Microsoft

Configuring Advanced Windows Server 2012 Services

Training Guide

Orin Thomas

Configuring Advanced Windows Server 2012 Services

Designed to help enterprise administrators develop real-world, job-role-specific skills—this *Training Guide* focuses on advanced configuration of services necessary to deploy, manage, and maintain a Windows Server 2012 infrastructure. Build hands-on expertise through a series of lessons, exercises, and suggested practices—and help maximize your performance on the job.

This Microsoft *Training Guide*:

- Provides in-depth, hands-on training you take at your own pace
- Focuses on job-role-specific expertise for deploying and managing advanced infrastructure services in Windows Server 2012
- Creates a foundation of skills which, along with on-the-job experience, can be measured by Microsoft Certification exams such as 70-412

Sharpen your skills. Increase your expertise.

- Configure full forest and domain trust relationships
- Configure Active Directory (AD) sites and manage AD replication
- Implement advanced DNS and DHCP solutions
- Install, configure, and manage AD Certificate Services
- Manage backups and recover servers
- Optimize storage and configure advanced file services
- Manage failover clustering and Network Load Balancing
- Move virtual machines from one Hyper-V server to another
- Implement Dynamic Access Control and Active Directory RMS
- Implement Active Directory Federation Services

About You

This *Training Guide* will be most useful to IT professionals who have at least three years of experience administering previous versions of Windows Server in midsize to large environments.

About the Author

Orin Thomas is a consultant, writer, and Microsoft MVP whose books include Microsoft Press *Training Kits* for Exams 70-646, 70-647, 70-662, and 70-680. He is also a contributing editor for *Windows IT Pro* magazine.

About the Practices

For most practices, we recommend using a Hyper-V virtualized environment.

For *system requirements*, see the Introduction.

Preparing for Microsoft Certification?

Get the official exam-prep guide for Exam 70-412.

Exam Ref 70-412: Configuring Advanced Windows Server 2012 Services
ISBN 9780735673618

microsoft.com/mspress

ISBN: 978-0-7356-7425-7

90000

9 780735 674257

U.S.A. $59.99
Canada $62.99
[*Recommended*]

Windows

Microsoft Press

Celebrating 30 years!

Microsoft

Training Guide: Configuring Advanced Windows Server 2012 Services

Orin Thomas

ISBN: 978-0-7356-7425-7

1 2 3 4 5 6 7 8 9 LSI 8 7 6 5 4 3

Printed and bound in the United States of America.

Microsoft Press books are available through booksellers and distributors worldwide. If you need support related to this book, email Microsoft Press Book Support at mspinput@microsoft.com. Please tell us what you think of this book at *http://www.microsoft.com/learning/booksurvey*.

The example companies, organizations, products, domain names, email addresses, logos, people, places, and events depicted herein are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

This book expresses the author's views and opinions. The information contained in this book is provided without any express, statutory, or implied warranties. Neither the authors, Microsoft Corporation,
nor its resellers, or distributors will be held liable for any damages caused or alleged to be caused either directly or indirectly by this book.

Acquisitions and Developmental Editor: Michael Bolinger

Production Editor: Christopher Hearse

Editorial Production: Box Twelve Communications

Technical Reviewer: Randall Galloway

Cover Design: Twist Creative • Seattle

Cover Composition: Randy Comer

Illustrator: Rebecca Demarest

Contents at a glance

Contents

Chapter 9 DAC and AD RMS 621

Introduction

When Microsoft puts together exam objectives for an exam, it doesn't randomly select pages from TechNet. Instead, in conjunction with subject matter experts and representatives of the product team, it puts together a list of tasks and areas of knowledge that represents what someone in a specific job role would do and need to know on a day-to-day, a weekly, or even a monthly basis.

Each exam maps to a different job role. The objectives for the 70-412 exam are a list of tasks and areas of knowledge that describe what an advanced administrator of the Windows Server 2012 operating system with several years of on-the-job experience (managing other server operating systems as well as Windows Server 2012) does and understands. These topics include some that experienced administrators may not have encountered before or have limited experience with, such as Active Directory Rights Management Services and Active Directory Federation Services.

This book covers the majority of the topics and skills that are the subject of the Microsoft certification exam 70-412. The idea behind this book is that by reading it and by performing the extensive practice exercises at the end of each chapter in your own lab, you can learn how to perform tasks with the technologies addressed by the exam. By performing the tasks yourself in a test environment, you'll learn enough about how these technologies work that you'll be able to leverage that knowledge in your real-world role as a Windows Server 2012 administrator. Reading and performing the lab exercises in this book will assist you in preparing for the exam, but it's not a complete exam preparation solution. If you are preparing for the exam, you should use additional study materials, such as practice tests and the forthcoming *Exam Ref 70-412: Configuring Advanced Windows Server 2012 Services* to help bolster your real-world experience.

By using this training guide, you will learn how to do the following:

- Configure and manage high availability
- Configure file and storage solutions
- Implement business continuity and disaster recovery
- Configure network services
- Configure the Active Directory infrastructure
- Configure identity and access solutions

System requirements

The following are the minimum system requirements your computer needs to meet to complete the practice exercises in this book. This book is designed assuming you will be using Hyper-V—either the client version available with some editions of Windows 8 or the version available in Windows Server 2012. You can use other virtualization software instead, such as VirtualBox or VMWare Workstation, but the practice setup instructions later in this introduction assume that you are using Hyper-V.

Hardware and software requirements

This section presents the hardware requirements for Hyper-V and the software requirements.

Virtualization hardware requirements

If you choose to use virtualization software, you need only one physical computer to perform the exercises in this book, except for in Chapter 8, which requires two identical computers. The physical host computer must meet the following minimum hardware requirements:

- x64-based processor that includes both hardware-assisted virtualization (AMD-V or Intel VT) and hardware data execution protection. (On AMD systems, the data execution protection feature is called the No Execute or NX bit. On Intel systems, this feature is called the Execute Disable or XD bit.) These features must also be enabled in the BIOS. (Note: You can run Windows Virtual PC without Intel-VT or AMD-V.) If you want to use Hyper-V on Windows 8, you need a processor that supports Second Layer Address Translation (SLAT).
- 8 gigabytes (GB) of RAM (more is recommended).
- 250 GB of available hard disk space.
- Internet connectivity.

Software requirements

The following software is required to complete the practice exercises:

- Windows Server 2012 evaluation. You can download an evaluation edition of Windows Server 2012 in ISO format from the Windows Server and Cloud Platform website at *http://www.microsoft.com/server*.

Virtual machine setup instructions

This set of exercises contains abbreviated instructions for setting up the SYD-DC, MEL-DC, ADL-DC, and CBR-DC computers used in the practice exercises in all chapters of this training kit. To perform these exercises, first install Windows Server 2012 Standard edition using the default configuration, setting the administrator password to Pa$$w0rd.

EXERCISE 1 SYD-DC to function as a Windows Server 2012 domain controller

1. Log on to the first computer on which you have installed Windows Server 2012 using the Administrator account and the password Pa$$w0rd.
2. Open an elevated PowerShell prompt and issue the following command:

   ```
   cmd
   ```

3. Enter the following command:

   ```
   Netsh interface ipv4 set address “Ethernet” static 10.10.10.10
   ```

4. Enter the following command:

   ```
   netdom renamecomputer %computername% /newname:SYD-DC
   ```

5. Restart the computer and log back on using the Administrator account.
6. Open an elevated PowerShell prompt and issue the following command:

   ```
   Add-WindowsFeature AD-Domain-Services -IncludeManagementTools
   ```

7. Open the Server Manager console. Click the Refresh icon.
8. Click on the Notifications icon and then click Promote This Server to Domain Controller.
9. On the Deployment Configuration page, choose Add a New Forest. Enter **Contoso.com** as the root domain name and then click Next.
10. On the Domain Controller Options page, configure the following settings and then click Next:
   - Forest Functional Level: Windows Server 2012
   - Domain Functional Level: Windows Server 2012
   - Specify Domain Controller Capabilities:
     - Domain Name System (DNS) Server
     - Global Catalog
   - DSRM Password: Pa$$w0rd

11. On the DNS Options page, click Next.

12. On the Additional Options page, click Next.

13. Accept the default settings for the Database, Log Files, and SYSVOL locations and click Next.

14. On the Review Options page, click Next.

15. On the Prerequisites Check page, click Install.

16. The computer will restart automatically.

EXERCISE 2 Prepare Active Directory Domain Server (AD DS)

1. Log on to server SYD-DC using the Administrator account.

2. Using Active Directory Users and Computers, create a user account named don_funk in the Users container and assign the account the password Pa$$w0rd. Configure the password to never expire. Add this user account to the Enterprise Admins, Domain Admins, and Schema Admins groups.

3. Open the DNS console and create a primary IPv4 Reverse Lookup Zone for the subnet 10.10.10.x. Ensure that the zone is stored within AD DS and is replicated to all DNS servers running on domain controllers in the forest and allows only secure dynamic updates.

EXERCISE 3 Prepare ADL-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.

2. Log on to the second computer on which you have installed Windows Server 2012 using the Administrator account and the password Pa$$w0rd.

3. Open an elevated PowerShell prompt and issue the following commands:

```
cmd

Netsh interface ipv4 set address “Ethernet” static 10.10.10.20

Netsh interface ipv4 set dnsservers “Ethernet” static 10.10.10.10 primary
```

4. Enter the following command:

```
netdom renamecomputer %computername% /newname:ADL-DC
```

5. Restart the computer and then log on again using the Administrator account.

6. Shut down the computer.

EXERCISE 4 Prepare CBR-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.

2. Log on to the third computer on which you have installed Windows Server 2012 using the Administrator account and the password Pa$$w0rd.

3. Open an elevated PowerShell prompt and issue the following commands:

```
cmd

Netsh interface ipv4 set address “Ethernet” static 10.10.10.30

Netsh interface ipv4 set dnsservers “Ethernet” static 10.10.10.10 primary
```

4. Enter the following command:

```
netdom renamecomputer %computername% /newname:CBR-DC
```

5. Restart the computer and then log on again using the Administrator account.

6. Shut down the computer.

EXERCISE 5 Prepare MEL-DC

1. Ensure that computer SYD-DC is turned on and connected to the network or virtual network to which the second computer is connected.

2. Log on to the third computer on which you have installed Windows Server 2012 using the Administrator account and the password Pa$$w0rd.

3. Open an elevated PowerShell prompt and issue the following commands:

```
cmd

Netsh interface ipv4 set address “Ethernet” static 10.10.10.40

Netsh interface ipv4 set dnsservers “Ethernet” static 10.10.10.10 primary
```

4. Enter the following command:

```
netdom renamecomputer %computername% /newname:MEL-DC
```

5. Restart the computer and then log on again using the Administrator account.

6. Shut down the computer.

EXERCISE 6 Snapshot all virtual machines

1. Snapshot all virtual machines. This is the state that they need to be in prior to performing exercises.

Acknowledgments

I'd like to thank the following people for their dedication and help in getting this book written: Troy Mott, Randall Galloway, Christopher Hearse, Michael Bolinger, and Charlotte Kughen. I'd also like to thank Oksana and Rooslan for their patience with me during the writing process.

Errata & book support

We made every effort to ensure the accuracy of this book and its companion content. Any errors that have been reported since this book was published are listed at:

http://aka.ms/TGCA2012S/errata

If you find an error that is not already listed, you can report it to us through the same page.

If you need additional support, send an email to Microsoft Press Book Support at mspinput@microsoft.com.

Please note that product support for Microsoft software is not offered through the previous addresses.

We want to hear from you

At Microsoft Press, your satisfaction is our top priority, and your feedback is our most valuable asset. Please tell us what you think of this book at:

http://aka.ms/tellpress

The survey is short, and we read every one of your comments and ideas. Thanks in advance for your input!

Stay in touch

Let’s keep the conversation going! We’re on Twitter: *http://twitter.com/MicrosoftPress*.

CHAPTER 1

Advanced Active Directory infrastructure

If you are the administrator of a medium to large organization, it is likely that you are responsible for managing multiple domains, perhaps even multiple forests, rather than managing a single domain forest. In this chapter you discover how and why you would configure forests with multiple domain trees and the benefits of each functional level. You also find out how to configure and manage different types of trust relationships to ensure users in one forest or domain are granted appropriate access to resources in another forest, domain, or Kerberos realm.

Lessons in this chapter:

- Lesson 1: Configure domains and forests
- Lesson 2: Configure trusts

Before you begin

To complete the practice exercises in this chapter, you need to have deployed computers SYD-DC, MEL-DC, CBR-DC, and ADL-DC as described in the Introduction, using the evaluation edition of Windows Server 2012.

Lesson 1: Configuring domains and forests

As an experienced administrator you're probably quite familiar with the configuration of single domain Active Directory forests. In this lesson, you find out more about multidomain and multiforest environments. You discover how to upgrade an existing domain and forest so that it uses only Windows Server 2012 domain controllers, and you find out how to configure UPN suffixes.

After this lesson, you will be able to

- Understand multidomain Active Directory environments
- Understand multiforest Active Directory environments
- Upgrade existing domains and forests
- Configure multiple user principal name (UPN) suffixes

Estimated lesson time: 45 minutes

Multidomain Active Directory environments

The majority of current Active Directory deployments in small- and medium-sized enterprises have a single domain. This hasn't always been the case because earlier versions of the Windows Server operating system, such as Windows NT4, supported far fewer user accounts. Supporting a smaller number of accounts often necessitated the use of multiple domains, and it wasn't unusual to see medium-sized organizations that used complicated domain structures.

Each Windows Server 2012 domain controller can create approximately 2.15 billion objects during its lifetime, and each domain supports the creation of up to approximately 2.15 billion relative identifiers (*RIDs*). Given these statistics, few administrators implement multiple domain forests because they need to support a large number of users. Of course, in very large organizations, the replication load between sites might make a domain with several hundred thousand user accounts problematic, but site and replication considerations are covered in Chapter 2, "Active Directory sites and replication."

There are many reasons why organizations implement multidomain forests. These can include but are not limited to:

- **Historical domain structure** Even though newer versions of the Windows Server operating system handle large numbers of objects more efficiently, some organizations have retained the forest structure that was established when the organization first adopted Active Directory.
- **Organizational or political reasons** Some organizations are conglomerates, and they might be composed of separate companies that share a common administrative and management core. An example of this is a university faculty in Europe or Australia, such as a Faculty of Science, that is composed of different departments or schools,

such as the school of physics and the department of botany. For political or organizational reasons it might have been decided that each department or school should have its own domain that is a part of the overall faculty forest. Active Directory gives organizations the ability to create domain namespaces that meet their needs, even if those needs might not directly map to the most efficient way of accomplishing a goal from a strict technical perspective.

- **Security reasons** Domains enable you to create security boundaries so that you can have one set of administrators who are able to manage computers and users in their own domain, but who are not able to manage computers and users in a separate domain. Although it's possible to accomplish a similar goal by delegating privileges, many organizations prefer to use separate domains to accomplish this goal.

REAL WORLD **POLITICS TRUMPS TECHNOLOGY**

It is very important to understand that geeks often see technology as something completely separate from organizational politics, with the most efficient technical solution being the best, but everyone else doesn't necessarily share this perception. When I worked as a systems administrator at an Australian University, there was a shared room in one building that hosted two different printers used by different departments, even though the departments were part of the same faculty. People in each department felt strongly that the printer should be labeled with a departmental identity on the network and that users from one department should, under no circumstances, be able to print to the printer owned by the other department. Although the machinations of interdepartmental politics are usually of little interest to the geeks in the information technology (IT) department, administrators who ignore unclearly defined boundaries do so at their own peril.

Domain trees

A domain tree is a set of names that share a common *root domain* name. For example contoso.com can have pacific.contoso.com and atlantic.contoso.com as child domains, and these domains can have child domains themselves. A forest can have multiple *domain trees*. When you create a new tree in a forest, the root of the new tree is a *child domain* of the original root domain. In Figure 1-1, adatum.com is the root of new domain tree in the contoso.com forest.

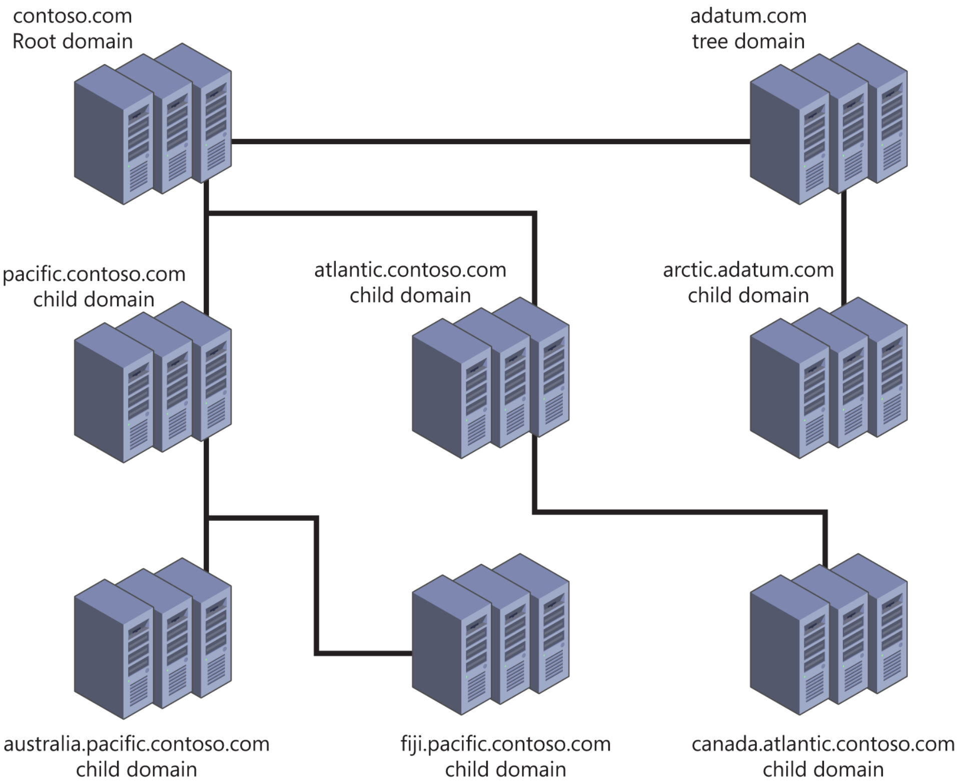


FIGURE 1-1 Contoso.com as the root domain in a two-tree forest

The depth of a domain tree is limited by a maximum fully qualified domain name (FQDN) length for a host of 64 characters. This means that the host name and the domain name combined cannot exceed 64 characters, including the periods that separate each component of the name. For example, the name 3rd-floor-printer could not be used in the melbourne.victoria.australia.pacific.contoso.com domain because it cannot be used as a hostname in an Active Directory forest as the hostname exceeds the 64-character limit.

Intra-forest authentication

All domains within the same forest automatically trust one another. This means that in the environment shown in Figure 1-1, you can assign a user in the Australia.pacific.contoso.com permissions to a resource in the arctic.adatum.com domain without performing any extra configuration.

Because of the built-in automatic *trust relationships*, a single forest implementation is not appropriate for separate organizations, even when they are in partnership with one another. A single forest makes it possible for one or more users to have administrative control. Most organizations aren't comfortable even with trusted partners having administrative control over their IT environments. When you do need to allow users from partner organizations to have access to resources, you can configure trust relationships or federation. You read more about trust relationships in Lesson 2 of this chapter and more about federation in Chapter 10, "Active Directory Federation Services."

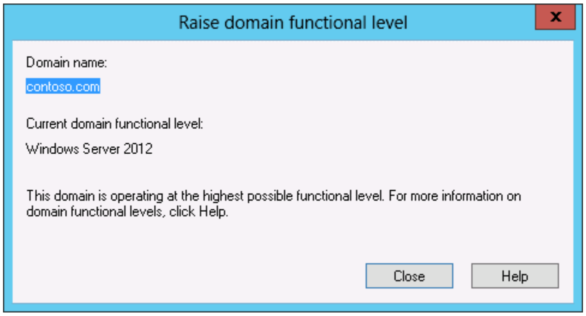
Domain functional levels

Domain functional levels determine the Active Directory functionality and features that are available. The higher the *domain functional level* is, the more functionality and features are available. You can use Windows Server 2012 domain controllers with the following domain functional levels:

- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012

The limiting factor on a domain functional level is the domain controllers used to host Active Directory. If your organization has Windows Server 2003 domain controllers, you aren't able to raise the functional level until you replace or upgrade those domain controllers to a more recent version of the Windows Server operating system.

You can alter the domain functional level using the Active Directory Users and Computers console, the Active Directory Domains and Trusts console as shown in Figure 1-2, or the Set-ADDomainMode Windows PowerShell cmdlet. Your account needs to be a member of the Domain Admins or Enterprise Admins groups to perform this operation.



Raise domain functional level

Domain name:
contoso.com

Current domain functional level:
Windows Server 2012

This domain is operating at the highest possible functional level. For more information on domain functional levels, click Help.

FIGURE 1-2 Raise or verify the domain functional level

WINDOWS SERVER 2003 FUNCTIONAL LEVEL

The Windows Server 2003 domain functional level is the lowest level at which you can introduce domain controllers running the Windows Server 2012 operating system. You can set this functional level if you have domain controllers running the Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 operating systems. The Windows Server 2003 domain functional level includes the following features, which are also available at higher domain functional levels:

- The LastLogonTimestamp attribute records a user's last domain logon.
- *Constrained Delegation* enables applications to securely delegate user credentials.
- *Selective authentication* enables you to configure specific resources in the forest so that only certain users and groups can authenticate. The default is to allow all users in the forest to authenticate before permissions to those resources are checked.
- Support for storing DNS zones in custom application partitions enables you to selectively replicate DNS zones to specific domain controllers that are enrolled in the custom partitions, rather than requiring that you configure replication to all domain controllers in the domain or the forest.
- Attribute-level replication for group and other multivalued attributes. Rather than replicating the whole Active Directory object, only altered attributes will be replicated.

WINDOWS SERVER 2008 FUNCTIONAL LEVEL

The Windows Server 2008 domain functional level requires that all domain controllers be running the Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 operating systems. The Windows Server 2008 domain functional level includes all the features available at the Windows Server 2003 functional level as well as the following:

- Improvements in Distributed File System (DFS) replication that make it possible for replication to occur more efficiently
- Support for fine-grained password policies, which enables you to apply multiple separate password policies within the same domain
- Support for Personal Virtual Desktops through RemoteApp and Remote Desktop when used with Hyper-V
- AES (Advanced Encryption Services) 128 and 256 Kerberos support

WINDOWS SERVER 2008 R2 FUNCTIONAL LEVEL

The Windows Server 2008 R2 domain functional level requires that all domain controllers are running the Windows Server 2008 R2 or Windows Server 2012 operating systems. This functional level supports the features of the Windows Server 2003 and Windows Server 2008 domain functional levels as well as:

- Managed service account support, which enables you to automatically manage service account passwords rather than manually managing them
- Support for command-line-based Active Directory Recycle Bin if the forest functional level is raised to Windows Server 2008 R2

WINDOWS SERVER 2012 FUNCTIONAL LEVEL

The Windows Server 2012 domain functional level requires that all domain controllers be running the Windows Server 2012 operating system. This functional level supports the features of all the lower functional levels as well as:

- Group managed service accounts, which enable you to install a single managed service account on multiple computers.
- Fine-Grained Password Policies through the Active Directory Administrative Center rather than by editing them using ADSI Edit.
- Active Directory Recycle Bin through Active Directory Administrative Center rather than through command-line utilities if the forest is configured at the Windows Server 2012 forest functional level.
- If the Key Distribution Center (KDC) support for claims, compound authentication, and Kerberos armoring is set to Always Provide Claims or Fail Unarmored Authentication Requests, these options aren't available unless the domain is raised to the Windows Server 2012 functional level.

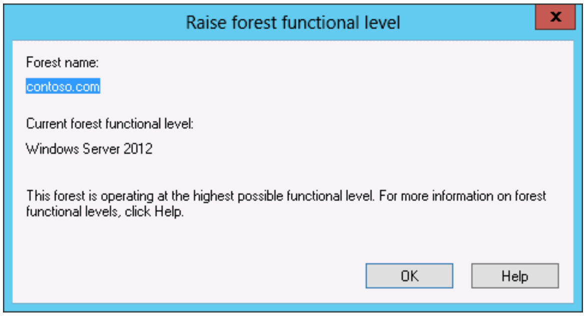
Forest functional levels

A forest can host domains running at different domain functional levels. *Forest functional level* is dependent on the minimum domain functional level of any domain in your forest. For example, if your organization has one domain running at the Windows Server 2008 functional level and all other domains running at the Windows Server 2012 functional level, you can't raise the forest functional level beyond Windows Server 2008. After you raise that one domain from the Windows Server 2008 functional level to the Windows Server 2012 domain functional level, you're also able to raise the forest functional level to Windows Server 2012.

MORE INFO **FUNCTIONAL LEVELS**

To learn more about functional levels, consult the following link: ***http://technet.microsoft.com/en-us/library/understanding-active-directory-functional-levels(v=ws.10).aspx*****.**

You can raise the forest functional level using the Active Directory Domains and Trusts console, as shown in Figure 1-3, or using the Set-ADForestMode Windows PowerShell cmdlet. You need to use a user account that is a member of the Enterprise Admins group to perform this task. In general you can't lower the forest functional level after you've raised it. The exception to this rule is that you can lower the forest functional level from Windows Server 2012 to Windows Server 2008 R2 if you haven't enabled Active Directory Recycle Bin.



Forest name:
contoso.com

Current forest functional level:
Windows Server 2012

This forest is operating at the highest possible functional level. For more information on forest functional levels, click Help.

FIGURE 1-3 Raise the forest functional level

Although Active Directory Recycle Bin becomes available at the Windows Server 2008 R2 forest functional level, you need to have configured your organization's forest to run at the Windows Server 2012 forest functional level to be able to use the Active Directory Administrative Center interface as opposed to the command-line interface. Setting the Windows Server 2012 forest functional level does not introduce other features, but it limits the forest to using only domain controllers running Windows Server 2012 or more recent versions of the Windows Server operating system.

✓ **Quick check**

- **What is the minimum forest functional level that enables you to implement Active Directory Recycle Bin?**

Quick check answer

- **You can implement Active Directory Recycle Bin at the Windows Server 2008 R2 forest functional level.**

Multiforest Active Directory environments

Not only do many organizations have more than one domain in their forest, but some organizations have multiple Active Directory forests. Multiple forests often result when organizations merge, during the period before the acquiring organization has subsumed the acquired organization's infrastructure.

Other reasons for having multiple Active Directory forests within a single organization include:

- **Security requirements** You can ensure that administrators of one part of the organization have no rights over another part of the organization by having each part of the organization in a separate forest.
- **Incompatible schemas** All domains in a forest share a schema. If two separate schemas are required for two different parts of the organization, it is necessary to implement multiple forests.
- **Political requirements** Multinational organizations might have to deal with different jurisdictional requirements. It might be simpler to meet these requirements by hav-

ing separate forests with trust relationships than it is to attempt to configure domains within the same forest to meet these different compliance benchmarks.

Upgrading existing domains and forests

You can use one of two strategies when upgrading an existing domain so that you can configure it at the Windows Server 2012 functional level:

- The first strategy is to upgrade the operating systems on each domain controller to Windows Server 2012. This method can be problematic because many organizations are running Windows Server 2003 on domain controllers, and you can't directly upgrade Windows Server 2003 to Windows Server 2012. It's also likely that existing domain controllers are running an x86 version of a Windows Server operating system. Windows operating systems never support direct upgrades from x86 versions to x64 versions.
- You can introduce Windows Server 2012 domain controllers into an existing domain and then decommission existing domain controllers running earlier versions of the Windows Server operating system. This method is less complex than performing a direct upgrade. If the hardware supports it, you can repurpose the existing hardware so that the decommissioned domain controllers have a new purpose as Windows Server 2012 domain controllers (although an increasing number of organizations have domain controllers run on virtual machines).

Unlike previous domain controller upgrades, you don't need to run adprep.exe directly to prepare Active Directory for the introduction of domain controllers running Windows Server 2012. Instead, if you promote the first Windows Server 2012 domain controller using an account that is a member of the Schema Admins and Enterprise Admins group, the schema upgrade occurs automatically. You need to run adprep.exe separately only if you are performing an in-place upgrade of a domain controller running an x64 version of Windows Server 2008 or Windows Server 2008 R2 and if this upgraded domain controller will be the first Windows Server 2012 domain controller in the domain.

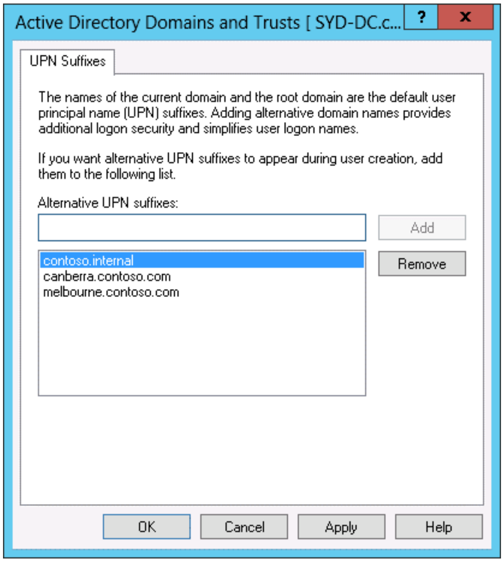
NOTE **ACTIVE DIRECTORY MIGRATION TOOL**

The Active Directory Migration Tool can assist you in migrating from an existing Active Directory environment rather than upgrading an existing environment. Version 3.2 of the Active Directory Migration Tool isn't supported on Windows Server 2012.

User Principal Name (UPN) suffixes

User Principal Name (UPN) suffixes are the part of a user's UPN that trails the @ symbol. For example, in the UPN don_funk@contoso.com, the UPN suffix is the domain name contoso.com. UPN suffixes enable users to sign on using an account name that includes the name of their domains. Because UPN suffixes look like email addresses, users find them easy to remember. This is useful in complex environments where users might be logging on to computers that are members of domains that are different from the domains that host their accounts. For example, Kim Aker's user account might be located in the accounts.contoso.com domain, but she needs to sign on to a computer that is a member of the computers.contoso.com domain. Rather than having to sign on as accounts\kim_akers as her user name, or selecting the accounts domain from a list, she can instead sign on using the UPN of kim_akers@contoso.com.

By default, all users use the UPN suffix that is the name of the root domain, even if their accounts are in a child domain. This is why Kim is able to sign on as kim_akers@contoso.com as contoso.com is the UPN suffix of the root domain. You configure UPN suffixes using the Active Directory Domains and Trusts console as shown in Figure 1-4.



Active Directory Domains and Trusts [SYD-DC.c...

UPN Suffixes

The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

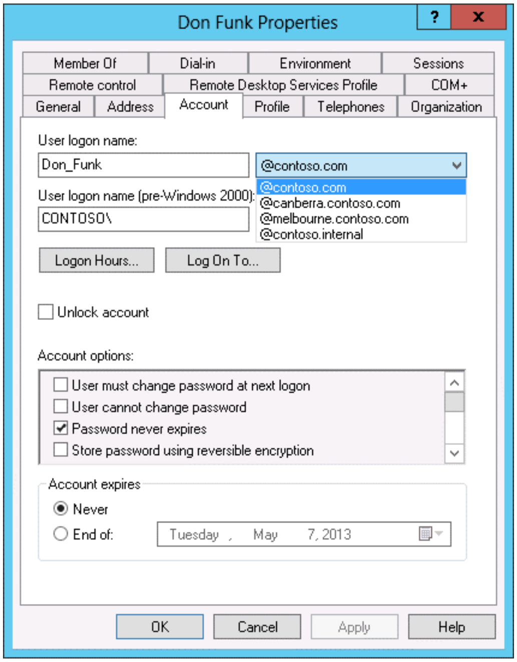
If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

contoso.internal
canberra.contoso.com
melbourne.contoso.com

FIGURE 1-4 Configure alternative UPN suffixes

You can configure the UPN suffix associated with a specific user account on the Account tab of the user account's properties through the Active Directory Users and Computers console as shown in Figure 1-5. When you are configuring forest trusts, you can block or allow user authentication based on UPN suffix.



User logon name:
Don_Funk @contoso.com

@contoso.com
@canberra.contoso.com
@melbourne.contoso.com
@contoso.internal

User logon name (pre-Windows 2000):
CONTOSO\

□ Unlock account

Account options:

□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Tuesday , May 7, 2013

FIGURE 1-5 Configure a specific UPN suffix

MORE INFO **UPN SUFFIXES**

To learn more about UPN suffixes, consult the following link *http://technet.microsoft.com/en-us/library/cc772007.aspx*.

Lesson summary

- A forest can contain multiple domains. Domain trees build on the same namespace. A forest can contain multiple domain trees.
- No hostname in an Active Directory forest can exceed 64 characters.
- The domain functional level is dependent on the earliest version of the Windows Server operating system used on a domain controller in a domain.
- A domain functional level defines the minimum version of the Windows Server operating system that can be used on domain controllers.
- Each domain in a forest can have a different functional level. The forest functional level depends on the lowest domain functional level in the forest.
- You can configure custom UPN suffixes to simplify the sign-on process for users in multidomain and multiforest environments.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of each answer choice in the "Answers" section at the end of this chapter.

1. You are in the process of designing a new Active Directory implementation for your organization. Two different departments in your organization will be adopting applications that have separate and mutually exclusive Active Directory schema requirements. Which of the following Active Directory structures should you use in your design to accommodate these requirements?

    A. A single forest with a single domain tree

    B. A single forest with multiple domain trees

    C. Multiple forests

    D. A single domain forest

2. You are the systems administrator for Tailspin Toys and its subsidiary company Wingtip Toys. You are in the process of designing a new Active Directory structure. You've been asked to ensure that employees who work in the Tailspin Toys part of the organization log into a domain named tailspintoys.com and that employees who work in the Wingtip Toys part of the organization log into a domain named wingtiptoys.com. You want to do this in the simplest way possible and minimize the creation of trust relationships. Which of the following Active Directory structures should you use in your design to accommodate these requirements?

    A. A single domain forest

    B. Multiple forests

    C. A single forest with multiple domain trees

    D. A single forest with a single domain tree

3. You want to deploy several domain controllers running the Windows Server 2012 operating system. You will eventually decommission existing domain controllers and bring the domain up to the Windows Server 2012 domain functional level. What is the minimum domain functional level required to support the introduction of domain controllers running the Windows Server 2012 operating system?

    A. Windows Server 2003 domain functional level

    B. Windows Server 2008 domain functional level

    C. Windows Server 2008 R2 domain functional level

    D. Windows Server 2012 domain functional level

4. At which forest functional levels is the Active Directory Recycle Bin available? (Choose all that apply.)

A. Windows Server 2012 forest functional level

B. Windows Server 2008 R2 forest functional level

C. Windows Server 2008 forest functional level

D. Windows Server 2003 forest functional level

Lesson 2: Configuring trusts

From time to time it's necessary to connect two different domains so that users who have accounts in one domain are able to access resources in another domain. If those domains are owned by the same organization, the simplest way of doing this is by configuring a trust. In this lesson you find out how to configure trusts between two different forests, between two separate domains in different forests, and between a domain and a Kerberos realm.

After this lesson, you will be able to:

- Configure external, forest, shortcut, and realm trusts
- Configure trust authentication
- Configure SID filtering
- Configure name suffix routing

Estimated lesson time: 45 minutes

Trusts

Trusts make it possible for users in one domain to be authenticated by domain controllers in a separate domain. For example, if there is a bidirectional trust relationship between the domains contoso.local and adatum.remote, users with accounts in the contoso.local domain are able to authenticate in the adatum.remote domain. By configuring a trust relationship, it's possible to allow users in one domain to access resources in another, such as being able to use shared folders and printers or being able to sign on locally to machines that are members of a different domain than the one that holds the user's account.

Some trusts are created automatically. For example, domains in the same forest automatically trust each other. Other trusts, such as *external trusts*, *realm trusts*, *shortcut trusts*, and forest trusts must be created manually. Trusts use the Kerberos V5 authentication protocol by default, and they revert to NTLM if Kerberos V5 if not supported. You configure and manage trusts using the Active Directory Domains and Trusts console or the netdom.exe command-line utility with the trust switch.

REAL WORLD **UNDERSTANDING TRUSTS**

Although trusts themselves are relatively easy to come to terms with, the terminology around trusts tends to confuse many people. It's important that you understand the difference between a trusting and a trusted domain and how trust direction, incoming or outgoing, relates to which security principals are able to authenticate.

To understand trusts, you need to understand the difference between a trusting domain or forest and a trusted domain or forest. The trusting domain or forest contains the resources to which you want to grant security principals from the trusted domain or forest access. The trusted domain or forest hosts the security principals that you want to allow to access resources in the trusting forest. For example, if you want to grant users in the adatum.remote domain access to resources in the contoso.local domain, the adatum.remote domain is the trusted domain and the contoso.local domain is the trusting domain. In by-directional trust relationships a domain or forest is both trusting and trusted.

MORE INFO **TRUSTS**

To learn more about the basics of trusts consult the following link: *http://technet.microsoft.com/en-us/library/cc731335.aspx*.

Trust transitivity

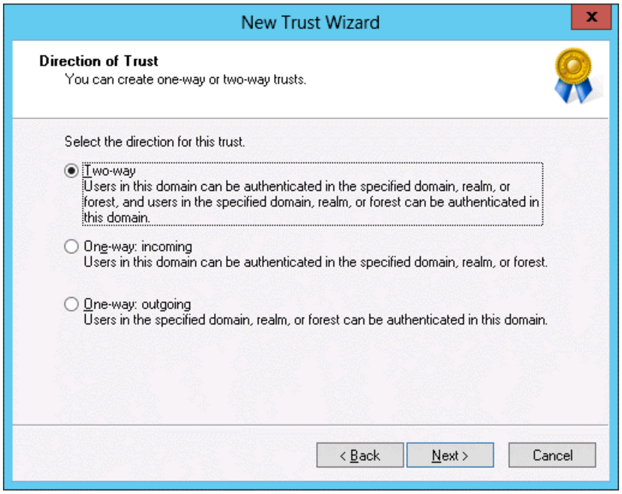
A *transitive trust* is one that extends beyond the original trusting domains. For example, if you have a trust between two domain forests and that trust is transitive, all the domains in each of the forests trust each other. Forest trusts are transitive by default. External trusts are not transitive by default. When you create a trust, keep in mind that there may be domains beyond the one you are establishing the relationship with that may be included. You might trust the administrator of adatum.remote not to allow access by nefarious users, but do you trust the administrator of subdomain.adatum.remote?

MORE INFO **TRUST TRANSITIVITY**

To learn more about trust transitivity, consult the following link: *http://technet.microsoft.com/en-us/library/cc754612.aspx*.

Trust direction

When you create a new trust, you specify a trust direction as shown in Figure 1-6. You can choose a two-way (or bidirectional) trust or a unidirectional trust, which is either one-way incoming or one-way outgoing.



New Trust Wizard

Direction of Trust

You can create one-way or two-way trusts.

Select the direction for this trust.

● Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.

○ One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.

○ One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.

FIGURE 1-6 Specify the trust direction

When you configure a one-way incoming trust, users in the local are authenticated in the remote domain, realm, or forest. Remember that if you are configuring a one-way incoming trust between the single domain forests contoso.local and adatum.remote, users with accounts in contoso.local are able to access resources in adatum.remote. Similarly if you are configuring a one-way outgoing trust between the single domain forests contoso.local and adatum.remote, users with accounts in adatum.remote are able to access resources hosted in contoso.local.

The terminology around trusts can be a little confusing. The key thing to remember is that the direction of trust is the opposite of the direction of access, as shown in Figure 1-7. An outgoing trust allows incoming access, and an incoming trust allows outgoing access.

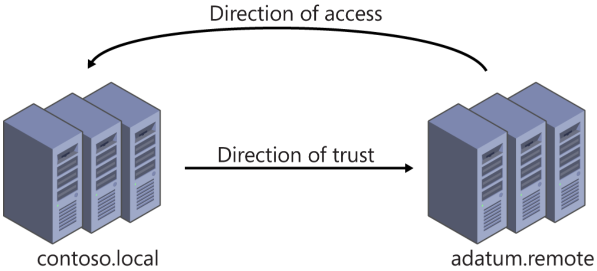


FIGURE 1-7 The direction of trust and direction of access

MORE INFO **TRUST DIRECTION**

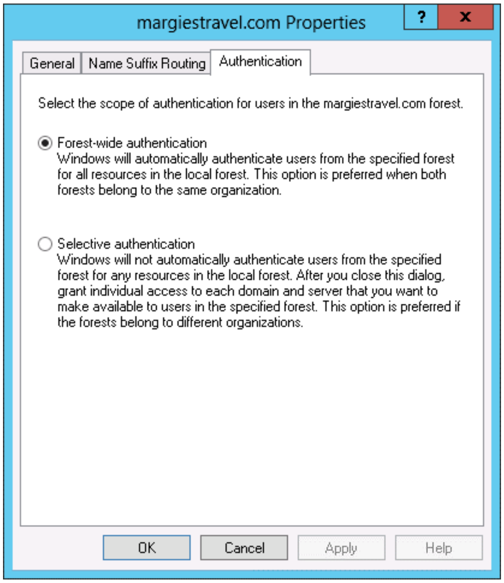
To learn more about trust direction, consult the following link: ***http://technet.microsoft.com/en-us/library/cc731404.aspx.***

Forest trusts

When you configure a forest trust, one Active Directory forest trusts the other one. Forest trusts are transitive. When you configure a forest trust, you can allow any domain in the trusting forest to be accessible to any security principal in the trusted forest. Forest trusts require that each forest be configured to run at the Windows Server 2003 forest functional level or higher. Forest trusts can be bi- or unidirectional. You are most likely to configure forest trusts if your organization has two or more Active Directory forests.

You can configure one of two authentications scopes when you configure a forest trust. The type of authentication scope that you configure depends on your security requirements. The options are:

- **Forest-wide authentication** When you choose forest-wide authentication, users from the trusted forest are automatically authenticated for all resources in the local forest. You should use this option when both the trusted and trusting forest are part of the same organization. Figure 1-8 shows a forest trust configured with this type of authentication.
- **Selective authentication** When you configure this option, Windows does not automatically authenticate users from the trusted forest. You can then configure specific servers and domains within the forest to allow users from the trusted forest to authenticate. Use this option when the two forests are from different organizations, or you have more stringent security requirements.



Select the scope of authentication for users in the margiestravel.com forest.

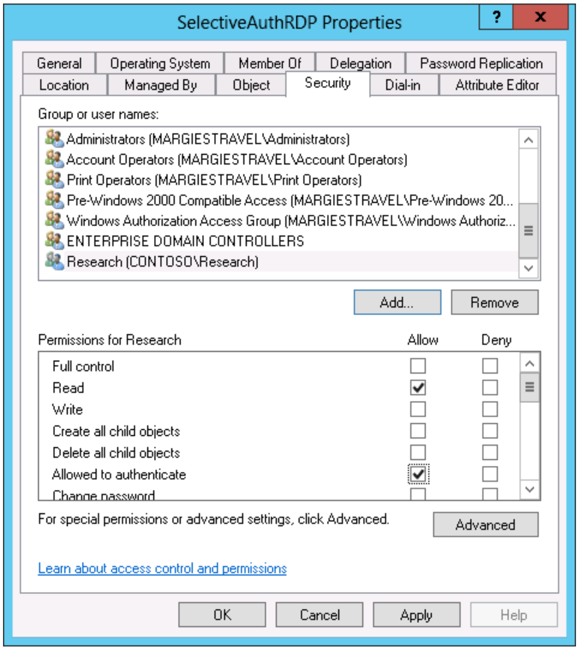
● Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.

○ Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you close this dialog, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.

FIGURE 1-8 Configure the authentication type

Configuring selective authentication

Configuring *selective authentication* means granting specific security principals in the trusted forest the Allowed to authenticate (allow) permission on the computer that hosts the resource to which you want to grant access. For example, assume you had configured a forest trust with selective authentication. You want to grant users in the Research universal group from the trusted forest access to a Remote Desktop Services (RDS) server in the trusting forest. To accomplish this goal, you can configure the properties of the RDS server's computer account in Active Directory Users and Computers and grant the Research universal group from the trusted forest the Allowed to authenticate permission as shown in Figure 1-9. Doing this only allows users from this group to authenticate; you still have to grant them access to RDS by adding them to the appropriate local group on the RDS server.



Group or user names:

- Administrators (MARGIESTRAVEL\Administrators)
- Account Operators (MARGIESTRAVEL\Account Operators)
- Print Operators (MARGIESTRAVEL\Print Operators)
- Pre-Windows 2000 Compatible Access (MARGIESTRAVEL\Pre-Windows 20...
- Windows Authorization Access Group (MARGIESTRAVEL\Windows Authoriz...
- ENTERPRISE DOMAIN CONTROLLERS
- Research (CONTOSO\Research)

Permissions for Research	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	☑	□
Change password	□	□

For special permissions or advanced settings, click Advanced.

Learn about access control and permissions

FIGURE 1-9 Configure the Allowed to Authenticate permission

External Trusts

External trusts enable you to configure one domain in one forest to trust a domain in another forest without enabling a transitive trust. For example, you configure an external trust if you want to allow the auckland.fabrikam.com domain to have a trust relationship with the wellington.adatum.com domain without allowing any other domains in the fabrikam.com or adatum.com forests to have a security relationship with one another.

MORE INFO **EXTERNAL TRUSTS**

To learn more about external trusts, consult the following link: ***http://technet.microsoft.com/en-us/library/cc732859.aspx*****.**

You can use External Trusts to configure trust relationships with domains running unsupported Windows Server operating systems, such as Windows 2000 Server and Windows NT 4.0, because these operating systems do not support Forest Trusts. Even though these operating systems are well beyond their supported lifespan, there are still organizations out there with servers, and even domains, running these operating systems. It's possible, however unlikely, that you might need to configure a trust relationship between a domain running these operating systems and one running Windows Server 2012 domain controllers.

✓ **Quick check**

- **You are the administrator of the single domain contoso.local forest. Users in the adatum.remote single domain forest need to access resources in the contoso.local domain. Users in contoso.local should not have access to resources in adatum.remote. You are configuring an external trust between these two single domain forests from the contoso.local domain. Which trust direction should you configure to support this configuration?**

Quick check answer

- **One-way outgoing. Remember that the direction of trust is opposite to the direction of authentication. To have incoming users authenticated, you configure an outgoing trust.**

Shortcut trusts

Shortcut trusts enable you to speed up authentication between domains in a forest that might be in separate branches or even separate trees. For example, in the hypothetical forest shown in Figure 1-10, if a user in the fiji.pacific.contoso.com domain wants to access a resource in the arctic.adatum.com domain, authentication needs to travel up through the pacific.contoso.com and contoso.com domains before passing across to the adatum.com domain and finally back to the arctic.adatum.com. If you implement a shortcut trust between the fiji.pacific.contoso.com and arctic.adatum.com domains, authentication traffic in-stead travels directly between these two domains without having to traverse the two domain trees in the forest.

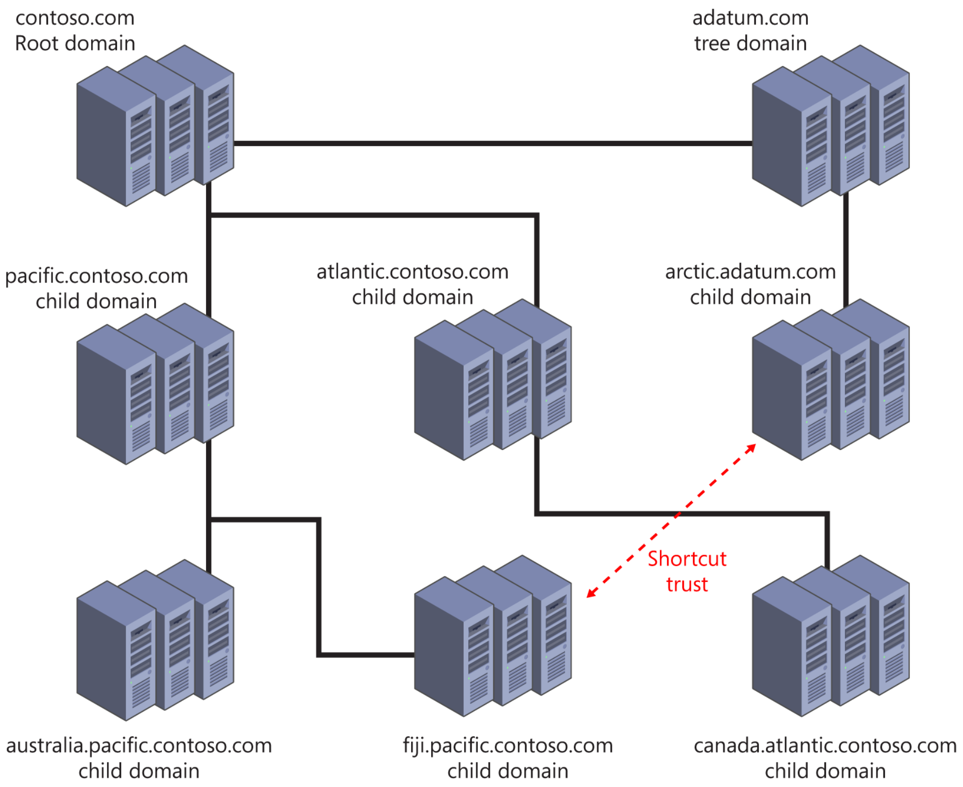
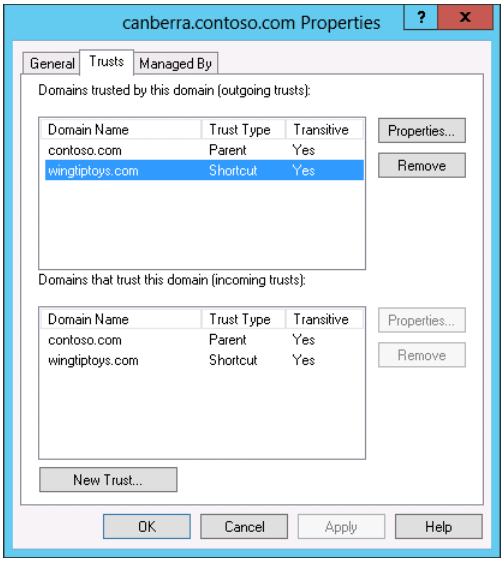


FIGURE 1-10 Shortcut trust

You configure a shortcut trust using the Active Directory Domains and Trusts console by editing the properties of one domain and triggering the New Trust Wizard on the Trusts tab. When the trust is created, it is listed as a shortcut trust as shown in Figure 1-11. Shortcut trusts can be uni- or bidirectional. As is the case with the creation of other trusts, ensure that you have name resolution working properly between the trusting and the trusted domains either by having the Domain Name System (DNS) zones propagate through the forest, by configuring conditional forwarders, or by configuring stub zones.



Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
contoso.com	Parent	Yes
wingtiptoys.com	Shortcut	Yes

Domains that trust this domain (incoming trusts):

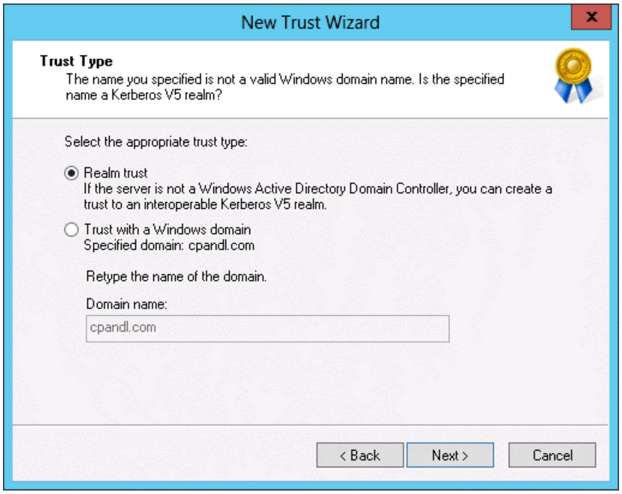
Domain Name	Trust Type	Transitive
contoso.com	Parent	Yes
wingtiptoys.com	Shortcut	Yes

FIGURE 1-11 A shortcut trust

Realm trusts

You use a realm trust to create a relationship between an Active Directory Services domain and a Kerberos V5 realm that uses a third-party directory service. Realm trusts can be transitive or nontransitive. They can also be uni- or bidirectional. You're most likely to configure a realm trust when you need to allow users who use a UNIX directory service to access resources in an Active Directory domain or users in an Active Directory domain to access resources in a UNIX Kerberos V5 realm.

You can configure a realm trust from the Active Directory Domains and Trust console. You do this by selecting the Realm trust option as shown in Figure 1-12. When configuring a realm trust, you specify a realm trust password that you use when configuring the other side of the trust in the Kerberos V5 realm.



Trust Type

The name you specified is not a valid Windows domain name. Is the specified name a Kerberos V5 realm?

Select the appropriate trust type:

● Realm trust
If the server is not a Windows Active Directory Domain Controller, you can create a trust to an interoperable Kerberos V5 realm.

○ Trust with a Windows domain
Specified domain: cpandl.com

Retype the name of the domain.

Domain name:
cpandl.com

FIGURE 1-12 Configure the realm trust

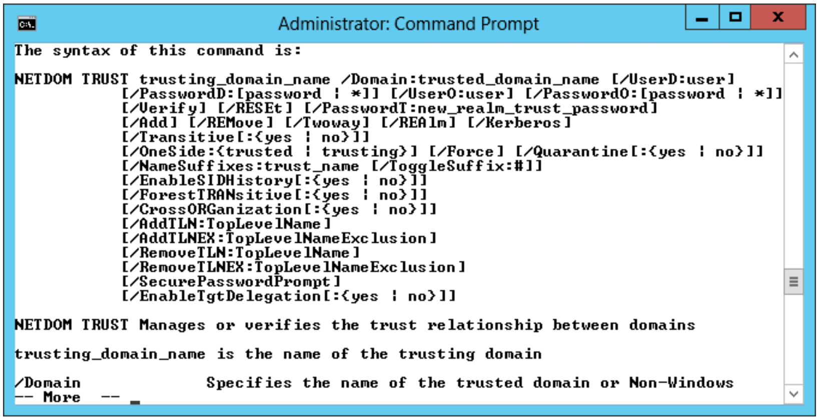
MORE INFO **REALM TRUSTS**

To learn more about realm trusts, consult the following link: ***http://technet.microsoft.com/en-us/library/cc731297.aspx*****.**

Netdom.exe

You use netdom.exe with the /trust switch to create and manage trusts from the command line. When using netdom.exe, you specify the trusting domain name and the trusted domain name. You can use netdom.exe with the /trust switch to create and manage forest, shortcut, realm, and external trusts.

The syntax of the netdom.exe command with the trust switch is shown in Figure 1-13.



```
The syntax of this command is:

NETDOM TRUST trusting_domain_name /Domain:trusted_domain_name [/UserD:user]
           [/PasswordD:[password | *]] [/UserO:user] [/PasswordO:[password | *]]
           [/Verify] [/RESEt] [/PasswordT:new_realm_trust_password]
           [/Add] [/REMove] [/Twoway] [/REAlm] [/Kerberos]
           [/Transitive[:{yes | no}]]
           [/OneSide:{trusted | trusting}] [/Force] [/Quarantine[:{yes | no}]]
           [/NameSuffixes:trust_name [/ToggleSuffix:#]]
           [/EnableSIDHistory[:{yes | no}]]
           [/ForestTRANsitive[:{yes | no}]]
           [/CrossORGanization[:{yes | no}]]
           [/AddTLN:TopLevelName]
           [/AddTLNEX:TopLevelNameExclusion]
           [/RemoveTLN:TopLevelName]
           [/RemoveTLNEX:TopLevelNameExclusion]
           [/SecurePasswordPrompt]
           [/EnableTgtDelegation[:{yes | no}]]

NETDOM TRUST Manages or verifies the trust relationship between domains

trusting_domain_name is the name of the trusting domain

/Domain             Specifies the name of the trusted domain or Non-Windows
-- More  -- _
```

FIGURE 1-13 The command syntax for netdom.exe

At release, Windows PowerShell in Windows Server 2012 does not include much in the way of cmdlets for creating and managing trust relationships beyond the Get-ADTrust cmdlet.

SID filtering

In a trusted domain, it's possible, though extremely difficult, for you to configure an account in your domain to have SIDs that are identical to those used by privileged accounts in a trusting domain. If you use this configuration then the accounts from trusted domains gain the privileges of the accounts in the trusting domain. For example, you can configure the SIDs of an account in a trusted domain so that it has domain administrator privileges in the trusting domain.

To block this type of configuration, Windows Server 2012 enables *SID filtering*, also known as *domain quarantine*, on all external trusts. SID filtering blocks users in a trusted forest or domain from being able to grant themselves elevated user rights in the trusting forest domain by discarding all SIDs that do not have the domain SID of the trusting domain.

It's possible to verify SID filtering settings on a trust using the Get-ADTrust cmdlet in a Windows PowerShell session run by a user with administrative privileges. For example, to verify that SID filtering is enabled on the trust with the margiestravel.com forest, issue the command:

```
Get-ADTrust margiestravel.com | fl *SID*
```

To disable SID filtering for the trusting forest, use the netdom trust command with the following option:

```
/enablesidhistory:Yes
```

Enabling SID history allows SIDs that don't have the domain SID of the trusting domain. You enable or disable SID filtering on the trusting side of the trust. For example, if you are an administrator in the contoso.com domain and you want to disable SID filtering, you can issue the following command from an elevated command prompt:

```
Netdom trust contoso.com /domain:margiestravel.com /enablesidhistory:Yes
```

In the same scenario, if you want to re-enable SID filtering, you can issue the following command:

```
Netdom trust contoso.com /domain:margiestravel.com /enablesidhistory:No
```

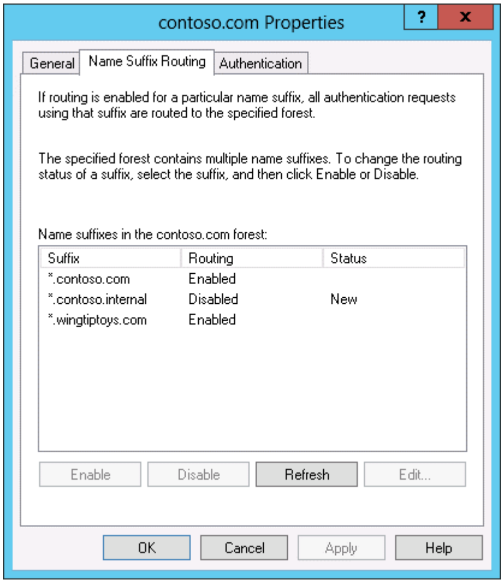
The default configuration, where SID filtering is enforced by default on trusts, is something that you should probably leave as it is. In the past it was necessary to allow SID history when trusts were created with forests running Windows 2000 Server domain controllers. As Windows 2000 is no longer supported by Microsoft, and SID history is not necessary for trust relationships with Windows Server 2003, Windows Server 2003 R2, Windows Server 2008, Windows Server 2008 R2, or Windows Server 2012 domain controllers, you probably won't need to disable it.

MORE INFO **SID FILTER QUARANTINING ON EXTERNAL TRUSTS**

To learn more about SID filtering, consult the following link: *http://technet.microsoft.com/en-us/library/cc794757(v=ws.10).aspx.*

Name suffix routing

Name suffix routing enables you to configure how authentication requests are routed when you configure a forest trust between two Active Directory forests. When you create a forest trust, all unique name suffixes are routed. Name suffix routing assists when users sign on with a UPN, such as don_funk@contoso.com. Depending upon the UPNs that are configured, you might want to allow or disallow the use of specific UPN suffixes. You do this by configuring name suffix routing on the Name Suffix Routing tab of the trust's properties as shown in Figure 1-14.



If routing is enabled for a particular name suffix, all authentication requests using that suffix are routed to the specified forest.

The specified forest contains multiple name suffixes. To change the routing status of a suffix, select the suffix, and then click Enable or Disable.

Name suffixes in the contoso.com forest:

Suffix	Routing	Status
*.contoso.com	Enabled	
*.contoso.internal	Disabled	New
*.wingtiptoys.com	Enabled	

FIGURE 1-14 Configure name suffix routing

MORE INFO **NAME SUFFIX ROUTING**

To learn more about name suffix routing, consult the following link: *http://technet.microsoft.com/en-us/library/cc731648.aspx.*

Lesson summary

- Trusts can be uni- or bidirectional. A one-way outgoing trust allows users in the remote domain to access resources in the local domain. A one-way incoming trust allows users in the local domain to access resources in the remote domain.
- Trust transitivity allows access to resources in child domains of the trusting domain.
- A forest trust allows one forest to trust another forest. This means that all domains in the first forest have a trust relationship with all domains in the second forest.
- Selective authentication in a forest trust enables you to limit which users and groups from the trusted domain are able to authenticate.
- An external trust is a trust between domains in different forests. External trusts are not transitive. You can configure external trusts to connect to Windows 2000 Server and Windows NT 4 domains.
- You use a realm trust when you want to configure a trust between an Active Directory domain and a Kerberos V5 realm.
- You can use a shortcut trust between domains in the same forest to speed the authentication process.
- SID filtering is enabled by default on all new external and forest trusts.
- You can configure name suffix routing to configure which users are able to authenticate in a forest.

Lesson review

Answer the following questions to test your knowledge of the information in this lesson. You can find the answers to these questions and explanations of each answer choice in the "Answers" section at the end of this chapter.

1. You have a 30-domain Active Directory forest that has contoso.com as its root domain. This forest has five separate domain trees. Users in the melbourne.australia.pacific.contoso.com domain report that there are substantial authentication delays when they try to access resources in the auckland.newzealand.adatum.com domain. Both domains are located in the same forest. Which of the following trust types would you configure to resolve this problem?

   A. Forest trust

   B. External trust

   C. Realm trust

   D. Shortcut trust

2. You are a systems administrator at a local university. The university has a deployment of Linux servers and workstations that are members of a Kerberos V5 realm. You want to allow users of the Linux workstations to have access to several file shares hosted in one of your organization's Active Directory domains. Which of the following trust types would you implement to accomplish this goal?

   A. Shortcut trust

   B. Realm trust

   C. Forest trust

   D. External trust

3. Your organization recently acquired a subsidiary company. Your organization currently has a 10-domain Active Directory forest running at the Windows Server 2012 functional level. The subsidiary company has a five-domain Active Directory forest running at the Windows Server 2008 functional level. The subsidiary company has implemented a number of schema modifications to support a custom application. You want to allow users in the subsidiary company to be able to access resources hosted in your organization's forest. Users in your organization's forest should also be able to access resources in the subsidiary company's forest. Which of the following trust relationships should you configure to accomplish this goal?

   A. External trust

   B. Forest trust

   C. Realm trust

   D. Shortcut trust

4. You are the senior systems administrator of the contoso.com forest. Users in the australia.pacific.contoso.com domain need access to resources hosted in one domain of a partner organization's Active Directory forest. These users shouldn't have access to any other domain in the partner organization's forest. Users from other domains in your organization's forest should also not have access to resources in the partner organization's forest. Which of the following trust types would you configure in this scenario?

   A. External trust

   B. Realm trust

   C. Shortcut trust

   D. Forest trust

Practice exercises

The goal of this section is to provide you with hands-on practice with the following:

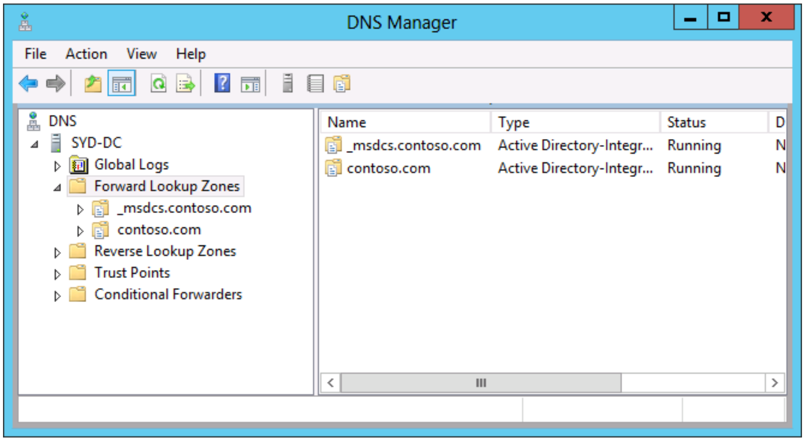
- Creating a forest trust
- Configuring name suffix routing
- Configuring selective authentication
- Configuring UPN suffixes
- Configuring a shortcut trust

To perform the exercises in this section, you need access to an evaluation version of Windows Server 2012. You should also have access to virtual machines SYD-DC, MEL-DC, CBR-DC, and ADL-DC, the setup instructions for which are as described in the Introduction. You should ensure that you have a snapshot of these virtual machines that you can revert to at the end of the practice exercises.

Exercise 1: Prepare a domain controller to host a child domain with a contiguous namespace

In this exercise, you prepare CBR-DC to function as a domain controller for a child domain of the contoso.com domain. To complete this exercise, perform the following steps:

1. Power on SYD-DC and log in as contoso\don_funk with the password Pa$$w0rd.
2. Click the Tools menu in the Server Manager console, and click DNS.
3. In the DNS Manager console, expand SYD-DC and Forward Lookup Zones.
4. Verify that the following lookup zones are present as shown in Figure 1-15:
   - _msdcs.contoso.com
   - contoso.com



Name	Type	Status	D
_msdcs.contoso.com	Active Directory-Integr...	Running	N
contoso.com	Active Directory-Integr...	Running	N

FIGURE 1-15 Verify the DNS configuration

5. Power on CBR-DC and sign on as Administrator with the password Pa$$w0rd.

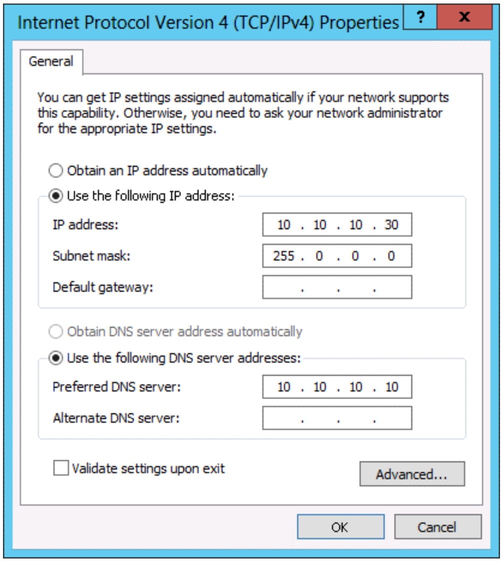
6. In Server Manager, click the Local Server node.

7. In the Properties area, click 10.10.10.30 next to Ethernet.

8. In the Network Connections window, right-click Ethernet and click Properties.

9. In the Ethernet Properties dialog box, click Internet Protocol Version 4 (TCP/IPv4) and click Properties.

10. Verify that the Preferred DNS Server is set to 10.10.10.10, as shown in Figure 1-16, click OK, and then click Close.



Internet Protocol Version 4 (TCP/IPv4) Properties

General

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 10 . 10 . 10 . 30

Subnet mask: 255 . 0 . 0 . 0

Default gateway: . . .

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 10 . 10 . 10 . 10

Alternate DNS server: . . .

□ Validate settings upon exit

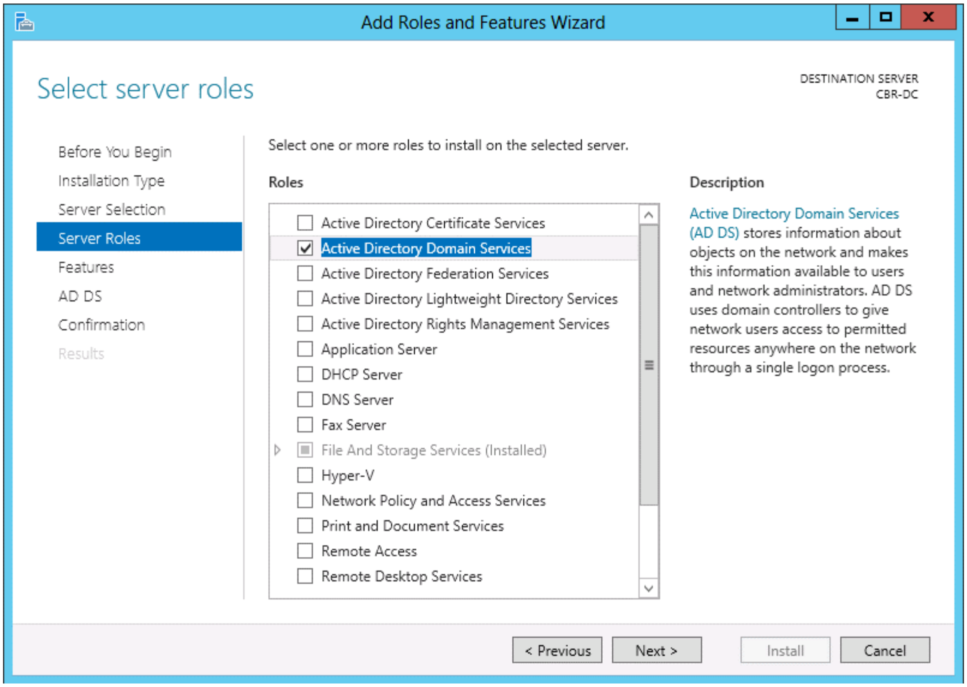
FIGURE 1-16 Verify the Internet Protocol (IP) address configuration

11. In the Server Manager console, click Manage and then click Add Roles and Features.

12. On the Before You Begin page of the Add Roles and Features Wizard, click Next three times.

13. On the Select Server Roles page, click the Active Directory Domain Services check box as shown in Figure 1-17.

14. On the Add Roles and Features Wizard, click Add Features.



Select server roles

DESTINATION SERVER
CBR-DC

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- ☑ Active Directory Domain Services
- □ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Application Server
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ▣ File And Storage Services (Installed)
- □ Hyper-V
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services

Description

Active Directory Domain Services (AD DS) stores information about objects on the network and makes this information available to users and network administrators. AD DS uses domain controllers to give network users access to permitted resources anywhere on the network through a single logon process.

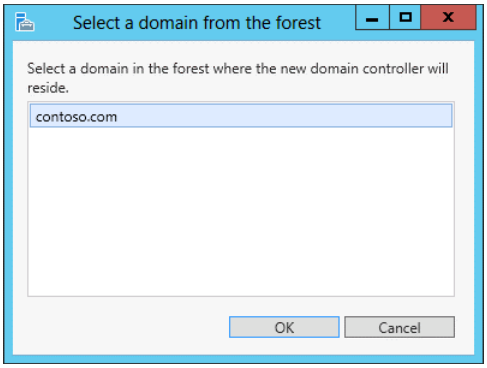
FIGURE 1-17 Add the AD DS role

15. On the Select Server Roles page, click Next three times and click Install. When the installation completes, click Close.

Exercise 2: Create a child domain with a noncontiguous namespace

In this exercise, you configure CBR-DC to host the Canberra.contoso.com child domain. To complete this exercise, perform the following steps:

1. In the Server Manager console on CBR-DC, click the Notifications item and then click Promote This Server to a Domain Controller.
2. On the Deployment Configuration page, click Add a New Domain to an Existing Forest.
3. On the Select Domain Type drop-down menu, select Child Domain.
4. Click Select next to Parent Domain Name.
5. In the Windows Security dialog box, enter the user name contoso\don_funk, enter the password Pa$$w0rd, and click OK.
6. In the Select a Domain from the Forest dialog box, click contoso.com as shown in Figure 1-18 and then click OK.

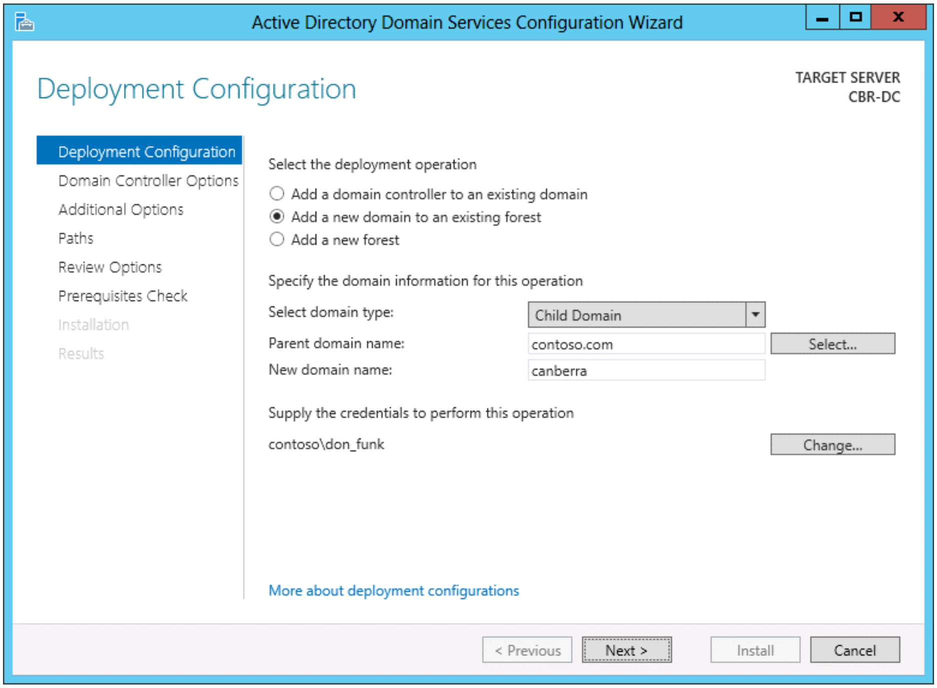


Select a domain in the forest where the new domain controller will reside.

contoso.com

FIGURE 1-18 Select the domain in the forest

7. In the New Domain Name text box enter the name Canberra as shown in Figure 1-19 and then click Next.



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

Select domain type: Child Domain
Parent domain name: contoso.com
New domain name: canberra

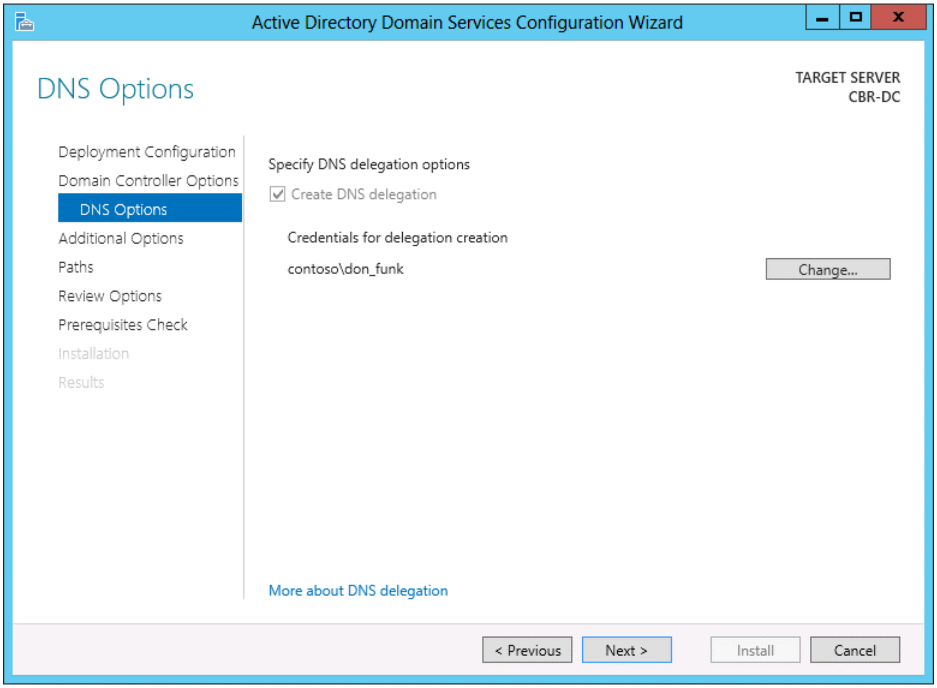
Supply the credentials to perform this operation

contoso\don_funk

FIGURE 1-19 Configure the child domain

8. On the Domain Controller Options page, set the DSRM password as Pa$$w0rd in both the Password and Confirm Password dialog boxes and click Next.

9. On the DNS Options page, ensure that the settings match those in Figure 1-20 and click Next.



Specify DNS delegation options

☑ Create DNS delegation

Credentials for delegation creation

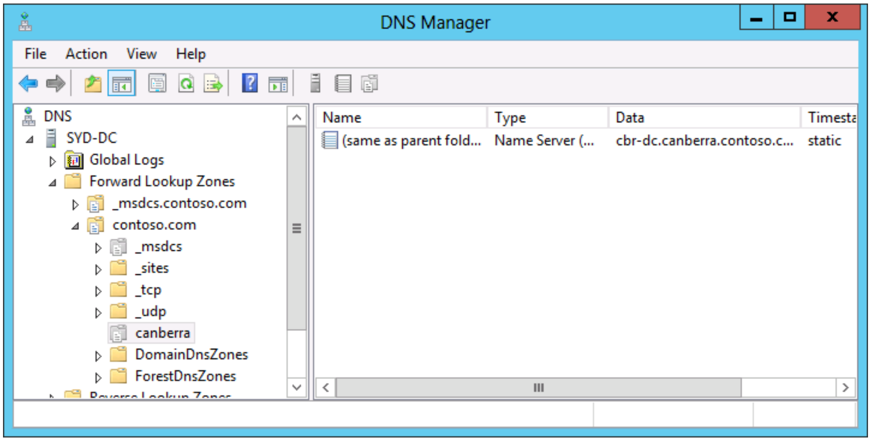
contoso\don_funk

FIGURE 1-20 Configure the delegation credentials

10. On the additional options page, verify that the NetBIOS domain name is set to CANBERRA, click Next three times, and click Install.

11. After CBR-DC restarts, sign on as Canberra\Administrator with the password Pa$$w0rd.

12. Switch to SYD-DC. In the DNS console, expand the contoso.com zone and verify the presence of the canberra.contoso.com zone as shown in Figure 1-21.



Name	Type	Data	Timesta
(same as parent fold...	Name Server (...	cbr-dc.canberra.contoso.c...	static

FIGURE 1-21 Verify the DNS zone

Exercise 3: Prepare domain controller to host the wingtiptoys.com tree in the contoso.com forest

In this exercise, you prepare computer ADL-DC so that it can be promoted to a domain controller. To complete this exercise, perform the following steps:

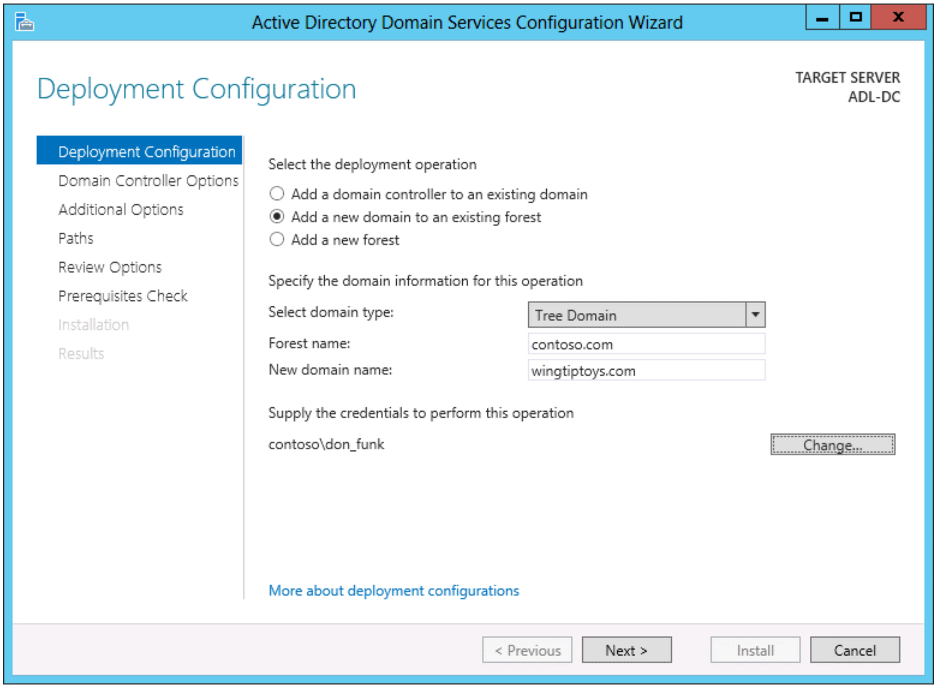
1. Sign on to ADL-DC as Administrator with the password Pa$$w0rd.
2. In Server Manager, click the Local Server node.
3. In the Properties area, click 10.10.10.20 next to Ethernet.
4. In the Network Connections window, right-click Ethernet and click Properties.
5. In the Ethernet Properties dialog box, click Internet Protocol Version 4 (TCP/IPv4) and click Properties.
6. Verify that the Preferred DNS server is set to 10.10.10.10 and then click OK. Click Close.
7. In the Server Manager console, click Manage and then click Add Roles and Features.
8. On the Before You Begin page of the Add Roles and Features Wizard, click Next three times.
9. On the Select Server Roles page, click the Active Directory Domain Services check box.
10. On the Add Roles and Features Wizard, click Add Features.
11. On the Select Server Roles page, click Next three times and click Install. When the installation completes, click Close.

Exercise 4: Promote domain controller for new tree in contoso.com forest

In this exercise, you promote ADL-DC to domain controller of a new domain tree in an existing Active Directory forest. To complete this exercise, perform the following steps:

1. In the Server Manager console on ADL-DC, click the Notifications item and then click Promote This Server to a Domain Controller.
2. On the Deployment Configuration page, click Add a New Domain to an Existing Forest.
3. On the Select Domain Type drop-down menu, click Tree Domain.
4. In the Forest Name text box, type contoso.com.
5. In the New Domain Name text box, type wingtiptoys.com.
6. Next to <No Credentials Provided>, click Change.
7. On the Windows Security dialog box, enter the user name as contoso\don_funk, enter the password as Pa$$w0rd, and click OK.

8. Verify that the Deployment Configuration page matches Figure 1-22 and then click Next.



Deployment Configuration

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

Select domain type: Tree Domain

Forest name: contoso.com

New domain name: wingtiptoys.com

Supply the credentials to perform this operation

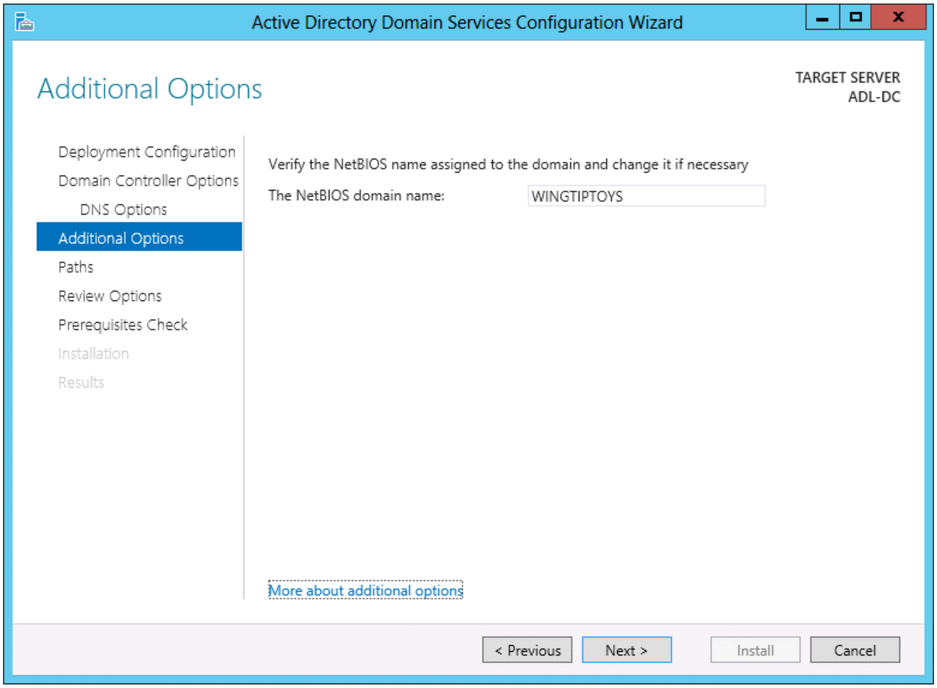
contoso\don_funk

FIGURE 1-22 Add a domain tree

9. On the Domain Controller Options page, enter the DSRM password Pa$$w0rd in both the Password and Confirm Password text boxes and then click Next.

10. On the DNS Options page, review the warning and click Next.

11. On the Additional Options page, verify that the NetBIOS name is set to WINGTIPTOYS as shown in Figure 1-23. Click Next three times and then click Install.



Verify the NetBIOS name assigned to the domain and change it if necessary

The NetBIOS domain name: WINGTIPTOYS

FIGURE 1-23 Verify the NetBIOS name

12. After the computer restarts, sign in as WINGTIPTOYS\Administrator with the password Pa$$w0rd.

Exercise 5: Prepare a domain controller to host a new forest

In this exercise, you configure MEL-DC so that it is able to host the new forest margiestravel.com. To complete this exercise, perform the following steps:

1. Sign on to MEL-DC as Administrator with the password Pa$$w0rd.
2. In Server Manager, click the Local Server node.
3. In the Properties area, click 10.10.10.40 next to Ethernet.
4. In the Network Connections window, right-click Ethernet and click Properties.
5. In the Ethernet Properties dialog box, click Internet Protocol Version 4 (TCP/IPv4) and click Properties.
6. Verify that the Preferred DNS server is set to 10.10.10.10, click OK, and then click Close.
7. In the Server Manager console, click Manage and then click Add Roles and Features.

8. On the Before You Begin page of the Add Roles and Features Wizard, click Next three times.

9. On the Select Server Roles page, click the Active Directory Domain Services check box.

10. On the Add Roles and Features Wizard, click Add Features.

11. On the Select Server Roles page, click Next three times and then click Install. When the installation completes, click Close.

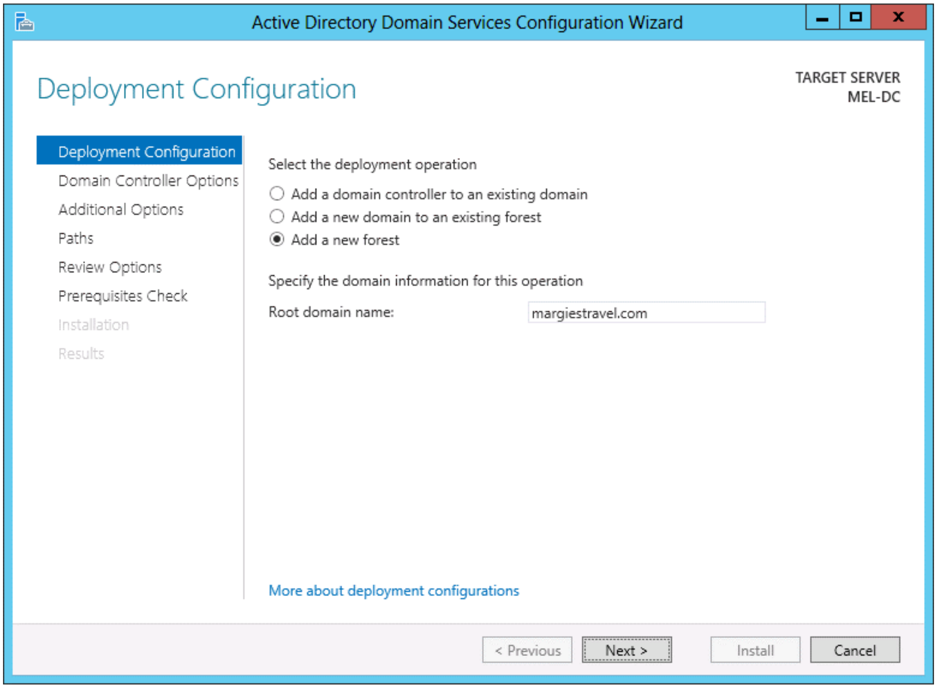
Exercise 6: Create new forest

In this exercise, you configure MEL-DC as the first domain controller in a new forest. To complete this exercise, perform the following steps:

1. In the Server Manager console on MEL-DC, click the Notifications item and then click Promote This Server to a Domain Controller.

2. On the Deployment Configuration page, click Add a new forest.

3. In the Root Domain Name textbox, type margiestravel.com as shown in Figure 1-24 and click Next.



Active Directory Domain Services Configuration Wizard

Deployment Configuration

TARGET SERVER
MEL-DC

Select the deployment operation

○ Add a domain controller to an existing domain
○ Add a new domain to an existing forest
● Add a new forest

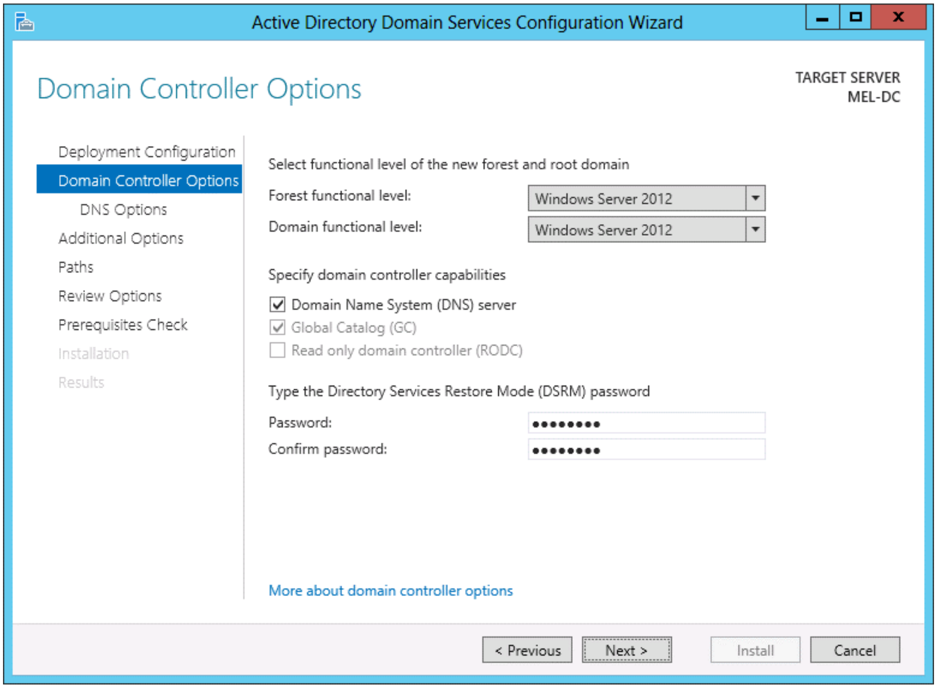
Specify the domain information for this operation

Root domain name: margiestravel.com

More about deployment configurations

FIGURE 1-24 Add a new forest

4. On the Domain Controller Options page, ensure that Domain Name System (DNS) server is selected and that you enter the DSRM password of Pa$$word twice as shown in Figure 1-25. Click Next twice.



Active Directory Domain Services Configuration Wizard

Domain Controller Options

TARGET SERVER
MEL-DC

Select functional level of the new forest and root domain

Forest functional level: Windows Server 2012

Domain functional level: Windows Server 2012

Specify domain controller capabilities

☑ Domain Name System (DNS) server

☑ Global Catalog (GC)

□ Read only domain controller (RODC)

Type the Directory Services Restore Mode (DSRM) password

Password: ●●●●●●●●

Confirm password: ●●●●●●●●

FIGURE 1-25 The Domain Controller options page

5. On the Additional Options page, verify that the NetBIOS domain name is set to MARGIESTRAVEL, click Next three times, and then click Install.

6. After the server restarts, sign on as MARGIESTRAVEL\Administrator with the password Pa$$w0rd.

Exercise 7: Prepare to configure a forest trust relationship

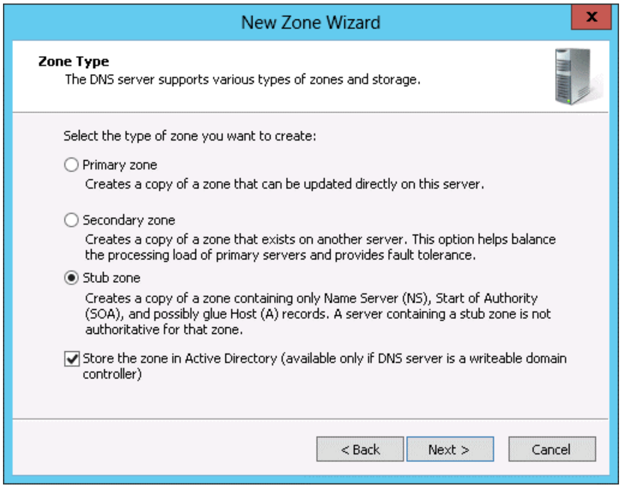
In this exercise, you configure a forest trust relationship between the contoso.com forest and the margiestravel.com forest. To complete this exercise, perform the following steps:

1. While logged onto SYD-DC as contoso\don_funk, open the DNS Manager console from the Tools menu in the Server Manager console.

2. Right-click on Forward Lookup Zones and click New Zone.

3. On the Welcome to the New Zone Wizard page, click Next.

4. On the Zone Type page, click Stub Zone and ensure that the Store the Zone in Active Directory check box is selected as shown in Figure 1-26. Click Next.



Zone Type

The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

○ Primary zone
Creates a copy of a zone that can be updated directly on this server.

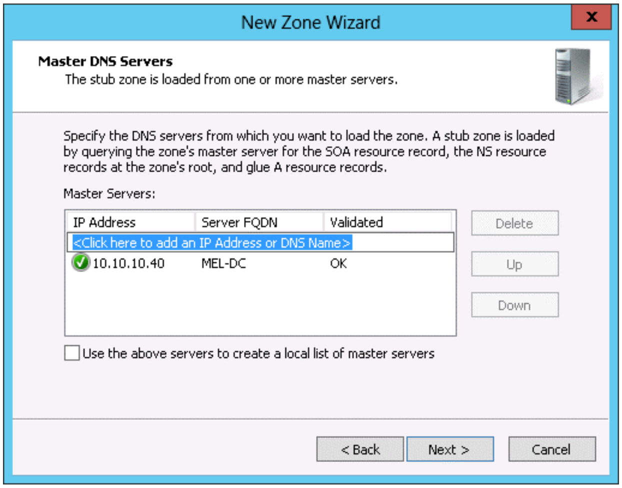
○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

● Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

FIGURE 1-26 Configure the zone type

5. On the Active Directory Zone Replication Scope page, click To All DNS Servers Running on Domain Controllers in this Forest: contoso.com and click Next.
6. In the Zone Name text box, enter margiestravel.com and click Next.
7. On the Master DNS Servers page, type the IP address 10.10.10.40 in the list of master servers as shown in Figure 1-27, click Next, and then click Finish.



Master DNS Servers

The stub zone is loaded from one or more master servers.

Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.

Master Servers:

IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
✓ 10.10.10.40	MEL-DC	OK

☐ Use the above servers to create a local list of master servers

FIGURE 1-27 Configure the stub zone master servers

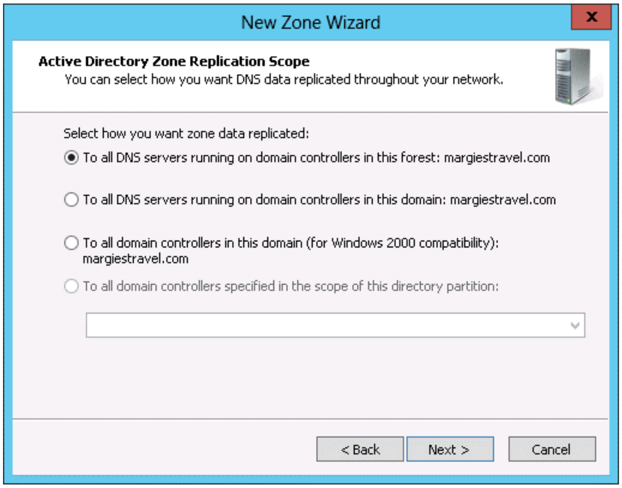
8. On MEL-DC, ensure that you are signed in as MARGIESTRAVEL\Administrator with the password Pa$$w0rd.
9. Open the DNS Manager console from the Tools menu in the Server Manager console.

10. In the DNS Manager console, right-click Forward Lookup Zones and click New Zone.

11. On the Welcome to the New Zone Wizard page, click Next.

12. On the Zone Type page, click Stub Zone and ensure that the Store the Zone in Active Directory check box is selected. Click Next.

13. On the Active Directory Zone Replication Scope page, click To All DNS Servers Running on Domain Controllers in This Forest: margiestravel.com as shown in Figure 1-28. Click Next.



New Zone Wizard

Active Directory Zone Replication Scope
You can select how you want DNS data replicated throughout your network.

Select how you want zone data replicated:

● To all DNS servers running on domain controllers in this forest: margiestravel.com

○ To all DNS servers running on domain controllers in this domain: margiestravel.com

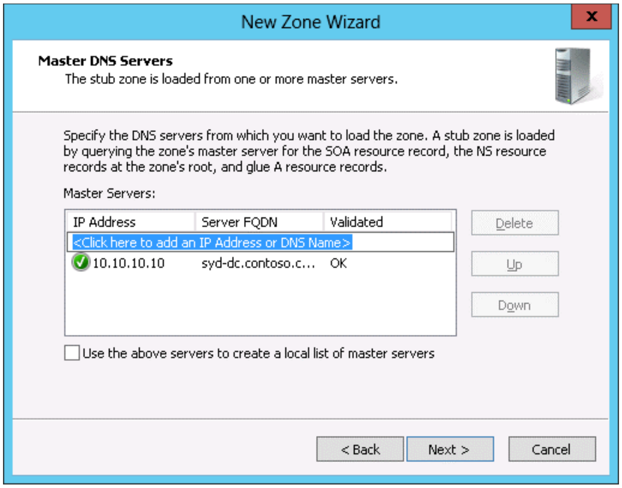
○ To all domain controllers in this domain (for Windows 2000 compatibility): margiestravel.com

○ To all domain controllers specified in the scope of this directory partition:

FIGURE 1-28 Configure the zone replication scope

14. On the Zone Name page, enter the name contoso.com in the Zone Name text box and click Next.

15. On the Master DNS Servers page, enter the IP address 10.10.10.10 in the Master Servers list as shown in Figure 1-29, click Next, and click Finish.



New Zone Wizard

Master DNS Servers

The stub zone is loaded from one or more master servers.

Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.

Master Servers:

IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
✓ 10.10.10.10	syd-dc.contoso.c...	OK

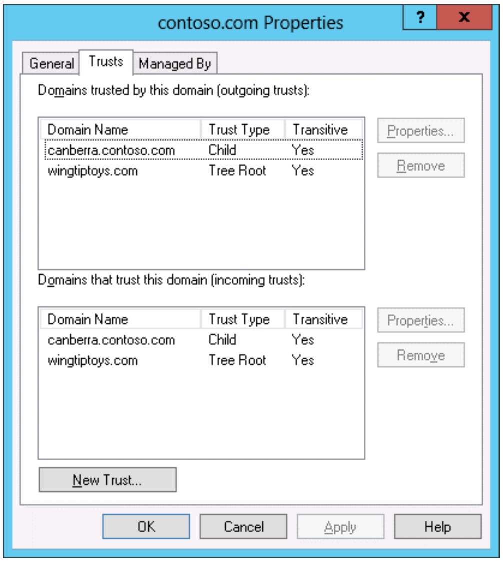
☐ Use the above servers to create a local list of master servers

FIGURE 1-29 Configure the master DNS servers

Exercise 8: Begin creating a forest trust relationship

In this exercise, you configure the contoso.com side of a forest trust relationship between the contoso.com and margiestravel.com forests. To complete this exercise, perform the following steps:

1. On the Tools menu of the Server Manager console on SYD-DC, click Active Directory Domains and Trusts.
2. In the Active Directory Domains and Trusts console, right-click contoso.com and click Properties.
3. On the Trusts tab of the contoso.com Properties dialog box, shown in Figure 1-30, click New Trust.



Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
canberra.contoso.com	Child	Yes
wingtiptoys.com	Tree Root	Yes

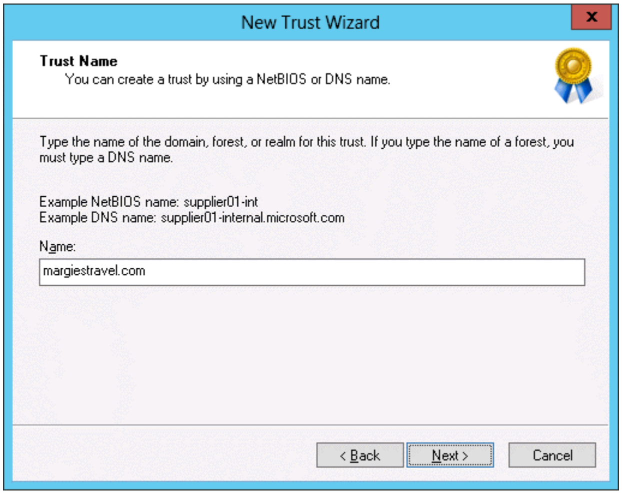
Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
canberra.contoso.com	Child	Yes
wingtiptoys.com	Tree Root	Yes

FIGURE 1-30 Create the new trust

4. On the Welcome to the New Trust Wizard page, click Next.

5. On the Trust Name page, type margiestravel.com as shown in Figure 1-31, and click Next.



Trust Name

You can create a trust by using a NetBIOS or DNS name.

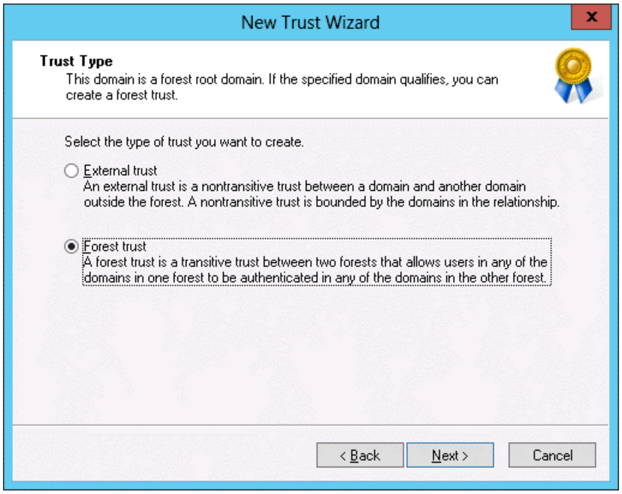
Type the name of the domain, forest, or realm for this trust. If you type the name of a forest, you must type a DNS name.

Example NetBIOS name: supplier01-int
Example DNS name: supplier01-internal.microsoft.com

Name:
margiestravel.com

FIGURE 1-31 Set the trust name

6. On the Trust Type page, click Forest Trust as shown in Figure 1-32 and click Next.


New Trust Wizard

Trust Type

This domain is a forest root domain. If the specified domain qualifies, you can create a forest trust.

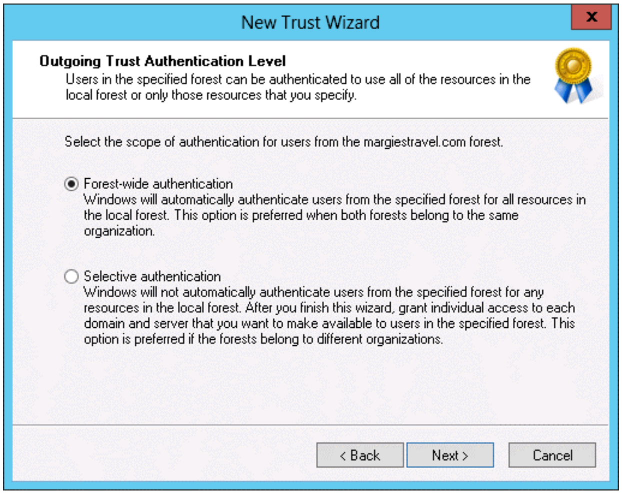
Select the type of trust you want to create.

○ External trust
An external trust is a nontransitive trust between a domain and another domain outside the forest. A nontransitive trust is bounded by the domains in the relationship.

● Forest trust
A forest trust is a transitive trust between two forests that allows users in any of the domains in one forest to be authenticated in any of the domains in the other forest.

FIGURE 1-32 Configure the trust type

7. On the Direction Of Trust page, click Two-Way and click Next.
8. On the Sides Of Trust page, click This Domain Only and then click Next.
9. On the Outgoing Trust Authentication Level page, click Forest-Wide Authentication as shown in Figure 1-33 and click Next.


New Trust Wizard

Outgoing Trust Authentication Level

Users in the specified forest can be authenticated to use all of the resources in the local forest or only those resources that you specify.

Select the scope of authentication for users from the margiestravel.com forest.

● Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.

○ Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you finish this wizard, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.

FIGURE 1-33 Configure the trust authentication level

10. On the Trust Password page, type Pa$$w0rd in the Trust Password and Confirm Trust Password text boxes. Click Next three times.

11. On the Confirm Outgoing Trust page, click No, Do Not Confirm the Outgoing Trust and click Next.

12. On the Confirm Incoming Trust page, click No, Do Not Confirm the Incoming Trust, click Next, and click Finish.

Exercise 9: Complete the creation of the forest trust relationship between contoso.com and margiestravel.com

In this exercise, you configure the margiestravel.com side of a forest trust relationship between the contoso.com and margiestravel.com forests. To complete this exercise, perform the following steps:

1. In the Tools menu of the Server Manager console on MEL-DC, click Active Directory Domains and Trusts.

2. In the Active Directory Domains and Trusts console, right-click Margiestravel.com and click Properties.

3. On the Trusts tab of the margiestravel.com Properties dialog box, shown in Figure 1-34, click New Trust.

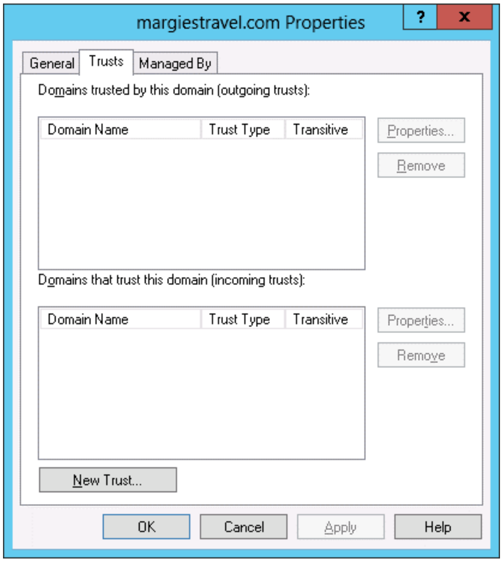


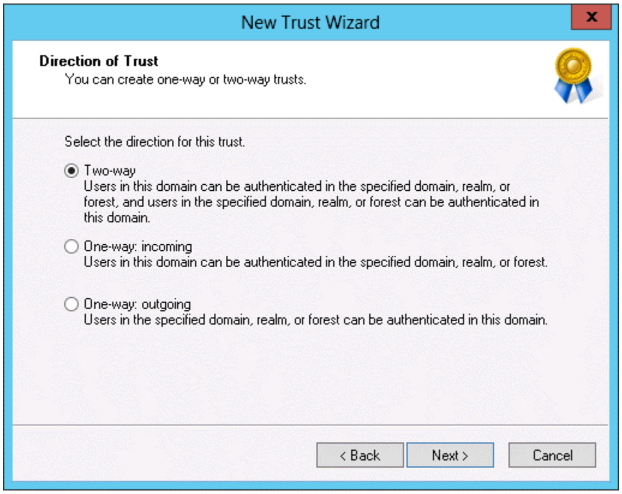
FIGURE 1-34 View the current trusts

4. On the Welcome to the New Trust Wizard page, click Next.

5. On the Trust Name page of the New Trust Wizard, type contoso.com in the Name text box and click Next.

6. On the Trust Type page, click Forest Trust and click Next.

7. On the Direction of Trust page, click Two-way as shown in Figure 1-35 and click Next.



Direction of Trust
You can create one-way or two-way trusts.

Select the direction for this trust.

● Two-way
Users in this domain can be authenticated in the specified domain, realm, or forest, and users in the specified domain, realm, or forest can be authenticated in this domain.

○ One-way: incoming
Users in this domain can be authenticated in the specified domain, realm, or forest.

○ One-way: outgoing
Users in the specified domain, realm, or forest can be authenticated in this domain.

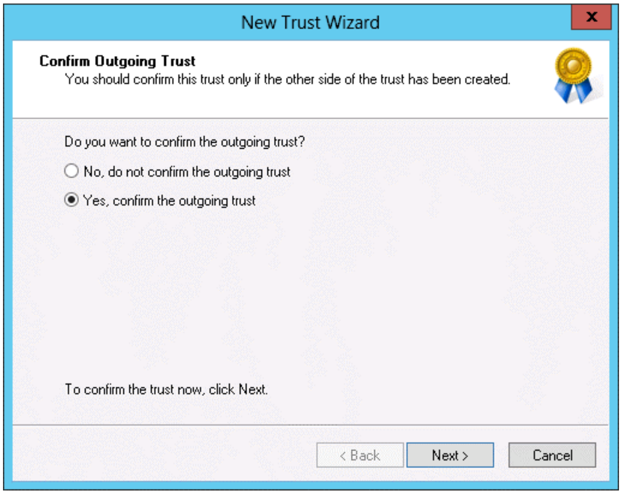
FIGURE 1-35 Configure the direction of the trust

8. On the Sides of Trust page, click This Domain Only and click Next.

9. On the Outgoing Trust Authentication Level page, click Forest-Wide Authentication and click Next.

10. On the Trust Password page, enter Pa$$w0rd in the Trust Password and Confirm Trust Password text boxes. Click Next three times.

11. On the Confirm Outgoing Trust page, click Yes, Confirm the Outgoing Trust as shown in Figure 1-36, and click Next.



Confirm Outgoing Trust
You should confirm this trust only if the other side of the trust has been created.

Do you want to confirm the outgoing trust?

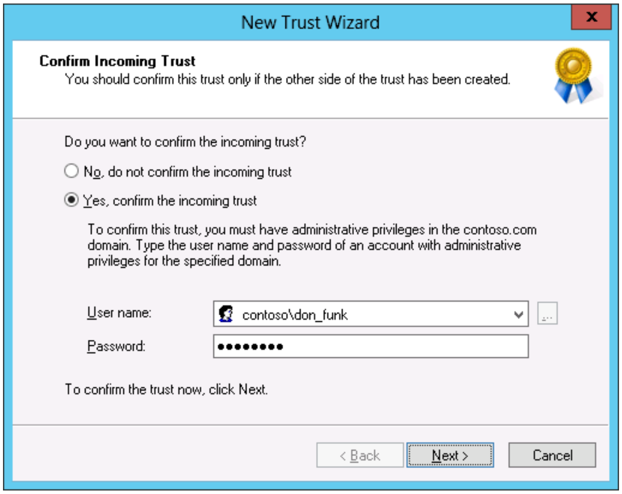
○ No, do not confirm the outgoing trust

● Yes, confirm the outgoing trust

To confirm the trust now, click Next.

FIGURE 1-36 Confirm the outgoing trust

12. On the Confirm Incoming Trust page, click Yes, Confirm the Incoming Trust. In the User Name text box, type contoso\don_funk and in the Password text box type Pa$$w0rd as shown in Figure 1-37. Click Next.



New Trust Wizard

Confirm Incoming Trust
You should confirm this trust only if the other side of the trust has been created.

Do you want to confirm the incoming trust?

○ No, do not confirm the incoming trust

● Yes, confirm the incoming trust

To confirm this trust, you must have administrative privileges in the contoso.com domain. Type the user name and password of an account with administrative privileges for the specified domain.

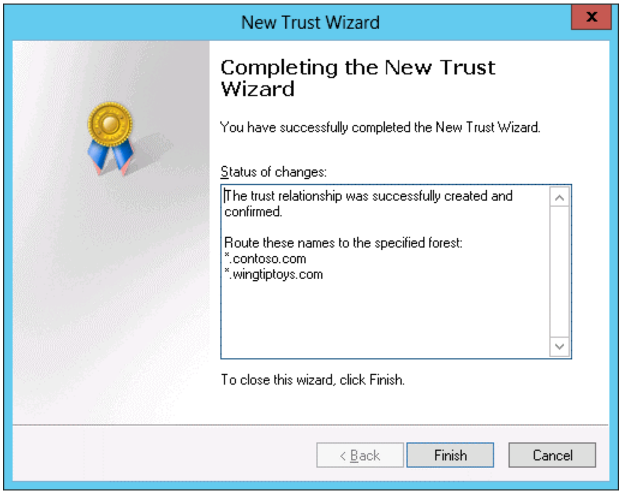
User name: contoso\don_funk

Password: ••••••••

To confirm the trust now, click Next.

FIGURE 1-37 Confirm the incoming trust

13. On the Completing the New Trust Wizard page verify that the trust is successfully created as shown in Figure 1-38 and click Finish. Click OK to close the margiestravel.com properties dialog box.



New Trust Wizard

Completing the New Trust Wizard

You have successfully completed the New Trust Wizard.

Status of changes:

The trust relationship was successfully created and confirmed.

Route these names to the specified forest:
*.contoso.com
*.wingtiptoys.com

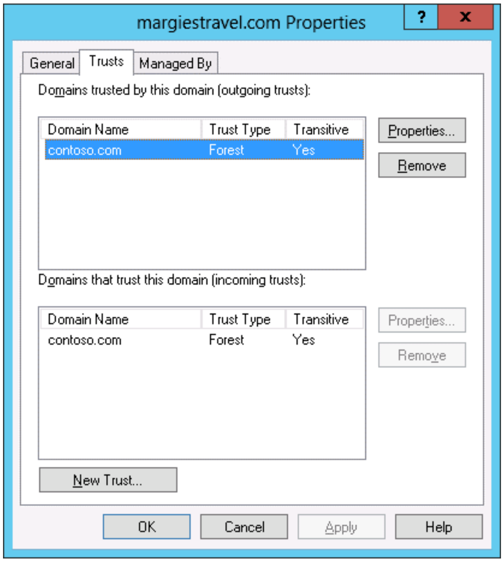
To close this wizard, click Finish.

FIGURE 1-38 Confirm the trust creation

Exercise 10: Configure name suffix routing

In this exercise, you configure the forest trust between the margiestravel.com forest and the contoso.com forest so that name suffix routing is supported for the wingtiptoys.com domain tree. To complete this exercise, perform the following steps:

1. In the Active Directory Domains and Trusts console on MEL-DC, right-click margiestravel.com and click Properties.
2. On the Trusts tab of the margiestravel.com Properties dialog box click contoso.com in the Domains Trusted by This Domain (Outgoing Trusts) area, as shown in Figure 1-39, and then click Properties.



Domains trusted by this domain (outgoing trusts):

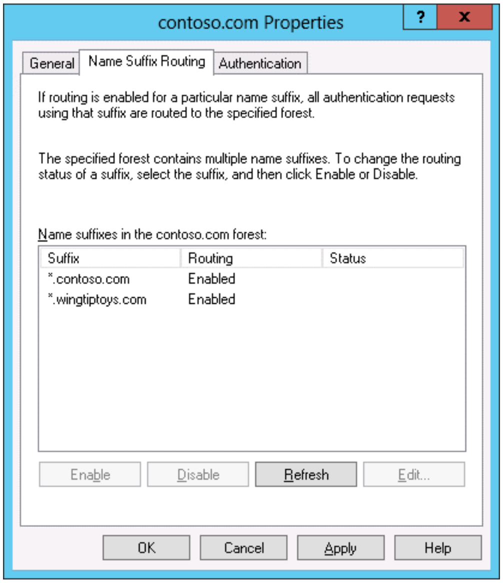
Domain Name	Trust Type	Transitive
contoso.com	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
contoso.com	Forest	Yes

FIGURE 1-39 Editing the properties of trusts

3. On the Name Suffix Routing tab of the contoso.com Properties dialog box, click *.wingtiptoys.com and then click Enable as shown in Figure 1-40.



If routing is enabled for a particular name suffix, all authentication requests using that suffix are routed to the specified forest.

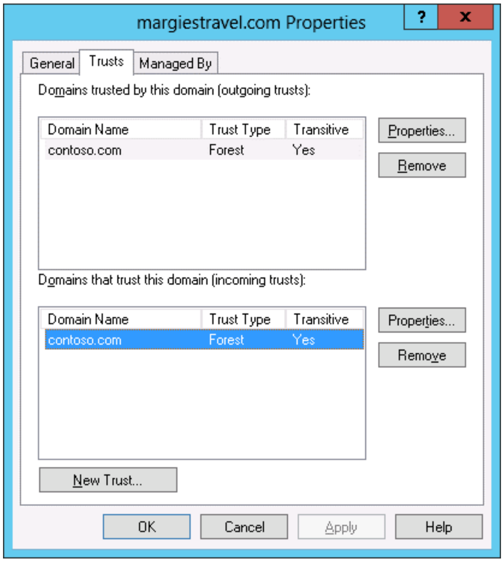
The specified forest contains multiple name suffixes. To change the routing status of a suffix, select the suffix, and then click Enable or Disable.

Name suffixes in the contoso.com forest:

Suffix	Routing	Status
*.contoso.com	Enabled	
*.wingtiptoys.com	Enabled	

FIGURE 1-40 Configure name suffix routing

4. On the General tab of the contoso.com Properties dialog box, click Validate.
5. On the Active Directory Domain Services dialog box, click Yes, Validate the Incoming Trust by entering the user name contoso\don_funk and the password Pa$$w0rd, and click OK.
6. Click OK on the Active Directory Domain Services dialog box and then click Yes on the second Active Directory Domain Services dialog box.
7. Click OK to close the contoso.com Properties dialog box.
8. Click contoso.com on the list of Domains That Trust This Domain (Incoming Trusts) dialog box as shown in Figure 1-41 and then click Properties.



Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
contoso.com	Forest	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
contoso.com	Forest	Yes

FIGURE 1-41 Trusts for the margiestravel.com domain

9. On the Name Suffix Routing tab of the contoso.com Properties dialog box verify that both *.contoso.com and *.wingtiptoys.com are enabled and then click OK.

10. Click OK to close the margiestravel.com Properties dialog box.

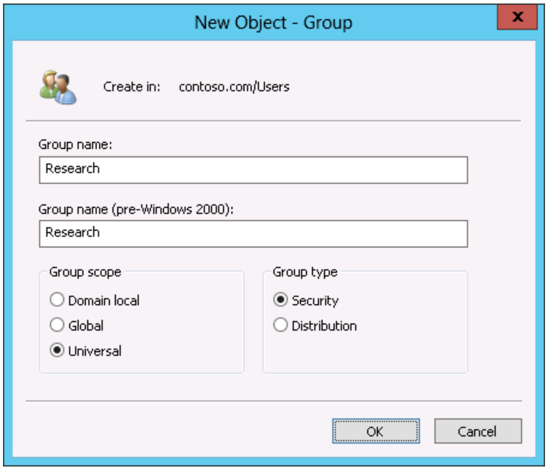
Exercise 11: Configure selective authentication

In this exercise, you configure selective authentication. You configure the trust to use selective authentication, create a user group in one forest, and create a computer account in the other forest. You then configure the computer account so that members of the user group in the trusted forest can authenticate when connecting to that computer. To complete this exercise, perform the following steps:

1. When signed on to SYD-DC as contoso\don_funk, click Active Directory Users and Computers on the Tools menu of the Server Manager console.

2. In Active Directory Users and Computers, right-click the Users container, click New, and click Group.

3. On the New Object – Group dialog box, enter the group name as Research, set the group scope to Universal as shown in Figure 1-42, and click OK.



Create in: contoso.com/Users

Group name: Research

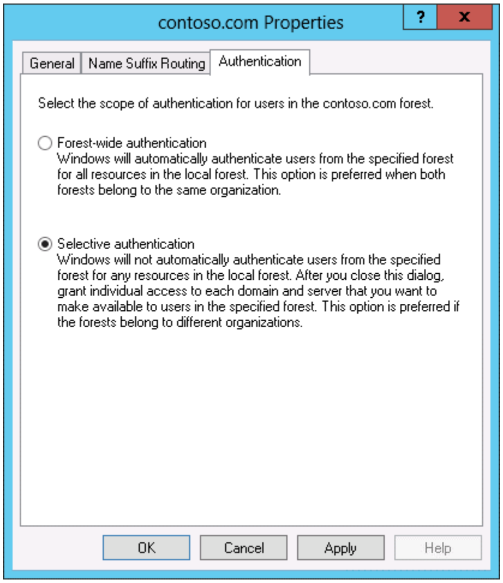
Group name (pre-Windows 2000): Research

Group scope
○ Domain local
○ Global
● Universal

Group type
● Security
○ Distribution

FIGURE 1-42 Create a new universal group

4. On MEL-DC, right-click margiestravel.com in the Active Directory Domains and Trust console and click Properties.
5. On the Trusts tab of the margiestravel.com Properties dialog box, click contoso.com in the Domains That Trust This Domain (Incoming Trusts) list and click Properties.
6. On the Authentication tab of the contoso.com Properties dialog box, click Selective Authentication as shown in Figure 1-43.



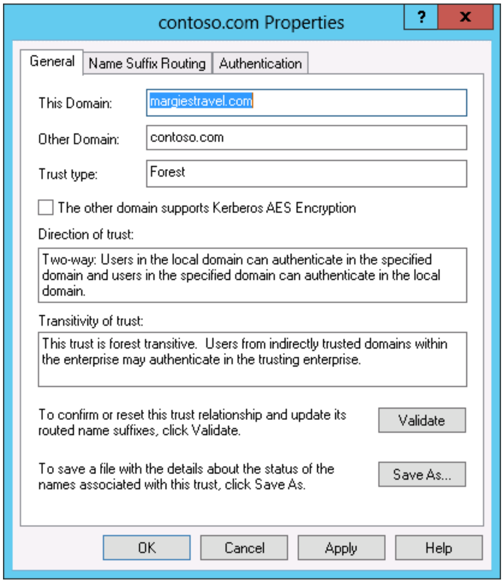
Select the scope of authentication for users in the contoso.com forest.

○ Forest-wide authentication
Windows will automatically authenticate users from the specified forest for all resources in the local forest. This option is preferred when both forests belong to the same organization.

● Selective authentication
Windows will not automatically authenticate users from the specified forest for any resources in the local forest. After you close this dialog, grant individual access to each domain and server that you want to make available to users in the specified forest. This option is preferred if the forests belong to different organizations.

FIGURE 1-43 Configure selective authentication

7. On the General tab of the contoso.com Properties dialog box, shown in Figure 1-44, click Validate.



This Domain: margiestravel.com

Other Domain: contoso.com

Trust type: Forest

□ The other domain supports Kerberos AES Encryption

Direction of trust:

Two-way: Users in the local domain can authenticate in the specified domain and users in the specified domain can authenticate in the local domain.

Transitivity of trust:

This trust is forest transitive. Users from indirectly trusted domains within the enterprise may authenticate in the trusting enterprise.

To confirm or reset this trust relationship and update its routed name suffixes, click Validate.

To save a file with the details about the status of the names associated with this trust, click Save As.

FIGURE 1-44 Validate authentication

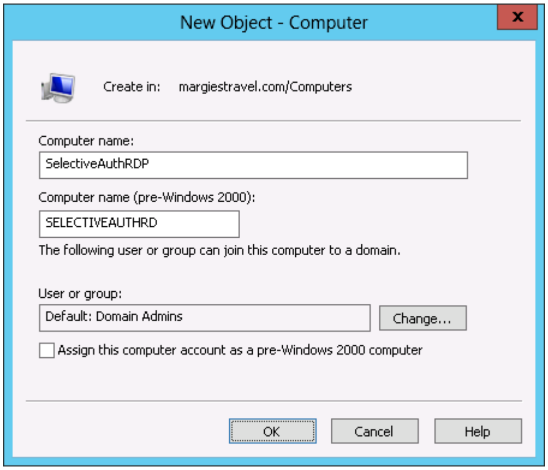
8. On the Active Directory Domain Services dialog box, click Yes, validate the incoming trust. Enter the user name as contoso\don_funk, enter the password as Pa$$w0rd, and then click OK twice.

9. Click Yes on the Active Directory Domain Services dialog box and then click OK twice to close the contoso.com Properties and margiestravel.com Properties dialog boxes.

10. Click Active Directory Users and Computers in the Tools menu of the Server Manager console.

11. Right-click the Computers node and click New and then click Computer.

12. In the New Object – Computer dialog box, enter the name SelectiveAuthRDP as shown in Figure 1-45 and click OK.



Create in: margiestravel.com/Computers

Computer name:
SelectiveAuthRDP

Computer name (pre-Windows 2000):
SELECTIVEAUTHRD

The following user or group can join this computer to a domain.

User or group:
Default: Domain Admins

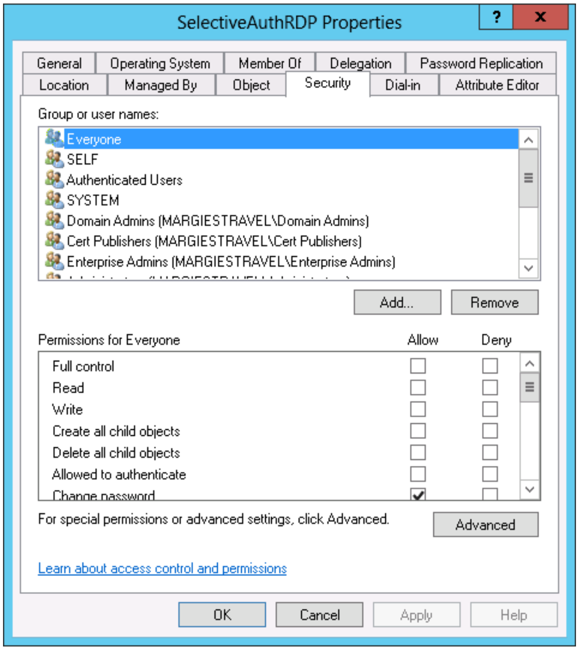
□ Assign this computer account as a pre-Windows 2000 computer

FIGURE 1-45 Create new computer object

13. Enabled Advanced Features on the View menu of the Active Directory Users and Computers console.

14. Right-click the SelectiveAuthRDP computer object and click Properties.

15. On the Security tab of the SelectiveAuthRDP Properties dialog box, shown in Figure 1-46, click Add.



Group or user names:

- Everyone
- SELF
- Authenticated Users
- SYSTEM
- Domain Admins (MARGIESTRAVEL\Domain Admins)
- Cert Publishers (MARGIESTRAVEL\Cert Publishers)
- Enterprise Admins (MARGIESTRAVEL\Enterprise Admins)

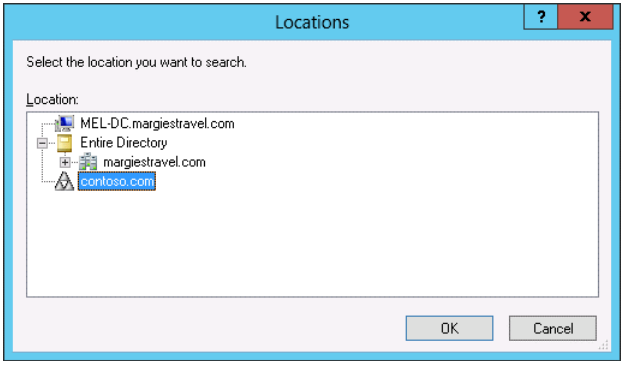
Permissions for Everyone	Allow	Deny
Full control	□	□
Read	□	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	□	□
Change password	☑	□

For special permissions or advanced settings, click Advanced.

FIGURE 1-46 Add a user

16. On the Select Users, Computers, Service Accounts, or Groups dialog box, click Locations.

17. On the Locations dialog box, click contoso.com as shown in Figure 1-47 and then click OK.



Select the location you want to search.

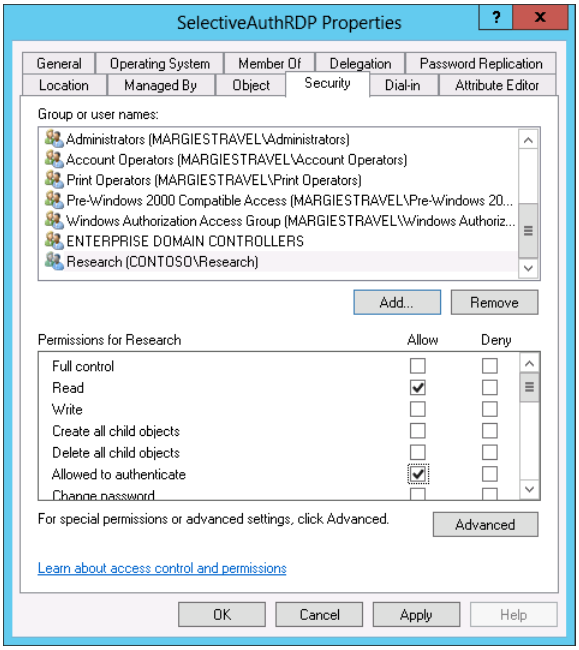
Location:

- MEL-DC.margiestravel.com
- Entire Directory
  - margiestravel.com
  - contoso.com

FIGURE 1-47 The Locations dialog box

18. In the Select Users, Computers, Service Accounts, or Groups dialog box, type Research, click Check Names, and click OK.

19. On the SelectiveAuthRDP Properties dialog box, click Research (Contoso\Research) and click Allowed to Authenticate (Allow) as shown in Figure 1-48. Click OK.



Group or user names:

- Administrators (MARGIESTRAVEL\Administrators)
- Account Operators (MARGIESTRAVEL\Account Operators)
- Print Operators (MARGIESTRAVEL\Print Operators)
- Pre-Windows 2000 Compatible Access (MARGIESTRAVEL\Pre-Windows 20...
- Windows Authorization Access Group (MARGIESTRAVEL\Windows Authoriz...
- ENTERPRISE DOMAIN CONTROLLERS
- Research (CONTOSO\Research)

Permissions for Research	Allow	Deny
Full control	□	□
Read	☑	□
Write	□	□
Create all child objects	□	□
Delete all child objects	□	□
Allowed to authenticate	☑	□
Change password	□	□

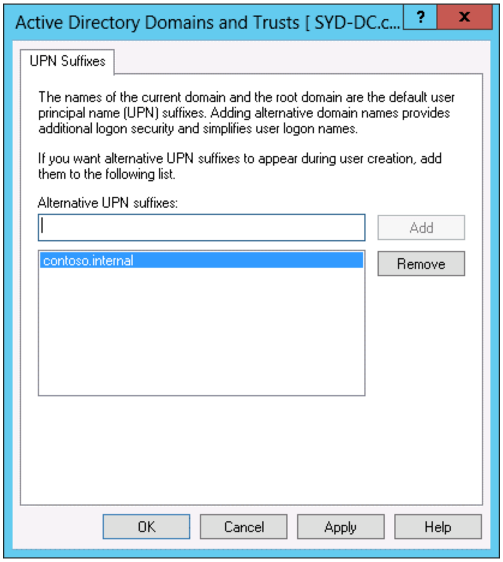
For special permissions or advanced settings, click Advanced.

FIGURE 1-48 Configure Allowed to Authenticate permission

Exercise 12: Configure additional UPN suffixes

In this exercise, you configure additional UPN suffixes. To complete this exercise, perform the following steps:

1. When signed on to SYD-DC as contoso\don_funk, switch to the Active Directory Domains and Trusts console.
2. In the Active Directory Domains and Trusts console, right-click Active Directory Domains and Trusts and click Properties.
3. On the UPN Suffixes tab of the Active Directory Domains and Trusts dialog box, type contoso.internal in the Alternative UPN suffixes dialog box and then click Add as shown in Figure 1-49. Click OK.



Active Directory Domains and Trusts [SYD-DC.c...

UPN Suffixes

The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

contoso.internal

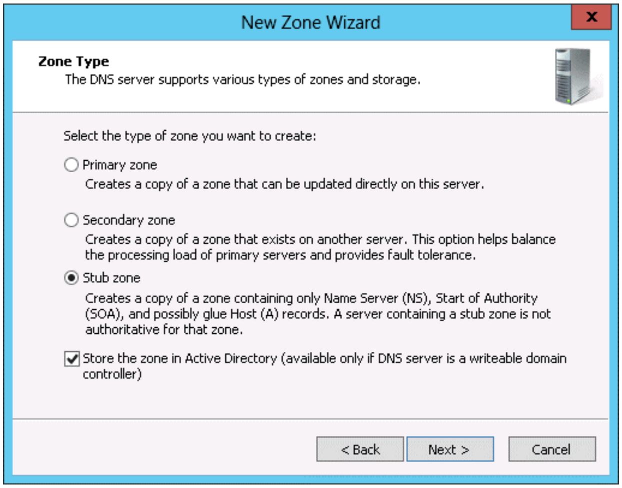
FIGURE 1-49 Configure a UPN suffix

Exercise 13: Configure a shortcut trust

In this exercise, you configure a shortcut trust between the canberra.contoso.com domain and the wingtiptoys.com domain. To complete this exercise, perform the following steps:

1. Sign on to CBR-DC as canberra\administrator.
2. In the Server Manager console, click the Tools menu and then click DNS.
3. In the DNS Manager console, expand CBR-DC, right-click Forward Lookup Zones, and click New Zone.
4. On the Welcome to the New Zone Wizard page, click Next.

5. On the Zone Type page of the New Zone Wizard, click Stub Zone and ensure that Store the Zone in Active Directory (available only if the DNS server is a writable domain controller) is selected as shown in Figure 1-50 and click Next twice.



New Zone Wizard

Zone Type
The DNS server supports various types of zones and storage.

Select the type of zone you want to create:

○ Primary zone
Creates a copy of a zone that can be updated directly on this server.

○ Secondary zone
Creates a copy of a zone that exists on another server. This option helps balance the processing load of primary servers and provides fault tolerance.

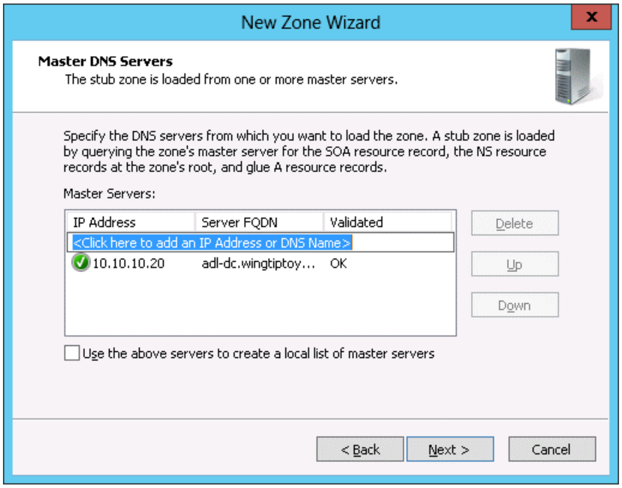
● Stub zone
Creates a copy of a zone containing only Name Server (NS), Start of Authority (SOA), and possibly glue Host (A) records. A server containing a stub zone is not authoritative for that zone.

☑ Store the zone in Active Directory (available only if DNS server is a writeable domain controller)

FIGURE 1-50 Create a stub zone

6. On the Zone name page, type wingtiptoys.com and click Next.

7. On the Master DNS Servers page, type 10.10.10.20 in the list of master DNS servers and press Enter as shown in Figure 1-51. Click Next and then click Finish.



New Zone Wizard

Master DNS Servers
The stub zone is loaded from one or more master servers.

Specify the DNS servers from which you want to load the zone. A stub zone is loaded by querying the zone's master server for the SOA resource record, the NS resource records at the zone's root, and glue A resource records.

Master Servers:

IP Address	Server FQDN	Validated
<Click here to add an IP Address or DNS Name>		
✓ 10.10.10.20	adl-dc.wingtiptoy...	OK

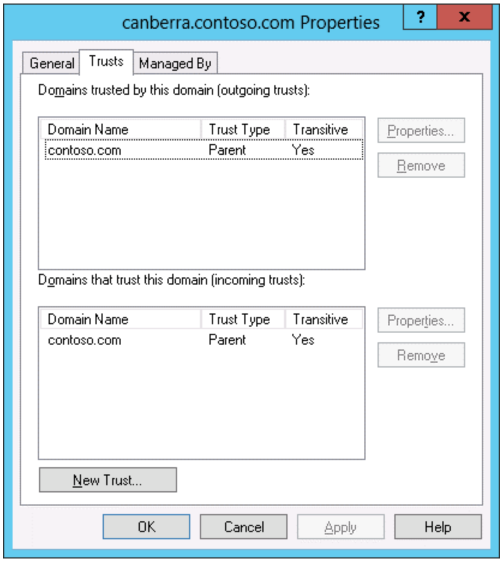
□ Use the above servers to create a local list of master servers

FIGURE 1-51 Configure a master DNS server

8. In the Server Manager console, click the Tools menu and then click Active Directory Domains and Trusts.

9. In the Active Directory Domains and Trusts console, expand the contoso.com node, right-click canberra.contoso.com, and click Properties.

10. On the Trusts tab of the canberra.contoso.com Properties dialog box, show in Figure 1-52, click New Trust.



Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
contoso.com	Parent	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
contoso.com	Parent	Yes

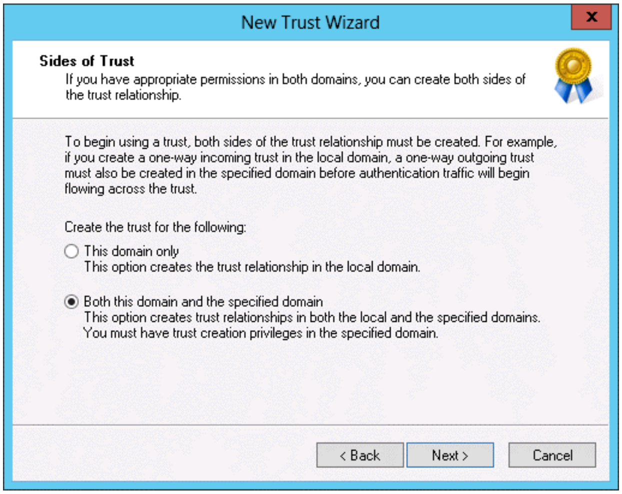
FIGURE 1-52 Create a new trust

11. On the Welcome to the New Trust Wizard page, click Next.

12. On the Trust Name page of the New Trust Wizard, type wingtiptoys.com and click Next.

13. On the Direction of Trust page, click Two-Way and click Next.

14. On the Sides of Trust page, click Both This Domain and the Specified Domain as shown in Figure 1-53 and click Next.



Sides of Trust

If you have appropriate permissions in both domains, you can create both sides of the trust relationship.

To begin using a trust, both sides of the trust relationship must be created. For example, if you create a one-way incoming trust in the local domain, a one-way outgoing trust must also be created in the specified domain before authentication traffic will begin flowing across the trust.

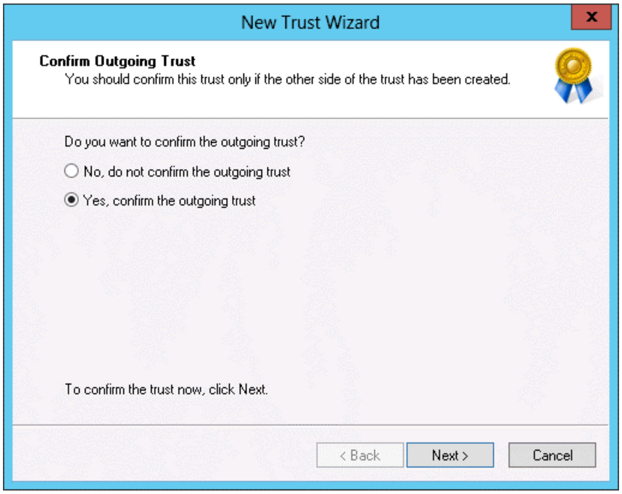
Create the trust for the following:

○ This domain only
This option creates the trust relationship in the local domain.

● Both this domain and the specified domain
This option creates trust relationships in both the local and the specified domains. You must have trust creation privileges in the specified domain.

FIGURE 1-53 Configure trust sides

15. On the User Name and Password page, type wingtiptoys\administrator in the user name text box, type Pa$$w0rd in the password text box, and click Next three times.
16. On the Confirm Outgoing Trust page, click Yes, Confirm the Outgoing Trust as shown in Figure 1-54, and click Next.



Confirm Outgoing Trust

You should confirm this trust only if the other side of the trust has been created.

Do you want to confirm the outgoing trust?

○ No, do not confirm the outgoing trust

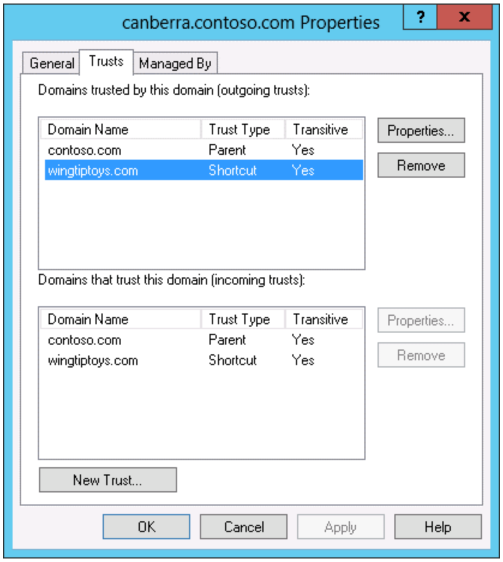
● Yes, confirm the outgoing trust

To confirm the trust now, click Next.

FIGURE 1-54 Confirm the trust

17. On the Confirm Incoming Trust page, click Yes, Confirm the Incoming Trust and click Next.
18. Verify that the trust relationship was successfully created and click Finish.

19. Verify that the wingtiptoys.com trust is listed as a shortcut trust as shown in Figure 1-55 and then click OK.



Domains trusted by this domain (outgoing trusts):

Domain Name	Trust Type	Transitive
contoso.com	Parent	Yes
wingtiptoys.com	Shortcut	Yes

Domains that trust this domain (incoming trusts):

Domain Name	Trust Type	Transitive
contoso.com	Parent	Yes
wingtiptoys.com	Shortcut	Yes

FIGURE 1-55 Verify the trust type

Suggested practice exercises

The following additional practice exercises are designed to give you more opportunities to practice what you've learned and to help you successfully master the lessons presented in this chapter.

- **Exercise 1:** Configure additional UPN suffixes for the margiestravel.com forest.
- **Exercise 2:** Use netdom.exe to disable and then re-enable SID filtering on the margiestravel.com forest.

Answers

This section contains the answers to the lesson review questions in this chapter.

Lesson 1

1. **Correct Answer:** C
   - **A. Incorrect:** This structure does not support the two different departments that have mutually exclusive Active Directory schema requirements. This structure supports only one Active Directory schema.
   - **B. Incorrect:** This structure does not support the two different departments that have mutually exclusive Active Directory schema requirements. This structure supports only one Active Directory schema.
   - **C. Correct:** This structure supports the two different departments that have mutually exclusive Active Directory schema requirements because each forest has a separate schema.
   - **D. Incorrect:** This structure does not support the two different departments that have mutually exclusive Active Directory schema requirements. This structure supports only one Active Directory schema.
2. **Correct Answer:** C
   - **A. Incorrect:** You need more than one domain to support the two separate domain names.
   - **B. Incorrect:** Implementing this solution requires the creation of additional trust relationships when compared to using a single forest with multiple domain trees.
   - **C. Correct:** You can accomplish this objective with a design that uses two domain trees, one for wingtiptoys.com and one for tailspintoys.com.
   - **D. Incorrect:** With a single domain tree, a child domain of the root domain needs to use a contiguous namespace. The requirements are that two domains with noncontiguous namespaces be available, which means at least two domain trees.
3. **Correct Answer:** A
   - **A. Correct:** You can add domain controllers running the Windows Server 2012 operating system to a domain running at the Windows Server 2003 functional level.
   - **B. Incorrect:** You can add domain controllers running the Windows Server 2012 operating system to a domain running at the Windows Server 2003 functional level.
   - **C. Incorrect:** You can add domain controllers running the Windows Server 2012 operating system to a domain running at the Windows Server 2003 functional level.
   - **D. Incorrect:** You can add domain controllers running the Windows Server 2012 operating system to a domain running at the Windows Server 2003 functional level.

4. **Correct Answers:** A and B
   - A. **Correct:** The Active Directory Recycle Bin is available at the Windows Server 2008 R2 and Windows Server 2012 forest functional levels.
   - B. **Correct:** The Active Directory Recycle Bin is available at the Windows Server 2008 R2 and Windows Server 2012 forest functional levels.
   - C. **Incorrect:** The Active Directory Recycle Bin is available at the Windows Server 2008 R2 and Windows Server 2012 forest functional levels.
   - D. **Incorrect:** The Active Directory Recycle Bin is available at the Windows Server 2008 R2 and Windows Server 2012 forest functional levels.

Lesson 2

1. **Correct Answer:** D
   - A. **Incorrect:** A forest trust is created between two forests when you want users in each forest to access resources in the counterpart forest. In this instance you need to create a shortcut trust between two domains in the same forest.
   - B. **Incorrect:** You configure an external trust between two domains in different forests, often when you don’t want to allow the trust to be transitive. In this instance you need to create a shortcut trust between two domains in the same forest.
   - C. **Incorrect:** You configure a realm trust between an Active Directory domain and a Kerberos V5 realm. In this instance you need to create a shortcut trust between two domains in the same forest.
   - D. **Correct:** In this instance you need to create a shortcut trust between two domains in the same forest.
2. **Correct Answer:** B
   - A. **Incorrect:** In this instance you need to create a shortcut trust between two domains in the same forest. You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.
   - B. **Correct:** You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.
   - C. **Incorrect:** A forest trust is created between two forests when you want users in each forest to access resources in the counterpart forest. You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.
   - D. **Incorrect:** You configure an external trust between two domains in different forests, often when you don’t want to allow the trust to be transitive. You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.

3. **Correct Answer:** B

   A. **Incorrect:** You configure an external trust between two domains in different forests, often when you don't want to allow the trust to be transitive.

   B. **Correct:** A forest trust is created between two forests when you want users in each forest to access resources in the counterpart forest.

   C. **Incorrect:** You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.

   D. **Incorrect:** In this instance you need to create a shortcut trust between two domains in the same forest.

4. **Correct Answer:** A

   A. **Correct:** You configure an external trust between two domains in different forests, often when you don't want to allow the trust to be transitive.

   B. **Incorrect:** You configure a realm trust between an Active Directory domain and a Kerberos V5 realm.

   C. **Incorrect:** In this instance you need to create a shortcut trust between two domains in the same forest.

   D. **Incorrect:** A forest trust is created between two forests when you want users in each forest to access resources in the counterpart forest.

Index

About the author

ORIN THOMAS is an MVP, an MCT and has a string of Microsoft MCSE and MCITP certifications. He has written more than 25 books for Microsoft Press and is a contributing editor at *Windows IT Pro* magazine. He has been working in IT since the early 1990's. He regularly speaks at events like TechED in Australia and around the world on Windows Server, Windows Client, System Center and security topics. Orin founded and runs the Melbourne System Center, Security, and Infrastructure Group. You can follow him on twitter at *http://twitter.com/orinthomas*.

Now that you’ve read the book...

Tell us what you think!

Was it useful?
Did it teach you what you wanted to learn?
Was there room for improvement?

Let us know at http://aka.ms/tellpress

Your feedback goes directly to the staff at Microsoft Press, and we read every one of your responses. Thanks in advance!

Microsoft