstration.

Demonstration Steps

Create and edit two GPOs

1. On LON-DC1, if necessary, open Server Manager.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. In the Group Policy Management Console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click the **Group Policy Objects** container, and then click **New**.
4. In the New GPO window, type **Remove Run Command** in the **Name** field, and then click **OK**.
5. In the Group Policy Management window, right-click the **Group Policy Objects** container, and then click **New**.
6. In the New GPO window, type **Do Not Remove Run Command** in the **Name** field, and then click **OK**.
7. Expand **Group Policy Objects**, right-click the **Remove Run Command** GPO, and then click **Edit**.
8. In Group Policy Management Editor, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, click **Start Menu and Taskbar**, and then double-click **Remove Run menu from Start Menu**.
9. In the Remove Run menu from Start Menu window, click **Enabled**, and then click **OK**.
10. Close the Group Policy Management Editor.
11. Right-click the **Do Not Remove Run Command** GPO, and then click **Edit**.
12. In Group Policy Management Editor, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, click **Start Menu and Taskbar**, and then double-click **Remove Run**

4: Implementing a Group Policy Infrastructure



menu from Start Menu.

13. In the Remove Run menu from Start Menu window, click **Disabled**, and then click **OK**.
14. Close the Group Policy Management Editor.

Link the GPOs to different locations

1. In the Group Policy Management window, right-click the **Adatum.com** domain node in the left pane, and then click **Link an Existing GPO**.
2. In the Select GPO window, click **Remove Run Command**, and then click **OK**. The Remove Run Command GPO is now attached to the Adatum.com domain.
3. Click and drag the **Do Not Remove Run Command** GPO to the **IT OU**.
4. In the **Group Policy Management** window, click **OK** to link the GPO.
5. Click the **IT OU** in the left pane, and then click the **Group Policy Inheritance** tab in the right pane. The **Group Policy Inheritance** tab shows the order of precedence for the GPOs.

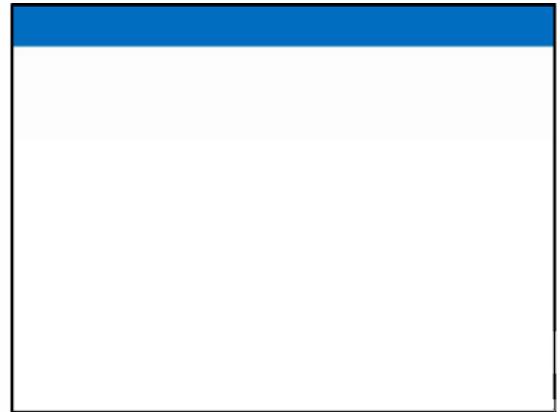
Disable a GPO link

1. In the left pane, right-click the **Remove Run Command** link that is listed under **Adatum.com**, and then click **Link Enabled** to clear the check mark. Refresh the Group Policy Inheritance window for the **IT OU**, and then notice the results in the right pane. The Remove Run Command GPO no longer is listed.

Delete a GPO link

1. In the left pane, expand the **IT OU**, right-click the **Do Not Remove Run Command** link, and then click **Delete**. Click **OK** in the pop-up window.
2. Click the **IT OU** in the left pane, and then click the **Group Policy Inheritance** tab in the right pane. Verify the removal of the Do Not Remove Run Command and the absence of the Remove Run Command GPOs.
3. In the left pane, right-click the **Remove Run Command** GPO that is listed under **Adatum.com**, and

4: Implementing a Group Policy Infrastructure



then click **Link Enabled** to re-enable the link. Refresh the Group Policy Inheritance window for the IT OU, and then notice the results in the right pane.

4. Close the Group Policy Management Console.

4: Implementing a Group Policy Infrastructure

Demonstration: Filtering Policies

In this demonstration, you will see how to:

- Filter group policy application by using security group filtering
- Filter Group Policy application by using WMI filtering

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

The required virtual machine, 20411D-LON-DC1, should be running after the preceding demonstration.

Demonstration Steps

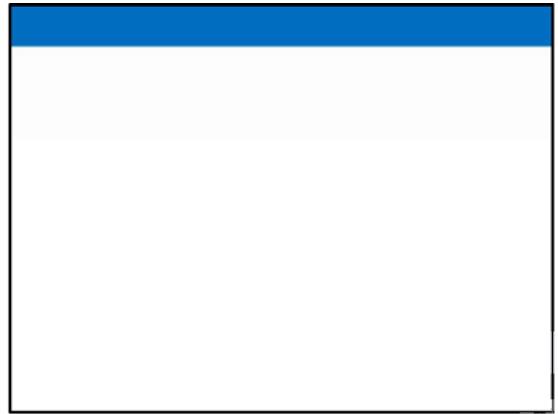
Create a new GPO, and link it to the IT OU

1. On LON-DC1, from **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the Group Policy Management Console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com** if not expanded already, and then click the **IT** OU.
3. Right-click **IT**, and then click **Create a GPO in this domain, and Link it here**.
4. In the **New GPO** window, type **Remove Help menu** in the **Name** field, and then click **OK**.
5. In the Group Policy Management window, expand **Group Policy Objects**, right-click the **Remove Help menu** GPO, and then click **Edit**.
6. In the Group Policy Management Editor, under **User Configuration**, expand **Policies**, expand **Administrative Templates**, click **Start Menu and Taskbar**, and then double-click **Remove Help menu from Start Menu**.
7. In the **Remove Help menu from Start menu** window, click **Enabled**, and then click **OK**.
8. Close the Group Policy Management Editor window.

Filter Group Policy application by using security group filtering

1. Expand **IT**, and then click the **Remove Help menu** GPO link.
2. In the **Group Policy Management Console** message box, click **OK**.
3. In the right pane, under **Security Filtering**, click **Authenticated Users**, and then click **Remove**.

4: Implementing a Group Policy Infrastructure



4. In the confirmation dialog box, click **OK**.
5. Under **Security Filtering**, click **Add**.
6. In the **Select User, Computer, or Group** dialog box, type **Ed Meadows**, and then click **OK**.

Filter the Group Policy application by using WMI filtering

1. In the Group Policy Management window, right-click **WMI Filters**, and then click **New**.
2. In the **New WMI Filter** dialog box, in the **Name** field, type **XP Filter**.
3. In the **Queries** pane, click **Add**.
4. In the **WMI Query** dialog box, in the **Query** field, type the following, and then click **OK**:

Select * from Win32_OperatingSystem where Version = "6.3.9600"

5. In the Warning pop-up window, click **OK**.
6. In the **New WMI Filter** dialog box, click **Save**.
7. Right-click the **Group Policy Objects** folder, and then click **New**.
8. In the **New GPO** window, type **Software Updates for XP** in the **Name** field, and then click **OK**.
9. Expand the **Group Policy Objects** folder, and then click the **Software Updates for XP GPO**.
10. In the right-hand pane, under WMI Filtering, in the **This GPO is linked to the following WMI Filter** list, select **XP Filter**.
11. In the confirmation dialog, click **Yes**.
12. Close the Group Policy Management Console.

4: Implementing a Group Policy Infrastructure

Demonstration: Performing What-If Analysis with the Group Policy Modeling Wizard

In this demonstration, you will see how to:

- Use GPResult.exe and the Group Policy Reporting Wizard
- Use the Group Policy Modeling Wizard

Emphasize that the Group Policy Modeling Wizard is not reporting actual application of Group Policy, but rather, is analyzing and reporting anticipated Group Policy application.

Ask students what scenarios would lend themselves to using Group Policy Modeling. Among the answers should be scenarios in which users or computers will be moved, scenarios in which group memberships will be changed to evaluate the potential changes to their configuration from Group Policy. Also, you can use modeling to evaluate the impact of a new GPO prior to rolling it into production.

When you are finished with this demonstration, you can revert all virtual machines.

Preparation Steps

The required virtual machine, 20411D-LON-DC1 already should be running after the preceding demonstration.Demonstration Steps

Use GPResult.exe to create a report

1. On LON-DC1, right-click the **Start** icon, and then click **Windows PowerShell (Admin)**.
2. In the Windows PowerShell window, type **cd desktop**, and then press Enter.
3. In the Windows PowerShell window, type the following, and press Enter:
GPResult /r

4. Review the output in the Windows PowerShell window.
5. In the Windows PowerShell window, type the following, and then press Enter:
GPResult /h results.html

6. Close the Windows PowerShell window, and then double-click the **results.html** file on the desktop.
7. In the Internet Explorer® window, view the results of the report.
8. Close Internet Explorer.

4: Implementing a Group Policy Infrastructure



Use the Group Policy Reporting Wizard to create a report

1. Open **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. In the Group Policy Management window, right-click **Group Policy Results**, and then click **Group Policy Results Wizard**.
3. In the **Group Policy Results Wizard**, click **Next**.
4. On the **Computer Selection** page, click **Next**.
5. On the **User Selection** page, click **Next**.
6. On the **Summary of Selections** page, click **Next**.
7. On the **Completing the Group Policy Results Wizard** page, click **Finish**.
8. Review the Group Policy results.
9. Under the Group Policy Results folder, right-click the **Administrator on LON-DC1** report, and then click **Save Report**.
10. In the **Save GPO Report** dialog box, click **Desktop**, and then click **Save**.

Use the Group Policy Modeling Wizard to create a report

1. Right-click the **Group Policy Modeling** folder, and then click **Group Policy Modeling Wizard**.
2. In the **Group Policy Modeling Wizard**, click **Next**.
3. On the **Domain Controller Selection** page, click **Next**.
4. On the **User and Computer Selection** page, under **User information**, click **User**, and then click **Browse**.
5. In the **Select User** dialog box, type **Ed Meadows**, and then click **OK**.
6. Under Computer information, click **Browse**.

4: Implementing a Group Policy Infrastructure



7. In the **Choose Computer Container** dialog box, expand **Adatum**, click **IT**, and then click **OK**.
8. On the **User and Computer Selection** page, click **Next**.
9. On the **Advanced Simulation Options** page, click **Next**.
10. On the **Alternate Active Directory Paths** page, click **Next**.
11. On the **User Security Groups** page, click **Next**.
12. On the **Computer Security Groups** page, click **Next**.
13. On the **WMI Filters for Users** page, click **Next**.
14. On the **WMI Filters for Computers** page, click **Next**.
15. On the **Summary of Selections** page, click **Next**.
16. On the **Completing Group Policy Modeling Wizard** page, click **Finish**.
17. Review the report.
18. Close all open windows.
19. After the demonstration, revert all of the virtual machines used for the demonstrations.

5: Managing User Desktops with Group Policy

Demonstration: Configuring Settings with Administrative templates

In this demonstration, you will see how to:

- Filter Administrative Template policy settings
- Apply comments to policy settings
- Add comments to a GPO
- Create a new GPO by copying an existing GPO
- Create a new GPO by importing settings that were exported from another GPO

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

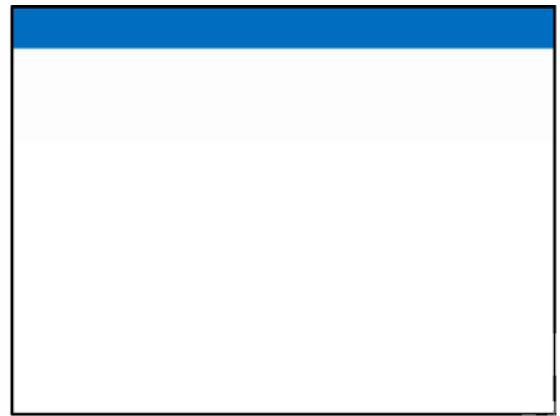
You require the 20411D-LON-DC1 virtual machine for this demonstration.

Demonstration Steps

Filter Administrative Template policy settings

1. Switch to LON-DC1.
2. Log in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. In Server Manager, click **Tools**, and then click **Group Policy Management**.
4. In the console tree, expand **Forest: Adatum.com**, **Domains**, and **Adatum.com**, and then click the **Group Policy Objects** container.
5. Right-click the **Group Policy Objects** container, and then click **New**.
6. In the **New GPO** dialog box, in the **Name** field, type **GPO1**, and then click **OK**.
7. In the details pane, right-click **GPO1**, and then click **Edit**. The Group Policy Management Editor appears.
8. In the console tree, expand **User Configuration**, expand **Policies**, and then click **Administrative Templates**.
9. Right-click **Administrative Templates**, and then click **Filter Options**.
10. Select the **Enable Keyword Filters** check box.
11. In the **Filter for word(s)** text box, type **screen saver**.
12. In the drop-down list next to the text box, select **Exact**, and then click **OK**.
Administrative templates policy settings are filtered to show only those that contain the words **screen saver**. Spend a few moments examining the settings that you have found.
13. In the console tree, under **User Configuration**, right-click **Administrative Templates**, and then

5: Managing User Desktops with Group Policy



click **Filter Options**.

14. Clear the **Enable Keyword Filters** check box.
15. In the **Configured** drop-down list, select **Yes**, and then click **OK**. Administrative Template policy settings are filtered to show only those that have been configured (enabled or disabled). No settings have been enabled.
16. In the console tree, under **User Configuration**, right-click **Administrative Templates**, and clear the **Filter On** option.

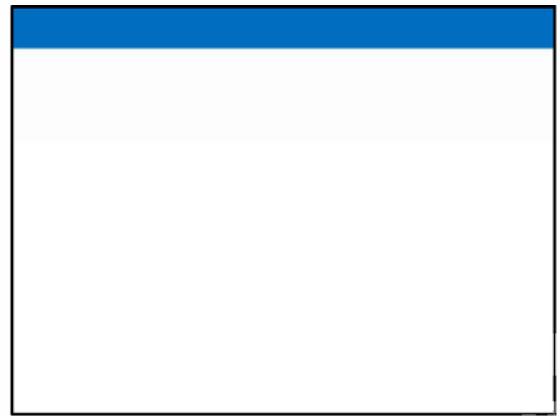
Add comments to a policy setting

1. In the console tree, expand **User Configuration**, **Policies**, **Administrative Templates**, and **Control Panel**, and then click **Personalization**.
2. Double-click the **Enable screen saver** policy setting.
3. In the **Comment** section, type **Corporate IT Security Policy implemented with this policy in combination with Password Protect the Screen Saver**, and then click **OK**.
4. Double-click the **Password protect the screen saver** policy setting. Click **Enabled**.
5. In the **Comment** section, type **Corporate IT Security Policy implemented with this policy in combination with Enable screen saver**, and then click **OK**.

Add comments to a GPO

1. In the console tree of the Group Policy Management Editor, right-click the root node, **GPO1 [LON-DC1.ADATUM.COM]**, and then click **Properties**.
2. Click the **Comment** tab.
3. Type **Adatum corporate standard policies. Settings are scoped to all users and computers in the domain. Person responsible for this GPO: your name**. This comment appears on the **Details** tab of the GPO in the Group Policy Management Console.

5: Managing User Desktops with Group Policy



4. Click **OK**, and then close the Group Policy Management Editor.

Create a new GPO by copying an existing GPO

1. In the GPMC console tree, click the **Group Policy Objects** container, right-click **GPO1**, and then click **Copy**.
2. Right-click the **Group Policy Objects** container, click **Paste**, and then click **OK**.
3. Click **OK**.

Create a new GPO by importing settings that were exported from another GPO

1. In the GPMC console tree, click the **Group Policy Objects** container, right-click **GPO1**, and then click **Back Up**.
2. In the **Location:** box, type **c:**, and then click **Back Up**.
3. When the backup finishes, click **OK**.
4. In the GPMC console tree, right-click the **Group Policy Objects** container, and then click **New**.
5. In the **Name:** box, type **ADATUM Import**, and then click **OK**.
6. In the GPMC console tree, right-click the **ADATUM Import** GPO, and then click **Import Settings**. The Import Settings Wizard appears.
7. Click **Next** three times.
8. Select **GPO1**, and then click **Next** two times.
9. Click **Finish**, and then click **OK**.
10. Close the Group Policy Management Console.

5: Managing User Desktops with Group Policy

Demonstration: Configuring Administrative templates

In this demonstration, you will see how to:

- Import the Office 2013 administrative template files
- Customize Office 2013 settings by using the administrative template

As you are modifying the Office 2013 settings, point out the overall scope of the available settings. Students should see that a wide range of settings is available. Also, mention that many of the settings are organized by Microsoft Office application such as Microsoft Word and Microsoft Office Excel®. Finally, mention that a detailed spreadsheet of all of the settings comes with the Office 2013 administrative template download. The file is named office2013groupolicyandoctsettings.xlsx and is located at E:\Labfiles\Mod05\Office 2013 on LON-DC1 if students are interested in looking at it.

Preparation Steps

The LON-DC1 virtual machine should be running from the previous demonstration.

Demonstration Steps

Add the Microsoft Office 2013 administrative template files to LON-DC1:

1. On LON-DC1, click **File Explorer** on the taskbar.
2. Navigate to the E:\Labfiles\Mod05\Office 2013\admx\en-us folder.
3. Copy all of the .adml files to the c:\Windows\PolicyDefinitions\en-US folder.
4. In File Explorer, navigate to the E:\Labfiles\Mod05\Office 2013\admx folder.
5. Copy all of the .admx files to the c:\Windows\PolicyDefinitions folder.

Configure Office 2013 settings:

1. On LON-DC1, click **Server Manager**, click **Tools**, and then click **Group Policy Management**.
2. Expand **Forest: adatum.com**.
3. Expand **Domains**.
4. Expand **adatum.com**.
5. Right-click **Group Policy Objects**, and then click **New**.
6. In the New GPO window, type **Office 2013** into the **Name** field, and then click **OK**.
7. Right-click the **Office 2013** GPO in the left pane, and then click **Edit**.
8. Under **User Configuration**, in the left pane, expand **Policies**.
9. Expand **Administrative Templates: Policy definitions (ADMX files) retrieved from the local computer**.
10. Expand **Microsoft Word 2013**.
11. Expand **Word Options**, and then click **Customize Ribbon**.
12. In the right pane, double-click the **Display Developer tab in the Ribbon** setting.
13. In the **Display Developer tab in the Ribbon** window, click the **Enabled** radio button, and then click **OK**.

5: Managing User Desktops with
Group Policy

14. In the left pane, expand **Proofing**, and then click **AutoCorrect**.
15. In the right pane, double-click the **Replace text as you type** setting.
16. In the Replace text as you type window, click **Disabled**, and then click **OK**.
17. Close the Group Policy Management Editor.
18. In the Group Policy Management Console, right-click the **Adatum.com** domain, and then click **Link an Existing GPO** in the context menu.
19. In the Select GPO window, click the **Office 2013** GPO, and then click **OK**.

5: Managing User Desktops with Group Policy

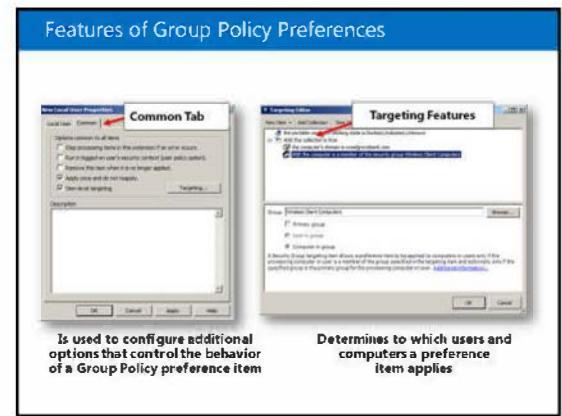
Item-Level Targeting Options

- Target 27 different categories
- Combine different categories together by using AND or OR Boolean logic. Instead of using a single category for targeting, you can use multiple categories
- Item-level targeting is refreshed during the Group Policy background refresh

Discuss with students the nearly unlimited possibilities created by item-level targeting. Refer to the screen capture in Figure 5.1 to come up with real world scenarios, such as the following example scenario:

- if computer is in a dev/lab network then it shouldn't get mapped drives to corporate file servers
 - if computer is a member of a specific domain and it is in the dev/lab network, then the IE security zone settings should be adjusted for maximum security

5: Managing User Desktops with Group Policy



Group Policy preferences provide better targeting through item-level targeting and action modes. In addition to providing significantly more coverage, better targeting, and easier management, Group Policy preferences enable you to deploy settings to client computers without restricting the users from changing the settings. This capability provides you with the flexibility to decide whether to enforce specific settings. You can deploy settings that you do not want to enforce by using Group Policy preferences.

5: Managing User Desktops with Group Policy

Strictly enforce policy settings by writing the settings to areas of the registry that standard users cannot modify	Are written to the normal locations in the registry that the application or operating system feature uses to store the setting
Typically disable the user interface for settings that Group Policy is managing	Do not cause the application or operating system feature to disable the user interface for the settings they configure
Refresh policy settings at a regular intervals	Refresh preferences by using the same interval as Group Policy settings by default

Explain to students that the main difference between policy settings and preference settings is that preference settings are not enforced. They should understand that this means the end user can change any preference setting that is applied through Group Policy, but not policy settings.

Preference items are intended to supplement policy settings, and you can configure the following as preference items:

- Settings that cannot be configured through policy settings.
- Settings that have limitations when they are configured by using policy settings.

5: Managing User Desktops with Group Policy

What Are Group Policy Preferences?

Group Policy preferences expand the range of configurable settings within a GPO.

Group Policy preferences:

- Enable IT professionals to configure, deploy, and manage settings that were not manageable by using Group Policy
- Are natively supported on Windows Server 2008 and Windows Vista SP2 or newer
- Can be created, deleted, replaced, or updated

Explain to students that you now can process Group Policy preferences because of several new Group Policy client-side extensions that expand the range of configurable settings in a GPO. Examples of the new Group Policy preference extensions include the following:

- Folder Options
- Drive Maps
- Printers
- Scheduled Tasks
- Services
- Start Menu

5: Managing User Desktops with Group Policy

Lesson 3: Configuring Group Policy Preferences

- What Are Group Policy Preferences?
- Comparing Group Policy Preferences and Administrative templates
- Features of Group Policy Preferences
- Item-Level Targeting Options
- Demonstration: Configuring Group Policy Preferences

5: Managing User Desktops with Group Policy



6. Expand **Adatum.com**, right-click the **Drivemap** GPO, and then click **Edit**.
7. In the Group Policy Management Editor, under **User Configuration**, expand **Policies**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.
8. In the details pane, double-click **Logon**.
9. In the **Logon Properties** dialog box, click **Show Files**. This opens the Netlogon share.
10. In the details pane, right-click a blank area, and then click **Paste**.
11. Close the Logon window.
12. In the **Logon Properties** dialog box, click **Add**.
13. In the **Add a Script** dialog box, click **Browse**.
14. Click the **Map.bat** script, and then click **Open**.
15. Click **OK** twice to close all dialog boxes.
16. Close the Group Policy Management Editor and the Group Policy Management Console.

Log in to the client to test the results

1. On LON-CL1, log in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Click **Desktop**, and, on the taskbar, click **File Explorer**.
3. Verify that you have a drive mapped to **\LON-DC1\redirect** by examining the navigation pane.
4. Log off of LON-CL1.

5: Managing User Desktops with Group Policy

Demonstration: Configuring Scripts with GPOs

In this demonstration, you will see how to:

- Create a login script to map a network drive
- Create and link a GPO to use the script and store the script in the Netlogon share
- Log on to client computer and test results

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

The required virtual machines, 20411D-LON-DC1 and 20411D-LON-CL1, should already be running after the preceding demonstration.

Demonstration Steps

Create a logon script to map a network drive

1. On LON-DC1, click **Start**, type **Notepad**, and then press Enter.
2. In Notepad, type the following command:

Net use t: \\LON-dc1\Redirect

3. Click the **File** menu, and then click **Save**.
4. In the **Save As** dialog box, in the **File name** box, type **Map.bat**.
5. In the **Save as type:** list, select **All Files (*.*)**.
6. In the navigation pane, click **Desktop**, and then click **Save**.
7. Close Notepad.
8. On the desktop, right-click the **Map.bat** file, and then click **Copy**.

Create and link a GPO to use the script, and then store the script in the Netlogon share

1. Open **Server Manager**.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. Expand **Forest: Adatum.com**, and then expand **Domains**.
4. Right-click **Adatum.com**, and then click **Create a GPO in this domain and link it here**.
5. In the **New GPO** dialog box, in the **Name** box, type **DriveMap**, and then click **OK**.

5: Managing User Desktops with Group Policy

Group Policy Settings for Applying Scripts

You can use scripts to perform many tasks, such as clearing page files or mapping drives, and clearing temp folders for users

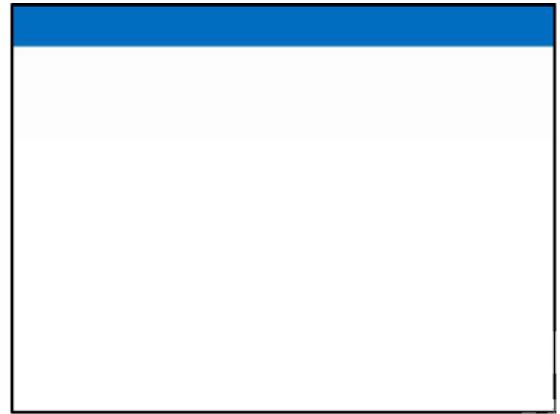
You can assign Group Policy script settings to assign:

- For computers:
 - Startup scripts
 - Shutdown scripts
- For users:
 - Logon scripts
 - Logoff scripts

Explain that you cannot set all configuration settings by using Group Policy settings. You can use scripts to perform many tasks, such as clearing page files or mapping drives, and clearing temporary folders for users. Describe the four types of scripts and when the scripts run.

Describe the difference between synchronous and asynchronous script processing. Explain that logon scripts run asynchronously by default, and startup scripts run synchronously by default, but that you can modify that setting. Mention that if scripts are set to run synchronously, then a failed script can cause a computer to stop responding.

5: Managing User Desktops with Group Policy



10. Right-click **Documents**, and then click **Properties**.
11. In the **Documents Properties** dialog box, note that the location of the folder is now the Redirect network share in a subfolder named for the user.
12. Log off of LON-CL1.

5: Managing User Desktops with Group Policy

Demonstration: Configuring Scripts with GPOs

In this demonstration, you will see how to:

- Create a login script to map a network drive
- Create and link a GPO to use the script and store the script in the Netlogon share
- Log on to client computer and test results

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

The required virtual machines, 20411D-LON-DC1 and 20411D-LON-CL1, should already be running after the preceding demonstration.

Demonstration Steps

Create a logon script to map a network drive

1. On LON-DC1, click **Start**, type **Notepad**, and then press Enter.
2. In Notepad, type the following command:

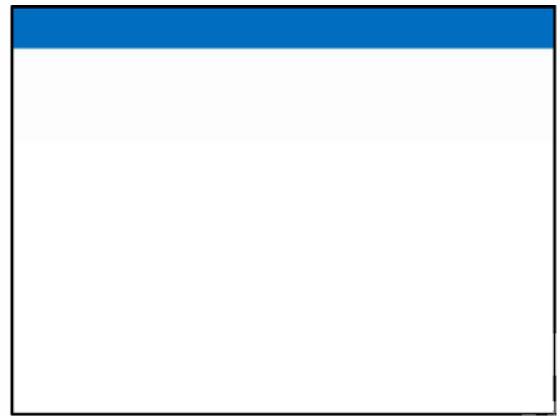
Net use t: \\LON-dc1\Redirect

3. Click the **File** menu, and then click **Save**.
4. In the **Save As** dialog box, in the **File name** box, type **Map.bat**.
5. In the **Save as type:** list, select **All Files (*.*)**.
6. In the navigation pane, click **Desktop**, and then click **Save**.
7. Close Notepad.
8. On the desktop, right-click the **Map.bat** file, and then click **Copy**.

Create and link a GPO to use the script, and then store the script in the Netlogon share

1. Open **Server Manager**.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. Expand **Forest: Adatum.com**, and then expand **Domains**.
4. Right-click **Adatum.com**, and then click **Create a GPO in this domain and link it here**.
5. In the **New GPO** dialog box, in the **Name** box, type **DriveMap**, and then click **OK**.

5: Managing User Desktops with Group Policy



6. Expand **Adatum.com**, right-click the **Drivemap** GPO, and then click **Edit**.
7. In the Group Policy Management Editor, under **User Configuration**, expand **Policies**, expand **Windows Settings**, and then click **Scripts (Logon/Logoff)**.
8. In the details pane, double-click **Logon**.
9. In the **Logon Properties** dialog box, click **Show Files**. This opens the Netlogon share.
10. In the details pane, right-click a blank area, and then click **Paste**.
11. Close the Logon window.
12. In the **Logon Properties** dialog box, click **Add**.
13. In the **Add a Script** dialog box, click **Browse**.
14. Click the **Map.bat** script, and then click **Open**.
15. Click **OK** twice to close all dialog boxes.
16. Close the Group Policy Management Editor and the Group Policy Management Console.

Log in to the client to test the results

1. On LON-CL1, log in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Click **Desktop**, and, on the taskbar, click **File Explorer**.
3. Verify that you have a drive mapped to **\LON-DC1\redirect** by examining the navigation pane.
4. Log off of LON-CL1.

5: Managing User Desktops with Group Policy

Demonstration: Configuring Group Policy Preferences

In this demonstration, you will see how to:

- Configure a desktop shortcut with Group Policy preferences
- Target the preference
- Configure a new folder with Group Policy preferences
- Target the preference
- Test the preferences

At the end of this demonstration, you can revert the virtual machines.

Preparation Steps

The required virtual machines, 20411D-LON-DC1 and 20411D-LON-CL1, should be running after the preceding demonstration.

Demonstration Steps

Configure a desktop shortcut with Group Policy preferences

1. On LON-DC1, from Server Manager, open the **Group Policy Management Console**.
2. In the Group Policy Management Console, click the **Group Policy Objects** folder, and, in the details pane, right-click the **Default Domain Policy**, and then click **Edit**.
3. Under **Computer Configuration**, expand **Preferences**, expand **Windows Settings**, right-click **Shortcuts**, point to **New**, and then click **Shortcut**.
4. In the **New Shortcut Properties** dialog box, in the **Action** list, select **Create**.
5. In the **Name** box, type **NotePad**.
6. In the **Location** box, click the arrow, and then select **All Users Desktop**.
7. In the **Target path** box, type **C:\Windows\System32\NotePad.exe**.

Target the preference

1. On the **Common** tab, select the **Item-level targeting** check box, and then click **Targeting**.
2. In the **Targeting Editor** dialog box, click **New Item**, and then click **Computer Name**.
3. In the **Computer name** box, type **LON-CL1**, and then click **OK** twice.

Configure a new folder with Group Policy preferences

1. Under **Windows Settings**, right-click **Folders**, point to **New**, and then click **Folder**.



2. In the **New Folder Properties** dialog box, in the **Action** list, select **Create**.
3. In the **Path** field, type **C:\Reports**.

Target the preference

1. On the **Common** tab, select the **Item-level targeting** check box, and then click **Targeting**.
2. In the **Targeting Editor** dialog box, click **New Item**, and then click **Operating System**.
3. In the **Product** list, select **Windows 8.1**, and then click **OK** twice.
4. Close the Group Policy Management Editor.

Test the preferences

1. Log in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On the Start screen, type **Windows PowerShell**, and then press Enter.
3. At the Windows PowerShell prompt, type the following command, and then press Enter:
`gpupdate /force`
4. Log in to LON-CL1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
5. From Start, click **Desktop**.
6. Verify the presence of the Notepad shortcut on the desktop.
7. On the taskbar, click **File Explorer**.
8. Verify the presence of the C:\Reports folder.
9. Revert the LON-DC1 and LON-CL1 virtual machines after this demonstration.

20411D

06: Installing, Configuring, and Troubleshooting the Network Policy Server Role

Demonstration: Installing the Network Policy Server Role Service

In this demonstration, you will see how to:

- Install the NPS role service
- Register NPS in AD DS

Leave the virtual machine running for subsequent demonstrations.

Preparation Steps

You require the 20411D-LON-DC1 virtual machine for this demonstration.

Demonstration Steps

Install the NPS Role

1. Sign in to LON-DC1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. If necessary, on the taskbar, click **Server Manager**.
3. In the details pane, click **Add roles and features**.
4. In the Add Roles and Features Wizard, click **Next**.
5. On the **Select installation type** page, click **Role-based or feature based installation**, and then click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, select the **Network Policy and Access Services** check box.
8. Click **Add Features**, and then click **Next** twice.
9. On the **Network Policy and Access Services** page, click **Next**.
10. On the **Select role services** page, verify that the **Network Policy Server** check box is selected, and then click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. Verify that the installation was successful, and then click **Close**.
13. Close the Server Manager window.

Register NPS in AD DS

20411D
06: Installing, Configuring, and
Troubleshooting the Network Policy
Server Role

- 
1. Click **Start**, and then click **Administrative Tools**.
 2. Double-click **Network Policy Server**.
 3. In Network Policy Server, in the navigation pane, right-click **NPS (Local)**, and then click **Register server in Active Directory**.
 4. In the **Network Policy Server** message box, click **OK**.
 5. In the subsequent **Network Policy Server** dialog box, click **OK**.
 6. Leave the Network Policy Server console window open.

20411D

06: Installing, Configuring, and Troubleshooting the Network Policy Server Role

In this demonstration, you will see how to:

- Configure a RADIUS server for VPN connections
- Save the configuration

Leave the virtual machines running for subsequent demonstrations.

Preparation Steps

One of the required virtual machines, 20411D-LON-DC1, should be running after the preceding demonstration. Please start 20411D-LON-RTR for this demonstration.

Demonstration Steps

Configure a RADIUS server for VPN connections

- On LON-DC1, in the Network Policy Server console, in the Getting Started details pane, open the drop-down list under **Standard Configuration**, and then click **RADIUS server for Dial-Up or VPN Connections**.
- Under Radius server for Dial-Up or VPN Connections, click **Configure VPN or Dial-Up**.
- In the Configure VPN or Dial-Up Wizard, click **Virtual Private Network (VPN) Connections**, accept the default name, and then click **Next**.
- On the **RADIUS clients** page, click **Add**.
- In the **New RADIUS Client** dialog box, in the **Friendly name** box, type **LON-RTR**, and then click **Verify**.
- In the **Verify Address** dialog box, in the **Address** box, type **LON-RTR**, click **Resolve**, and then click **OK**.
- In the **LON-RTR Properties** dialog box, in the **Shared secret** and **Confirm shared secret** boxes, type **Pa\$\$w0rd**, and then click **OK**.
- On the **Specify Dial-Up or VPN Server** page, click **Next**.
- On the **Configure Authentication Methods** page, ensure that the **Microsoft Encrypted Authentication version 2 (MS-CHAPv2)** check box is selected, and then click **Next**.

20411D
06: Installing, Configuring, and
Troubleshooting the Network Policy
Server Role



10. On the **Specify User Groups** page, click **Next**.
11. On the **Specify IP Filters** page, click **Next**.
12. On the **Specify Encryption Settings** page, click **Next**.
13. On the **Specify a Realm Name** page, click **Next**.
14. On the **Completing New Dial-up or Virtual Private Network Connections and RADIUS clients** page, click **Finish**.

Save the configuration

1. On the taskbar, click **Windows PowerShell**.
2. At the Windows PowerShell® command prompt, type the following command, and then press Enter:

Export-NpsConfiguration –path I:\n-dc1.xml

1. At the Windows PowerShell command prompt, type the following command, and then press Enter:

Notepad I:\n-dc1.xml

1. Scroll through the file, and then discuss the contents. Close the file.

20411D

06: Installing, Configuring, and Troubleshooting the Network Policy Server Role

Demonstration: Configuring a RADIUS Client

In this demonstration, you will see how to configure a RADIUS client

Shut down LON-RTR because it is not required for subsequent demonstrations. Leave LON-DC1 running for subsequent demonstrations.

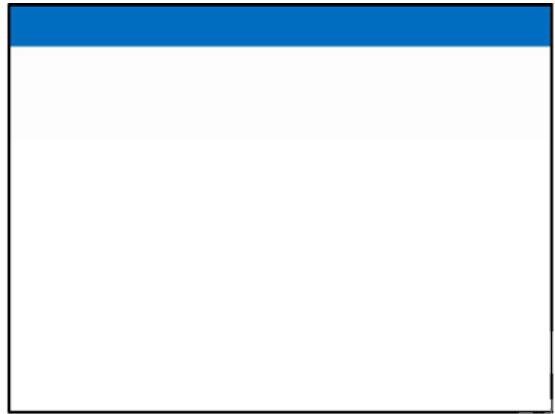
Preparation Steps

The required virtual machines 20411D-LON-DC1 and 20411D-LON-RTR should be running after the preceding demonstration.

Demonstration Steps

1. Switch to LON-RTR.
2. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Click **Start**.
4. On the Start screen, click **Administrative Tools**, and then double-click **Routing and Remote Access**.
5. If required, in the Enable DirectAccess Wizard dialog box, click **Cancel**, and then click **OK**.
6. In the Routing and Remote Access console, right-click **LON-RTR (local)**, and then click **Disable Routing and Remote Access**.
7. In the **Routing and Remote Access** dialog box, click **Yes**.
8. In the Routing and Remote Access console, right-click **LON-RTR (local)**, and then click **Configure and Enable Routing and Remote Access**.
9. Click **Next**, ensure that **Remote access (dial-up or VPN)** is selected, and then click **Next**.
10. Select the **VPN** check box, and then click **Next**.
11. Click the network interface named **Ethernet 2**. Clear the **Enable security on the selected interface by setting up static packet filters** check box, and then click **Next**.
12. On the **Network Select** page, ensure that the Ethernet network interface is selected, and then click **Next**.

20411D
06: Installing, Configuring, and
Troubleshooting the Network Policy
Server Role



13. On the **IP Address Assignment** page, select **From a specified range of addresses**, and then click **Next**.
14. On the **Address Range Assignment** page, click **New**. Next to Start IP address, type **172.16.0.100**. Next to End IP address, type **172.16.0.110**, and then click **OK**. Verify that 11 IP addresses were assigned for remote clients, and then click **Next**.
15. On the **Managing Multiple Remote Access Servers** page, click **Yes, set up this server to work with a RADIUS server**, and then click **Next**.
16. On the **RADIUS Server Selection** page, in the **Primary RADIUS server** box, type **LON-DC1**.
17. In the **Shared secret** box, type **Pa\$\$w0rd**, and then click **Next**.
18. Click **Finish**.
19. In the **Routing and Remote Access** dialog box, click **OK**.
20. If prompted again, click **OK**.

20411D

06: Installing, Configuring, and Troubleshooting the Network Policy Server Role

Demonstration: Creating a Connection Request Policy

In this demonstration, you will see how to create a VPN connection request policy

Revert all virtual machines.

Preparation Steps

The required virtual machine 20411D-LON-DC1 should be running after the preceding demonstration.

Demonstration Steps

1. Switch to the LON-DC1 computer.
2. Switch to the Network Policy Server console.
3. In Network Policy Server, expand **Policies**, and then click **Connection Request Policies**. Notice the presence of the Virtual Private Network (VPN) Connections policies. The wizard created these automatically when you specified the NPS role of this server.
4. Right-click **Connection Request Policies**, and then click **New**.
5. In the New Connection Request Policy Wizard, in the **Policy name** box, type **Adatum VPN**.
6. In the **Type of network access server** list, click **Remote Access Server(VPN-Dial up)**, and then click **Next**.
7. On the **Specify Conditions** page, click **Add**.
8. In the **Select condition** dialog box, select **NAS Port Type**, and then click **Add**.
9. In the **NAS Port Type** dialog box, select the **Virtual (VPN)** check box, and then click **OK**. Click **Next**.
10. On the **Specify Connection Request Forwarding** page, click **Next**.
11. On the **Specify Authentication Methods** page, click **Next**.
12. On the **Configure Settings** page, click **Next**.
13. On the **Completing Connection Request Policy Wizard** page, click **Finish**.
14. In the **Connection Request Policies** list, right-click **Adatum VPN**, and then click **Move Up**.

20411D
06: Installing, Configuring, and
Troubleshooting the Network Policy
Server Role

- 
15. Ensure that the Adatum VPN policy has a processing order of 1. If not, repeat step 14.

07: Implementing Network Access Protection

Demonstration: Configuring NAP

In this demonstration, you will see how to:

- Install the NPS server role
- Configure NPS as an NAP health policy server
- Configure health policies
- Configure network policies for compliant computers
- Configure network policies for noncompliant computers
- Configure the DHCP server role for NAP
- Configure client NAP settings
- Test NAP

Leave all virtual machines in their current state for subsequent demonstrations.

Preparation Steps

You will need to use the 20411D-LON-DC1 and 20411D-LON-CL1 virtual machines to perform this demonstration.

Demonstration Steps

Install the NPS server role

1. Switch to LON-DC1 and sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. If necessary, on the taskbar, click **Server Manager**.
3. In the details pane, click **Add Roles and Features**.
4. In the Add Roles and Features Wizard, click **Next**.
5. On the **Select installation type** page, ensure that **Role-based or feature based installation** is selected, and then click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, select the **Network Policy and Access Services** check box.
8. Click **Add Features**, and then click **Next** twice.
9. On the **Network Policy and Access Services** page, click **Next**.
10. On the **Select role services** page, verify that the **Network Policy Server** check box is selected, and then click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. Verify that the installation was successful, and then click **Close**.
13. Close the Server Manager window.

Configure NPS as a NAP health policy server

1. Click **Start**.
2. Click **Administrative Tools**, and then double-click **Network Policy Server**.
3. In the navigation pane, expand **Network Access Protection**, expand **System Health Validators**, expand **Windows Security Health Validator**, and then click **Settings**.
4. In the right pane under **Name**, double-click **Default Configuration**.
5. In the navigation pane, ensure that the **Windows 8/Windows 7/Windows Vista** option is selected.
6. In the details pane, clear all check boxes except the **A firewall is enabled for all network connections** check box. Note that some check boxes will appear dimmed when you begin clearing other check boxes.
7. Click **OK** to close the **Windows Security Health Validator** dialog box.

Configure health policies

1. In the navigation pane, expand **Policies**.
2. Right-click **Health Policies**, and then click **New**.
3. In the **Create New Health Policy** dialog box, under **Policy name**, type **Compliant**.
4. Under **Client SHV checks**, verify that **Client passes all SHV checks** is selected.
5. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box.
6. Click **OK**.
7. Right-click **Health Policies**, and then click **New**.
8. In the **Create New Health Policy** dialog box, under **Policy Name**, type **Noncompliant**.
9. Under **Client SHV checks**, select **Client fails one or more SHV checks**.

10. Under **SHVs used in this health policy**, select the **Windows Security Health Validator** check box.
11. Click **OK**.

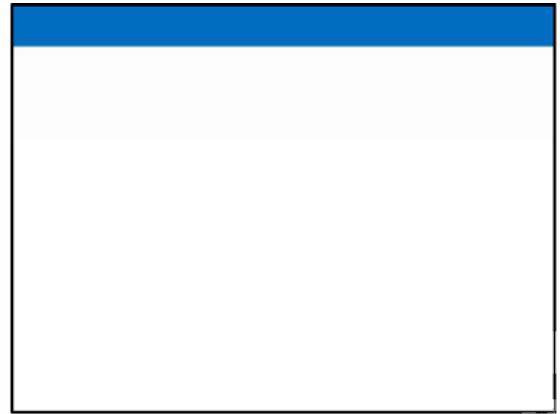
Configure network policies for compliant computers

1. In the navigation pane, under **Policies**, click **Network Policies**.

Note: Important: Disable the two default policies found under Policy Name by right-clicking the policies, and then clicking Disable.

1. Right-click **Network Policies**, and then click **New**.
2. On the **Specify Network Policy Name and Connection Type** page, under **Policy name**, type **Compliant-Full-Access**, and then click **Next**.
3. On the **Specify Conditions** page, click **Add**.
4. In the **Select condition** dialog box, double-click **Health Policies**.
5. In the **Health Policies** dialog box, under **Health policies**, select **Compliant**, and then click **OK**.
6. On the **Specify Conditions** page, click **Next**.
7. On the **Specify Access Permission** page, click **Next**.
8. On the **Configure Authentication Methods** page, clear all check boxes, select the **Perform machine health check only** check box, and then click **Next**.
9. Click **Next** again.
10. On the **Configure Settings** page, click **NAP Enforcement**. Verify that **Allow full network access** is selected, and then click **Next**.
11. On the **Completing New Network Policy** page, click **Finish**.

Configure network policies for noncompliant computers



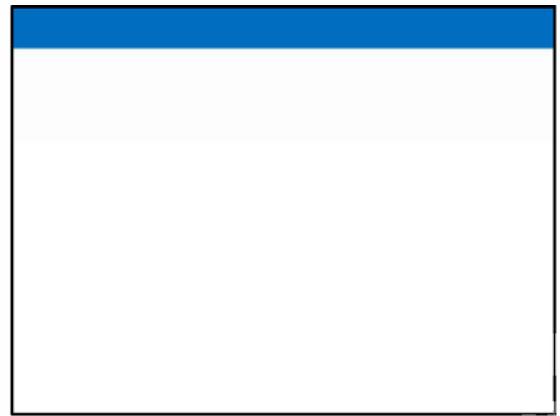
1. Right-click **Network Policies**, and then click **New**.
2. On the **Specify Network Policy Name and Connection Type** page, under **Policy name**, type **Noncompliant-Restricted**, and then click **Next**.
3. On the **Specify Conditions** page, click **Add**.
4. In the **Select condition** dialog box, double-click **Health Policies**.
5. In the **Health Policies** dialog box, under **Health policies**, select **Noncompliant**, and then click **OK**.
6. On the **Specify Conditions** page, click **Next**.
7. On the **Specify Access Permission** page, verify that **Access granted** is selected, and then click **Next**.
8. On the **Configure Authentication Methods** page, clear all check boxes, select the **Perform machine health check only** check box, and then click **Next**.
9. Click **Next** again.
10. On the **Configure Settings** page, click **NAP Enforcement**. Click **Allow limited access**.
11. Clear the **Enable auto-remediation of client computers** check box.
12. Click **Next**, and then click **Finish**.

Configure the DHCP server role for NAP

1. Click **Start**.
2. In Start, click **Administrative Tools**, and then double-click **DHCP**.
3. In DHCP, expand **LON-DC1.Adatum.com**, expand **IPv4**, expand **Scope [172.16.0.0] Adatum**, right-click **Scope [172.16.0.0] Adatum**, and then click **Properties**.
4. In the **Scope [172.16.0.0] Adatum Properties** dialog box, click the **Network Access Protection**

tab, click **Enable for this scope**, and then click **OK**.

5. In the navigation pane, under **Scope [172.16.0.0] Adatum**, click **Policies**.
 6. Right-click **Policies**, and then click **New Policy**.
 7. In the DHCP Policy Configuration Wizard, in the **Policy Name** box, type **NAP Policy**, and then click **Next**.
 8. On the **Configure Conditions for the policy** page, click **Add**.
 9. In the **Add/Edit Condition** dialog box, in the **Criteria** list, click **User Class**.
 10. In the **Operator** list, ensure that the **Equals** option is selected.
 11. In the **Value** list, click **Default Network Access Protection Class**, and then click **Add**.
 12. Click **OK**, and then click **Next**.
 13. On the **Configure settings for the policy** page, select **No**, and then click **Next**.
 14. On the subsequent **Configure settings for the policy** page, in the **Vendor class** list, ensure that **DHCP Standard Options** vendor class is selected.
 15. In the **Available Options** list, select the **006 DNS Servers** check box.
 16. In the **IP address** box, type **172.16.0.10**, and then click **Add**.
 17. In the **Available Options** list, select the **015 DNS Domain Name** check box.
 18. In the **String value** box, type **restricted.adatum.com**, and then click **Next**.
 19. On the **Summary** page, click **Finish**.
 20. Close DHCP.
- 21. Configure client NAP settings**
22. Switch to the LON-CL1 computer, and then sign in as **Adatum\Administrator** with the password



Pa\$\$w0rd.

2. Right-click **Start**, and then click **Command Prompt**.
3. At the command prompt, type **MMC**, and then press Enter.
4. In the MMC labeled Console1, click **File**, and then click **Add/Remove Snap-in**.
5. In the Add or Remove Snap-ins window, click **NAP Client Configuration**, click **Add**, and then click **OK**.
6. In the Add or Remove Snap-ins window, click **OK**.
7. In Console1, in the navigation pane, expand **NAP Client Configuration (Local Computer)**, and then click **Enforcement Clients**.
8. In the results pane, right-click **DHCP Quarantine Enforcement Client**, and then click **Enable**.
9. Close Console1 and do not save any changes.
10. Switch back to the Command Prompt window.
11. At the command prompt, type **Services.msc**, and then press Enter.
12. In Services, in the results pane, double-click **Network Access Protection Agent**.
13. In the **Network Access Protection Agent Properties (Local Computer)** dialog box, in the **Startup** type list, click **Automatic**.
14. Click **Start**, and then click **OK**.
15. Press the Windows key, and then press R to bring up the Run window.
16. On the Run window, type **gpedit.msc**, and then press Enter.
17. In the console tree, under Computer Configuration, expand **Administrative Templates**, expand **Windows Components**, and then click **Security Center**.



18. Double-click **Turn on Security Center (Domain PCs only)**, click **Enabled**, and then click **OK**.
19. Close the console window.
20. Right-click the **Start** menu, and then click **Control Panel**.
21. In Control Panel, click **Network and Internet**.
22. In Network and Internet, click **Network and Sharing Center**.
23. In **Network and Sharing Center**, in the left pane, click **Change adapter settings**.
24. Right-click **Ethernet**, and then click **Properties**.
25. In the **Ethernet Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
26. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, click **Obtain an IP address automatically**.
27. Click **Obtain DNS server address automatically**, and then click **OK**.
28. In the **Ethernet Properties** dialog box, click **OK**.

Test NAP

1. Switch back to the Command Prompt window.
2. At the command prompt, type the following command, and then press Enter:

`Ipconfig`

1. Switch to services.
2. In **Services**, in the results pane, double-click **Windows Firewall**.
3. In the **Windows Firewall Properties (Local Computer)** dialog box, in the **Startup type** list, click **Disabled**.
4. Click **Stop**, and then click **OK**.

5. In the System Tray area, click the **Network Access Protection** pop-up warning. Review the information in the **Network Access Protection** dialog box. Click **Close**.

Note: You may not receive a warning in the System Tray area, depending upon the point at which your computer becomes noncompliant.

1. At the command prompt, type the following command, and then press Enter:

`Ipconfig`

1. Notice that the computer has a subnet mask of 255.255.255.255 and a Domain Name System (DNS) suffix of restricted.Adatum.com. Leave all windows open.

07: Implementing Network Access Protection

Demonstration: Configuring NAP Tracing

In this demonstration, you will see how to:

- Configure tracing from the GUI
- Configure tracing from the command line

Revert all virtual machines.

Preparation Steps

You require the 20411D-LON-DC1 and 20411D-LON-CL1 virtual machines to perform this demonstration. These should already be running from the preceding demonstration.

Demonstration Steps

Configure tracing from the GUI

1. Switch to LON-CL1.
2. At the command prompt, type **MMC**, and then press Enter.
3. In the MMC labeled Console1, click **File**, and then click **Add/Remove Snap-in**.
4. In the Add or Remove Snap-ins window, click **NAP Client Configuration**, click **Add**, and then click **OK**.
5. In the Add or Remove Snap-ins window, click **OK**. In Console1, in the navigation pane, right-click **NAP Client Configuration (Local Computer)** from the console tree, and then click **Properties**.
6. On the **General** tab, click **Enabled**, and in the **Basic** list, click **Advanced**, and then click **OK**.

Configure tracing from the command line

1. Switch to the command prompt.
2. At the command prompt, type the following command, and then press Enter:

```
netsh nap client set tracing state = enable
```

08: Implementing Remote Access

Demonstration: Installing and Managing the Remote Access Role

In this demonstration, you will see how to:

- Install the Remote Access role
- Manage the Remote Access role

After completing this demonstration, revert all virtual machines.

Preparation Steps

Start and sign in to 20411D-LON-DC1, 20411D -LON-SVR1, and 20411D -LON-CL1 with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

Demonstration Steps

Install the Remote Access Role

1. On LON-SVR1, switch to the Server Manager console, click **Manage**, and then click **Add Roles and Features**.
2. On the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, click **Remote Access**, and then click **Next**.
6. On the **Select Features** page, click **Next**.
7. On the **Remote Access** page, click **Next**.
8. On the **Select role services** page, click **DirectAccess and VPN (RAS)**, and in the **Add Roles and Features Wizard** page, click **Add Features**.
9. Verify that **DirectAccess and VPN (RAS)** is selected, and on the **Select role services** page, click **Next**.
10. On the **Confirm installation selections** page, click **Install**, and then when the installation finishes, click **Close**.

Manage the Remote Access Role

1. In the Server Manager console, in the upper-right part of the console, click **Tools**, and then click **Remote Access Management**.

08: Implementing Remote Access

2. In the Remote Access Management Console, review the options for configuring and managing remote access.
3. In the Server Manager console, in the upper-right part of the console, click **Tools**, and then click **Routing and Remote Access**.
4. In the Routing and Remote Access console, review the options for configuring and managing remote access.

08: Implementing Remote Access

Demonstration: Running the Getting Started Wizard

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

After completing this demonstration, do not revert the virtual machines.

Preparation Steps

Sign in to **20411D-LON-DC1**, **20411D-LON-SVR1**, **20411D-LON-RTR**, and **20411D-LON-CL1** with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

Sign in to 20411D-INET1 with the username **Administrator** and the password **Pa\$\$w0rd**.

In order to prepare for this demo, perform following actions:

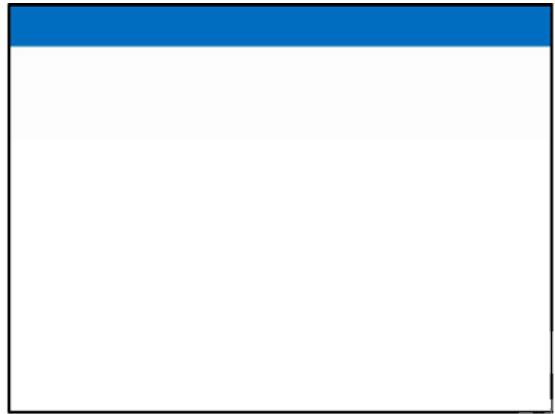
1. In the Routing and Remote Access console, you should disable Routing and Remote Access that was preconfigured for this lab on LON-RTR.
2. On LON-RTR, in the Network Connections window, disable and then again enable the Ethernet network adapter.
3. On LON-RTR, in the Network Connections window, disable and then again enable the Internet network adapter.
4. On LON-RTR, in the Network Connections window, disable the Ethernet 2 network adapter

Demonstration Steps

Create security group for DirectAccess client computers

1. On LON-DC1, from the taskbar, click the Server Manager console.
2. In the Server Manager console, in the upper-right corner, click **Tools**, and then click **Active Directory Users and Computers**.
3. In the Active Directory Users and Computers console tree, right-click **Adatum.com**, click **New**, and then click **Organizational Unit**.
4. In the **New Object – Organizational Unit** dialog box, in the **Name** box, type **DA_Clients OU**, and then click **OK**.
5. In the Active Directory Users and Computers console tree, expand **Adatum.com**, right-click

08: Implementing Remote Access



DA_Clients OU, click **New**, and then click **Group**.

6. In the **New Object - Group** dialog box, in the **Group name** box, type **DA_Clients**.
7. Under Group scope, ensure that **Global** is selected, and under Group type, ensure that **Security** is selected, and then click **OK**.
8. In the details pane, right-click **DA_Clients**, and then click **Properties**.
9. In the **DA_Clients Properties** dialog box, click the **Members** tab, and then click **Add**.
10. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**, select the **Computers** check box, and then click **OK**.
11. In the **Enter the object names to select (examples)** box, type **LON-CL1**, and then click **OK**.
12. Verify that **LON-CL1** is displayed under Members, and then click **OK**.
13. Close the Active Directory Users and Computers console.

Configure DirectAccess by Running the Getting Started Wizard

1. On LON-RTR, on the Start screen, click **Server Manager**.
2. In Server Manager, click **Tools**, and then select **Remote Access Management**.
3. In the Remote Access Management console, under Configuration, click **DirectAccess and VPN**.
4. Click **Run the Getting Started Wizard**.
5. On the **Configure Remote Access** page, click **Deploy DirectAccess only**.
6. Verify that **Edge** is selected, in the **Type the public name or IPv4 address used by clients to connect to the Remote Access server** box, type **131.107.0.10**, and then click **Next**.
7. On the **Configure RemoteAccess** page, click the **here** link.
8. On the **Remote Access Review** page, verify that two GPO objects are created, **DirectAccess Server Settings** and **DirectAccess Client settings**.
9. Click the **Change** link beside **Remote Clients**.

08: Implementing Remote Access

10. Select **Domain Computers (Adatum\Domain Computers)**, and then click **Remove**.
11. Click **Add**, type **DA_Clients**, and then click **OK**, ensure that the **Enable DirectAccess for mobile computers only** check box is cleared, and then click **Next**.
12. On the **Network Connectivity Assistant** page, click **Finish**.
13. On the **Remote Access Review** page, click **OK**.
14. On the **Configure Remote Access** page, click **Finish** to finish the DirectAccess Getting Started Wizard.
15. Click **Close** in the **Applying Getting Started Wizard Settings** dialog box.
16. Restart **LON-RTR**.

08: Implementing Remote Access

Demonstration: Identifying the Getting Started Wizard Settings

In this demonstration, you will see how to identify changes made by the DirectAccess Getting Started Wizard

After completing this demonstration, do not revert the virtual machines.

Preparation Steps

Sign in to **20411D-LON-DC1**, **20411D-LON-SVR1**, **20411D-LON-RTR**, and **20411D-LON-CL1** with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

Sign in to **20411D-INET1** with the username **Administrator** and the password **Pa\$\$w0rd**.

Demonstration Steps

1. On LON-RTR, switch to the Server Manager console, click **Tools**, and then click **Remote Access Management**.
2. In the Remote Access Management console, in the left pane, click **DirectAccess and VPN**.
3. In the Remote Access Setup window, under the image of the client computer labeled as **Step 1 Remote Clients**, click **Edit**.
4. In the DirectAccess Client Setup window, click **Deployment Scenario** and review the default settings; click **Select Groups** and review the default settings; click **Network Connectivity Assistant**, and then review the default settings.
5. Click **Cancel**, and then click **OK**.
6. In the Remote Access Setup window, under the image of the server computer labeled as **Step 2 Remote Access Servers**, click **Edit**.
7. In the Remote Access Server Setup window, click **Network Topology** and record the default settings; click **Network Adapters** and record the default settings; click **Authentication**, and then record the default settings.
8. Click **Cancel**, and then click **OK**.
9. In the Remote Access Setup window, under the image of the server computer labeled as **Step 3 Infrastructure Servers**, click **Edit**.
10. In the Infrastructure Server Setup window, click **Network Location Server** and review the default settings; click **DNS** and review the default settings; click **DNS Suffix Search List** and

08: Implementing Remote Access

review the default settings; click **Management**, and then review the default settings.

11. Click **Cancel**, and then click **OK**.
12. In the Remote Access Setup window, under the image of the server computer labeled as **Step 4 Application Servers**, click **Edit**.
13. In the DirectAccess Application Server Setup window, review the default settings, click **Cancel**, and then click **OK**.
14. Close all open windows.

Review the Infrastructure Changes in the Group Policy Management Console

1. On LON-RTR, click the **Server Manager** icon, click **Tools**, and then click **Group Policy Management**.
2. In the Group Policy Management console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com** and notice two new group policy objects are created: **DirectAccess Client Settings**, and **DirectAccess Server Settings**.
3. In the navigation pane, click the **DirectAccess Server Settings** GPO.
4. In the **Group Policy Management Console** dialog box, click **OK**, and then in the details pane, click the **Settings** tab.
5. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Settings** row, click the **show** link on the right side, and then in the **Windows Firewall with Advanced Security** row, click the **show** link.
6. Notice that there are three groups of firewall settings configured for the DirectAccess servers: **Global Settings**, **Inbound Rules**, and **Connection Security Settings**.
7. In the **Global Settings** row, click the **show** link, and then review the IPsec Internet Control Message Protocol (ICMP) exception setting.
8. In the **Inbound Rules** row, click the **show** link, and then review the following settings:
 - **Core Networking – IPHTTPS (TCP-In)**. This rule allows the inbound Internet Protocol

08: Implementing Remote Access

over Secure Hypertext Transfer Protocol (IP-HTTPS) traffic to provide connectivity across HTTP proxies and firewalls.

- **Domain Name Server (UDP-In), and Domain Name Server (TCP-In).** These rules allow traffic to the DNS64 server that is deployed on the remote access server. Notice the IPv6 address in the rules. It is the address of the **London_Network** adapter on LON-RTR, which can be verified by running the **ipconfig /all** command in the Windows PowerShell® window.
9. In the Connection Security Settings row, click the **show** link, and then in the Rules row, click the **show** link. Review the following settings:
 - **DirectAccess Policy-DaServerToCorpSimplified.** Review the IPv6 address prefixes, and compare them with the IPv6 address prefixes you recorded in step 7 of the previous section in this demonstration. Notice that they are the same prefixes configured in the Getting Started Wizard.
 10. In the Rules row, click the **hide** link.
 11. Under the Connection Security Settings row, in the First Authentication row, click the **show** link, and then review the Kerberos authentication setting.
 12. Repeat step 11 for **Second Authentication, Key Exchange (Main Mode), and Data Protection (Quick Mode).**
 13. In the navigation pane, click the **DirectAccess Client Settings GPO**.
 14. In the **Group Policy Management Console** dialog box, click **OK**, and then in the details pane, click the **Settings** tab.
 15. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Setting** row, click the **show** link on the right side, then in the **Public Key Policies/Trusted Root Certification Authorities** row, click the **show** link, and then in the **Certificates** row, click on the **Show** link. Notice that the GPO is configuring the DirectAccess client computers to trust

08: Implementing Remote Access

the self-signed certificates with the IP address of **131.107.0.10** and the name of **DirectAccess-NLS.Adatum.com**.

16. In the details pane, under **Computer Configuration (Enabled)**, in the **Security Setting** row, and in the Windows Firewall with Advanced Security row, click the **show** link.
17. Notice that there are three groups of firewall settings configured for the DirectAccess clients: **Global Settings**, **Outbound Rules**, and **Connection Security Settings**.
18. In the Global Settings row, click the **show** link, and then review the IPsec ICMP exception setting.
19. In the Outbound Rules row, click the **show** link, and then review the following setting:

16. Core Networking – IPHTTPS (TCP-Out). This rule allows the outbound IP-HTTPS traffic to provide connectivity across HTTP proxies and firewalls.
20. In the Connection Security Settings row, click the **show** link, and then in the Rules row, click the **show** link.
21. Review the three rules, and then compare the IPv6 address prefixes with the IPv6 address prefixes that you recorded in step 7 in the previous section of this demonstration. Notice that they are the same prefixes configured with the Getting Started Wizard.
22. In the Rules row, click the **hide** link.
23. Under the Connection Security Settings row, in the First Authentication row, click the **show** link, and then review the Kerberos authentication setting.
24. Repeat step 23 for **Second Authentication**, **Key Exchange (Main Mode)** and **Data Protection (Quick Mode)**.
25. Close the Group Policy Management Console.
26. On LON-DC1, click the **Server Manager** icon.
27. In Server Manager, click **Tools**, and then click **DNS**.
28. In the Domain Name System (DNS) Manager console, in the navigation pane, expand **Forward Lookup**

08: Implementing Remote Access

Zones, expand **Adatum.com**, and then review the **A** or **AAAA** records for the following hosts: **directaccess-corpConnectivityHost**, **DirectAccess-NLS**, and **directaccess-WebProbeHost**. These records are created by the Getting Started Wizard.

08: Implementing Remote Access

Demonstration: Modifying the DirectAccess Infrastructure

In this demonstration, you will see how to:

- Modify the DirectAccess infrastructure deployed by using the Getting Started Wizard
- Apply advanced configuration settings

After completing the demonstration, do not revert the virtual machines.

Preparation Steps

Sign in to **20411D-LON-DC1**, **20411D-LON-SVR1**, **20411D-LON-RTR**, and **20411D-LON-CL1** with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

Sign in to 20411D-INET1 with the username **Administrator** and the password **Pa\$\$w0rd**.

Demonstration Steps

Configure the Remote Access Role

1. On LON-RTR, in Server Manager, on the **Tools** menu, click **Remote Access Management**.
2. In the Remote Access Management window, click **DirectAccess and VPN**.
3. Click **Edit** on Step 1 to select which clients will use DirectAccess.
4. On the **Deployment Scenario** page, click **Next**.
5. Under Select Groups, in the details pane, ensure that **Enable DirectAccess for mobile computers only** checkbox is cleared, and then click **Next**.
6. On the **Network Connectivity Assistant** page, double-click the empty row under the Resource column.
7. In the Configure Corporate Resources for NCA window, verify that **HTTP** is selected, and then type **https://lon-svr1.adatum.com**. Click **Validate**, and then click **Add**.
8. In the **Network Connectivity Assistant** page, click **Finish** to close configuration for Step 1.
9. Click **Edit** on Step 2.
10. On the **Network Topology** page, verify that **Edge** is selected, and then type **131.107.0.10**.
11. Click **Next**.
12. On the **Network Adapters** page, verify that **Use a self-signed certificate created automatically by DirectAccess** is selected, verify that **CN=131.107.0.10** is used as a certificate to authenticate IP-

08: Implementing Remote Access

HTTPS connections, and then click **Next**.

13. On the **Authentication** page, select **Use computer certificates**, click **Browse**, select **AdatumCA**, and then click **OK**.
14. Select **Enable Windows 7 client computers to connect via DirectAccess**, and then click **Finish** to close configuration for Step 2.
15. In the Remote Access Setup pane, under Step 3, click **Edit**.
16. On the **Network Location Server** page, select **The network location server is deployed on a remote web server (recommended)**, type **https://lon-svr1.adatum.com**, click **Validate**, and then click **Next**.
17. On the **DNS** page, click **Next**.
18. In the **DNS Suffix Search List** page, click **Next**.
19. On the **Management** page, click **Finish** to close configuration for Step 3.
20. Under Step 4, click **Edit**.
21. On the **DirectAccess Application Server Setup** page, click **Finish**.
22. Click **Finish** to apply the changes.
23. In the **Remote Access Review** page, click **Cancel**.

Note: The DirectAccess configuration is not applied because additional prerequisites also need to be configured, such as Active Directory Domain Services (AD DS) configuration, firewall settings, and certificate deployment.

08: Implementing Remote Access

Demonstration: Monitoring and Troubleshooting DirectAccess Connectivity

In this demonstration, you will see how to monitor and troubleshoot DirectAccess connectivity.

After completing the demonstration, do not revert the virtual machines.

Preparation Steps

Sign in to **20411D-LON-DC1**, **20411D-LON-SVR1**, **20411D-LON-RTR**, and **20411D-LON-CL1** with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

Sign in to 20411D-INET1 with the username **Administrator** and the password **Pa\$\$w0rd**.

Demonstration Steps

Verify DirectAccess Group Policy Configuration Settings for Windows 8 Clients

1. Switch to LON-CL1.
2. Restart LON-CL1, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
Open the Command Prompt window, type the following commands, and then press Enter:

```
gpupdate /force  
gpresult /R
```

3. Verify that **DirectAccess Client Settings GPO** is displayed in the list of the Applied Policy objects for the Computer Settings.

Note: If DirectAccess Client Settings GPO is not applied, restart LON-CL1, sign in as **Adatum\Administrator** by using the password **Pa\$\$w0rd**, and then repeat step 2 on LON-CL1.

Move the Client Computer to the Internet Virtual Network

1. Switch to LON-CL1.
2. To move the client from the intranet to the public network, on LON-CL1, to open Control Panel, at the command prompt, type **control**, and then press Enter.
3. In Control Panel, click **Network and Internet**, and then click **Network and Sharing Center**.
4. In the Network and Sharing Center window, click **Change adapter settings**.

08: Implementing Remote Access

5. Right-click **Ethernet**, and then click **Disable**.
6. Right-click **Ethernet 2**, and then click **Enable**.
7. Right-click **Ethernet 2**, and then click **Properties**.
8. In the **Ethernet 2 Properties** dialog box, double-click **Internet Protocol Version 4 (TCP/IPv4)**.
9. In the **Internet Protocol Version 4 (TCP/IPv4) Properties** dialog box, ensure that following is displayed, and then click **OK**.
 - o IP address: **131.107.0.20**
 - o Subnet mask: **255.255.0.0**
 - o Preferred DNS server: **131.107.0.100**
10. In the **Ethernet 2 Properties** dialog box, click **Close**.
11. Close the Network Connections window.

Verify Connectivity to the DirectAccess Server

1. On LON-CL1, open a command prompt, type the following command, and then press Enter:
`ipconfig`
2. Notice the IP address that starts with **2002**. This is an IP-HTTPS address.
3. If you notice that there is no IP address for **iphhttpsinterface**, type the following commands, and then restart the computer and repeat steps 1 and 2:

`Netsh interface teredo set state disabled`

`Netsh interface 6to4 set state disabled`

4. At the command prompt, type the following command, and then press Enter:

`Netsh name show effectivepolicy`

08: Implementing Remote Access



Monitoring DirectAccess Connectivity

1. Switch to LON-RTR.
2. Open the Remote Access Management console, and then in the left pane, click **Dashboard**.
3. Review the information in the central pane, under the DirectAccess and VPN Client Status.
If no information appears, restart LON-CL1, and then repeat steps 2 and 3.
4. In the left pane, click **Remote Client Status**, and then, in the central pane, review the information under the Connected Clients list.
5. In the left pane, click **Reporting**, and then, in the central pane, click **Configure Accounting**.
6. In the Configure Accounting window, under Select Accounting Method, click **Use inbox accounting**, click **Apply**, and then click **Close**.
7. In the central pane, under Remote Access Reporting, review the options for monitoring historical data.

08: Implementing Remote Access

Demonstration: Configuring VPN

In this demonstration, you will see how to:

- Review the default VPN configuration
- Verify certificate requirements for IKEv2 and SSTP
- Configure the remote access server

After completing the demonstration, do not revert the virtual machines.

Preparation Steps

Sign in to for **20411D-LON-DC1**, **20411D-LON-SVR1**, **20411D-LON-RTR**, and **20411D-LON-CL1** with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

Sign in to 20411D-INET1 with the user name **Administrator** and the password **Pa\$\$w0rd**.

Demonstration Steps

Review the Default VPN Configuration

1. Switch to LON-RTR.
2. In Server Manager, on the **Tools** menu, click **Remote Access Management**.
3. In the Remote Access Management Console, click **DirectAccess and VPN**, and then on the Tasks pane, under the **VPN** section, click **Enable VPN**, and in the **Changes not saved** dialog box click **Yes**.
4. On the **Enable VPN** dialog box, click **OK**, and then click **Close**.
5. In Server Manager, on the **Tools** menu, click **Routing and Remote Access**.
6. In the Routing and Remote Access console, expand **LON-RTR**, right-click **Ports** and then click **Properties**.
7. In the Ports Properties window, -click **WAN Miniport (SSTP)** and then click **Configure**. In the **Maximum ports** box, type **5**, and then click **OK**. In the **Routing and Remote Access** message box, click **Yes**.
8. Repeat step 7 for IKEv2, PPTP, and L2TP.
9. To close the **Ports Properties** dialog box, click **OK**.
10. Right-click **LON-RTR**, click **Properties**, and then on the **General** tab, verify that IPv4 Remote

08: Implementing Remote Access



Access Server is selected.

11. Click **Security**, and then verify that Certificate 131.107.0.10 is selected for SSL Certificate Binding.
12. Click **Authentication Methods**, verify that **EAP** is selected as the authentication protocol, and then click **OK**.
13. Click the **IPv4** tab, and verify that the VPN server is configured in **IPv4 address assignment** with **Dynamic Host Configuration Protocol (DHCP)**.
14. To close the LON-RTR **Properties** dialog box, click **OK**.

Verify Certificate Requirements for IKEv2 and SSTP

1. Switch to LON-RTR.
2. On the Start screen, type **mmc**, and then press Enter.
3. On the **File** menu, select **Add or Remove Snap-in**.
4. Select **Certificates**, click **Add**, Select **Computer Account**, and then click **Next**.
5. Verify that Local computer is selected, and then click **Finish**.
6. To close the Add or Remove Snap-in, click **OK**.
7. Expand **Certificates** (Local Computer), expand **Personal**, and then click **Certificates**.
8. Notice that certificate 131.107.0.10 has Intended Purpose for Server Authentication (this is required for SSTP and IKEv2 VPN connectivity).
9. Close the console without saving the changes.

Configure the Remote Access Server

1. On LON-RTR, in Server Manager, on the **Tools** menu, click **Network Policy Server**.
2. In the Network Policy Server console, expand **Policies**, and then click **Network Policies**.
3. In the details pane, right-click the policy at the top of the list, and then click **Disable**.

08: Implementing Remote Access

4. In the details pane, right-click the policy at the bottom of the list, and then click **Disable**.
5. In the navigation pane, right-click **Network Policies**, and then click **New**.
6. In the New Network Policy Wizard, in the **Policy name** box, type **VPN Policy**.
7. In the **Type of network access server** list, click **Remote Access Server(VPN-Dial up)**, and then click **Next**.
8. On the **Specify Conditions** page, click **Add**.
9. In the **Select condition** dialog box, click **Windows Groups**, and then click **Add**.
10. In the **Windows Groups** dialog box, click **Add Groups**.
11. In the **Select Group** dialog box, in the **Enter the object name to select (examples)** box, type **IT**, and then click **OK**.
12. Click **OK** again, click **Next**, on the **Specify Access Permission** page, click **Access granted**, and then click **Next**.
13. On the **Configure Authentication Methods** page, clear the **Microsoft Encrypted Authentication (MS-CHAP)** check box.
14. To add EAP Types, click **Add**.
15. On the **Add EAP** page, select **EAP-MSCHAP v2**, and then click **OK**.
16. To add EAP Types, click **Add**.
17. On the **Add EAP** page, select **Microsoft: Smart Card or other certificate**, and then click **OK**.
18. Click **Next**.
19. On the **Configure Constraints** page, click **Next**.
20. On the **Configure Settings** page, click **Next**.
21. On the **Completing New Network Policy** page, click **Finish**.

08: Implementing Remote Access

Demonstration: How to Create a Connection Profile

In this demonstration, you will see how to:

- Install the CMAK feature
- Create a connection profile
- Examine the profile

After completing the demonstration, do not revert the virtual machines.

Preparation Steps

The required virtual machines **20411D-LON-DC1**, **20411D -LON-RTR**, and **20411D -LON-CL1**, should already be running after the preceding demonstration.

Demonstration Steps

Install the CMAK Feature

1. If necessary, on LON-CL1, sign in as **Adatum\administrator** with the password **Pa\$\$w0rd**.
2. On LON-CL1, click **Start**, on the Start screen, type **Control Panel**, and then press **Enter**.
3. In Control Panel, click **Programs**, and then click **Programs and Features**.
4. In Programs, click **Turn Windows features on or off**.
5. In Windows Features, select the **RAS Connection Manager Administration Kit (CMAK)** check box, and then click **OK**.
6. Click **Close**.

Create a Connection Profile

1. In Control Panel, click **Control Panel Home**.
2. In the **View by** list, click **Large icons**.
3. Click **Administrative Tools**, and then double-click **Connection Manager Administration Kit**.
4. In the Connection Manager Administration Kit Wizard, click **Next**.
5. On the **Select the Target Operating System** page, click **Windows Vista or above**, and then click **Next**.
6. On the **Create or Modify a Connection Manager profile** page, click **New profile**, and then click **Next**.

08: Implementing Remote Access

7. On the **Specify the Service Name and the File Name** page, in the **Service name** text box, type **Adatum HQ**, and in the **File name** text box, type **Adatum**, and then click **Next**.
8. On the **Specify a Realm Name** page, click **Do not add a realm name to the user name**, and then click **Next**.
9. On the **Merge Information from Other Profiles** page, click **Next**.
10. On the **Add Support for VPN Connections** page, select the **Phone book from this profile** check box.
11. In the **VPN server name or IP address** text box, type **131.107.0.10**, and then click **Next**.
12. On the **Create or Modify a VPN Entry** page, click **Next**.
13. On the **Add a Custom Phone Book** page, clear the **Automatically download phone book updates** check box, and then click **Next**.
14. On the **Configure Dial-up Networking Entries** page, click **Next**.
15. On the **Specify Routing Table Updates** page, click **Next**.
16. On the **Configure Proxy Settings for Internet Explorer** page, click **Next**.
17. On the **Add Custom Actions** page, click **Next**.
18. On the **Display a Custom Logon Bitmap** page, click **Next**.
19. On the **Display a Custom Phone Book Bitmap** page, click **Next**.
20. On the **Display Custom Icons** page, click **Next**.
21. On the **Include a Custom Help File** page, click **Next**.
22. On the **Display Custom Support Information** page, click **Next**.
23. On the **Display a Custom License Agreement** page, click **Next**.
24. On the **Install Additional Files with the Connection Manager profile** page, click **Next**.

08: Implementing Remote Access

25. On the **Build the Connection Manager Profile and Its Installation Program** page, click **Next**.
26. On the **Your Connection Manager Profile is Complete and Ready to Distribute** page, click **Finish**.

Examine the Created Profile

1. Open File Explorer.
2. In File Explorer, expand drive **C**, expand **Program Files**, expand **CMAK**, expand **Profiles**, expand **Windows Vista and above**, and then click **Adatum**. These are the files that you must distribute to users.
3. Close all open windows.

08: Implementing Remote Access

Demonstration: Publishing a Secure Website

In this demonstration, you will see how to:

- Install the Web Application Proxy role service
- Configure access to an internal web site
- Disable DirectAccess on a client computer
- Verify access to the internal web site from the client computer

After the module is completed, revert all virtual machines.

Preparation Steps

Sign in to **20411D-LON-DC1**, **20411D-LON-SVR1**, **20411D-LON-SVR4**, **20411D-LON-RTR** and **20411D-LON-CL1** with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

Sign in to **20411D-INET1** **Administrator** and the password **Pa\$\$w0rd**.

Install the Web Application Proxy Role Service

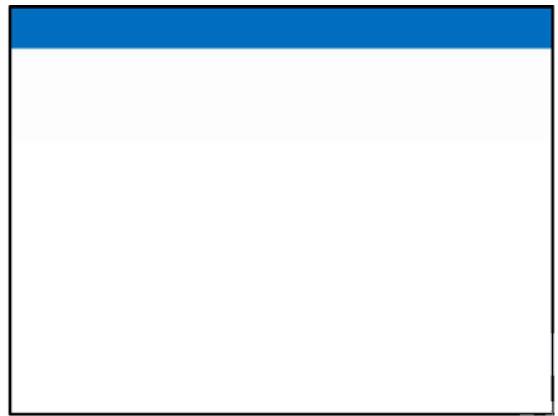
1. Switch to LON-RTR.
2. On the Start screen, click **Server Manager**.
3. On the **Dashboard** page, click **Add roles and features**.
4. In the Add Roles and Features Wizard, click **Next** three times to get to the server role selection page.
5. On the **Select server roles** page, expand **Remote Access (2 of 3 installed)**, select **Web Application Proxy**, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. On the **Installation progress** page, verify that the installation is successful, and then click **Close**.

08: Implementing Remote Access

Obtain Certificate for the ADFS1 Farm

1. On the Start screen, type **cmd**, and then press Enter.
2. In the Command Prompt window, type **mmc**, and then press Enter.
3. In the MMC console, on the **File** menu, click **Add/Remove Snap-In**.
4. In **Add or Remove Snap-ins**, select **Certificates**, click **Add**, select **Computer account**, and then click **Next**.
5. Verify that **Local Computer** is selected, click **Finish**, and then click **OK** to close the Add or Remove Snap-ins window.
6. Expand **Certificates (local Computer)**, **Personal**, and then click **Certificates**.
7. Right-click **Certificates**, select **All Tasks**, and then click **Request new Certificate**.
8. On the **Before You Begin** page, click **Next**.
9. On the **Select Certificate Enrollment Policy** page, click **Next**.
10. Select **Adatum Web Certificate**, and then click **More information is required to enroll for this certificate. Click here to configure settings**.
11. From Subject Name in Type, select **Common Name**, in the **Value** box, type **adfs1.adatum.com**, and then click **Add**.
12. In the **Alternative name** list, select **DNS**; in the **Value** box, type **adfs1.adatum.com**, and then click **Add**.
13. In the **Alternative name** list, select **DNS**; in the **Value** box, type

08: Implementing Remote Access



enterpriseregistration.adatum.com, and then click **Add**.

14. In the **Alternative name** list, select **DNS**; in the **Value** box, type **lon-svr1.adatum.com**, and then click **Add**.
15. To close the **Certificate Properties** dialog box, click **OK**, and then click **Enroll** to proceed with Certificate Enrollment.
16. To close the **Certificate Enrollment** dialog box, click **Finish**.
17. Close all open windows.

Assign a certificate for the Web Site on LON-SVR1

1. In the **Internet Information Services (IIS) Manager** message box, expand **LON-SVR1 (ADATUM\Administrator)**, and then if the **Internet Information Service Manager** message box appears, click **No** to close the message box.
2. In the console tree of Internet Information Services (IIS) Manager, navigate to **LON-SVR1/Sites**, and then click **Default Web site**.
3. In the Actions pane, click **Bindings**, and then click **Add**.
4. In the **Add Site Binding** dialog box, from the **Type** drop-down list select **https**, in the **Host name** box type **lon-svr1.adatum.com**, in the **SSL Certificate** drop-down list, select the certificate with the name **lon-svr1.adatum.com**, click **OK**, and then click **Close**.
5. Close the Internet Information Services (IIS) console.

Configure Web Application Proxy

1. On LON-RTR, in Server Manager, click the **Tools** menu, and then click **Remote Access Management**.
2. In the Remote Access Management console, in the navigation pane, click **Web Application Proxy**.
3. In the middle pane, click **Run the Web Application Proxy Configuration Wizard**.
4. In the Web Application Proxy Configuration Wizard, on the **Welcome** page, click **Next**.

08: Implementing Remote Access

5. On the **Federation Server** page, perform the following steps:
 - In the **Federation service name** box, enter the FQDN of the federation service; **adfs1.adatum.com**.
 - In the **User name** and **Password** boxes, enter **Administrator** and **Pa\$\$w0rd** and then click **Next**.
6. On the **AD FS Proxy Certificate** page, in the list of certificates currently installed on the Web Application Proxy server, select the **adfs1.adatum.com** certificate that will be used by Web Application Proxy for AD FS proxy functionality, and then click **Next**.
7. On the **Confirmation** page, review the settings. If required, you can copy the Windows PowerShell cmdlet to automate additional installations. Click **Configure**.
8. On the **Results** page, verify that the configuration is successful, and then click **Close**.
9. If you receive an error message, switch to **LON-SVR4**, and then ensure that all services that are configured to start automatically are started. If not, start the services manually. Repeat steps from 1 through 8.

Note: If you are not able to start **Device Registration Service**, switch to LON-SVR4 and in **Windows PowerShell** window, type the following cmdlets, and then press **Enter**:

```
update-adfscertificate -CertificateType: Token-Signing -Urgent:$True  
update-adfscertificate -CertificateType: Token-Decrypting -Urgent:$True
```

Restart LON-SVR4 and repeat steps from 1 to 8.

Publish Internal Website

1. On LON-RTR, in the Remote Access Management console, in the navigation pane, click **Web Application Proxy**, and then in the Tasks pane, click **Publish**.
2. In the Publish New Application Wizard, on the **Welcome** page, click **Next**.
3. On the **Preauthentication** page, click **Pass-through**, and then click **Next**.

08: Implementing Remote Access

4. On the **Publishing Settings** page, perform following steps:
 - In the **Name** box, enter a friendly name for the application, **LON-SVR1 Web**.
 - In the **External URL** box, enter the external URL for this application **https://lon-svr1.adatum.com**.
 - In the **External certificate** list, select the certificate **adfs1.adatum.com**.
 - In the **Backend server URL** box, ensure that **https://lon-svr1.adatum.com** is listed, and then click **Next**. Note that this value is automatically entered when you enter the external URL.
5. On the **Confirmation** page, review the settings, and then click **Publish**. You can copy the Windows PowerShell command to set up additional published applications.
6. On the **Results** page, ensure that the application published successfully, and then click **Close**.

Configure Internal Website Authentication

1. Switch to **LON-SVR1**.
2. In Server Manager, from the **Tools** menu, click **Internet Information Services (IIS) Manager**.
3. In the Internet Information Services (IIS) Manager console, expand **LON-SVR1 (ADATUM\Administrator)**, and then if a dialog box appears, click **No**.
4. In the console tree of Internet Information Services (IIS) Manager, navigate to **LON-SVR1/Sites**, and then click **Default Web site**.
5. In the Internet Information Services (IIS) Manager console, in the Default Web Site Home pane, double-click **Authentication**.
6. In the Internet Information Services (IIS) Manager console, in the Authentication pane, right-click **Windows Authentication**, and then click **Enable**.
7. In the Internet Information Services (IIS) Manager console, in the Authentication pane, right-click **Anonymous Authentication**, and then click **Disable**.

08: Implementing Remote Access

8. Close the Internet Information Services (IIS) Manager console.

Disable DirectAccess on Client Computer

1. Switch to LON-CL1.
2. On the Start screen, type **control**, and then press **Enter** to open **Control Panel**.
3. In Control Panel, click **System** and then under Computer name, domain and workgroup settings, click **Change Settings**.
4. In the **System Properties** dialog box, click **Change**.
5. In the **Computer Name/Domain Changes** dialog box, select **Workgroup**, type **WORKGROUP**, click **OK**, and then in **Computer Name/Domain Changes** dialog box click **OK**.
6. If a **Windows Security** dialog box appears, for username type **Administrator**, for password type **Pa\$\$w0rd**, and then click **OK**.
7. In the **Welcome to the WORKGROUP workgroup** dialog box, click **OK**.
8. To restart the computer, click **OK**.
9. To close the **System Properties** dialog box, click **Close**.
10. Click **Restart Now**.

Verify Access to the Internal Website from the Client Computer

1. Switch to LON-CL1.
2. Sign in with the username **Admin** and password **Pa\$\$w0rd**.
3. On the Start screen, click **Internet Explorer**, type the following address **https://lon-svr1.adatum.com** and then press **Enter**
4. In the Internet Explorer window, click **Continue to this website (not recommended)**.

Note: This is expected behavior, because in this lab environment, the LON-SVR1 certificate is not trusted by LON-CL1. In real world scenario, a trusted certificate should be used by the published server.

08: Implementing Remote Access

5. When prompted, in the **Internet Explorer** dialog box, type **Adatum\Bill** for the user name and **Pa\$\$w0rd** for password, and then click **OK** to verify that the default IIS 8.0 web page for LON-SVR1 opens.
6. If you are unable to connect to **https://lon-svr1.adatum.com**, perform the following steps:
 - On LON-CL1, on the Start screen, type **cmd**, and then press **Enter**.
 - In the Command Prompt window, type **regedit**, press **Enter**, and then, in the **User Account Control** dialog box, click **Yes**.
 - In the Registry Editor window, in the navigation pane, navigate to **HKLM\Software\Policies\Microsoft\Windows NT\DNSClient\DNSPolicyConfig**, and then notice the three entries starting with DA.
 - In the Registry Editor window, in the navigation pane, right-click each of the entries starting with DA, click **Delete**, and then in the **Confirm Key Delete** dialog box, click **Yes**.
 - Close the Registry Editor window.
 - Restart **LON-CL1** and perform steps 2 through 4 to verify connectivity to the default IIS 8.0 web page on LON-SVR1.

09: Optimizing File Services

Demonstration: How to Install and Configure FSRM

In this demonstration, you will see how to install and configure FSRM

Keep the virtual machines running for the next demonstration

Preparation Steps

You require the 20411D-LON-DC1 and 20411D-LON-SVR1 virtual machines for this demonstration.

Demonstration Steps

Install the FSRM role service

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
3. In the Add Roles and Features Wizard, click **Next**.
4. Confirm that role-based or feature-based installation is selected, and then click **Next**.
5. Confirm that LON-SVR1.Adatum.com is selected, and then click **Next**.
6. On the **Select server roles** page, expand **File and Storage Services (Installed)**, expand **File and iSCSI Services**, and then select the **File Server Resource Manager** check box.
7. In the pop-up window, click **Add Features**.
8. Click **Next** twice to confirm role service and feature selection.
9. On the **Confirm installation selections** page, click **Install**.
10. When the installation completes, click **Close**.

Specify FSRM configuration options

1. In Server Manager, click **Tools**, and then click **File Server Resource Manager**.
2. In the File Server Resource Manager window, in the navigation pane, right-click **File Server Resource Manager (Local)**, and then click **Configure Options**.
3. In the File Server Resource Manager Options window, click the **File Screen Audit** tab, and then select the **Record file screening activity in auditing database** check box.

09: Optimizing File Services

4. Click **OK** to close the File Server Resource Manager Options window. Close the File System Resource Manager management console.

Use Windows PowerShell® to manage FSRM

1. On the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell command prompt, type the following, and then press Enter.

```
Set-FSRMSetting -SMTPServer "LON-SVR1" –AdminEmailAddress "fileadmin@adatum.com" –FromEmailAddress "fileadmin@adatum.com"
```

1. Close the Windows PowerShell window.
2. Open the File Server Resource Manager management console.
3. In the File Server Resource Manager window, in the navigation pane, right-click **File Server Resource Manager (Local)**, and then click **Configure Options**.
4. On the **Email Notifications** tab, review the configured options to confirm that they are the same as the options specified in the **Set-FSRMSettings** command.
5. Close all open windows.

09: Optimizing File Services

Demonstration: Using FSSRM to Manage Quotas and File Screens, and to Generate On-Demand Storage Reports

In this demonstration, you will see how to:

- Create a quota
- Test a quota
- Create a file screen
- Test a file screen
- Generate a storage report

Ensure students understand the Windows PowerShell commands. Text wrap in the instructions can make one command appear to be two separate commands.

Keep the virtual machines running for the next demonstration.

Preparation Steps

For this demonstration, you will use the 20411D-LON-DC1 and 20411D-LON-SVR1 virtual machines.

Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Create a quota

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. On the taskbar, click the **Server Manager** shortcut.
3. In Server Manager, click **Tools**, and then click **File Server Resource Manager**.
4. In File Server Resource Manager, expand the **Quota Management** node, and then click **Quota Templates**.
5. Right-click the **100 MB Limit** template, and then click **Create quota from template**.
6. In the Create Quota window, click **Browse**.
7. In the Browse for Folder window, expand **Allfiles (E:)**, expand **Labfiles**, expand **Mod09**, click **Data**, and then click **OK**.
8. In the Create Quota window, click **Create**.
9. In the File Server Resource Manager window, click **Quotas** to view the newly created quota.

Test a quota

1. On the taskbar, click the **Windows PowerShell** icon.

09: Optimizing File Services

2. In the Windows PowerShell window, type the following two commands, and then press Enter after each command:

```
cd E:\labfiles\Mod09\data
```

```
Fsutil file createnew largefile.txt 130000000
```

1. Notice that the following message displays: **Error: There is not enough space on the disk.**
2. Close the Windows PowerShell window.

Create a file screen

1. In the File Server Resource Manager window, expand the **File Screening Management** node, and then click **File Screen Templates**.
2. Right-click the **Block Image Files** template, and then click **Create File Screen from Template**.
3. In the Create File Screen window, click **Browse**.
4. In the Browser for Folder window, expand **Allfiles (E:)**, expand **Labfiles**, expand **Mod09**, click **Data**, and then click **OK**.
5. In the Create File Screen window, click **Create**.

Test a file screen

1. Open File Explorer.
2. In the File Explorer window, expand **This PC**, and then expand **Allfiles (E:)**, expand **Labfiles**, and then click **Mod09**.
3. In File Explorer, click the **Home** tab, click **New Item**, and then click **Bitmap Image**.
4. Type **testimage**, and then press Enter.
5. Confirm that the file was successfully created.

09: Optimizing File Services

6. Right-click **testimage**, and then click **Copy**.
7. Right-click **Data**, and then click **Paste**.
8. You will receive a message that you need permission to perform this action. Click **Cancel** to clear the message.
9. Close File Explorer.

Generate a storage report

1. In **File Server Resource Manager**, in the navigation pane, click and right-click **Storage Reports Management**, and then click **Generate Reports Now**.
2. In the Storage Reports Task Properties window, select the **Large Files** check box.
3. Click the **Scope** tab, and then click **Add**.
4. In the Browse for Folder window, click **Allfiles (E:)**, and then click **OK**.
5. In the Storage Reports Task Properties window, click **OK**.
6. In the Generate Storage Reports window, click **OK** to generate the report.
7. In the window that displays, double-click the html file and examine the report.
8. Close the report window.
9. Close the Interactive window.
10. Close the File Server Resource Manager window.
11. Close the Server Manager window.

09: Optimizing File Services

Demonstration: Configuring File Classification

In this demonstration you will see how to:

- Create a classification property
- Create a classification rule

In this demonstration you will create a property value named Corporate Documentation that has a Yes/No value possibility, and then you will create a rule that will set all of the files in the corporate documents folder to have the Corporate Documentation property value set to 'Yes'. Point out that now you can perform other actions on those files, such as assigning a business impact value based on the Corporate Documents property value being set to Yes.

Preparation Steps

The required virtual machines will still be running from the last demonstration.

Demonstration Steps

1. On LON-SVR1, click the **Server Manager** icon on the taskbar. In the Server Manager console, in the upper-right corner, click **Tools**, and then click **File Server Resource Manager**.
2. In File Server Resource Manager, expand **Classification Management**, click and then right-click **Classification Properties**, and then click **Create Local Property**.
3. In the Create Local Classification Property window, in the **Name** field, type **Corporate Documentation**, in the **Property Type** drop-down list box, ensure that Yes/No is selected, and then click **OK**.
4. In File Server Resource Manager, expand **Classification Management**, click **Classification Rules**, and then, in the Action pane, click **Create Classification Rule**.
5. In the Create Classification Rule window, on the **General** tab, in the **Rule name** field, type **Corporate Documents Rule**, and ensure that the **Enable** check box is selected.
6. In the Create Classification Rule window, in the **Scope** tab, click **Add**.
7. In the Browse For Folder window, expand **Allfiles (E:)**, expand **Labfiles**, expand **Mod09**, click the **Corporate Documentation** folder, and then click **OK**.
8. In the Create Classification Rule window, on the **Classification** tab, in the **Classification method** drop-down list box, click **Folder Classifier**. In the **Property-Choose a property to assign to files** drop-down list box, click **Corporate Documentation**, and then, in the **Property-Specify a value** drop-down list box, click **Yes**.

09: Optimizing File Services

9. In the Create Classification Rule window, on the **Evaluation type** tab, click **Re-evaluate existing property values**, ensure that the **Aggregate the values** radio button is selected, and then click **OK**.
10. In File Server Resource Manager, in the Action pane, click **Run Classification With All Rules Now**.
11. In the Run classification window, select the **Wait for classification to complete** radio button, and then click **OK**.
12. Review the **Automatic classification report** that displays in Windows® Internet Explorer®, and ensure that report lists the same number of files classified as in the **Corporate Documentation** folder. There will be two files.
13. Close Internet Explorer.

09: Optimizing File Services

Demonstration: How to Configure File Management Tasks

In this demonstration, you will see how to:

- Create a file management task
- Configure a file management task to expire documents

In this demonstration, you will modify a file in the Data folder to update the date\time stamp of the file. You will create a file management task to find all of the files in the Data folder that have not been modified in 100 days. You will then move the files to the Expired folder.

Preparation Steps

For this demonstration, you will use the 20411D-LON-DC1 and 20411D-LON-SVR1 virtual machines. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Update the Date\Timestamp of a File

1. On LON-SVR1, on the taskbar, click the **File Explorer** shortcut.
2. Navigate to **E:\Labfiles\Mod09\Data** and then open the **April.txt** file. Type your name, and then save and close the file.

Create a File Management Task

1. On LON-SVR1, on the taskbar, click the **Server Manager** shortcut.
2. In Server Manager, click **Tools**, and then click **File Server Resource Manager**.
3. In **File Server Resource Manager**, select and then right-click the **File Management Tasks** node, and then click **Create File Management Task**.
4. In the **Task name** field, type **Expire Documents**.
5. In the **Description** field, type **Move old documents to another folder**.
6. Click the **Scope** tab.
7. In the Scope section, click the **Add** button.
8. Expand **Allfiles (E:)**, expand **Labfiles**, expand **Mod09**, click **Data**, and then click **OK**.

Configure a File Management Task to expire documents

09: Optimizing File Services

1. In the Create File Management Task window, click the **Action** tab.
2. On the **Action** tab, under Type, select **File expiration**.
3. In **Expiration directory**, type **E:\Labfiles\Mod09\Expired**.
4. In the Create File Management Task window, click the **Condition** tab.
5. On the **Condition** tab, select the **Days since file was last modified** check box, and then type **100** in the field.
6. In the Create File Management Task window, click the **Schedule** tab.
7. Select **Monthly**, and then select the **Last** check box.
8. In the Create File Management Task window, click **OK**.
9. Right-click the **Expire Documents** task, and then click **Run File Management Task Now**.
10. In the Run File Management Task window, choose **Wait for task to complete**, and then click **OK**.
11. View the generated report, and confirm that six files were moved. Click the **Expiration directory** link in the report header, and then expand the directories to view the expired files.
12. Open the **E:\Labfiles\Mod09\Data** folder, and view the contents. The **April.txt** file will be the only file left in the folder.
13. Close all open windows.

09: Optimizing File Services

Demonstration: How to Install the DFS Role

In this demonstration, you will see how to install the DFS Role

Preparation Steps

For this demonstration, you will use the 20411D-LON-DC1 and 20411D-LON-SVR1 virtual machines. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Install the DFS role

1. Switch to LON-SVR1.
2. On the taskbar, click **Server Manager**.
3. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
4. In the Add Roles and Features Wizard, click **Next**.
5. On the **Select installation type** page, click **Next**.
6. On the **Select destination server** page, click **Next**.
7. On the **Select server roles** page, expand **File and Storage Services**, expand **File and iSCSI Services**, and then select the **DFS Namespaces** check box.
8. In the Add Roles and Features pop-up window, click **Add Features**.
9. Select the **DFS Replication** check box, and then click **Next**.
10. On the **Select features** page, click **Next**.
11. On the **Confirm installation selections** page, click **Install**.
12. When the installation completes, click **Close**.
13. Close Server Manager.

09: Optimizing File Services

Demonstration: How to Create Namespaces

In this demonstration, you will see how to:

- Create a new namespace
- Create a new folder and folder target

Preparation Steps

For this demonstration, you will use the 20411D-LON-DC1 and 20411D-LON-SVR1 virtual machines. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Create a new namespace

1. Switch to LON-SVR1.
2. On the taskbar, click the **Server Manager** shortcut.
3. In Server Manager, click **Tools**, and then click **DFS Management**.
4. In the **DFS Management** console, click **Namespaces**.
5. Right-click **Namespaces**, and then click **New Namespace**.
6. In the New Namespace Wizard, on the **Namespace Server** page, under Server, type **LON-SVR1**, and then click **Next**.
7. On the **Namespace Name and Settings** page, under Name, type **Research**, and then click **Next**.
8. On the **Namespace Type** page, ensure that both **Domain-based namespace** and **Enable Windows Server 2008 mode** are selected, and then click **Next**.
9. On the **Review Settings and Create Namespace** page, click **Create**.
10. On the **Confirmation** page, verify that the create namespace task is successful, and then click **Close**.
11. In the console, expand the **Namespace** node, and then click **\Adatum.com\Research**. Review the four tabs in the details pane.
12. In the console, right-click **\Adatum.com\Research**, and then click **Properties**. Review the options on the **General**, **Referrals**, and **Advanced** tabs.

09: Optimizing File Services

13. Click **OK** to close the **\Adatum.com\Research Properties** dialog box.

Create a new folder and folder target

1. In the DFS Management console, right-click **\Adatum.com\Research**, and then click **New Folder**.
2. In the **New Folder** dialog box, under Name, type **Proposals**.
3. In the **New Folder** dialog box, under Folder targets, click **Add**.
4. In the **Add Folder Target** dialog box, type **\LON-SVR1\Proposal_docs**, and then click **OK**.
5. In the **Warning** dialog box, click **Yes** to create the shared folder.
6. On the **Create Share** dialog box, configure the following, and then click **OK**.
 - Local path of shared folder: **C:\Proposal_docs**
 - Shared folder permissions: **Administrators have full access; other users have read and write permissions**
1. In the **Warning** dialog box, click **Yes** to create the folder.
2. Click **OK** to close the **New Folder** dialog box.
3. In the console, expand **\Adatum.com\Research**, and then click **Proposals**. Notice that currently there is only one **Folder Target**. To provide redundancy, a second folder target may be added with **DFS Replication** configured.

To test the namespace, open File Explorer, and, in the address bar, type **\Adatum.com\Research**, and then press Enter. The Proposals folder displays.

09: Optimizing File Services

Demonstration: How to Configure DFS Replication

In this demonstration, you will see how to:

- Create a new folder target for replication
- Create a new replication group

Preparation Steps

For this demonstration, you will use the 20411D-LON-DC1, 20411D-LON-SVR1 and 20411D-LON-SVR4 virtual machines. Sign in to all virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Before you complete this demonstration, install DFS Replication on LON-SVR4. You can use the steps in Lab B, Exercise 1, Task 2, if needed.

Demonstration Steps

Create a new folder target for replication

1. Switch to LON-SVR1.
2. In DFS Management, right-click the **Proposals** folder, and then click **Add Folder Target**.
3. In the **New Folder Target** dialog box, type **\LON-SVR4\Proposal_docs**, and then click **OK**.
4. In the **Warning** dialog box, click **Yes** to create the shared folder.
5. On the **Create Share** dialog box, in the **Local path of shared folder** field, type **C:\Proposal_docs**.
6. In the **Shared folder permissions** field, select **Administrators have full access; other users have read and write permissions**, and then click **OK**.
7. In the **Warning** dialog box, click **Yes** to create the folder.
8. In the **Replication** dialog box, click **Yes** to create a replication group. The Replicate Folder Wizard starts.

Create a new replication group

1. In **DFS Management**, in the Replicate Folder Wizard, on the **Replication Group and Replicated Folder Name** page, accept the default settings, and then click **Next**.
2. On the **Replication Eligibility** page, take note that LON-SVR4 and LON-SVR1 are both eligible as DFS Replication members, and then click **Next**.
3. On the **Primary Member** page, select **LON-SVR1** as the primary member, and then click **Next**.

(More notes on the next slide)

4. On the **Topology Selection** page, leave the default selection of Full mesh, which will replicate all

09: Optimizing File Services

data between all members of the replication group.

5. **Note:** If you had three or more members within the replication group, you can also choose Hub and spoke, which allows you to configure a publication scenario where data is replicated from a common hub to the rest of the members. You can also choose No topology, which allows you to configure the topology at a later time.
6. Upon reviewing all the selections, click **Next**.
7. On the **Replication Group Schedule and Bandwidth** page, leave the default selection of Replicate continuously, and then configure the setting to use **Full bandwidth**. Note that you can also schedule replication to occur during specified days and times. Click **Next**.
8. On the **Review Settings and Create Replication Group** page, click **Create**.
9. On the **Confirmation** page, ensure that all tasks are successful, and then click **Close**. Take note of the **Replication Delay** warning, and then click **OK**.
10. In the console, expand **Replication**.
11. Under Replication, click **Adatum.com\research\proposals**. Click and review each of the tabs in the details pane.

10: Configuring Encryption and Advanced Auditing

Demonstration: Configuring BitLocker

In this demonstration, you will see how to

- Edit Group Policy to configure BitLocker
- Add the BitLocker Drive Encryption feature
- Turn on BitLocker and then validate that BitLocker is encrypting the data volume

Run Active Directory Users and Computers, find the computer object for LON-SVR1, and then go to the BitLocker Recovery tab. Show students the recovery information on the tab. Mention that this is stored in Active Directory® Domain Services (AD DS) because of the Group Policy settings that were enabled as part of the demonstration.

Preparation Steps

To perform this demonstration, you will need the 20411D-LON-DC1 and **20411D-LON-SVR1** virtual machines. Start the virtual machines before the demonstration.

Edit Group Policy to configure BitLocker

1. Log in to LON-DC1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, click **Tools**, and then click **Group Policy Management**.
3. In Group Policy Management Console, double-click **Forest: Adatum.com**, double-click **Domains**, double-click **Adatum.com**, expand **Group Policy Objects**, right-click the **Default Domain Policy**, and then click **Edit**.
4. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **Windows Components**, expand **BitLocker Drive Encryption**, and then click **Fixed Data Drives**.
5. In the right pane, double-click the **Choose how BitLocker-protected fixed drives can be recovered** setting.
6. In the Choose how BitLocker-protected fixed drives can be recovered window, click **Enabled**, ensure that the checkbox next to the **Save BitLocker recovery information to AD DS for fixed data drives** option is selected, click the **Do not enable BitLocker until recovery information is stored to AD DS for fixed data drives** option, and then click **OK**.
7. Close the Group Policy Management Console and the Group Policy Management Editor.
8. Switch to LON-SVR1.

10: Configuring Encryption and Advanced Auditing

9. Log in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
10. On the taskbar, click **Windows PowerShell**.
11. At the Windows PowerShell command prompt, run the **gpupdate /force** command.
12. Restart LON-SVR1.

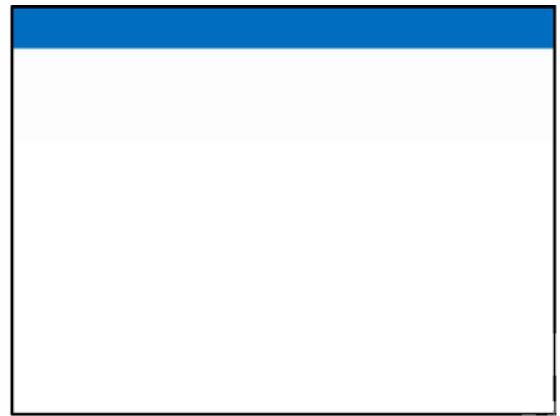
Add the BitLocker Drive Encryption feature

1. Log in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. In Server Manager, click **Manage**, and then click **Add Roles and Features**.
3. In the Before you begin window, click **Next**.
4. In the Select installation type window, click **Next**.
5. In the Select destination server window, click **Next**.
6. In the Select server roles window, click **Next**.
7. In the Select features window, click **BitLocker Drive Encryption**. In the Add features that are required for BitLocker Drive Encryption window, click **Add Features**, and then click **Next**.
8. In the Confirm installation selections window, click **Restart the destination server automatically if required**, click **Yes** in the warning dialog box, and then click **Install**.
9. After the restart, log in to the LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**. In the Add Roles and Features Wizard, note the successful installation of the feature, and then click **Close**.

Turn on BitLocker and then validate that BitLocker is encrypting the data volume

1. Go to Control Panel, and then type **BitLocker** in the **Search Control Panel** search box.
2. In the search results, click **BitLocker Drive Encryption**. If BitLocker Drive Encryption does not appear in the search results, click the **Windows PowerShell** icon on the taskbar, run the **gpupdate /force** command, and then restart LON-SVR1. Then, start again from Step 1.
3. In the BitLocker Drive Encryption window, click the Down Arrow icon, next to the drive F, and then
(More notes on the next slide)

10: Configuring Encryption and Advanced Auditing



click **Turn on BitLocker**.

4. In the Choose how you want to unlock this drive window, click **Use a password to unlock the drive**, type and confirm the password **Pa\$\$w0rd**, and then click **Next**.
5. In the How do you want to back up your recovery key window, click **Save to a file**.
6. In the Save BitLocker recovery key as window, navigate to **E:\Labfiles\Mod10**, and then click **Save**.
7. In the **BitLocker Drive Encryption** dialog box, click **Yes** to save the recovery key to the computer.
8. Click **Next** after the recovery key is saved to the file.
9. In the Are you ready to encrypt this drive window, click **Start encrypting**.
10. Click **Close** when the encryption is complete.
11. On the taskbar, click the **Windows PowerShell** button.
12. At the Windows PowerShell command prompt, run the **manage-bde -status** command to view the current status. The F: volume should show "Protection On" as the protection status.

10: Configuring Encryption and Advanced Auditing

Demonstration: Encrypting a File by Using EFS

In this demonstration, you will see how to:

- Verify that a computer account supports EFS on a network share
- Use EFS to encrypt a file on a network share
- View the certificate used for encryption
- Test access to an encrypted file

Preparation Steps

Start the **20411D-LON-DC1** and **20411D-LON-CL1** virtual machines. Log in to **20411D-LON-DC1** as **Adatum\Administrator** with the password of **Pa\$\$w0rd**. Do not log in to **20411D-LON-CL1** until directed to do so.

Demonstration Steps

Verify that a computer account supports EFS on a network share

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. In Active Directory Users and Computers, if necessary, expand **Adatum.com**, and then click **Domain Controllers**.
3. Right-click **LON-DC1**, and then click **Properties**.
4. In the **LON-DC1 Properties** dialog box, on the **Delegation** tab, verify that **Trust this computer for delegation to any service (Kerberos only)** is selected, and then click **Cancel**. This setting is on by default for domain controllers, but needs to be enabled for most file servers to support EFS.
5. Close Active Directory Users and Computers.

Use EFS to encrypt a file on a network share

1. On LON-CL1, log in as **Adatum\Doug** with a password of **Pa\$\$w0rd**.
2. On the **Start** screen, type **\LON-DC1\Mod10Share**, and then press Enter.
3. In File Explorer, right-click an open area, point to **New**, and then click **Microsoft Word Document**.
4. Type **MyEncryptedFile**, and then press Enter to name the file.
5. Double-click **MyEncryptedFile** to open it.
6. If necessary, click **Close** in the Microsoft Office Activation Wizard, click **Ask me later** on the First things first window about update installations, and then click **Accept to close the window**.

10: Configuring Encryption and Advanced Auditing

7. On the Welcome to your new Office window, click the **X** icon in the upper right corner of the windows to close it.
8. In the document, type **My secret data**, and then click the **Save** button.
9. Close Microsoft Word.
10. Right-click **MyEncryptedFile**, and then click **Properties**.
11. In the **MyEncryptedFile Properties** dialog box, on the **General** tab, click **Advanced**.
12. In the **Advanced Attributes** dialog box, select the **Encrypt contents to secure data** check box, and then click **OK**.
13. In the **MyEncryptedFile Properties** dialog box, click **OK**.
14. Sign out of LON-CL1.

View the certificate used for encryption

1. On LON-DC1, in the File Explorer window, expand drive **C**, and then expand **Users**. Notice that Doug has a profile on the computer. This is where the self-signed certificate is stored. It cannot be viewed in the Microsoft Management Console (MMC) Certificates snap-in unless Doug logs on locally to the server.
2. In the File Explorer window, type **C:\Users\Doug\AppData**, and then press Enter.
3. Expand **Roaming**, expand **Microsoft**, expand **SystemCertificates**, expand **My**, and then expand **Certificates**. This is the folder that stores the self-signed certificate for Doug.

Test access to an encrypted file

1. On LON-CL1, log in as **Adatum\Alex** with a password of **Pa\$\$w0rd**.
2. On the **Start** screen, type **\LON-DC1\Mod10Share**, and then press Enter.
3. Double-click **MyEncryptedFile**.
4. Click **OK** to clear the access denied message.

10: Configuring Encryption and Advanced Auditing

5. In the Microsoft Office Activation Wizard dialog box, click **Close**.
6. In the First things first window, click **Ask me later**, and then click **Accept**.
7. In the Welcome to your new Office window, click the **X** icon in the upper right corner to close the window.
8. Close Microsoft Word.

10: Configuring Encryption and Advanced Auditing

Demonstration: Configuring Advanced Auditing

In this demonstration, you will see how to create and edit a GPO for audit policy configuration

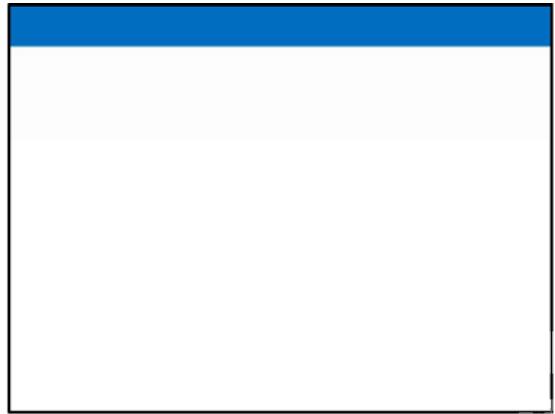
Preparation Steps

To perform this demonstration, you will need the **20411D-LON-DC1** virtual machine. This machine should be running from the previous demonstration.

Demonstration Steps

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In Group Policy Management, double-click **Forest: Adatum.com**, double-click **Domains**, double-click **Adatum.com**, right-click **Group Policy Objects**, and then click **New**.
3. In the New GPO window, type **File Audit** in the Name field, and then press Enter.
4. Double-click the **Group Policy Objects** container, right-click **File Audit**, and then click **Edit**.
5. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Advanced Audit Policy Configuration**, expand **Audit Policies**, and then click **Object Access**.
6. Double-click **Audit Detailed File Share**.
7. In the Properties window, select the **Configure the following audit events** check box.
8. Select the **Success** and **Failure** check boxes, and then click **OK**.
9. Double-click **Audit Removable Storage**.
10. In the Properties window, select the **Configure the following audit events** check box.
11. Select the **Success** and **Failure** check boxes, and then click **OK**.
12. Close the Group Policy Management Editor.
13. Close Group Policy Management.

11: Deploying and Maintaining Server Images



List the features enabled on an image

1. Note the name of the image in the .wim file: **Windows Server 2012 R2 SERVERSTANDARDCORE**.
2. At the command prompt, type the following commands, pressing **Enter at the end of each line**:

MD Offline

```
Dism /Mount-WIM /WimFile:install.wim /Name:"Windows Server 2012 R2 SERVERSTANDARDCORE" /MountDir:E:\Offline
```

Enable a feature on an image.

1. To view the features currently installed on the image, at the command prompt, type the following command, and then press **Enter**:

```
Dism /Image:E:\Offline /Get-Features
```

2. To install the Telnet Server role on the image, type the following in the command, and then press **Enter**:

Note: The source files are required to install this specific feature

```
Dism /Image:E:\Offline /Enable-Feature /FeatureName:TelnetServer
```

3. To save the changes that you made to the image, type the following at the command prompt, and then press **Enter**:

```
Dism /Unmount-WIM /MountDir:E:\Offline /Commit
```

11: Deploying and Maintaining Server Images



List the features enabled on an image

1. Note the name of the image in the .wim file: **Windows Server 2012 R2 SERVERSTANDARDCORE**.
2. At the command prompt, type the following commands, pressing **Enter at the end of each line**:

MD Offline

```
Dism /Mount-WIM /WimFile:install.wim /Name:"Windows Server 2012 R2 SERVERSTANDARDCORE" /MountDir:E:\Offline
```

Enable a feature on an image.

1. To view the features currently installed on the image, at the command prompt, type the following command, and then press **Enter**:

```
Dism /Image:E:\Offline /Get-Features
```

2. To install the Telnet Server role on the image, type the following in the command, and then press **Enter**:

Note: The source files are required to install this specific feature

```
Dism /Image:E:\Offline /Enable-Feature /FeatureName:TelnetServer
```

3. To save the changes that you made to the image, type the following at the command prompt, and then press **Enter**:

```
Dism /Unmount-WIM /MountDir:E:\Offline /Commit
```

11: Deploying and Maintaining Server Images

Demonstration: How to Administer Images

In this demonstration, you will see how to:

- Install and configure the Windows Deployment Services role.
- Add a boot image.
- Add an install image.

Preparation Steps

For this demonstration, you require the **220411D-LON-DC1** and **20411D-LON-SVR1** virtual machines. Log on to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

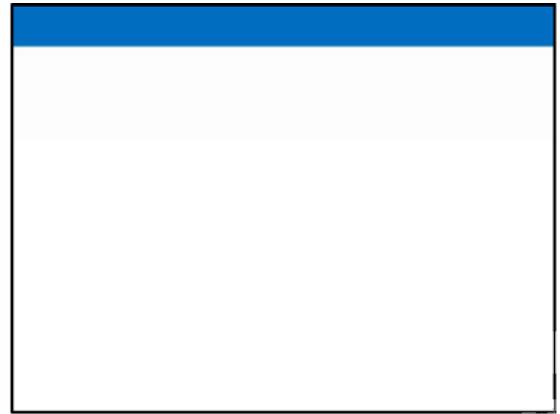
You also must have **D:\Program Files\Microsoft Learning\20411\Drives\Windows2012R2.iso** mounted to the virtual DVD Drive on **20411D-LON-SVR1**.

Demonstration Steps

Install and configure the Windows Deployment Services role

1. Switch to **LON-SVR1**.
2. In **Server Manager**, click **Manage**, and then click **Add Roles and Features**.
3. In the **Add Roles and Features Wizard**, click **Next**.
4. On the **Select installation type** page, click **Next**.
5. On the **Select destination server** page, click **Next**.
6. On the **Select server roles** page, select the **Windows Deployment Services** check box.
7. In the **Add Roles and Features Wizard**, click **Add Features**.
8. On the **Select server roles** page, click **Next**.
9. On the **Select features** page, click **Next**.
10. On the **WDS** page, review the information presented, and then click **Next**.
11. On the **Select role services** page, click **Next**.
12. On the **Confirm installation selections** page, click **Install**.
13. On the **Installation Results** page, click **Close**.
14. In **Server Manager**, click **Tools**, and then click **Windows Deployment Services**.
15. In the **Windows Deployment Services** console, expand **Servers**.

11: Deploying and Maintaining Server Images



16. Right-click **LON-SVR1.Adatum.com**, click **Configure Server**, and then click **Next**.
17. On the **Install Options** page, click **Next**.
18. On the **Remote Installation Folder Location** page, click **Next**.
19. In the **System Volume Warning** dialog box, click **Yes**.
20. On the **PXE Server Initial Settings** page, click **Respond to all client computers (known and unknown)**, and then click **Next**.
21. On the **Operation Complete** page, clear the **Add images to the server now** check box, and then click **Finish**.

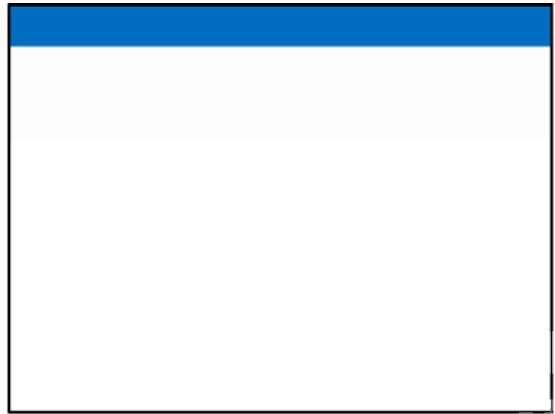
Add a boot image

1. In **Windows Deployment Services**, in the console tree, expand **LON-SVR1.Adatum.com**.
2. Right-click **Boot Images**, and then click **Add Boot Image**.
3. In the **Add Image Wizard**, on the **Image File** page, click **Browse**.
4. In the **Select Windows Image File** dialog box, in the navigation pane, click **This PC**, double-click **DVD Drive (D:)**, double-click **sources**, and then double-click **boot.wim**.
5. On the **Image File** page, click **Next**.
6. On the **Image Metadata** page, click **Next**.
7. On the **Summary** page, click **Next**.
8. On the **Task Progress** page, click **Finish**.

Add an install image

1. In the Windows Deployment Services console, right-click **Install Images**, and then click **Add Image Group**.
2. In the **Add Image Group** dialog box, in the **Enter a name for the image group** text box, type

11: Deploying and Maintaining Server Images



Windows Server 2012 R2, and then click **OK**.

3. In the Windows Deployment Services console, right-click **Windows Server 2012 R2**, and then click **Add Install Image**.
4. In the Add Image Wizard, on the **Image File** page, click **Browse**.
5. In the **File name** text box, type **D:\sources\install.wim**, and then click **Open**.
6. On the **Image File** page, click **Next**.
7. On the **Available Images** page, under the list of available images, clear all check boxes, select the **Windows Server 2012 R2 SERVERSTANDARDCORE** check box, and then click **Next**.
8. On the **Summary** page, click **Next**.
9. On the **Task Progress** page, click **Finish**.
10. Minimize the Windows Deployment Services window.

11: Deploying and Maintaining Server Images

Windows Deployment Services

To automate the Windows Setup process:

1. Create the Unattend.xml file
2. Copy the file to the Windows Deployment Services server
3. View the properties of the appropriate install image
4. Enable unattended mode and select the answer file

In this demonstration, you will see how to configure multicast transmission

Preparation Steps

For this demonstration, you require the **20411D-LON-DC1** and **20411D-LON-SVR1** virtual machines.

Log on to **LON-SVR1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

1. On LON-SVR1, in Windows Deployment Services, in the console tree, right-click **Multicast Transmissions**, and then click **Create Multicast Transmission**.
2. In the Create Multicast Transmission Wizard, on the **Transmission Name** page, in the **Type a name for this transmission** text box, type **Windows Server 2012 R2 Branch Servers**, and then click **Next**.
3. On the **Image Selection** page, in the **Select the image group that contains the image list**, click **Windows Server 2012 R2**.
4. In the **Name** list, click **Windows Server 2012 R2 SERVERSTANDARDCORE**, and then click **Next**.
5. On the **Multicast Type** page, verify that **Auto-Cast** is selected, and then click **Next**.
6. Click **Finish**.

When you finish the demonstration, revert the virtual machines to their initial state

1. On the host computer, start Hyper-V Manager.
2. In the **Virtual Machines** list, right-click **20411D-LON-DC1**, and then click **Revert**.
3. In the **Revert Virtual Machine** dialog box, click **Revert**.
4. Repeat these steps for **20411D-LON-SVR1**.

12: Implementing Update Management

Demonstration: Deploying Updates by Using WSUS

In this demonstration, you will learn how to:

- Approve an update
- Deploy an update

Preparation Steps

20411D-LON-DC1 and 20411D-LON-SVR1 are required to complete this demonstration. Sign in to the virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

1. On LON-SVR1, open the Windows Server Update Services console.
2. In Windows Server Update Services, under Updates, click **All Updates**, right-click **Update for Microsoft Office 2013 (KB2760267), 32-bit Edition**, and then click **Approve**.
3. In the Approve Updates window, in the **All Computers** drop-down list box, select **Approved for Install**.
4. Click **OK**, and then click **Close**.
5. Verify that the Approval column shows **Install**.
6. Close the Update Services console.

13: Monitoring Windows Server 2012

Demonstration: Capturing Counter Data with a Data Collector Set

In this demonstration, you will see how to:

- Create a data collector set
- Create a disk load on the server
- Analyze the resulting data in a report

Leave the virtual machines running for subsequent demonstrations.

Preparation Steps

You require the 20411D-LON-DC1 and 20411D-LON-SVR1 virtual machines for this demonstration.

Demonstration Steps

Create a data collector set

1. Switch to the LON-SVR1 computer.
2. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Click **Start**, and then type **Perf** in the search box.
4. In the **Apps** list, click **Performance Monitor**.
5. In Performance Monitor, in the navigation pane, expand **Data Collector Sets**, and then click **User Defined**.
6. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
7. In the Create New Data Collector Set Wizard, in the **Name** box, type **LON-SVR1 Performance**.
8. Click **Create manually (Advanced)**, and then click **Next**.
9. On the **What type of data do you want to include?** page, select the **Performance counter** check box, and then click **Next**.
10. On the **Which performance counters would you like to log?** page, click **Add**.
11. In the **Available counters** list, expand **Processor**, click **% Processor Time**, and then click **Add >>**.
12. In the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add >>**.
13. In the **Available counters** list, expand **PhysicalDisk**, click **% Disk Time**, and then click **Add >>**.
14. Click **Avg. Disk Queue Length**, and then click **Add >>**.

13: Monitoring Windows Server 2012

15. In the **Available counters** list, expand **System**, click **Processor Queue Length**, and then click **Add >>**.
16. In the **Available counters** list, expand **Network Interface**, click **Bytes Total/sec**, click **Add >>**, and then click **OK**.
17. On the **Which performance counters would you like to log?** page, in the **Sample interval** box, type **1**, and then click **Next**.
18. On the **Where would you like the data to be saved?** page, click **Next**.
19. On the **Create the data collector set?** page, click **Save and close**, and then click **Finish**.
20. In Performance Monitor, in the results pane, right-click **LON-SVR1 Performance**, and then click **Start**.

Create a disk load on the server

1. On the taskbar, click the **Windows PowerShell** icon.
2. At the Windows PowerShell® prompt, type the following command, and then press Enter:

```
Fsutil file createnew bigfile 104857600
```

3. At the command prompt, type the following command, and then press Enter:

```
Copy bigfile \\LON-dc1\c$
```

4. At the command prompt, type the following command, and then press Enter:

```
Copy \\LON-dc1\c$\bigfile bigfile2
```

5. At the command prompt, type the following command, and then press Enter:

```
Del bigfile*.*
```

6. At the command prompt, type the following command, and then press Enter:

13: Monitoring Windows Server 2012



Del \\LON-dc1\c\$\bigfile*.*

7. Close the command prompt.

Analyze the resulting data in a report

1. Switch to Performance Monitor.
2. In the navigation pane, right-click **LON-SVR1 Performance**, and then click **Stop**.
3. In Performance Monitor, in the navigation pane, click **Performance Monitor**.
4. On the toolbar, click **View log data icon**.
5. In the **Performance Monitor Properties** dialog box, on the **Source** tab, click **Log files**, and then click **Add**.
6. In the **Select Log File** dialog box, double-click **Admin**.
7. Double-click **LON-SVR1 Performance**, double-click the **LON-SVR1_date-000001** folder, and then double-click **DataCollector01.blg**.
8. Click the **Data** tab, and then click **Add**.
9. In the **Add Counters** dialog box, in the **Available counters** list, expand **Memory**, click **Pages/sec**, and then click **Add >>**.
10. Expand **Network Interface**, click **Bytes Total/sec**, and then click **Add >>**.
11. Expand **PhysicalDisk**, click **%Disk Time**, and then click **Add >>**.
12. Click **Avg. Disk Queue Length**, and then click **Add >>**.
13. Expand **Processor**, click **%Processor Time**, and then click **Add >>**.
14. Expand **System**, click **Processor Queue Length**, click **Add >>**, and then click **OK**.
15. In the **Performance Monitor Properties** dialog box, click **OK**.
16. On the toolbar, on the **Change graph type** icon, click the down arrow, and then click **Report**.

13: Monitoring Windows Server 2012

Demonstration: Configuring an Alert

In this demonstration, you will see how to:

- Create a data collector set with an alert counter
- Generate a server load that exceeds the configured threshold
- Examine the event log for the resulting event

Leave the virtual machines running for subsequent demonstrations.

Preparation Steps

The required virtual machines, 20411D-LON-DC1 and 20411D-LON-SVR1, should be running after the preceding demonstration.

Demonstration Steps

Create a data collector set with an alert counter

1. On LON-SVR1 computer, in Performance Monitor, in the navigation pane, expand **Data Collector Sets**, and then click **User Defined**.
2. Right-click **User Defined**, point to **New**, and then click **Data Collector Set**.
3. In the **Create New Data Collector Set Wizard**, in the **Name** box, type **LON-SVR1 Alert**.
4. Click **Create manually (Advanced)**, and then click **Next**.
5. On the **What type of data do you want to include?** page, click **Performance Counter Alert**, and then click **Next**.
6. On the **Which performance counters would you like to monitor?** page, click **Add**.
7. In the **Available counters** list, expand **Processor**, click **%Processor Time**, click **Add >**, and then click **OK**.
8. On the **Which performance counters would you like to monitor?** page, in the **Alert when** list, click **Above**.
9. In the **Limit** box, type **10**, and then click **Next**.
10. On the **Create the data collector set?** page, click **Finish**.
11. In the navigation pane, expand the **User Defined** node, and then click **LON-SVR1 Alert**.
12. In the results pane, right-click **DataCollector01**, and then click **Properties**.

13: Monitoring Windows Server 2012

13. In the **DataCollector01 Properties** dialog box, in the **Sample interval** box, type **1**, and then click the **Alert Action** tab.
14. Select the **Log an entry in the application event log** check box, and then click **OK**.
15. In the navigation pane, right-click **LON-SVR1 Alert**, and then click **Start**.

Generate a server load that exceeds the configured threshold

1. At the Windows PowerShell prompt, type the following commands, and then press Enter after each command:

C:

Cd \Labfiles

2. At the Windows PowerShell prompt, type the following commands, and then press Enter:

.\StressTool.exe 95

3. Wait one minute to allow generation of alerts.
4. Press Ctrl+C.
5. Close the command prompt.

Examine the event log for the resulting event

1. Click **Start**, and on the **Start** screen, type **Event**, and then in the **Apps** list, click **Event Viewer**.
2. In Event Viewer, in the navigation pane, expand **Applications and Services Logs**, expand **Microsoft**, expand **Windows**, expand **Diagnosis-PLA**, and then click **Operational**.
3. Examine the log for performance-related messages. These have an Event ID of 2031. Leave Event Viewer running.

13: Monitoring Windows Server 2012

Demonstration: Viewing Reports in Performance Monitor

In this demonstration, you will see how to view a performance report

Preparation Steps

The required virtual machines, 20411D-LON-DC1 and 20411D-LON-SVR1, should be running after the preceding demonstration.

Demonstration Steps

View a performance report

1. On LON-SVR1, in Performance Monitor, in the navigation pane, expand **Reports**, expand **User Defined**, and then click **LON-SVR1 Performance**.
2. Expand the folder beneath **LON-SVR1 Performance**. The data collector set's previous collection process generated this report. You can change from the chart view to any other supported view.
3. If the report is not displayed, click the **Refresh** button on the toolbar, and then repeat **Step 2**.
4. Close all open windows.

13: Monitoring Windows Server 2012

Demonstration: Creating a Custom View

In this demonstration, you will see how to:

- View Server Roles custom views
- Create a custom view

Leave the virtual machines running for subsequent demonstrations.

Preparation Steps

The required virtual machines, 20411D-LON-DC1 and 20411D-LON-SVR1, should be running after the preceding demonstration.

Demonstration Steps

View Server Roles custom views

1. On LON-SVR1, open Event Viewer.
2. In the navigation pane, expand **Custom Views**, expand **Server Roles**, and then click **Web Server (IIS)**. This is the Web Server role-specific custom view.

Create a custom view

1. In the navigation pane, right-click **Custom Views**, and then click **Create Custom View**.
2. In the **Create Custom View** dialog box, select the **Critical**, **Warning**, and **Error** check boxes.
3. In the **Create Custom View** dialog box , in the **Event logs** drop-down list, expand **Windows Logs**, and then select the **System** and **Application** check boxes. Click the mouse pointer back into the **Create Custom View** dialog box, and then click **OK**.
4. In the **Save Filter to Custom View** dialog box, in the **Name** box, type **Adatum Custom View**, and then click **OK**.
5. In Event Viewer, in the right pane, view the events that are visible within your custom view.

13: Monitoring Windows Server 2012

Demonstration: Configuring an Event Subscription

In this demonstration, you will see how to:

- Configure the source computer
- Configure the collector computer
- Create and view the subscribed log

Preparation Steps

The required virtual machines, 20411D-LON-DC1 and 20411D-LON-SVR1, should be running after the preceding demonstration.

Demonstration Steps

Configure the source computer

1. Switch to LON-DC1.
2. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
3. Click **Start**, and then type **Cmd** in the search box.
4. In the **Apps** list, click **Command Prompt**.
5. At the command prompt, type the following command, and then press Enter:

```
winrm quickconfig
```

Note that the service is already running.

6. From the **Server Manager**, click **Tools**, and then click **Active Directory Users and Computers**.
7. In Active Directory Users and Computers console, in the navigation pane, expand **Adatum.com**, and then click **Builtin**.
8. In the results pane, double-click **Administrators**.
9. In the **Administrators Properties** dialog box, click the **Members** tab.
10. Click **Add**, and, in the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, click **Object Types**.
11. In the **Object Types** dialog box, select the **Computers** check box, and then click **OK**.
12. In the **Select Users, Contacts, Computers, Service Accounts, or Groups** dialog box, in the **Enter**

13: Monitoring Windows Server 2012

the **object names to select** box, type **LON-SVR1**, and then click **OK**.

13. In the **Administrator Properties** dialog box, click **OK**.

Configure the collector computer

1. Switch to LON-SVR1.
2. Click **Start**, and then type **Cmd** in the **Search box**.
3. In the **Apps** list, click **Command Prompt**.
4. At the command prompt, type the following command, and then press Enter:
5. **Wecutil qc**
6. When prompted, type **Y**, and then press Enter.

Create and view the subscribed log

1. In Event Viewer, in the navigation pane, click **Subscriptions**.
2. Right-click **Subscriptions**, and then click **Create Subscription**.
3. In the **Subscription Properties** dialog box, in the **Subscription name** box, type **LON-DC1 Events**.
4. Click **Collector Initiated**, and then click **Select Computers**.
5. In the **Computers** dialog box, click **Add Domain Computers**.
6. In the **Select Computer** dialog box, in the **Enter the object name to select** box, type **LON-DC1**, and then click **OK**.
7. In the **Computers** dialog box, click **OK**.
8. In the **Subscription Properties – LON-DC1 Events** dialog box, click **Select Events**.
9. In the **Query Filter** dialog box, select the **Critical**, **Warning**, **Information**, **Verbose**, and **Error** check boxes.

13: Monitoring Windows Server 2012

10. In the **Logged** drop-down list, click **Last 30** days.
11. In the **Event logs** drop-down list, select **Windows Logs**. Click the mouse pointer back into the **Query Filter** dialog box, and then click **OK**.
12. In the **Subscription Properties – LON-DC1 Events** dialog box, click **OK**.
13. In Event Viewer, in the navigation pane, expand **Windows Logs**.
14. Click **Forwarded Events**.
15. Examine any listed events.

1: Implementing Advanced Network Services

Demonstration: Configuring DHCP Failover

- In this demonstration, you will see how to configure a DHCP failover relationship

Leave the virtual machines running after you have completed the demonstration.

Preparation Steps

Demonstration Steps

Configure a DHCP failover relationship

- Sign in on LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
- In Server Manager, click **Tools**, and then on the drop-down list, click **DHCP**. Note that the server is authorized, but that no scopes are configured.
- Switch to LON-DC1. In Server Manager, click **Tools**, and then on the drop-down list, click **DHCP**.
- In the DHCP console, expand **lon-dc1.adatum.com**, select and then right-click **IPv4**, and then click **Configure Failover**.
- In the Configure Failover Wizard, click **Next**.
- On the **Specify the partner server to use for failover** page, in the **Partner Server** field, enter **172.16.0.21**, and then click **Next**.
- On the **Create a new failover relationship** page, in the **Relationship Name** field, enter **Adatum**.
- In the **Maximum Client Lead Time** field, set the hours to **zero**, and then set the minutes to **15**.
- Ensure the **Mode** field is set to **Load balance**.
- Ensure that the **Load Balance Percentage** is set to **50%**.
- Select the **State Switchover Interval** check box. Leave the default value of 60 minutes.
- In the **Enable Message Authentication Shared Secret** field, type **Pa\$\$w0rd**, and then click **Next**.
- Click **Finish**, and then click **Close**.
- Switch to LON-SVR1.

15. Refresh the **IPv4** node, expand the **IPv4** node, and then expand **Scope [172.16.0.0]** **Adatum.com**.
16. Click **Address Pool**, and note that the address pool is configured.
17. Click **Scope Options**, and note that the scope options are configured.
18. Close the DHCP console on both LON-DC1 and LON-SVR1.
19. Revert LON-SVR1.

1: Implementing Advanced Network Services

Demonstration: Configuring DNSSEC

- In this demonstration, you will see how to configure DNSSEC

Leave the virtual machines running after you have completed the demonstration.

Preparation Steps

You require the 20412D-LON-DC1 virtual machine for this demonstration.

Demonstration Steps

Configure DNSSEC

- Sign in on **LON-DC1** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
- In Server Manager, click **Tools**, and then in the drop-down list, click **DNS**.
- In DNS, expand **LON-DC1**, expand **Forward Lookup Zones**, and then select and right-click **Adatum.com**.
- On the menu, click **DNSSEC>Sign the Zone**.
- In the Zone Signing Wizard, click **Next**.
- Click **Customize zone signing parameters**, and then click **Next**.
- On the **Key Master** page, click **The DNS server LON-DC1 is the Key Master**. Click **Next**.
- On the **Key Signing Key (KSK)** page, click **Next**.
- On the **Key Signing Key (KSK)** page, click **Add**.
- On the **New Key Signing Key (KSK)** page, click **OK**.
- On the **Key Signing Key (KSK)** page, click **Next**.
- On the **Zone Signing Key (ZSK)** page, click **Next**.
- On the **Zone Signing Key (ZSK)** page, click **Add**.
- On the **New Zone Signing Key (ZSK)** page, click **OK**.
- On the **Zone Signing Key (ZSK)** page, click **Next**.
- On the **Next Secure (NSEC)** page, click **Next**.

17. On the **Trust Anchors (TAs)** page, check the **Enable the distribution of trust anchors for this zone** check box, and then click **Next**.
18. On the **Signing and Polling Parameters** page, click **Next**.
19. On the **DNS Security Extensions** page, click **Next**, and then click **Finish**.
20. In DNS Manager, expand **Trust Points**, expand **com**, and then click **Adatum**. Ensure that the **DNSKEY** resource records exist, and that their status is valid.
21. In Server Manager, click **Tools**, and then on the drop-down list, click **Group Policy Management**.
22. In the Group Policy Management Console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, right-click **Default Domain Policy**, and then click **Edit**.
23. In the Group Policy Management Editor, under **Computer Configuration**, expand **Policies**, expand **Windows Settings**, and then click the **Name Resolution Policy** folder.
24. In the Create Rules section, in the **Suffix** field, type **Adatum.com** to apply the rule to the suffix of the namespace.
25. Select the **Enable DNSSEC in this rule** check box.
26. Select the **Require DNS clients to check that the name and address data has been validated by the DNS server** check box, and then click **Create**.
27. Scroll down and click **Apply**.
28. Close all open windows.

1: Implementing Advanced Network Services

Demonstration: Implementing IPAM

- In this demonstration, you will see how to install and configure IPAM management

Leave the virtual machines running after you have completed the demonstration.

Preparation Steps

You require the 20412D-LON-DC1 and 20412D-LON-SVR2 virtual machines for this demonstration.

Some sequences in this demonstration can take considerable time. Instead of waiting, discuss the tasks with the students, or move ahead with teaching and return to this demonstration when you finish this lesson.

Demonstration Steps

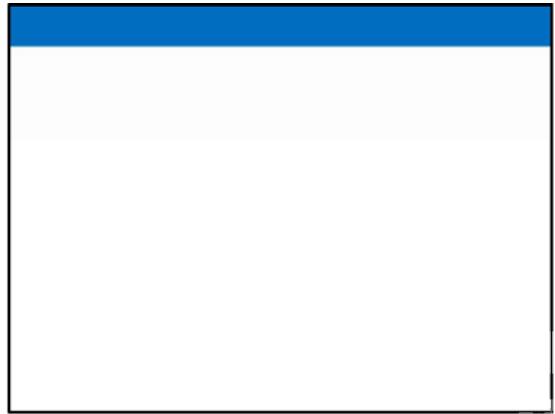
Install IPAM

- Sign in on **LON-SVR2** as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
- In the Server Manager, click **Add roles and features**.
- In the Add Roles and Features Wizard, click **Next**.
- On the **Select installation type** page, click **Next**.
- On the **Select destination server** page, click **Next**.
- On the **Select server roles** page, click **Next**.
- On the **Select features** page, select the **IP Address Management (IPAM) Server** check box.
- In the **Add features that are required for IP Address Management (IPAM) Server** popup, click **Add Features**, and then click **Next**.
- On the **Confirm installation selections** page, click **Install**.
- When the Add Roles and Features Wizard completes, close the wizard.

Configure IPAM

- In the Server Manager navigation pane, click **IPAM**.
- In the IPAM Overview pane, click **Connect to IPAM server**. Click **LON-SVR2.Adatum.com**, and then click **OK**.

1: Implementing Advanced Network Services



3. Click **Provision the IPAM server**.
4. In the Provision IPAM Wizard, click **Next**.
5. On the **Configure database** page, click **Next**.
6. On the **Select provisioning method** page, ensure that **Group Policy Based** is selected. In the **GPO name prefix** box, type **IPAM**, and then click **Next**.
7. On the **Confirm the Settings** page, click **Apply**. Provisioning will take a few minutes to complete.
8. When provisioning has completed, click **Close**.
9. On the IPAM Overview pane, click **Configure server discovery**.
10. In the **Configure Server Discovery** dialog box, click **Add** to add the Adatum.com domain, and then click **OK**.
11. On the IPAM Overview pane, click **Start server discovery**. Discovery may take five to 10 minutes to run. The yellow bar indicates when discovery is complete.
12. On the IPAM Overview pane, click **Select or add servers to manage and verify IPAM access**. Notice that the IPAM Access Status is blocked. Scroll down to the Details view, and note the status report. The IPAM server has not yet been granted permission to manage LON-DC1 via Group Policy.
13. On the taskbar, right-click the Windows PowerShell icon, and then click **Run as Administrator**.
14. At the Windows PowerShell prompt, type the following command, and then press Enter:

```
Invoke-IpamGpoProvisioning –Domain Adatum.com –GpoPrefixName IPAM –IpamServerFqdn LON-SVR2.adatum.com –DelegatedGpoUser Administrator
```

1. When you are prompted to confirm the action, type **Y**, and then press Enter. The command will take a few minutes to complete.
2. Close Windows PowerShell.

1: Implementing Advanced Network Services

3. Switch to Server Manager. In the IPv4 details pane, right-click **LON-DC1**, and then click **Edit Server**.
4. In the **Add or Edit Server** dialog box, set the **Manageability status** field to **Managed**, and then click **OK**.
5. Switch to **LON-DC1**.
6. From the start screen, start a command prompt.
7. In the command prompt, type **Gpupdate /force**, and then press Enter.
8. Wait for the Gpupdate process to complete, and then close the command prompt.
9. Return to LON-SVR2, and in Server Manager, right-click LON-DC1, and then click **Refresh Server Access Status**. Discovery may take five to 10 minutes to run. The yellow bar indicates when discovery is complete. After discovery is complete, refresh IPv4 by clicking the **Refresh** icon. It may take up to five minutes for the status to change.
10. In the IPAM Overview pane, click **Retrieve data from managed servers**. This action will take a few minutes to complete.

1: Implementing Advanced Network Services

Demonstration: Using IPAM to Manage IP Addressing

- In this demonstration, you will see how to use IPAM to manage IP addressing

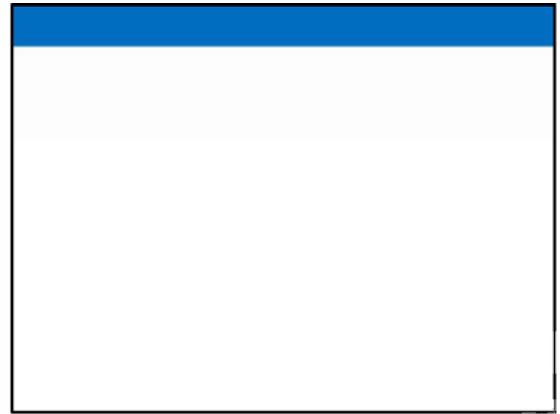
Leave the virtual machines running after you have completed the demonstration.

Preparation Steps

You require the 20412D-LON-DC1 and 20412D-LON-SVR2 virtual machines for this demonstration.

Demonstration Steps

- On LON-SVR2, in the Server Manager, in the IPAM console tree, click **IP Address Blocks**.
- In the right pane, click the **Tasks** drop-down arrow, and then click **Add IP Address Block**.
- In the **Add or Edit IPv4 Address Block** dialog box, provide the following values, and then click **OK**:
 - Network ID: **172.16.0.0**
 - Prefix length: **16**
 - Description: **Head Office**
- In the IPAM console tree, click **IP Address Inventory**.
- In the right pane, click the **Tasks** drop-down arrow, and then click **Add IP Address**.
- In the **Add IP Address** dialog box, under **Basic Configurations**, provide the following values, and then click **OK**:
 - IP address: **172.16.0.1**
 - MAC address: **112233445566**
 - Device type: **Routers**
 - Description: **Head Office Router**
- Click the **Tasks** drop-down arrow, and then click **Add IP Address**.
- In the **Add IP Address** dialog box, under **Basic Configuration**, provide the following values:
 - IP address: **172.16.0.101**



- MAC address: **223344556677**
 - Device type: **Host**
9. In the Add IPv4 Address pane, click **DHCP Reservation**, and then enter the following values:
- Client ID: **Check the Associate MAC to Client ID** checkbox
 - Reservation server name: **LON-DC1.Adatum.com**
 - Reservation name: **Webserver**
 - Reservation type: **Both**
10. In the Add IPv4 Address pane, click **DNS Record**, enter the following values, and then click **OK**:
- Device name: **Webserver**
 - Forward lookup zone: **Adatum.com**
 - Forward lookup primary server: **LON-DC1.Adatum.com**
 - Check the **Automatically create DNS records for this IP address** checkbox.
11. On LON-DC1, open the DHCP console, expand **IPv4**, expand **Scope (172.16.0.0) Adatum**, and then click **Reservations**. Ensure that the Webserver reservation for 172.16.0.101 displays.
12. Open the DNS console, expand **Forward Lookup Zones**, and then click **Adatum.com**. Ensure that a host record displays for Webserver.

1: Implementing Advanced Network Services

Demonstration: Using IPAM Monitoring

- In this demonstration, you will see how to use IPAM to monitoring.

After you complete the demonstration, revert all of the virtual machines.

Preparation Steps

You require the 20412D-LON-DC1 and 20412D-LON-SVR2 virtual machines for this demonstration.

Demonstration Steps

- On LON-SVR2, in Server Manager, in the IPAM console tree, click **DNS and DHCP Servers**.
- In the Details view, discuss the **LON-DC1.adatum.com** Server Properties.
- Click the **Event Catalog** tab, and discuss the events shown.
- In the IPAM console tree, click on **DHCP scopes**.
- Select the **Adatum** scope, and discuss the information in the **Scope Properties**.
- Click the **Options** tab, and discuss the information displayed.
- Click the **Event Catalog** tab, and discuss the events shown.
- In the IPAM console tree, click on **DNS Zone Monitoring**.
- Select the **adatum.com** zone, and discuss the information in the **Zone Properties**.
- Click the **Authoritative Servers** tab, and discuss the information displayed.
- In the IPAM console tree, click on **Server Groups**.
- Select the **LON-DC1.adatum.com** entry with the **DNS** server role, and discuss the information in the **Server Properties**.
- Click the **DNS Zones** tab, and discuss the information displayed.
- Click the **Event Catalog** tab, and discuss the events shown.

2: Implementing Advanced File Services

Demonstration: Configuring an iSCSI Target

In this demonstration, you will see how to:

- Add the iSCSI target server role service
- Create two iSCSI virtual disks and an iSCSI target

Preparation Steps

For this demonstration, you must start the 20412D-LON-DC1 and 20412D-LON-SVR2 virtual machines. Sign in to the virtual machines with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

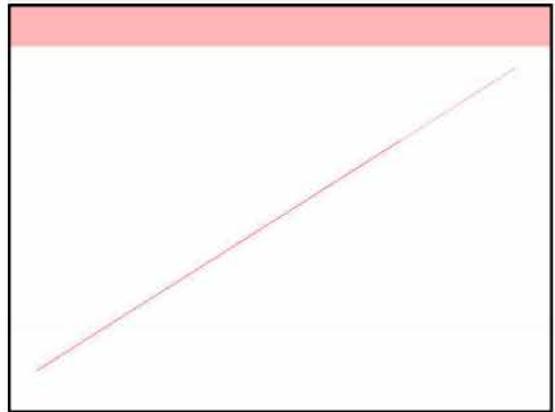
Demonstration Steps

Add the iSCSI target server role service

1. On LON-DC1, in the Server Manager, click **Manage**, and then click **Add roles and features**.
2. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **Select server from the server pool** is selected, and then click **Next**.
5. On the **Select server roles** page, expand **File And Storage Services (2 of 12 Installed)**, expand **File and iSCSI Services (1 of 11 Installed)**, select the **iSCSI Target Server** check box, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. When installation completes, click **Close**.

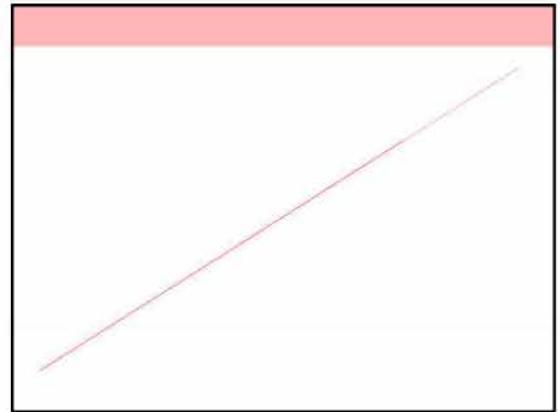
Create two iSCSI virtual disks and an iSCSI target

1. On LON-DC1, in the Server Manager, in the navigation pane, click **File and Storage Services**.
2. In the File and Storage Services pane, click **iSCSI**.
3. In the iSCSI VIRTUAL DISKS pane, click **TASKS**, and then in the **TASKS** drop-down list box, click **New iSCSI Virtual Disk**.
4. In the New iSCSI Virtual Disk Wizard, on the **Select iSCSI virtual disk location** page, under



Storage location, click drive **C**, and then click **Next**.

5. On the **Specify iSCSI virtual disk name** page, type **iSCSIDisk1**, and then click **Next**.
6. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **5**, in the drop-down list box, ensure that **GB** is selected, and then click **Next**.
7. On the **Assign iSCSI target** page, click **New iSCSI target**, and then click **Next**.
8. On the **Specify target name** page, in the **Name** box, type **LON-SVR2**, and then click **Next**.
9. On the **Specify access servers** page, click **Add**.
10. In the **Select a method to identify the initiator** dialog box, click **Enter a value for the selected type**. In the **Type** drop-down list box, click **IP Address**, in the **Value** field, type **172.16.0.22**, and then click **OK**.
11. On the **Specify access servers** page, click **Next**.
12. On the **Enable Authentication** page, click **Next**.
13. On the **Confirm selections** page, click **Create**.
14. On the **View results** page, wait until creation completes, and then click **Close**.
15. In the iSCSI VIRTUAL DISKS pane, click **TASKS**, and then in the **TASKS** drop-down list box, click **New iSCSI Virtual Disk**.
16. In the New iSCSI Virtual Disk Wizard, on the **Select iSCSI virtual disk location** page, under **Storage location**, click drive **C**, and then click **Next**.
17. On the **Specify iSCSI virtual disk name** page, type **iSCSIDisk2**, and then click **Next**.
18. On the **Specify iSCSI virtual disk size** page, in the **Size** box, type **5**. In the drop-down list box, ensure that **GB** is selected, and then click **Next**.
19. On the **Assign iSCSI target** page, click **lon-svr2**, and then click **Next**.



20. On the **Confirm selections** page, click **Create**.
21. On the **View results** page, wait until creation completes, and then click **Close**.

Note: Keep the computers running, because you will need them for the next demonstration.

2: Implementing Advanced File Services

Demonstration: Connecting to the iSCSI Storage

In this demonstration, you will see how to:

- Connect to the iSCSI target
- Verify the presence of the iSCSI drive

Show the Targets and Discovery tabs of the initiator, and explain the different discovery methods.

Preparation Steps

For this demonstration, you must start the 20412D-LON-DC1 and 20412D-LON-SVR2 virtual machines. Sign in with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**. The virtual machines should still be running from the previous demonstration. In addition, you must have performed the previous demonstration before you continue with this demonstration.

Demonstration Steps

Connect to the iSCSI target

1. On 20412D-LON-SVR2, in Server Manager, click the **Tools** menu, and then click **iSCSI Initiator**.
2. In the **Microsoft iSCSI** message box, click **Yes**.
3. In the **iSCSI Initiator Properties** dialog box, on the **Targets** tab, type **LON-DC1**, and then click **Quick Connect**.
4. In the **Quick Connect** window, in the **Discovered targets** section, click **iqn.1991-05.com.microsoft:lon-dc1-lon-svr2-target**, and then click **Done**.
5. In the **iSCSI Initiator Properties** dialog box, click **OK** to close the dialog box.

Verify the presence of the iSCSI drive

1. On 20412D-LON-SVR2, in Server Manager, on the **Tools** menu, click **Computer Management**.
2. In the Computer Management console, under **Storage node**, click **Disk Management**. Notice that the new disks are added. However, they all are currently offline and not formatted.
3. Close the Computer Management console.

Note: Keep the computers running, because you will need them for the next demonstration.

2: Implementing Advanced File Services

Demonstration: Configuring BranchCache

In this demonstration, you will see how to:

- Add BranchCache for the Network Files role service
- Configure BranchCache in Local Group Policy Editor
- Enable BranchCache for a file share

Preparation Steps

For this demonstration, you must start the **20412D-LON-DC1** and **20412D-LON-SVR2** virtual machines. Sign in to the virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**. The virtual machines should still be running from the previous demonstration, and the previous two demonstrations should have been completed.

Demonstration Steps

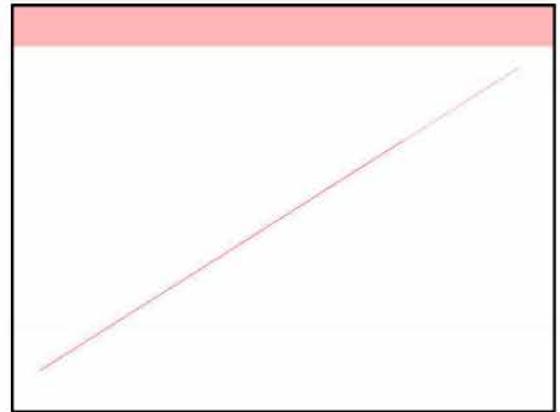
Add BranchCache for the Network Files role service

1. On LON-DC1, in the Server Manager, click **Add roles and features**.
2. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **Select server from the server pool** is selected, and then click **Next**.
5. On the **Select server roles** page, expand **File and Storage Services (3 of 12 Installed)**, expand **File and iSCSI Services (2 of 11 Installed)**, select the **BranchCache for Network Files** check box, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. When installation completes, click **Close**.

Enable BranchCache for the server

1. On LON-DC1, click the Start screen.
2. On the Start screen, type **gpedit.msc**, and then press Enter.
3. Expand **Computer Configuration**, expand **Administrative Templates**, expand **Network**, click **Lanman Server**, and then double-click **Hash Publication for BranchCache**.

2: Implementing Advanced File Services



4. In the **Hash Publication for BranchCache** dialog box, click **Enabled**.
5. In the **Options** box, under **Hash publication actions**, select **Allow hash publication only for shared folder on which BranchCache is enabled**, and then click **OK**.
6. Close the Local Group Policy Editor.

Enable BranchCache for a file share

1. On the taskbar, click the **File Explorer** icon.
2. In the File Explorer window, in the left pane, click **Local Disk (C:)**.
3. On the quick access bar located on the upper-left side of the window, click **New Folder**, type **Share**, and then press Enter.
4. Right-click **Share**, and click **Properties**.
5. In the **Share Properties** dialog box, click the **Sharing** tab, and then click **Advanced Sharing**.
6. In the **Advanced Sharing** dialog box, click **Share this folder**, and then click **Caching**.
7. In the **Offline Settings** dialog box, select the **Enable BranchCache** check box, and then click **OK**.
8. In the **Advanced Sharing** dialog box, click **OK**, and then click **Close**.
9. Close all open windows.

2: Implementing Advanced File Services

Demonstration: How to Configure Classification Management

In this demonstration, you will see how to:

- Create a classification property
- Create a classification rule
- Modify the classification schedule

Preparation Steps

For this demonstration, you will use the 20412D-LON-DC1 and 20412D-LON-SVR1 virtual machines.

Start 20412D-LON-SVR1 and sign in to the virtual machines with the user name **Adatum\Administrator** and the password **Pa\$\$w0rd**.

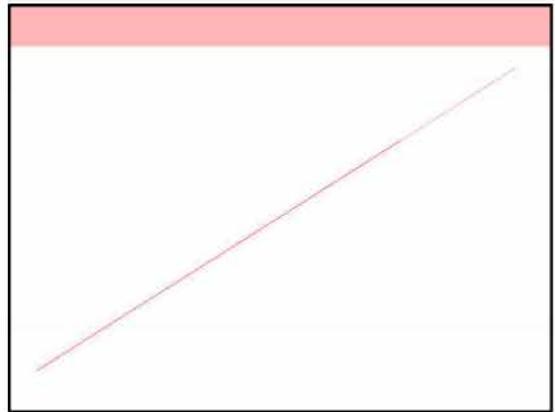
Demonstration Steps

Create a classification property

1. On LON-SVR1, on the toolbar, click the **Server Manager** shortcut.
2. In the **Server Manager**, click **Tools**, and then click **File Server Resource Manager**.
3. In **File Server Resource Manager**, expand the **Classification Management** node, and then click **Classification Properties**.
4. Right-click **Classification Properties**, and click **Create Local Property**.
5. In the **Create Local Classification Property** window, in the **Name** field, type **Confidential**, and in the **Description** field, type **Assigns a confidentiality value of Yes or No**.
6. Under **Property type**, click the drop-down list box, and then select **Yes/No**.
7. In the **Create Local Classification Property** window, click **OK**.

Create a classification rule

1. In **File Server Resource Manager**, click the **Classification Rules** node.
2. Right-click the **Classification Rules** node, and click **Create Classification Rule**.
3. In the **Rule name** field, type **Confidential Payroll Documents**.
4. In the **Description** field, type **Classify documents containing the word payroll as confidential**, and then click the **Scope** tab.
5. In the **Scope** section, click **Add**.



6. In the **Browse for Folder** window, expand **Allfiles (E:)**, expand **Labfiles**, click **Data**, and then click **OK**.
7. In the **Create Classification Rule** window, click the **Classification** tab.
8. In the **Classification method** area, click the drop-down list box, and then click **Content Classifier**.
9. In the **Property** section, choose a Property name of **Confidential** and a Property value of **Yes**, and then click **Configure**.
10. On the **Parameters** tab, below the **Expression Type** column, click the drop-down list box, and then select **String**.
11. Double-click in the **Expression** column, type **payroll**, and then click **OK**.
12. In the **Create Classification Rule** window, click **OK**.

Modify the classification schedule

1. Right-click the **Classification Rules** node, and click **Configure Classification Schedule**.
2. In the **File Server Resource Manager Options** window, ensure that the **Automatic Classification** tab is selected.
3. In the **Schedule** window, click the **Enable fixed schedule** check box.
4. In the **Run at** field, type **8:30 AM**, select **Sunday**, and then click **OK**.
5. Right-click the **Classification Rules** node, and click **Run Classification With All Rules Now**.
6. In the **Run Classification** window, click **Wait for classification to complete**, and then click **OK**.
7. View the report, and ensure that **File3.txt** is listed at the bottom of the report.
8. In a **File Explorer** window, click drive **E**, expand **Labfiles**, expand **Data**, double-click the file **File3.txt**, and then view its contents. Ensure that it contains the word "payroll." Open the other files in the folder and ensure they do not contain the word "payroll."

2: Implementing Advanced File Services

Demonstration: Configuring Data Deduplication

In this demonstration, you will see how to:

- Add the Data Deduplication role service
- Enable data deduplication
- Test data deduplication

Preparation Steps

For this demonstration, continue to use the **20412D-LON-DC1** and **20412D-LON-SVR2** virtual machines from the previous demonstration. Sign in to the virtual machine as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

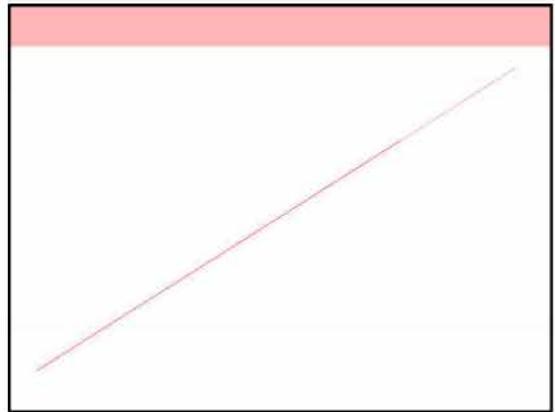
Demonstration Steps

Add the Data Deduplication role service

1. On LON-SVR2, in the Server Manager, click **Manage**, and then click **Add roles and features**.
2. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, ensure that **Select server from the server pool** is selected, and then click **Next**.
5. On the **Select server roles** page, expand **File And Storage Services (1 of 12 Installed)**, expand **File and iSCSI Services**, and then select the **Data Deduplication** check box.
6. In the Add Roles and Features Wizard dialog box, click **Add Features**, and then click **Next**.
7. On the **Select features** page, click **Next**.
8. On the **Confirm installation selections** page, click **Install**.
9. When installation completes, click **Close**.

Enable Data Deduplication

1. In Server Manager, in the navigation pane, click **File and Storage Services**.
2. In the File and Storage Services pane, click **Volumes**.
3. In the Volumes pane, right-click drive **E:**, and in the drop-down list box, click **Configure Data Deduplication**.
4. In the **Allfiles (E:)\ Deduplication Settings** dialog box, in the Data Deduplication drop-down list



box, select **General purpose file server**, in the **Deduplicate files older than (in days)** box, type **3**, and then click **Set Deduplication Schedule**.

5. In the **LON-SVR2 Deduplication Schedule** dialog box, click **Enable throughput optimization**, and in the **Start time** drop-down list box, click **2 AM.**, and then click **OK**.
6. In the **Allfiles (E:\) Deduplication Settings** dialog box, click **OK**.

Test Data Deduplication

1. On LON-SVR2, open a File Explorer window, navigate to drive **E**, right-click **Group Policy Preferences.docx** file, and then click **Copy**.
2. Paste the **Group Policy Preferences.docx** file to the **LabFiles** folder.
3. On LON-SVR2, open the **E:\LabFiles** folder, right-click **Group Policy Preferences.docx**, and then click **Properties**.
4. In the **Properties** dialog box, note the values for Size and Size on Disk.
5. Repeat steps five through seven for **Group Policy Preferences.docx** in the root folder of the **E:** drive.
6. On LON-SVR2, open the **Windows PowerShell** window.
7. At the Windows PowerShell prompt, type the following cmdlet, and then press Enter:

Start-DedupJob –Type Optimization –Volume E:

8. Type **Get-DedupJob**, then press **Enter**. Ensure that the process is running.
9. Wait a minute or two, and repeat the **Get-Dedupjob** command.
10. If you get no result, it means that the deduplication job is complete.
11. In the root folder of the **E:** drive, right-click **Group Policy Preferences.docx**, and then click **Properties**.
12. In the **Properties** dialog box, note the values for Size and Size on Disk. Size on disk should be much smaller than it was previously.

3: Implementing Dynamic Access Control

15. Close the Group Policy Management Editor and the Group Policy Management Console.
16. On LON-SVR1, on the taskbar, click the **Windows PowerShell** icon.
17. At a Windows PowerShell command-line interface command prompt, type **gpupdate /force**, and then press Enter.
18. Close Windows PowerShell.
19. On the taskbar, click the **File Explorer** icon.
20. In File Explorer, browse to **Local Disk (C:)**, right-click the **Docs** folder, and then click **Properties**.
21. In the **Properties** dialog box, click the **Security** tab, and then click **Advanced**.
22. In the **Advanced Security Settings for Docs** window, click the **Central Policy** tab, and then click **Change**.
23. In the drop-down list box, select **Protect confidential docs**, and then click **OK** twice.
24. Right-click the **Research** folder, and then click **Properties**.
25. In the **Properties** dialog box, click the **Security** tab, and then click **Advanced**.
26. In the **Advanced Security Settings for Research** window, click the **Central Policy** tab, and then click **Change**.
27. In the drop-down list box, click **Department Match**, and then click **OK** twice.

3: Implementing Dynamic Access Control

Demonstration: Creating and Deploying Central Access Policies

In this demonstration, your instructor will show you how to create and deploy central access policy

Preparation Steps

To perform this demonstration, you must have completed the previous demonstrations successfully.

Demonstration Steps

1. On LON-DC1, in the Active Directory Administrative Center, click **Dynamic Access Control**, and then double-click **Central Access Policies**.
2. In the Tasks pane, click **New**, and then click **Central Access Policy**.
3. In the **Name** field, type **Protect confidential docs**, and then click **Add**.
4. Click the **Access Confidential Docs** rule, click **>>**, and then click **OK** twice.
5. In the Tasks pane, click **New**, and then click **Central Access Policy**.
6. In the **Name** field, type **Department Match**, and then click **Add**.
7. Click the **Department Match** rule, click **>>**, and then click **OK** twice.
8. Close the Active Directory Administrative Center.
9. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
10. In the Group Policy Management Console, under Domains, expand **Adatum.com**, right-click **DAC-Protected**, and then click **Create a GPO in this domain, and link it here**.
11. Type **DAC Policy**, and then click **OK**.
12. Right-click **DAC Policy**, and then click **Edit**.
13. Expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **File System**, right-click **Central Access Policy**, and then click **Manage Central Access Policies**.
14. Press and hold the Ctrl button and click both **Department Match** and **Protect confidential docs**, click **Add**, and then click **OK**.

3: Implementing Dynamic Access Control

Planning Central Access Policies for File Servers

When planning deployment of central access policies, you should:

- Identify the resources that you want to protect
- Define the authorization policies
- Translate the authorization policies that you require into expressions
- Identify attributes for access filtering

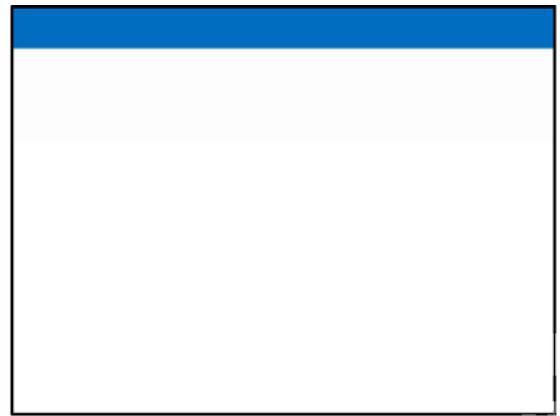
Discuss DAC policy planning.

20412D

3: Implementing Dynamic Access Control

Lesson 3: Implementing DAC for Access Control

- Planning Central Access Policies for File Servers
- Demonstration: Creating and Deploying Central Access Policies
- How Does Access Check Work When DAC Is in Use
- Managing and Monitoring DAC
- Demonstration: Evaluating and Managing DAC



14. In File Server Resource Manager, in the Actions pane, click **Run Classification With All Rules Now**.
15. Click **Wait for classification to complete**, and then click **OK**.
16. After the classification is complete, you will be presented with a report. Verify that two files were classified. You can confirm this in the Report Totals section.
17. Close the report.
18. On the taskbar, click the **File Explorer** icon.
19. In the File Explorer window, expand **Local Disk (C:)**, and then click the **Docs** folder.
20. In the Docs folder, right-click **Doc1.txt**, click **Properties**, and then click the **Classification** tab. Verify that Confidentiality is set to **High**.
21. Repeat step 20 on files Doc2.txt and Doc3.txt. Doc2.txt should have the same Confidentiality as Doc1.txt, while Doc3.txt should have no value. This is because only Doc1.txt and Doc2.txt have the word “secret” in their content.

3: Implementing Dynamic Access Control

Demonstration: Configuring Classification Rules

In this demonstration, you will learn how to classify files by using a file classification mechanism

Preparation Steps

You must have completed the previous demonstration successfully before you start this one.

Demonstration Steps

1. On LON-SVR1, in Server Manager, click **Tools**, and then click **File Server Resource Manager**.
2. In **File Server Resource Manager**, expand **Classification Management**.
3. Select and then right-click **Classification Properties**, and then click **Refresh**.
4. Verify that the **Confidentiality** and **Department** properties are listed.
5. Click **Classification Rules**.
6. In the Actions pane, click **Create Classification Rule**.
7. In the **Create Classification Rule** window, for the Rule name, type **Set Confidentiality**.
8. Click the **Scope** tab, and then click **Add**.
9. In the **Browse For Folder** dialog box, expand **Local Disk (C:)**, click the **Docs** folder, and then click **OK**.
10. Click the **Classification** tab, make sure that the following settings are set, and then click **Configure**:
 - Classification method: **Content Classifier**
 - Property: **Confidentiality**
 - Value: **High**
11. In the **Classification Parameters** dialog box, click the **Regular expression** drop-down list box, and then click **String**.
12. In the **Expression** field, which is next to the word String, type **secret**, and then click **OK**.
13. Click the **Evaluation Type** tab, select **Re-evaluate existing property values**, click **Overwrite the existing value**, and then click **OK**.

20412D

3: Implementing Dynamic Access

Control

Implementing and Managing File Classifications

- Resource property definitions are defined in AD DS
- Resource property definitions can be used during file classifications
- File classifications can be run automatically



Explain what the File Classification Infrastructure (FCI) is and how it works. Also, be sure to explain it in the context of DAC, and also explain how file classification can help extend DAC functionality.



condition.

Note: If you cannot find Managers in the last drop-down list box, click **Add items**. Then in the Select user, Computer, Service Account, or Group window, type **Managers**, click **Check Names**, in Multiple Names Found window click **Managers** and then click **OK**.

49. Set the second condition to: **Device-Group-Member of each-Value-ManagersWKS**, and then click **OK** three times.

3: Implementing Dynamic Access Control

Demonstration: Configuring Classification Rules

In this demonstration, you will learn how to classify files by using a file classification mechanism

Preparation Steps

You must have completed the previous demonstration successfully before you start this one.

Demonstration Steps

1. On LON-SVR1, in Server Manager, click **Tools**, and then click **File Server Resource Manager**.
2. In **File Server Resource Manager**, expand **Classification Management**.
3. Select and then right-click **Classification Properties**, and then click **Refresh**.
4. Verify that the **Confidentiality** and **Department** properties are listed.
5. Click **Classification Rules**.
6. In the Actions pane, click **Create Classification Rule**.
7. In the **Create Classification Rule** window, for the Rule name, type **Set Confidentiality**.
8. Click the **Scope** tab, and then click **Add**.
9. In the **Browse For Folder** dialog box, expand **Local Disk (C:)**, click the **Docs** folder, and then click **OK**.
10. Click the **Classification** tab, make sure that the following settings are set, and then click **Configure**:
 - Classification method: **Content Classifier**
 - Property: **Confidentiality**
 - Value: **High**
11. In the **Classification Parameters** dialog box, click the **Regular expression** drop-down list box, and then click **String**.
12. In the **Expression** field, which is next to the word String, type **secret**, and then click **OK**.
13. Click the **Evaluation Type** tab, select **Re-evaluate existing property values**, click **Overwrite the existing value**, and then click **OK**.



14. In File Server Resource Manager, in the Actions pane, click **Run Classification With All Rules Now**.
15. Click **Wait for classification to complete**, and then click **OK**.
16. After the classification is complete, you will be presented with a report. Verify that two files were classified. You can confirm this in the Report Totals section.
17. Close the report.
18. On the taskbar, click the **File Explorer** icon.
19. In the File Explorer window, expand **Local Disk (C:)**, and then click the **Docs** folder.
20. In the Docs folder, right-click **Doc1.txt**, click **Properties**, and then click the **Classification** tab. Verify that Confidentiality is set to **High**.
21. Repeat step 20 on files Doc2.txt and Doc3.txt. Doc2.txt should have the same Confidentiality as Doc1.txt, while Doc3.txt should have no value. This is because only Doc1.txt and Doc2.txt have the word “secret” in their content.

3: Implementing Dynamic Access Control

Demonstration: Creating and Deploying Central Access Policies

In this demonstration, your instructor will show you how to create and deploy central access policy

Preparation Steps

To perform this demonstration, you must have completed the previous demonstrations successfully.

Demonstration Steps

1. On LON-DC1, in the Active Directory Administrative Center, click **Dynamic Access Control**, and then double-click **Central Access Policies**.
2. In the Tasks pane, click **New**, and then click **Central Access Policy**.
3. In the **Name** field, type **Protect confidential docs**, and then click **Add**.
4. Click the **Access Confidential Docs** rule, click **>>**, and then click **OK** twice.
5. In the Tasks pane, click **New**, and then click **Central Access Policy**.
6. In the **Name** field, type **Department Match**, and then click **Add**.
7. Click the **Department Match** rule, click **>>**, and then click **OK** twice.
8. Close the Active Directory Administrative Center.
9. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
10. In the Group Policy Management Console, under Domains, expand **Adatum.com**, right-click **DAC-Protected**, and then click **Create a GPO in this domain, and link it here**.
11. Type **DAC Policy**, and then click **OK**.
12. Right-click **DAC Policy**, and then click **Edit**.
13. Expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **File System**, right-click **Central Access Policy**, and then click **Manage Central Access Policies**.
14. Press and hold the Ctrl button and click both **Department Match** and **Protect confidential docs**, click **Add**, and then click **OK**.

3: Implementing Dynamic Access Control

15. Close the Group Policy Management Editor and the Group Policy Management Console.
16. On LON-SVR1, on the taskbar, click the **Windows PowerShell** icon.
17. At a Windows PowerShell command-line interface command prompt, type **gpupdate /force**, and then press Enter.
18. Close Windows PowerShell.
19. On the taskbar, click the **File Explorer** icon.
20. In File Explorer, browse to **Local Disk (C:)**, right-click the **Docs** folder, and then click **Properties**.
21. In the **Properties** dialog box, click the **Security** tab, and then click **Advanced**.
22. In the **Advanced Security Settings for Docs** window, click the **Central Policy** tab, and then click **Change**.
23. In the drop-down list box, select **Protect confidential docs**, and then click **OK** twice.
24. Right-click the **Research** folder, and then click **Properties**.
25. In the **Properties** dialog box, click the **Security** tab, and then click **Advanced**.
26. In the **Advanced Security Settings for Research** window, click the **Central Policy** tab, and then click **Change**.
27. In the drop-down list box, click **Department Match**, and then click **OK** twice.

3: Implementing Dynamic Access Control

Demonstration: Evaluating and Managing DAC

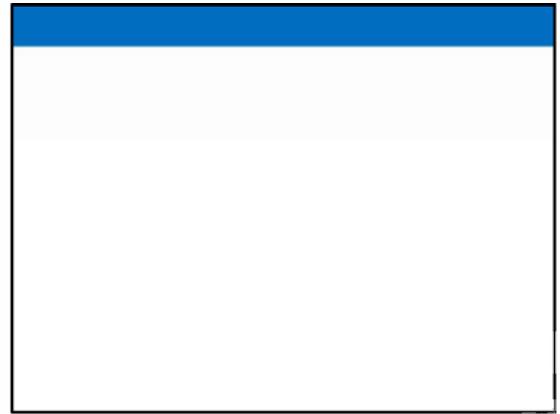
In this demonstration, you will learn how to evaluate and manage DAC

Preparation Steps

To perform this demonstration, you must have completed the previous demonstrations successfully.

Demonstration Steps

1. On LON-DC1, open Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In the Group Policy Management Console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click **Group Policy Objects**.
3. Right-click **DAC Policy**, and then click **Edit**.
4. In the Group Policy Management Editor, expand **Computer Configuration**, expand **Policies**, expand **Windows Settings**, expand **Security Settings**, expand **Advanced Audit Policy Configuration**, expand **Audit Policies**, and then click **Object Access**.
5. Double-click **Audit Central Access Policy Staging**, select all three check boxes, and then click **OK**.
6. Double-click **Audit File System**, select all three check boxes, and then click **OK**.
7. Close the Group Policy Management Editor and the Group Policy Management Console.
8. On LON-DC1, open Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
9. In the navigation pane, click **Dynamic Access Control**.
10. Double-click **Central Access Rules**, right-click **Department Match**, and then click **Properties**.
11. Scroll down to the Proposed Permissions section, click **Enable permission staging configuration**, and then click **Edit**.
12. Click **Authenticated Users**, and then click **Edit**.
13. Change the condition to **User-Company Department-Equals-Value-Marketing**, and then click **OK**.
14. Click **OK** twice to close all windows.



15. Switch to LON-SVR1.
16. On the taskbar, click the **Windows PowerShell** icon.
17. At the Windows PowerShell command prompt, type **gpupdate /force**, and then press Enter. Wait until Group Policy is updated for both user and computer.
18. Close Windows PowerShell.

3: Implementing Dynamic Access Control

Demonstration: Implementing Access Denied Assistance

In this demonstration, your instructor will show you how to configure and implement Access Denied Assistance.

Preparation Steps

To perform this demonstration, you must have completed the previous demonstrations successfully.

Demonstration Steps

1. On LON-DC1, in Server Manager, click **Tools**, and then click **Group Policy Management**.
2. In the Group Policy Management Console, expand **Forest: Adatum.com**, expand **Domains**, expand **Adatum.com**, and then click **Group Policy objects**.
3. Right-click **DAC Policy**, and then click **Edit**.
4. Under **Computer Configuration**, expand **Policies**, expand **Administrative Templates**, expand **System**, and then click **Access-Denied Assistance**.
5. In the details pane, double-click **Customize Message for Access Denied errors**.
6. In the Customize Message for Access Denied errors window, click **Enabled**.
7. In the **Display the following message to users who are denied access** text box, type **You are denied access because of permission policy. Please request access**.
8. Select the **Enable users to request assistance** check box. Review other options, but do not make any changes, and then click **OK**.
9. In the details pane of the Group Policy Management Editor, double-click **Enable access-denied assistance on client for all file types**. Click **Enabled**, and then click **OK**.
10. Close the Group Policy Management Editor and the Group Policy Management Console.
11. Switch to LON-SVR1, and on the taskbar, click the **Windows PowerShell** icon.
12. At the Windows PowerShell command prompt, type **gpupdate /force**, and then press Enter. Wait until Group Policy is updated for both user and computer.

3: Implementing Dynamic Access Control

Demonstration: Implementing Work Folders

In this demonstration, you will learn how to implement Work Folders

Preparation Steps

Note: To perform this demonstration, you must first perform Tasks 1 and 2, “Installing Work Folders functionality” and “Provisioning a share for Work Folders,” which are in Exercise 4 of the lab.

Demonstration Steps

1. On LON-SVR2, in Server Manager, click **File and Storage Services**, and then click **Work Folders**.
2. In the **WORK FOLDERS** tile, click **Tasks**, and then click **New Sync Share...**
3. In the New Sync Share Wizard, on the **Before you begin** page, click **Next**.
4. On the **Select the server and path** page, click **Select by file share**, ensure that **WF-Share** is highlighted, and then click **Next**.
5. On the **Specify the structure for user folders**, accept the default selection (User alias), and then click **Next**.
6. On the **Enter the sync share name** page, accept the default, and then click **Next**.
7. On the **Grant sync access to groups** page, note the default selection to disable inherited permissions and grant users exclusive access, and then click **Add**.
8. In the **Select User or Group** dialog box, in the **Enter the object names to select**, type **WFSync**, click **Check Names**, and then click **OK**.
9. On the **Grant sync access to groups** page, click **Next**.
10. On the **Specify device policies** page, note the selections, accept the default selection, and then click **Next**.
11. On the **Confirm selections** page, click **Create**.
12. On the **View results** page, click **Close**.
13. Switch to LON-DC1, and then sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
14. Open Server Manager, click **Tools**, and then click **Group Policy Management**.

3: Implementing Dynamic Access Control

15. Expand **Forest: Adatum.com-Domains-Adatum.com**, click **Group Policy Objects**, right-click the **Group Policy Objects** container, and then click **New**.
16. In the New GPO window, type **Work Folders GPO** in the **Name** field, and then click **OK**.
17. Right-click **Work Folders GPO**, and then click **Edit**.
18. In the Group Policy Management Editor, expand **User Configuration\ Policies\Administrative Templates\Windows Components**, and then click **Work Folders**.
19. Double-click **Specify Work Folders settings** in the details pane.
20. In the **Specify Work Folders settings** dialog box, click **Enabled**.
21. In the **Work Folders URL** text box, type **<https://lon-svr2.adatum.com>**, and then select **Force automatic setup**.
22. Click **OK** to close the **Specify Work Folders settings** dialog box, and then close the Group Policy Management Editor.
23. In the Group Policy Management Console, right-click the **Adatum.com** domain object, and then select **Link an Existing GPO...**
24. In the Select GPO window, select **Work Folders GPO**, and then click **OK**.
25. Close the Group Policy Management Console.

20412D

4: Implementing Distributed Active Directory® Domain Services Deployments

Demonstration: Installing a Domain Controller in a New Domain in an Existing Forest

In this demonstration, you will see how to:

- Configure an AD DS domain controller
- Access the AD DS domain controller

Preparation Steps

1. Start 20412D-LON-DC1, and sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.
2. Start 20412D-TOR-DC1, and sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

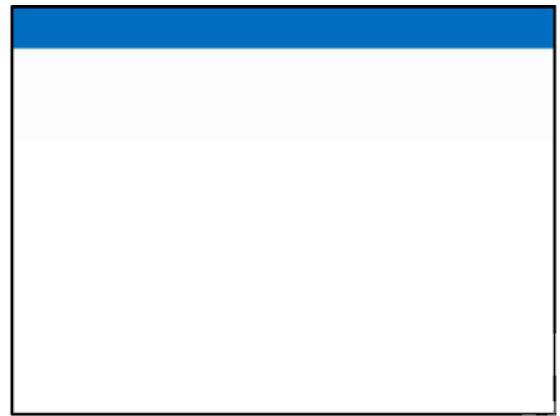
Install the AD DS binaries on TOR-DC1

1. On **TOR-DC1**, in the Server Manager, click **Add Roles and Features**.
2. In the Add Roles and Features Wizard, click **Next**.
3. On the **Select installation type** page, ensure that **Role-based or feature-based installation** is selected, and then click **Next**.
4. On the **Select destination server** page, ensure that **Select a server from the pool** is selected. In the **Server Pool** page, verify that **TOR-DC1.Adatum.com** is highlighted, and then click **Next**.
5. On the **Select server roles** page, select the **Active Directory Domain Services** check box, click **Add Features**, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Active Directory Domain Services** page, review the message, and then click **Next**.
8. On the **Confirm installation selections** page, review the message, and then click **Install**. Installation will take several minutes.
9. On the **Results** page, click **Promote this server to a domain controller**. The wizard continues.

Configure TOR-DC1 as an AD DS domain controller using the AD DS Installation Wizard

1. On the Deployment Configuration page, select the **Add a new domain to an existing forest** option, and then, next to **Select domain type**, confirm that **Child Domain** is selected.
2. In the Parent domain name field, verify that **Adatum.com** is listed.
3. In the **New domain name** box, type **NA**, and then click **Next**.
4. On the **Domain Controller Options** page, ensure that **Windows Server 2012 R2** is selected as (More notes on the next slide)

20412D
**4: Implementing Distributed Active
Directory® Domain Services
Deployments**



Domain functional level, that **Domain Name System (DNS) server** is selected, and that **Global Catalog (GC)** is selected.

5. In the **Type the Directory Services Restore Mode (DSRM) password** text boxes, type **Pa\$\$w0rd** in both boxes, and then click **Next**.
6. On the **DNS Options** page, click **Next**.
7. On the following three windows (**Additional Options**, **Paths**, and **Review Options**), click **Next**. In the **Prerequisites Check** window, click **Install**.
8. Review the information, and allow TOR-DC1 to reboot as an AD DS domain controller in the new AD DS domain that you created in the AD DS forest.
9. Sign in to TOR-DC1 as **NALAdministrator** with the password **Pa\$\$w0rd**, and review some of the AD DS tools to confirm the installation of the new domain.

20412D

4: Implementing Distributed Active Directory® Domain Services Deployments

Demonstration: Configuring a Forest Trust

In this demonstration, you will see how to:

- Configure DNS Name Resolution by using a conditional forwarder
- Configure a two-way selective forest trust

Explain to the students that in the lab they will configure a selective forest trust between adatum.com and treyresearch.net. They also will enable users to authenticate to the LON-SVR2 server, and they will test it.

Preparation Steps

- Start 20412D-LON-DC1, and sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**. LON-DC1 has an IP address of 172.16.0.10, and is configured to use itself as the primary DNS server.
- Start 20412D-TREY-DC1, and sign in as **treyresearch\Administrator** with the password **Pa\$\$w0rd**. TREY-DC1 has an IP address of 172.16.10.10, and is configured to use itself as the primary DNS server.

Demonstration Steps

Configure DNS name resolution by using a conditional forwarder

- On LON-DC1, in Server Manager, click the **Tools** menu, and in the drop-down list, click **DNS**. The DNS manager opens.
- In the DNS Manager, expand **LON-DC1**, click and then right-click **Conditional Forwarders**, and then click **New Conditional Forwarder**.
- In the New Conditional Forwarder window, in the **DNS Domain:** box, type **TreyResearch.net**.
- In the **IP addresses of the master servers:** text box, type **172.16.10.10**. Click in the open space, and then click **OK**. (If an error displays, ignore it).
- Close the **DNS Manager**.
- Switch to **TREY-DC1**, and repeat steps 1 through 5. Use the domain name **Adatum.com** with the IP address **172.16.0.10**.

Configure a two-way selective forest trust

- In LON-DC1, from the **Tools** menu, click **Active Directory Domains and Trusts**.
- When the Active Directory Domains and Trusts window opens, right-click **Adatum.com**, and then



click **Properties**.

3. In the **Adatum.com Properties** dialog box, on the **Trusts** tab, click **New Trust**.
4. In the **New Trust Wizard**, click **Next**.
5. On the **Trust Name** page, in the **Name** text box, type **treyresearch.net**, and then click **Next**.
6. In the **New Trust Wizard**, click **Forest trust**, and then click **Next**.
7. In the **Direction of Trust** page, click **Two-way**, and then click **Next**.
8. In the **Sides of Trust** page, click **Both this domain and the specified domain**, and then click **Next**.
9. In the **User name:** text box, type **Administrator**. In the **Password** text box, type **Pa\$\$w0rd**, and then click **Next**.
10. In the **Outgoing Trust Authentication Level--Local Forest** page, click **Selective authentication**, and then click **Next**.
11. In the **Outgoing Trust Authentication Level-Specified Forest** page, click **Selective authentication**, and then click **Next**.
12. In the **Trust Selections Complete** page, click **Next**.
13. In the **Trust Creation Complete** page, click **Next**.
14. In the **Confirm Outgoing Trust** page, click **Yes, confirm the outgoing trust**, and then click **Next**.
15. In the **Confirm Incoming Trust** page, click **Yes, confirm the incoming trust**, and then click **Next**.
16. On the **Completing the New Trust Wizard** page, click **Finish**.
17. In the **Adatum.com Properties** dialog box, click **OK**.

20412D

5: Implementing Active Directory

Domain Services Sites and Replication

Demonstration: Configuring AD DS Sites

In this demonstration, you will see how to configure AD DS sites

Demonstrate or discuss the most basic procedures for creating a site and assigning a subnet to the site.

Mention that many of these tasks require credentials provided by the Enterprise Admin or Domain Admin of the root domain, by default, but that you can delegate them.

Mention to the students that the default site-link, DEFAULTTIPSITELINK, will be the only site-link available until you create additional site-links.

Preparation Steps

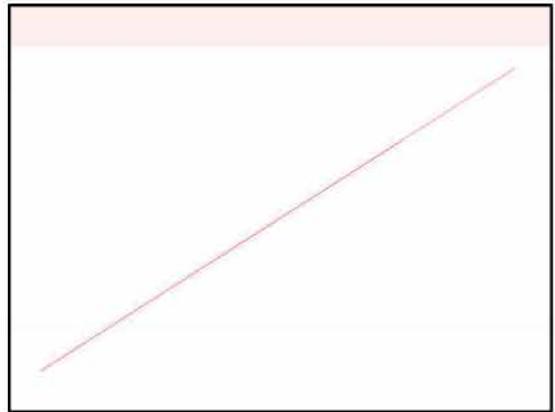
To complete this demonstration, you must ensure that the 20412D-LON-DC1 and the 20412D-TOR-DC1 virtual machines are running. Sign in on all virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Note: To complete this and subsequent demonstrations, you also need to complete Lab A, Exercise 1, Task 1. This will configure TOR-DC1 as a domain controller.

Demonstration Steps

1. On LON-DC1, in the Server Manager, click **Tools**, and then click **Active Directory Sites and Services**.
2. In Active Directory Sites and Services, expand **Sites**, and then click **Default-First-Site-Name**.
3. Right-click **Default-First-Site-Name**, and then click **Rename**.
4. Type **LondonHQ**, and then press Enter.
5. In the navigation pane, right-click **Sites**, and then click **New Site**.
6. In the **New Object – Site** dialog box, in the **Name** text box, type **Toronto**.
7. Select **DEFAULTTIPSITELINK**, and then click **OK**.
8. In the **Active Directory Domain Services** dialog box, click **OK**.
9. In the navigation pane, right-click **Subnets**, and then click **New Subnet**.

20412D
5: Implementing Active Directory
Domain Services Sites and
Replication



10. In the **New Object – Subnet** dialog box, in the **Prefix** text box, type **172.16.0.0/24**.
11. Under **Select a site object for this prefix**, click **LondonHQ**, and then click **OK**.
12. In the navigation pane, right-click **Subnets**, and then click **New Subnet**.
13. In the **New Object – Subnet** dialog box, in the **Prefix** text box, type **172.16.1.0/24**.
14. Under **Select a site object for this prefix**, click **Toronto**, and then click **OK**.
15. In the navigation pane, expand **LondonHQ**, and then expand **Servers**.
16. Right-click **TOR-DC1**, and then click **Move**.
17. In the **Move Server** dialog box, select **Toronto**, and then click **OK**.
18. In the navigation pane, expand **Toronto**, and then expand **Servers**.
19. Verify that TOR-DC1 is now located in the Toronto Site.

20412D

5: Implementing Active Directory Domain Services Sites and Replication

Demonstration: Configuring AD DS Intersite Replication

In this demonstration, you will see how to configure AD DS intersite replication

Preparation Steps

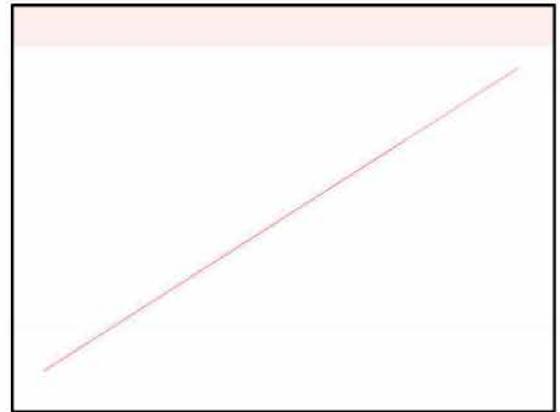
To complete this demonstration, you must have the 20412D-LON-DC1 and 20412D-TOR-DC1 virtual machines running. Sign in on all virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

You also must have completed all previous demonstrations in this module.

Demonstration Steps

1. On TOR-DC1, in Server Manager, click **Tools**, and then click **Active Directory Sites and Services**.
2. In Active Directory Sites and Services, expand **Sites**, and then expand **Inter-Site Transports**.
3. Click **IP**, right-click **DEFAULTIPSITELINK**, and then click **Rename**.
4. Type **LON-TOR**, and then press Enter.
5. Right-click **LON-TOR**, and then click **Properties**. Explain the **Cost**, **Replicate every**, and **Change Schedule** options.
6. In the **LON-TOR Properties** dialog box, next to **Replicate every**, configure the value to be **60** minutes.
7. Click **Change Schedule**.
8. Highlight the range from **Monday 12 PM** to **Friday 4 PM**, as follows:
 - Using the mouse, click at the Monday at 12:00 PM tile.
 - With the mouse button still pressed down, drag the cursor to the Friday at 4:00 PM tile.
9. Click **Replication Not Available** and then click **OK**.
10. Click **OK** to close the **LON-TOR Properties** dialog box.
11. In the navigation pane, right-click **IP**, and then click **Properties**.
12. In the **IP Properties** dialog box, point out and explain the **Bridge all site links** option.

20412D
5: Implementing Active Directory
Domain Services Sites and
Replication



13. Click **OK** to close the **IP Properties** dialog box.

20412D

5: Implementing Active Directory Domain Services Sites and Replication

Demonstration: Configuring Password Replication Policies

In this demonstration, you will see how to configure password replication policies

Preparation Steps

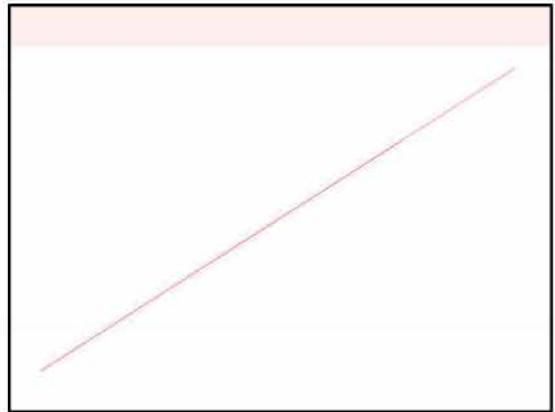
To complete this demonstration, you must ensure that the 20412D-LON-DC1 and 20412D-TOR-DC1 virtual machines are running. Sign in on all virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

You must also have completed all previous demonstrations in this module.

Demonstration Steps

1. On LON-DC1, from Server Manager, click **Tools**, and then click **Active Directory Users and Computers**.
2. In the console tree, expand the **Adatum.com** domain, and then click the **Domain Controllers** organizational unit (OU).
3. Right-click **Domain Controllers**, and then click **Pre-create Read-only Domain Controller account**.
4. In the Active Directory Domain Services Installation Wizard, on the **Welcome** page, click **Next**.
5. On the **Network Credentials** page, click **Next**.
6. On the **Specify the Computer Name** page, type **LON-RODC1**, and then click **Next**.
7. On the **Select a Site** page, click **Toronto**, and then click **Next**.
8. On the **Additional Domain Controller Options** page, click **Next**.
9. On the **Delegation of RODC Installation and Administration** page, click **Next**.
10. Review your selections on the **Summary** page, and then click **Next**.
11. On the **Completing the Active Directory Domain Services Installation Wizard** page, click **Finish**.
12. In the console, click the **Domain Controllers** OU.
13. Right-click **LON-RODC1**, and then click **Properties**.

20412D
5: Implementing Active Directory
Domain Services Sites and
Replication



14. Click the **Password Replication Policy** tab, and then view the default policy.
15. Click **Cancel** to close **LON-RODC1 Properties**.
16. In the **Active Directory Users and Computers** console, click the **Users** container.
17. Double-click **Allowed RODC Password Replication Group**, and then click the **Members** tab.
18. Examine the default membership of Allowed RODC Password Replication Group, and then click **OK**. There should be no members by default.
19. Double-click **Denied RODC Password Replication Group**.
20. Click the **Members** tab.
21. Click **Cancel** to close the **Denied RODC Password Replication Group** properties.

6: Implementing AD CS

Demonstration: Signing a Document Digitally

In this demonstration, your instructor will show you how to digitally sign a document in Microsoft Word

After you have finished this demo, leave the virtual machines running for the next demo.

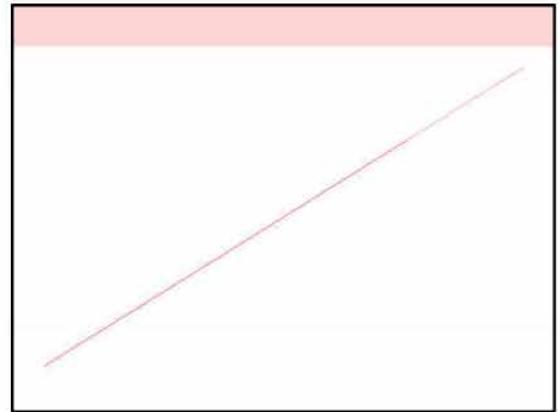
Preparation Steps

For this demonstration, you will need the 20412D-LON-DC1 and 20412D-LON-CL1 virtual machines. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**. After you have finished this demo, leave the virtual machines running for the next demo.

Demonstration Steps

1. On LON-CL1, open Windows PowerShell®.
2. At the Windows PowerShell command prompt, type **mmc.exe**, and then press Enter.
3. Click the **File** menu, and then select **Add/Remove Snap-in**.
4. Select **Certificates**, click **Add**, select **My user account**, click **Finish**, and then click **OK**.
5. Expand **Certificates-Current User**, right-click **Personal**, select **All Tasks**, and then click **Request New Certificate**.
6. In the Certificate Enrollment Wizard, click **Next** twice.
7. On the **Certificate Enrollment** page, in the list of available templates, select **User**, click **Enroll**, and then click **Finish**.
8. Close the **Console 1** window without saving changes.
9. Open Microsoft Word 2013.
10. In a blank document, type some text, and then save the file to the desktop.
11. On the toolbar, click **INSERT**, and then in the **Text** pane, in the **Signature Line** drop-down list box, click **Microsoft Office Signature Line**.
12. In the **Signature setup** window, type your name in the **Suggested signer** text box, type **Administrator** in the **Suggested signer's title** text box, type **Administrator@adatum.com** in the

6: Implementing AD CS



Suggested signer's email address text box, and then click **OK**.

13. Right-click the signature line in the document, and then click **Sign...**
14. In the **Sign** window, click **Change**.
15. On the **Certificate** list, select the certificate with today's date, and then click **OK**.
16. In the text box right to the sign X, type your name, click **Sign**, and then click **OK**.

Note: Explain to the students that besides typing your name, you also can select an image instead. This image can be your scanned, handwritten signature.

17. Ensure that the document cannot be edited anymore.
18. Close Word 2013, and save the changes when prompted.
19. Stay signed in for the next demonstration.

6: Implementing AD CS

Demonstration: Deploying a Root CA

In this demonstration, you will see how to deploy an enterprise root CA

When you have completed the demonstration, leave the virtual machines running for the subsequent demonstrations.

Preparation Steps

This demonstration is mandatory to perform, because it establishes the PKI and CA that you will use in the following demonstrations in this module.

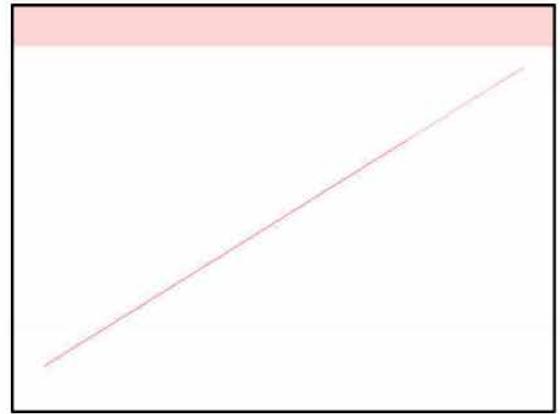
For this demonstration, start 20412D-LON-DC1 and 20412D-LON-SVR1. Sign in to both virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Deploy a root CA

1. On LON-SVR1, in the Server Manager, click **Add roles and features**.
2. On the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, select **Active Directory Certificate Services**. In the Add Roles and Features Wizard, click **Add Features**, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Active Directory Certificate Services** page, click **Next**.
8. On the **Select role services** page, ensure that **Certification Authority** is selected, and then click **Next**.
9. On the **Confirm installation selections** page, click **Install**.
10. On the **Installation progress** page, after the installation completes successfully, click the text **Configure Active Directory Certificate Services on the destination server**.

6: Implementing AD CS



11. In the AD CS Configuration Wizard, on the **Credentials** page, click **Next**.
12. On the **Role Services** page, select **Certification Authority**, and then click **Next**.
13. On the **Setup Type** page, select **Enterprise CA**, and then click **Next**.
14. On the **CA Type** page, click the **Root CA** option, and then click **Next**.
15. On the **Private Key** page, ensure that **Create a new private key** is selected, and then click **Next**.
16. On the **Cryptography for CA** page, keep the default selections for Cryptographic Service Provider (CSP) and Hash Algorithm, but set the **Key length** to **4096**, and then click **Next**.
17. On the **CA Name** page, in the **Common name for this CA** box, type **AdatumRootCA**, and then click **Next**.
18. On the **Validity Period** page, click **Next**.
19. On the **CA Database** page, click **Next**.
20. On the **Confirmation** page, click **Configure**.
21. On the **Results** page, click **Close**.
22. On the **Installation progress** page, click **Close**.

6: Implementing AD CS

Demonstration: Configuring CA Properties

In this demonstration, your instructor will show you how to configure CA properties

When you have completed the demonstration, leave the virtual machines running for the subsequent demonstrations.

Preparation Steps

For this demonstration, you will need the 20412D-LON-DC1 and 20412D-LON-SVR1 virtual machines. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

1. On LON-SVR1, open the Server Manager, click **Tools**, and then click **Certification Authority**.
2. In the certsrv console, right-click **AdatumRootCA**, and then select **Properties**.
3. On the **General** tab, click **View Certificate**. When the Certificate window opens, review the data on the **General**, **Details**, and **Certification Path** tabs, and then click **OK**.
4. On the **Policy Module** tab, click **Properties**. Review the settings available for the Default policy module, and then click **OK**.
5. On the **Exit Module** tab, click **Properties**. Show the Publication Settings available in the default Exit module, and then click **OK**.
6. On the **Extensions** tab, review the options available for the certificate revocation list distribution point (CDP) and authority information access (AIA) locations.
7. On the **Security** tab, review the available options on the access control list (ACL), and then review the default permissions.
8. On the **Certificate Managers** tab, review the options and explain how to restrict security principals to specific certificate templates, and then click **Cancel**.
9. Close the certsrv console

6: Implementing AD CS

Demonstration: Modifying and Enabling a Certificate Template

In this demonstration, you will see how to modify and enable a certificate template.

When you have completed the demonstration, leave the virtual machines running for the subsequent demonstrations.

Preparation Steps

For this demonstration, start 20412D-LON-DC1 and 20412D-LON-SVR1. Sign in to both virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

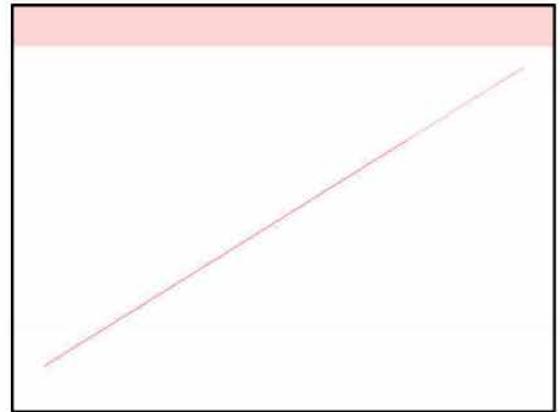
Be sure to complete all previous demonstrations before you begin this demonstration.

Demonstration Steps

Modify and enable a certificate template

1. On LON-SVR1, on the taskbar, click the **Server Manager** icon.
2. In the Server Manager, click **Tools**, and then click **Certification Authority**.
3. In the Certification Authority console, expand **AdatumRootCA**, right-click **Certificate Templates**, and then click **Manage**.
4. Review the list of default templates. Examine the templates and their properties.
5. In the **Details** pane, double-click **IPsec**.
6. In the **IPsec Properties** dialog box, scroll through the tabs, and note what you can modify on each tab. Note that on the Security tab, you can define permissions for enrollment. Click **Cancel** to close the template.
7. In the Certificate Templates console, in the Details pane, right-click the **Exchange User** certificate template, and then click **Duplicate Template**.
8. In the **Properties of New Template** dialog box, review options on the **Compatibility** tab.
9. Click the **General** tab, and then in the **Template display name** text box, type **Exchange User Test1**.
10. Click the **Superseded Templates** tab, and then click **Add**.

6: Implementing AD CS



11. Click the **Exchange User** template, and then click **OK**.
12. Click the **Security** tab, and then click **Authenticated Users**.
13. Under the **Permissions for Authenticated Users** node, select the **Allow** check boxes for **Read**, **Enroll**, and **Autoenroll**, and then click **OK**.
14. Close the Certificate Templates console.
15. In the Certification Authority console, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template to Issue**.
16. In the **Enable Certificate Templates** dialog box, select the **Exchange User Test1** certificate, and then click **OK**.

6: Implementing AD CS

Demonstration: Configuring the Restricted Enrollment Agent

In this demonstration, you will see how to configure the Restricted Enrollment Agent.

When you have completed the demonstration, leave the virtual machines running for the subsequent demonstrations.

Preparation Steps

For this demonstration, start 20412D-LON-DC1, 20412D-LON-SVR1, and 20412D-LON-CL1. Sign in to 20412D-LON-DC1 and 20412D-LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Do not sign in to 20412D-LON-CL1 until directed to do so.

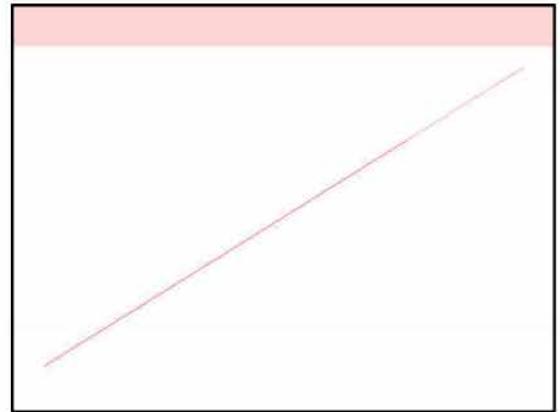
Be sure to complete all previous demonstrations before you start this demonstration.

Demonstration Steps

Configure the Restricted Enrollment Agent

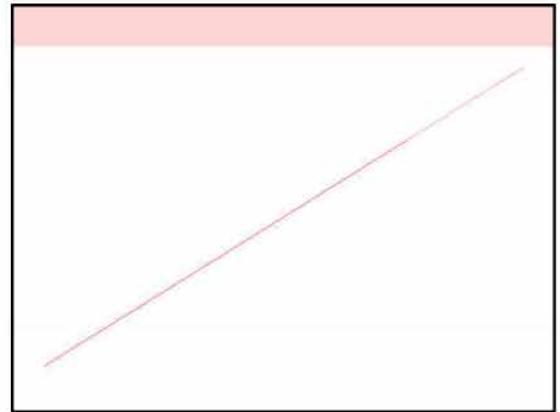
1. On LON-SVR1, on the taskbar, click the **Server Manager** icon.
2. In the Server Manager console, click **Tools**, and then open the **Certification Authority**.
3. In the certsrv console, expand **AdatumRootCA**, right-click **Certificate Templates**, and then click **Manage**.
4. In the Certificate Templates console, double-click **Enrollment Agent**, click the **Security** tab, and then click **Add**.
5. In the Select Users, Computers, Service Accounts, or Groups window, type **Allie**, click **Check Names**, and then click **OK**.
6. On the **Security** tab, click **Allie Bellew**, select **Allow for Read** and **Enroll** permissions, and then click **OK**.
7. Close the Certificate Templates console.
8. In the certsrv console, right-click **Certificate Templates**, point to **New**, and then click **Certificate Template to Issue**.

6: Implementing AD CS



9. In the list of templates, click **Enrollment Agent**, and then click **OK**.
10. Switch to LON-CL1, and sign in as **Adatum\Allie** with the password **Pa\$\$w0rd**.
11. On the Start screen, type **mmc.exe**, and then press Enter.
12. In **Console1**, open the **File** menu, and then click **Add/Remove Snap-in**.
13. Click **Certificates**, click **Add**, and then click **OK**.
14. Expand **Certificates – Current User**, and then click **Personal**.
15. Right-click **Personal**, point to **All Tasks**, and then click **Request New Certificate**.
16. In the Certificate Enrollment Wizard, on the **Before You Begin** page, click **Next**.
17. On the **Select Certificate Enrollment Policy** page, click **Next**.
18. On the **Request Certificates** page, select **Enrollment Agent**, click **Enroll**, and then click **Finish**.
19. Switch to **LON-SVR1**.
20. In the Certification Authority console, right-click **AdatumRootCA**, and then click **Properties**.
21. In the **AdatumRootCA Properties** dialog box, click the **Enrollment Agents** tab.
22. On the **Enrollment Agents** tab, click **Restrict Enrollment agents**.
23. In the pop-up window, click **OK**.
24. On the **Enrollment Agents** tab, under **Enrollment Agents**, click **Add**.
25. In the Select User, Computer, or Group window, type **Allie**, click **Check Names**, and then click **OK**.
26. Click **Everyone**, and then click **Remove**.
27. In the **certificate templates** section, click **Add**.
28. In the list of templates, select **User**, and then click **OK**.
29. In the **Certificate Templates** section, click **<All>**, and then click **Remove**.
30. In the permission section, click **Add**.

6: Implementing AD CS



31. In the Select User, Computer, or Group window, type **Marketing**, click **Check Names**, and then click **OK**.
32. In the Permission section, click **Everyone**, click **Remove**, and then click **OK**.

6: Implementing AD CS

Demonstration: Configuring an Online Responder

In this demonstration, you will see how to configure an Online Responder.

When you have completed the demonstration, leave the virtual machines running for the subsequent demonstrations.

Preparation Steps

For this demonstration, start 20412D-LON-DC1 and 20412D-LON-SVR1. Sign in to both virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

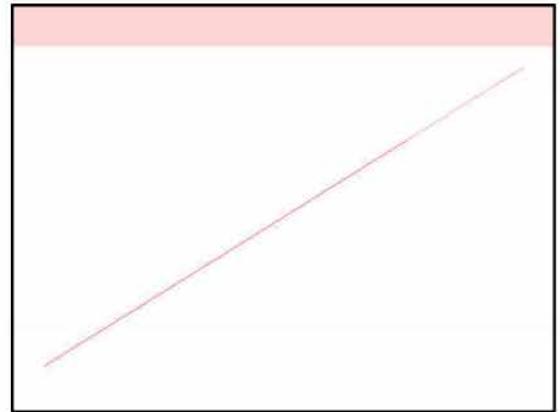
Be sure to complete all previous demonstrations before you start this demonstration.

Demonstration Steps

Configure an Online Responder

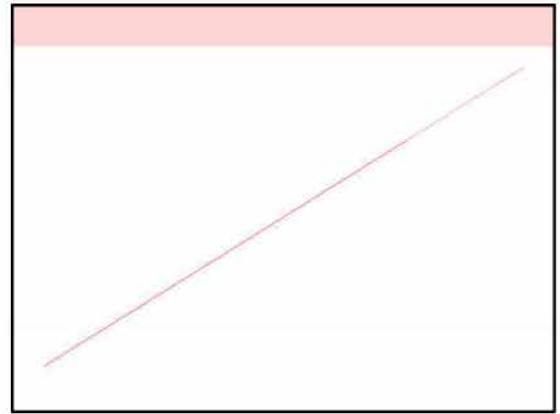
1. On LON-SVR1, on the taskbar, click the **Server Manager** icon.
2. In the **Server Manager**, click **Add roles and features**.
3. Click **Next** three times.
4. On the **Select server roles** page, expand **Active Directory Certificate Services (1 of 6 installed)**, and then select **Online Responder**.
5. Click **Add Features**.
6. Click **Next** two times, and then click **Install**.
7. When the message displays that installation is successful, click **Configure Active Directory Certificate Services on the destination server**.
8. In the AD CS Configuration Wizard, click **Next**.
9. Select **Online Responder**, and then click **Next**.
10. Click **Configure**, and then click **Close** two times.
11. In the **Server Manager** console, click **Tools**, and then click the Certification Authority console on **LON-SVR1**.
12. In the Certification Authority console, right-click **AdatumRootCA**, and then click **Properties**.

6: Implementing AD CS



13. In the **AdatumRootCA Properties** dialog box, on the **Extensions** tab, in the **Select extension** list, click **Authority Information Access (AIA)**, and then click **Add**.
14. In the **Add Location** dialog box, type **http://LON-SVR1/ocsp**, and then click **OK**.
15. Select the **Include in the AIA extension of issued certificates** check box.
16. Select the **Include in the online certificate status protocol (OCSP) extension** check box, and then click **OK**.
17. In the **Certificate Authority** box, restart Active Directory Certificate Services by clicking **Yes**.
18. In the certsrv console, expand **AdatumRootCA**, right-click the **Certificate Templates** folder, and then click **Manage**.
19. In the Certificate Templates console, double-click the **OCSP Response Signing** template.
20. In the **OCSP Response Signing Properties** dialog box, click the **Security** tab. Under **Permissions for Authenticated Users**, select the **Allow for Enroll** check box, and then click **OK**.
21. Close the Certificate Templates console.
22. In the Certification Authority console, right-click the **Certificate Templates** folder, point to **New**, and then click **Certificate Template to Issue**.
23. In the **Enable Certificate Templates** dialog box, select the **OCSP Response Signing** template, and then click **OK**.
24. On LON-SVR1, in Server Manager, click **Tools**, and then click **Online Responder Management**.
25. In the Online Responder Management console, right-click **Revocation Configuration**, and then click **Add Revocation Configuration**.
26. In the Add Revocation Configuration Wizard, click **Next**.
27. On the **Name the Revocation Configuration** page, in the **Name** text box, type **AdatumCA Online Responder**, and then click **Next**.

6: Implementing AD CS



28. On the **Select CA Certificate Location** page, click **Next**.
29. On the **Choose CA Certificate** page, click **Browse**, click the **AdatumRootCA** certificate, click **OK**, and then click **Next**.
30. On the **Select Signing Certificate** page, verify that both **Automatically select a signing certificate is selected** and **Auto-Enroll for an OCSP signing certificate** are selected, and then click **Next**.
31. On the **Revocation Provider** page, click **Finish**. The revocation configuration status will display as **Working**.
32. Close the Online Responder console.

6: Implementing AD CS

Demonstration: Configuring a CA for Key Archival

In this demonstration, you will see how to configure a CA for key archival.

When you have completed the demonstration, leave the virtual machines running for the subsequent demonstrations.

Preparation Steps

For this demonstration, start 20412D-LON-DC1 and 20412D-LON-SVR1. Sign in to both virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Be sure to complete all previous demonstrations before you start this demonstration.

Demonstration Steps

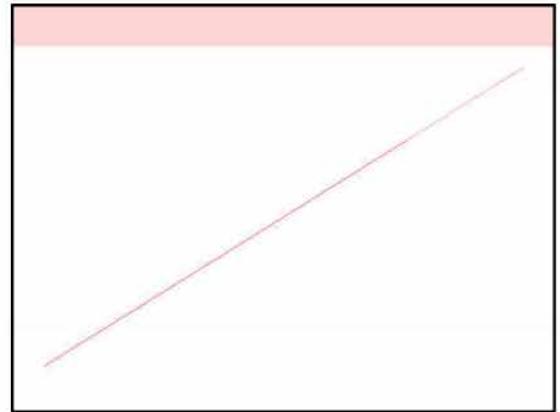
Configure automatic key archival

1. On LON-SVR1, open the Certification Authority console.
2. In the Certificate Authority console, expand the **AdatumRootCA** node, right-click the **Certificate Templates** folder, and then click **Manage**.
3. In the Details pane, right-click the **Key Recovery Agent** certificate, and then click **Properties**.
4. In the **Key Recovery Agent Properties** dialog box, on the **Issuance Requirements** tab, clear the **CA certificate manager approval** check box.

Note: This is for test purposes only. In a production environment, you should not change this value.

5. On the **Security** tab, notice that Domain Admins and Enterprise Admins are the only groups that have the Enroll permission, and then click **OK**. Make no changes here.
6. Close the Certificates Templates console.
7. In the Certificate Authority console, right-click **Certificate Templates**, click **New**, click **Certificate Template to issue**, click **Key Recovery Agent**, and then click **OK**. This process configures a CA to issue certificates based on the Key Recovery Agent template.
8. Click the **Start** screen, type **mmc.exe**, and then press Enter.
9. In the Console 1 window, click **File**, and then click **Add/remove Snap-In**.

6: Implementing AD CS



10. On the **Add/Remove Snap-ins** page, select **Certificates**, and then click **Add**.
11. Select **My user account**, click **Finish**, and then click **OK**.
12. Expand **Certificates - Current User**, and then click **Personal**. Right-click **Personal**, select **All tasks**, and then click **Request New Certificate**.
13. In the Certificate Enrollment Wizard, click **Next** twice.
14. On the **Request Certificates** page, select **Key Recovery Agent**, and then click **Enroll**.
15. Click **Finish**.
16. Confirm that the new certificate displays in the Certificates store. If it displays, then you have enrolled the Administrator as the KRA. Minimize the Certificates console.
17. Open the properties of AdatumRootCA.
18. On the **Recovery Agents** tab, click **Archive the Key**, click **Add**, and then select the **Administrator** certificate. Click **OK**.
19. Click **OK**, and then click **Yes** to restart AD CS.
20. Right-click **Certificate Templates**, and then click **Manage**.
21. Double-click the **Exchange User Test1** certificate to open the **Properties** dialog box. On the **Request Handling** tab, click both **Archive subject's encryption private key** and **Include symmetric algorithms allowed by the subject**. If a popup window displays, click **OK**.
22. Click **OK** to close the template.

6: Implementing AD CS

Demonstration: Recovering a Lost Private Key

In this demonstration, you will see how to recover a lost private key

When you have completed the demonstration, revert the virtual machines to their initial state.

Preparation Steps

For this demonstration, start 20412D-LON-DC1 and 20412D-LON-SVR1. Sign in to both virtual machines as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Be sure to complete all previous demonstrations before you start this demonstration.

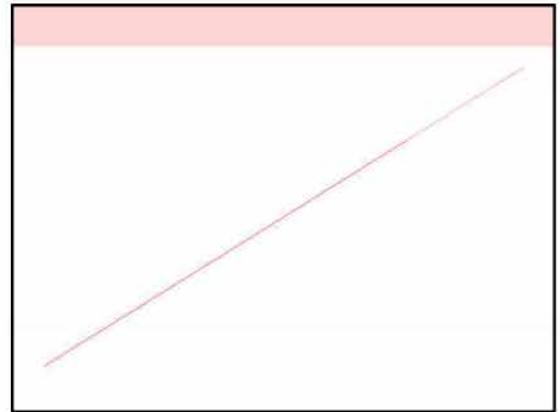
If you do not have enough time, you can skip this demonstration, because the students will be doing this in a lab.

Demonstration Steps

Recover a lost private key

1. On LON-SVR1, click to the **Start** screen, type **mmc.exe**, and then press Enter.
2. Click **File**, and then click **Add/Remove Snap-in**.
3. Select **Certificates**, and then click **Add**.
4. Click **My user account**, click **Finish**, and then click **OK**.
5. Expand **Certificates - Current User**, expand **Personal**, and right-click **Certificates**. Select **All tasks**, and then click **Request New Certificate**. Click **Next** twice.
6. Enroll for the Exchange User Test1 certificate by using the wizard. When you select the **Exchange User Test1** template in the wizard, click to open settings to enter Subject name. In the **Type** list, click **Email**, in the value field, type **administrator@adatum.com**, click **Add**, click **OK**, and then click **Enroll**. Click **Finish**.
7. Verify that the certificate displays in the Personal->Certificates store.
8. Simulate a lost private key by deleting the **administrator@adatum.com** certificate from the Personal certificate store. Right-click **administrator@adatum.com**, click **Delete**, and then click **Yes**. Minimize the Certificates (Console1) console.

6: Implementing AD CS



9. In the Certification Authority console, in the **Issued Certificates** folder, double-click the certificate with **Exchange User Test1** as the template name. This is the certificate that you issued in an earlier step. From the **Details** tab, record the serial number. (You can copy and paste it to Notepad, and then remove spaces between numbers.)
10. Open a command-prompt window with elevated privileges. (On the **Start** menu, type **cmd**, right-click **Command Prompt**, and then click **Run as Administrator**.)
11. In the command-prompt window, switch to the root of drive C by typing **cd..**, and then press Enter. (You might have to do this twice.)
12. Select the certificate serial number from Notepad, right-click it, and then select **Copy**.
13. Switch back to the command-prompt window, and type the following command, where **<serialnumber>** is a number that you paste from Notepad:

Certutil -getkey <serialnumber> outputblob

Press Enter.

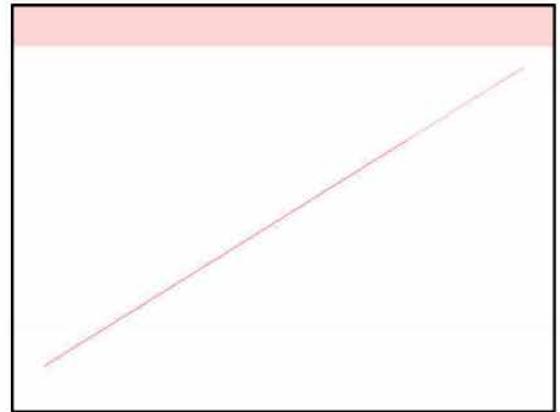
Note: If a question mark appears at the beginning of the number after you paste it in, delete it. Also, ensure that you remove all spaces from the serial number, or enclose the serial number in quotation marks.

14. After the command completes successfully, open drive C and verify that the **Outputblob** file displays.
15. Switch back to the command-prompt window. At a command prompt, type the following, and then press Enter:

Certutil -recoverkey outputblob recover.pfx

16. When prompted, type **Pa\$\$w0rd** as the new password, and then confirm the password.
17. Browse to drive C, and then verify that the Recover.pfx file—the recovered key—is created.

6: Implementing AD CS



18. Right-click the file **recover.pfx**, and then click **Install PFX**. (Note: If Install PFX option is not available, select **Open with**, and then click **Crypto Shell Extensions**.)
19. Click **Next** two times.
20. Enter the password **Pa\$\$w0rd**, click **Next** twice, click **Finish**, and then click **OK**.
21. Restore the Certificates console (Console 1). Refresh the Certificates store.
22. Verify that the **administrator@adatum.com** certificate now displays.

7: Implementing Active Directory Rights Management Services

Demonstration: Installing the First Server of an AD RMS Cluster

In this demonstration, you will see how to install the first server of an AD RMS cluster

When you are working through the demonstration, show the students all of the steps that you need to take prior to deploying AD RMS. You should discuss the requirements of the service account. Mention that in production environments, you should consider using a managed service account.

Make clear to the students that the cluster address must be correct. If the cluster address is configured incorrectly, they will have to delete the service connection point AD DS object.

Mention to the students that in a production environment, they would use an encrypted connection rather than an unencrypted connection when they configure the cluster address.

Preparation Steps

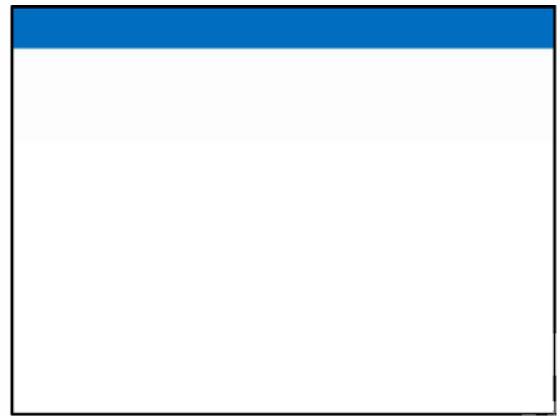
Ensure that the 20412D-LON-DC1 and 20412D-LON-SVR1 virtual machines are running. Sign in to LON-DC1 as **Adatum\Administrator** using the password **Pa\$\$w0rd**.

Demonstration Steps

Configure Service Account

1. On **LON-DC1**, in the Server Manager, click **Tools**, and then click **Active Directory Administrative Center**.
2. Select and then right-click **Adatum (local)**, click **New**, and then click **Organizational Unit**.
3. In the **Create Organizational Unit** dialog box, in the **Name** text box, type **Service Accounts**, and then click **OK**.
4. Right-click the **Service Accounts** organizational unit (OU), click **New**, and then click **User**.
5. In the **Create User** dialog box, enter the following details, and then click **OK**:
 - First name: **ADRMSSVC**
 - User UPN logon: **ADRMSSVC**

7: Implementing Active Directory Rights Management Services



Password: **Pa\$\$w0rd**

2. Confirm Password: **Pa\$\$w0rd**
3. Password never expires: **Enabled**
4. User cannot change password: **Enabled**
5. Close the **Active Directory Administrative Center**.

Prepare DNS

1. In the Server Manager, click **Tools**, and then click **DNS**.
2. In the DNS Manager console, expand **LON-DC1**, and then expand **Forward Lookup Zones**.
3. Select and then right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the **New Host** dialog box, enter the following information, and then click **Add Host**:
 - 5. Name: **adrms**
 - 6. IP address: **172.16.0.21**
7. Click **OK**, and then click **Done**.
8. Close the DNS Manager console.

Install the AD RMS role

1. Sign in to LON-SVR1 with the **Adatum\Administrator** account and the password **Pa\$\$w0rd**.
2. In the Server Manager, click **Manage**, and then click **Add Roles and Features**.
3. In the Add Roles and Features Wizard, click **Next** three times.
4. On the **Server Roles** page, click **Active Directory Rights Management Services**.
5. In the **Add Roles and Features Wizard** dialog box, click **Add Features**, and then click **Next** four times.

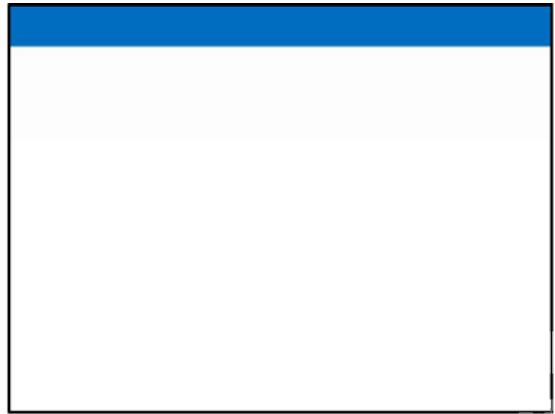
7: Implementing Active Directory Rights Management Services

6. Click **Install**, and when it finishes, click **Close**.

Configure AD RMS

1. In Server Manager, click the **AD RMS** node.
2. Next to **Configuration required for Active Directory Rights Management Services at LON-SVR1**, click **More**.
3. On the **All Servers Task Details and Notifications** page, click **Perform additional configuration**.
4. In the **AD RMS Configuration: LON-SVR1.Adatum.com** dialog box, click **Next**.
5. On the **AD RMS Cluster** page, click **Create a new AD RMS root cluster**, and then click **Next**.
6. On the **Configuration Database** page, click **Use Windows Internal Database on this server**, and then click **Next**.
7. On the **Service Account** page, click **Specify**.
8. In the **Windows Security** dialog box, enter the following details, click **OK**, and then click **Next**:
 - Username: **ADRMSSVC**
 - Password: **Pa\$\$w0rd**
9. On the **Cryptographic Mode** page, click **Cryptographic Mode 2**, and then click **Next**.
10. On the **Cluster Key Storage** page, click **Use AD RMS centrally managed key storage**, and then click **Next**.
11. On the **Cluster Key Password** page, enter the password **Pa\$\$w0rd** twice, and then click **Next**.
12. On the **Cluster Web Site** page, verify that the **Default Web Site** is selected, and then click **Next**.
13. On the **Cluster Address** page, provide the following information, and then click **Next**:
 - Connection Type: **Use an unencrypted connection (http://)**

7: Implementing Active Directory Rights Management Services



- Fully-Qualified Domain Name: adrms.adatum.com
 - \Port: **80**
14. On the **Licensor Certificate** page, type **Adatum AD RMS**, and then click **Next**.
 15. On the **SCP Registration** page, click **Register the SCP now**, and then click **Next**.
 16. Click **Install**, and then click **Close**. The installation might take several minutes.
 17. Click to the Start screen, click **Administrator**, and then click **Sign Out**.

Note: You must sign out before you can manage AD RMS.

7: Implementing Active Directory Rights Management Services

Demonstration: Creating a Rights policy Template

In this demonstration, you will see how to create a rights policy template that allows users to view a document, but not to perform other actions.

When you create the rights policy template, discuss the other options that are available, and why you would use them. For example, discuss why you would add multiple groups with different rights to the same template.

Discuss the benefit of including revocation in templates that have sensitive information.

Preparation Steps

Ensure that the 20412D-LON-DC1 and 20412D-LON-SVR1 virtual machines are running.

Before you perform this demonstration, you need to create a global security group named **Executives**, and associate the email address **executives@adatum.com** with this group. See Exercise 1, Task 1, step 9 and 10 for instructions.

Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

1. In the Server Manager, click **Tools**, and then click **Active Directory Rights Management Services**.
2. In the Active Directory Rights Management Services console, click the **lon-svr1 (Local)\Rights Policy Templates** node.
3. In the Actions pane, click **Create Distributed Rights Policy Template**.
4. In the Create Distributed Rights Policy Template Wizard, on the **Add Template Identification Information** page, click **Add**.
5. On the **Add New Template Identification Information** page, enter the following information, then click **Add**, and then click **Next**:
 - Language: **English (United States)**
 - Name: **ReadOnly**
 - Description: **Read-only access. No copy or print.**
6. On the **Add User Rights** page, click **Add**.

7: Implementing Active Directory Rights Management Services

7. On the **Add User or Group** page, type **executives@adatum.com**, and then click **OK**.
8. When **executives@adatum.com** is selected, under **Rights**, click **View**. Verify that **Grant owner (author) full control right with no expiration** is selected, and then click **Next**.
9. On the **Specify Expiration Policy** page, choose the following settings, and then click **Next**:
 - Content Expiration: Expires after the following duration (days): **7**
 - Use license expiration: Expires after the following duration (days): **7**
10. On the **Specify Extended Policy** page, click **Require a new use license every time content is consumed (disable client-side caching)**, click **Next**, and then click **Finish**.

Demonstration: Creating an Exclusion Policy to Exclude an Application

In this demonstration, you will see how to exclude the Microsoft PowerPoint application from AD RMS

When you perform this demonstration, describe to the students the scenarios where they would want to exempt particular applications from AD RMS. In addition, reiterate that it is necessary to use the appropriate version notation.

Preparation Steps

Ensure that the 20412D-LON-DC1 and 20412D-LON-SVR1 virtual machines are running.

Demonstration Steps

1. On LON-SVR1, switch to the Active Directory Rights Management Services console.
2. Click the **Exclusion Policies** node, and then click **Manage application exclusion list**.
3. In the Actions pane, click **Enable Application Exclusion**.
4. In the Actions pane, click **Exclude Application**.
5. In the **Exclude Application** dialog box, enter the following information, and then click **Finish**:
 - Application File name: **Powerpnt.exe**
 - Minimum version: **14.0.0.0**
 - Maximum version: **16.0.0.0**

Demonstration: Installing the AD FS Server Role

- In this demonstration, you will see how to install and configure the AD FS server role

During the demonstration, you can create the key distribution services (KDS) root key while you wait for the AD FS installation to complete.

Remind the students that the name you use for AD FS should be different from the server name, so that you can utilize load balancing.

Preparation Steps

To complete this demonstration, the 20412D-LON-DC1 virtual machine must be running. Sign in to the server as **Adatum\Administration** with the password **Pa\$\$w0rd**.

Demonstration Steps

Install Active Directory® Federation Services (AD FS)

- On LON-DC1, in the Server Manager, click **Manage**, and then click **Add Roles and Features**.
- In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**.
- On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
- On the **Select destination server** page, click **LON-DC1.Adatum.com**, and then click **Next**.
- On the **Select server roles** page, select the **Active Directory Federation Services** check box, and then click **Next**.
- On the **Select features** page, click **Next**.
- On the **Active Directory Federation Services (AD FS)** page, click **Next**.
- On the **Confirm installation selections** page, click **Install**.
- Wait until installation is complete, and then click **Close**.

Add a Domain Name System (DNS) record for AD FS

- On LON-DC1, in the Server Manager, click **Tools**, and then click **DNS**.



2. In DNS Manager, expand **LON-DC1**, expand **Forward Lookup Zones**, and then click **Adatum.com**.
3. Right-click **Adatum.com**, and then click **New Host (A or AAAA)**.
4. In the New Host window, in the **Name** box, type **adfs**.
5. In the **IP address** box, type **172.16.0.10**, and then click **Add Host**.
6. In the DNS window, click **OK**, and then click **Done**.
7. Close DNS Manager.

Configure AD FS

1. In the Server Manager, click the **Notifications** icon, and then click **Configure the federation service on this server**.
2. In the Active Directory Federation Services Configuration Wizard, on the **Welcome** page, click **Create the first federation server in a federation server farm**, and then click **Next**.
3. On the **Connect to Active Directory Domain Services** page, click **Next** to use **Adatum\Administrator** to perform the configuration.
4. On the **Specify Service Properties** page, in the **SSL Certificate** box, select **adfs.adatum.com**.
5. In the **Federation Service Display Name** box, type **A. Datum Corporation**, and then click **Next**.
6. On the **Specify Service Account** page, click **Create a Group Managed Service Account**.
7. In the **Account Name** box, type **ADFS**, and then click **Next**.
8. On the **Specify Configuration Database** page, click **Create a database on this server using Windows Internal Database**, and then click **Next**.
9. On the **Review Options** page, click **Next**.
10. On the **Pre-requisite Checks** page, click **Configure**.
11. On the **Results** page, click **Close**.

- In this demonstration, you will see how to:
 - Configure a claims provider trust
 - Configure a certificate for a web-based app
 - Configure a WIF application for AD FS
 - Configure a relying party trust

Preparation Steps

To complete this demonstration, the 20412D-LON-DC1 and 20412D-LON-SVR1 virtual machines must be running. Sign in to both servers as **Adatum\Administrator** with the password **Pa\$\$w0rd**. You must have completed the previous demonstration before you start this demonstration.

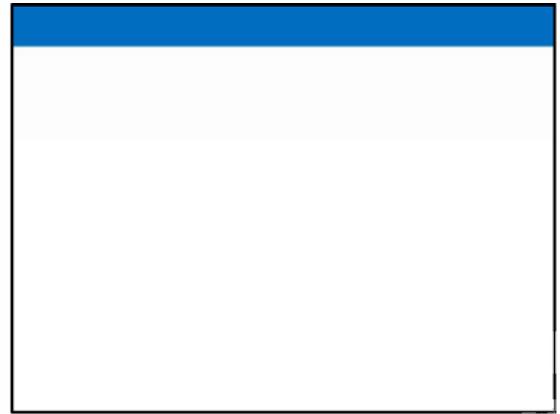
Demonstration Steps

Configure a Claims Provider Trust

1. On LON-DC1, in the Server Manager, click **Tools**, and then click **AD FS Management**.
2. In the AD FS Management console, expand **Trust Relationships**, and then click **Claims Provider Trusts**.
3. Right-click **Active Directory**, and then click **Edit Claim Rules**.
4. In the Edit Claim Rules for Active Directory window, on the **Acceptance Transform Rules** tab, click **Add Rule**.
5. In the Add Transform Claim Rule Wizard, on the **Select Rule Template** page, in the **Claim rule template** box, select **Send LDAP Attributes as Claims**, and then click **Next**.
6. On the **Configure Rule** page, in the **Claim rule name** box, type **Outbound LDAP Attributes Rule**.
7. In the **Attribute store** drop-down list, select **Active Directory**.
8. In the **Mapping of LDAP attributes to outgoing claim types** section, select the following values for the LDAP Attribute and the Outgoing Claim Type:
 - E-Mail-Addresses: **E-Mail Address**
 - User-Principal-Name: **UPN**
9. Click **Finish**, and then click **OK**.

Configure a certificate for a web-based app

1. On LON-SVR1, in Server Manager, click **Tools**, and then click **Internet Information Services (IIS)**

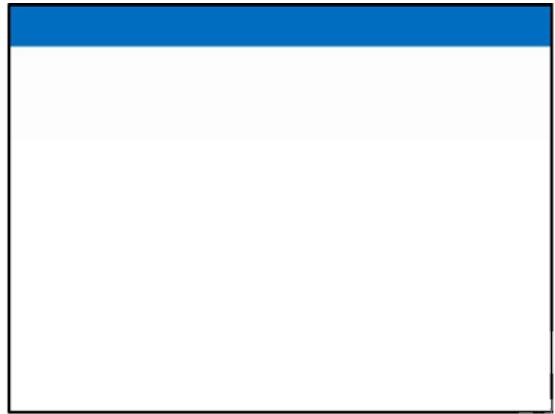


1. **Manager.**
2. If necessary, in the prompt for connecting to Microsoft Web Platform components, select the **Do not show this message** check box, and then click **No**.
3. In IIS Manager, click **LON-SVR1 (ADATUM\Administrator)**, double-click **Server Certificates**.
4. In the Actions pane, click **Create Domain Certificate**.
5. In the Create Certificate window on the Distinguished Name Properties page, enter the following and then click **Next**.
 - Common name: **lon-svr1.adatum.com**
 - Organization: **A. Datum**
 - Organizational unit: **IT**
 - City/locality: **London**
 - State/Province: **England**
 - Country/region: **GB**
6. On the Online Certification Authority page, and then click **Select**.
7. In the Select Certification Authority window, click **AdatumCA**, and then click **OK**.
8. On the **Online Certification Authority** page, in the **Friendly name** box, type **AdatumTestApp Certificate**, and then click **Finish**.
9. In IIS Manager, expand **LON-SVR1 (ADATUM\Administrator)**, expand **Sites**, click **Default Web Site**, and then in the Actions Pane, click **Bindings**.
10. In the Site Bindings window, click **Add**.
11. In the Add Site Binding window, in the **Type** box, select **https**.
12. In the **SSL certificate** box, select **AdatumTestApp Certificate**, and then click **OK**.
13. In the Site Bindings window, click **Close**.

14. Close Internet Information Services (IIS) Manager.

Configure a Windows Identity Foundation (WIF) application for AD FS

1. On LON-SVR1, in the Server Manager, click **Tools**, and then click **Windows Identity Foundation Federation Utility**.
2. On the **Welcome to the Federation Utility Wizard** page, in the **Application configuration location** box, type **C:\inetpub\wwwroot\AdatumTestApp\web.config** for the location of the sample web.config file.
3. In the **Application URI** box, type **https://lon-svr1.adatum.com/AdatumTestApp/** to indicate the path to the sample application that will trust the incoming claims from the federation server, and then click **Next** to continue.
4. On the **Security Token Service** page, click **Use an existing STS**, and in the **STS WS-Federation metadata document location** box, type **https://adfs.adatum.com/federationmetadata/2007-06/federationmetadata.xml**, and then click **Next** to continue.
5. On the **STS signing certificate chain validation error** page, click **Disable certificate chain validation**, and then click **Next**.
6. On the **Security token encryption** page, click **No encryption**, and then click **Next**.
7. On the **Offered claims** page, review the claims that will be offered by the federation server, and then click **Next**.
8. On the **Summary** page, review the changes that will be made to the sample application by the Federation Utility Wizard, scroll through the items to understand what each item is doing, and then click **Finish**.
9. In the Success window, click **OK**.



Configure a Relying Party Trust

1. On LON-DC1, in the AD FS console, click **Relying Party Trusts**.
2. In the Actions pane, click **Add Relying Party Trust**.
3. In the Relying Party Trust Wizard, on the **Welcome** page, click **Start**.
4. On the **Select Data Source** page, click **Import data about the relying party published online or on a local network**.
5. In the **Federation Metadata address (host name or URL)** box, type **https://lon-svr1.adatum.com/adatumtestapp/**, and then click **Next**. This downloads the metadata configured in the previous section.
6. On the **Specify Display Name** page, in the **Display name** box, type **A. Datum Test App**, and then click **Next**.
7. On the **Configure Multi-factor Authentication Now** page, click **I do not want to configure multi-factor authentication settings for this relying party trust at this time**, and then click **Next**.
8. On the **Choose Issuance Authorization Rules** page, click **Permit all users to access this relying party**, and then click **Next**.
9. On the **Ready to Add Trust** page, review the relying-party trust settings, and then click **Next**.
10. On the **Finish** page, click **Close**.
11. Leave the Edit Claim Rules for A. Datum Test App window open for the next demonstration.

Demonstration: Configuring Claim Rules

- In this demonstration, you will see how to configure claim rules

Preparation Steps

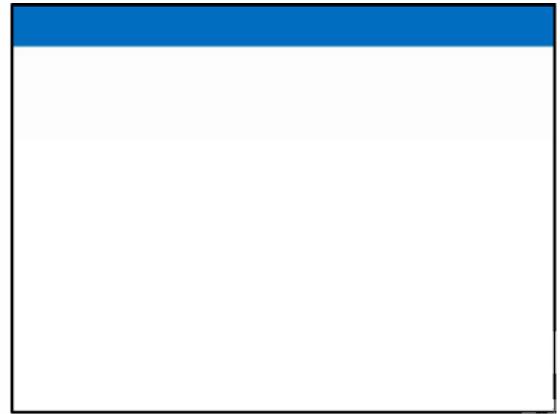
To complete this demonstration, the 20412D-LON-DC1 and 20412D-LON-SVR1 virtual machines must be running. Sign in to both servers as **Adatum\Administrator** with the password **Pa\$\$w0rd**. You must have completed the previous demonstrations before you start this demonstration.

Demonstration Steps

- On LON-DC1, in the AD FS Manager, in the Edit Claim Rules for A. Datum Test App window, on the **Issuance Transform Rules** tab, click **Add Rule**.
- In the **Claim rule template** box, select **Pass Through or Filter an Incoming Claim**, and then click **Next**.
- In the **Claim rule name** box, type **Send Group Name Rule**.
- In the **Incoming claim type** drop-down list, click **Group**, and then click **Finish**.
- In the Edit Claim Rules for A. Datum Test App window, on the **Issuance Authorization Rules** tab, click the rule named **Permit Access to All Users**, and then click **Remove Rule**.
- Click **Yes** to confirm.

Note: If you do not configure rules, users are not permitted access.

- On the **Issuance Authorization Rules** tab, click **Add Rule**.
- On the **Select Rule Template** page, in the **Claim rule template** box, select **Permit or Deny Users Based on an Incoming Claim**, and then click **Next**.
- On the **Configure Rule** page, in the **Claim rule name** box, type **Permit Production Group Rule**.
- In the **Incoming claim type** drop-down list, select **Group**.
- In the **Incoming claim value** box, type **Production**, click **Permit access to users with this incoming claim**, and then click **Finish**.
- On the **Issuance Authorization Rules** tab, click **Add Rule**.



13. On the **Select Rule Template** page, in the **Claim rule template** box, select **Permit or Deny Users Based on an Incoming Claim**, and then click **Next**.
14. On the **Configure Rule** page, in the **Claim rule name** box, type **Allow A. Datum Users**.
15. In the **Incoming claim type** drop-down list, select **UPN**.
16. In the **Incoming claim value** box, type **@adatum.com**, click **Permit access to users with this incoming claim**, and then click **Finish**.
17. Click the **Allow A. Datum Users** rule, and then click **Edit Rule**.
18. In the **Edit Rule – Allow Adatum Users** dialog box, click **View Rule Language**.
19. Click **OK**, and then click **Cancel**.
20. In the Edit Claim Rules for A. Datum Test App window, click **OK**.

- In this demonstration, you will see how to:
 - Install Web Application Proxy
 - Export the certificate from the AD FS server
 - Import the certificate to the Web Application Proxy server
 - Configure Web Application Proxy

The application created in Web Application Proxy is not a valid application that you can test. This is by design, to save time in the demonstration. To test the application that is running on LON-SVR1, you must export the certificate from LON-SVR1 and import it to LON-SVR2. In the lab, the students perform this process, and then verify that the application works through the Web Application Proxy.

Preparation Steps

To complete this demonstration, the 20412D-LON-DC1 and 20412D-LON-SVR2 virtual machines must be running. Sign in to both servers as **Adatum\Administrator** with the password **Pa\$\$w0rd**. You must have completed the previous demonstrations before you start this demonstration.

Demonstration Steps

Install the Web Application Proxy

1. On LON-SVR2, in the Server Manager, click **Manage**, and then click **Add Roles and Features**.
2. In the Add Roles and Features Wizard, on the **Before you begin** page, click **Next**.
3. On the **Select installation type** page, click **Role-based or feature-based installation**, and then click **Next**.
4. On the **Select destination server** page, click **LON-SVR2.Adatum.com**, and then click **Next**.
5. On the **Select server roles** page, expand **Remote Access (1 of 3 installed)**, select the **Web Application Proxy** check box, and then click **Next**.
6. On the **Select features** page, click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. On the **Installation progress** page, click **Close**.

Export the adfs.adatum.com certificate from LON-DC1

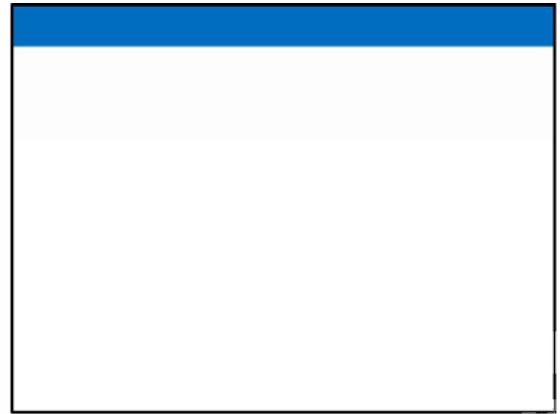
1. On LON-DC1, on the Start screen, type **mmc**, and then press Enter.



2. In the Microsoft Management Console, click **File**, and then click **Add/Remove Snap-in**.
3. In the Add or Remove Snap-ins window, in the **Available snap-ins** column, double-click **Certificates**.
4. In the Certificates snap-in window, click **Computer account**, and then click **Next**.
5. In the Select Computer window, click **Local Computer (the computer this console is running on)**, and then click **Finish**.
6. In the Add or Remove Snap-ins window, click **OK**.
7. In the Microsoft Management Console, expand **Certificates (Local Computer)**, expand **Personal**, and then click **Certificates**.
8. Right-click **adfs.adatum.com**, point to **All Tasks**, and then click **Export**.
9. In the Certificate Export Wizard, click **Next**.
10. On the **Export Private Key** page, click **Yes, export the private key**, and then click **Next**.
11. On the **Export File Format** page, click **Next**.
12. On the **Security** page, select the **Password** check box.
13. In the **Password** and **Confirm password** boxes, type **Pa\$\$w0rd**, and then click **Next**.
14. On the **File to Export** page, in the **File name** box, type **C:\adfs.pfx**, and then click **Next**.
15. On the **Completing the Certificate Export Wizard** page, click **Finish**, and then click **OK** to close the success message.
16. Close the Microsoft Management Console and do not save the changes.

Import the adfs.adatum.com certificate on LON-SVR2

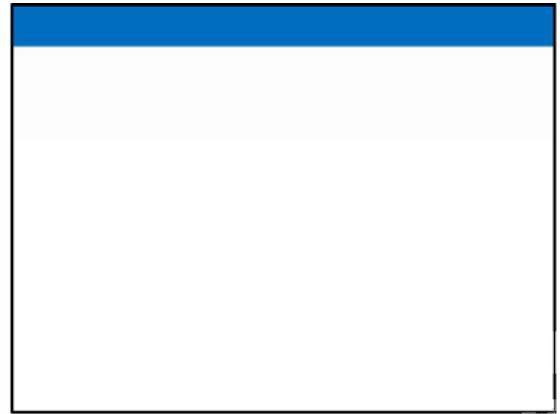
1. On LON-SVR2, on the Start screen, type **mmc**, and then press Enter.
2. In the Microsoft Management Console, click **File**, and then click **Add/Remove Snap-in**.



3. In the Add or Remove Snap-ins window, in the **Available snap-ins** column, double-click **Certificates**.
4. In the Certificates snap-in window, click **Computer account**, and then click **Next**.
5. In the Select Computer window, click **Local Computer (the computer this console is running on)**, and then click **Finish**.
6. In the Add or remove Snap-ins window, click **OK**.
7. In the Microsoft Management Console, expand **Certificates (Local Computer)**, and then click **Personal**.
8. Right-click **Personal**, point to **All Tasks**, and then click **Import**.
9. In the Certificate Import Wizard, click **Next**.
10. On the **File to Import** page, in the **File name** box, type **\LON-DC1\c\$\adfs.pfx**, and then click **Next**.
11. On the **Private key protection** page, in the **Password** box, type **Pa\$\$w0rd**.
12. Select the **Mark this key as exportable** check box, and then click **Next**.
13. On the **Certificate Store** page, click **Place all certificates in the following store**.
14. In the **Certificate store** box, select **Personal**, and then click **Next**.
15. On the **Completing the Certificate Import Wizard** page, click **Finish**.
16. Click **OK** to clear the success message.
17. Close the Microsoft Management Console and do not save the changes.

Configure the Web Application Proxy

1. On LON-SVR2, in the Server Manager, click the **Notifications** icon, and then click **Open the Web Application Proxy Wizard**.
2. In the Web Application Proxy Wizard, on the **Welcome** page, click **Next**.



3. On the **Federation Server** page, enter the following information, and then click **Next**:
 - Federation service name: **adfs.adatum.com**
 - User name: **Adatum\Administrator**
 - Password: **Pa\$\$w0rd**
4. On the **AD FS Proxy Certificate** page, in the **Select a certificate to be used by the AD FS proxy** box, select **adfs.adatum.com**, and then click **Next**.
5. On the **Confirmation** page, click **Configure**.
6. On the **Results** page, click **Close**.
7. Leave the Remote Access Management Console open for the next task.

Configure an Application

1. On LON-SVR2, in the remote Access Management Console, click **Web Application Proxy**, and then click **Publish**.
2. In the Publish New Application Wizard, on the **Welcome** page, click **Next**.
3. On the **Preattentation** page, click **Pass-through**, and then click **Next**.
4. On the Publishing Settings page, in the **Name** box, type **External App**.
5. In the **External URL** and **Backend server URL** boxes, type **https://adfs.adatum.com/externalapp/**.
6. In the **External certificate** box, select **adfs.adatum.com**, and then click **Next**.
7. On the **Confirmation** page, click **Publish**.
8. On the **Results** page, click **Close**.

Demonstration: Deploying NLB

In this demonstration, you will see how to create a Windows Server 2012 R2 NLB cluster

Preparation Steps

For this demonstration, you will need the 20412D-LON-DC1, 20412D-LON-SVR1, and 20412D-LON-SVR2 virtual machines. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Create a Windows Server 2012 R2 NLB cluster

1. Sign in to LON-SVR1 as **Adatum\Administrator** with the password **Pa\$\$w0rd**, and on the taskbar, click the **Server Manager** icon.
2. In the Server Manager console, click the **Tools** menu, and then click **Windows PowerShell ISE**.
3. In the Windows PowerShell® ISE window, enter the following command, and then press Enter:

Invoke-Command -Computername LON-SVR1,LON-SVR2 -command {Install-WindowsFeature NLB,RSAT-NLB}

4. Enter the following command, and then press Enter:

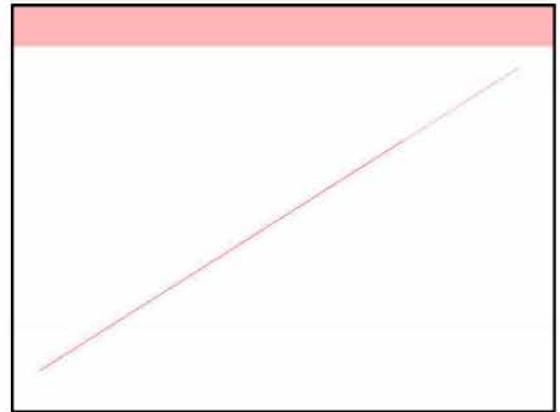
New-NlbCluster -InterfaceName "Ethernet" -OperationMode Multicast -ClusterPrimaryIP 172.16.0.42 -ClusterName LON-NLB

5. Enter the following command, and then press Enter:

Add-NlbClusterNode -InterfaceName "Ethernet" -NewNodeName "LON-SVR2" -NewNodeInterface "Ethernet"

6. In the Server Manager console, click the **Tools** menu, and then click **Network Load Balancing Manager**.
7. Verify that nodes LON-SVR1 and LON-SVR2 display with the status of **Converged** for the LON-NLB cluster.
8. Right-click the **LON-NLB** cluster, and then click **Cluster properties**.
9. In the **LON-NLB(172.16.0.42)** dialog box, on the **Cluster Parameters** tab, verify that the cluster is

9: Implementing Network Load Balancing



set to use the Multicast operations mode.

10. On the **Port Rules** tab, verify that there is a single port rule named **All** that starts at port **0** and ends at port **65535** for both Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), and uses Single affinity.
11. Click **OK** to close the dialog box.

9: Implementing Network Load Balancing

Demonstration: Configuring NLB Affinity and Port Rules

In this demonstration, you will see how to:

- Configure affinity for NLB cluster nodes
- Configure NLB port rules

After you complete the demonstration, revert virtual machines 20412D-LON-DC1, 20412D-LON-SVR1, and 20412D-LON-SVR2.

Preparation Steps

For this demonstration, you will need the 20412D-LON-DC1, 20412D-LON-SVR1, and 20412D-LON-SVR2 virtual machines. Sign in as **Adatum\Administrator** with the password **Pa\$\$w0rd**.

Demonstration Steps

Configure affinity for NLB cluster nodes

1. On LON-SVR2, on the taskbar, click the Windows PowerShell icon.
2. At the Windows PowerShell prompt, type the following commands, and press Enter after each command:

Cmd.exe

Mkdir c:\porttest

Xcopy /s c:\inetpub\wwwroot c:\porttest

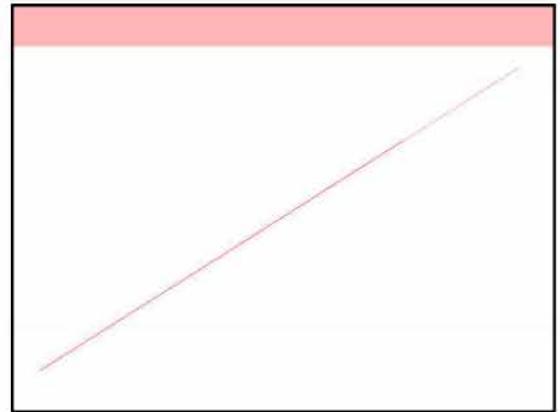
Exit

New-Website -Name PortTest -PhysicalPath "C:\porttest" -Port 5678

New-NetFirewallRule -DisplayName PortTest -Protocol TCP -LocalPort 5678

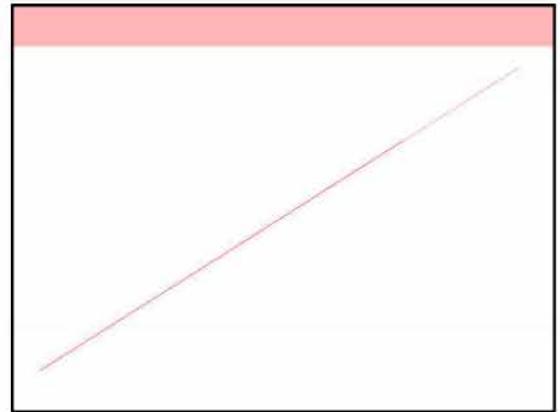
Configure NLB port rules

1. On LON-SVR1, in Server Manager, click **Tools**, and then click **Network Load Balancing Manager**.
2. In the Network Load Balancing Manager console, right-click **LON-NLB**, and then click **Cluster Properties**.
3. In the **LON-NLB(172.16.0.42)**, on the **Port Rules** tab, select the **All** port rule, click **Remove**, and then click **OK** to close the **LON-NLB(172.16.0.42)**.



4. In the Network Load Balancing Manager console, right-click **LON-NLB**, and then click **Cluster Properties**.
5. In the **LON-NLB(172.16.0.42)**, on the **Port Rules** tab, click **Add**.
6. In the **Add/Edit Port Rule** dialog box, enter the following information, and then click **OK**:
 - Port range: **80 to 80**
 - Protocols: **Both**
 - Filtering mode: **Multiple Host**
 - Affinity: **None**
7. Click **OK** to close the **LON-NLB(172.16.0.42)**.
8. In the Network Load Balancing Manager console, right-click **LON-NLB**, and then click **Cluster Properties**.
9. On the **Port Rules** tab, click **Add**.
10. In the **Add/Edit Port Rule** dialog box, enter the following information, and then click **OK**:
 - Port range: **5678 to 5678**
 - Protocols: **Both**
 - Filtering mode: **Single Host**
11. Click **OK** to close the **LON-NLB(172.16.0.42)**.
12. In the Network Load Balancing Manager console, right-click **LON-SVR1**, and then click **Host Properties**.
13. On the **Port Rules** tab, click the port rule that has **5678** as the Start and End value, and then click **Edit**.
14. Click the **Handling priority** value, and change it to **10**.

9: Implementing Network Load
Balancing



15. Click **OK** twice to close the **Add/Edit Port Rule** dialog box and the **Host Properties** dialog box.

10: Implementing Failover Clustering

Demonstration: Validating and Configuring a Failover Cluster

In this demonstration, you will see how to validate and configure a cluster

Preparation Steps

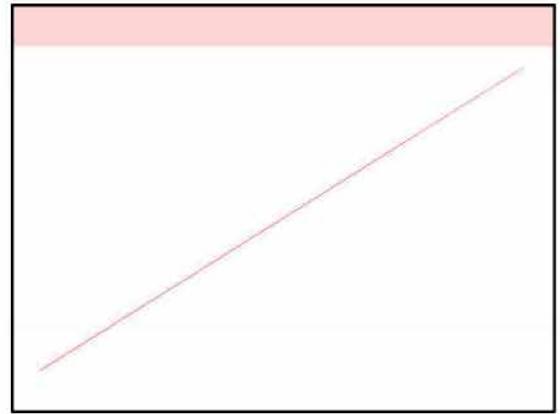
For this demonstration, start the 20412D-LON-DC1, 20412D-LON-SVR1, 20412D-LON-SVR3, and 20412D-LON-SVR4 virtual machines. Sign in to all virtual machines as **Adatum\Administrator**, with the password **Pa\$\$w0rd**.

Complete the Lab Exercise 1: Task 1 and Task 2 before performing this demonstration.

Demonstration Steps

1. On LON-SVR3, in Server Manager, click **Tools**, and then click **Failover Cluster Manager**.
2. In the Failover Cluster Manager, in the console tree, ensure that **Failover Cluster Manager** is selected, and then, under Management, click **Validate Configuration**, and then click **Next**.
3. In the **Enter name** field, type **LON-SVR3**, and then click **Add**.
4. In the **Enter name** field, type **LON-SVR4**, click **Add**, and then click **Next**.
5. Verify that **Run all tests (recommended)** is selected, and then click **Next**.
6. In the Confirmation window, click **Next**.
7. Wait for the validation tests to finish, and then in the Summary window, click **View Report**.
8. Close the report window, remove the check mark next to **Create the cluster now using the validated nodes**, and then click **Finish**.
9. On LON-SVR3, in the Failover Cluster Manager, in the **Management** section of the center pane, select **Create Cluster**.
10. Read the **Before You Begin** information page.
11. Click **Next**, type **LON-SVR3**, and then click **Add**. Type **LON-SVR4**, and then click **Add**.
12. Verify the entries, and then click **Next**.
13. In the **Access Point for Administering the Cluster** section, enter **Cluster1** as the **Cluster Name**.

10: Implementing Failover Clustering



14. Under Address, type **172.16.0.125** as the **IP address**, and then click **Next**.
15. On the **Confirmation** page, verify the information, and then click **Next**.
16. On the **Summary** page, click **Finish** to return to the Failover Cluster Manager.

10: Implementing Failover Clustering

Demonstration: Clustering a File Server Role

In this demonstration, you will see how to cluster a file server role

Preparation Steps

You should have completed the previous demonstration, Validating and Configuring a Failover Cluster, to continue with this demonstration.

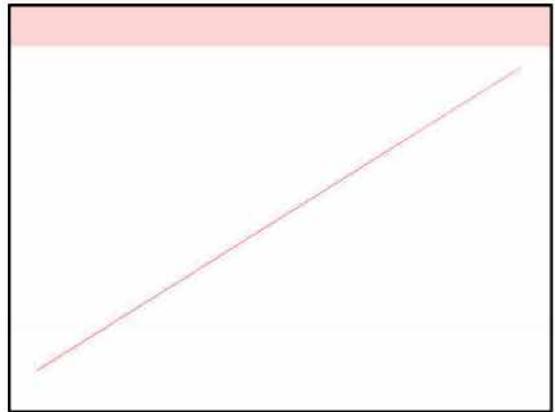
You also need to install the File Server Role service on LON-SVR4. The File Server Role service is already installed on LON-SVR3. To install the service, perform the following steps :

1. On LON-SVR4, in the Server Manager, click **Dashboard**, and then click **Add roles and features**.
2. On the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, click **Next**.
5. On the **Select server roles** page, expand **File and Storage Services (Installed)**, expand **File and iSCSI services**, and select **File Server**.
6. Click **Next** two times.
7. On the **Confirmation** page, click **Install**.
8. When the **installation succeeded** message appears, click **Close**.

Demonstration Steps

1. On LON-SVR3, open the Failover Cluster Manager, and then expand **Cluster1.adatum.com**.
2. Expand **Storage**, and then click **Disks**. Verify that three cluster disks are available.
3. Right-click **Roles**, and then select **Configure Role**.
4. On the **Before You Begin** page, click **Next**.
5. On the **Select Role** page, select **File Server**, and then click **Next**.
6. On the **File Server Type** page, click **File Server for general use**, and then click **Next**.
7. On the **Client Access Point** page, in the **Name** box, type **AdatumFS**, in the **Address** box, type

10: Implementing Failover Clustering



172.16.0.130, and then click **Next**.

8. On the **Select Storage** page, click **Cluster Disk 2**, and then click **Next**.
9. On the **Confirmation** page, click **Next**.
10. On the **Summary** page, click **Finish**.

10: Implementing Failover Clustering

Demonstration: Configuring CAU

In this demonstration, you will see how to configure CAU

Preparation Steps

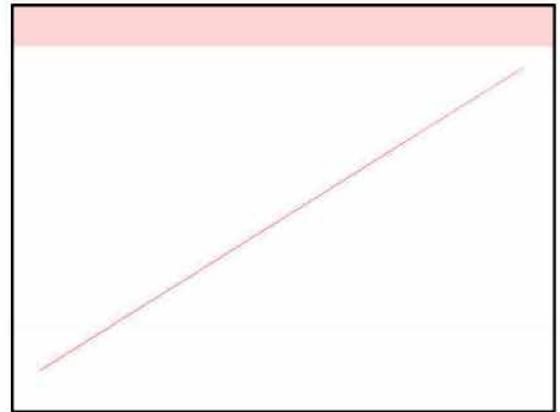
You must have completed all previous demonstrations before you start this demonstration. After you finish this demo, revert all virtual machines to their initial snapshots.

1. On LON-DC1, in Server Manager, click **Add roles and features**.
2. In the Add Roles and Features Wizard, on the **Before You Begin** page, click **Next**.
3. On the **Select installation type** page, click **Next**.
4. On the **Select destination server** page, make sure that **Select server from the server pool** is selected, and then click **Next**.
5. On the **Select server roles** page, click **Next**.
6. On the **Select features** page, in the list of features, click **Failover Clustering**. In the **Add features that are required for Failover Clustering?** dialog box, click **Add Features**. Click **Next**.
7. On the **Confirm installation selections** page, click **Install**.
8. When installation is complete, click **Close**.
9. On LON-DC1, in the Server Manager dashboard, click **Tools**, and then click **Cluster-Aware Updating**.
10. In the Cluster-Aware Updating window, in the **Connect to a failover cluster** drop-down list box, select **CLUSTER1**, and then click **Connect**.
11. In the Cluster Actions pane, click **Preview updates for this cluster**.
12. In the Cluster1-Preview Updates window, click **Generate Update Preview List**.

Note: You must have an Internet connection for this step.

13. After several minutes, updates will be shown in the list. Review updates, and then click **Close**.
14. In the Cluster Actions pane, click **Create or modify Updating Run Profile**.

10: Implementing Failover Clustering



15. Review and explain the available options. Do not make any changes, and then click **Close** when you are finished.
16. Click **Apply updates to this cluster**.
17. On the **Getting Started** page, click **Next**.
18. On the **Advanced options** page, review options for updating clustered nodes, and then click **Next**.
19. On the **Additional Update Options** page, click **Next**.
20. On the **Confirmation** page, click **Update**, and then click **Close**.
21. In the Cluster nodes pane, you can review the updating progress.

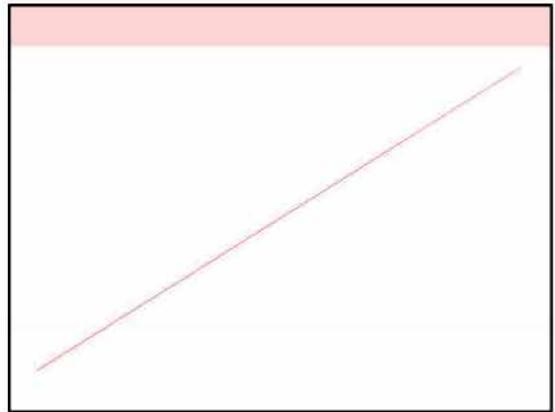
Note: You should emphasize that one node of the cluster is in Waiting state, while the other node is restarting after it is updated.

22. Wait until the process is finished.

Note: This may require a restart of both nodes.

23. Sign in to LON-SVR3 with the username **Adatum\Administrator** and the password **Pa\$\$w0rd**.
24. On LON-SVR3, in the Server Manager dashboard, click **Tools**, and then click **Cluster-Aware Updating**.
25. In the Cluster-Aware Updating window, in the **Connect to a failover cluster** drop-down list box, select **CLUSTER1**. Click **Connect**.
26. Click **Configure cluster self-updating options**.
27. On the **Getting Started** page, click **Next**.
28. On the **Add CAU Clustered Role with Self-Updating Enabled** page, click **Add the CAU clustered role, with self-updating mode enabled, to this cluster**, and then click **Next**.
29. In the **Specify self-updating schedule** area, click **Weekly**, select **4:00 AM** for **Time of day**, and

10: Implementing Failover Clustering



then select **Sunday** for **Day of the week**. Click **Next**.

30. On the **Advanced Options** page, click **Next**.
31. On the **Additional Update Options** page, click **Next**.
32. On the **Confirmation** page, click **Apply**.
33. After the clustered role is added successfully, click **Close**.

11: Implementing Failover Clustering with Hyper-V

Demonstration: Implementing Virtual Machines on Clusters (optional)

In this demonstration, you will see how to implement highly available virtual machines with failover clustering

After you complete this lab, you should destroy the cluster that you have created. This is necessary if you want to perform the Hyper-V Replica demonstration. To do this, open the Failover Cluster Manager console on LON-HOST1, expand VMCluster and then click on Roles. In the middle pane, right-click the LON-CORE virtual machine, select Remove, and then click Yes. Next, right-click VMCluster, select More Actions, select Destroy Cluster, and then click Yes.

Leave both LON-DC1 and LON-SVR1 running, and keep the hosts running for the Hyper-V Replica demonstration.

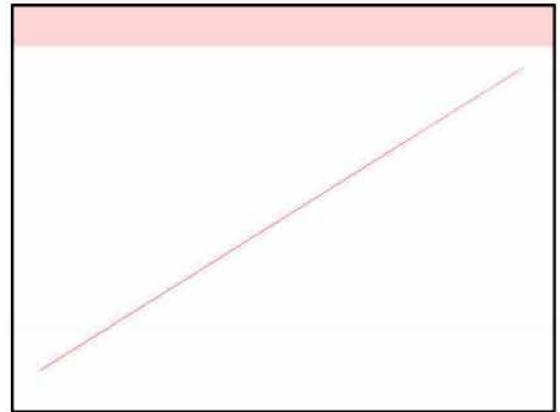
Preparation Steps

To perform this demonstration, you must have two physical hosts available, LON-HOST1 and LON-HOST2. If you do not have two hosts, you should skip this demonstration. To prepare for the demonstration, you have to perform all steps from the Lab, Exercise 2, and Tasks 1, 2, and 3. Before you start the preparation steps, you should start and sign in as **Adatum\Administrator**, with the password **Pa\$\$w0rd** to LON-DC1-B on LON-HOST1 and to LON-SVR1-B on LON-HOST2.

Demonstration Steps

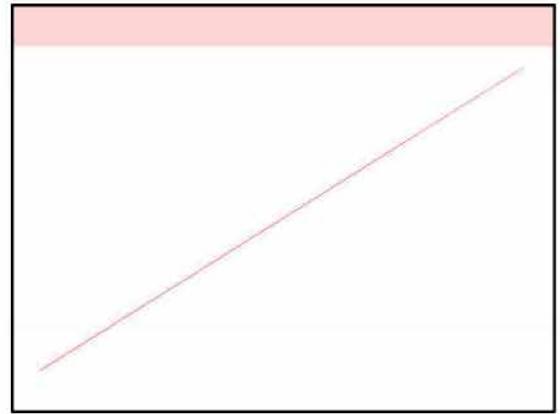
1. Ensure that LON-HOST1 is the owner of the ClusterVMs disk in Failover Cluster Manager. You can verify this by reading the value in the Owner column. If it is not, then move the ClusterVMs resource to LON-HOST1 before you do this procedure.
2. On LON-HOST1, open File Explorer, browse to **E:\Program Files\Microsoft Learning\20412\Drives\20412D-LON-CORE\Virtual Hard Disks**, and then copy the **20412D-LON-CORE.vhd** virtual hard disk file to the **C:\ClusterStorage\Volume1** location. (Note: The drive letter might be different based upon the number of drives on the physical host machine)
3. In the Failover Cluster Manager console, click **Roles**, and then in the Actions pane, click **Virtual Machines**.
4. Click **New Virtual Machine**.
5. Select **LON-HOST1** as the cluster node, and click **OK**.

11: Implementing Failover Clustering with Hyper-V



6. In the New Virtual Machine Wizard, click **Next**.
7. On the **Specify Name and Location** page, type **TestClusterVM** for the Name, click **Store the virtual machine in a different location**, and then click **Browse**.
8. Browse to and select **C:\ClusterStorage\Volume1**, click **Select Folder**, and then click **Next**.
9. On the **Specify Generation** page, select **Next**.
10. On the **Assign Memory** page, type **1536**, and then click **Next**.
11. On the **Configure Networking** page, click **External Network**, and then click **Next**.
12. On the **Connect Virtual Hard Disk** page, click **Use an existing virtual hard disk**, and then click **Browse**.
13. Locate **C:\ClusterStorage\Volume1**, select **20412D-LON-CORE.vhd**, and then click **Open**.
14. Click **Next**, and click **Finish**.
15. On the **Summary** page of the High Availability Wizard, click **Finish**.
16. Right-click the **TestClusterVM**, and click **Settings**.
17. In the **Settings for TestClusterVM** on LON-Host1, expand **Processor** in the left navigation pane, and then click **Compatibility**.
18. In the right pane, select the check box before the **Migrate to a physical computer with a different processor version** option.
19. Click **OK**.
20. Right-click **TestClusterVM**, and click **Start**.
21. Ensure that the machine starts successfully.
22. Open **Failover Cluster Manager** on LON-HOST2.
23. Expand **VMCluster.Adatum.com**, and click **Roles**.
24. Right-click **TestClusterVM**, select **Move**, select **Live Migration**, and then click **Select Node**.
25. Click **LON-HOST2**, and click **OK**.

11: Implementing Failover Clustering with Hyper-V



26. Right-click **TestClusterVM**, and click **Connect**.
27. Ensure that you can access and operate the virtual machine while it is migrating to another host.
28. Wait until the migration is finished.

11: Implementing Failover Clustering with Hyper-V

Demonstration: Implementing Hyper-V Replica (optional)

In this demonstration, you will see how to implement Hyper-V Replica

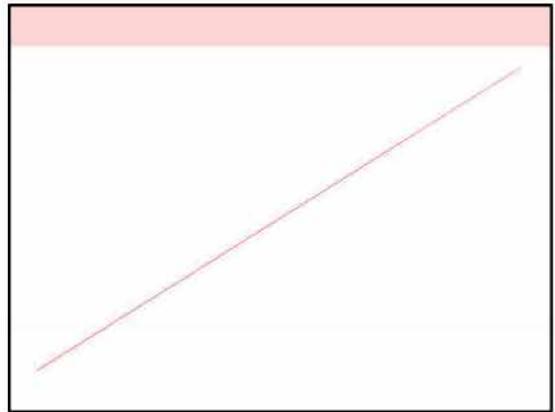
Preparation Steps

To perform this demonstration, you must have two physical hosts available, LON-HOST1 and LON-HOST2. If you do not have two hosts, you should skip this demonstration. To prepare for this demonstration, perform all of the steps specified in the Lab, Exercise 1, Task 1.

Demonstration Steps

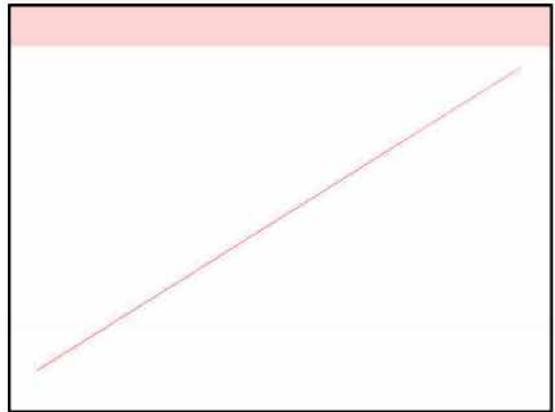
1. On LON-HOST2, open the Hyper-V Manager console.
2. In Hyper-V Manager, right-click **LON-HOST2**, and then select **Hyper-V Settings**.
3. In Hyper-V Settings for LON-HOST2, click **Replication Configuration**.
4. In the Replication Configuration pane, click **Enable this computer as a Replica server**.
5. In the Authentication and ports section, select **Use Kerberos (HTTP)**.
6. In the Authorization and storage section, click **Allow replication from any authenticated server**, and then click **Browse**.
7. Click **Computer**, double-click **Local Disk (E)**, and then click **New folder**. Type **VMReplica** for folder name, and press Enter. Select the **E:\VMReplica** folder, and click **Select Folder**.
8. In the Hyper-V Settings for LON-HOST2, click **OK**.
9. In the Settings window, read the notice, and then click **OK**.
10. Click the **Start** screen, and click the **Control Panel**.
11. In the Control Panel, click **System and Security**, and then click **Windows Firewall**. Click **Advanced settings**, and then click **Inbound Rules**.
12. In the right pane, in the rule list, find and right-click the **Hyper-V Replica HTTP Listener (TCP-In)** rule, and then click **Enable Rule**.
13. Close the Windows Firewall with Advanced Security console, and close **Windows Firewall**.
14. Repeat Steps 1 through 13 on LON-HOST1.

11: Implementing Failover Clustering with Hyper-V



15. On LON-HOST1, open Hyper-V Manager. Click **LON-HOST1**, and right-click **20412D-LON-CORE**.
16. Click **Enable Replication**.
17. On the **Before You Begin** page, click **Next**.
18. On the **Specify Replica Server** page, click **Browse**.
19. In the Select Computer window, type **LON-HOST2**, and click **Check Names**, and click **OK**. Then click **Next**.
20. On the **Specify Connection Parameters** page, review the settings, and ensure that **Use Kerberos authentication (HTTP)** is selected, and then click **Next**.
21. On the **Choose Replication VHDs** page, ensure that **20412D-LON-CORE.vhd** is selected, and then click **Next**.
22. On the **Configure Replication Frequency** page, select 30 seconds from the drop-down list box, and click **Next**.
23. On the **Configure Additional Recovery Points** page, select **Maintain only the latest recovery point**, and then click **Next**.
24. On the **Choose Initial Replication Method** page, click **Send initial copy over the network**, select **Start replication immediately**, and then click **Next**.
25. On the **Completing the Enable Replication Wizard** page, click **Finish**.
26. Wait five to 10 minutes. You can monitor the progress of initial replication in the Status column in the Hyper-V Manager console. When it completes (progress reaches 100 percent), ensure that **20412D-LON-CORE** has appeared on LON-HOST2 in Hyper-V Manager.
27. On LON-HOST2 in Hyper-V Manager, right-click **20412D-LON-CORE**.
28. Select **Replication**, and then click **View Replication Health**.
29. Review the content of the window that appears, ensure that there are no errors, and then click

11: Implementing Failover Clustering with Hyper-V



Close.

30. On LON-HOST1, open Hyper-V Manager, and verify that **20412D-LON-CORE** is turned off.
31. Right-click **20412D-LON-CORE**, select **Replication**, and then click **Planned Failover**.
32. In the Planned Failover window, ensure that the option **Start the Replica virtual machine after failover** is selected, and then click **Fail Over**.
33. On LON-HOST2, in Hyper-V Manager, ensure that **20412D-LON-CORE** is running.
34. On LON-HOST1, right-click **20412D-LON-CORE**, point to **Replication**, and then click **Remove Replication**.
35. In the **Remove Replication** dialog box, click **Remove Replication**.
36. On LON-HOST2, right-click **20412D-LON-CORE**, and then select **Shut Down**. In the **Shut Down Machine** dialog box, click **Shut Down**.

12: Implementing Business Continuity and Disaster Recovery

Demonstration: Using Windows Server Backup to Restore a Folder

In this demonstration, you will see how to use the Recovery Wizard to restore a folder

At the end of the demonstration revert 20412D-LON-DC1 and 20412D-LON-SVR1.

Preparation Steps

You must have the 20412D-LON-DC1 and 20412D-LON-SVR1 virtual machines to complete this demonstration. Sign in on the virtual machines with the username **Adatum\Administrator** and the password **Pa\$\$word**. You must also have completed all previous demonstrations. If you are short on time, you can choose to skip this demonstration.

Demonstration Steps

On LON-SVR1, open Windows Explorer, browse to drive C, and then delete the **HR Data** folder.

2. From the Server Manager, start **Windows Server Backup**, and then click **Recover**.
3. In the Recovery Wizard, on the **Getting Started** page, click **A backup stored on another location**, and then click **Next**.
4. On the **Specify Location Type** page, click **Remote shared folder**, and then click **Next**.
5. On the **Specify Remote Folder** page, type **\LON-DC1\Backup**, and then click **Next**.
6. On the **Select Backup Date** page, click **Next**.
7. On the **Select Recovery Type** page, click **Next**.
8. On the **Select Items to Recover** page, expand **LON-SVR1**, click **Local disk (C:)** drive, and in the right pane, click **HR Data**, and then click **Next**.
9. On the **Specify Recovery Options** page, under **Another Location**, type **C:**, and then click **Next**.
10. On the **Confirmation** page, click **Recover**.
11. On the **Recovery Progress** page, click **Close**.

In Windows Explorer, browse to drive C, and ensure that the **HR Data** folder is restored.