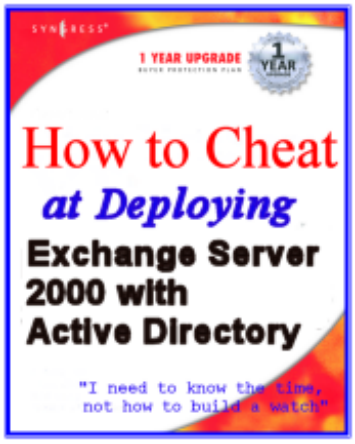
How to Cheat at Deploying Exchange Server 2000 with Active Directory



This special Syngress e-book is designed to provide quick, step-by-step help to anybody trying to wrestle with Deploying Exchange Server

BEFORE YOU BEGIN 3

TOPIC 1: PREPARING ACTIVE DIRECTORY 4

USING FORESTPREP 4

TOPIC 2: PREPARING YOUR DOMAINS 7

USING DOMAINPREP 7

TOPIC 3: DEPLOYING SERVERS RUNNING EXCHANGE 2000 9

ESTABLISHING THE FIRST ADMINISTRATIVE GROUP 9
DEPLOYING EXCHANGE USING TERMINAL SERVICES 10
DEPLOYING EXCHANGE ON A WINDOWS 2000 CLUSTER 10

TOPIC 4: UNATTENDED INSTALLATION 12

TOPIC 5: DEPLOYING EXCHANGE SYSTEM MANAGER 13

TOPIC 6: UPGRADING FROM PREVIOUS VERSIONS OF EXCHANGE 14

TOPIC 7: UPGRADING THE DIRECTORIES TO ACTIVE DIRECTORY 15

TOPIC 8: WHEN TO CONSOLIDATE BEFORE DEPLOYING 19

TOPIC 9: TOOLS USED TO UPGRADE THE WINDOWS NT 4.0 SAM 20

USING THE ACTIVE DIRECTORY MIGRATION TOOL 20

TOPIC 10: TOOLS USED TO UPGRADE THE EXCHANGE SERVER 5.5 DIRECTORY 22

USING THE ACTIVE DIRECTORY CONNECTOR 22
User Connection Agreements 23
Public Folder Connection Agreements 26
Configuration Connection Agreements 26
SITE REPLICATION SERVICE 26
USING THE ACTIVE DIRECTORY ACCOUNT CLEANUP WIZARD 27
DIRECTORY UPGRADE SCENARIOS 28
Using the In-Place Upgrade Method 28

Upgrade Using ADMT then ADC *29*
ADC then In-Place Upgrade then ADClean *30*
Upgrade Using ADC then ADMT then ADClean *33*

TOPIC 11: DIRECTORY UPGRADE CONSIDERATIONS 36

When to Require a Native Mode Domain 36
How to Successfully Use Universal Groups 37

TOPIC 12: UPGRADING THE MESSAGING ENVIRONMENT 38

TOPIC 13: PERFORMING AN IN-PLACE UPGRADE 39

TOPIC 14: PERFORMING A MOVE-MAILBOX UPGRADE 40

Using the Leapfrog Method 40

TOPIC 15: MOVING TO A NEW ORGANIZATION 42

Using the Exchange Mailbox Migration Program 42
Upgrading Supporting Servers 42
Upgrading Connector Servers 42
Upgrading Client Access Using Front-end Servers 42

TOPC 16: TESTING YOUR SCENARIO 44

Before you Begin

Deploying Exchange 2000 can be a very simple or very complex process. The complexity of your deployment will depend on several factors—but mostly it will depend on the complexity of your existing messaging environment. If you currently have no messaging system or if your existing messaging system consists of one or two servers running Exchange Server 5.5, then deployment is a fairly simple process. However, if your existing messaging system supports 225,000 users across four continents and 500 physical locations with varying levels of network connectivity and reliability, your Exchange 2000 deployment may be a tad more complex.

One of the unique aspects of upgrading from Windows NT 4.0 and Exchange Server 5.5 to Windows 2000 and Exchange 2000 is that two "directories" are being upgraded or consolidated into a single Active Directory. Windows NT 4.0 was only the security subsystem for Exchange Server 5.5. Exchange Server 5.5 has its own directory. Windows NT 4.0 accounts are associated with Exchange Server 5.5 mailboxes, but they are two different directories (if you can call the NT 4.0 Security Account Manager—or SAM—a directory). Exchange 2000 lost its directory to Windows 2000 Active Directory. The Windows 2000 security subsystem is Active Directory, not an NT 4.0 SAM. This means that when you upgrade your Windows NT 4.0 SAM to Active Directory you also will be upgrading your Exchange Server 5.5 directory to Active Directory, consolidating the two into a single directory.

This poses several challenges that must be carefully planned for and tested. Microsoft has provided the tools to manage this process effectively, but it's up to you to make sure the tools are used correctly and in the proper order. This white paper will give you the information you need to upgrade your directories to Active Directory.

Upgrading the directory is only half the story. Everything else needs to be upgraded from Exchange Server 5.5 to Exchange 2000. This includes mailbox servers, connectors, public folder servers, and bridgehead servers. Fortunately this process is fairly straightforward. The main challenge here is getting from point A to point B. If you have ten Exchange Server 5.5 sites you want to consolidate into three Exchange 2000 routing groups spanning two Administrative Groups, the process becomes more complex and requires more planning. As you can see, the key word here is *planning*.

Before we delve into the complexities of upgrading from Exchange Server 5.5 to Exchange 2000, there are some basic deployment strategies that can and should be used during deployment. Also, if you are not upgrading from a previous version of Exchange but are migrating from a different messaging system such as cc:Mail or Lotus Notes, you will likely deploy Exchange 2000 and migrate messaging data from your existing messaging environment to the new Exchange 2000 organization. This type of Exchange deployment, a so-called green field deployment, simply takes an Exchange 2000 design and deploys it across the organization. The term *green field* is used to symbolize rolling out the product onto a green field of grass that has never been touched. It is something we Exchange administrators dream of.

TOPIC 1: Preparing Active Directory

Exchange 2000 makes a considerable number of changes to the Active Directory schema and configuration partition. These changes are made when the first Exchange 2000 server is installed in the Active Directory forest. They are necessary to support the objects and attributes required by Exchange 2000.

A single schema and configuration partition exists for every Active Directory forest. The Active Directory schema and configuration partitions are hosted on each and every domain controller in the forest; they can only be modified by members of the Active Directory Schema Administrators Group. This means that when Exchange Server 2000 setup makes changes to the Active Directory schema and configuration partition, these changes must be replicated throughout the Active Directory forest to each domain controller. It also means that an administrator who is a member of the Schema Administrators Group must install the first Exchange 2000 server.

This poses a couple of issues:

- The Schema Administrators Group should contain a very limited number of administrators, most of whom will likely be centralized at one or two locations within the company. Typically, these administrators are not your Exchange implementers. It is impractical in a large organization to think these members of the Schema Administrators Group are the only administrators in the company who could run Exchange 2000 setup.
- It would be best if many schema modifications could be made early in the deployment of Active Directory, well before Exchange 2000 is deployed, so that the Exchange 2000 schema modifications could be included in the schema during the Active Directory deployment. This would avoid an excessive replication overhead when Exchange 2000 is finally deployed.
- Don’t wait until your Exchange deployment plan to perform modifications to your Active Directory Schema. You want to make these changes in the early stages of your Active Directory/Windows 2000 deployment of domain controllers.

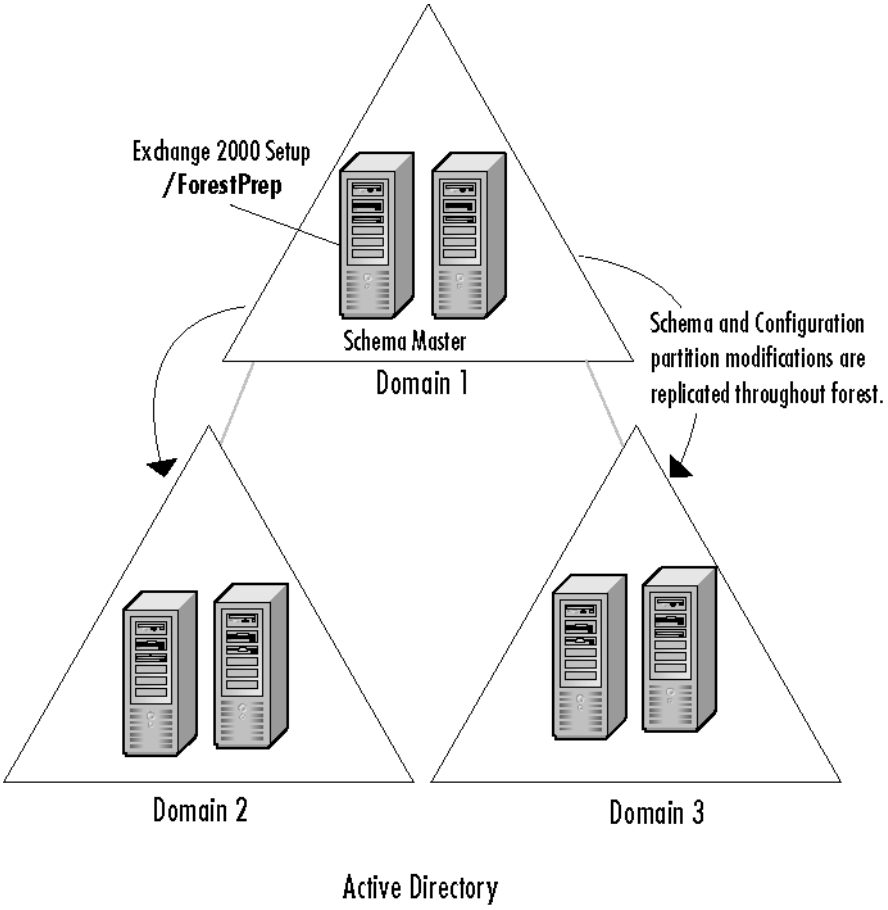
These potential difficulties with Exchange deployment were discovered during the Exchange 2000 beta process. Exchange 2000 setup always installed the product, but also performed special modifications to Active Directory when first run. The answer was to create a setup switch that ran a special Exchange 2000 setup process.

Using Forestprep

This setup switch is named /forestprep. Forestprep is run once by a Schema Administrator to prepare your Active Directory for Exchange 2000 by making changes to the Active Directory schema without actually installing Exchange 2000.

As seen in the following figure, forestprep makes the necessary changes to the Active Directory schema and establishes the Exchange 2000 organization by making modifications to the Active Directory configuration partition.

Exchange 2000 Setup Schema Modifications



If your organization will deploy Exchange 2000, but is currently in the planning or deployment phase of your Windows 2000 project, then consider incorporating the Exchange 2000 schema and configuration partition changes into your Active Directory deployment by using forestprep at the early stages of your Active Directory deployment.

This can be done by having a Schema Administrator run forestprep in the root domain on the Active Directory domain controller designated as the Schema Master over a weekend—or whenever the schema and configuration partition changes can be replicated across the organization efficiently and without impacting system performance.

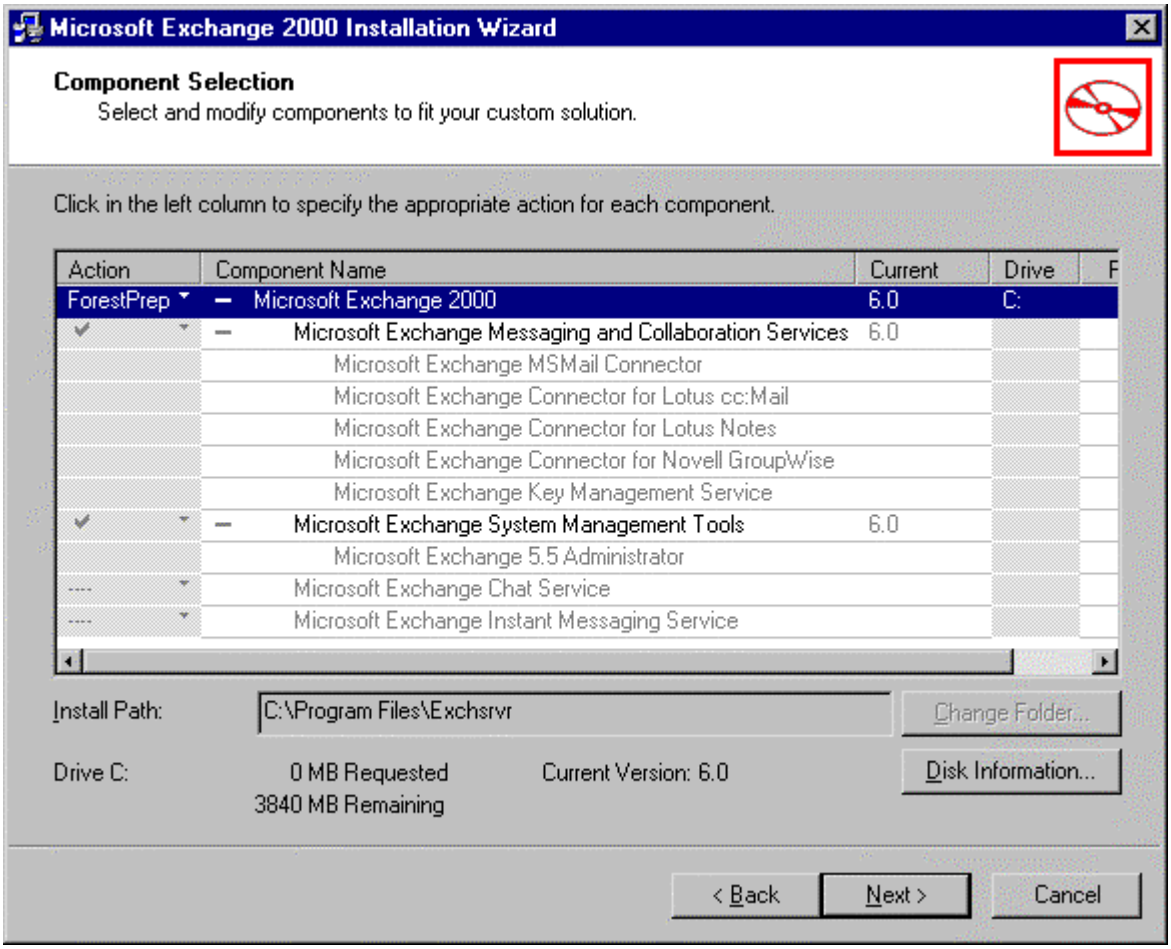
When running Exchange 2000 setup with the forestprep switch, Exchange 2000 setup will prompt you for the following information:

- Your 25-digit product identification code. This code is located on the Exchange 2000 compact disc jewel case.
- An indication that tells whether you are creating a new Exchange 2000 organization or joining an existing Exchange Server 5.5 organization. You must have the service account name and password if joining an existing Exchange Server 5.5 site. You must also have the Exchange version of the Active Directory Connector (ADC) installed in the forest.
- The organization name. This should be defined in your Exchange 2000 design or functional specification. Choose this name wisely, because it cannot be changed.

- The Active Directory user you want to specify as the initial Exchange 2000 Administrator. This account will be granted permission on the Exchange 2000 objects and object containers created in the Exchange 2000 portion of the Active Directory configuration partition.

When you use the forestprep setup switch, ForestPrep is the only choice—as shown below—when selecting components.

ForestPrep Component Selection



Setup will fail if you are not logged in as an Active Directory user who is a member of the Schema Administrator Group, or if Exchange 2000 setup is unable to successfully write changes to the Active Directory schema..

WARNING

Be careful when starting Exchange 2000 setup with the forestprep switch on the command line. If you misspell /forestprep, the standard Exchange 2000 setup will start and allow you to install Exchange 2000.

If you run Exchange 2000 setup without first running Exchange 2000 setup with the /forestprep switch, the schema and configuration partition modifications will first be made, then Exchange 2000 will be installed. You do not have to run /forestprep before an Exchange 2000 server can be installed, but it is a best practice and recommended by Microsoft.

TOPIC 2: Preparing Your Domains

Several of the same principles that apply to forestprep also apply to the Active Directory domains. An administrator who has Domain Administrator permissions for that domain needs to have Exchange 2000 setup do several things to each Active Directory domain.

Exchange 2000 administrators do not need any special permissions in Active Directory other than those granted them by the Exchange Delegation Wizard from within the Exchange System Manager. This means that you can have a group of Exchange 2000 administrators who can only manage the Exchange 2000 objects and object containers in Active Directory. They don't have to be domain administrators or have any other special permission in the domain. This type of division is preferred by many organizations, but can become an issue during setup when Exchange is first being installed into the Active Directory domain. This is because Exchange 2000 setup performs the following tasks:

- A user account named EUSER_EXSTOREEVENTS is created for use with the script event host.
- An Exchange Domain Servers domain global group is created; this group contains all computers running Exchange 2000 in the domain.
- An Exchange Enterprise Servers domain local group is created; this group contains all computers running Exchange 2000 in the enterprise.
- Each of these groups is granted permission on objects in the Active Directory domain.

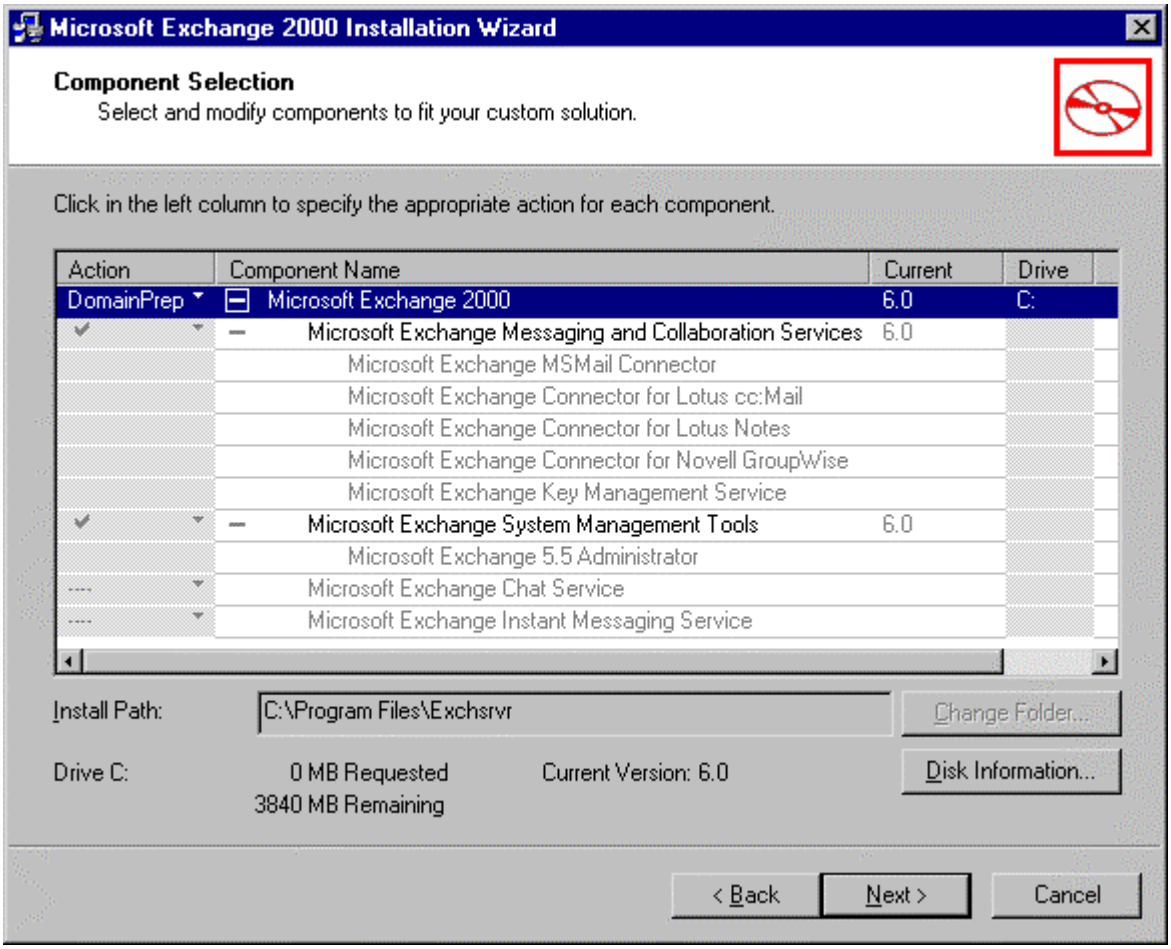
An administrator who has permissions in the domain can only perform these tasks by running Exchange 2000 setup with the domainprep switch.

Using Domainprep

Domainprep is a command-line switch used during deployment to prepare each Active Directory domain. If there are no Exchange implementers in the domain who are members of the Domain Administrators Group, then an administrator who is a member of the Domain Administrators Group can run domainprep to prepare the domain for Exchange 2000.

When running Exchange 2000 setup with the domainprep switch, DomainPrep will be the only component you can select, as shown in the following figure.

DomainPrep Component Selection



Setup will fail if you are not logged in as an Active Directory user who is a member of the Domain Administrators Group when domainprep is being run or when the first Exchange 2000 server is installed into the domain.

WARNING

If you misspell /domainprep when starting Exchange 2000 setup with the domainprep switch on the command line, the standard Exchange 2000 setup will start and allow you to install Exchange 2000.

If you run Exchange 2000 setup without first running Exchange 2000 setup with the /domainprep switch, the domain modifications will be made; then Exchange 2000 will be installed. It is not necessary to run /domainprep before installing an Exchange 2000 server into the domain, but it is the best practice and recommended by Microsoft.

TOPIC 3: Deploying Servers Running Exchange 2000

Exchange 2000 servers should be rolled out in a manner that provides the most efficient use of implementation resources and the most complete user experience. You would not want to deploy Exchange 2000 servers populated with user mailboxes across several routing groups, and only then connect those routing groups with connectors using bridgehead servers. A general guideline for deploying Exchange 2000 servers (not relevant when upgrading) includes:

- Establish the Administrative Groups and apply permissions using the Exchange Delegation Wizard, per your Exchange 2000 design using Exchange System Manager.
- Establish the Routing Groups per your Exchange 2000 design using Exchange System Manager.
- Deploy Exchange 2000 bridgehead servers in each routing group per your Exchange 2000 design.
- Connect routing groups with the connectors specified in your Exchange 2000 design.
- Test connectivity.
- Deploy mailbox and public folder servers per your Exchange 2000 design; populate with user mailboxes and public folder data.

Establishing the First Administrative Group

When you install Exchange 2000, setup looks for a list of Administrative Groups that the new server can be installed into. If no Administrative Groups exist, such as when the first server is installed, an Administrative Group is created named *First Administrative Group*. It's not a very useful name and will likely not be included in your Exchange 2000 Administrative Group design.

To better control which Administrative Groups exist and which Administrative Groups the Exchange implementers install their servers into, you can establish all your Administrative Groups *after* forestprep has been run and *before* you install your first Exchange 2000 server. Use these steps:

1. Run Exchange 2000 setup with the /forestprep switch to prepare your Active Directory forest.
2. Run Exchange 2000 setup with the /domainprep switch to prepare your Active Directory domain.
3. Run Exchange 2000 setup and only select the Exchange 2000 Management Components.
4. Start the Exchange System Manager and create all the Administrative Groups defined in your Exchange 2000 design.
5. Install your first Exchange 2000 server and select the Administrative Group the server will be installed into as defined by your Exchange 2000 design or functional specification.

Incorporating these steps into your Exchange 2000 deployment plan will ensure that you establish the Administrative Groups before Exchange servers are installed. When your assisting Exchange implementers proceed to install their Exchange 2000 servers, they will have a complete drop-down list of Administrative Groups to choose from. There will be no question, when following the instructions provided by your deployment plan, which Administrative Group to install their server into.

WARNING

You cannot move Exchange 2000 servers between Administrative Groups. This means that the Administrative Group selected during setup is the Administrative Group where that server will reside unless reinstalled.

Creating Administrative Groups in this way only pertains to new Exchange 2000 organizations. If you install an Exchange 2000 server into an Exchange Server 5.5 site, the Administrative Groups will be created in Active Directory in the same topology as the Exchange Server 5.5 sites. This is because Exchange 2000 treats Administrative Groups like Exchange Server 5.5 sites during coexistence.

Deploying Exchange Using Terminal Services

Windows 2000 Terminal Services is included with Windows 2000. This handy feature allows you to connect to a remote server and establish a session on that server that emulates the remote servers console. It's like actually being there.

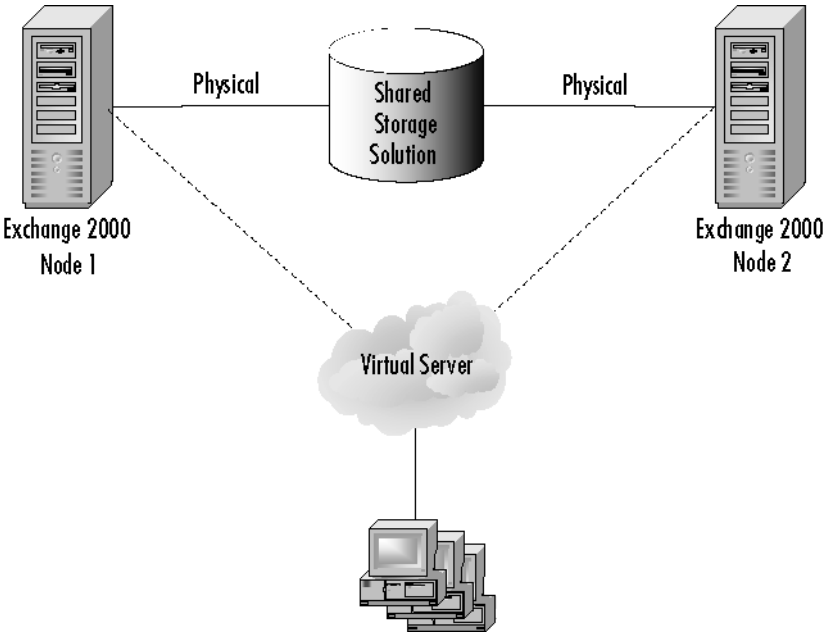
In remote locations that will host an Exchange 2000 server, it may be desirable for *you* to install Exchange 2000, not the local system administrator. Finally we administrators can ensure a remote exchange installation is installed according to our requirements. This is possible using Windows 2000 Terminal Services. The local system administrator prepares the Windows 2000 server, joining the domain and installing Windows 2000 Terminal Services. You, or another Exchange 2000 implementer, then establish a Windows 2000 terminal services session with the remote server and install Exchange 2000.

> **NOTE**
> It is not necessary to use terminal services to manage the Exchange 2000 server. All configuration of the server is contained in the configuration partition of Active Directory and can be accomplished using Exchange System Manager.

Deploying Exchange on a Windows 2000 Cluster

With the advances in Windows 2000 clustering and the ability to support multiple information stores on a single Active/Active Exchange 2000 cluster, the consolidation of several Exchange Server 5.5 servers into one or more large Exchange 2000 clusters with multiple information stores is becoming more popular. As seen below, many economies—including greater availability —can be realized by having fewer large servers.

An Exchange 2000 Cluster



If your Exchange 2000 design calls for Exchange 2000 to be installed on a Windows 2000 cluster, there are some guidelines to follow.

- The same Exchange 2000 components must be installed on both nodes of the cluster.
- Exchange 2000 must be installed into the same drive letter and directory for both nodes of the cluster.
- After Exchange 2000 has been installed on the cluster, a virtual server must be created. To do this you create a resource group and define computer resources such as a TCP/IP address, network name, and shared disk, for the cluster nodes. Once complete, you will have a functioning Exchange 2000 server that is made up of multiple nodes. Take this time to test the cluster and its fail-over functionality before creating or moving mailboxes to the server.

TOPIC 4: Unattended Installation

Exchange 2000 is using a new setup engine for Microsoft BackOffice products. The Software Installation Toolkit (SIT) provides the ability to perform an unattended setup. An unattended setup is done in two phases.

- First, an unattended setup file is created by running Exchange 2000 setup with the **/createunattended** command-line switch. This switch causes Exchange 2000 setup to walk through the setup process and prompt the installer to define the type of installation that will be done—including the components to install, and the Administrative Group and routing group that the server will be installed into. Then, rather than installing the server, an unattended setup file is created with an .ini extension.
- Next, Exchange 2000 setup is run with the **/unattendfile** command-line setup switch that uses the information in the unattended setup file (created in the first phase) to install the Exchange 2000 server.

It is also possible to encrypt the unattended setup file that is created by using the **/encryptedmode** command-line setup switch. This way neither the implementer at the remote site nor anyone else along the way can view the content of the unattended setup file, which may contain a service account password if the Exchange 2000 server will coexist with Exchange Server 5.5.

Depending on the type of deployment your organization calls for, you may want to use unattended setup files during your deployment of Exchange 2000. If you choose to do so, make sure you test the creation of the unattended setup file and its use during installation.

TOPIC 5: Deploying Exchange System Manager

Exchange 2000 is configured and managed using two tools. The configuration of Exchange 2000 is done using the Exchange System Manager and recipients are managed using Active Directory Users and Computers. From the Exchange System Manager you can define and configure global settings, Administrative Groups, routing groups and their connectors, along with servers and their objects such as information stores. Exchange recipients, such as users, mail-enabled contacts, mail-enabled groups, and public folders are created and managed using Active Directory Users and Computers, not Exchange System Manager. This is fundamentally different from previous versions of Exchange where the Exchange Administrator was used to configure Exchange and to manage Exchange recipients.

Now with Exchange 2000, your Exchange Administrators will manage Exchange using Exchange System Manager, and the administrators that manage Active Directory users, contacts, and groups will manage Exchange recipients using Active Directory Users and Computers. When a user is created using Active Directory Users and Computers, the administrator can choose to create a mailbox for that user and choose which Exchange server the mailbox will be created on.

The ability to manage Exchange recipients is not built into the standard Active Directory Users and Computers. Rather, this functionality is added when the Exchange System Manager is installed. For deployment, this means that you must install the Exchange System Management components on all computers where recipients are managed using Active Directory Users and Computers, as well as those workstations where Exchange will be managed using Exchange System Manager.

TOPIC 6: Upgrading from Previous Versions of Exchange

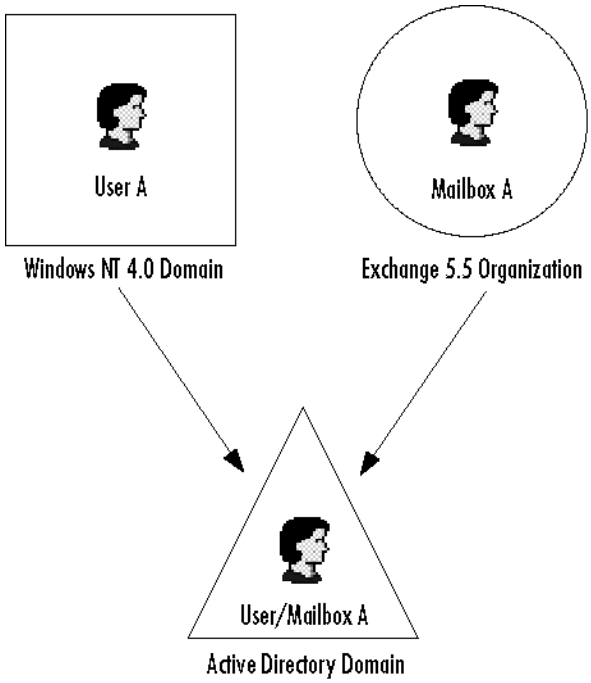
How do you get from your existing Exchange Server 5.5 organization running on Windows NT 4.0 to Exchange 2000 running Windows 2000 with Active Directory? That is the task at hand. In this section we will try to arm you with the information and tools necessary to answer that question with a reasonable degree of certainty.

There are two components that need to be addressed in upgrading an Exchange Server 5.5 to Exchange 2000: upgrading the directory and upgrading the messaging infrastructure. The directory upgrade is more difficult to manage, because two directories with duplicate accounts need to be melded into a single Active Directory. The messaging system upgrade is heavy lifting because of the sheer volumes of data that need to be migrated or upgraded. With enough information, planning, and testing, your upgrade will be a challenging and successful project.

TOPIC 7: Upgrading the Directories to Active Directory

Understanding how your Windows NT 4.0 directory and Exchange Server 5.5 directory will come together to make up your Windows 2000 Active Directory is very important to the success of your migration project. The goal is to consolidate two different directories with similar object types into a third directory, maintaining dependencies along the way (see the next figure).

Merging Two Directories into Active Directory



For most companies that have multiple Exchange sites and/or NT 4.0 domains there will be a period of coexistence between Windows NT 4.0, Exchange Server 5.5, and Active Directory. To make coexistence between these messaging systems possible, certain restrictions had to be placed on how you can configure Exchange 2000 during coexistence. Like Windows 2000, which has a mixed mode to support coexistence with Windows NT, Exchange 2000 has a mixed mode to support coexistence with Exchange Server 5.5. When the first Exchange 2000 server is installed, the organization is in mixed mode. Once there is no longer any need to support Exchange Server 5.5 servers or services, the Exchange 2000 organization can be configured for native mode. Make certain you no longer need to coexist however, because once you flip this switch there's no going back.

For Exchange Server 5.5 to coexist with Exchange 2000, the Exchange 2000 servers must look and feel like another Exchange Server 5.5 server. To accomplish this, certain restrictions are placed on the flexibility of Exchange 2000 Administrative Groups and routing. In mixed mode, the Exchange 2000 Administrative Group and the routing group are directly associated, so that they look to Exchange Server 5.5 like another Exchange Server 5.5 site. The restrictions on how Administrative Groups and routing groups can be configured while in mixed mode are as follows.

- Routing groups cannot span Administrative Groups.
- A server in a routing group cannot belong to a different Administrative Group.
- Mailboxes cannot be moved between Administrative Groups.

- Administrative Groups can contain multiple routing groups, but Exchange 5.5 servers will not recognize more than one routing group and will treat all Exchange servers in the Administrative Group as if it were a single site.

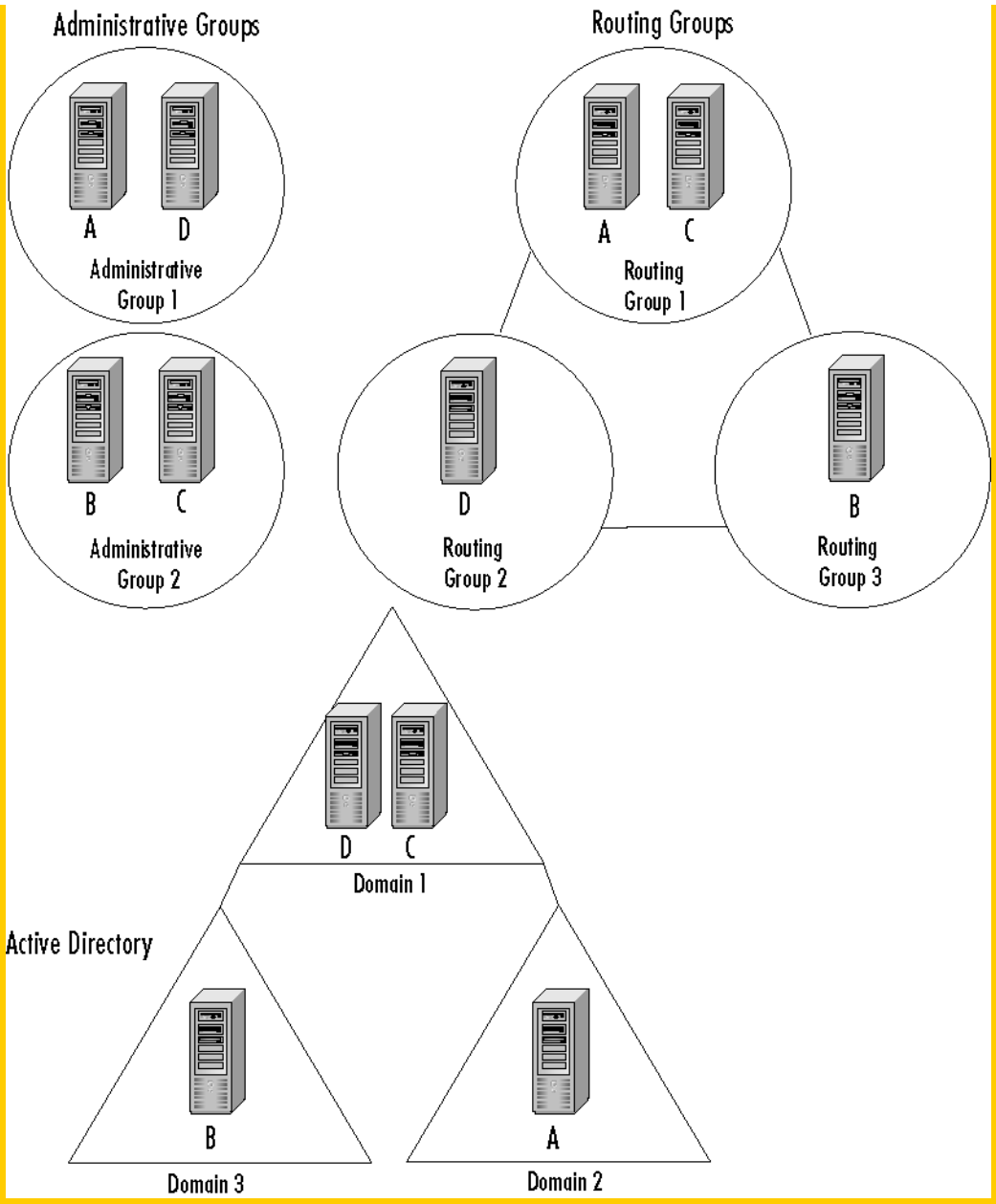
When you install your first Exchange 2000 server, after running forestprep and domainprep, coexistence between the Exchange Server 5.5 directory and Active Directory will be established. From the Exchange Server 5.5 directory, Exchange configuration information will replicate to Active Directory, and you will see Administrative Groups starting to appear that will mirror the sites defined in Exchange Server 5.5. During coexistence, therefore, your Administrative Groups will mirror your Exchange Server 5.5 sites, locking your administrative model into something similar to what you had with Exchange Server 5.5.

Making Exchange 2000 look like Exchange Server 5.5

When planning your Exchange 2000 deployment, it's important to understand the basic components of an Exchange 2000 organization. This is important because, as the person responsible for planning the deployment, you need to be familiar with how Exchange Server 5.5 and Exchange 2000 fit together. In previous versions of Exchange, the Exchange organization was made up of sites. Exchange sites defined the administrative model, how messages flowed through the organization, and the X.500 namespace. Each of these aspects of an Exchange site would likely have a unique set of design considerations. The ideal Exchange 5.5 administrative model was different from the ideal routing model. However, since these two design points are folded into a single object—the site—this often leads to compromises during the site design process. Usually, Exchange Server 5.5 sites were designed on the basis of available network bandwidth, with the administrative model taking a back seat. The consequence is that most Exchange organizations have a loose administrative model where users who are defined as Exchange Administrators within a site have full control over all objects in that site.

In Exchange 2000 sites no longer exist. They have been dismantled into three independently configurable components: Administrative Groups, Routing Groups, and the Active Directory namespace (see the following figure).

Exchange 2000



Each of these Exchange 2000 components can be designed independently of the others to meet specific design considerations. This is only true when Exchange 2000 is in native mode. When in mixed mode, to support coexistence, Administrative Groups and Routing Groups are dependent.

An administrative model that meets your organization's requirements can be implemented without affecting the routing topology, and vice versa.

Administrative groups

Objects in Exchange 2000 are contained in manageable groups named Administrative Groups. The objects in an Administrative Group inherit the permissions assigned the Administrative Groups. Administrative Groups can, but don't have to, contain any Exchange 2000 object. This means that all your routing groups and public folder hierarchies can be contained in one centralized Administrative

Group, while your Exchange 2000 server objects are contained in regional Administrative Groups. This type of flexibility allows for new administrative models not previously available with Exchange.

Routing groups

Message flow within and between routing groups is similar to previous versions of Exchange. Messages are delivered between servers within a routing group in a single hop, or point-to-point. Between routing groups, messages are routed through bridgehead servers and across connectors. Despite similarities in how messages flow, there are vast differences between the inner workings of Exchange Server 5.5 and Exchange 2000 message transfer. Some of the major changes to message transfer in Exchange 2000 include SMTP being the primary protocol used to deliver messages within a routing group and the preferred protocol between routing groups. Also, Exchange 2000 is much smarter about how to route a message between routing groups. The state of all connectors that connect routing groups is contained in a database on all servers. Once a connector fails, all servers are notified, and that connector will not be used again until it becomes available.

Those who are responsible for your Exchange 2000 deployment should have a working knowledge of Exchange 2000. Too often those who design the Exchange 2000 topology get all the training while those who do the deployment, it is assumed, will be able to get by on their Exchange Server 5.5 skill set. This may not be the case.

TOPIC 8: When to Consolidate before Deploying

When you coexist with Exchange Server 5.5, you inherit the Exchange Server 5.5 site topology into your Exchange 2000 organization. What's more, you can't move servers between Exchange 2000 Administrative Groups to reorganize once the coexistence phase of your deployment is complete. This means that if your Exchange 2000 design or functional specification has a different Administrative Group structure than your Exchange Server 5.5 site topology, you're in a bind (but not alone). There are two approaches to overcoming this problem.

- After your upgrade to Exchange 2000 is complete, you can go to native mode and move mailboxes between Administrative Groups (not servers, mind you, just mailboxes). You could then create additional Administrative Groups that contain Exchange 2000 servers, and move users out of unwanted Exchange Server 5.5 sites, then retire those sites.
- With Exchange Server 5.5 service pack 1 you can move servers between Exchange Server 5.5 sites using the Move Server Wizard. This presents the other option. You could reorganize your Exchange Server 5.5 site structure to look like your Exchange 2000 Administrative Group structure using the Move Server Wizard, then upgrade from Exchange Server 5.5 to Exchange 2000, resulting in the Administrative Group structure defined in your Exchange 2000 design.

Neither of these options are inviting. Each would require a great deal of effort and resources in addition to extending the deployment process and causing more end-user downtime. However, until Microsoft releases an Exchange 2000 version of the Move Mailbox Wizard, there are not many other choices.

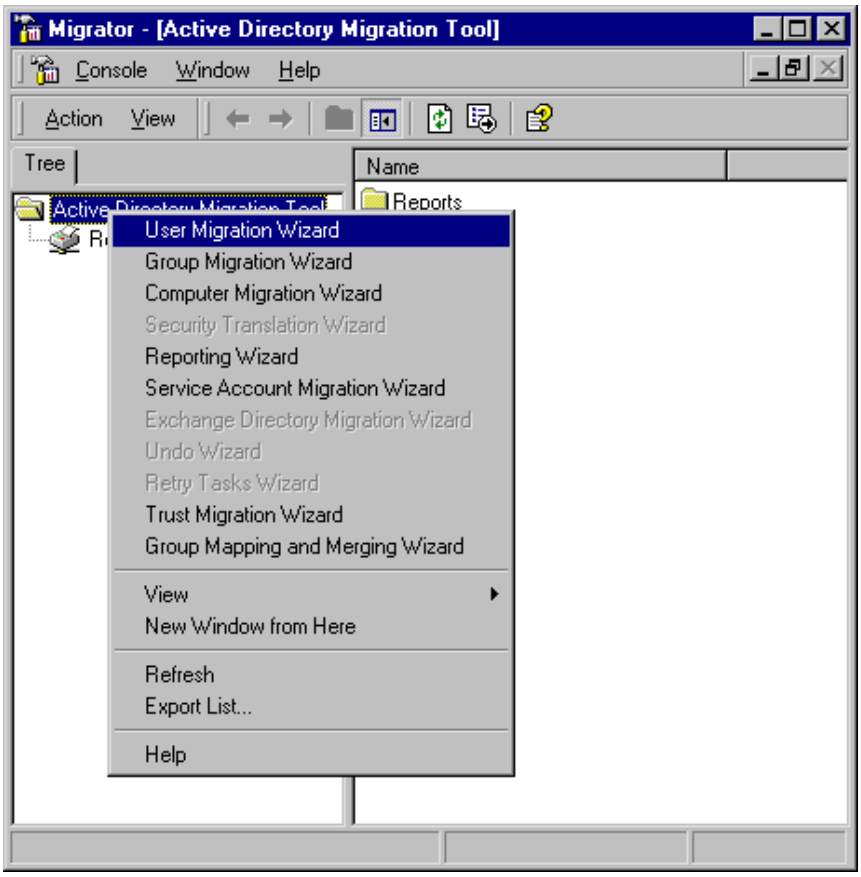
TOPIC 9: Tools Used to Upgrade the Windows NT 4.0 SAM

Despite the lack of a Move Server Wizard for Exchange 2000, Microsoft has provided us with several useful tools for upgrading our Windows NT 4.0 directory to Active Directory. The simplest method of upgrading, of course, is the in-place upgrade method. This takes your existing Windows NT 4.0 domain structure and upgrades it to Active Directory. However, as with Exchange 2000, where you may not want the same directory structure as Exchange Server 5.5, many organizations will want to migrate from an existing Windows NT 4.0 directory structure to a new Active Directory directory structure, preserving as much user data as possible. Fortunately, there's a tool to do just that: the Active Directory Migration Tool (ADMT).

Using the Active Directory Migration Tool

The Active Directory Migration Tool (ADMT) provides an efficient way to migrate accounts and trusts from Windows NT 4.0 domains to Active Directory domains. It is a feature-rich tool, shown in the following figure, that works with Windows 2000 to retain SID data as objects are moved from one domain to another.

Active Directory Migration Tool



When a user is moved from a Windows NT 4.0 domain to an Active Directory domain the user's SID, which is the identification key that allows that user access to resources in the NT domain, is copied to an attribute of the Active Directory user. This attribute, named SIDHistory, is used to grant the new

Active Directory user access to the resources still contained in an NT 4.0 domain. It is this attribute that allows for a controlled and phased migration from Windows NT 4.0 to Active Directory using ADMT.

TOPIC 10: Tools Used to Upgrade the Exchange Server 5.5 Directory

Active Directory is made up of three types of partitions: domain partitions (one for each domain), a configuration partition, and a schema partition. The Exchange Server 5.5 directory contains data we want to upgrade into the domain and configuration partitions (the schema is upgraded during setup). To accomplish this we use the Active Directory Connector (ADC).

Using the Active Directory Connector

The ADC plays a crucial role in Exchange Server 5.5 and Active Directory coexistence. The ADC synchronizes directory objects between Exchange Server 5.5 and Active Directory, both recipient directory objects and configuration directory objects. This allows organizations that have maintained an attribute-rich Exchange Server 5.5 directory to bring that data across to their Active Directory and keep it synchronized. The configuration objects of Exchange Server 5.5 sites are synchronized to Active Directory so that Exchange 2000 servers have knowledge of the sites, servers, and other configuration objects necessary to coexist. For coexistence, it is required to use the Exchange 2000 version of the ADC.

During synchronization, Exchange Server 5.5 objects are matched with equivalent Active Directory objects.

- Exchange Server 5.5 mailboxes are equivalent to Active Directory mail-enabled users.
- Exchange Server 5.5 distribution lists are equivalent to Active Directory mail-enabled groups.
- Exchange Server 5.5 custom recipients are equivalent to Active Directory mail-enabled contacts.

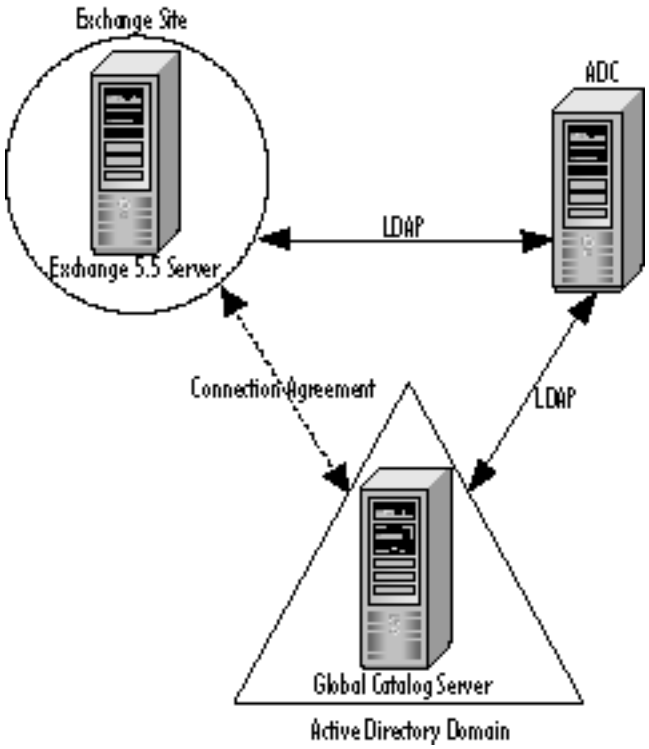
There are two versions of the ADC, one that comes with Windows 2000 and a version that is included with Exchange 2000. The Windows 2000 version can only synchronize mail recipient objects with Active Directory users and can be used to populate Active Directory and to centralize administration of the two directories. The Exchange 2000 version of the ADC also synchronizes mail recipient objects between directories. However, the Exchange 2000 version of the ADC also synchronizes configuration objects between Exchange Server 5.5 and Active Directory, allowing for coexistence between the directories.

NOTE

Exchange 2000 setup will not allow an Exchange 2000 server to join an Exchange Server 5.5 site if the Exchange 2000 version of the ADC is not installed in the enterprise.

The ADC performs synchronization by associating portions of one directory with a portion of the other directory. These associations are defined in what are called *connection agreements*. Connection agreements are established between Exchange Server 5.5 sites and Active Directory domains to define what objects from each directory should be synchronized and where. A container in the Exchange Server 5.5 directory, such as a recipient container, is associated with a container in the Active Directory domain, such as an Organizational Unit (OU). The objects in these containers are synchronized based on the schedule defined in the connection agreement. Synchronization occurs using Lightweight Directory Access Protocol (LDAP) between an Exchange Server 5.5 server with Service Pack 3, a Windows 2000 server running ADC, and an Exchange 2000 domain controller configured as a global catalog server (see the following figure).

The Active Directory Connector



WARNING

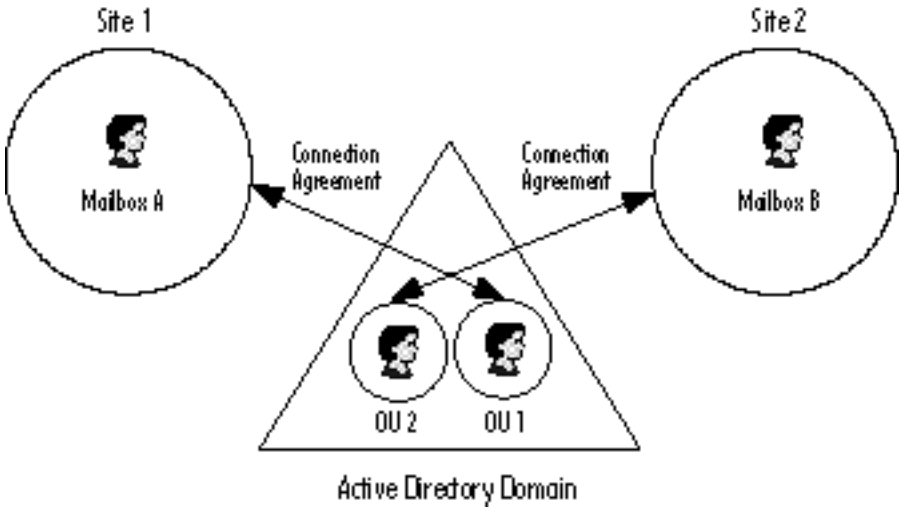
If you are going to run Exchange Server 5.5 on a Windows 2000 server, you must change the Exchange LDAP port to something other than port 389, which will be used by Windows 2000.

User Connection Agreements

User Connection Agreements define which object containers in each directory will have their objects synchronized. Therefore you must plan carefully which containers in each directory you want objects to synchronize between. You must define and configure User Connection Agreements to assure objects are synchronized between your two directories properly. It is important to define where ADC connection agreements are needed in your environment before implementing the ADC.

In the following figure there are two Exchange Server 5.5 sites and a single Active Directory domain. If you want the recipients from each site to be synchronized with different domains or with different OUs within a domain, then you must define multiple connection agreements. In this case, two connection agreements are defined to synchronize objects from each site to the domain. This is a simple example of how connection agreements are used, but you can see the importance of making sure you correctly defined where you want your objects in each directory synchronized.

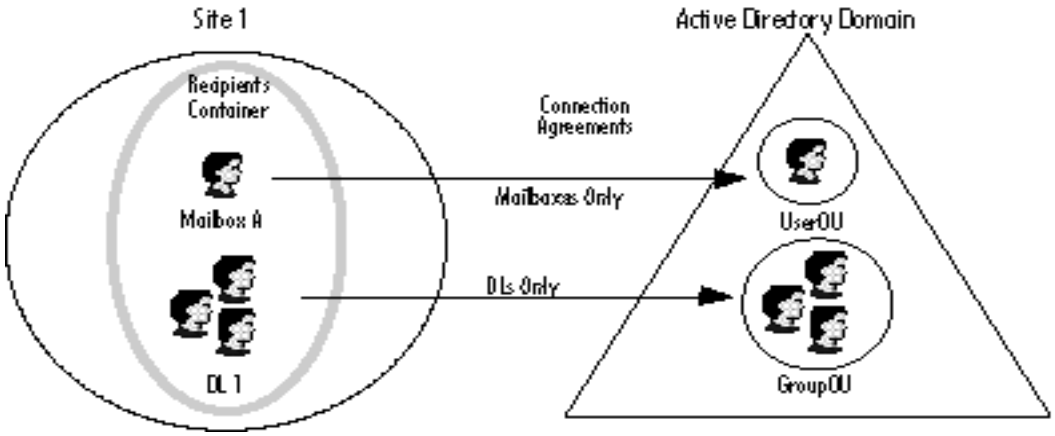
User Connection Agreements



Connection Agreement configuration is very flexible, and therefore can be complex. The connection agreement can be configured for one-way synchronization, in either direction, or two-way synchronization, based on your requirements. One-way connection agreements only write changes to the directory in one direction. This can be useful in lab or pilot projects where you don't want Active Directory to affect your production Exchange Server 5.5 directory. It is also possible to configure the types of objects a connection agreement will synchronize. To define the connection agreements necessary for your organization, you must analyze the objects in your Exchange Server 5.5 directory and your Active Directory design to determine where the Exchange objects will reside after you upgrade to Exchange 2000.

Another example of the flexibility of connection agreements can be seen in the next figure, where there are two connection agreements between Site 1 and Domain A. One connection agreement is configured between the Exchange Server 5.5 site recipient's container and an Active Directory OU named UserOU. This connection agreement is configured to only synchronize *mailbox* objects from Exchange Server 5.5 to Active Directory. The other connection agreement, between the recipient's container and an OU named GroupOU, is configured to only synchronize *distribution lists* from Exchange Server 5.5 to Active Directory. So, even if you have multiple types of objects in a recipient container or OU, you can synchronize the objects in those containers by object type.

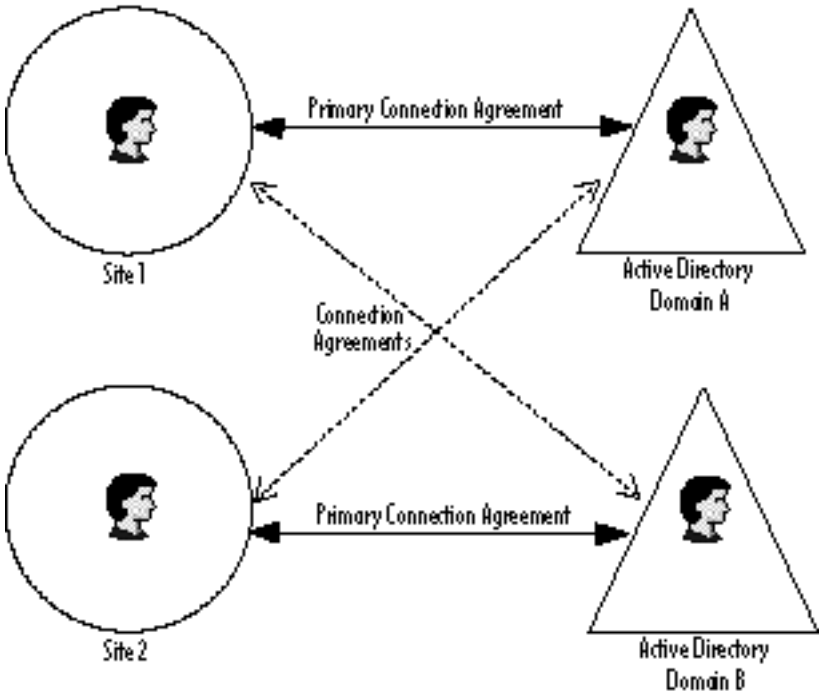
Object Synchronization



It is also possible to have multiple connection agreements configured to synchronize the same type of objects to two different destinations. This may be necessary when users from multiple NT 4.0 domains have mailboxes in a single site. When those domains are upgraded to Active Directory domains, connection agreements are put in place to synchronize the objects in the two domains with the single site. The ADC is capable of determining which connection agreement will synchronize each object because of an attribute that is written to the object. This allows for two connection agreements from the same site to two different Active Directory domains. However, what happens when you create new object in the Exchange Server 5.5 site? Which domain will it synchronize with? That is determined by which connection agreement is configured as the *primary connection agreement.* At least one connection agreement per site and domain should be defined as the primary connection agreement. The primary connection agreement will create new objects in the destination directory, if one does not exist. Though not required, it is recommended that only one primary connection agreement be defined for each site and domain to avoid creating duplicate objects in the forest.

In this next figure both Site 1 and Site 2 has two user connection agreements, one with Domain A and another with Domain B. The user connection agreement between Site 1 and Domain A is defined as a primary connection agreement. The user connection agreement between Site 2 and Domain B is defined as a primary connection agreement. When a new object, such as a custom recipient, is created in Site 1, a contact object will be created in Domain A. When a new object—such as a distribution list—is created in Site 2, a mail-enabled group will be created in Domain B. If both connection agreements from Site 1 were defined as primary connection agreements, it would be possible for duplicate objects to be created in domain A and domain B.

Primary Connection Agreements



In multisite and multidomain environments, plan carefully to assure objects are going to be synchronized as needed. Where you defined your user connection agreements and which ones you designate as primary connection agreements will depend partly on the ultimate location of your user accounts. It is important to fully understand the ADC and how it is used in different environments. You

will quickly realize the ADC and its configuration can be quite complex and should be planned and deployed carefully.

Public Folder Connection Agreements

Exchange Server 5.5 public folders are both containers that store public folder items in the public information store, and recipients that have an address in the Exchange 5.5 global address list. The public folder recipients are contained in the Exchange 5.5 directory like any other recipient. Every public folder must have an address in the Exchange 5.5 directory, though it may be hidden. These addresses are used for various things and make up part of the Exchange 2000 public folder system.

When coexisting with Exchange 2000 it is necessary to have these public folder addresses represented in Active Directory so that the Exchange 2000 public folder system continues to work as usual. Synchronization of public folder addresses between Exchange Server 5.5 and Active Directory is achieved using public *folder connection agreements*.

One public folder connection agreement should be set up between each Exchange 5.5 site and Active Directory. There is very little to configure in the public folder connection agreement; however, they are important to include in your deployment plan—along with definitions of user connection agreements.

Configuration Connection Agreements

User connection agreements and public folder connection agreements are at the heart of a directory upgrade solution and planning for them is critical. However, the Exchange 2000 version of the ADC can also synchronize the configuration portion of the Exchange directory to the configuration portion of Active Directory. This is just as important to the deployment process because it enables Exchange 5.5 servers and Exchange 2000 servers to coexist. When Exchange 2000 servers coexist with Exchange Server 5.5 servers in an Exchange Server 5.5 site, they must know the configuration of the Exchange Server 5.5 organization. When a change is made to an Exchange Server 5.5 directory—for instance, when a server is removed from the site—that change is synchronized though the configuration connection agreement to Active Directory. The Exchange 2000 server that's a member of the Exchange Server 5.5 site then knows the server no longer exists in the site. Directory configuration synchronization is supplied through one or more configuration connection agreements. Fortunately, Exchange 2000 setup automatically defines the configuration connection agreements necessary to support coexistence. When you are installing the first Exchange 2000 server into an Exchange Server 5.5 site, setup checks Active Directory to confirm you have installed the Exchange 2000 version of the ADC. Setup will not continue unless the ADC is installed because setup requires that you have defined the configuration connection agreements necessary to support coexistence.

Site Replication Service

The ADC and its configuration connection agreements are but one component required for coexistence. Another is the Site Replication Service (SRS). Within an Exchange site, the Exchange Server 5.5 directory services communicate directly with one another using remote procedure calls (RPCs). When an Exchange 2000 server is put into the Exchange 5.5 site, it also must participate in directory replication. However, as we know now, the Exchange 2000 server doesn't have a copy of the directory that has been moved to Active Directory. Since Exchange 2000 has no local directory, the SRS provides an Exchange Server 5.5 directory service during coexistence.

NOTE

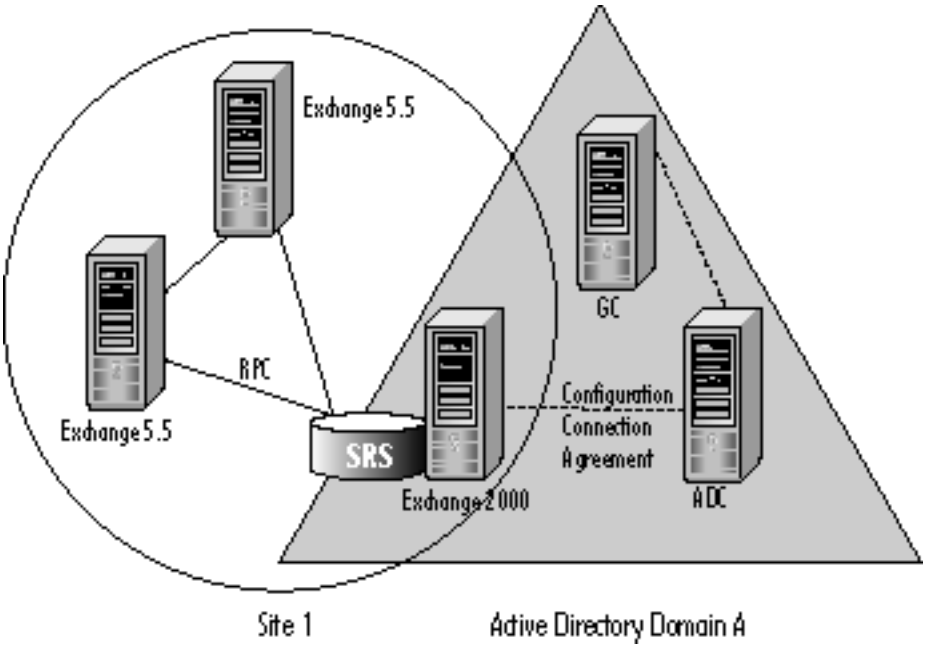
The SRS is only used for coexistence. The client and administrator interface have been disabled.

The SRS is a pseudo-directory that runs on the Exchange 2000 server only for replication to and from Exchange 5.5 servers. The SRS directory becomes part of the Exchange site, communicating with

the other Exchange Server 5.5 servers using RPC. When a directory change from an Exchange 5.5 server is replicated to the SRS on Exchange 2000, the SRS accepts the directory change. From there, the directory change is synchronized with Active Directory through the configuration connection agreement.

As shown in the following figure, as changes are replicated around the Exchange site, they are replicated to the Exchange 2000 SRS. The ADC configuration connection agreement in Domain A synchronizes these changes and replicates them to the configuration partition of Active Directory.

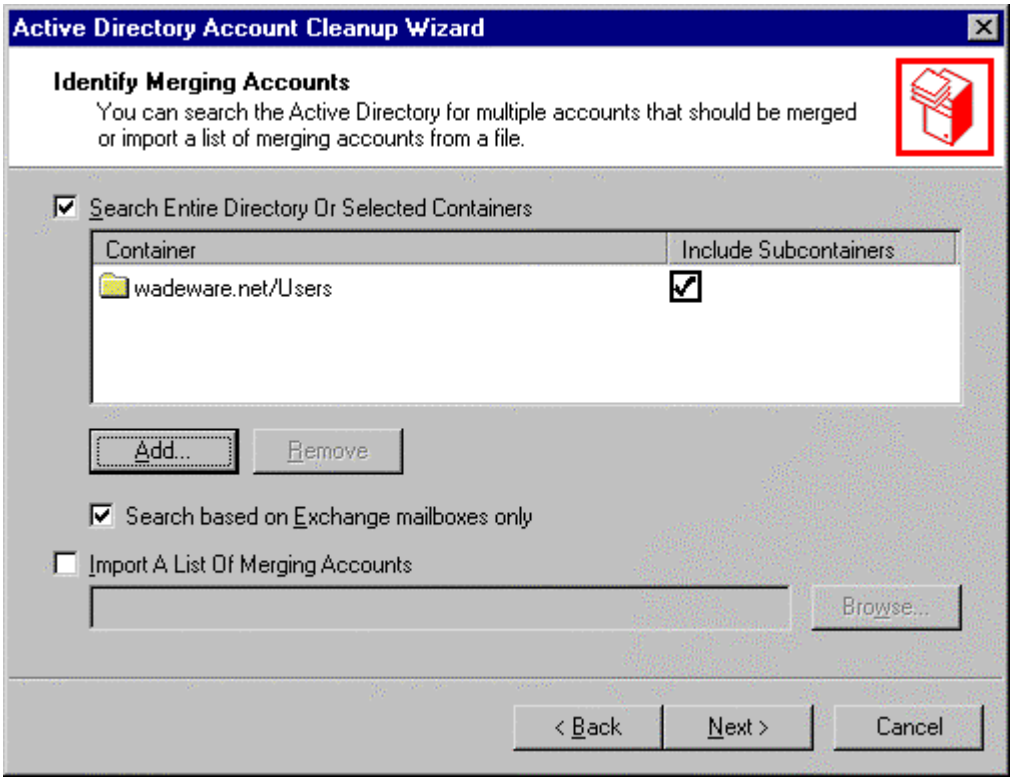
Site Replication Service



Using the Active Directory Account Cleanup Wizard

During the upgrade and during synchronization, objects such as user accounts can be created by an in-place upgrade, the ADMT, or the ADC. In some cases it is possible that one or more of these tools may create duplicate Active Directory objects. When this happens it will be necessary to use the Active Directory Account Cleanup Wizard, or ADClean. Duplicate accounts can be created during migration when two or more directories, such as Windows NT and Exchange Server 5.5, are consolidated into a single Active Directory. ADClean (see the following figure) merges these accounts, preserving the important attributes of both and creating a single account.

Active Directory Account Cleanup Wizard



For example, if you use the ADC to create accounts in Active Directory, then upgrade a Windows NT 4.0 domain to Active Directory, you will be left with two accounts for each user: one created by ADC and the other created by upgrading the domain. ADClean will consolidate these duplicate accounts. During the consolidation, group and distribution list membership is preserved (as well as the SIDs of each account) so resource access is not affected.

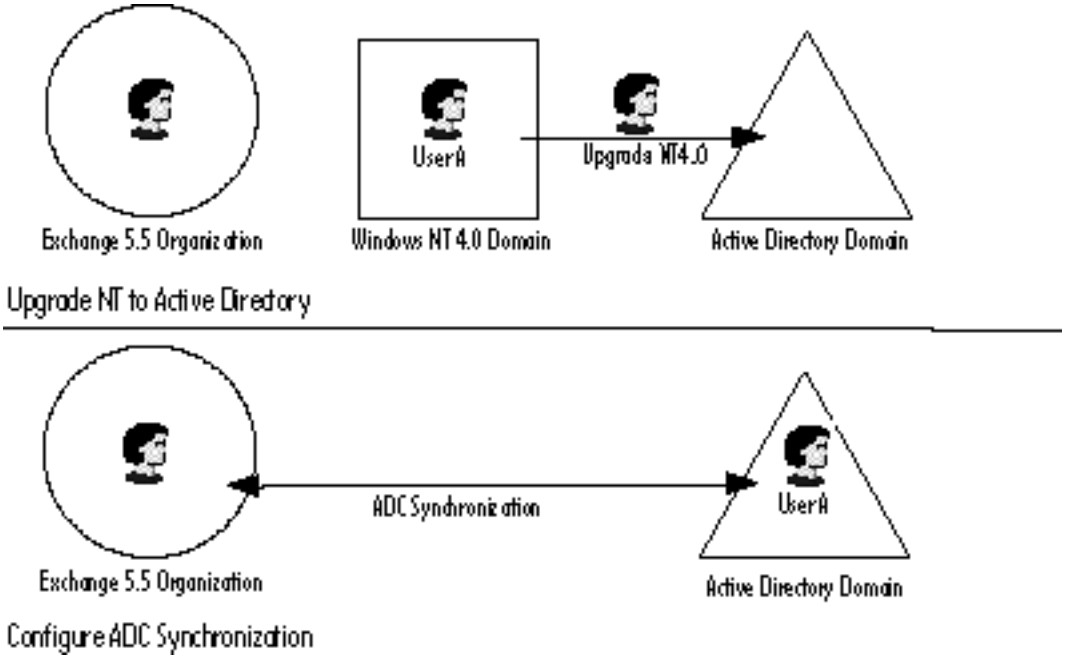
Directory Upgrade Scenarios

Now that you are familiar with the tools that will be used during the upgrade and deployment of Exchange 2000, it is important to understand the impact they will have on the directory when they are used. In your deployment it may be necessary to use the tools in a particular order, especially if you are doing a phased deployment of Exchange 2000 or Windows 2000. This section outlines some of the possible directory upgrade scenarios, showing which tools are used and the impact they will have.

Using the In-Place Upgrade Method

The simplest and most straightforward approach to upgrading your directory is an in-place upgrade. Upgrading the Windows NT 4.0 primary domain controller (PDC) in-place to Windows 2000 creates Active Directory accounts. The ADC is then configured to synchronize Active Directory and the Exchange Server 5.5 directory (see the following figure).

In-Place Upgrade then ADC

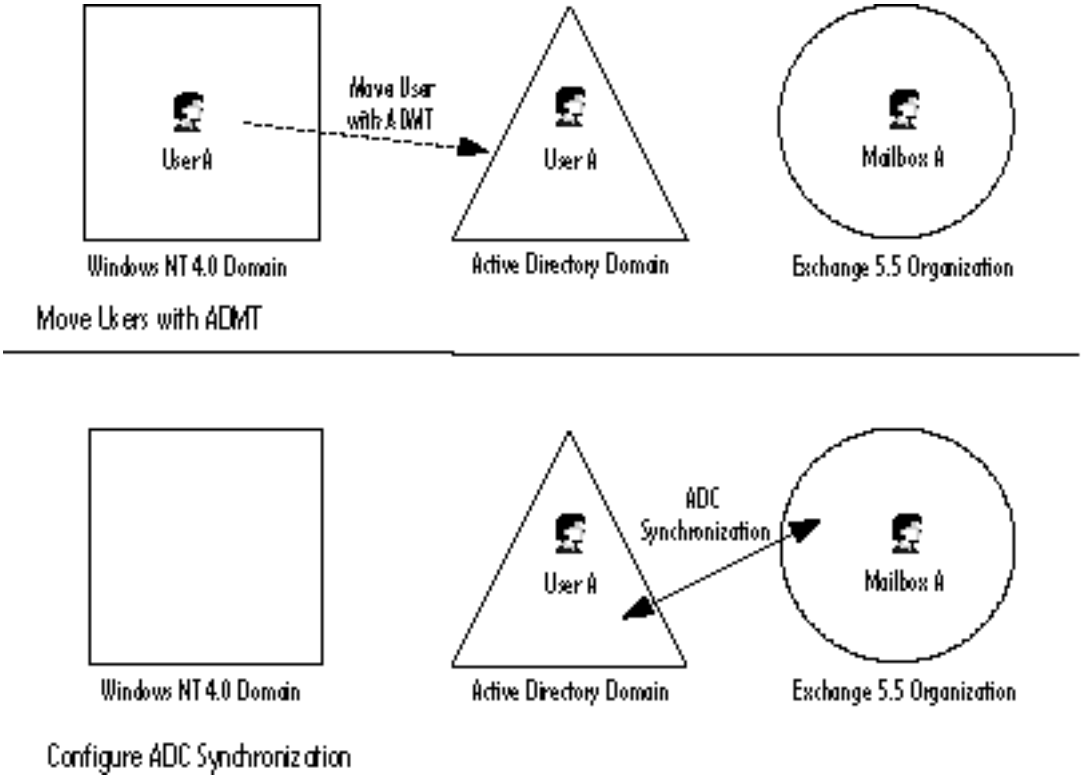


This is a common upgrade approach for smaller- to medium-size organizations and organizations that plan on keeping a similar Active Directory domain topology as they had with Windows NT 4.0. One advantage to this method is each user's original security identifier (SID) is preserved during the upgrade and stored in the upgraded users Active Directory account. This allows the upgraded user to access resources inside and outside their domain.

Upgrade Using ADMT then ADC

Active Directory is quite different from Windows NT 4.0. The reasons for and capabilities of Active Directory domains are different from those of Windows NT 4.0 domains. Because of this, many organizations are moving to a new Active Directory domain topology. This migration from an NT 4.0 domain topology to a new Active Directory domain topology will include moving users and computers between domains using ADMT. The ADMT, like an in-place upgrade, preserves the SID from the source objects as they are moved to the destination domain. Once the objects have been moved to the destination domain, the ADC is configured to synchronize between Active Directory and Exchange Server 5.5 (see below).

Migrating Using ADMT then ADC



In this scenario, the Windows 2000 deployment project is in full swing before the Exchange 2000 deployment begins. Once Active Directory users have been moved from their NT 4.0 domain to their Active Directory domain and the ADC is configured, the Exchange directory upgrade is essentially complete. Upgrading the Exchange Server 5.5 servers to Exchange 2000 will keep the association between mailbox and directory object in place.

ADC then In-Place Upgrade then ADClean

Up to this point, the scenarios have assumed Windows 2000 and Active Directory are deployed before Exchange 2000. However, many organizations don't want to wait for Windows 2000 and Active Directory to be fully deployed before they can enjoy the benefits of Exchange 2000. It is possible to begin the deployment of Exchange 2000 before Active Directory has been deployed throughout the organization. To accomplish this, at least one Active Directory domain must be created that will host Exchange 2000 servers and recipient objects. The recipient objects in Active Directory will only be used by Exchange 2000 clients for address book lookups. The users will continue to log on to their NT 4.0 accounts to access their NT 4.0 resources.

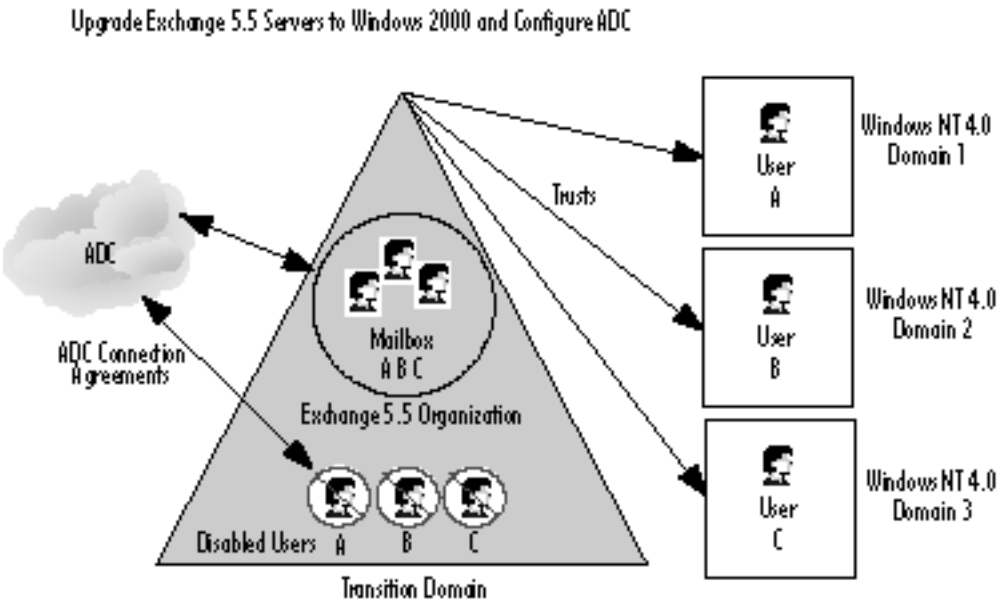
NOTE

The first domain in a forest plays a special role in the forest and cannot be removed. It is for this reason that you may want to establish your Active Directory forest with a domain that will continue to be at the root of your domain structure. In this instance, the Exchange 2000 domain would be the second domain in the forest.

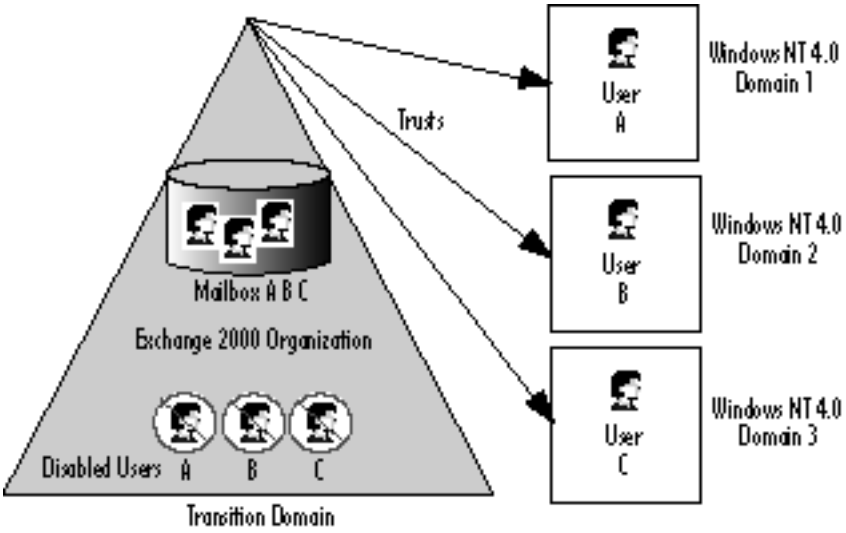
The Active Directory domain created to support Exchange 2000 is called a *transition domain*. The ADC is used to create and synchronize all Windows NT user accounts to the transition domain. The

ADC creates disabled Active Directory users that in turn make up the global address list for Exchange 2000 users. You can then upgrade your Exchange Server 5.5 servers to Exchange 2000 (see the following figures).

Using the ADC to Create Disabled Accounts



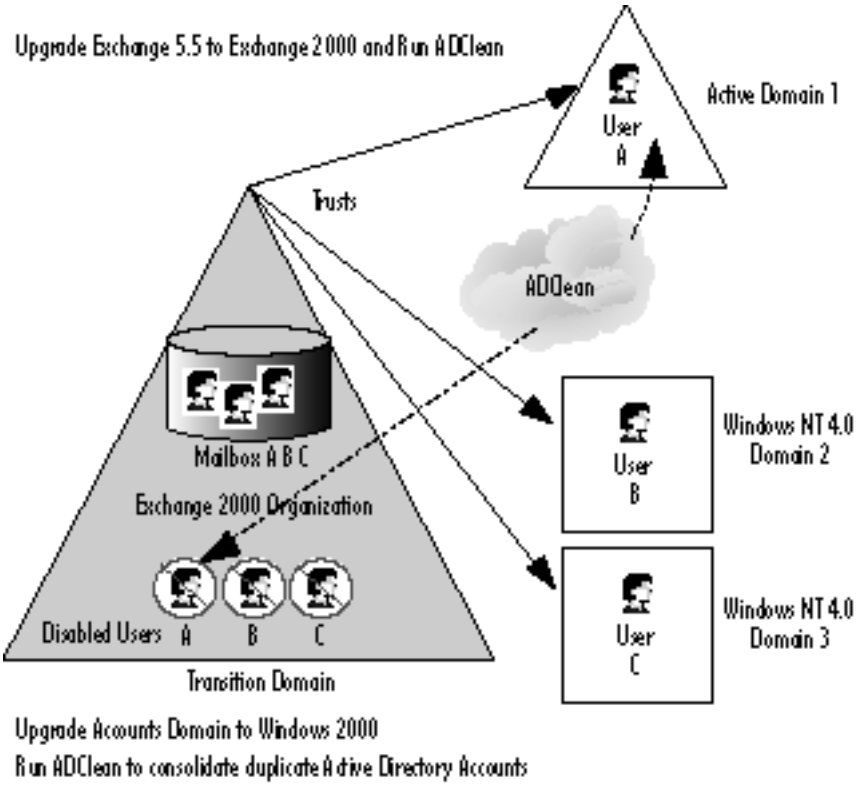
Upgrading Exchange 5.5 Servers to Exchange 2000



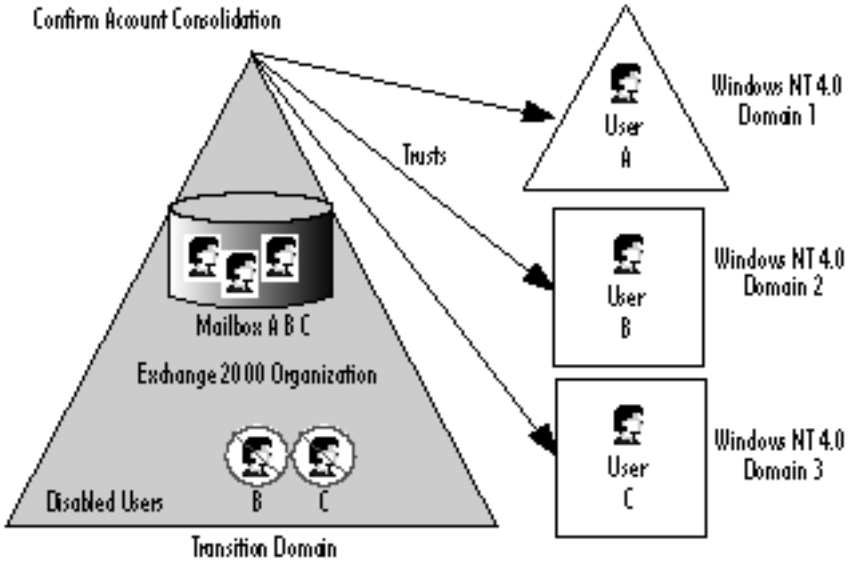
Once complete, you continue to have your NT 4.0 account domains in place; however, once your users access their Exchange mailbox, the mailbox will reside in an Active Directory domain and be hosted on Exchange 2000. With this configuration, you can benefit from Exchange 2000 in a Windows NT 4.0 environment indefinitely, and upgrade your Windows NT 4.0 domains to Windows 2000 at your leisure.

Once you are ready to upgrade your NT 4.0 accounts domains to Active Directory domains, duplicate accounts will be created in Active Directory: one that was created by the ADC and another that was created by the NT domain upgrade. Therefore, as you upgrade your NT 4.0 domains to Windows 2000, you must run ADClean to consolidate the duplicate accounts. The disabled Active Directory account created by the ADC in the transition domain will be merged into the account residing in the upgraded Active Directory domain (see the following figures).

Upgrading NT 4.0 Domains to Active Directory



Confirming ADClean Merged Duplicate Accounts



Once ADClean is complete, the user account will be associated with the user's mailbox in the Exchange domain.

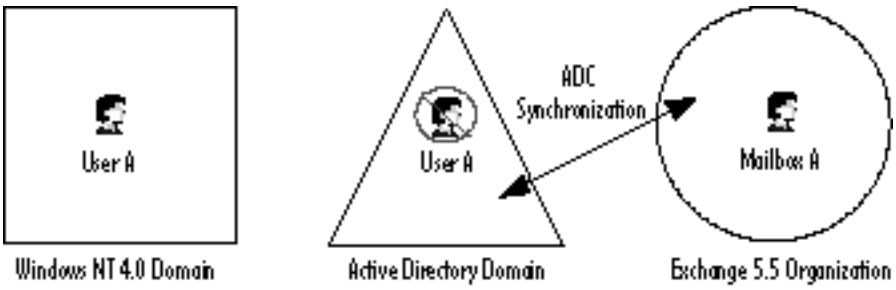
The remaining NT 4.0 account domains can be upgraded following the same process. Once the domains have gone to native mode, the Exchange 2000 servers can be moved to the domains where their users reside and the transition domain can be retired.

Upgrade Using ADC then ADMT then ADClean

Another scenario where duplicate accounts are created is one that uses ADMT to migrate accounts from NT 4.0 to Active Directory after the ADC has been configured and has created disabled Active Directory accounts for each Exchange 5.5 mailbox. This scenario is similar to the previous one; however, rather than upgrading the NT 4.0 accounts domains in place, the NT 4.0 accounts are being migrated to new Active Directory domains using ADMT.

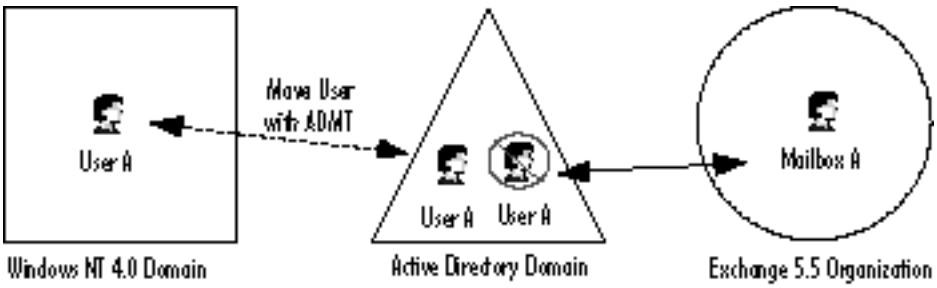
As before, the ADC creates disabled user accounts in a transition domain (see below). This time, however, the NT 4.0 accounts are moved using ADMT to a new Active Directory domain (see below).

Active Directory Users Created by ADC



ADC Creates Users in New Active Directory Domain

ADMT Creates Duplicate Accounts

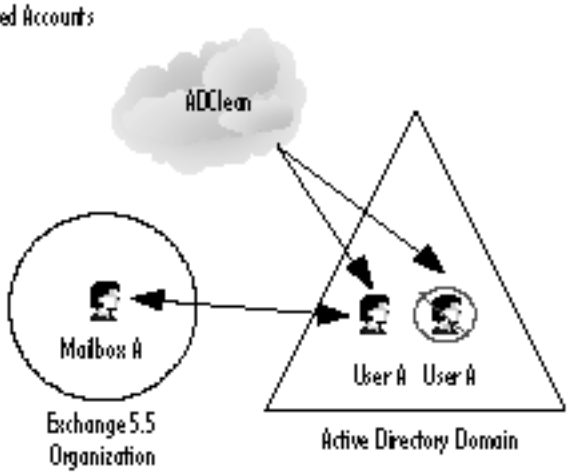


ADMT Creates Dupicate User During NT 4.0 Migration

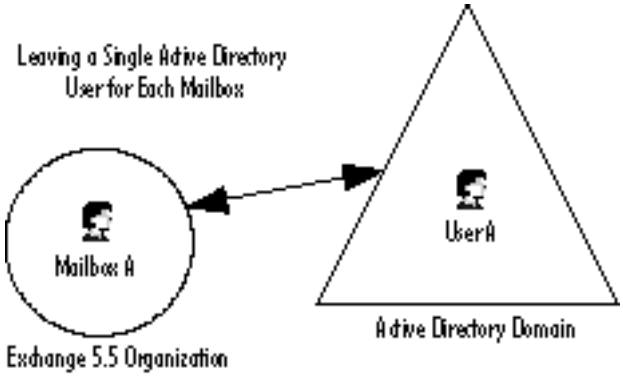
This creates duplicate accounts: one created by the ADC, the other created by the ADMT. ADClean is then run to consolidate duplicate accounts (see the following figure). The disabled Active Directory account created by the ADC in the transition domain is merged into the account residing in the new Active Directory domain (see below).

ADClean is Used to Merge Twin Accounts

ADClean Consolidates
Duplicated Accounts



Twins are Merged and One Account Remains



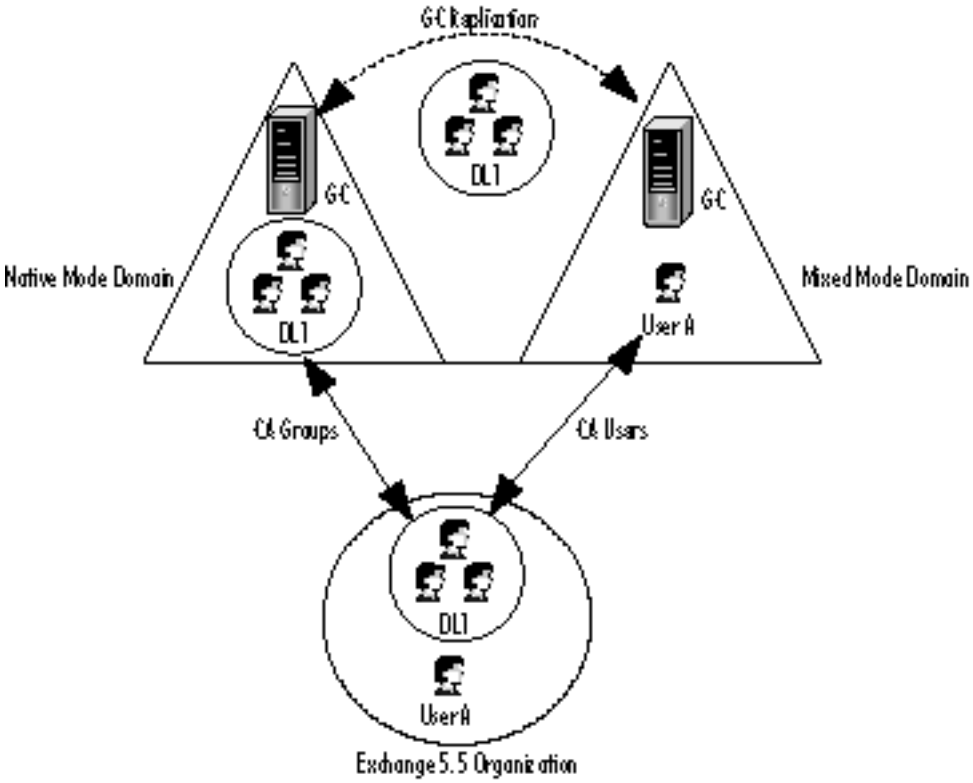
TOPIC 11: Directory Upgrade Considerations

Trying to meld two different directories into one can be challenging. It can also raise some complexities that require a creative solution. One of these challenges is due to the fundamental difference in how permissions are applied to public folders in Exchange 2000 and Exchange Server 5.5. In Exchange 2000, Active Directory objects such as users and groups are used to apply permissions to public folders. In Exchange Server 5.5, Exchange objects such as mailboxes and distribution lists are used to assign permissions to public folders. This means, for the purpose of applying permission to public folders, there must be an Exchange distribution list equivalent in Active Directory. Unfortunately, the equivalent is the Active Directory Universal Security Group, which only exists in Windows 2000 native mode.

When to Require a Native Mode Domain

To support public folder security coexistence between Exchange Server 5.5 and Exchange 2000 public folder permissions, it is necessary to have at least one native mode domain in your forest. A user connection agreement is configured between Exchange Server 5.5 and the native mode domain to synchronize groups between the two directories. When synchronization between the Exchange site and Active Directory domain occurs, the Exchange 5.5 distribution lists will become Active Directory universal security groups in the native mode domain. Universal security groups have their group membership published in the global catalog (see the next figure). When the public folder hierarchy is replicated between Exchange 5.5 and Exchange 2000 servers, Active Directory universal security groups will be used wherever Exchange 5.5 distribution lists have been assigned permissions to public folders.

Native Mode Domain for Public Folder Coexistence



This works because universal security groups are included, along with their membership, in the global catalog. Since Exchange Server 5.5 distribution lists are being translated into universal security groups in the native mode domain, a representation of the distribution list is included in Active Directory. This representation of distribution lists, in the form of universal security groups in Active Directory, allows for public folder permission to be consistent between Exchange Server 5.5 and Exchange 2000. The Exchange 2000 servers in the mixed mode domains are able to access these security principles from the global catalog and then use them to apply permissions to public folders. If you choose not to set up a native mode domain, and distribution lists are being used to apply permissions to public folders, you will lose those permissions. Permissions will have to be manually applied using Domain Global Groups or user objects.

The other option, which may make sense in smaller organizations with limited numbers of public folders, is to forego this problem and its complex solution by manually reassigning permissions to public folders once they have appeared in Active Directory. This way, you don't have to create a native mode domain or the special connection agreements to support it.

How to Successfully Use Universal Groups

Another important consideration with Exchange 2000 is the use of Active Directory global and universal groups. Windows 2000 Active Directory experts will tell you that you should avoid using universal groups and try to use global groups whenever possible. This is because there is a certain amount of overhead associated with universal groups. This overhead is incurred when a user logs in and because universal group membership is included in the global catalog and must be replicated throughout the organization.

On the other hand, Exchange experts will tell you that you should avoid using global mail-enabled groups and try to use universal mail-enabled groups. This is because global group membership is *not* available outside of the global group's domain. So if a user in one domain sends a message to the global group in another domain, the Exchange 2000 server in the sending user's domain will expand the global group from the other domain and find no members. The Exchange 2000 server wrongly deduces that there are no recipients and the message goes nowhere. The Exchange experts will tell you that if you use universal groups, whose membership is replicated to all global catalog servers, you'll never have this problem.

Another more practical solution would be to define the *expansion server* attribute for each global group to be an Exchange 2000 server in the domain that hosts the global group. This way, when a user from one domain sends a message to a global group in another domain, the Exchange 2000 server that expands the global group is from the global group's domain. It queries a domain controller in the local domain for the global group membership, the global group is successfully expanded, and the mail is delivered. Unfortunately, there is no group policy to force an expansion server to be specified on all global groups. The policy required here is a procedural one. In order to successfully use mail-enabled global groups in a multidomain environment, an operational policy has to be put in place that requires the creator of a global group to specify an expansion server that exists in the domain where the global group is being defined. This way you can use mail-enabled global groups without incurring the overhead of universal groups, and still be assured that messages will be delivered to their destination.

TOPIC 12: Upgrading the Messaging Environment

Once you have chosen an upgrade path for your Exchange 2000 deployment from Windows NT 4.0 and Exchange 5.5 to Active Directory, you must consider how to upgrade your messaging environment from Exchange Server 5.5 to Exchange 2000. Upgrading from Exchange Server 5.5 to Exchange 2000 is a considerably different upgrade from that of previous versions of Exchange to Exchange Server 5.5. This is because the structure of the Exchange 2000 organization has changed. Based on this, it may be reasonable to consider the move to Exchange 2000 as more of a migration than an upgrade, especially if your Exchange 2000 design is much different that your current Exchange Server 5.5 design. With that said, there are two approaches to moving to Exchange 2000 from Exchange Server 5.5:

- If your Exchange 2000 design is similar to your Exchange Server 5.5 design, upgrade your messaging environment in place, taking care to maintain connectivity to any foreign messaging system, such as the Internet, during the upgrade.
- If your Exchange 2000 design is considerably different from your Exchange Server 5.5 design, migrate your existing Exchange Server 5.5 environment to Exchange 2000. This way, your focus is on deploying the Exchange 2000 design and migrating data from the legacy Exchange system to Exchange 2000.

It is also important to move familiar functionality from your Exchange Server 5.5 environment to your Exchange 2000 environment. The look and feel of the client should not change without proper training and change management of the end users. This includes features like:

- Creating Exchange 2000 Address Lists that are similar to your Exchange Server 5.5 Address Book Views
- Defining an Exchange 2000 offline address book server
- Creating Exchange 2000 recipient policies that provide users with the same e-mail addresses they had in Exchange Server 5.5

By comparing your Exchange 2000 design (which may define things like Address Lists) and your existing Exchange Server 5.5 environment, you can list those things that need to be configured in Exchange 2000 as they were configured in Exchange Server 5.5—as well as those things that will be new to users and require training or some other form of communication.

TOPIC 13: Performing an In-Place Upgrade

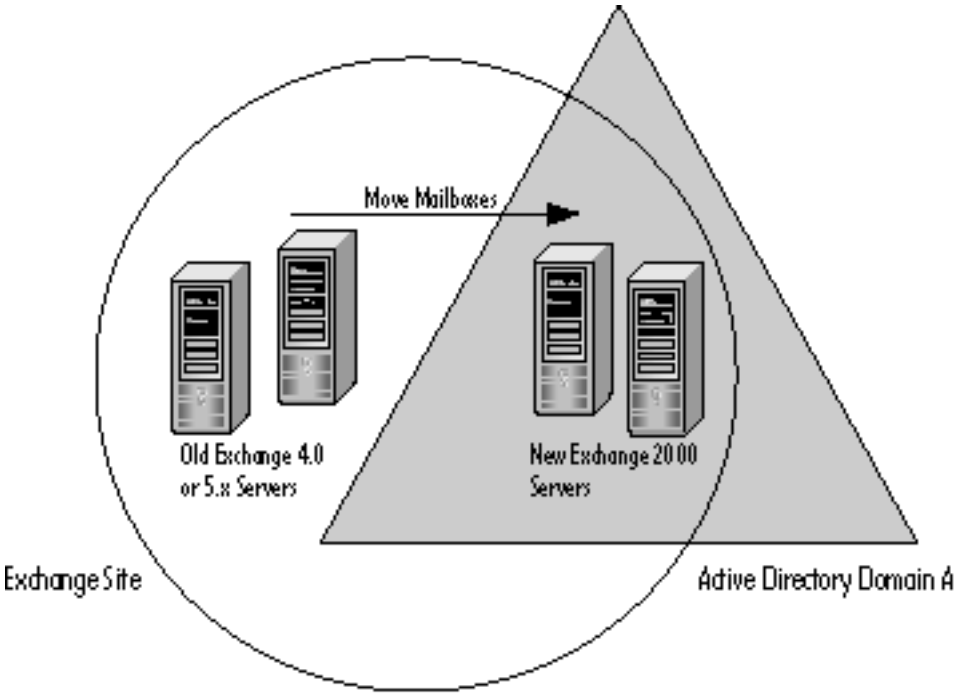
The first approach to getting to Exchange 2000 is the in-place upgrade. The in-place upgrade offers the path of least resistance, but it may only be practical in a few servers in your organization. After upgrading your Exchange Server 5.5 servers to Windows 2000, you simply run the Exchange 2000 setup to install the new software and upgrade the information stores. Exchange servers that do not have any data on them, such as connector servers, need not be upgraded. Simply reinstall Exchange 2000 and implement the connectors defined in your Exchange 2000 design. The in-place upgrade is the preferred method of upgrade in smaller environments with a limited number of servers, when the same hardware is to be used. There are several reasons why an in-place upgrade may not be the best choice for some of your servers:

- The server to be upgraded must be taken offline to do the upgrade. Other methods do not require this.
- If you are using Exchange 4.0 or 5.0, you'll first have to upgrade to Exchange Server 5.5 before going to Exchange 2000. How long the upgrade will take depends on the size and number of folders in the information store and the version of Exchange you are upgrading from. Again, other upgrade methods do not require you to upgrade to Exchange Server 5.5 first.

TOPIC 14: Performing a Move-Mailbox Upgrade

The move-mailbox method curtails many of the disadvantages of the in-place upgrade. The move-mailbox method entails moving mailboxes from existing Exchange servers to new Exchange 2000 servers. Unlike the in-place upgrade method, the move-mailbox method does not require that the Exchange server be taken offline, nor does it require that the Exchange servers be version 5.5. The new Exchange 2000 server joins the existing Exchange Server 5.5 site, coexisting with Exchange Server 5.5 through the ADC and SRS. Once the Exchange 2000 server belongs to the Exchange 5.5 site, mailboxes are simply moved from the old Exchange servers to the new Exchange 2000 servers (see the following figure). This method will be popular with organizations that plan to support Exchange 2000 on new hardware.

Move Mailbox Upgrade Method



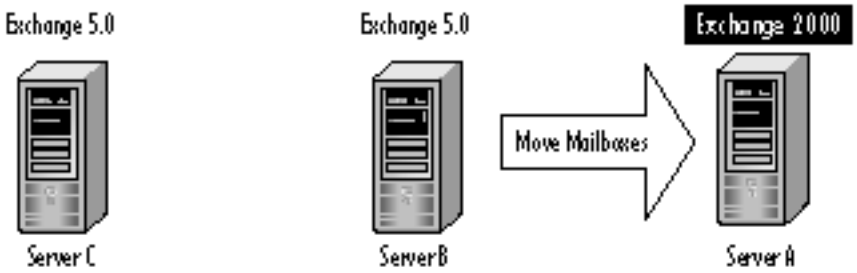
If you have dedicated connector servers, which do not host mailboxes or public folders but are bridgeheads to other sites or the Internet, the move-mailbox method doesn't apply. This is where your approach becomes more like a migration than an upgrade. The connector servers, and the bridgeheads that connect your Exchange 5.5 sites, will be replaced with Exchange 2000 servers that have their own connectors. There really is no upgrade for this process. It's more in line with a standard deployment. How you schedule the deployment tasks that will support your new Exchange 2000 architecture with the upgrade tasks that will bring your user data over to Exchange 2000 is what can separate a quality deployment plan from a mediocre deployment plan.

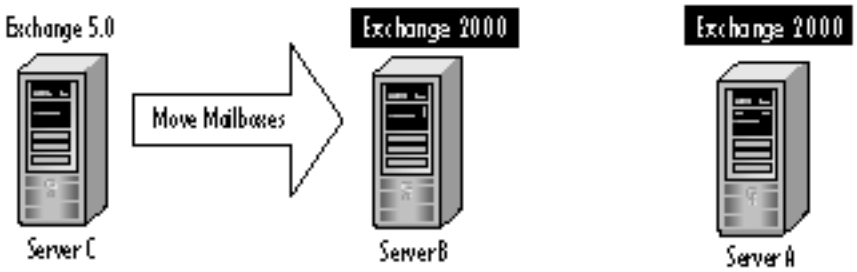
Using the Leapfrog Method

The move-mailbox method of upgrading to Exchange 2000, with all its advantages, does require new hardware. To move your existing Exchange mailboxes to Exchange 2000 requires new Exchange 2000 servers. For organizations whose current server hardware will support Exchange 2000, an added twist to the move-mailbox method can be used. The *leapfrog migration method* entails adding only a few new servers to the migration, moving users from existing Exchange servers to the new server, then installing

Windows 2000 and Exchange 2000 on the old servers and moving the mailboxes from the next Exchange server to the newly installed Exchange 2000 server (see the following figure). If you're not familiar with the term *leapfrog,* it's the name of a children's game in which the last person in a line leaps one by one over the others to move to the front of the line.

Leapfrog Upgrade Method





This leapfrog process is repeated until all servers have been upgraded to Exchange 2000. All the advantages of the move-mailbox method apply here, with a couple of additional advantages:

- Only a few new servers are required to get the leapfrog started.
- Once all mailboxes have been moved off a server, the computer can be wiped clean and a fresh Windows 2000 and Exchange 2000 installation can occur without upgrading anything.

As you can see, the deployment plan that defines your leapfrog process would have to be very specific. Scheduling mailboxes to be moved and servers to have Windows 2000 and Exchange 2000 installed, all the while ensuring that your mixed Exchange 5.5 and Exchange 2000 environment continues to support your users.

TOPIC 15: Moving to a New Organization

There are also tools available to move mailboxes to entirely new Exchange 2000 organizations. This method of migrating may be attractive to organizations that do not want to coexist. However, the tools available are somewhat cumbersome; they should be carefully tested to assure the results meet your requirements and are within your threshold for pain.

Using the Exchange Mailbox Migration Program

The Exchange Mailbox Migration program, or *exmerge*, is a tool that moves mailboxes between organizations through the use of personal store files (.pst). This process can be done in one or two phases. The one-phase process assumes the mailbox names are identical between the organizations. The two-phase process allows you to map the destination of the .pst files to new mailbox names in the new organization.

There are many drawbacks to this type of migration. For one, the single instance relationship within the information store is lost, resulting in an increase in information store size. Another is that migrated messages may have to be readdressed if replied to. Remember, the reply address will be for the old organization, not the new organization, so this can be a mess. Make sure you understand the ramifications of using *exmerge* and try it out in the lab before writing it into your deployment plan.

Upgrading Supporting Servers

Much of the focus on upgrading to Exchange 2000 has to do with upgrading mailbox servers and directories. As you know, however, there are other services and components that make up an Exchange organization. These components are just as necessary to the delivery of messages as the directory and mailbox servers, and their upgrade and deployment must be planned just as carefully.

When upgrading an Exchange Server 5.5 organization to Exchange 2000, the goal of most upgrades is to move messaging and directory data from one system to another without disrupting user availability or performance. Supporting servers, such as connector servers or bridgehead servers, do not have any data to upgrade—so in some cases it may not make sense (or even be necessary) to upgrade a particular server to Exchange 2000. Rather, it's the functionality that needs to be upgraded to Exchange 2000.

For example, if an Exchange Server 5.5 organization has two Exchange 5.5 servers configured with the Internet Mail Service (IMS) to send and receive messages from the Internet, it's not necessary to do an in-place upgrade of those servers—mainly because the Exchange 2000 SMTP connector is very different from the Exchange Server 5.5 IMS. To replace the two IMS servers there would only be one SMTP connector with two bridgehead servers configured. Here you can see that it's the functionality of the IMS that's being upgraded, not the service itself.

Upgrading Connector Servers

As with the example above, other types of connector servers should also be considered for the service they provide and the role they play in the architecture. This is key. If your Exchange 2000 organization has three routing groups connected by routing group connectors, and your Exchange Server 5.5 organization has three sites connected with X.400 connectors using bridgehead servers, the focus should be on how to implement the routing group connectors to connect the routing groups, not how to upgrade the X.400 servers.

Upgrading Client Access Using Front-end Servers

Another service provided by Exchange Server 5.5 that is very different in Exchange 2000 is Internet client access. Internet clients are those clients that use Internet standard protocols to access mailboxes.

These protocols include Post Office Protocol 3 (POP3), Internet Message Access Protocol 4 (IMAP4), Hypertext Transfer Protocol (HTTP), and Network News Transfer Protocol (NNTP). Exchange 2000 has the ability to separate the components that make up a messaging system into different physical servers: front-end servers that manage Internet client requests and back-end servers that store data. In Exchange Server 5.5 Internet clients have to connect directly to the server that hosts the user's mailbox. In Exchange 2000, with front-end servers, the Internet client only needs to connect to the front-end server and the front-end server will pass the requests to the appropriate back-end server. This way, the front-end server can be placed in a demilitarized zone (DMZ) or outside a firewall to provide added security and the Internet client does not need to know the specific mailbox server where their mailbox resides.

NOTE

MAPI clients, such as Outlook, must connect directly to the mailbox server and cannot use front-end servers. However, Outlook will automatically redirect user profiles if a user mailbox changes from one server to another.

The deployment of front-end servers in an Exchange 2000 organization does not replace any existing servers in an Exchange 5.5 organization. However, users must be made aware of the existence of the front-end servers and how to configure their Internet clients to connect to them. This should be defined in the deployment plan.

TOPC 16: Testing Your Scenario

By now you should have a better understanding of what goes into a deployment plan that will take your existing Exchange organization and upgrade it to Exchange 2000. Several choices will have to be made about which method you will use to upgrade your directories and messaging system to Exchange 2000. Whichever method or combination of methods you choose must be tested and proven to be viable in your environment.

When your Active Directory and Exchange 2000 design was being developed, it is very likely that one or more candidate designs considered for your organization were tested in a lab. You should use this same lab to test your chosen deployment methods. This can be done in two phases:

Tools and Configuration Phase This phase uses the lab to test the tools used during the migration. Several tools have particular requirements, such as trusts between domains, registry modification requirements, and the like. This phase allows you to become familiar with each tool and what it takes to make the tool work in your environment.

Upgrade Walkthrough Phase Here the lab is configured to emulate your production Exchange Server 5.5 environment and to test how each of your chosen methods work in upgrading to your Exchange 2000 design.

Much can be learned from the lab. You may discover that your choice for upgrading to Exchange 2000 does not work within the parameters you define. It may require too much user downtime for your Active Directory deployment to be completed. Once you've completed your lab testing, you should have a complete understanding of how you will deploy Exchange 2000. You should be confident in the steps required to accomplish the upgrade or migration. Nothing should be learned during the actual production upgrade; all learning should be done in the lab.

Once you've nailed down your deployment plan from what you've learned in the lab, you may want to consider performing a pilot deployment of Exchange 2000 to a select group of users across your organization. This pilot is another way for you to confirm that the deployment path you've chosen is the right one for your organization. You may find that outside the lab you discover steps that need to be added to your deployment plan. Typically, lessons learned during a pilot are that more end-user or administrator training is needed, and also that end-user expectations need to be well defined before their mailbox server is upgraded, so that they know what to expect from the upgrade. This will go a long way in keeping your customers satisfied and making your deployment a success.

