Microsoft®
Training &
Certification

Module 10: Creating and Managing Trees and Forests

Contents

Microsoft®

Overview

- Introduction to Trees and Forests
- Creating Trees and Forests
- Trust Relationships in Trees and Forests
- The Global Catalog
- Strategies for Using Groups in Trees and Forests
- Troubleshooting Creating and Managing Trees and Forests
- Best Practices

Creating a single domain in Active Directory® directory service is the one of the most efficient and easy ways to administer the Active Directory infrastructure. However, when implementing the Active Directory infrastructure, you may want to consider additional domains if your organization requires additional functionalities. Some examples of these additional functionalities are security settings, such as account and password Group Policy settings, which must be applied at the domain level so that distinct security settings apply to the users in each domain. Multiple domains also allow you to decentralize administration to retain complete administrative control of the domain controllers in their domain. Another benefit of multiple domains is that they enable you to reduce replication traffic so that the only data replicated between domains are the changes to the global catalog server, configuration information, and schema.

Depending on your requirements, you can create additional domains, called *child domains*, in the same domain tree. Alternatively, you can create a *forest*. A forest consists of multiple domain trees. All domains that have a common root domain are said to form a *contiguous namespace*. The domain trees in a forest do not form a contiguous namespace.

At the end of this module, you will be able to:

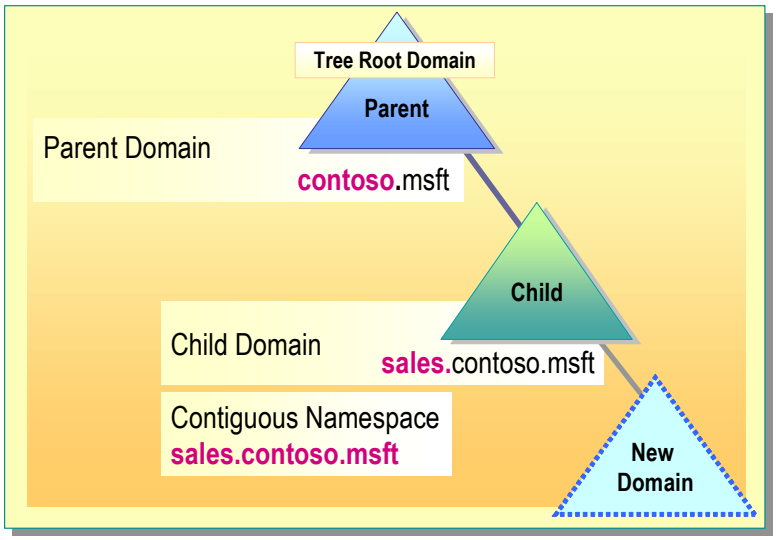
- Identify the purpose of trees and forests in Microsoft® Windows® 2000.
- Create and manage trees and forests in Windows 2000.
- Use trust relationships in trees and forests.
- Use the global catalog to log on to a Windows 2000 network.
- Implement the most effective group strategies to gain access to resources across trees and forests.
- Troubleshoot common problems that can occur when creating and managing trees and forests in Windows 2000.
- Apply best practices to creating and managing trees and forests in Active Directory.

Introduction to Trees and Forests

- What Is a Tree?
- What Is a Forest?
- What Is the Forest Root Domain?
- Characteristics of Multiple Domains

By using both domain trees and forests, you can use both contiguous and noncontiguous naming conventions. Trees and forests are useful for organizations with independent divisions that must each maintain its own Domain Name System (DNS) names.

What Is a Tree?

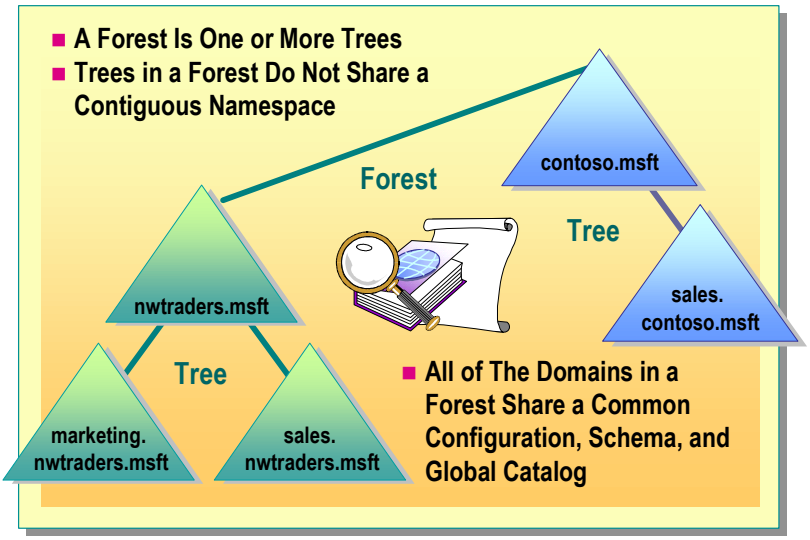


A *tree* is a hierarchical arrangement of Windows 2000 domains that share a *contiguous namespace*. A tree consists of one or more domains. A domain must exist in a tree.

When you add a new domain to a tree, the new domain is called a *child* domain. The name of the domain above the child domain is called a *parent* domain. The name of the child domain is a combination of the child domain name and the parent domain name separated by a period, to form its *DNS name*. This DNS name forms a contiguous namespace hierarchy. The top-level domain in a domain tree is sometimes called the *tree root domain*.

For example, a child domain named sales that has a parent domain named contoso.msft would form a fully qualified DNS domain name of sales.contoso.msft. Any new domain added to sales.contoso.msft becomes its child domain.

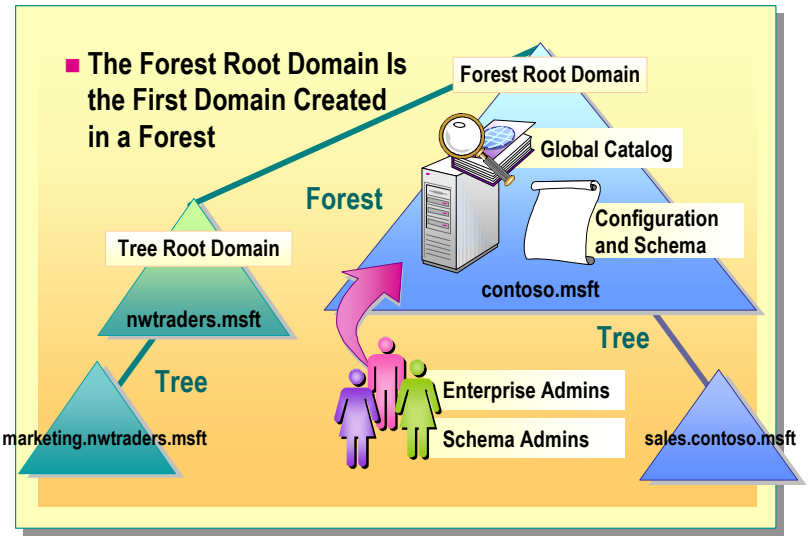
What Is a Forest?



A *forest* is a collection of one or more trees. Trees in a forest do not share a contiguous namespace. The domains in a forest share a common configuration, schema, and global catalog.

For example, Contoso, Ltd. creates a separate organization called Northwind Traders. Contoso, Ltd. decides to create a new Active Directory domain name for Northwind Traders, called nwtraders.msft. As shown in the slide, the two organizations do not share a common namespace; however, by adding the new Active Directory domain as a new tree in an existing forest, the two organizations are able to share resources and administrative functions.

What Is the Forest Root Domain?



The *forest root domain* is the first domain created in a forest. The name of the forest root domain is used to refer to a given forest. The top-level domain of each tree, which is the tree root domain, has a trust relationship to the forest root domain. Therefore, the name of the forest root domain must not change.

The first domain controller in the forest root domain is configured to store the global catalog information. The forest root domain also contains the configuration and schema information for the forest.

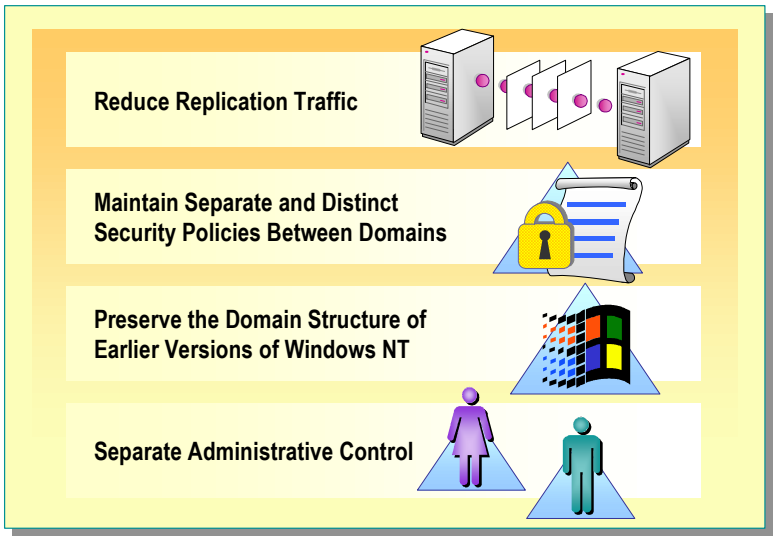
The forest root domain contains two predefined forest-wide groups, Enterprise Admins and Schema Admins. These groups exist only in the forest root domain of an Active Directory forest. You add users who perform administrative tasks for the entire forest to these groups. When a domain is switched to native mode from mixed mode, these two predefined global groups automatically change to universal groups. The roles of these groups are the same in mixed mode and native mode, only the group scope changes.

The following table describes these groups and the predefined roles they are given when the forest root domain is created.

Predefined group name	Description
Enterprise Admins	It is a universal group if the domain is in native mode, a global group if the domain is in mixed mode. The group is authorized to make changes to the entire forest in Active Directory, such as by adding child domains. By default, the only member of the group is the Administrator account for the forest root domain.
Schema Admins	It is a universal group if the domain is in native mode, a global group if the domain is in mixed mode. The group is authorized to make schema changes in Active Directory. By default, the only member of the group is the Administrator account for the forest root domain.

Note The members of the Domain Admins group in the forest root domain can modify the membership of the Enterprise Admins and Schema Admins groups.

Characteristics of Multiple Domains



Consider having multiple domains in your organization because you can use multiple domains in Windows 2000 to:

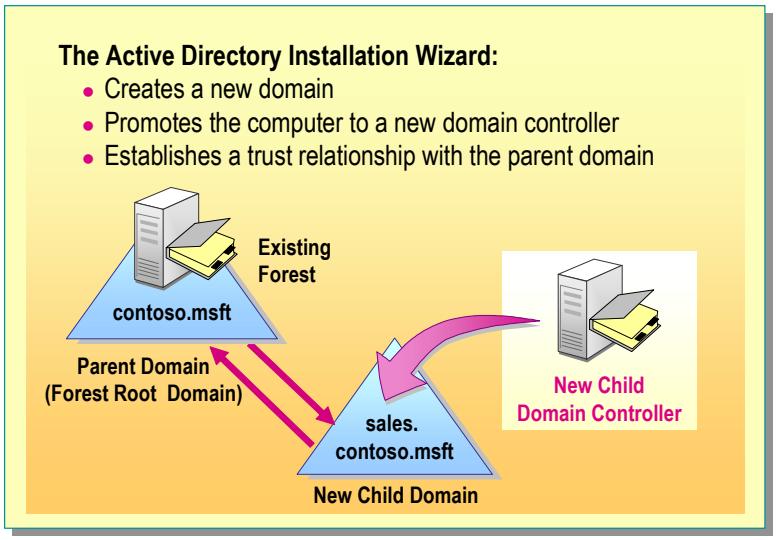
- Reduce replication traffic. Implementing multiple domains, instead of one large single domain, allows you to optimize replication traffic. In multiple domains, only the changes to the global catalog server, configuration information, and schema, are replicated. Not all objects and attributes to all domain controllers in the domain are replicated. For example, if the network uses a slow wide area network (WAN) link, the replication of all objects in the forest uses up unnecessary bandwidth because objects are being replicated to locations where they are rarely used. Creating a separate domain for different locations reduces replication traffic and maintains network performance because replication occurs only in the locations that need the objects.
- Maintain separate and distinct security settings for different domains. To be able to apply different domain-level security settings to group of users, you must have multiple domains. For example, you can use a separate domain for administrators and other users if you want to have a more strict password Group Policy, such as a shorter interval of password changes for administrators.
- Preserve the domain structure of earlier versions of Microsoft Windows NT®. To avoid or postpone restructuring your existing Windows NT domains, you can upgrade each domain to Windows 2000 while preserving the existing domain structure.
- Separate administrative control. The members of the domain administrators group in a domain have complete control over all objects in that domain. If you have a subdivision in your organization that does not allow administrators outside the subdivision control over their objects, place those objects in a separate domain. For example, for legal reasons, it might not be prudent for a subdivision of an organization that works on highly sensitive projects to accept domain supervision from a higher-level Information Technology (IT) group.

Creating Trees and Forests

- Creating a New Child Domain
- Creating a New Tree
- Creating a New Forest

After you have installed Active Directory and created a single domain, you can use the Active Directory Installation wizard, Dcpromo.exe, to guide you through the process of adding additional domains by creating trees and forests. The information that you must provide when you install Active Directory depends on whether you are creating a child domain in an existing forest or creating a new tree in an existing forest.

Creating a New Child Domain



After you establish the root domain, you can create additional domains within the tree if your network plan requires multiple domains. You must be a member of the Enterprise Admins group to create a child domain.

Each new domain within the tree will be a child domain of the root domain, or a child domain of another child domain.

For example, you create a domain named sales.contoso.msft, which is a child domain of the root domain, contoso.msft. The next domain that you create within that tree can be a child of constoso.msft or a child of sales.contoso.msft.

To create a child domain, perform the following steps:

1. In the **Run** box, type **dcpromo.exe** and then press ENTER.
2. In the Active Directory Installation wizard, complete the installation by using the information in the following table.

On this wizard page	Do this
Domain Controller Type	Click **Domain controller for a new domain**.
Create Tree or Child Domain	Click **Create a new child domain in an existing domain tree**.
Network Credentials	Specify the user name, password, and domain name of a user account in the Enterprise Admins group, which exists in the root domain of the forest.
Child Domain Installation	Specify the DNS name of the parent domain and the name of the new child domain.
Domain NetBIOS Name	Specify the NetBIOS name for the new domain.
Database and Log Locations	Specify locations for the Active Directory database and log files.

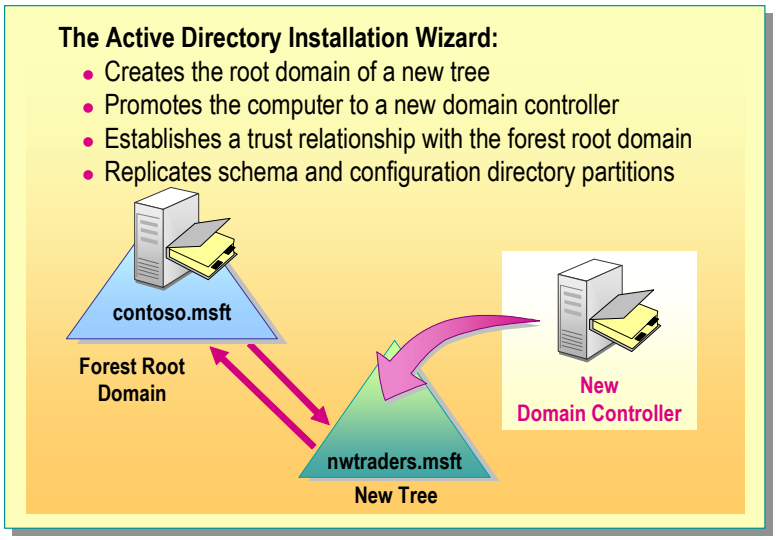
(*continued*)

On this wizard page	Do this
Shared System Volume	Specify the location for the shared system volume.
Permissions	Specify whether to set the default permissions on user and group objects to be compatible with computers running earlier versions of Windows, or only with Windows 2000–based servers. Enabling pre-Windows 2000 compatible permissions adds the Everyone group to the Pre-Windows 2000 Compatible Access group. This group has Read access to user and group object attributes that existed in Windows NT 4.0. You should select this option only after considering the impact that weaker permissions have on Active Directory security.
Directory Services Restore Mode Administrator Password	Specify a password to use when starting the computer in Directory Services Restore Mode.

After you specify the installation information, the Active Directory Installation wizard performs the following tasks:

- Creates a new domain.
- Promotes the computer in the new child domain to a domain controller.
- Establishes trust relationships between the child domain and the parent domain.

Creating a New Tree



After you establish the root domain, you can add a new tree to the existing forest if your network plan requires multiple trees.

To create a new tree in an existing forest, perform the following steps:

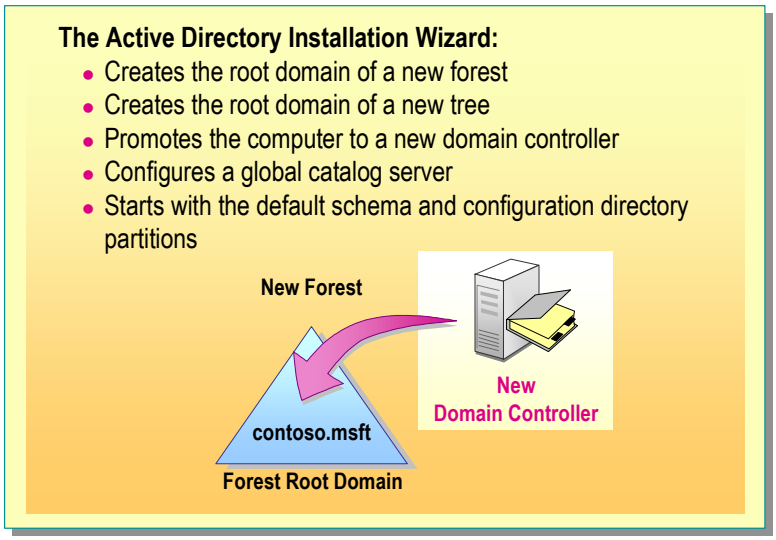
1. In the **Run** box, type **dcpromo.exe** and then press ENTER.
2. In the Active Directory Installation wizard, complete the installation by using the information in the following table.

On this wizard page	Do this
Domain Controller Type	Click **Domain controller for a new domain**.
Create Tree or Child Domain	Click **Create a new domain tree**.
Create or Join Forest	Click **Place this new domain tree in an existing forest**.
Network Credentials	Specify the user name, password, and domain name of a user account in the Enterprise Admins group, which exists in the root domain of the forest.
New Domain Tree	Specify the DNS name for the new tree.

The remaining options in the Active Directory Installation wizard are identical to the options used for creating the new child domain. After you finish specifying the installation information, the Active Directory Installation wizard performs the following steps:

- Creates the root domain of a new tree.
- Promotes the computer in the new tree to a domain controller.
- Establishes trust relationships to the forest root domain.
- Replicates schema and configuration directory partitions.

Creating a New Forest



When you create a new forest, the root domains of all domain trees in the forest establish transitive trust relationships with the forest root domain. You must be a member of the local administrators group to create a new forest.

To create a new forest, perform the following steps:

1. In the **Run** box, type **dcpromo.exe** and then press ENTER.
2. In the Active Directory Installation wizard, complete the installation by using the information in the following table.

On this wizard page	Do this
Domain Controller Type	Click **Domain controller for a new domain**.
Create Tree or **Child Domain**	Click **Create a new domain tree**.
Create or **Join Forest**	Click **Create a new forest of domain trees**.

The remaining options in the Active Directory Installation wizard are identical to the options used for creating a new tree.

After you finish specifying the installation information, the Active Directory Installation wizard performs the following steps:

- Creates the root of a new forest.
- Creates the root of a new tree.
- Promotes the computer in the new forest to a domain controller.
- Configures a global catalog server.
- Starts with the default schema and configuration directory partition information.

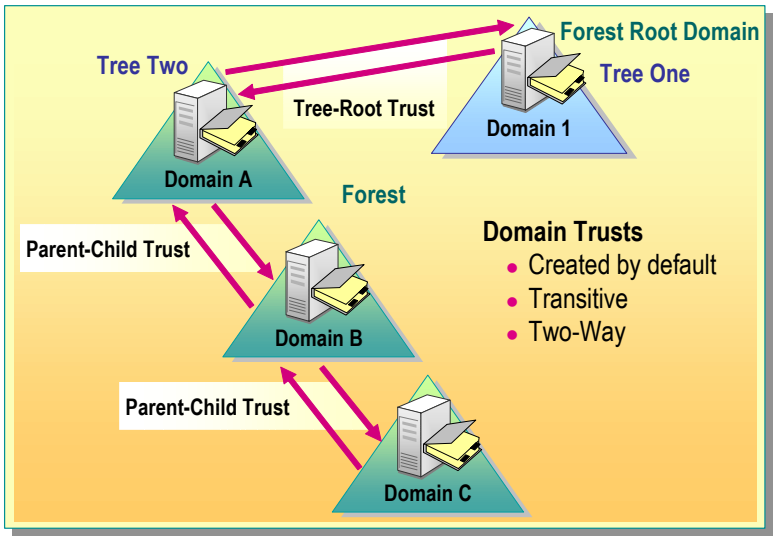
Trust Relationships in Trees and Forests

- Transitive Trusts in Windows 2000
- How Trusts Work
- How Kerberos V5 Works
- Shortcut Trusts in Windows 2000
- Nontransitive Trusts in Windows 2000
- Verifying and Revoking Trusts

Active Directory provides security across multiple domains through domain trust relationships based on the Kerberos version 5 protocol. A *domain trust* is a relationship established between domains that enables a domain controller in one domain to authenticate users in the other domain. The authentication requests follow a *trust path*.

A series of trust relationships for passing authentication requests between two domains defines a trust path. Trust paths are created automatically when you add domains to a Windows 2000 network. You can also manually create trusts when you want to share resources across domains that are not trusted or when you want to shorten the trust path.

Transitive Trusts in Windows 2000



Each time you create a new domain tree in a forest, a trust path is automatically created between the forest root domain and the new domain tree. The trust path allows trust relationships to flow through all domains in the forest. Authentication requests follow these trust paths, so accounts from any domain in the forest can be authenticated by any other domain in the forest. These trusts are sometimes called *default domain trusts*.

Types of Domain Trusts

The following are the two types of domain trusts in Windows 2000:

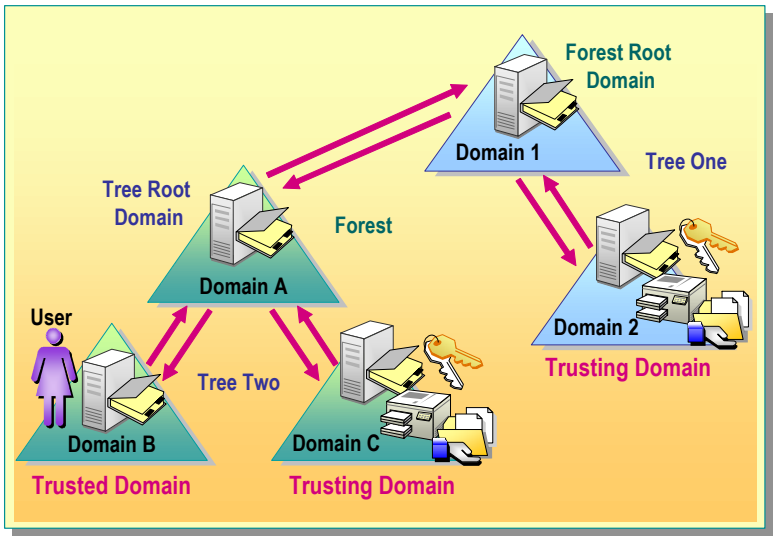
- *Transitive trust*. A transitive trust means that the trust relationship extended to one domain is automatically extended to all other domains that trust that domain. For example, domain A directly trusts domain B. Domain B directly trusts domain C. Because both trusts are transitive, domain A indirectly trusts domain C.
- *Two-way trust.* A two-way trust means that there are two trust paths going in both directions between two domains. For example, domain A trusts domain B in one direction, and domain B trusts domain A in the other direction.

Types of Transitive Trusts

The advantage of transitive trusts in Windows 2000 domains is that there is complete trust between all domains in an Active Directory forest. Because every child domain has a transitive trust relationship with its parent domain, and every tree root domain has a transitive trust relationship with the forest root domain, all domains in the forest trust each other. The following types of transitive trust relationships can be established with Windows 2000 domains:

- *Tree-root trust.* A tree-root trust relationship is the trust relationship that is established when you add a new tree to a forest. Installing Active Directory automatically creates a trust relationship between the domain that you are creating and the forest root domain that is also the new tree root domain. A tree-root trust relationship has the following restrictions:
  - It can be set up only between the roots of two trees in the same forest.
  - It must be a transitive and two-way trust.
- *Parent-child trust.* A parent-child trust relationship is established when you create a new domain in a tree. Installing Active Directory automatically creates within the namespace hierarchy a trust relationship between the new domain, which is the child domain, and the domain that immediately precedes it, which is the parent domain. The parent-child trust relationship has the following characteristics:
  - It can exist only between two domains in the same tree and namespace.
  - The child domain trusts the parent domain.
  - The parent domain trusts the child domain.
  - The trusts between parent and child domains are transitive.

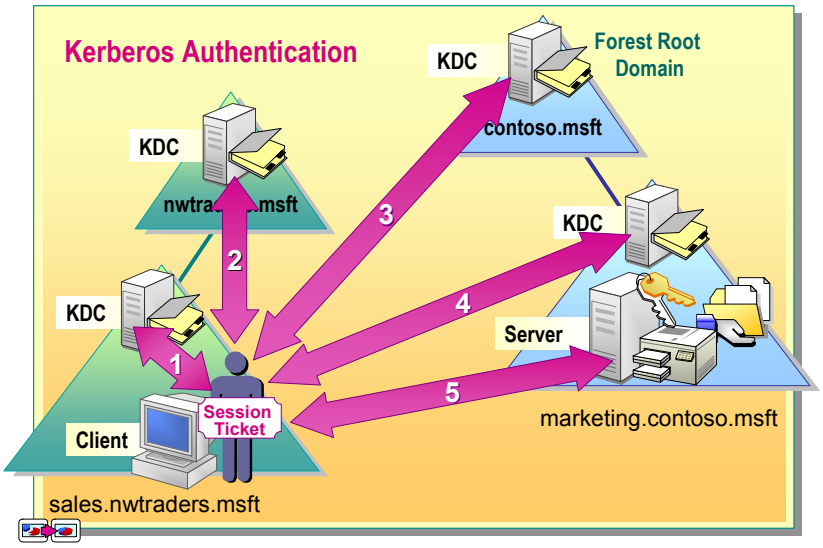
How Trusts Work



When a user attempts to gain access to a resource in another domain, the Kerberos V5 protocol must determine whether the *trusting* domain, which is the domain containing the resource to which the user is trying to gain access, has a trust relationship with the *trusted* domain, which is the domain to which the user is logging on. To determine this relationship, the Kerberos V5 security protocol travels the trust path between the domain controller in the trusting domain to the domain controller in the trusted domain.

When a user in the trusted domain attempts to gain access to a resource in another domain, the user's computer first contacts the domain controller in its domain to get authentication to the resource. If the resource is not in the user's domain, the domain controller uses the trust relationship with its parent and refers the user's computer to a domain controller in its parent domain. This attempt for locating a resource continues up the trust hierarchy, possibly to the forest root domain, and down the trust hierarchy until contacting a domain controller in the domain where the resource is located. The path that is taken from domain to domain is the trust path. The path that is taken is the shortest path following the trust hierarchy.

How Kerberos V5 Works



The Kerberos V5 protocol is the primary authentication protocol in Windows 2000; it verifies both the identity of the user and the integrity of the network services. The main components of the Kerberos V5 protocol are a client, a server, and a trusted third party to mediate between them. The trusted intermediary in the protocol is known as the *Key Distribution Center* (KDC). In Windows 2000, the domain controller functions as the KDC. The KDC runs on each domain controller as part of Active Directory, which stores all client passwords and other account information.

The Kerberos V5 services are installed on each domain controller, and a Kerberos V5 client is installed on each Windows 2000 workstation and server. A user's initial Kerberos authentication provides the user with a single logon to enterprise resources.

The Kerberos V5 authentication mechanism issues session tickets for accessing network services. These tickets contain encrypted data, including an encrypted key, which confirms the user's identity to the requested service.

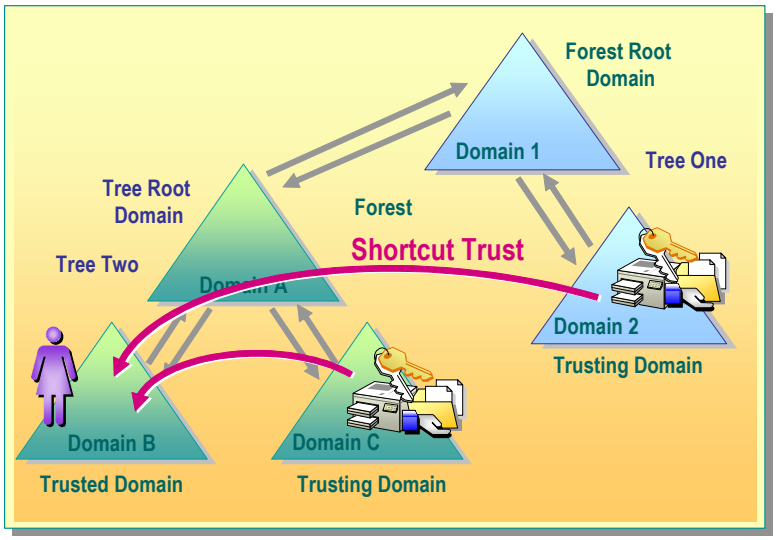
When accessing resources across a forest, the client follows the Kerberos V5 protocol trust path. As an example to illustrate the authentication path, consider a tree, contoso.msft, in a forest and its child domain, sales.contoso.msft. The other tree, nwtraders.msft, in the forest consists of the child domain marketing.nwtraders.msft.

If a user in sales.nwtraders.msft needs to gain access to resources in marketing.contoso.msft. This process assumes that the user has previously authenticated with the network and has a Ticket Granting Ticket (TGT) for the sales.nwtraders.msft domain populated with the user's global and universal group memberships. The following Kerberos V5 authentication process occurs:

1. The user asks for a session ticket for the server in marketing.contoso.msft. The KDC in the sales.nwtraders.msft domain issues a TGT for the nwtraders.msft domain known as a referral ticket.
2. The user presents the KDC in the nwtraders.msft the TGT for that domain and is issued a TGT for the contoso.msft domain.
3. The user presents the KDC in the contoso.msft the TGT for that domain and is issued a TGT for the marketing.contoso.msft domain.
4. The user presents the KDC in the marketing.contoso.msft the TGT for that domain and is issued a ST for the contoso.msft domain. This ST is populated with the domain local group memberships from the marketing.contoso.msft domain.
5. The user presents the server session ticket to the server to gain access to resources on the server in marketing.contoso.msft. The server compares the SIDs include in the session ticket to the ACEs on the requested resource to determine if the user is authorized to access the resource.

Important For more detailed information about the steps in the Kerberos V5 authentication process, see *Windows 2000 Kerberos Authentication* under **Additional Reading** on the Web page on the Student Materials compact disc.

Shortcut Trusts in Windows 2000



Shortcut trusts are one-way transitive trusts that you can use to optimize performance by shortening the trust path for authentication purposes. You manually create one-way shortcut trusts between Windows 2000 domains from the trusting domain to the trusted domain in the same forest. Even though shortcut trusts are one-way, you can also create a two-way relationship by manually creating two one-way trusts in each direction.

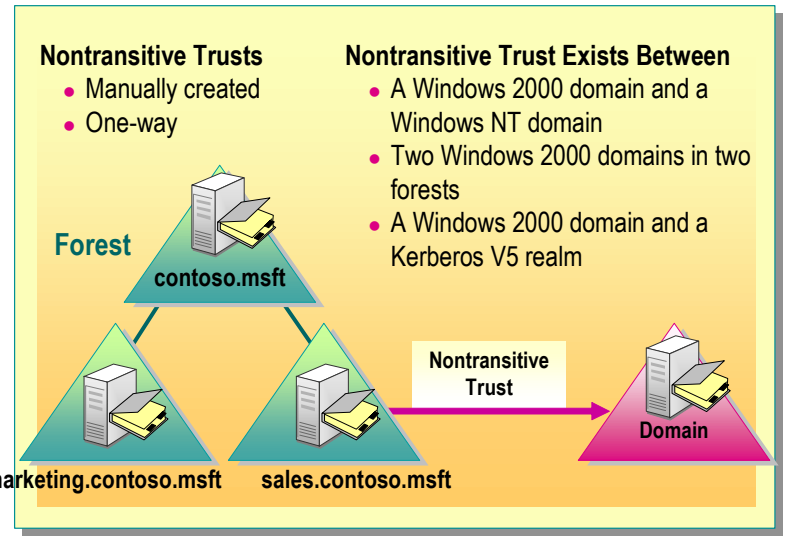
Shortcut trusts reduce the trust path by allowing a more direct connection between two domains that otherwise would require the path to travel up the hierarchy, possibly to the forest root domain, before it travels down to the other domain. The most effective use of shortcut trusts is when there is a number of users frequently accessing resources in another domain in the forest and the number of domains in the trust path that the client needs to connect to is numerous.

To illustrate an example of a shortcut trust in the same tree, assume users in domain B often need to gain access to resources in domain C. You can create a direct link from the trusting domain C to the trusted domain B by using a shortcut trust relationship so that domain A can be bypassed in the trust path.

To illustrate an example of a shortcut trust between two trees, assume users in domain B often need to gain access to resources in domain 2. You can create a direct link from the trusting domain 2 to the trusted domain B through a shortcut trust relationship so that data does not have to travel up through the forest root from one domain tree through the other.

Note For more information about how to create and manage shortcut trusts by using Active Directory Domains and Trusts, see the Windows 2000 Help.

Nontransitive Trusts in Windows 2000



A *nontransitive trust relationship* can be created between Windows 2000 domains if a transitive trust relationship is not automatically provided.

What Is a Nontransitive Trust?

You must explicitly create a nontransitive trust. A nontransitive trust is one-way. To create a two-way nontransitive trust, you can manually create two one-way trusts in each direction.

Nontransitive trusts are the trust relationships that are possible between only the following:

- A Windows 2000 domain and a Windows NT domain. If one of these domains is an account domain and the other is a resource domain, the trust relationship is usually created as a one-way trust relationship.
- A Windows 2000 domain in one forest and a Windows 2000 domain in another forest. The relationship between these two domains is often called an *external trust.*
- A Windows 2000 domain and an Kerberos V5 protocol security realm.

Note A Kerberos V5 realm is a security boundary similar to a Windows 2000 domain.

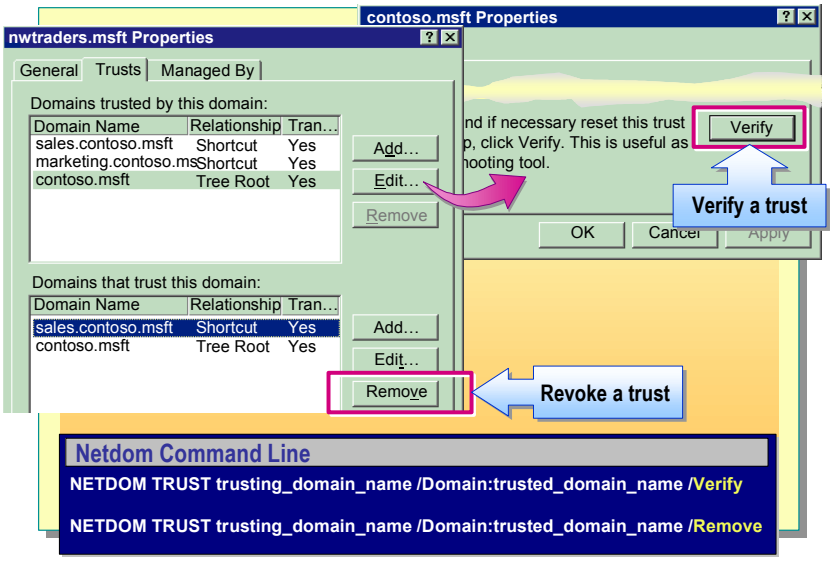
Creating a Nontransitive Trust

To create a nontransitive trust, you must know the domain names to be included in the relationship and have a user account with permission to create trusts in each domain. Each trust is assigned a password that the administrators of both domains in the relationship must know.

To create a nontransitive trust, perform the following steps:

1. In Active Directory Domains and Trusts, in the console tree, right-click the domain that you want to administer, and then click **Properties**.
2. On the **Trusts** tab, depending on which domain you are on, click **either Domains trusted by this domain** or **Domains that trust this domain**, and then click **Add**.
3. Depending on the type of domain, perform one of the following tasks:
   - If the domain to be added is a Windows 2000 domain, type the full DNS name of the domain.
   - If the domain is running an earlier version of Windows, type the domain name.
4. Type the password for this trust, and then confirm the password.
5. Repeat steps 1 through 4 on the domain that forms the other part of the nontransitive trust relationship.

Verifying and Revoking Trusts



If you create nontransitive trusts, you will sometimes need to verify and delete, or revoke, the trust paths you created. You verify a trust to make sure it is working correctly and can validate authentication requests from other domains. You revoke a trust to prevent that authentication path from being used during authentication. You can use Active Directory Domains and Trusts or the **netdom** command to verify and revoke trust paths.

Verifying Trusts

To verify a trust by using Active Directory Domains and Trusts, perform the following steps:

1. In Active Directory Domains and Trusts, in the console tree, right-click one of the domains involved in the trust that you want to verify, and then click **Properties**.
2. On the **Trusts** tab, depending on which domain you are in, you use **Domains trusted by this domain** or **Domains that trust this domain** to select the trust to be verified.
3. Click the trust, and then click **Edit**.
4. Click **Verify/Reset**.
5. Repeat steps 1 through 4 to verify the trust for the other domain involved in the relationship.

Revoking Trusts

To revoke a trust by using Active Directory Domains and Trusts, perform the following steps:

1. In Active Directory Domains and Trusts, in the console tree, right-click one of the domains involved in the trust that you want to revoke, and then click **Properties**.
2. On the **Trusts** tab, depending on which domain you are in**,** use **Domains trusted by this domain** or **Domains that trust this domain** to select the trust to be revoked.
3. Select the trust, and then click **Remove**.
4. Repeat steps 1 through 3 to revoke the trust for the other domain involved in the relationship.

Verifying and Revoking Trusts Using Netdom

Netdom is a command-line utility that you can use to manage Windows 2000 domains and trust relationships from a command prompt window.

Use **netdom** to perform the following tasks:

- View all trust relationships.
- Enumerate direct trust relationships.
- Enumerate all (direct and indirect) trust relationships.

To verify a trust by using **netdom**, perform the following steps:

1. Open a command prompt window.
2. Type
   NETDOM TRUST trusting_domain_name
   /Domain:trusted_domain_name /Verify and press ENTER.

To revoke a trust using **netdom**, perform the following steps:

1. Open a command prompt window.
2. Type
   NETDOM TRUST trusting_domain_name
   /Domain:trusted_domain_name /Remove and press ENTER.

Lab A: Creating Domain Trees and Establishing Trusts

Objectives

After completing this lab, you will be able to:

- Create child domains in an existing forest.
- Remove an existing forest.
- Examine and verify trusts between domains.

Prerequisites

Before working on this lab, you must have knowledge and experience installing and removing Active Directory.

Lab Setup

To complete this lab, you need the Windows 2000 Advanced Server compact disc for the installation of the support tools during the lab.

Important The lab does not reflect the real-world environment. It is recommended that you always use complex passwords for any administrator accounts, and never create accounts without a password.

Important Outside of the classroom environment, it is strongly advised that you use the most recent software updates that are necessary. Because this is a classroom environment, we may use software that does not include the latest updates.

Student Computer IP Address, Domain, and FQDN Information

During this lab, you will be asked for your Internet Protocol (IP) address, domain, and fully qualified domain name (FQDN). Use this information from the following table to determine what to enter for these values. Your instructor will assign you a student number and provide the number to use in place of the *x* in the IP address.

Student number	IP address	Domain (*domain*)	FQDN
1	192.168.*x*.1	namerica1	vancouver.namerica1.nwtraders.msft
2	192.168.*x*.2	namerica1	denver.namerica1.nwtraders.msft
3	192.168.*x*.3	spacific1	perth.spacific1.nwtraders.msft
4	192.168.*x*.4	spacific1	brisbane.spacific1.nwtraders.msft
5	192.168.*x*.5	europe1	lisbon.europe1.nwtraders.msft
6	192.168.*x*.6	europe1	bonn.europe1.nwtraders.msft
7	192.168.*x*.7	samerica1	lima.samerica1.nwtraders.msft
8	192.168.*x*.8	samerica1	santiago.samerica1.nwtraders.msft
9	192.168.*x*.9	asia1	bangalore.asia1.nwtraders.msft
10	192.168.*x*.10	asia1	singapore.asia1.nwtraders.msft
11	192.168.*x*.11	africa1	casablanca.africa1.nwtraders.msft
12	192.168.*x*.12	africa1	tunis.africa1.nwtraders.msft
13	192.168.*x*.13	namerica2	acapulco.namerica2.nwtraders.msft
14	192.168.*x*.14	namerica2	miami.namerica2.nwtraders.msft
15	192.168.*x*.15	spacific2	auckland.spacific2.nwtraders.msft
16	192.168.*x*.16	spacific2	suva.spacific2.nwtraders.msft
17	192.168.*x*.17	europe2	stockholm.europe2.nwtraders.msft
18	192.168.*x*.18	europe2	moscow.europe2.nwtraders.msft
19	192.168.*x*.19	samerica2	caracas.samerica2.nwtraders.msft
20	192.168.*x*.20	samerica2	montevideo.samerica2.nwtraders.msft
21	192.168.*x*.21	asia2	manila.asia2.nwtraders.msft
22	192.168.*x*.22	asia2	tokyo.asia2.nwtraders.msft
23	192.168.*x*.23	africa2	khartoum.africa2.nwtraders.msft
24	192.168.*x*.24	africa2	nairobi.africa2.nwtraders.msft

Estimated time to complete this lab: 60 minutes

Exercise 1
Removing an Existing Forest

Scenario

After testing the features in Active Directory and the computer hardware, you will create the Northwind Traders forest. Before creating a new domain, you must remove the existing test forest environment and prepare your network settings for the new domain.

Goal

In this exercise, you will use the Active Directory Installation wizard to remove your existing domain and forest so that you can become a domain controller for a child domain. You will configure your network settings in preparation for the new domain.

Tasks	Detailed Steps
1. Remove your existing domain and forest. When prompted, restart your computer.	**a.** Log on as Administrator in your domain with a password of **password**. **b.** Run **dcpromo** to start the Active Directory Installation wizard. **c.** On the **Welcome to the Active Directory Installation Wizard** page, click **Next** to continue, and then click **OK** to close the message indicating that this domain controller is also a global catalog server. **d.** On the **Remove Active Directory** page, select the **This server is the last domain controller in the domain** check box, and then click **Next**. **e.** On the **Network Credentials** page, in the **User name** box, type **Administrator** **f.** In the **Password** box, type **password** and then click **Next**. **g.** On the **Administrator Password** page, in the **Password** and **Confirm password** boxes, type **password** and then click **Next**. **h.** On the **Summary** page, review the summary information, and then click **Next**. *The wizard takes several minutes to complete the removal of Active Directory from this computer.* **i.** On the **Completing the Active Directory Installation Wizard** page, click **Finish**, and then click **Restart Now** to restart your computer.
2. Remove the DNS subcomponent of Networking Services.	**a.** Log on as Administrator with a password of **password**. **b.** On the desktop, right-click **My Network Places**, and then click **Properties**. **c.** In the Network and Dial-up Connections window, on the **Advanced** menu, click **Optional Networking Components**. **d.** On the **Windows Components** page, under **Components**, clear the **Networking Services** check box, and then click **Next** to complete the removal of the DNS service. *The wizard finishes removing the DNS service.*

Tasks	Detailed Steps
3. Configure the Internet Protocol (TCP/IP) properties of your Local Area Connection to use the instructor computer, London 192.168.*x*.200 (where *x* is your assigned classroom network ID), for your preferred DNS server.	**a.** In the Network and Dial-up Connections window, right-click **Local Area Connection**, and then click **Properties**. **b.** Click **Internet Protocol (TCP/IP)**, and then click **Properties**. **c.** In the **Preferred DNS Server** box, type the IP address of London, which is **192.168.*x*.200** (where *x* is your assigned classroom network ID) and then click **OK**. **d.** In the **Local Area Connections Properties** dialog box, click **OK**, and then close the Network and Dial-up Connections window.
4. Configure the DNS suffix for your computer. When prompted, restart your computer. The primary DNS suffix is *domain*.nwtraders.msft (where *domain* is your assigned domain name).	**a.** On the desktop, right-click **My Computer**, and then click **Properties**. **b.** In the **System Properties** dialog box, on the **Network Identification** tab, click **Properties**. **c.** In the **Identification Changes** dialog box, click **More**. **d.** In the **DNS Suffix and NetBIOS Computer Name** dialog box, in the **Primary DNS suffix of this computer** box, type *domain***.nwtraders.msft** (where *domain* is your assigned domain name) and then click **OK**. **e.** In the **Identification Changes** dialog box, click **OK**, and then click **OK** again to restart the computer for the changes to take effect. **f.** In the **System Properties** dialog box, click **OK**, and then click **Yes** to restart your computer.
5. Verify the proper configuration of Host Name, Primary DNS Suffix, and DNS servers according to the configuration table located in the Lab Setup section of this lab.	**a.** Log on as Administrator with a password of **password**. **b.** Open a command prompt window. **c.** At the command prompt, type **ipconfig /all** and then press ENTER to view your computer's TCP/IP configuration. **d.** Verify that the value of **Host Name** is your host name. Ensure that this value matches the first label of your FQDN entry, which is listed in the table in the Lab Setup section of this lab. **e.** Verify that the value of **Primary DNS Suffix** is the full domain name of your computer. Ensure that this value matches the last three labels of your FQDN entry listed, which is in the table in the Lab Setup section of this lab. **f.** Verify that the value of **DNS Servers** matches London's IP address: **192.168.*x*.200** **g.** Close all open windows.

Exercise 2
Creating a Child Domain

Scenario

Northwind Traders has designed their forest structure, which consists of a single domain tree with the root DNS name of nwtraders.msft. The corporate office is overseeing the rollout of the domain tree, and has already created the forest root domain nwtraders.msft. You must create the child domain for your region.

Goal

In this exercise, you will run the Active Directory Installation wizard to create the child domain for your region.

Tasks	Detailed Steps
Important: Perform this entire exercise only on the computer with the lower student number of the pair that is in the same child domain.	
1. Start the Active Directory Installation wizard to create: • A new domain controller for a new domain. • An existing domain tree. • For network credentials, use Administrator, password, and nwtraders.msft.	**a.** Run **dcpromo** to start the Active Directory Installation wizard. **b.** On the **Welcome to the Active Directory Installation Wizard** page, click **Next** to continue. **c.** On the **Domain Controller Type** page, ensure that **Domain controller for a new domain** is selected, and then click **Next**. **d.** On the **Create Tree or Child Domain** page, click **Create a new child domain in an existing domain tree**, and then click **Next**. **e.** On the **Network Credentials** page, type **Administrator** in the **User name** box, type **password** in the **Password** box, type **nwtraders.msft** in the **Domain** box, and then click **Next**.

Tasks	Detailed Steps
2. Complete the Active Directory installation process, providing the following information: • Full DNS name of domain.nwtraders.msft. • NetBIOS domain name of domain in uppercase characters. • Default locations for the database, log files, and shared system volume. • Permission compatible only with servers running Windows 2000. • A password of password for the Directory Services Restore Mode Administrator password. • Restart your computer when prompted.	**a.** On the Child Domain Installation page, click Browse. **b.** In the **Browse for Domain** dialog box, click **nwtraders.msft**, and then click **OK**. **c.** On the **Child Domain Installation** page, in the **Child domain** box, type *domain* and then click **Next**. **d.** On the **NetBIOS Domain Name** page, in the **Domain NetBIOS name** box, ensure that the value is the domain name, and then click **Next**. **e.** On the **Database and Log Locations** page, click **Next** to accept the default folder locations for both database files and log files. **f.** On the **Shared System Volume** page, click **Next** to accept the default folder location. **g.** On the **Permissions** page, click **Permissions compatible only with Windows 2000 servers**, and then click **Next**. **h.** On the **Directory Services Restore Mode Administrator Password** page, in the **Password** and **Confirm password** boxes, type **password** and then click **Next**. **i.** On the **Summary** page, review the summary information, and then click **Next**. *The wizard takes several minutes to complete the installation of Active Directory on this computer.* **j.** On the Completing the Active Directory Installation Wizard page, click Finish, and then click Restart Now to restart your computer.
3. Log on as Administrator in your domain after the domain controller restarts.	▪ Log on as Administrator in your domain with a password of **password**.

Exercise 3
Creating a Replica in a Child Domain

Scenario

Northwind Traders has designed their forest structure, which consists of a single domain tree with the root DNS name of nwtraders.msft. The corporate office is overseeing the rollout of the domain tree, and has already created all of the domains in the forest. Now the corporate office is strictly enforcing the guidelines that all domains should have at least two domain controllers to provide fault tolerance in case of a failure.

Goal

In this exercise, you will run the Active Directory Installation wizard to create a replica for the child domain of your region.

Tasks	Detailed Steps
Important: Perform this entire exercise only on the computer with the higher student number of the pair that is in the same child domain, and only after exercise 2 is complete.	
1. Start the Active Directory Installation wizard to create: • An additional domain controller for an existing domain. • For network credentials, use Administrator, **password**, and *domain***.nwtraders.msft.**	**a.** Run **dcpromo** to start the Active Directory Installation wizard. **b.** On the **Welcome to the Active Directory Installation Wizard** page, click **Next** to continue. **c.** On the **Domain Controller Type** page, click **Additional domain controller for an existing domain**, and then click **Next**. **d.** On the **Network Credentials** page, type **Administrator** in the **User name** box, type **password** in the **Password** box, type *domain***.nwtraders.msft** in the **Domain** box, and then click **Next**.
2. Complete the Active Directory installation process, providing the following information: • Full DNS name of *domain*.nwtraders.msft. • Default locations for the database, log files, and shared system volume. • A password of **password** for the Directory Services Restore Mode Administrator password. • Restart your computer when prompted.	**a.** On the Additional Domain Controller page, click Browse. **b.** In the **Browse for Domain** dialog box, expand **nwtraders.msft**, click *domain***.nwtraders.msft**, and then click **OK**. **c.** On the **Additional Domain Controller** page, click **Next**. **d.** On the **Database and Log Locations** page, click **Next** to accept the default folder locations for both database files and log files. **e.** On the **Shared System Volume** page, click **Next** to accept the default folder location. **f.** On the **Directory Services Restore Mode Administrator Password** page, in the **Password** and **Confirm password** boxes, type **password** and then click **Next**. **g.** On the **Summary** page, review the summary information, and then click **Next**. *The wizard takes several minutes to complete the installation of Active Directory on this computer.* **h.** On the **Completing the Active Directory Installation Wizard** page, click **Finish**, and then click **Restart Now** to close the message asking to reboot your computer now.
3. Log on as Administrator in your child domain after the domain controller restarts.	▪ Log on as Administrator in your child domain with a password of **password**.

Exercise 4
Examining Trusts in a Forest

Scenario

Northwind Traders corporate administrators want to ensure that each region's domain in the nwtraders.msft domain tree is working correctly before moving forward with the second phase of their deployment plan. You must verify that the parent-child trusts between your region's domain and nwtraders.msft are working correctly.

Goal

In this exercise, you will verify the operation of the trusts between your region's domain and nwtraders.msft. This verification is necessary for the corporate office to determine that the nwtraders.msft domain tree that has just been created is functional and stable. You will also use the Netdom.exe support tool to verify the parent-child trust relationship.

Tasks	Detailed Steps
1. Test the trust between your child domain and nwtraders.msft, by using the Active Directory Domains and Trusts console.	**a.** Open Active Directory Domains and Trusts from the **Administrative Tools** menu, expand **nwtraders.msft**, and then click *domain***.nwtraders.msft**. **b.** Right-click *domain***.nwtraders.msft**, and then click **Properties**. **c.** In the *domain***.nwtraders.msft Properties** dialog box, click the **Trusts** tab.
How many parent-child trust relationships does your child domain have?	
1. *(continued)*	**d.** In the **Domains trusted by this domain** list, click **nwtraders.msft**, and then click **Edit** to view the properties of this trust link. **e.** In the **nwtraders.msft Properties** dialog box, click **Verify**. **f.** In the **Active Directory** dialog box, in the **User name** box, type **Administrator** In the **Password** box, type **password** **g.** Click **OK**, and then click **OK** again to close the message indicating that the trust has been verified.

Tasks	Detailed Steps
1. *(continued)*	**h.** If necessary, click **OK** to close the message indicating that a secure channel could not be established because there are currently are no logon servers available. **i.** Click **OK** to close the **nwtraders.msft Properties** dialog box, click **OK** to close the *domain***.nwtraders.msft Properties** dialog box, and then close Active Directory Domains and Trusts.
2. Install the Windows 2000 Support Tools, if they are not already installed, by using all of the default options.	**a.** On your Windows 2000 Advanced Server compact disc, in the Support/Tools folder, run **Setup** to start the Windows 2000 Support Tools Setup wizard. **b.** On the **Welcome to the Windows 2000 Support Tools Setup Wizard** page, click **Next** to continue. **c.** On the **User Information** page, type your name in the **Name** box, type your organization in the **Organization** box, and then click **Next**. **d.** On the **Select An Installation Type** page, ensure that **Typical** is selected, and then click **Next**. **e.** On the **Begin Installation** page, click **Next** to begin the installation of the Windows 2000 Support Tools. *The wizard takes a short time to complete the installation.* **f.** On the **Completing the Windows 2000 Support Tools Setup Wizard** page, click **Finish**.
3. Verify the trust relationship between your child domain and nwtraders.msft by using the Netdom.exe tool, and then log off.	**a.** Open a command prompt window. **b.** At the command prompt, type **netdom help trust** and then press ENTER to view the available options. **c.** At the command prompt, type **netdom trust** *domain* **/Domain:nwtraders /UserD:Administrator /PasswordD:password /UserO:Administrator /PasswordO:password /verify** and then press ENTER to determine the state of the trust relationship. **d.** Close all open windows, and then log off.

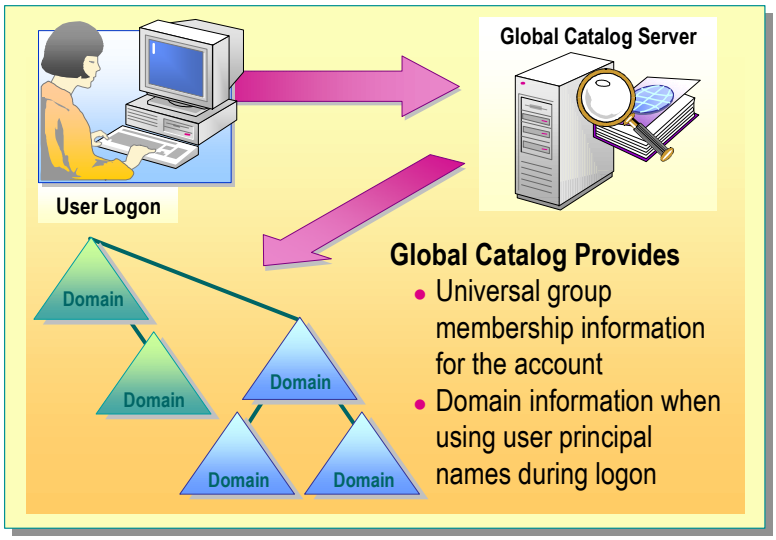
The Global Catalog

- The Global Catalog and the Logon Process
- Creating a Global Catalog Server

The *global catalog* contains the information that is necessary to determine the location of any object in Active Directory. The global catalog enables a user to log on to the network by providing universal group membership information and user principal name domain mapping information to a domain controller. Also, the global catalog server enables a user to find Active Directory information in the entire forest, regardless of the location of the information.

The first domain controller that you create in Active Directory is a global catalog server. You can configure additional domain controllers to be global catalog servers to balance the traffic from logon authentication and queries.

The Global Catalog and the Logon Process



When you log on to a domain in native mode, the global catalog server provides universal group membership information for your account to the domain controller that processes the user logon information, and authenticates the user principal name.

Global Catalog and Universal Group Membership

When a user logs on to a domain in native mode, the global catalog server provides universal group membership information for the account to the domain controller that processes the user logon information. If a global catalog server is not available when a user initiates the network logon process and the user has logged on to the domain previously, Windows 2000 uses cached credentials to log on the user. If the user has not logged on to the domain previously, the user is able to log on to only the local computer.

During the logon process, an access token, which contains the groups to which the user belongs, is associated with the user. Because universal group membership is centrally stored in the global catalog, global catalog servers are used to identify the universal groups of which a user is a member.

Global Catalog and Authentication

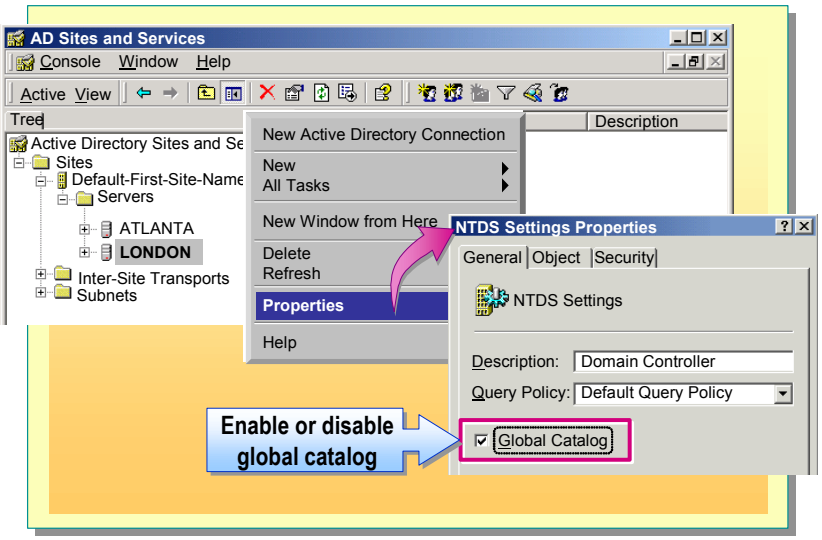
A global catalog server is also required when a user logs on with a user principal name and the authenticating domain controller does not have direct knowledge of the account.

For example, Suzan Fine's account is in contoso.msft. She uses a computer that is in the domain sales.contoso.msft. She logs on as suzanf@contoso.msft. When the domain controller in sales.contoso.msft is unable to authenticate the user account for Suzan Fine, it must contact a global catalog server to complete the logon process.

In a single domain network, a global catalog server is not required for the logon process because every domain controller contains the information that is needed to authenticate a user. Although a global catalog server is not queried during the logon process in a single domain network, a global catalog server is required for other types of directory service queries.

Note When the user is a member of the Domain Admins group, the user can log on to the network even when the global catalog server is not available.

Creating a Global Catalog Server



The first domain controller in a forest is automatically designated as a global catalog server. You can authorize any domain controller to be a global catalog server; however, one global catalog server is typically useful in each site.

To enable or disable a global catalog server, perform the following steps:

1. In Active Directory Sites and Services, in the console tree, expand the domain controller that will host or is hosting the global catalog.
2. Right-click **NTDS Settings**, and then click **Properties**.
3. Select or clear the **Global Catalog** check box.

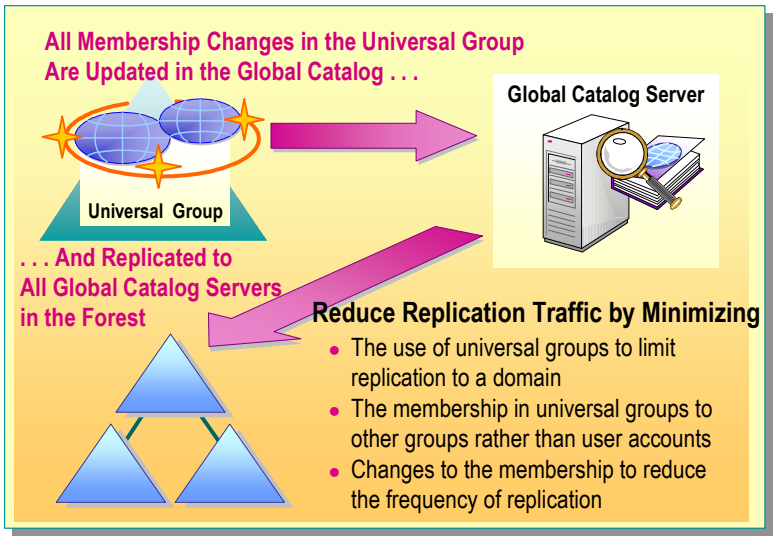
Strategies for Using Groups in Trees and Forests

- Universal Groups and Replication
- Nesting Strategy Using Universal Groups
- Class Discussion: Using Groups in Trees and Forests

Windows 2000 allows you to organize users and other domain objects into security groups to assign the same security permissions. Assigning security permissions to a group instead of to individual users ensures consistent security permissions across all members of a group. By using security groups to assign permissions, you can ensure that the discretionary access control lists (DACLs) on resources do not change often and are easy to manage and audit.

You can add or remove users from the appropriate security groups as needed. When you create a new user, you can add the user to an existing security group to completely define the user's permissions and access limits. You can add groups to other groups. Changing permissions for the group affects all users and groups within the group.

Universal Groups and Replication



A list of universal group memberships is maintained in the global catalog. Global and domain local groups are listed in the global catalog, but their membership is not. Changes to the data stored in the global catalog are replicated to every global catalog in a forest. Whenever one member of a group with universal scope changes, the entire group membership must be replicated to all global catalogs in the domain tree or forest.

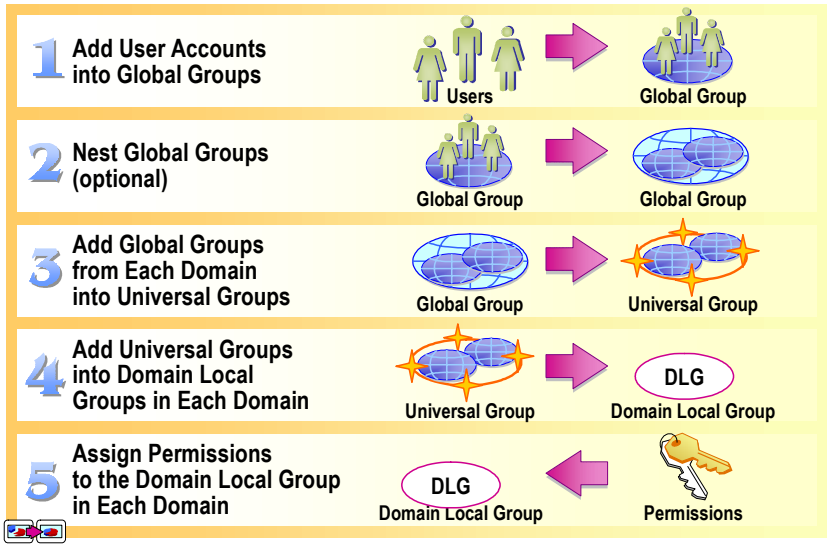
By minimizing the use of universal groups, you can limit the replication traffic to a single domain.

Consider minimizing the membership in universal groups to global groups, instead of to user accounts. This allows you to adjust the user accounts that are members of the universal group by adjusting the membership of the groups that are members of the universal group. Because adjusting the membership of the groups does not directly affect the membership of the universal group, no replication traffic is generated.

Reduce the amount of changes made to the membership of a universal group. This reduces the number of times the membership data is replicated to all the global catalog servers. If any change is made to the membership, the entire membership list is replicated.

Note An access token can contain up to 1,024 groups. Groups can have up to 5,000 members. The user's primary group membership, such as Domain Users, is not stored in the group membership list.

Nesting Strategy Using Universal Groups



Use universal groups to consolidate groups that span multiple domains.

To consolidate groups that span multiple domains, perform the following steps:

1. In each domain, add user accounts for users with the same job function to global groups.
2. Nest global groups into a single global group to consolidate users. This step is optional, but is very useful if you need to manage large groups of users.
3. Nest the global group or multiple global groups from each domain into one universal group.
4. Add the universal groups to the domain local groups that are created for each resource.
5. Assign to the domain local groups the appropriate permissions for users in the group to gain access to resources.

By using this strategy, any membership changes in the global groups do not affect the membership in the universal groups.

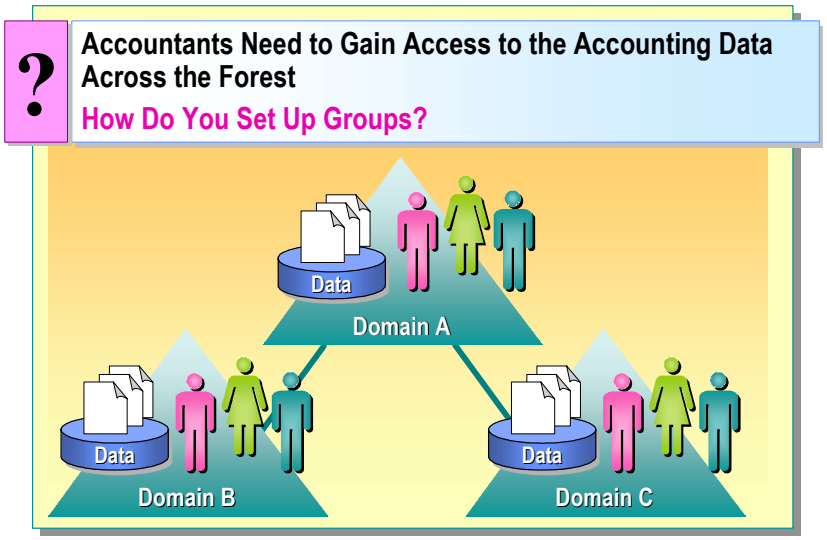
The strategy described on this page uses A-G-G-U-DL-P and applies to the following circumstances:

- File and print permission.
- Active Directory Permissions in the domain name controller.

You can use A-G-U-P strategy for assigning permissions to:

- Configure naming conventions in Active Directory.
- Attribute permissions for attributes published to the global catalog.

Class Discussion: Using Groups in Trees and Forests



In this example, Contoso, Ltd. wants to react more quickly to market demands. It has been determined that the accounting data spanning multiple domains in the enterprise needs to be available to all of the accounting staff, which is also located in multiple domains. Contoso, Ltd. wants to create the entire group structure for the Accounting division, which includes the Accounts Payable and Accounts Receivable departments.

1. What would you do to ensure that the managers have the required access and that there is a minimum of administration?

2. Contoso, Ltd. has experienced growth in their business and you must create a new domain. What changes would you make to your group structure to make sure that all accountants in the organization, including those in the new domain, have access to all of the accounting data?

Lab B: Using Groups in a Forest

Objectives

After completing this lab, you will be able to:

- Create and nest domain local, global, and universal security groups.
- Add global groups from other domains into universal groups.
- Switch the domain mode from mixed mode to native mode.
- Verify access to resources by using a group strategy that includes global, universal, and domain local groups.
- View the logged on user's access token, and observe the effects of group nesting.

Prerequisites

Before working on this lab, you must have:

- Knowledge about mixed and native domain modes.
- Knowledge and skills using domain local, global, and universal groups.
- Knowledge about replication latency, and how to manually initiate replication.
- Knowledge about access tokens and how group membership affects them.

Lab Setup

To complete this lab, you need to do the following:

- Run the batch file C:\Moc\Win2154a\Labfiles\Lrights.bat to set the log on locally user right for the users group.

Student Computer Information

During this lab, you will be asked for your student number, host name, and domain. Use the information from the following table to determine what to enter for these values. Your instructor will assign you a student number.

Student number (*n*)	Host name (*servername*)	Domain (*domain*)	FQDN
1	vancouver	namerica1	vancouver.namerica1.nwtraders.msft
2	denver	namerica1	denver.namerica1.nwtraders.msft
3	perth	spacific1	perth.spacific1.nwtraders.msft
4	brisbane	spacific1	brisbane.spacific1.nwtraders.msft
5	lisbon	europe1	lisbon.europe1.nwtraders.msft
6	bonn	europe1	bonn.europe1.nwtraders.msft
7	lima	samerica1	lima.samerica1.nwtraders.msft
8	santiago	samerica1	santiago.samerica1.nwtraders.msft
9	bangalore	asia1	bangalore.asia1.nwtraders.msft
10	singapore	asia1	singapore.asia1.nwtraders.msft
11	casablanca	africa1	casablanca.africa1.nwtraders.msft
12	tunis	africa1	tunis.africa1.nwtraders.msft
13	acapulco	namerica2	acapulco.namerica2.nwtraders.msft
14	miami	namerica2	miami.namerica2.nwtraders.msft
15	auckland	spacific2	auckland.spacific2.nwtraders.msft
16	suva	spacific2	suva.spacific2.nwtraders.msft
17	stockholm	europe2	stockholm.europe2.nwtraders.msft
18	moscow	europe2	moscow.europe2.nwtraders.msft
19	caracas	samerica2	caracas.samerica2.nwtraders.msft
20	montevideo	samerica2	montevideo.samerica2.nwtraders.msft
21	manila	asia2	manila.asia2.nwtraders.msft
22	tokyo	asia2	tokyo.asia2.nwtraders.msft
23	khartoum	africa2	khartoum.africa2.nwtraders.msft
24	nairobi	africa2	nairobi.africa2.nwtraders.msft

Estimated time to complete this lab: 30 minutes

Exercise 1
Implementing Groups Strategy

Scenario

Northwind Traders wants to react more quickly to market demands. It has been determined that the accounting data is located in various folders throughout the domains and needs to be available to the entire accounting staff which is located in multiple domains. Northwind Traders wants to create the entire group structure for the Accounting division, which includes the Accounts Payable and Accounts Receivable departments.

Goal

In this exercise, you will create three global groups: Accounting, Accounts Payable, and Accounts Receivable. You will add Accounts Payable and Accounts Receivable as members of Accounting. You will create the universal group, All Accounting, and then add the Accounting groups from all domains into this group. This will consolidate all of the accounting employees in the forest into the single universal group. You will create the domain local group, Local Data, and add the universal group as a member. You will assign Read permissions of the accounting data to the Local Data domain local group. To test the group structure, you will create a test user account and add this user account to the Accounts Payable group.

Tasks	Detailed Steps
Important: Perform task 1 only on the computer with the lower student number of the pair that is in the same child domain.	
1. Switch *domain*.nwtraders.msft (where *domain* is your assigned domain name) to native mode to allow extended group nesting and universal security groups.	**a.** Log on as Administrator in your domain with a password of **password**. **b.** Open Active Directory Users and Computers from the **Administrative Tools** menu. **c.** In the console tree, right-click *domain***.nwtraders.msft** (where *domain* is your assigned domain name), and then click **Properties**. **d.** Click **Change Mode**, click **Yes** to close the confirmation dialog box, click **OK**, and then click **OK** again to close the message indicating that it may take 15 minutes or more for this information to replicate to all domain controllers.
Important: Perform task 2 only on the computer with the higher student number of the pair that is in the same child domain. Wait until task 1 is completed before starting task 2.	

Tasks	Detailed Steps
2. Manually initiate replication from your partner's domain controller to your domain controller to quickly replicate the domain mode change.	**a.** Open Active Directory Sites and Services from the **Administrative Tools** menu, expand **Sites**, expand **Default-First-Site-Name**, expand **Servers**, expand *servername* (where *servername* is the host name of your computer), and then click **NTDS Settings**. **b.** In the details pane, right-click the connection object that is from *partnerserver* (where *partnerserver* is the host name of your partner's computer), and then click **Replicate Now** to initiate the copying of changes from your partner's domain controller to your domain controller. **c.** Click **OK** to close the message indicating that replication has been initiated, and then close Active Directory Sites and Services. *If an error message indicating the RPC service is unavailable, simply wait a moment and then repeat the Replicate Now operation.*
Important: Perform the remaining tasks on both computers.	
3. Within *domain*.nwtraders.msft, create the following OU: *n*_Accounting (where *n* is your assigned student number).	**a.** Open, or switch to, Active Directory Users and Computers, and then in the console tree, expand *domain***.nwtraders.msft**. **b.** Right-click *domain***.nwtraders.msft**, point to **New**, and then click **Organizational Unit**. **c.** In the **New Object – Organizational Unit** dialog box, in the **Name** box, type *n***_Accounting** (where *n* is your assigned student number), and then click **OK**.
4. Within the *n*_Accounting OU, create the following global security groups: *n*_Accounts Payable *n*_Accounts Receivable.	**a.** Right-click the *n***_Accounting** OU, point to **New**, and then click **Group**. **b.** In the **New Object – Group** dialog box, in the **Group name** box, type *n***_Accounts Payable** **c.** Ensure that **Group scope** is **Global** and **Group type** is **Security**, and then click **OK**. **d.** Repeat steps a and b, changing step b as required, to create the *n***_Accounts Receivable** global security group.
5. Within the *n*_Accounting OU, create the *n*_Domain Accountants global group, and then add the department global groups, *n*_Accounts Payable and *n*_Accounts Receivable, as members.	**a.** Right-click the *n***_Accounting** OU, point to **New**, and then click **Group**. **b.** In the **New Object – Group** dialog box, in the **Group name** box, type *n***_Domain Accountants** **c.** Ensure that **Group scope** is **Global** and **Group type** is **Security**, and then click **OK**. **d.** Click the *n***_Accounting** OU, in the details pane, right-click the *n***_Domain Accountants** global group, and then click **Properties**. **e.** In the *n***_Domain Accountants Properties** dialog box, click the **Members** tab, and then click **Add**.

Tasks	Detailed Steps
5. *(continued)*	**f.** In the **Select Users, Contacts, Computers, or Groups** dialog box, in the **Name** box, scroll to the bottom of the list and click *n*_**Accounts Payable**, click **Add**, click *n*_**Accounts Receivable**, click **Add**, and then click **OK**. **g.** In the *n*_**Domain Accountants Properties** dialog box, on the **Members** tab, ensure that *n*_Accounts Payable and *n*_Accounts Receivable are listed, and then click **OK**.
6. Within the *n*_Accounting OU, create the *n*_All Accountants universal security group and then add *n*_Domain Accountants as a member.	**a.** Right-click the *n*_**Accounting** OU, point to **New**, and then click **Group**. **b.** In the **New Object – Group** dialog box, in the **Group name** box, type *n*_**All Accountants** **c.** Under **Group scope**, click **Universal**, ensure **Group type** is set to **Security**, and then click **OK**. **d.** Click the *n*_**Accounting** OU, and in the details pane, right-click the *n*_**All Accountants** universal group, and then click **Properties**. **e.** In the *n*_**All Accountants Properties** dialog box, click the **Members** tab, and then click **Add**. **f.** In the **Select Users, Contacts, Computers, or Groups** dialog box, in the **Name** box, scroll to the bottom of the list and click *n*_**Domain Accountants**, click **Add**, and then click **OK**. **Note**: Typically a universal group contains members from multiple domains. Adding groups from other domains can be performed by selecting the domain in the Look in box, and selecting a group from the list. **g.** In the *n*_**All Accountants Properties** dialog box, on the **Members** tab, ensure that *n*_Domain Accountants is listed, and then click **OK**.
7. Create the *n*_Local Data domain local security group, and then add *n*_All Accountants as a member.	**a.** Right-click *n*_**Accounting**, point to **New**, and then click **Group**. **b.** In the **New Object – Group** dialog box, in the **Group name** box, type *n*_**Local Data** **c.** Ensure that **Group scope** is set to **Domain Local** and **Group type** is set to **Security**, and then click **OK**. **d.** Click the *n*_**Accounting** OU, in the details pane, right-click the *n*_**Local Data** domain local group, and then click **Properties**. **e.** In the *n*_**Local Data Properties** dialog box, on the **Members** tab, click **Add**. **f.** In the **Select Users, Contacts, Computers, or Groups** dialog box, in the **Name** box, scroll to the bottom of the list and click *n*_**All Accountants**, click **Add**, and then click **OK**. **g.** In the *n*_**Local Data Properties** dialog box, on the **Members** tab, ensure that *n*_All Accountants is listed as members of the *n*_**Local Data** domain local group, and then click **OK**.

Tasks	Detailed Steps
8. Create an empty text document C:\Report.txt and give Full Control permissions to only the *n*_Local Data domain local group.	**a.** In the **Run** box, type **C:** and then click **OK** to open the C:\ window. **b.** In the C:\ window, right-click an area of blank space, point to **New**, and then click **Text Document**. **c.** Rename the text document to **Report.txt**. **d.** Right-click **Report.txt**, and then click **Properties**. **e.** In the **Report Properties** dialog box, on the **Security** tab, and click **Add**. **f.** In the **Select Objects** dialog box, in the **Name** box, scroll to the bottom of the list and click *n*_**Local Data**, click **Add**, and then click **OK**. **g.** In the **Report Properties** dialog box, in the **Permissions** box, select the **Full Control Allow** check box. **h.** Clear the **Allow inheritable permissions from parent to propagate to this object** check box, and then click **Remove** to close the message asking whether to copy or remove the inherited permissions. **i.** Ensure that *n*_**Local Data** is the only entry and that it has Full Control permissions, and then click **OK**. **j.** Close the C:\ window.
9. Within the *n*_Accounting OU, create a user account with the following properties to test the group structure: • Full name: *n*_TestAccount • User logon name: *n*_TestAccount@nwtraders.msft • Add this user account to the *n*_Accounts Payable global group.	**a.** In Active Directory Users and Computers, click the *n*_**Accounting** OU. **b.** Right-click *n*_**Accounting**, point to **New**, and then click **User**. **c.** On the **New Object – User** page, in the **Full name** box, type *n*_**TestAccount** In the **User logon name** box, type *n*_**TestAccount** and then click **Next**. **d.** Click **Next**, and then click **Finish** to complete the wizard by using the defaults. **e.** Click the *n*_**Accounting** OU, and in the details pane, right-click the user *n*_**TestAccount**, and then click **Properties**. **f.** In the *n*_**TestAccount Properties** dialog box, on the **Member Of** tab, click **Add**. **g.** In the **Select Groups** dialog box, under the **Name** column, click *n*_**Accounts Payable**, click **Add**, and then click **OK**. **h.** In the *n*_**TestAccount Properties** dialog box, ensure the *n*_Accounts Payable global group is listed, and then click **OK**. **i.** Close Active Directory Users and Computers.
10. Log off from the domain controller, and then log on as *n*_TestAccount. Verify that you can gain access to the resource C:\Report.txt, and then delete the document.	**a.** Log off, and then log on as *n*_TestAccount in your domain without typing a password. **b.** Open the file, C:\Report.txt, and then type **Some Modifications** **c.** In this document, save and close the document. **d.** Delete the document C:\Report.txt.

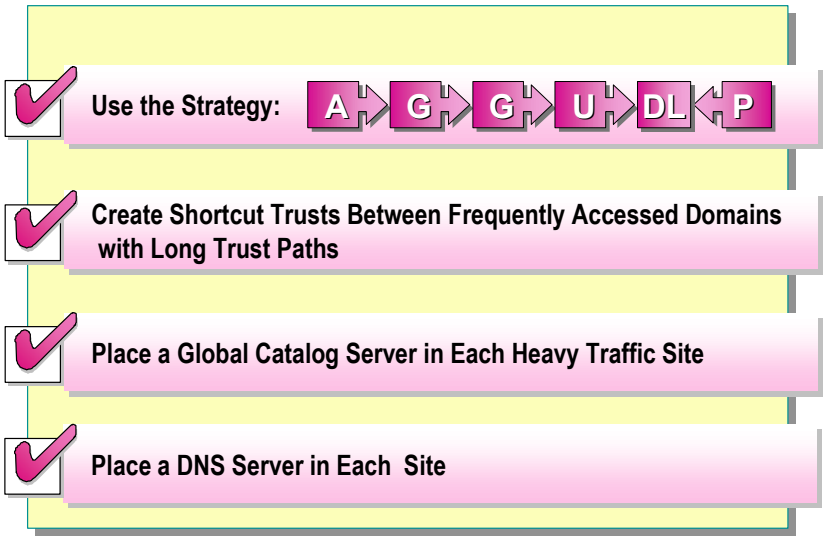
Tasks	Detailed Steps
Were you able to access the resource C:\Report.txt?	
11. Run C:\MOC\Win2154A\Labfiles\Mytoken.exe to determine which groups *n*_TestAccount has in its access token.	**a.** Open a command prompt window. **b.** At the command prompt, type **C:\MOC\Win2154A\Labfiles\Mytoken.exe** and then press ENTER. *The access token information appears. First, the information displays the user information and other general information about the access token. Second, it displays the group information one security identifier (SID) entry per line. Finally, privileges of the user are displayed.*
Does the access token for *n*_TestAccount contain the appropriate nested global groups, the universal group, and the domain local group following the membership path? Can you determine from the output of Mytoken which groups are nested?	
11. *(continued)*	**c.** Close the command prompt window.
12. Log off and log on as Administrator, delete the *n*_Accounting OU, and then log off.	**a.** Log off, and then log on as Administrator in your domain with a password of **password**. **b.** Open Active Directory Users and Computers from the **Administrative Tools** menu, and then expand *domain***.nwtraders.msft**. **c.** Right-click the *n*_**Accounting** OU, click **Delete**, click **Yes** to close the confirmation dialog box, and then click **Yes** to close the dialog box indicating that all of the objects contained in this object will also be deleted. **d.** Close Active Directory Users and Computers, close all open windows, and then log off.

Troubleshooting Creating and Managing Trees and Forests

You may encounter problems when creating and managing trees and forests in Windows 2000. Here are some of the common problems that you may encounter and some strategies for resolving them:

- Shortcut trust is not being used. The possible cause could be that the trust was created in the wrong direction. Verify that the trusting and trusted domains are correct. If they are not, then delete both halves of the existing shortcut trust and recreate the shortcut trust in the other direction. Verify that the trust is functioning by using the **Verify** button in Active Directory Domains and Trusts or the Netdom.exe utility.
- Cannot log on to a domain. The possible cause could be that a global catalog server could not be located. The global catalog is needed to access universal group information and map user principal names to domains. Ensure that a global catalog server is running and available. Ensure that the network is functioning correctly from the authenticating domain controller and a global catalog server. Ensure that the DNS service is functioning. Also, verify the entries for global catalog servers in DNS to make sure that they are correct. The Global Catalog SRV record exists in the forest root domain only.
- Cannot create universal groups in some domains. The possible cause could be that the domains where you cannot create universal groups may not be in native mode. Verify the domain mode, and if required, change the domain mode from mixed mode to native mode, and then create universal groups.

Best Practices



Consider the following best practices for creating and managing Windows 2000 trees and forests:

- Use the A➔G➔G➔U➔DL➔P group strategy. Keep membership in universal groups small, and use memberships that do not change often to reduce network replication traffic. This solution is recommended for file and print permissions and Active Directory permissions in the domain naming context. It is recommended that you use the A➔G➔U➔P group strategy for Configuration naming context in Active Directory and attribute permissions for attributes published to the global catalog.
- Create shortcut trusts when many users from one domain frequently access resources in a domain with long trust paths. Shortcut trusts reduce the latency and network traffic needed to authenticate a user for the resource.
- Place a global catalog server in each site that has many users logging on to reduce network traffic and allow users to log on if the WAN link fails.
- Place a DNS server at each site. A DNS server must exist at each site so that local domain controllers and global catalog servers can be found if a WAN link fails. The DNS server must contain a replica of the forest root domain zone to enable users to find global catalog resource records.

Review

- Introduction to Trees and Forests
- Creating Trees and Forests
- Trust Relationships in Trees and Forests
- The Global Catalog
- Strategies for Using Groups in Trees and Forests
- Troubleshooting Creating and Managing Trees and Forests
- Best Practices

1. What role does the forest root domain play when new trees are created in the forest?

2. Why would you create shortcut trusts?

3. What role does the global catalog play during the logon process?

4. What is the benefit of small and relatively static membership for a universal group?

5. The three domains in your network correspond to different branches of your organization in North America, Asia, and Europe respectively. Accountants in the three domains need to gain access to documents in all three domains. How do you set up the accountants' access to documents in all domains?