Learnthat
Because great minds learn a lot

Introduction to Active Directory

Learn Active Directory and Get Ahead

By Jeremy Reis, MBA

Install, Configure, and Maintain Active Directory

Introduction to Active Directory

Copyright © 2011 by Jeremy Reis, Learnthat.com

All Rights Reserved. This content is for personal use only and may not resell it or republish it.

No patent liability is assumed with respect to the use of information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors and omissions. Neither is any liability assumed for damages resulting from the use of information contained herein.

Published in the United States.

Table of Contents

What is Active Directory?

Active Directory (AD) is a technology created by Microsoft to provide network services including LDAP directory services, Kerberos based authentication, DNS naming, secure access to resources, and more. Active Directory uses a single Jet database which a variety of services and applications can use to access and store a variety of information. Active Directory is used by system administrators to store information about users, assign security policies, and deploy software. AD is used in many different types and size of environments from the very small (a dozen users) to hundreds of thousands of users in a global environment.

In this tutorial, you will learn the basic structure of Active Directory, gain an understanding of how Active Directory works, learn how to install Active Directory, and learn the components of AD.

This tutorial is divided into these sections:

What is Active Directory: An overview of Active Directory and its use in technology environments.

Active Directory Structure: Learn the basics of AD, its components (such as domains, domain controllers, trust relationships, forests, organizational units, etc), hierarchies within AD, and DNS.

How to Install Active Directory: Active Directory installation is not complex in its process, but can be difficult in the future if you do not plan the installation correctly. Learn the tricks and tips you need to know to properly plan an AD installation and why administrators install AD the way they do.

This free Active Directory tutorial is not a comprehensive one on the topic, but an introduction to Active Directory and its structure and use.

Who is This Tutorial For?

This tutorial is focused at junior system administrators and PC technicians, though it can be used by anyone seeking to increase their knowledge about Active Directory and how it works. This tutorial will teach you the building blocks of Active Directory and how to install Active Directory. If you are pursuing an IT career, this tutorial is a good step toward system administration and architecture.

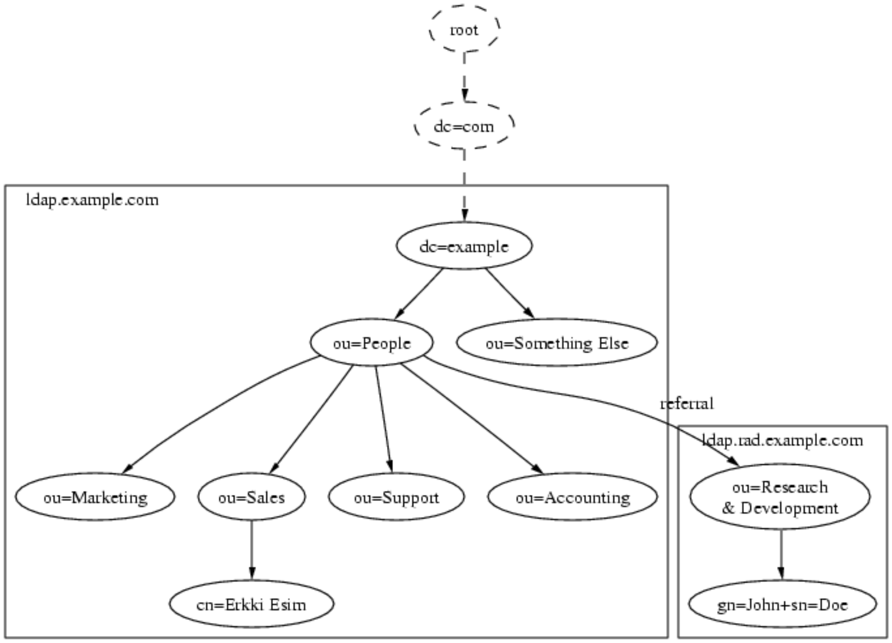
History of Active Directory

Active Directory was introduced to the world in the mid-1990s by Microsoft as a replacement for Windows NT-style user authentication. Windows NT included a flat and non-extensible domain model which did not scale well for large corporations. Active Directory, on the other hand, was created as a true *directory service* versus a flat user-management service that NT had. Though it was introduced in the 1990s, it did not become a part of the Operating System until Windows 2000 Server was released in 2000. Since then, Windows Server 2003 and Server 2008 have been introduced and Active Directory has gone under some expansion.

This tutorial is based on Windows Server 2003 as it is currently the most widely installed version of the Windows network Operating System (NOS), though in the future we will release versions for Windows Server 2008 and future Windows releases as it becomes necessary. Though this tutorial is not focused on Windows Server 2008, much of the basic knowledge and instruction relates to either OS.

LDAP

Active Directory is based loosely on LDAP – Lightweight Directory Access Protocol – an application protocol for querying and modifying directory services developed at the University of Michigan in the early 1990s. An LDAP directory tree is a hierarchical structure of organizations, domains, trees, groups, and individual units.



Example of an LDAP Tree

Active Directory is a Directory

Sometimes, it’s easy to get lost in all of the technology and functions that are provided with AD and forget that Active Directory is a *directory*. It is a directory in both the common use of the term like a white pages (you can add in a person’s first name, last name, phone number, address, email address, etc) and a directory of information for use by applications and services (such as Microsoft Exchange for email). AD is functionally a place to store information about people, things (computers, printers, etc), applications, domains, services, security access permissions, and more. Applications and services then use the *directory* to perform a function.

For example, Microsoft Windows uses Active Directory information to allow a user to login to their computer and provide access to the security rights assigned in Active Directory. Windows is accessing the directory and then providing rights based on what it finds. If a user account is disabled in Active Directory, the directory itself is just setting a flag which Windows uses to disallow a user from logging in.

We mentioned in the introduction that administrators use Active Directory to deploy software – this is an incomplete description. Administrators can set policies and information that a certain software application should be deployed to a certain user – AD itself does not deploy the software, but a Windows service reads the information from Active Directory and then installs the software.

Once you grasp the concept that Active Directory is a *directory*, you're halfway to understanding why it is built the way it is!

Active Directory Structure

Unlike Windows NT, Active Directory is designed for you to create a functional and usable hierarchy for your environment. Not only does this make the environment look cleaner, but it also allows central system administrators to delegate specific authority over areas to other administrators, team members, and groups. AD has a very flexible structure, allowing you to build a hierarchy in whatever way you wish – one big unit, broken down by geographic location, by department, by astronomical sign, or however you desire.

Achieving this flexibility in hierarchical design is a defined structure. The structure of Active Directory starts with forests and domains and goes down to organizational units and individual objects (such as a user or computer account). The flexibility in hierarchical design is a benefit to network architects, but if you do not design the structure correctly in the beginning, it can be a nightmare down the road. We recommend spending a lot of time thinking about the best hierarchical structure for your Active Directory environment before diving in and building it.

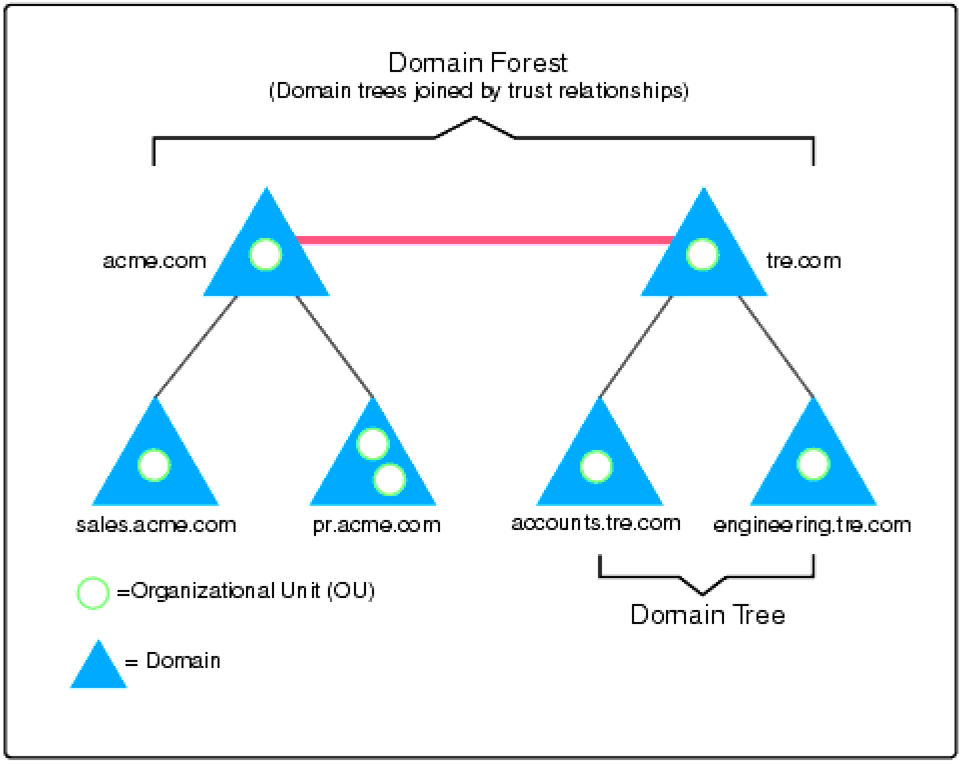
In this section, we are going to look at the basic building blocks of Active Directory – all those things which make it such a flexible directory service.

Basic Active Directory Components

At its core, Active Directory needs structure to work properly. It provides the basic building blocks for people to build their own directory. These basic building blocks of Active Directory include domains, domain controllers, trusts, forests, organizational units, groups, sites, replication, and the global catalog.

Understanding Forests

At the top of the Active Directory structure is a *forest*. A forest holds all of the objects, organizational units, domains, and attributes in its hierarchy. Under a forest are one or more trees which hold domains, OUs, objects, and attributes.



As illustrated in this image, there are two trees in the forest. You might use a structure like this for organizations with more than one operating company.

You could also design a structure with multiple forests, but these are for very specific reasons and not common.

Domains

At the heart of the Active Directory structure is the *domain*. The domain is typically of the Internet naming variety (e.g. Learnthat.com), but you are not forced to stick with this structure – you could technically name your domain whatever you wish.

Microsoft recommends using as few domains and possible in building your Active Directory structure and to rely on Organizational Units for structure. Domains can contain multiple nested OUs, allowing you to build a pretty robust and specific structure.

Domain Controllers

In Windows NT, domains used a Primary Domain Controller (PDC) and Backup Domain Controller (BDC) model. This had one server, the PDC, which was “in charge” while the other DCs where subservient. If the PDC failed, you had to promote a BDC to become the PDC and be the server in charge.

In Active Directory, you have multiple Domain Controllers which are equal peers. Each DC in the Active Directory domain contains a copy of the AD database and synchronizes changes with all other DCs by *multi-master replication*. Replication occurs frequently and on a *pull* basis instead of a *push* one. A server requests updates from a fellow domain controller. If information on one DC changes (e.g. a user changes their password), it sends signal to the other domain controllers to begin a pull replication of the data to ensure they are all up to date.

Servers not serving as DCs, but in the Active Directory domain, are called 'member servers.'

Active Directory requires at least one Domain Controller, but you can install as many as you want (and it's recommended you install at least two domain controllers in case one fails).

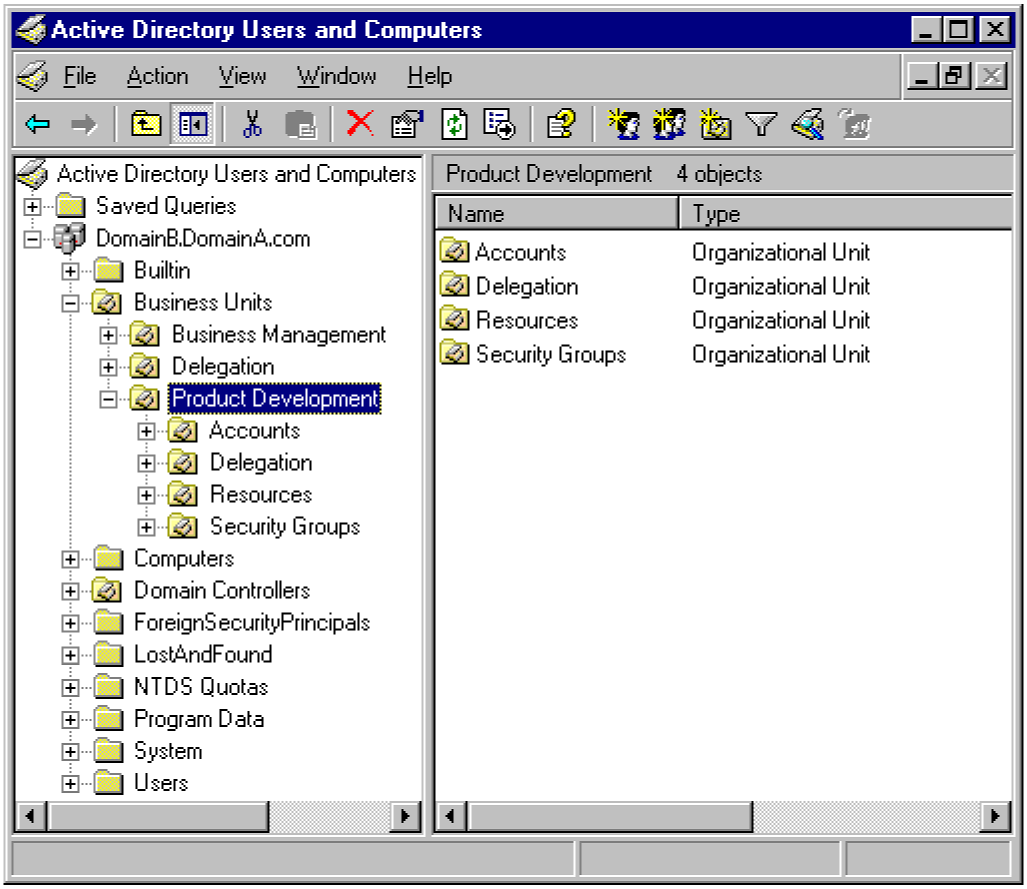
Trust Relationships

Trust Relationships are important in an Active Directory environment so forests and domains can communicate with one another and pass credentials. Within a single forest, trusts are created when a domain is created. By default, domains have an implicit two-way transitive trust created. This means each domain trusts each other for security access and credentials. A user in domain A can access resources permitted to him in domain B while a user in domain B can access resources permitted to her in domain A.

AD allows several different types of trusts to be created, but understanding the two-way transitive trust is the most important to understanding AD.

Organizational Units

An Organizational Unit (OU) is a container which gives a domain hierarchy and structure. It is used for ease of administration and to create an AD structure in the company's geographic or organizational terms.



- Active Directory Users and Computers
  - Saved Queries
  - DomainB.DomainA.com
    - Builtin
    - Business Units
      - Business Management
      - Delegation
      - Product Development
        - Accounts
        - Delegation
        - Resources
        - Security Groups
    - Computers
    - Domain Controllers
    - ForeignSecurityPrincipals
    - LostAndFound
    - NTDS Quotas
    - Program Data
    - System
    - Users

Product Development 4 objects

Name	Type
Accounts	Organizational Unit
Delegation	Organizational Unit
Resources	Organizational Unit
Security Groups	Organizational Unit

Organizational Units

An OU can contain OUs, allowing for the creating of a multi-level structure, as shown in the image above. There are three primary reasons for creating OUs:

Organizational Structure: First, creating OUs allows a company to build a structure in Active Directory which matches their firm’s geographic or organizational structure. This permits ease of administration and a clean structure.

Security Rights: The second reason to create an OU structure is to assign security rights to certain OUs. This, for example, would allow you to apply Active Directory Policies to one OU which are different than another. You could setup policies which install an accounting software application on computers in the Accounting OU.

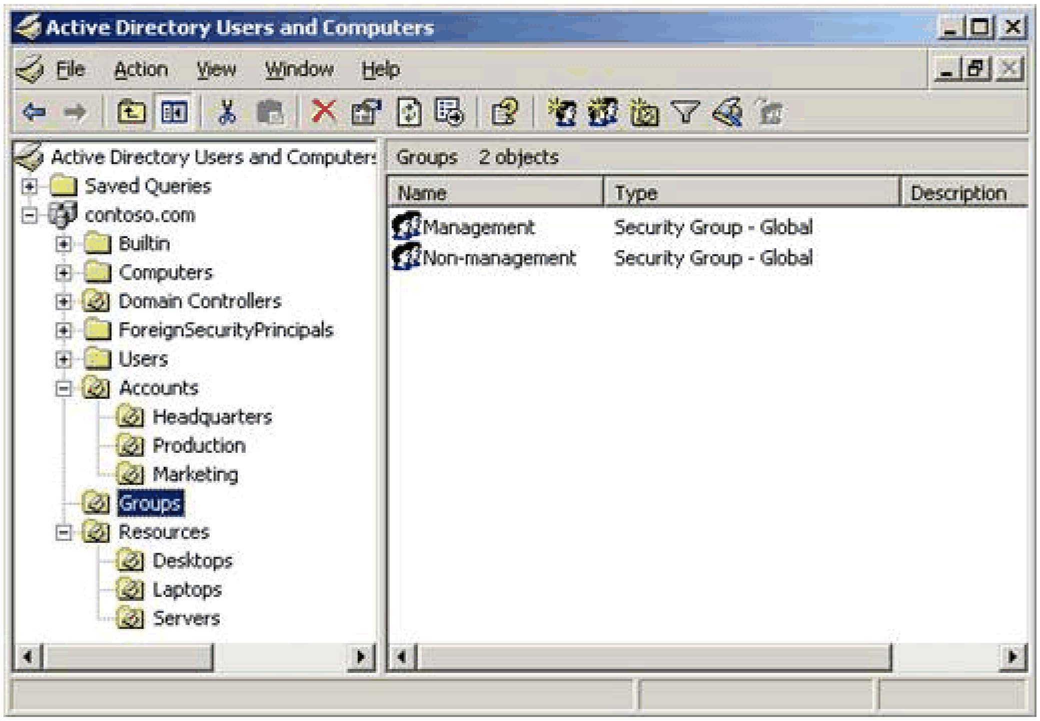
Delegated Administration: The third reason to create OUs is to delegate administrative responsibility. AD Architects can design the structure to allow local administrators certain administrative responsibility for their OU and no other. This allows for a delegated administration not available in Windows NT networks.

Groups

Groups serve two functions in Active Directory: security and distribution.

A **security** group contains accounts which can be used for security access. For example, a security group could be assigned rights to a particular directory on a file server.

A **distribution** group is used for sending information to users. It cannot be used for security access.



Name	Type	Description
Management	Security Group - Global	
Non-management	Security Group - Global	

There are three group scopes:

Global: Global scope security groups contains users only from the domain in which is created. Global security groups can be members of both Universal and Domain Local groups.

Universal: Universal scope security groups can contain users, global groups, and universal groups from any domain. These groups are typically used in a multi-domain environment if access is required across domains.

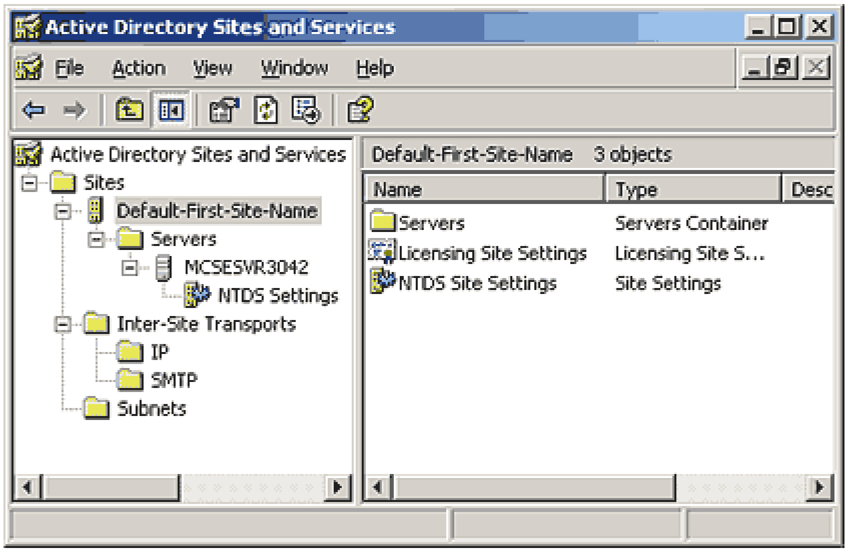
Domain Local: Domain Local scope groups are often created in domains to assign security access to a particular local domain resource. Domain Local scope groups can contain user accounts, universal groups, and global groups from any domain. Domain Local scope groups can contain domain local groups in the same domain.

Sites

An Active Directory site object represents a collection of IP subnets, usually constituting a physical Local Area Network (LAN). Multiple sites are connected for replication by site links. Typically, sites are used for:

Physical Location Determination: Enables clients to find local resources such as printers, shares, or domain controllers.

Replication: You can optimize replication between domain controllers by creating links.



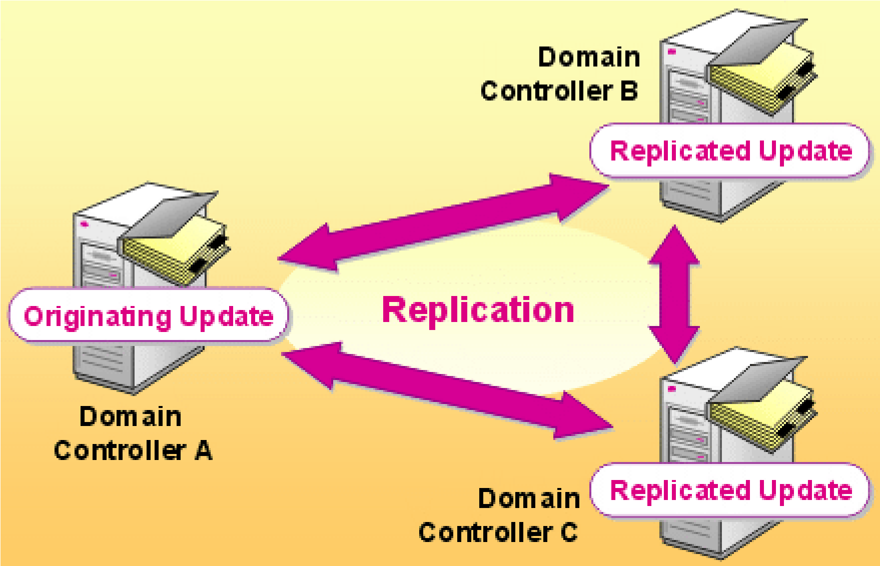
Name	Type	Desc
Servers	Servers Container	
Licensing Site Settings	Licensing Site S...	
NTDS Site Settings	Site Settings	

By default, Active Directory uses automatic site coverage, though you can purposefully setup sites and resources.

Replication

Since most Active Directory networks contain multiple domain controllers and users could theoretically attach to any DC for authentication or information, each of the servers needs to be kept up to date. Domain Controllers stay up to date by replicating the database between each other. It performs this using a *pull* method – a server requests new information from a different DC frequently. After a change, the DC initiates a replication after waiting 15 seconds (in Windows 2003) or 5 minutes (in Windows 2000). Windows Server 2003 uses technology to only replicate changed information and compressions replication over WAN links.

Windows Server sets up a replication topology to determine where a server updates from. In a large network, this keeps replication time down as servers replicate in a form of a ring network.



Active Directory uses *multi-master replication*. Multimaster replication does not rely on a single primary domain controller, but instead treats each DC as an authority. When a change is made on any DC, it is replicated to all other DCs. Although each DC is replicated alike, all of the DCs aren't *equal*. There are several *flexible single-master operation* roles which are assigned to one domain controller at a time.

AD uses Remote Procedure Calls (RPC) for replication and can use SMTP for changes to schema or configuration.

FSMO Roles

All domain controllers are not equal. We know, it's hard to hear. You've spent this whole time reading this tutorial thinking that all DCs are created equal and now we have to burst your bubble. Some DCs have more responsibility than others. It's just part of life!

There are five roles which are called operations masters, or flexible single-master operations (FSMOs). Two are forestwide roles and three are domainwide roles. The forestwide roles are:

Schema master: Controls update to the Active Directory schema.

Domain naming master: Controls the addition and removal of domains from the forest.

The three domainwide roles are:

RID master: Allocates pools of unique identifier to domain controllers for use when creating objects. (RID is relative identifier).

Infrastructure master: Synchronizes cross-domain group membership changes. The infrastructure master cannot run on a global catalog server, unless all of the DCs are global catalog servers.

PDC Emulator: Provides backward compatibility for NT 4 clients for PDC operations – such as a password change. The PDC also serves as the master time server.

Global Catalog

As a network gets larger, it can contain multiple domains and many domain controllers. Each domain only contains records from its own domain in its AD database to keep the database small and replication manageable. The Active Directory domain relies on a **global catalog** database which contains a global listing of all objects in the forest. The Global Catalog is held on DCs configured as *global catalog servers*.

The global catalog contains a subset of information – such as a user's first name and last name – and the *distinguished name* of the object so your client can contact the proper domain controller if you need more information. The distinguished name is the full address of an object in the directory. For example, a printer in the OU Accounting in the Learnthat.com domain might have a distinguished name of:

CN=AcctLaser1,OU=Accounting,DC=Learnthat,DC=com

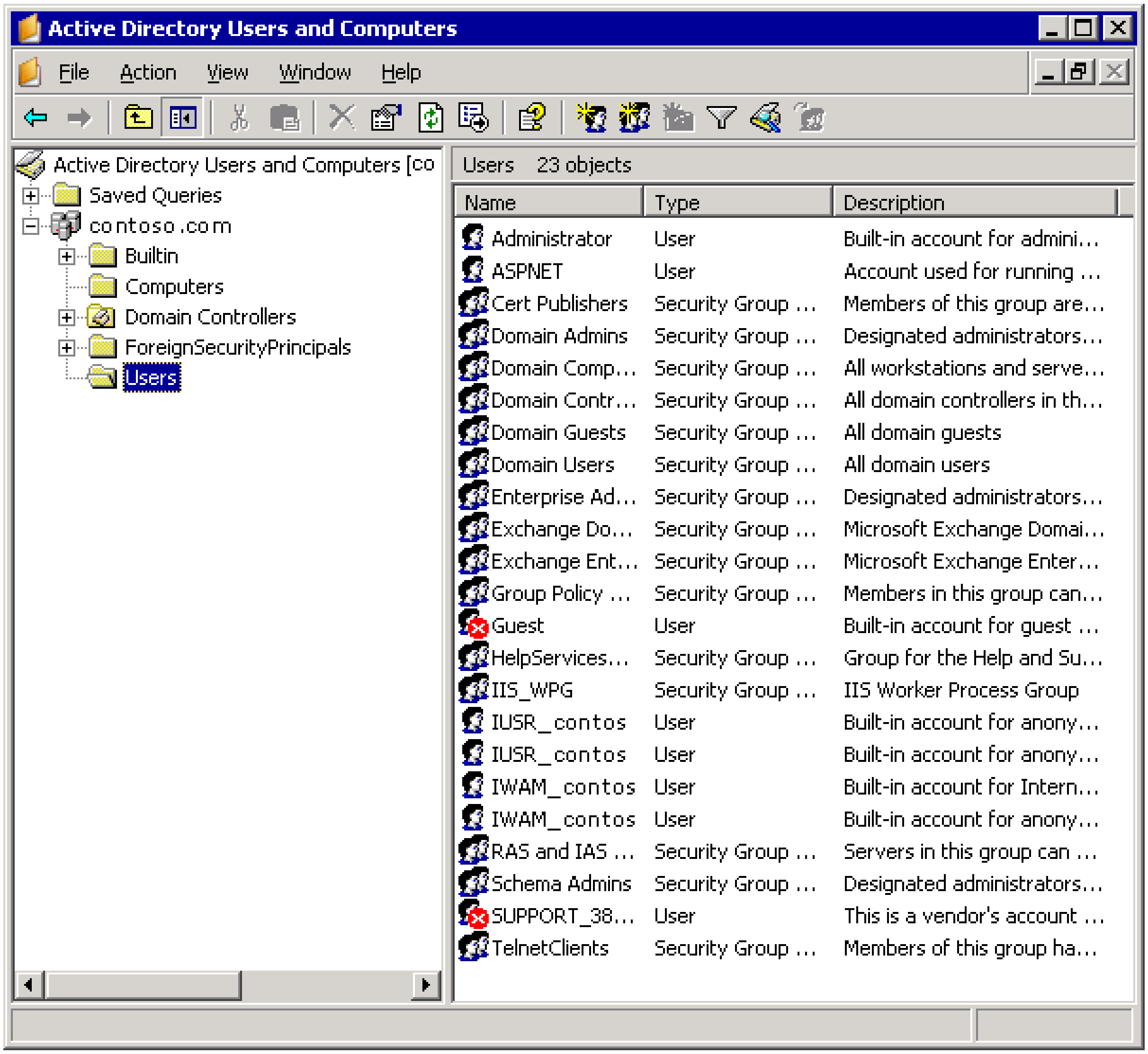
The GC database is only a subset of the entire database called the Partial Attribute Set (PAS), containing 151 of the 1,070 properties available in Windows Server 2003. You can define additional properties for replication to the GC by modifying schema.

Active Directory Hierarchies

Now that you understand the building blocks of Active Directory, you can start to understand how to build a hierarchy in Active Directory. One of the foundations of design for AD has been a flexibility to allow companies to build a structure which fits into their organization. This flexibility allows organizations of all sizes to use Active Directory to meet their needs.

Domains and OUs

The most basic design of an Active Directory is a single forest, single domain, no Organizational Unit design.


Active Directory Users and Computers
File
Action
View
Window
Help
Active Directory Users and Computers [co
Saved Queries
contoso.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

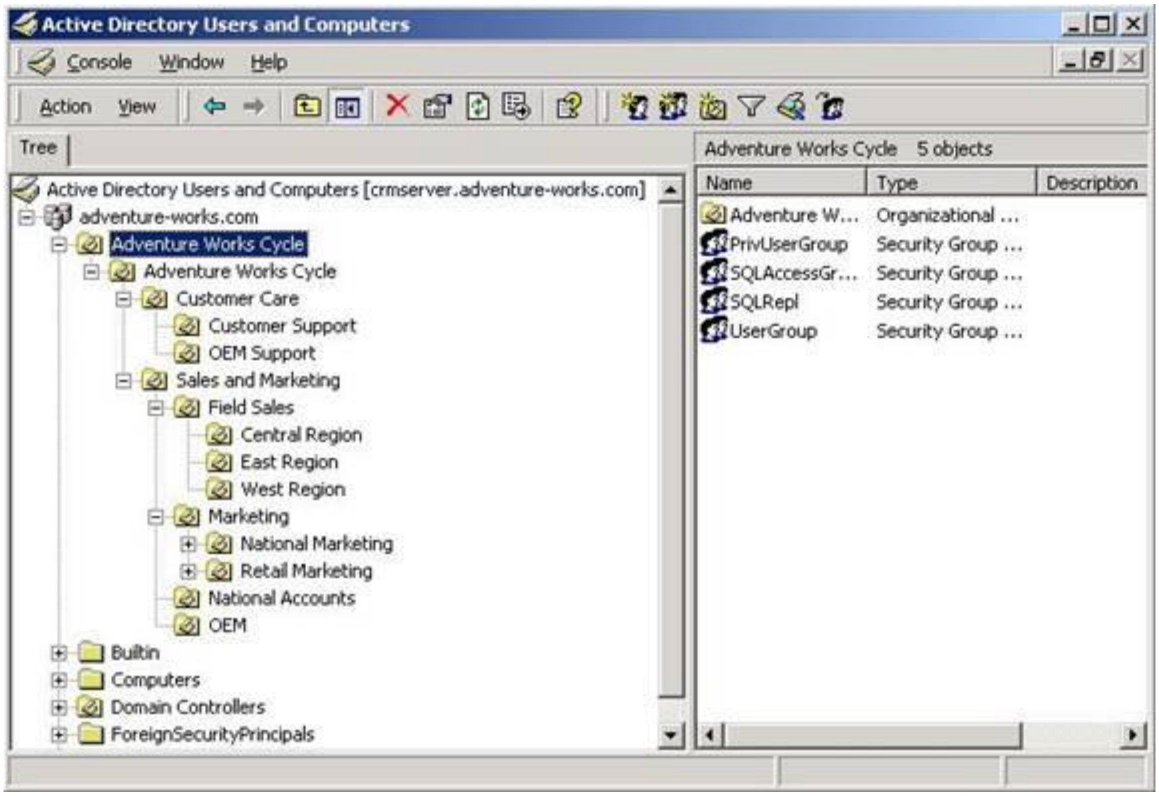
Users 23 objects

Name	Type	Description
Administrator	User	Built-in account for admini...
ASPNET	User	Account used for running ...
Cert Publishers	Security Group ...	Members of this group are...
Domain Admins	Security Group ...	Designated administrators...
Domain Comp...	Security Group ...	All workstations and serve...
Domain Contr...	Security Group ...	All domain controllers in th...
Domain Guests	Security Group ...	All domain guests
Domain Users	Security Group ...	All domain users
Enterprise Ad...	Security Group ...	Designated administrators...
Exchange Do...	Security Group ...	Microsoft Exchange Domai...
Exchange Ent...	Security Group ...	Microsoft Exchange Enter...
Group Policy ...	Security Group ...	Members in this group can...
Guest	User	Built-in account for guest ...
HelpServices...	Security Group ...	Group for the Help and Su...
IIS_WPG	Security Group ...	IIS Worker Process Group
IUSR_contos	User	Built-in account for anony...
IUSR_contos	User	Built-in account for anony...
IWAM_contos	User	Built-in account for Intern...
IWAM_contos	User	Built-in account for anony...
RAS and IAS ...	Security Group ...	Servers in this group can ...
Schema Admins	Security Group ...	Designated administrators...
SUPPORT_38...	User	This is a vendor's account ...
TelnetClients	Security Group ...	Members of this group ha...

Basic AD Installation

For a small organization, this might be adequate, but almost every organization can benefit from some structure.

Creating multiple domains is not always the best design solution, so Microsoft created *organizational units* in Active Directory which can be nested to provide hierarchical control of your AD environment. It is a great idea to think about and map out your OU design before committing it into Active Directory.



Name	Type	Description
Adventure W...	Organizational ...	
PrivUserGroup	Security Group ...	
SQLAccessGr...	Security Group ...	
SQLRepl	Security Group ...	
UserGroup	Security Group ...	

Typically, companies design their OU trees based on either geographic separation (e.g. Americas, EMEA, PacificRim) or based on organizational design (e.g. Accounting, Marketing, Technology, Sales). There is no incorrect way to design your AD environment, however, consistency should be key. You shouldn’t mix the two design methods and have a top level Americas OU and a top level Sales OU. Doing so makes administration difficult as you won’t know where a particular salesperson’s account is.

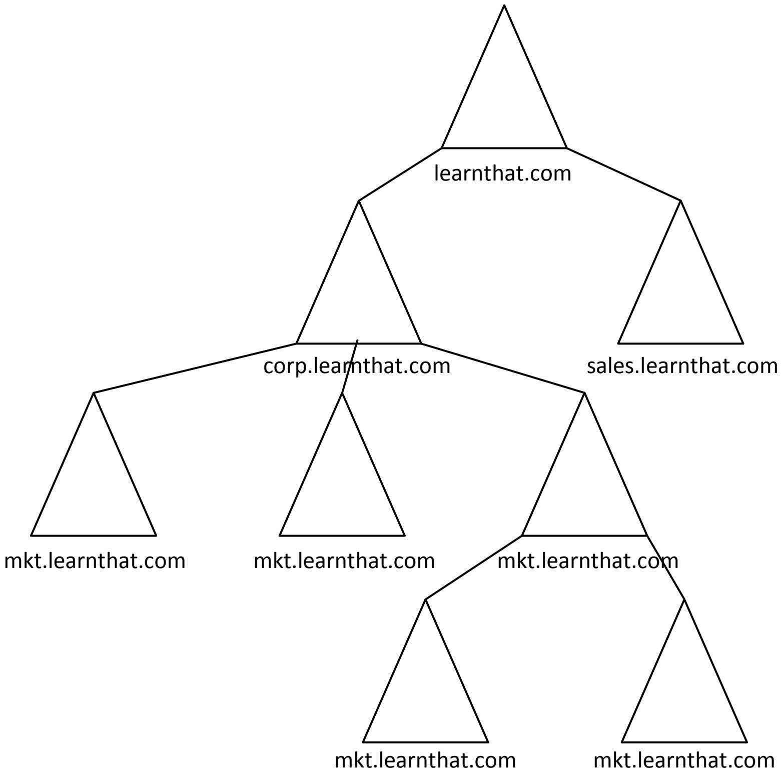
Also, remember that OUs allow enterprise administrators to delegate administration responsibility to local teams. Building an effective OU design will allow you to properly delegate authority.

The other reason OUs are used is to apply *policies*. Policies are rules for security, access, and functionality which can apply to several different containers in Active Directory. Frequently, policies are applied by OU – so though you might separated geographically (and therefore want to set up your structure based solely on geography), it might make more sense to setup your AD by organizational divisions. Why? Because if all of your marketing employees need the same software and settings, you will setup policies based on the department instead of the physical location of the employees.

Domain Trees

Once an organization becomes large and you cannot have the entire AD database replicated everywhere, it might make sense to move to a **domain tree**. A domain tree allows an organization to become more decentralized as it is more independent than using an OU tree.

Domain-wide policies can be changed per domain in a domain tree which is not possible with only an OU structure. Policies such as minimum and maximum password age, minimum password length, and account lockout are domain-wide policies and cannot be changed on a per-OU basis. By creating multiple domains, administrators can set these policies for each domain.



Domain Tree

In the illustration above, learnthat.com has a domain tree in the Active Directory domain.

Forest of Domain Trees

In more complex environments, a company may use multiple domain trees in a single forest. This might be a large operating company with multiple subsidiaries – each requiring their own domain, for example, ThatNetwork.com is the parent company and subsidiaries might include

Learnthat.com, Romancetips.com, Exampractice.com. This structure makes sense if you have different administrative staff for each domain, along with different policies and different security requirements.

You can still setup trusts between the domains to allow users to authenticate for resources in either domain.

Multiple Forests

The last possibility is using multiple forests. This is the less frequent design choice, but can be used with you want an absolute separation for one reason or another. This structure is most often found when companies merge or in the case of acquisitions. In Windows 2003, you can setup forest trusts between forests to allow some access.

DNS

Active Directory is integrated with Domain Naming System (DNS) and requires it to be present to function. DNS is the naming system used for the Internet and on many Intranets. You can use DNS which is built into Windows 2000 and newer, or use a third party DNS infrastructure such as BIND if you have it in the environment. It is recommended you use Window's DNS service as it is integrated into Windows and provides the easiest functionality.

AD uses DNS to name domains, computers, servers, and locate services.

A DNS server maps an object's name to its IP address. For example, on the Internet, it is used to map a domain name (such as www.learnthat.com) to an IP address (such as 64.34.165.234). In an Active Directory network, it is used not only to find domain names, but also objects and their IP address. It also uses *service location records* (SRV) to locate services.

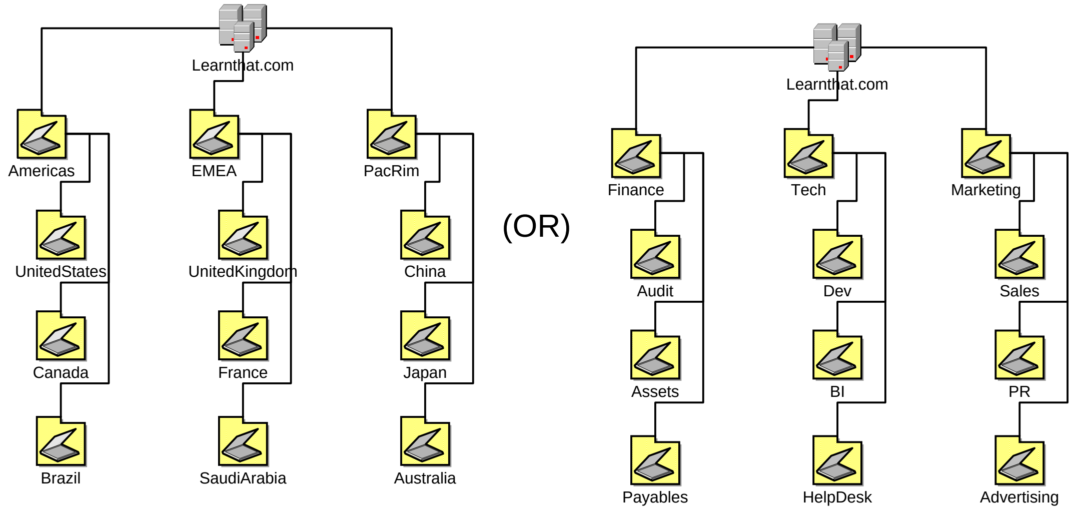
Active Directory Installation

Some larger organizations take months (and in some cases, over a year) to plan a proper Active Directory design and get input from a global organization of technology leaders. It is extremely important to give a lot of thought to your AD design to ensure it meets your organization's needs.

Choosing Your AD Layout

As we mentioned earlier, there are many ways you can structure your Active Directory. From a top level down perspective, most companies either start with a geographic separation or a organizational structure separation, for example Americas, EMEA, PacificRIM for geographic or Accounting, Marketing, Technology, Sales for organizational structure. It does not matter which you select: either will provide a fine starting point for your domain structure, but you need to ensure you pick one direction and be consistent with your choices.

Many organizations start with geography at the top level, then break down into business units or departments underneath that top level. It is important to write naming conventions and standards down so a team in Europe does not call an OU "SalesMarketing" while a team in North America calls an OU "Sales." Consistency provides for an efficient and manageable Active Directory layout.



There are many different combinations you could choose when designing your AD structure.

Installation Requirements

In this section, we will look at the installation requirements of Active Directory. Installing AD isn't a complex process, but the design and configuration can be.

Here are the requirements for installing Active Directory on Windows Server 2003:

- An NTFS partition with enough free space
- An Administrator's username and password
- NIC with Network Connection
- Properly configured TCP/IP (IP address, subnet mask and - optional - default gateway)
- An operational DNS server (which can be installed on the DC itself)
- A Domain name that you want to use
- Windows Server 2003 CD media or the i386 Folder

Functional Levels

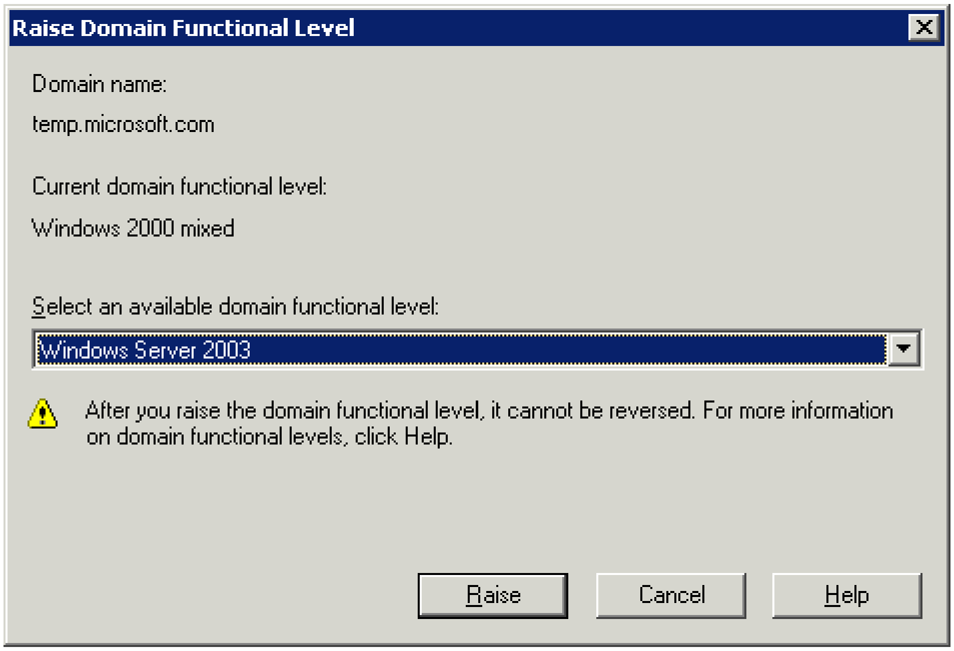
In Windows 2000, you chose from two levels: mixed mode or native mode. When Windows 2000 Server was introduced, NT 4 was still a popular server option. To ensure backward compatibility with these servers and clients, Windows 2000 defaulted to mixed mode where you could add Windows NT 4 servers to the Windows 2000 Active Directory domain.

Windows Server 2003 introduced functional levels - a set level of backward compatibility for previous operating systems. If you are in an environment with NT 4 servers and Windows 2000 servers which are still accessed, you can set a functional level to ensure backwards compatibility.

Windows 2003 expands from those two modes to one of many domain functional levels including Windows 2000 Mixed, Windows 2000 Native, Windows Server 2003 Interim, and Windows Server 2003. Also, in Windows Server 2003, you have three forest functional levels available: Windows 2000, Windows Server 2003 Interim, or Windows server 2003. Each functional level brings new features available and lose compatibility with some set of servers or clients.

By default, Windows Server 2003 starts at Windows 2000 Mixed functional level. Not all of the features of 2003 are available in this mode, so if you are designing a new Windows 2003 AD environment, you will want to take advantage of the new features added in Windows Server 2003.

In Windows 2000, we referred to this change as “changing the mode,” but in Windows 2003, we now raise the functional level with either *Active Directory Users and Computers* or *Domains and Trusts*.



Raise Domain Functional Level

Domain name:

temp.microsoft.com

Current domain functional level:

Windows 2000 mixed

Select an available domain functional level:

Windows Server 2003

After you raise the domain functional level, it cannot be reversed. For more information on domain functional levels, click Help.

This change cannot be reversed – once you make a decision to raise the functional level, you cannot go back to a lower functional level.

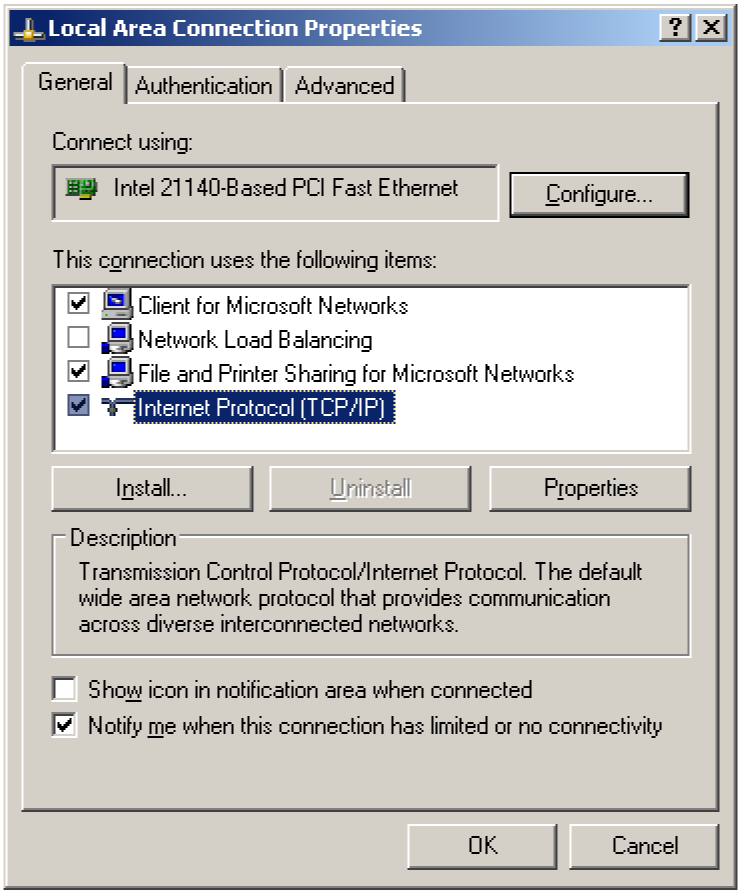
Installing Active Directory

Please note: these installation instructions are for a brand new domain – not for adding a server as a member server or domain controller in an existing domain. Following these instructions in a production network is not recommended.

We are going to review the AD installation process from a clean install of Windows Server 2003. You may have already set some of these settings, so look through the steps and perform any tasks you have failed to do.

Set Network Settings

1. This server will be both a domain controller and a DNS server, so we are going to set a static IP address.
2. Click **Start**, **Control Panel**, **Network Connections** and select your network connection.
3. Click **Properties**.



Connect using:

Intel 21140-Based PCI Fast Ethernet

This connection uses the following items:

- ☑ Client for Microsoft Networks
- □ Network Load Balancing
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol (TCP/IP)

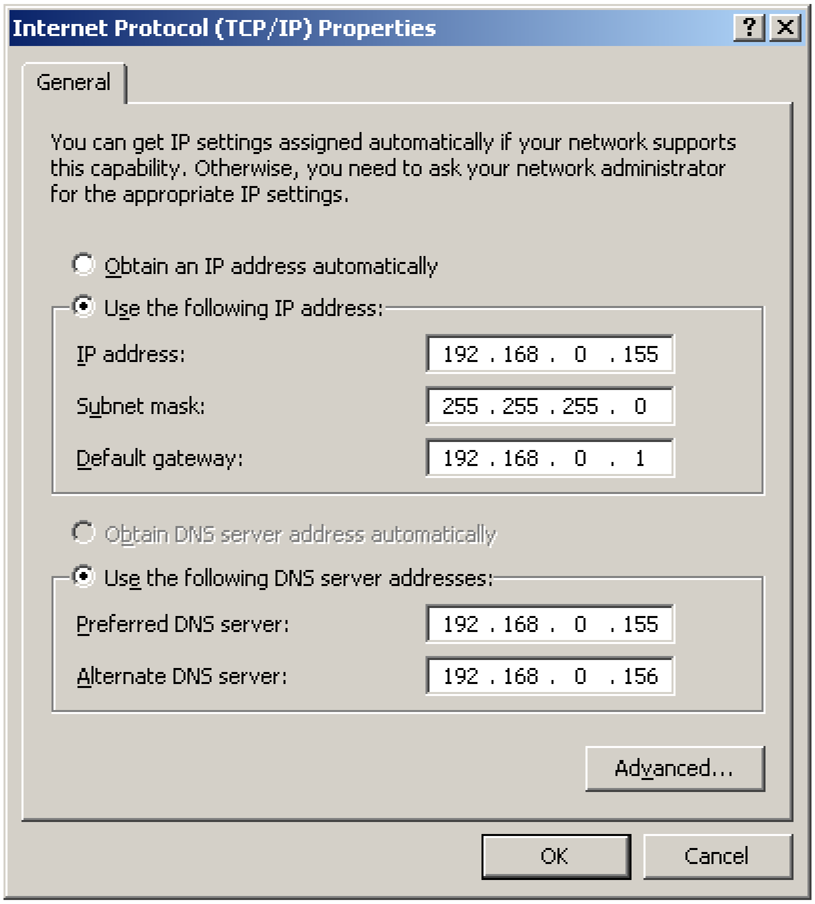
Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

□ Show icon in notification area when connected

☑ Notify me when this connection has limited or no connectivity

4. Click **Internet Protocol (TCP/IP)** and click **Properties**.


Internal Protocol (TCP/IP) 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: 192 . 168 . 0 . 155

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

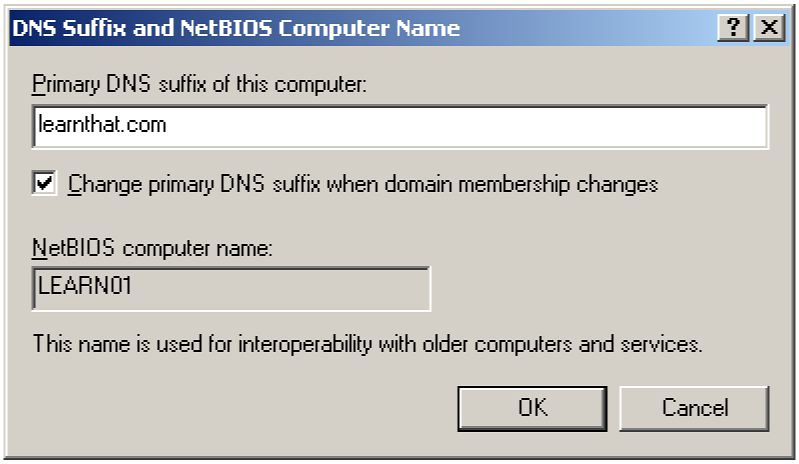
○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 155

Alternate DNS server: 192 . 168 . 0 . 156

5. Enter in your static IP address information and preferred DNS servers. Notice one of the DNS servers I listed is the server itself – this will be a DNS server in a minute.
6. Click **OK**.
7. Click **Close**.
8. Click **Close.**
9. Click **Start**. Right-click on **My Computer** and select **Properties**.
10. Click on the **Computer Name** tab.
11. Click on the **More** button.



DNS Suffix and NetBIOS Computer Name

Primary DNS suffix of this computer:

learnthat.com

☑ Change primary DNS suffix when domain membership changes

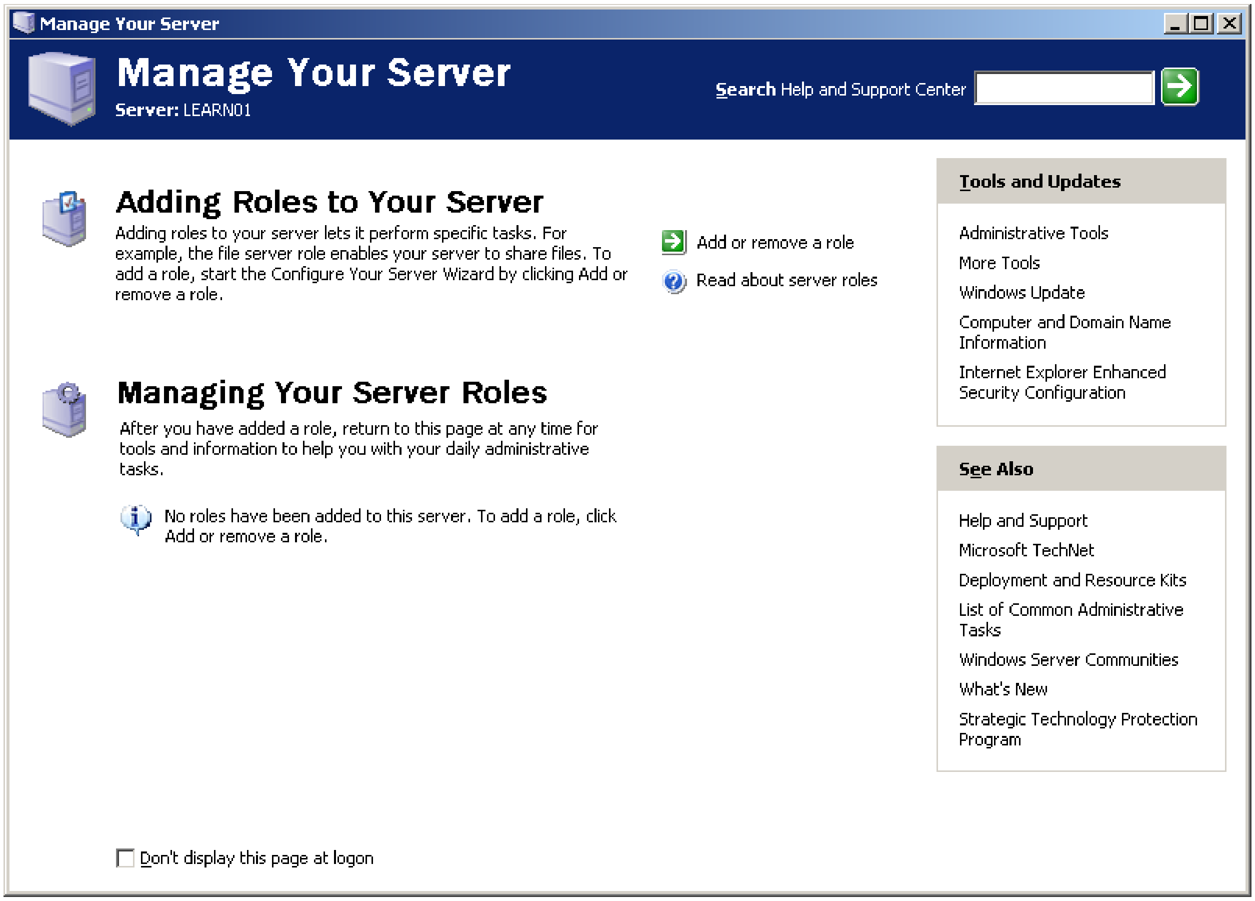
NetBIOS computer name:

LEARN01

This name is used for interoperability with older computers and services.

12. Enter in the domain name you are going to be using for your AD domain in the *Primary DNS suffix of this computer* text field.
13. Click **OK**.
14. Click **OK**. Acknowledge that you have to reboot and click **OK**.
15. Click **Yes** to the prompt asking you if you want to reboot.

Install the DNS Service



Manage Your Server

Manage Your Server

Server: LEARN01

Adding Roles to Your Server

Adding roles to your server lets it perform specific tasks. For example, the file server role enables your server to share files. To add a role, start the Configure Your Server Wizard by clicking Add or remove a role.

Managing Your Server Roles

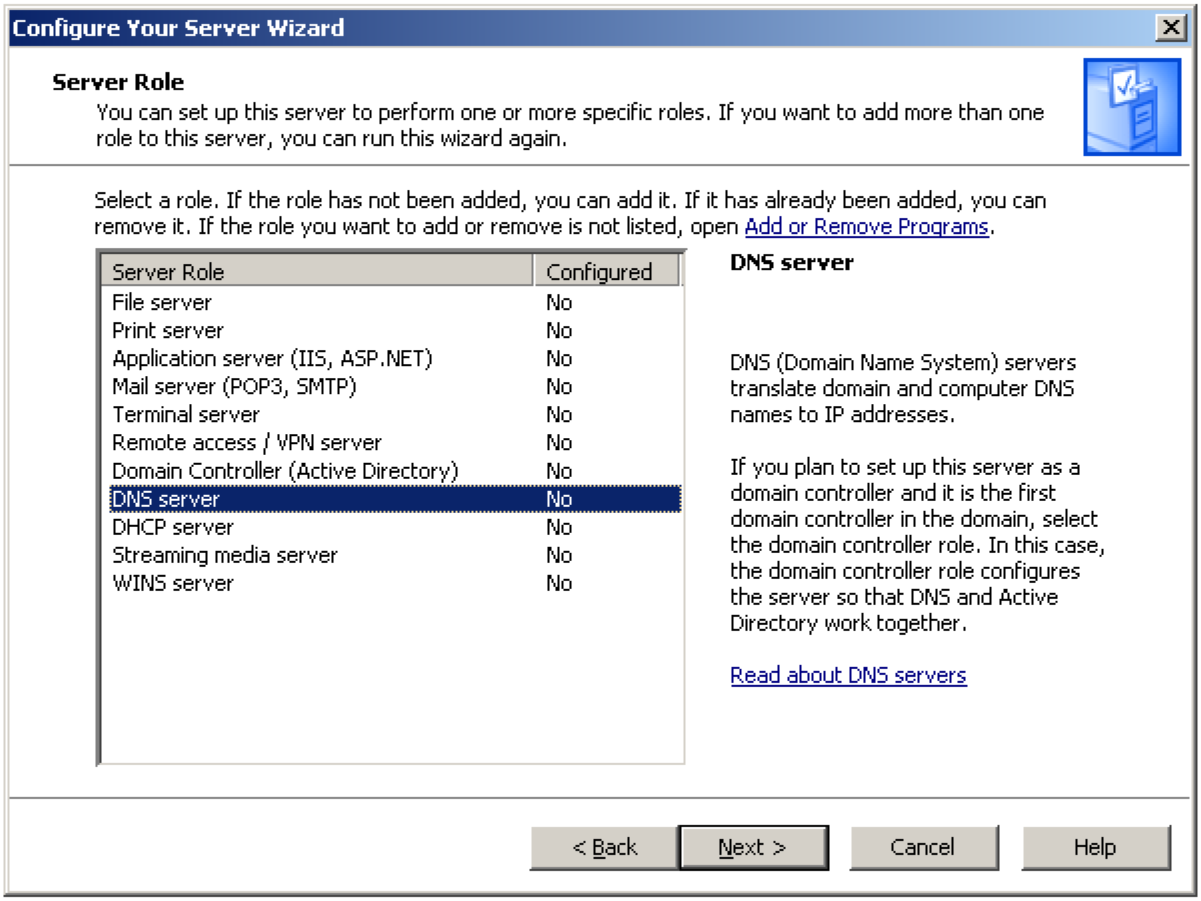
After you have added a role, return to this page at any time for tools and information to help you with your daily administrative tasks.

No roles have been added to this server. To add a role, click Add or remove a role.

□ Don't display this page at logon

Search Help and Support Center
Add or remove a role
Read about server roles
Tools and Updates
Administrative Tools
More Tools
Windows Update
Computer and Domain Name Information
Internet Explorer Enhanced Security Configuration
See Also
Help and Support
Microsoft TechNet
Deployment and Resource Kits
List of Common Administrative Tasks
Windows Server Communities
What's New
Strategic Technology Protection Program

16. On the *Manage Your Server* window, select **Add or remove a role.** (Don't see this window at startup? Find it at **Start > All Programs > Administrative Tools > Manage Server**)
17. Click **Next**.



Server Role

You can set up this server to perform one or more specific roles. If you want to add more than one role to this server, you can run this wizard again.

Select a role. If the role has not been added, you can add it. If it has already been added, you can remove it. If the role you want to add or remove is not listed, open Add or Remove Programs.

Server Role	Configured
File server	No
Print server	No
Application server (IIS, ASP.NET)	No
Mail server (POP3, SMTP)	No
Terminal server	No
Remote access / VPN server	No
Domain Controller (Active Directory)	No
DNS server	No
DHCP server	No
Streaming media server	No
WINS server	No

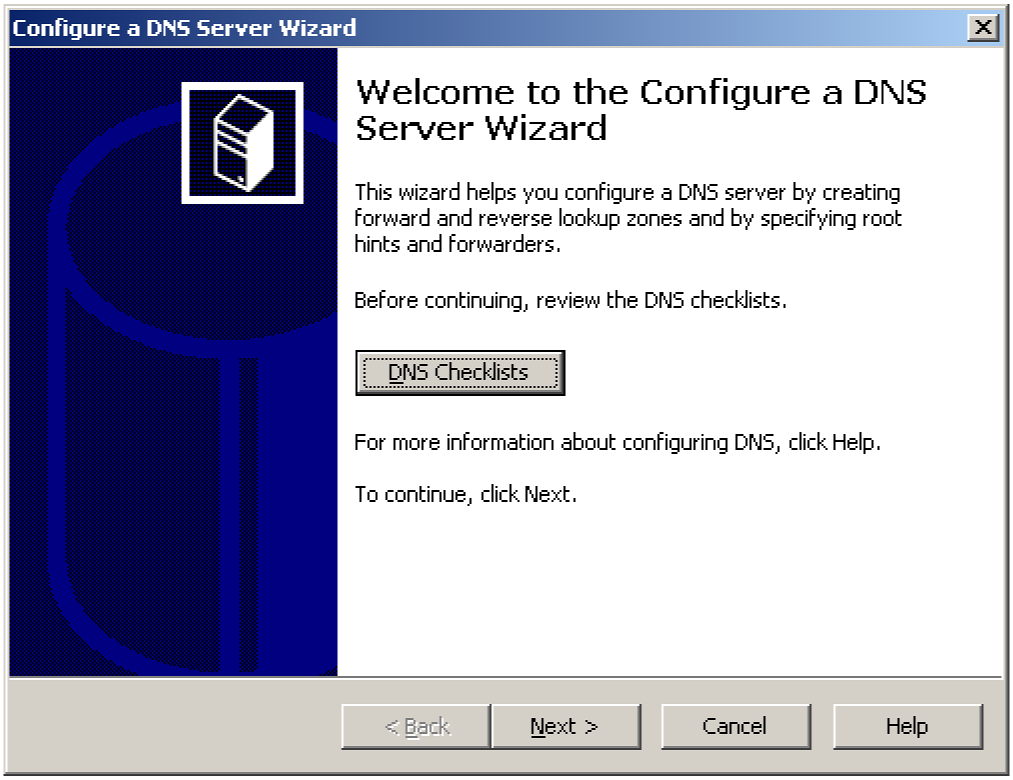
DNS server

DNS (Domain Name System) servers translate domain and computer DNS names to IP addresses.

If you plan to set up this server as a domain controller and it is the first domain controller in the domain, select the domain controller role. In this case, the domain controller role configures the server so that DNS and Active Directory work together.

Read about DNS servers

18. Click **DNS Server** and click **Next**.
19. Click **Next**.
20. Insert your Windows Server 2003 setup cd and click **OK**.
21. Navigate to where the i386 folder is and click **OK**.



Configure a DNS Server Wizard

Welcome to the Configure a DNS Server Wizard

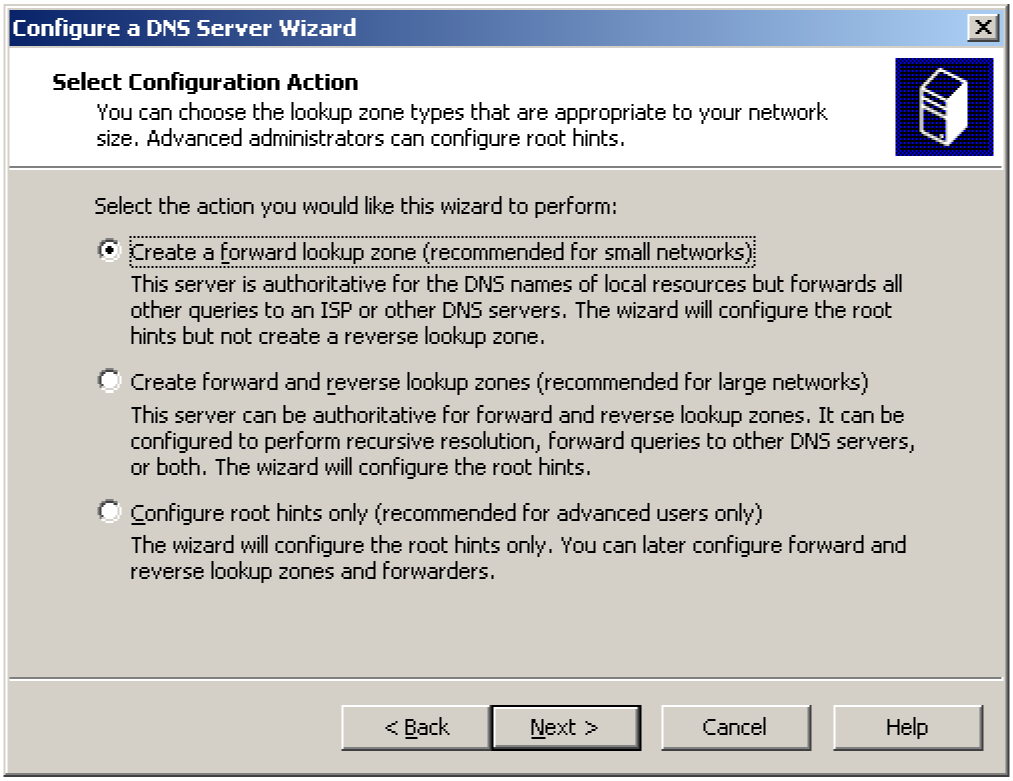
This wizard helps you configure a DNS server by creating forward and reverse lookup zones and by specifying root hints and forwarders.

Before continuing, review the DNS checklists.

For more information about configuring DNS, click Help.

To continue, click Next.

22. Click **Next** to start the DNS wizard.



Configure a DNS Server Wizard

Select Configuration Action

You can choose the lookup zone types that are appropriate to your network size. Advanced administrators can configure root hints.

Select the action you would like this wizard to perform:

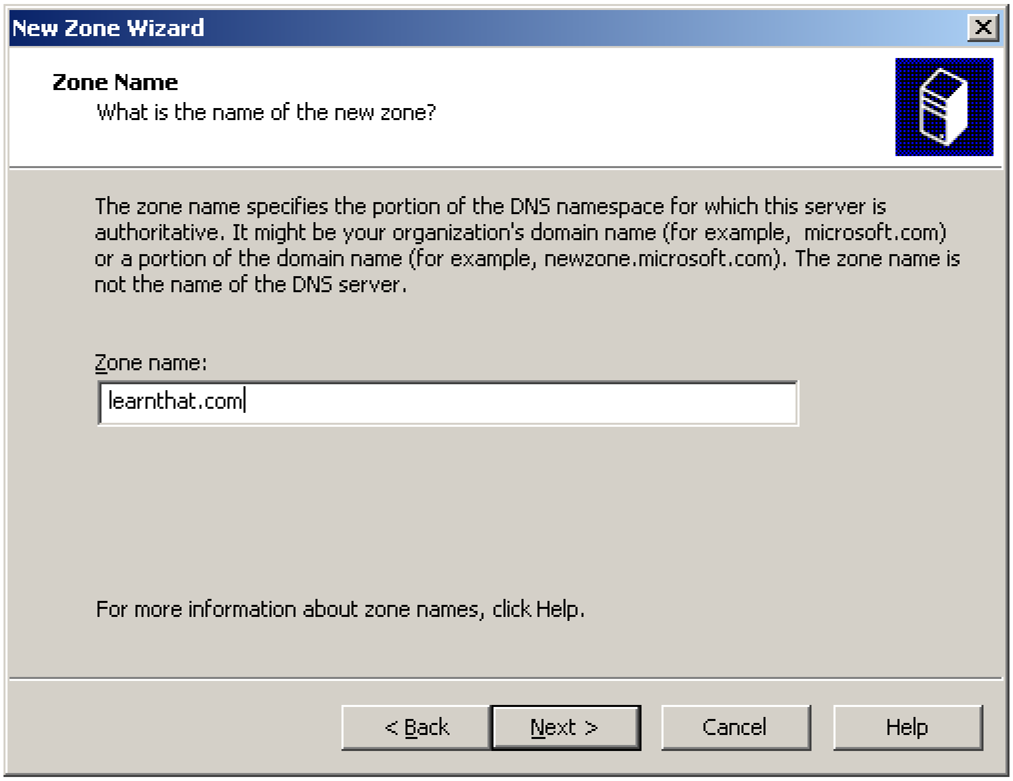
● Create a forward lookup zone (recommended for small networks)
This server is authoritative for the DNS names of local resources but forwards all other queries to an ISP or other DNS servers. The wizard will configure the root hints but not create a reverse lookup zone.

○ Create forward and reverse lookup zones (recommended for large networks)
This server can be authoritative for forward and reverse lookup zones. It can be configured to perform recursive resolution, forward queries to other DNS servers, or both. The wizard will configure the root hints.

○ Configure root hints only (recommended for advanced users only)
The wizard will configure the root hints only. You can later configure forward and reverse lookup zones and forwarders.

23. Click **Next** to create a forward lookup zone.

24. Click **Next** that this server retains a the zone.



New Zone Wizard

Zone Name

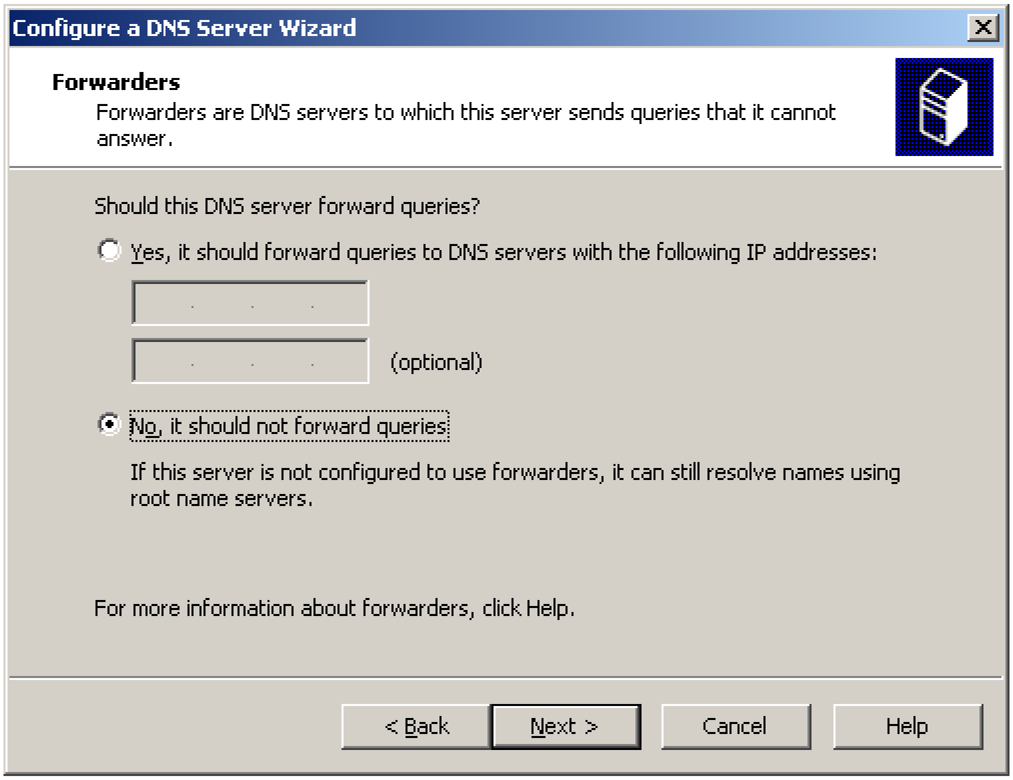
What is the name of the new zone?

The zone name specifies the portion of the DNS namespace for which this server is authoritative. It might be your organization's domain name (for example, microsoft.com) or a portion of the domain name (for example, newzone.microsoft.com). The zone name is not the name of the DNS server.

Zone name: learnthat.com

For more information about zone names, click Help.

25. Name your zone with your domain name. Click **Next**.
26. Accept the default filename and click **Next**.
27. Click **Allow both nonsecure and secure dynamic updates.** Click **Next**.



Configure a DNS Server Wizard

Forwarders

Forwarders are DNS servers to which this server sends queries that it cannot answer.

Should this DNS server forward queries?

○ Yes, it should forward queries to DNS servers with the following IP addresses:

(optional)

● No, it should not forward queries

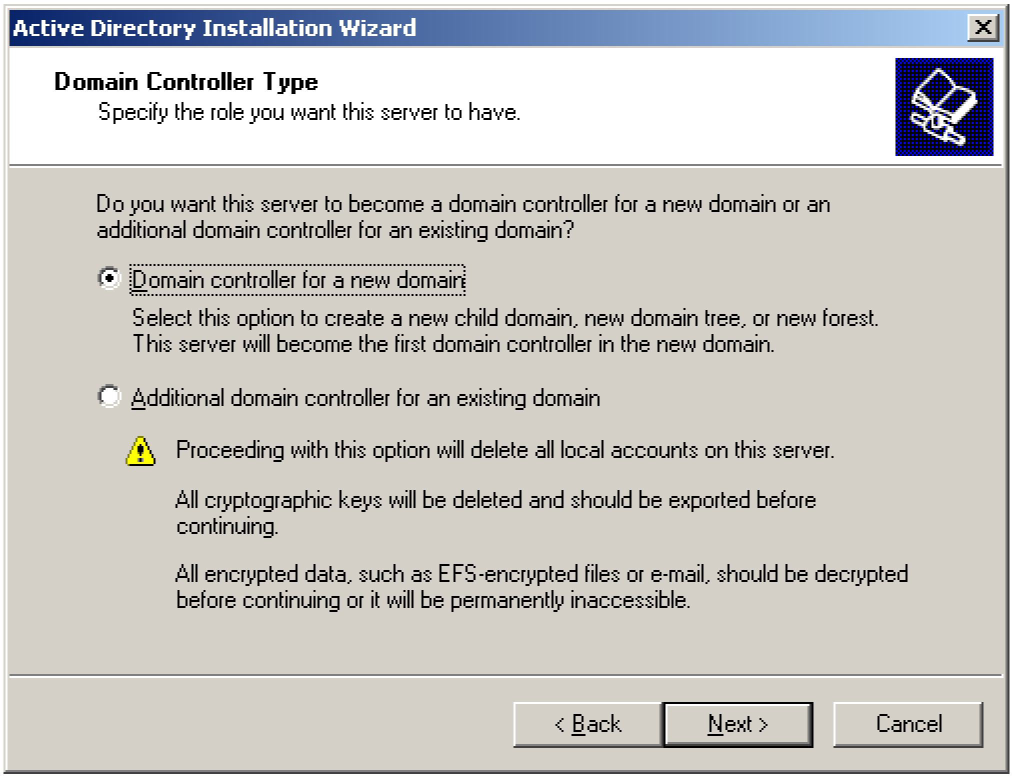
If this server is not configured to use forwarders, it can still resolve names using root name servers.

For more information about forwarders, click Help.

28. Select whether or not this DNS server should forward queries. If you use an ISP for DNS resolution for Internet sites, enter in your ISP's DNS servers in the first option. If this DNS server will resolve all queries, select the second option. Click **Next**.
29. Click **Finish**.
30. Click **Finish**.
31. Congratulations! You have setup a DNS server!

Setting Up Active Directory

32. On the *Manage Your Server* window, click **Add or remove a role**.
33. Click **Next**.
34. Select **Domain Controller (Active Directory)** and click **Next**.
35. Click **Next**.
36. Click **Next** when the Active Directory wizard opens.
37. Click **Next**.



Domain Controller Type

Specify the role you want this server to have.

Do you want this server to become a domain controller for a new domain or an additional domain controller for an existing domain?

● Domain controller for a new domain

Select this option to create a new child domain, new domain tree, or new forest. This server will become the first domain controller in the new domain.

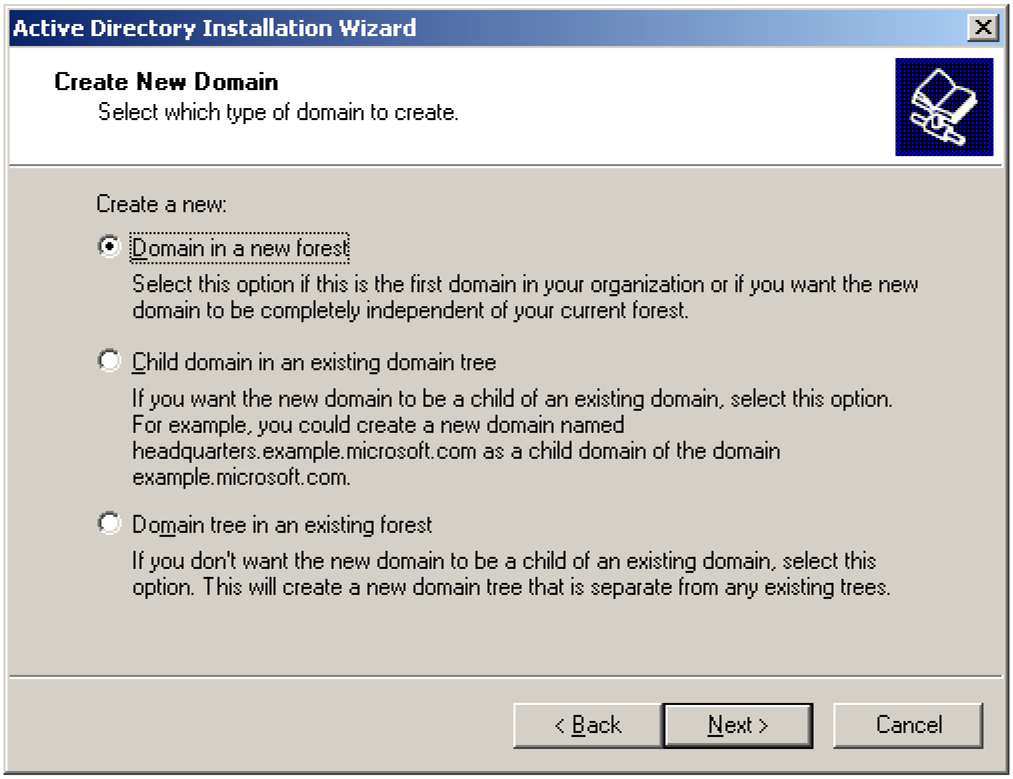
○ Additional domain controller for an existing domain

Proceeding with this option will delete all local accounts on this server.

All cryptographic keys will be deleted and should be exported before continuing.

All encrypted data, such as EFS-encrypted files or e-mail, should be decrypted before continuing or it will be permanently inaccessible.

38. Click **Next**.



Create New Domain

Select which type of domain to create.

Create a new:

● Domain in a new forest

Select this option if this is the first domain in your organization or if you want the new domain to be completely independent of your current forest.

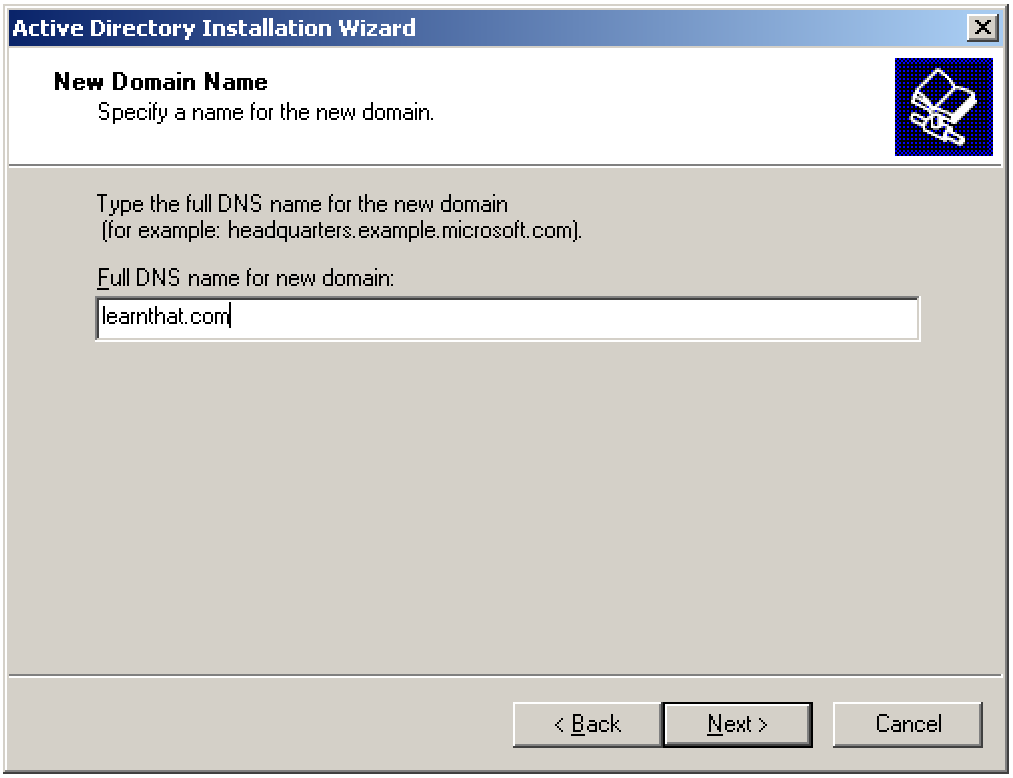
○ Child domain in an existing domain tree

If you want the new domain to be a child of an existing domain, select this option. For example, you could create a new domain named headquarters.example.microsoft.com as a child domain of the domain example.microsoft.com.

○ Domain tree in an existing forest

If you don't want the new domain to be a child of an existing domain, select this option. This will create a new domain tree that is separate from any existing trees.

39. Click **Next**.



Active Directory Installation Wizard

New Domain Name

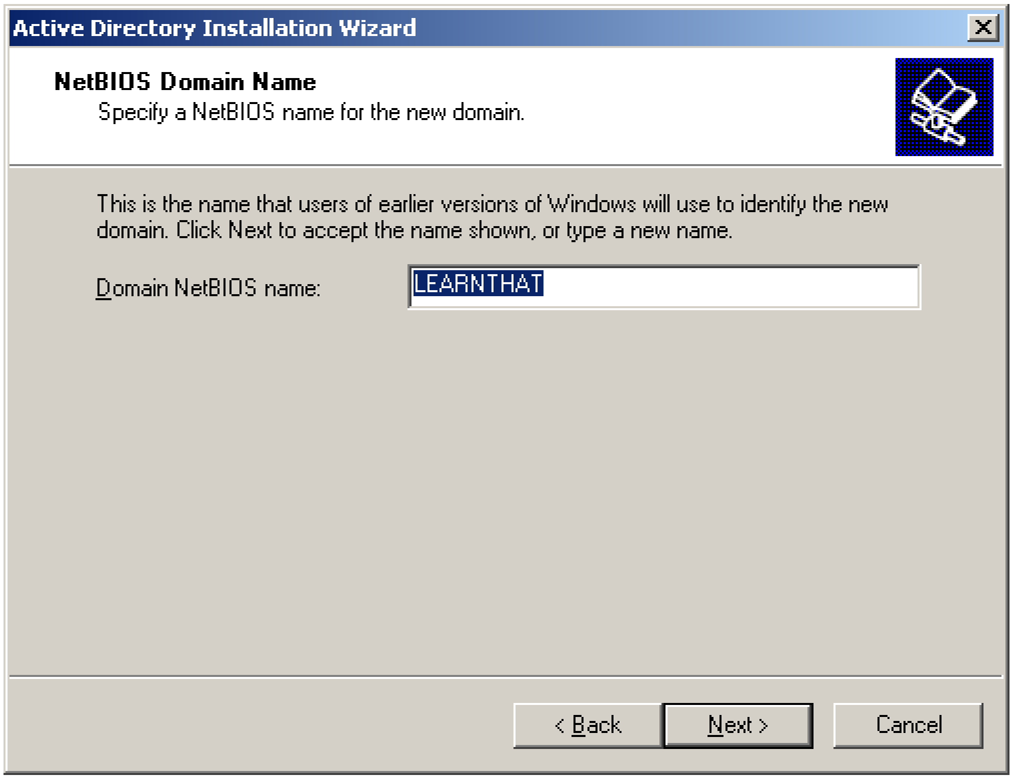
Specify a name for the new domain.

Type the full DNS name for the new domain
(for example: headquarters.example.microsoft.com).

Full DNS name for new domain:

learnthat.com

40. Enter in your domain name and click **Next**.



Active Directory Installation Wizard

NetBIOS Domain Name

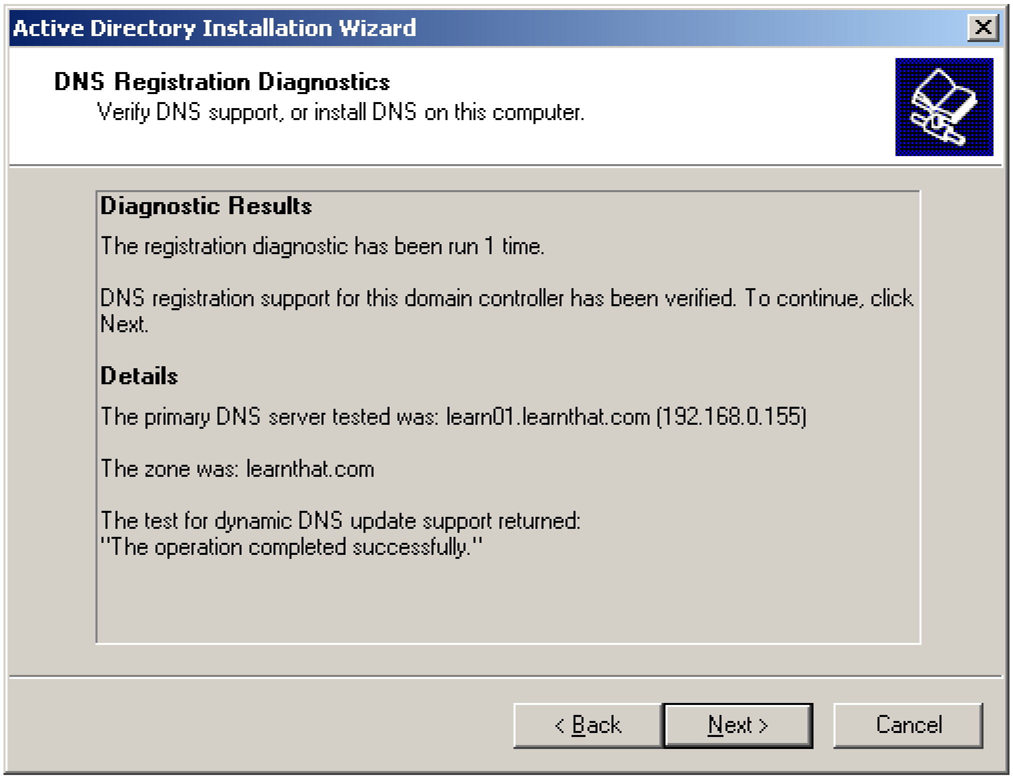
Specify a NetBIOS name for the new domain.

This is the name that users of earlier versions of Windows will use to identify the new domain. Click Next to accept the name shown, or type a new name.

Domain NetBIOS name: LEARNTHAT

41. Enter in a NetBIOS name or accept the default and click **Next**.

42. Click **Next** to accept the default locations for the database and log, or select a location for these files.
43. Enter a location for the *Shared System Volume* and click **Next**.



DNS Registration Diagnostics

Verify DNS support, or install DNS on this computer.

Diagnostic Results

The registration diagnostic has been run 1 time.

DNS registration support for this domain controller has been verified. To continue, click Next.

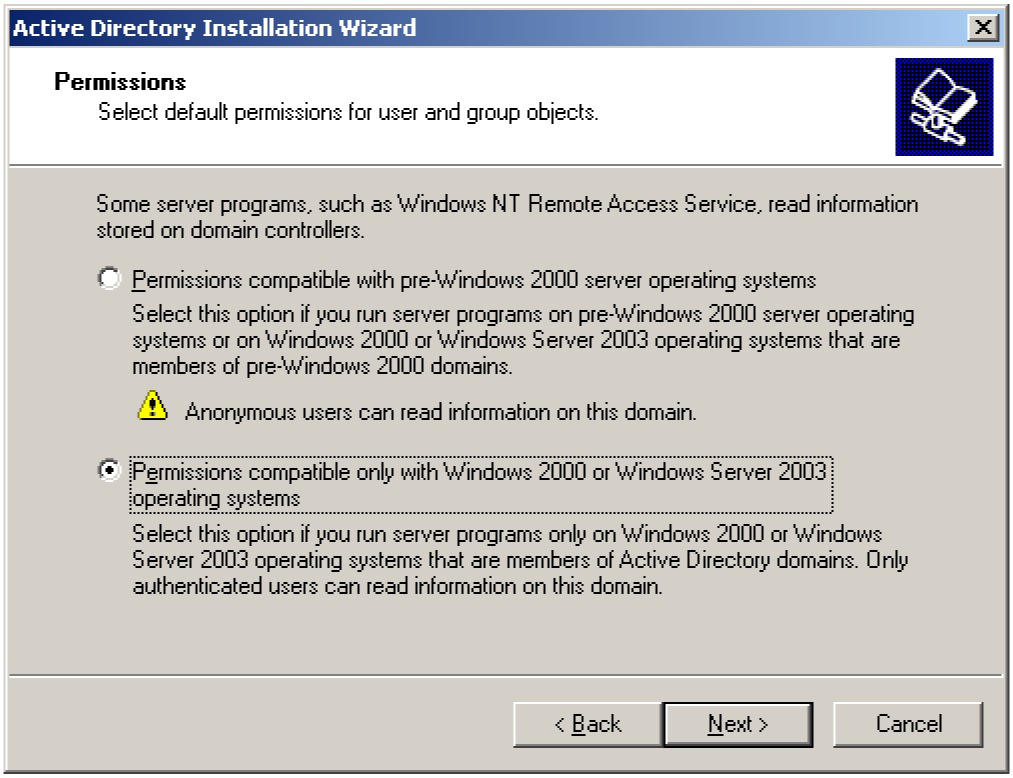
Details

The primary DNS server tested was: learn01.learnthat.com (192.168.0.155)

The zone was: learnthat.com

The test for dynamic DNS update support returned:
"The operation completed successfully."

44. Click **Next**.



Active Directory Installation Wizard

Permissions

Select default permissions for user and group objects.

Some server programs, such as Windows NT Remote Access Service, read information stored on domain controllers.

○ Permissions compatible with pre-Windows 2000 server operating systems

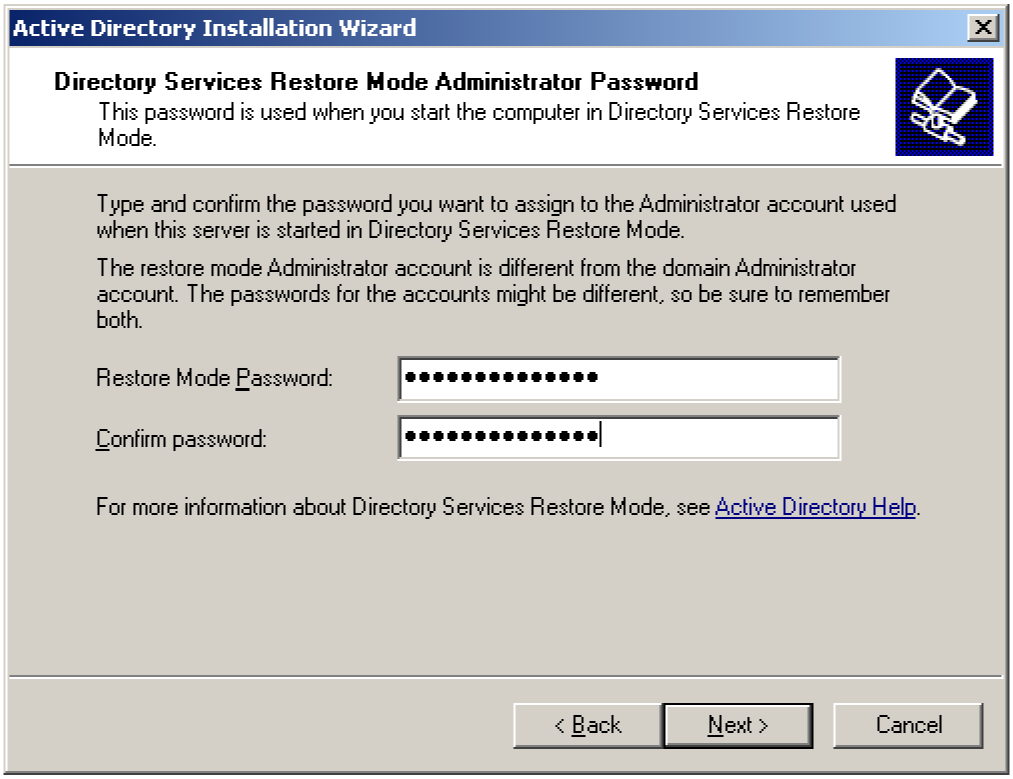
Select this option if you run server programs on pre-Windows 2000 server operating systems or on Windows 2000 or Windows Server 2003 operating systems that are members of pre-Windows 2000 domains.

⚠ Anonymous users can read information on this domain.

● Permissions compatible only with Windows 2000 or Windows Server 2003 operating systems

Select this option if you run server programs only on Windows 2000 or Windows Server 2003 operating systems that are members of Active Directory domains. Only authenticated users can read information on this domain.

45. Click **Next**.



Active Directory Installation Wizard

Directory Services Restore Mode Administrator Password

This password is used when you start the computer in Directory Services Restore Mode.

Type and confirm the password you want to assign to the Administrator account used when this server is started in Directory Services Restore Mode.

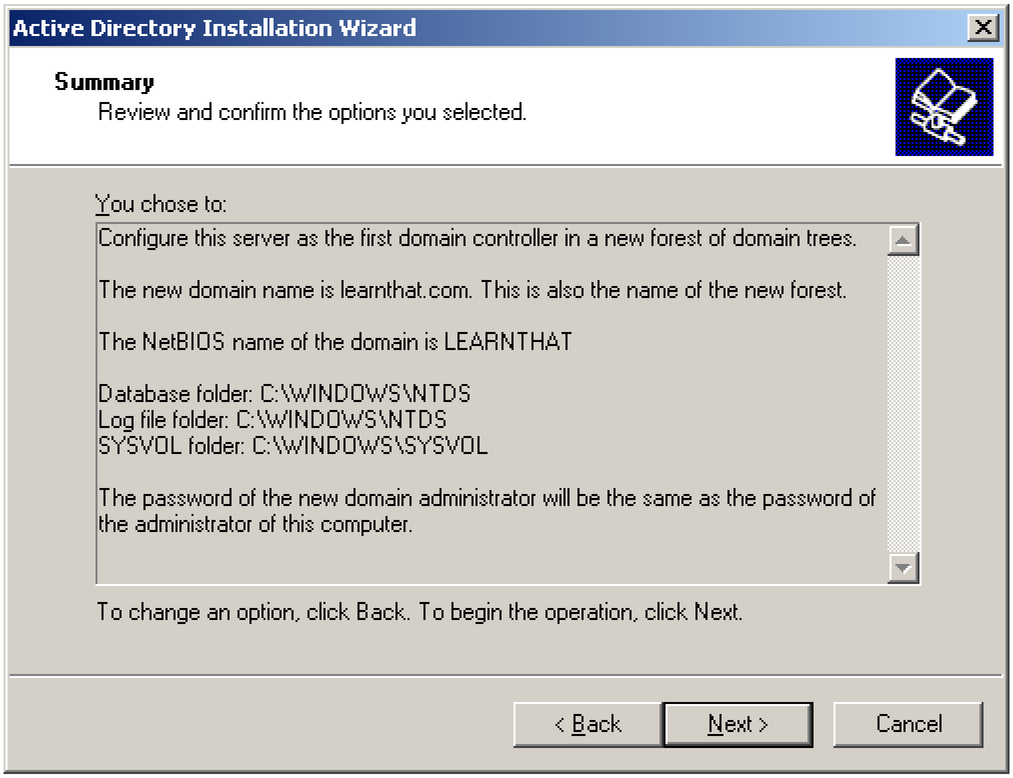
The restore mode Administrator account is different from the domain Administrator account. The passwords for the accounts might be different, so be sure to remember both.

Restore Mode Password: •••••••••••••••

Confirm password: •••••••••••••••

For more information about Directory Services Restore Mode, see Active Directory Help.

46. Enter in a password and click **Next**.


Active Directory Installation Wizard
Summary
Review and confirm the options you selected.
< Back
Next >
Cancel

You chose to:

Configure this server as the first domain controller in a new forest of domain trees.

The new domain name is learnthat.com. This is also the name of the new forest.

The NetBIOS name of the domain is LEARNTHAT

Database folder: C:\WINDOWS\NTDS
Log file folder: C:\WINDOWS\NTDS
SYSVOL folder: C:\WINDOWS\SYSVOL

The password of the new domain administrator will be the same as the password of the administrator of this computer.

To change an option, click Back. To begin the operation, click Next.

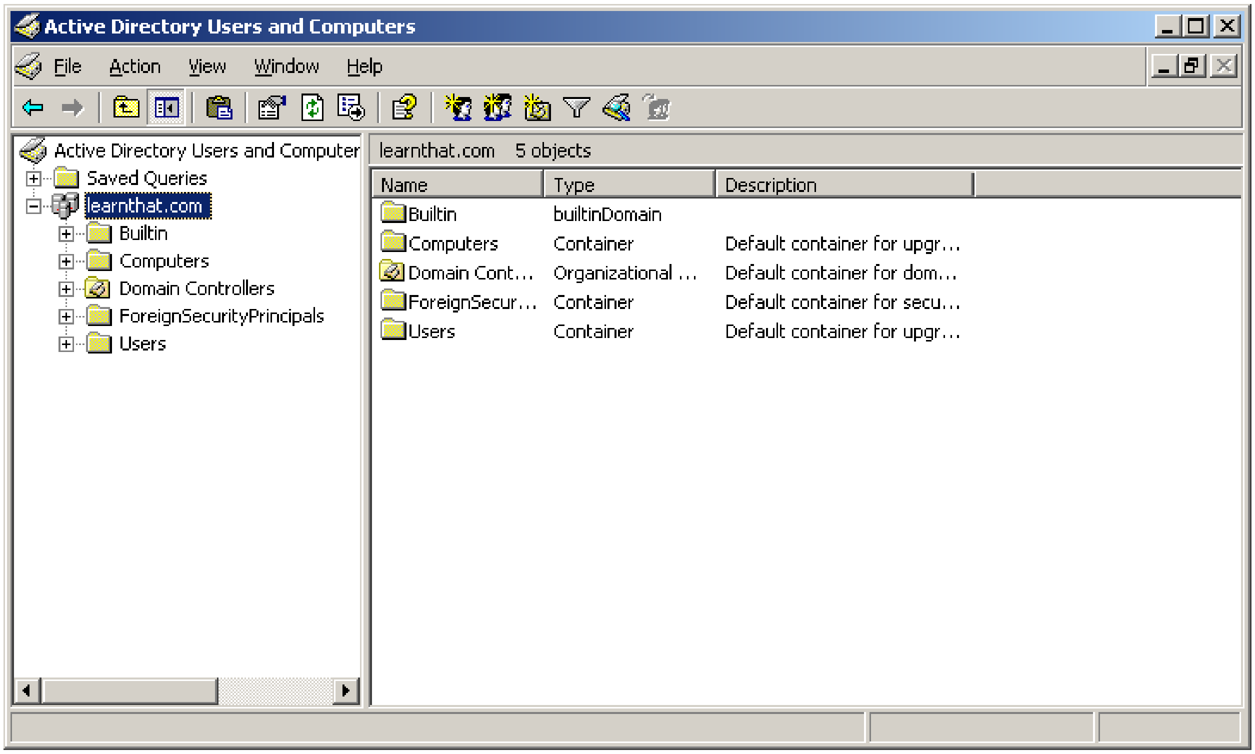
47. Click **Next**.
48. The wizard will configure Active Directory.
49. Click **Finish** to complete the wizard.
50. Click **Restart Now**.

Congratulations, you have now completed the Active Directory wizard and AD is installed.

Creating Organizational Units

As we discussed earlier, Organizational Units provide a mechanism to design a hierarchical structure within your Active Directory environment. Once you have designed your AD structure, you are ready to create the OUs in the environment.

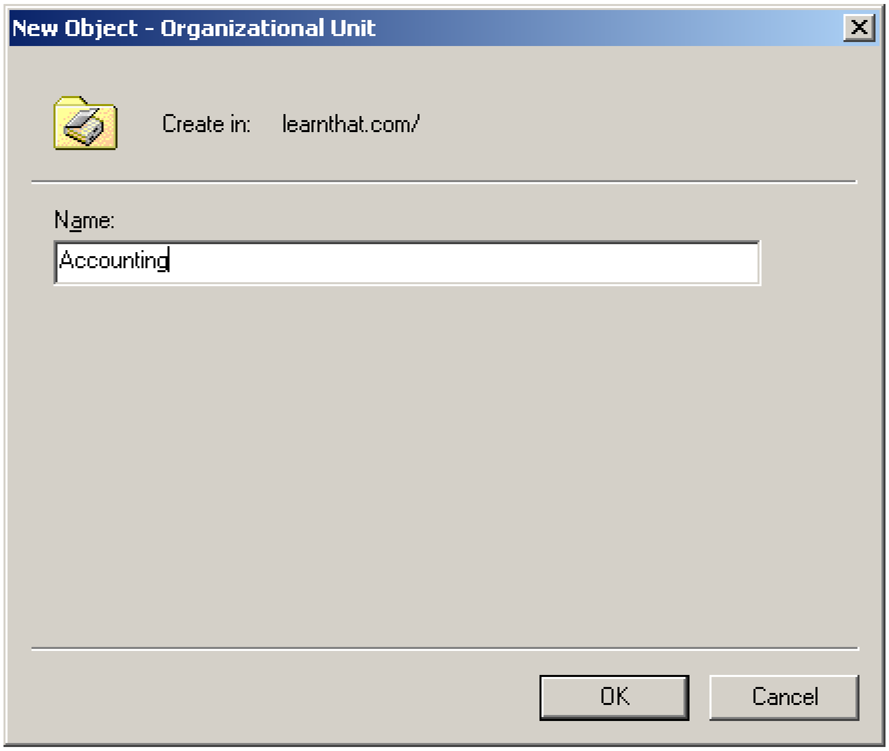
1. Click **Start** > **Administrative Tools** > **Active Directory Users and Computers**.
2. Double-click the domain name to open it up.


Active Directory Users and Computers
File Action View Window Help
Active Directory Users and Computer
Saved Queries
learnthat.com
Builtin
Computers
Domain Controllers
ForeignSecurityPrincipals
Users

learnthat.com 5 objects

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgr…
Domain Cont…	Organizational …	Default container for dom…
ForeignSecur…	Container	Default container for secu…
Users	Container	Default container for upgr…

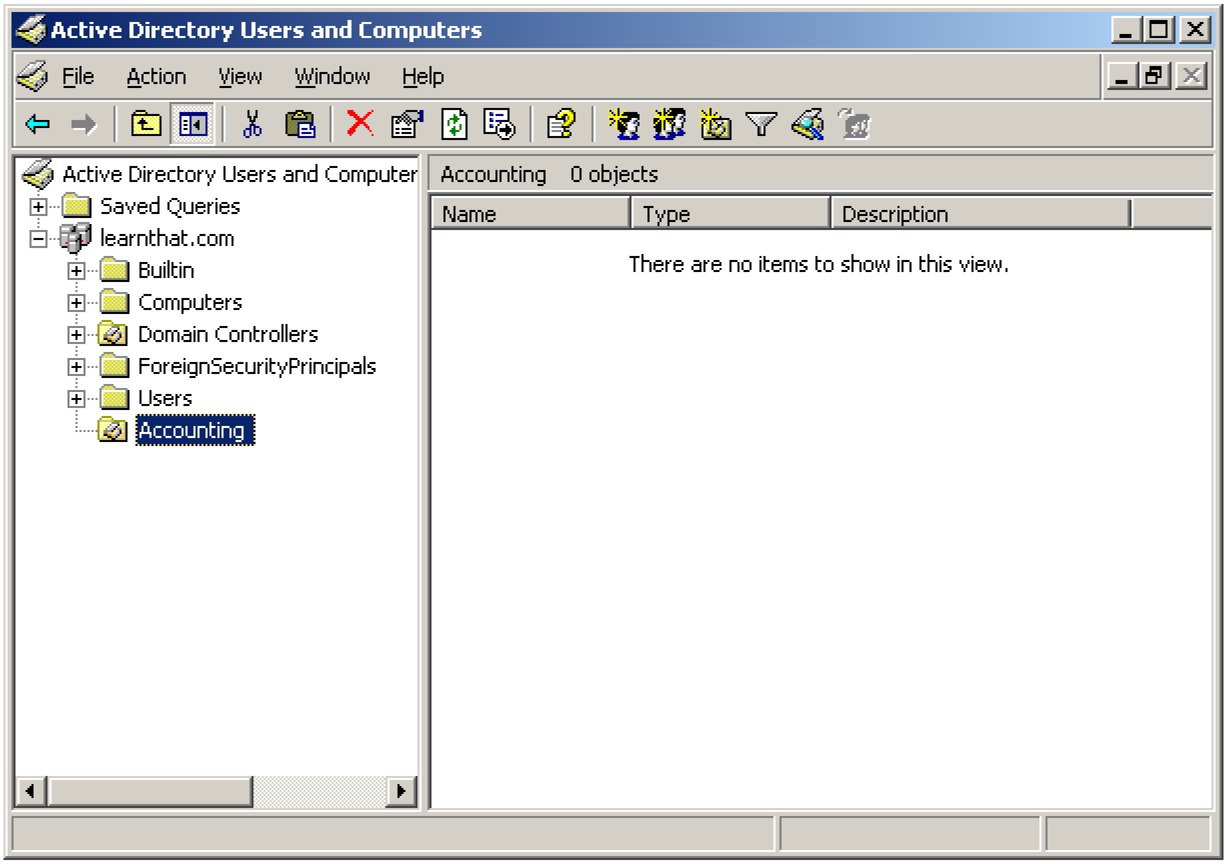
3. You will see a default structure with no Organizational Units. Right-click on **the domain name** and select **New** > **Organizational Unit**.



Create in: learnthat.com/

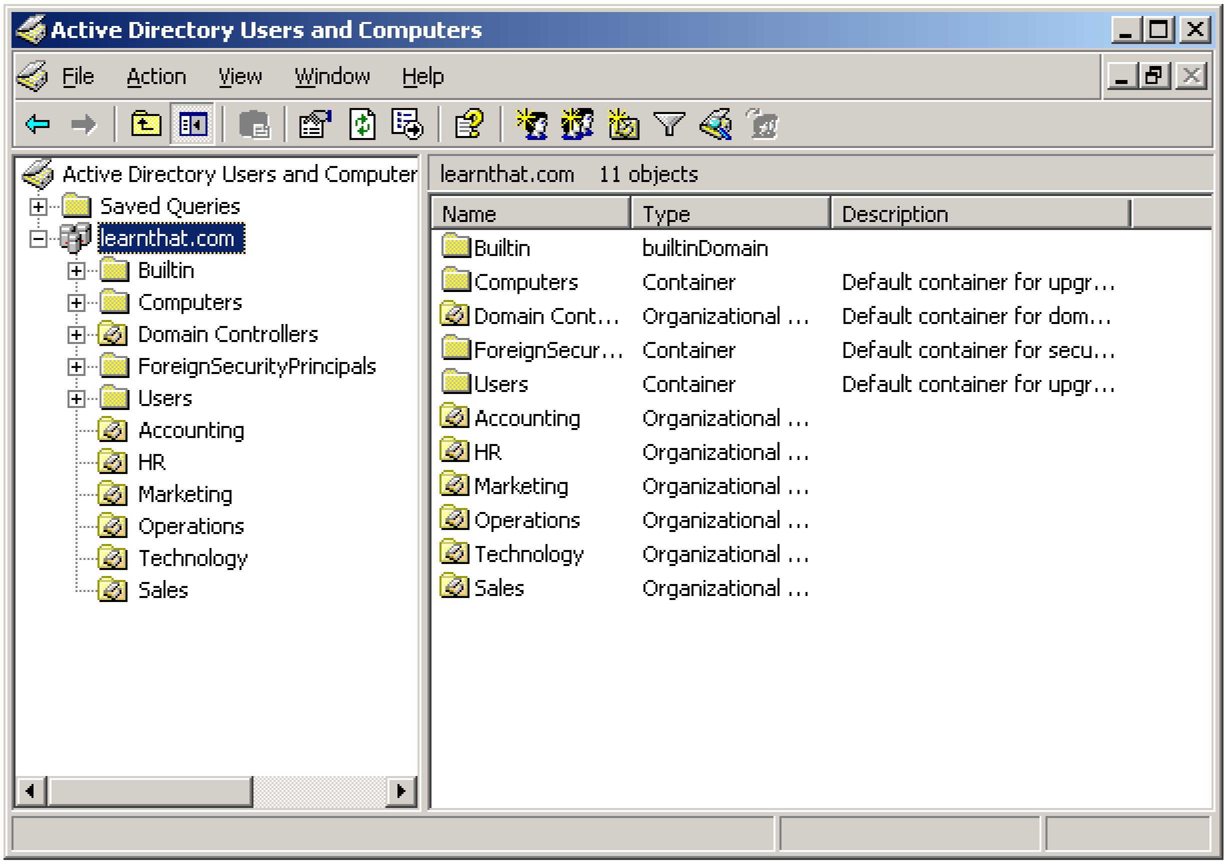
Name: Accounting

4. Enter the name of the OU you want to create and click **OK**.



There are no items to show in this view.

5. You will now see the OU you just created. Continue the process and build out the top level OUs.

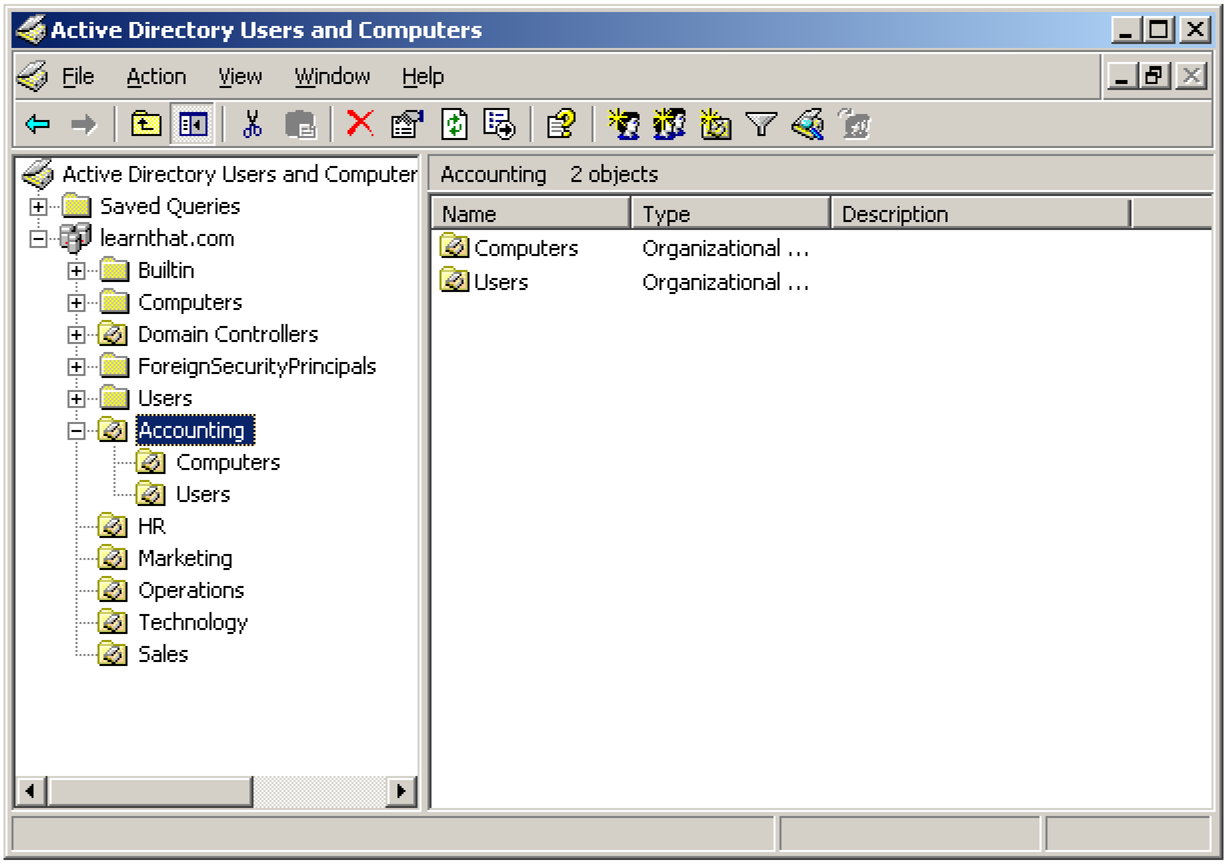


Active Directory Users and Computer
- Saved Queries
- learnthat.com
  - Builtin
  - Computers
  - Domain Controllers
  - ForeignSecurityPrincipals
  - Users
  - Accounting
  - HR
  - Marketing
  - Operations
  - Technology
  - Sales

learnthat.com 11 objects

Name	Type	Description
Builtin	builtinDomain	
Computers	Container	Default container for upgr...
Domain Cont...	Organizational ...	Default container for dom...
ForeignSecur...	Container	Default container for secu...
Users	Container	Default container for upgr...
Accounting	Organizational ...	
HR	Organizational ...	
Marketing	Organizational ...	
Operations	Organizational ...	
Technology	Organizational ...	
Sales	Organizational ...	

6. You now have a structure from which to build your organizational structure. For a small organization, we would create a *Users* and *Computers* organizational unit under each of the top level OUs.
7. Right-click on **Accounting** and select **New** > **Organizational Unit** and enter in *Computers*. Click **OK**. Repeat this process for the *Users* OU.



Name	Type	Description
Computers	Organizational ...	
Users	Organizational ...	

8. Now repeat the process for each department and you will have a structure of OUs created.

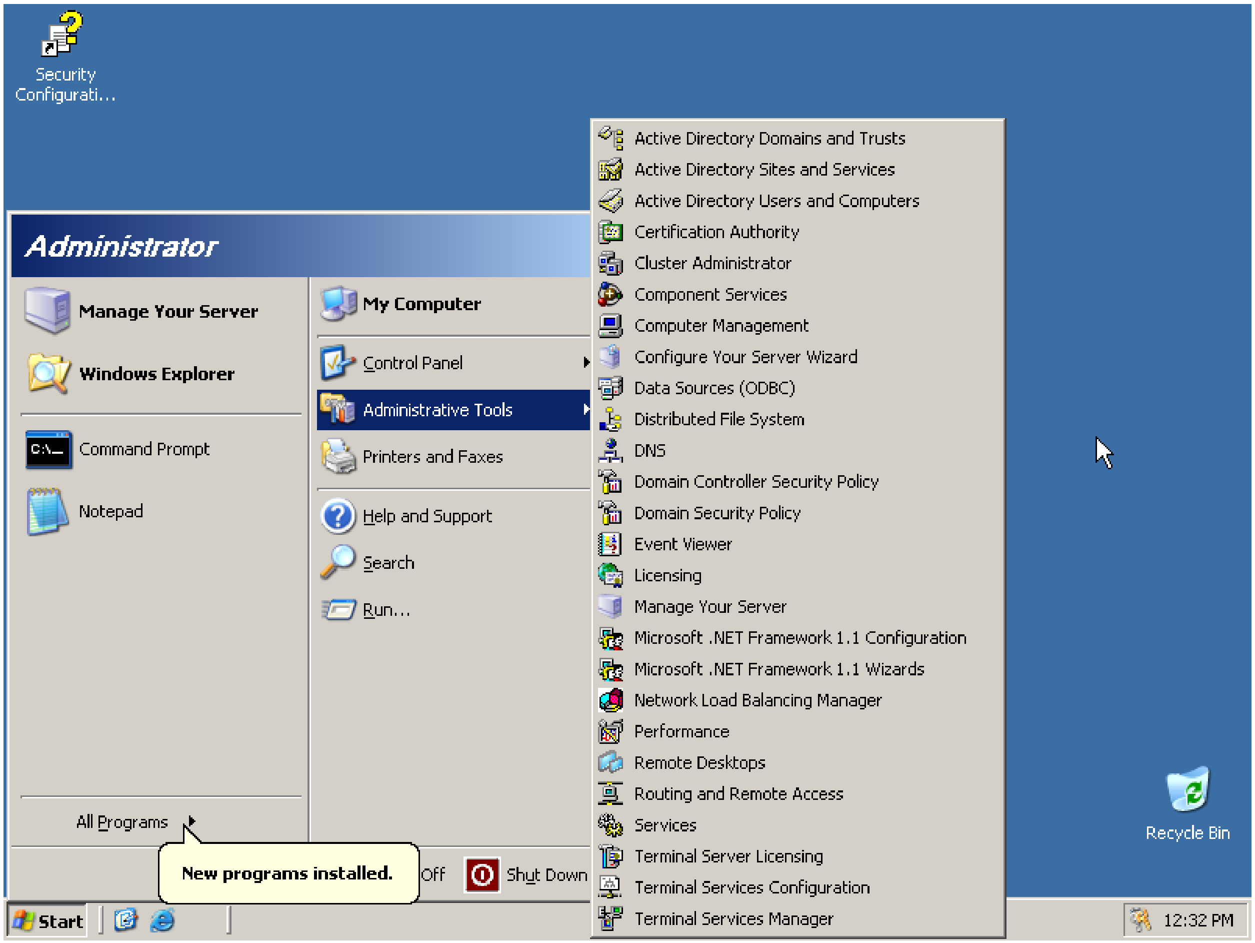
Post Active Directory Install

There are several steps you should do after the Active Directory installation to ensure installation went correctly and make sure AD operates properly in your environment.

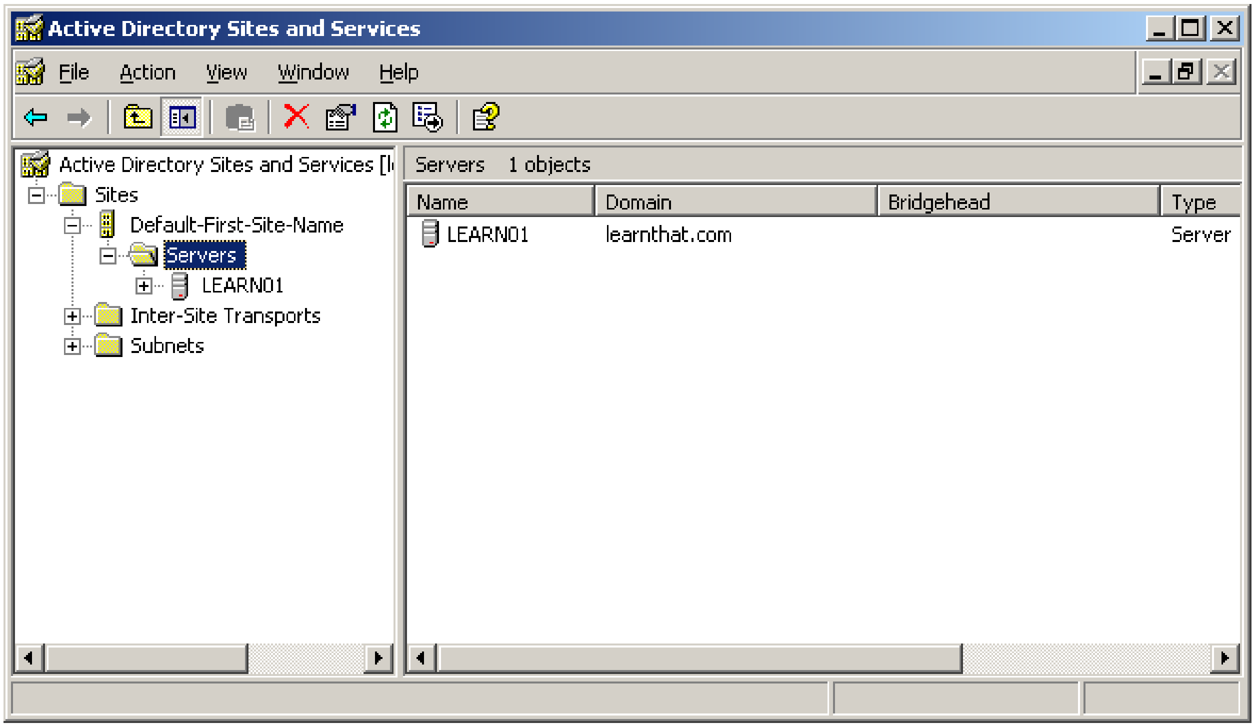
Verify Installation

After you have installed Active Directory, there are several steps you can take to ensure setup functioned correctly.

First, you can ensure the AD tools are installed. Click on **Start** and click **Administrative Tools.** You should have these tools installed:

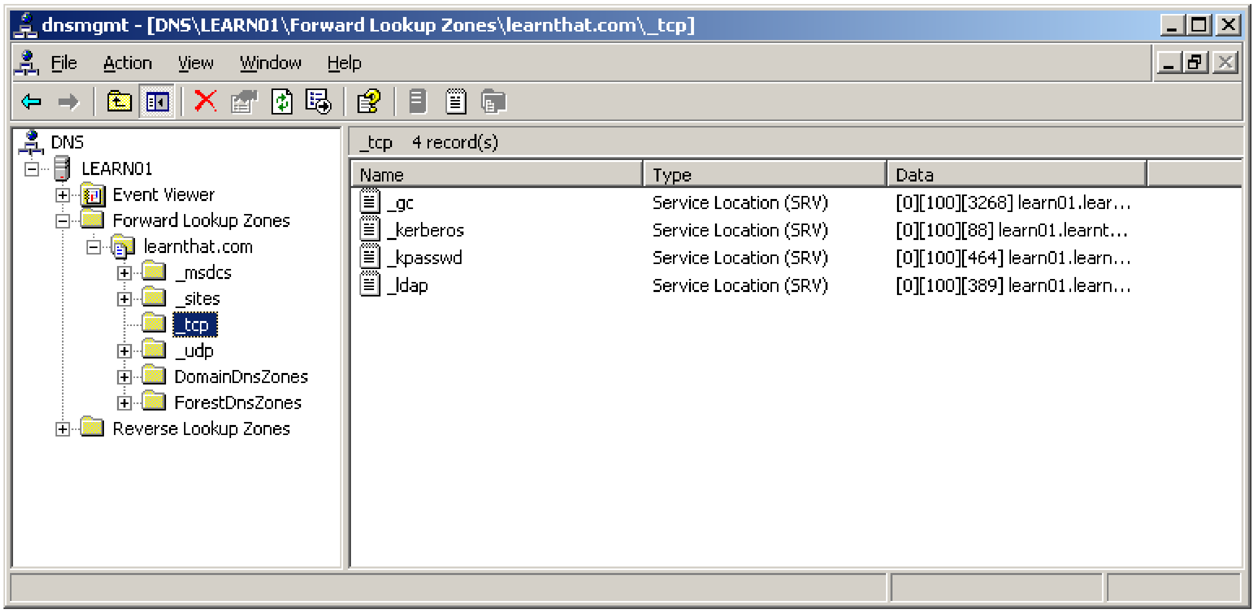


Next, open **Active Directory Sites and Services**. You should have a *Default-First-Site-Name* listed and when you open it up, you should find your domain controller listed as a server.


Active Directory Sites and Services
File Action View Window Help
Active Directory Sites and Services [l
Sites
Default-First-Site-Name
Servers
LEARN01
Inter-Site Transports
Subnets
Servers 1 objects

Name	Domain	Bridgehead	Type
LEARN01	learnthat.com		Server

Finally, open up DNS management. Open up the DNS server name, the *Forward Lookup Zones, the domain name,* and *_tcp*. It should look like this with four SRV records:



Name	Type	Data
_gc	Service Location (SRV)	[0][100][3268] learn01.lear...
_kerberos	Service Location (SRV)	[0][100][88] learn01.learnt...
_kpasswd	Service Location (SRV)	[0][100][464] learn01.learn...
_ldap	Service Location (SRV)	[0][100][389] learn01.learn...

Once you've performed these tasks, you've confirmed that your AD environment is installed.

Management Utilities

There are several management utilities you use to manage the Active Directory environment. As you saw after installation, you have these utilities (which are MMC snap-ins):

Active Directory Domains and Trusts: Manage domains and trusts between domains using this tool.

Active Directory Sites and Services: Setup and manage sites (physical networks).

Active Directory Users and Computers: Create and manage users, computers, other objects, OUs.

In later Active Directory tutorials, you will learn more about these tools and how to use them.

Active Directory Review

Thank you for taking this free Active Directory tutorial. In this tutorial, you learned the basic structure of Active Directory, why we use Active Directory, and how to install Active Directory.

Active Directory is a powerful networking tool in use at hundreds of thousands of organizations worldwide. Learning how Active Directory works is one step towards learning system administration and architecture.