CHAPTER 12

Migrating from Legacy Exchange

Up to this point in the book, you've worked with a pristine installation of Exchange 2003 in either a Windows Server 2003 or Windows 2000 forest. But while you've worked through the examples and studied the process descriptions and configured your lab, you've probably been wondering how you're going to put this information to use in a production environment that already contains legacy Exchange servers.

Throughout this chapter, the term "legacy Exchange server" refers to servers running Exchange 5.5 or earlier. Features and options that apply solely to Exchange 2000 servers are called out separately.

Before taking on the complex task of migrating your Exchange organization, I invite you to relax and take a few moments to consider the broad expanse of history before computers and digital communications and e-mail, before even the advent of the printed word itself. Back to a simpler time when common folk such as ourselves found inspiration in tales of great heroes who battled mighty foes in pursuit of lofty goals.

One ancient character embodied the very definition of heroism itself, the Greek warrior Heracles. Overcome by madness in his early life, Heracles killed his wife and children. When he sought purification for this act, he was given 12 deadly labors, which he undertook while prepared to die. Instead, he overcame the odds and bested all his opponents. In his maturity, Heracles went on to avenge many evils and eventually had his own action figure and a slot in the AWWF (Ancient World Wrestling Federation).

The story of Heracles puts me in mind of an Exchange 2003 migration because one of the 12 deadly labors involved in defeating the many-headed Hydra. The Hydra posed a special challenge for Heracles.

Not only was each individual head of the monster especially ferocious, but if he lopped off one of the heads, two more would grow back in its place. Every apparent success put him closer to defeat, a perfect metaphor for e-mail administration, regardless of the messaging platform you use.

When you get in the middle of your Exchange migration and you face problems that seem to multiply geometrically like the heads of the Hydra, you might want to take a hint from the way Heracles solved the problem. He didn't try to do the job himself. He sought help from his nephew, who cauterized each neck as Heracles swooped off the head, preventing a new head from growing. Thus they were able to bring down the monster and move on to the next labor.

I'm not telling you to hire your nephew for your Exchange 2003 migration. What I'm advising is this: Approach the migration with all due respect and work with your colleagues to prepare for unexpected calamities. Set reasonable expectations for your management and users. Don't promise a completely transparent and problem-free transition, although that might very well happen. Instead, promise that you'll do your best to stand between your users and any monsters as you make the transition. When everything goes smoothly, your users might not declare you a hero like Heracles, but they'll be happy enough with the experience to continue bringing you cookies and chocolate cake when they want you to do something special with their e-mail. What more could an Exchange administrator want?

Pre-Migration Operational Evaluations

At some point early in your migration planning, you're going to need to sit down with a clean sheet of paper (or a blank computer screen) and figure out what you're going to do. You should test all your actions in a lab first before rolling them out into production. You might also want to arrange for a pilot program where selected users are placed in a separate forest where you perform the entire migration in an environment that more closely matches the production configurations than might be possible in a lab.

It's also important to document your current configurations. You would be surprised how often you'll need to know where a user's mailbox *used* to be, or what server used to be located in Sheboygan, or what information is available only on old backup tapes buried in a mountain somewhere.

Here is a list of items that you should include in your pre-migration planning. You'll also find a prerequisite list later on in the chapter along with a roadmap for the major steps in the migration.

Active Directory Domains

Evaluate your current domain configuration with an eye toward making sure that it will support Exchange 2003 operations. The deployment tools that come with Exchange 2003 help you to test for these conditions, but it's a good idea to get familiar with the requirements in advance. Here are some items to consider:

- **Domain controller location.** You'll need at least one domain controller in each office that has an Exchange 2003 server.
- **Global Catalog server location.** You'll need at least one Global Catalog server in each office that has an Exchange 2003 server. This can also act as the local domain controller. The simplest way to accomplish this is to make all branch office DCs into GCs. Microsoft recommends a minimum of one Global Catalog server for every four Exchange *processors*, not servers.
- **DNS configuration.** Make certain that DNSLint shows no errors. See Chapter 1, "Installing an Exchange 2003 Server," for details.
- **Active Directory Native Mode.** The Active Directory domain containing the Exchange servers must be in Native Mode so that you can use Universal Security Groups for e-mail distribution.
- **Replication or authentication problems.** Verify by a sweep of the event logs that you have no errors from directory service replication, KCC topology calculations, or authentication errors originating from domain controller accounts. You can use the EventCombMT utility, a free download from Microsoft, to perform this sweep. EventCombMT is part of the Account Lockout and Management and Lockout, available at `http://snipurl.com/5z37`.

If you're willing to spend a few dollars and a couple of weekends learning the configuration, you'll find that Microsoft Operations Manager (MOM) or a third-party product will do a better job of monitoring your event logs.

Current Exchange Organization

Evaluate your current production Exchange organization to make sure that you don't have any outstanding issues that might cause a problem during the transition to Exchange 2003.

The ExMap utility from the Exchange Resource Kit and the ExInfo utility (a free download—see Microsoft Knowledge-Base article 305816) can assist in this information-gathering phase. Here are some key points:

- **Exchange server version.** You'll need at least one Exchange 5.5 server with SP3 or higher in each site.
- **Site configuration.** Verify that you have an active Exchange server in each site. If you have sites that are no longer used, remove them from the legacy Exchange directory service prior to commencing the Exchange 2003 deployment. It is extraordinarily difficult to remove a site from the Link State Table once it has been placed there.
- **Site connectors and Directory Replication connectors.** Make sure that you get proper message routing and directory service updates through your existing connectors. Resolve any problems prior to commencing the Exchange 2003 deployment.
- **Internet connectors.** Identify the servers that are acting as Internet Messaging Service (IMS) bridgeheads. You'll want to plan on replacing these servers with Exchange 2003 servers early in your deployment.
- **Unsupported connectors.** If you have connectors to third-party messaging systems that do not have Exchange 2003 connectors, such as PROFS and SNADS, you'll need to find another way to connect the systems or plan on installing at least one Exchange 2000 server to act as the gateway.
- **Key Management Services.** If you are using digital certificates issued by an Exchange Key Management Service to encrypt and digitally sign e-mail, then you'll need to deploy a Windows Server 2003 PKI and migrate the KMS database to a Windows Server 2003 Configuration Authority. This procedure falls outside the scope of this book. Microsoft has an excellent white paper on migrating a legacy KMS.
- **Compatible backup.** Make sure the backup software you're using supports Exchange 2003 and that you have the most current backup agents installed on the Exchange 2003 servers. You can

use NTBackup that comes with Windows Server 2003 until your vendor gets a compatible agent. See Chapter 13, "Service Continuity," for details.

- **Antivirus and antispam software.** Make sure that your centrally managed antivirus and antispam solutions have agents for both legacy Exchange and Exchange 2003. Make sure that any new servers are included in signature distribution. If your antispam solution runs at a smart host in the perimeter, make sure that any tagging done by the application is compatible with the Exchange 2003 antispam API. See Chapter 13 for more information.
- **E-mail dependent applications.** If you use third-party applications that depend on Exchange, such as fax, telephony, or collaboration services, make sure that the application has a version that runs on Exchange 2003. Check their product databases for special configuration requirements and any known problems.
- **Exchange 2000 instant messaging.** Must be isolated from Exchange 2000 mailbox/public folder servers that are going to be upgraded to 2003.

Network Infrastructure

Evaluate your WAN connections and network routing topology to make sure that you have sufficient capacity for Exchange 2003 and to give you an idea where to create Routing groups. Here are some important considerations:

- **Traffic patterns.** If your WAN infrastructure handles the current Exchange message traffic with no problems or errors, you should not experience problems with Exchange 2003. However, keep in mind that the combination of Outlook 2003 in cached mode and Exchange 2003 can result in a significant amount of traffic on Monday mornings when users refresh their local message cache with e-mails received over the weekend. Warn your network services colleagues and check the Microsoft white paper titled "Client Network Traffic with Microsoft Exchange Server 2003." Download it from `www.microsoft.com/exchange/techinfo/outlook/CliNetTraf.asp`.
- **Outages.** Have you experienced any significant outages in the last six months that might recur and impact your deployment? Instabilities in WAN connections can also cause message routing issues as you make the transition from legacy Exchange routing

based on the Gateway Address Routing Table and the Link State Table used by Exchange 2003.

- **Remote users.** If remote Outlook users currently connect to the Exchange system via a VPN or dial-up to get their e-mail, you might want to consider deploying RPC over HTTP to support remote e-mail access, especially if e-mail is the only reason that users need a VPN. See Chapter 11, "Deploying a Distibuted Architecture," for more information.
- **Routing groups.** Use your Active Directory site map to help define your routing group topology. You don't need to follow them slavishly, though. SMTP works fine over high-latency connections that might cause a problem for Active Directory. Consider consolidating existing sites into a single Routing group based on the traffic volume you see after the deployment. For example, you might have several campuses in the same city connected by fractional T1s in a frame relay cloud. You might have defined separate legacy sites to control bandwidth, but with Exchange 2003, you can use a single Routing group for the entire city. This simplifies mail routing and makes it simpler to manage public folder access.

Costs

Deploying Exchange 2003 requires money, time, and people.

- **Server software.** Exchange 2003 Standard Edition lists for $699. Enterprise Edition lists for $3,999. You'll need to purchase Exchange 2003 Enterprise Edition if you want to set up shared-disk clusters or if you need multiple mailbox stores with virtually an unlimited database size. (Standard Edition allows only one mailbox store and limits it to 16GB.)
- **Client Access Licenses (CALs).** You do not need to deploy a new client, but you will need to pay for and upgrade your CALs. Each CAL lists at $67 with substantial discounts for upgrade licenses and volume purchases. If you deploy Exchange in several business units, it's theoretically possible to delay the upgrade for a particular business unit until they have the money for the CALs. But in practical terms, you should purchase your licenses up front before you begin deployment.
- **Additional personnel.** When estimating the personnel component of your deployment costs, don't forget to factor in a consult-

ant or two who can help you streamline the deployment as well as budgeting for support calls to Microsoft Product Support Services (PSS) if something doesn't go well.

- **Training.** Budget for in-depth training for the Exchange administrators and high-level summary training for the Windows system administrators, since they interact with Active Directory objects that affect Exchange operation. End-user training is important, too, if you are going to roll out new clients.
- **Client software.** When deciding whether to deploy a new client in conjunction with the Exchange 2003 deployment, keep in mind that you get the full range of features, including cached message handling, if you roll out Office System 2003 or Outlook 2003. (The standalone version of Outlook 2003 can be used for no additional change once you pay for the Exchange 2003 Client Access License.)

When deciding how to size your servers, take a look at the Microsoft white paper titled "Server Consolidation Using Exchange Server 2003." This paper takes a fair look at the factors that affect server sizing and gives you a good baseline to start your testing.

Additional Considerations

Categorize and define the potential problems and challenges you might face during the upgrade. Here are some of the more important items to consider:

- **Directory service connection failures.** If you have underlying DNS issues, either with client configuration or the DNS server itself, you can find yourself in situations where the Exchange servers can't locate domain controllers and Global Catalog servers. This results in a variety of errors. See Appendix A, "Building a Stable Exchange 2003 Deployment Infrastructure," for more information about DNS configuration and troubleshooting.
- **Inability to access public folders.** If public folder permission mapping fails for some reason, such as invalid permission list entries, then users might lose access to their public folders. See Appendix B, "Legacy Exchange Operation," for more details about permission mapping.
- **Inability to replicate public folders with legacy Exchange.** Before you can decommission your legacy Exchange servers, you

must move all public folder content to the new Exchange 2003 servers. This includes system folders that contain critical calendaring and offline address book information. It sometimes happens that this replication fails, so part of your testing should monitor for correct content of all folders prior to removing a legacy server from operation.

- **Incompatible historical backups.** If you deploy Exchange 2003 and decommission all your legacy servers, and then need to restore a mailbox from a date preceding the deployment, you won't be able to restore the legacy Exchange mailbox database onto an Exchange 2003 server. Leave the Exchange organization in Exchange Native mode until you're sure that you won't need the old backups.
- **Hardware failures.** You're going to be deploying new servers running Exchange 2003. There's always the likelihood that you'll find incompatibilities in the new hardware or component drivers. Be prepared to get quick help in the event of a failure, and make sure all hardware is listed in the Windows Server Catalog (which used to be the Hardware Compatibility List).
- **Software compatibility failures.** You could find that your selection of backup, antivirus, and antispam tools or other server utilities causes the server to become unstable. If you encounter problems keeping the server operating, one of your first steps should be to deactivate all third-party software, just to see if that makes the problem go away.

Goals

- **No service interruptions**. In today's IT environment, messaging is supposed to be as pervasive and available as a dial tone. The major contributors to downtime during a typical Exchange migration are incorrectly configured DNS settings, unstable Active Directory replication, improper hardware, improperly configured Routing groups, and lack of coordination between the Exchange administrators and the other IT staff.
- **Single mailbox-enabled account for each user**. In your existing Exchange environment, you might have many legacy mailboxes owned by a single user. Or you might have mailboxes that have no owner. During the migration to Exchange 2003, you will normalize

your mailbox ownership so that each legacy mailbox has one and only one valid user. This is done as part of the ADC deployment.

- **Retain existing mailbox and public folder permissions**. Exchange maps legacy Exchange MAPI permissions to the ACL-based security descriptors in Exchange 2003. It's important that this mapping work correctly. Be cautious and do lots of testing before making any large-scale changes to permissions.
- **Fastest possible introduction of new features.** To take full advantage of the new features in Exchange 2003, you need to complete the Exchange migration and decommission all legacy Exchange servers. Don't let weeks turn into months turn into years. Until you shift to Native mode, you won't be able to take full advantage of the features you paid for.
- **Maximize existing hardware**. It's one thing to pay for the Exchange 2003 server software and CALs. It's quite another to pay for a new fleet of servers to run Exchange. Be sure to inventory your server hardware with an eye toward adding RAM, faster disks, more storage, and possibly an updated network adapter that can offload SSL and TCP/IP services.

Exchange Migration Roadmap

You cannot do an in-place upgrade from Exchange 5.5 to Exchange 2003. This applies even if you run Exchange 5.5 on Windows 2000. All upgrades from Exchange 5.5 to Exchange 2003 involve setting up new Exchange 2003 servers and moving mailboxes and connectors to those servers.

A basic migration has three phases: upgrade the domain to Windows Server 2003 (or Windows 2000, if you want to use the older operating system), deploy new Exchange 2003 servers, and then decommission the legacy servers. Here are the high-level details for each phase. The remainder of the chapter describes the details for performing each stage.

Domain Upgrade

The roadmap for a typical single domain upgrade looks like this:

1. **Upgrade the current PDC to Windows Server 2003.** Use a leapfrog upgrade so that you have fresh hardware on the newly upgraded server. A leapfrog upgrade involves installing a new NT BDC, promoting it to PDC, and then upgrading it to Windows Server 2003. This puts the domain (and forest) at an Interim functional level, which enables certain replication features in Windows Server 2003 (such as replicating individual group members rather than the entire Member attribute) while retaining backward compatibility with NT domain controllers.
2. **Install additional Windows Server 2003 domain controllers.** Don't tempt fate by having fewer than three domain controllers in a domain. This lets you take one domain controller down for maintenance and still have two up and running. Make as many of those domain controllers into GC servers as possible.
3. **Decommission all NT BDCs.** This eliminates the need to support legacy LanMan replication.
4. **Shift the domain and forest to Windows Server 2003 functional level.** This enables you to create Universal Security Groups, a requirement in a multiple domain forest.

Exchange 2003 Server Deployment

In the second phase, you'll deploy Exchange Server 2003 alongside your legacy Exchange servers. The roadmap looks like this:

1. **Install SP4 and the latest security patches on all Exchange 5.5 servers.** The ADC requires that any legacy Exchange server that acts as a Connection Agreement endpoint runs Exchange 5.5 SP3 or higher. This gives it the ADC the ability to read and write the legacy directory service via LDAP.

2. **Normalize mailboxes.** You need to spend an afternoon, maybe a long afternoon, validating that you have a one-to-one match between each legacy Exchange mailbox and an Active Directory user. At the same time, verify that each mailbox owner actually exists in Active Directory. The ADC tools perform this check, but you don't want to wait until the middle of the deployment to

find out that you have a problem. Download the NTDSNoMatch utility from Microsoft to help with this work. See Knowledge-Base article 274173 for download and configuration information.

3. **Verify public folder permissions.** Spend another long afternoon going through the permission list for each public folder to ensure that the recipients and distribution lists actually exist. This avoids having *zombies* on the permission lists; that is, distinguished names that do not point at a valid account in the legacy Exchange directory service. Exchange 2003 contains safeguards against problems caused by zombies, but you'll have more success in your deployment if you avoid the problem completely. The Pfadmin tool is great for doing this work. Microsoft Knowledge Base article 188629 discusses how to remove invalid permission entries using Pfadmin.
4. **Install the ADC.** This updates the Active Directory schema to include all changes required by Exchange Server 2003, so it takes some preparation on the Windows side. This chapter describes those preparations.
5. **Configure Recipient and Public Folder connection agreements.** A Connection Agreement (CA) defines a pathway between Active Directory and the legacy Exchange directory service. The ADC uses CAs to transfer mailbox information from legacy Exchange to mailbox-enabled users in Active Directory and to create Distribution groups and Contact objects in Active Directory that match the distribution lists and custom recipients in legacy Exchange.
6. **Install the first Exchange 2003 server.** This creates a Configuration connection agreement in the ADC that copies information about the legacy Exchange organization into Active Directory. This server also runs an instance of the Site Replication Service (SRS) so the Exchange 2003 server can replicate directly with legacy Exchange servers in its site.
7. **Move Connection Agreement endpoints.** An Exchange 2003 server running SRS can act as an endpoint for connection agreements. The ADC Connection Agreement Wizard initially assigns endpoints to legacy Exchange servers. You have to manually move the endpoints of Recipient and Public Folder CAs to an Exchange 2003 SRS server.

Legacy Exchange Server Decommissioning

The final phase includes moving all Exchange operations over to the new servers and removing the legacy servers from the organization. Here's the roadmap:

1. **Move mailboxes.** Now that you have a fully functional Exchange 2003 server, you can move mailboxes to it from the legacy Exchange servers in the same site. You might want to install additional Exchange 2003 servers if you need the additional storage capacity and horsepower, or you can install Exchange 2003 Enterprise Edition and create additional storage groups and mailbox stores. Exchange is still in Mixed mode, so you cannot move mailboxes directly between servers in different legacy sites, which correspond to Exchange 2003 Administrative Groups.
2. **Move connectors.** The legacy Exchange server probably hosts a variety of connectors, such as the Internet Mail Connector (IMC), Site connector, Directory Replication connector, and possibly additional connectors for X.400 or third-party e-mail systems. You'll need to create new connectors on the Exchange 2003 server and make sure that those connectors work satisfactorily before removing the legacy connectors. You'll need Enterprise Edition if you have an X.400 connector.
3. **Decommission legacy servers.** At this point, you no longer need the legacy Exchange servers in this particular site. Uninstall Exchange from the servers. This removes their objects from the organization both in the legacy Exchange directory service and from Active Directory.
4. **Repeat for all other sites.** During the time that you're upgrading the first Exchange site to Exchange 2003, you can start upgrading the other sites using the same steps. You'll wake up one morning and all the legacy Exchange servers will be gone. This stage invariably takes twice as long as you originally had in the schedule.
5. **Shift to Exchange Native mode.** This step involves removing the Site Replication Service from all Exchange 2003 servers then setting a flag in the organization that releases it from compatibility with legacy Exchange.

6. **Celebration.** Don't forget this very important final step. Your Mode Shift Party (MSP) does not necessarily need to feature the unconscious forms of grinning Exchange administrators draped over piles of empty pizza boxes outside the server room, but that's certainly a possibility.

Special Considerations

The basic roadmap I'm following assumes that you start with a single domain and all legacy Exchange servers. Just a few of the possible scenarios include the following:

- Legacy Exchange servers running in several NT domains
- Legacy Exchange servers running in a Windows 2000 forest
- Mix of legacy Exchange servers and Exchange 2000 servers running in a Windows 2000 forest

Here are the additional considerations you need to include in your planning for these more complex situations.

Multiple NT Domains

If you have multiple NT4 domains and you choose to consolidate them into a single, pristine Windows Server 2003 domain, then your Exchange 2003 deployment roadmap changes just a little.

In an in-place migration, your efforts focus on transferring recipient and configuration information from the legacy Exchange directory service to Active Directory via the ADC. In a domain migration, you must first concern yourself with migrating security principals (user accounts, servers and desktops, and groups) from the NT domain to the Active Directory domain. Then you can set up the ADC and start your Exchange 2003 deployment.

An Active Directory attribute called SIDHistory contains the SID from the legacy NT domain so that users retain access to NT domain resources, such as their legacy Exchange mailboxes. Always migrate accounts using a tool that populates SIDHistory. Microsoft provides a free tool called the Active Directory Migration Tool (ADMT v2) on the Windows Server 2003 CD. You can get additional features and reporting capabilities by using third-party tools such as Domain Migration Wizard from Aelita Software or NetIQ's Domain and Exchange Migration Administrator.

Don't use the ADC to populate Active Directory with user accounts from the NT domain. The ADC does not populate SIDHistory and does not migrate user passwords, two critical features of a migration tool such as ADMT. Once you've migrated user accounts into Active Directory, then you can use the ADC to transfer legacy Exchange mailbox information to the objects, in the same way you did for an in-place migration.

From there, the roadmap matches an in-place upgrade. You install Exchange 2003 servers, move mailboxes and public folders and connectors to the new servers, decommission the old servers, shift to Native mode, and celebrate.

Legacy Exchange in a Windows 2000 Forest

If you have already deployed Windows 2000 but you still run legacy Exchange, you have a somewhat easier deployment roadmap. You can run Exchange 2003 in a Windows 2000 forest, but without some of the features you might want. (The feature set is detailed later in the chapter.) You should strongly consider upgrading your forest to Windows Server 2003 prior to deploying Exchange 2003 to get all the new features.

The details of upgrading your forest lie outside the scope of this book. (See my book, *Inside Windows Server 2003*, or *The Ultimate Windows Server 2003 System Administrator's Guide* by Robert Williams and Mark Walla. Both books are from Addison-Wesley.)

In general, the upgrade consists of modifying the Windows 2000 schema by running a tool called Adprep, and then either upgrading your Windows 2000 domain controllers to Windows Server 2003, or introducing new Windows Server 2003 domain controllers and decommissioning the old domain controllers.

An upgrade leaves the domain functional level at its current state. For example, if the Windows 2000 domain were in Mixed mode, the Windows Server 2003 domain and forest would be set to Windows 2000 Mixed functional level. You'll need to shift to a Windows 2000 Native functional level to get the ability to create Universal Security Groups prior to deploying Exchange 2003.

Once you've completed the Windows Server 2003 upgrade, you can begin deploying Exchange 2003. I do not recommend doing both upgrades at the same time because this introduces too much complexity into the deployment plan, makes recoverability more problematical, and complicates troubleshooting.

Mix of Exchange 5.5 and Exchange 2000 Servers

Speaking of keeping things simple, you should avoid deploying Exchange 2003 in the midst of an Exchange 2000 deployment that involves an upgrade from Exchange 5.5. Microsoft refers to this as a TIPTOS deployment, derived from the chemical symbols of the code names for the three Exchange products: Titanium for Exchange 2003, Platinum for Exchange 2000, and Osmium for Exchange 5.5.

Imagine the Monday meetings where you discuss configuration changes in sites with servers that have one, two, or all three versions of Exchange, maybe running with different service packs and security patches. You would need to include multiple strategies for directory service replication and multiple strategies for message routing; and you would need to keep track of the eccentricities of each type of server with your mix of antivirus, antispam, and backup agents.

Now imagine diagnosing and fixing problems caused when those servers don't want to interoperate for some inexplicable reason.

Now imagine what your resume might look like after you explain to your boss for the hundredth time why the CIO didn't get her e-mail.

If you decide to get a head start by deploying Windows Server 2003 in a mixed environment of Exchange 2000 and Windows 2000, before running Adprep, it's important that you correct an issue with the InetOrgPerson attributes in the Schema. The syntax for several attributes does not follow RFC guidelines, and if you update the schema without doing the fix, you'll "scramble" the attributes, and they cannot be fixed later on. Look at Microsoft Knowledge-Base article 325379 for more details.

Prerequisites and Precautions

Include the following items in your preparation checklist as you begin planning your upgrade:

- **Security patches.** I'm sure you don't need me to tell you to put the most current security patches on a server prior to putting it into production. This reminder is here for the "other guy" who neglects this rudimentary precaution.
- **Windows service packs.** Exchange 2003 runs fine on Windows Server 2003 without service packs, but you might want to install SP1 on your Exchange servers and domain controllers to get the security rollups. If you install Exchange 2003 on Windows 2000, you must be running Service Pack 3 or higher.
- **Exchange service packs.** Exchange 2003 SP1 should be installed as part of your deployment plan
- **Schema Master availability.** Installing Exchange 2003 requires updating the Active Directory schema. Only one domain controller can change the schema—the Schema Master. You can find the identity of the Schema Master using the Dumpfsmos utility in the Resource Kit or the Exchange Deployment Tools, which can be run anytime.
- **Upgrade domain controllers.** You can deploy Exchange 2003 into a Windows 2000 forest, but if you have many sites that have slow WAN connections, you might want to first upgrade the forest to Windows Server 2003. This lessens the impact of the Global Catalog updates performed by Exchange 2003.
- **Mobile Information Server (MIS).** Exchange 2003 has no direct upgrade path for MIS 2000. If you want to preserve functionality for existing mobile users during the Exchange 2003 deployment, keep at least one MIS 2000 server running as you migrate your mobile users to Exchange 2003.
- **Instant Messaging (IM) and Chat.** Exchange 2003 has no upgrade path for Exchange 2000 IM or Chat. This functionality has been replaced by Live Communication Server (LCS), which has a per-user license fee. If you decide to deploy LCS, keep at least one Exchange 2000 IM server running as you migrate your users to LCS.
- **ccMail connector.** Exchange 2003 does not include a ccMail connector. If you still run ccMail in your organization along with Exchange, it's time to finally make the transition.

- **Backup, antivirus, and antispam compatibility.** Your current backup, antivirus, and antispam solutions must have full compatibility with Exchange 2003 and Windows Server 2003. De-install these applications prior to performing an in-place upgrade to prevent possible compatibility problems during Setup.
- **ADC upgrades.** You should avoid TIPTOS deployments (combination of Exchange 5.5, Exchange 2000, and Exchange 2003), but circumstances might require you to begin preparations for your Exchange 2003 deployment during the final stages of the migration away from Exchange 5.5. You *must* upgrade the ADC servers to Exchange 2003 ADC prior to introducing any Exchange 2003 servers into the organization. The ADC upgrade modifies the schema, so make sure that the Schema Master is available.
- **Front-end/back-end upgrades.** If you have an existing deployment of Exchange 2000 that uses a distributed architecture, upgrade the front-end servers first and then upgrade the back-end servers. Upgrade Exchange first, and then Windows.

Many organizations choose to replace their Exchange 2000 front-end servers rather than upgrade them. Exchange 2000 requires Enterprise Edition for a front-end server, a considerable expense. Exchange 2003 supports front-end servers on Standard Edition. You cannot upgrade Exchange 2000 Enterprise Edition to Exchange 2003 Standard Edition, so it makes economic sense to replace the front-end servers completely. Minimize the hardware expense by using a "swing" upgrade—introduce a new Exchange 2003 front-end server to replace the Exchange 2000 front-end server, and then wipe the drives of the old server. Do a pristine install of Windows Server 2003 and Exchange 2003, and then redeploy it.

Active Directory Connector Operation

One of the challenges in making the transition to Exchange 2003 consists of extracting all the operational parameters for e-mail recipients, distribution lists, custom recipients, public folders, address lists, and message routing parameters from the existing legacy Exchange directory

service and putting that information into Active Directory. You as the administrator can move mailboxes and connectors off the old Exchange 5.x servers and onto sleek, new Exchange 2003 servers with minimal service disruption.

The tool Microsoft supplies to perform this operation is called the *Active Directory Connector*, or ADC. As illustrated in Figure 12.1, the ADC locates objects of interest in both directory services—legacy Exchange and Active Directory—and copies attributes for those objects back and forth to keep the objects in sync. An exception would be a one-way Connection agreement, used in specialized circumstances.

- Legacy mailbox owners replicate to Active Directory as mailbox-enabled user objects.
- Legacy distribution lists become mail-enabled Universal Distribution Groups, which get promoted to Universal Security Groups if used to control access to public folders or user mailboxes.
- Legacy custom recipients become mail-enabled contacts.

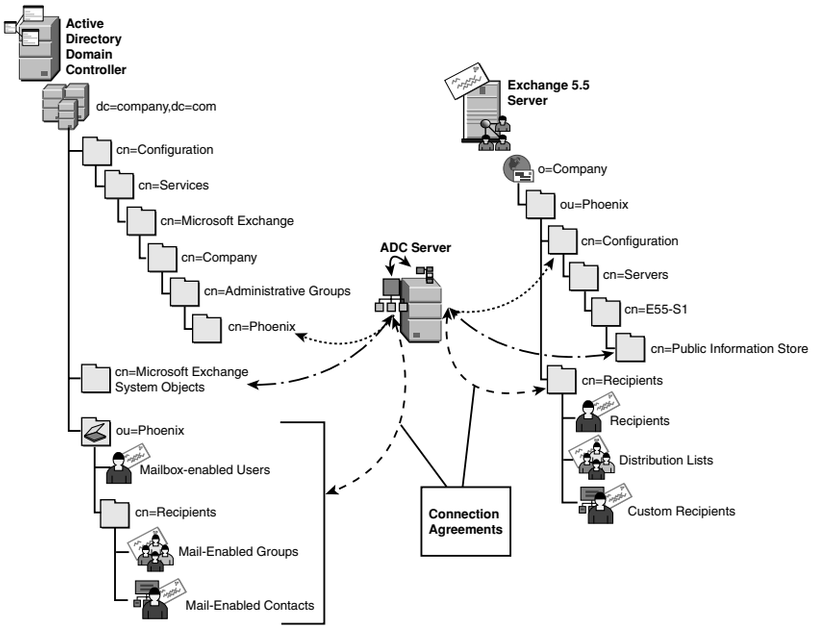

Figure 12.1 Diagram of object replication to and from the legacy Exchange directory service and Active Directory.

With the ADC working in the background, you can manage legacy Exchange objects from the Active Directory Users and Computers console. Once all mailboxes, public folders, and connectors have been moved, you can decommission the legacy servers and remove the ADC from service.

Don't use the ADC that comes on the Windows 2000 or Windows Server 2003 Setup CD. That version of ADC does not map special attributes required by Exchange recipients and public folders. If you have already installed the operating system version of the ADC, remove it before installing the Exchange version. Also, unlike the Exchange files themselves, you can do the initial installation of the ADC using the Exchange service pack files.

Connection Agreements

The ADC stores configuration parameters in Active Directory objects called Connection Agreements (CAs). A CA defines object types for the ADC to copy, the source and target containers for the objects, a replication schedule, credentials to use for making inter-server replication connections, and the name of an Exchange server to act as an endpoint on the legacy side of the CA.

The ADC uses LDAP to query and update servers on both sides of a CA, so the legacy Exchange server must run Exchange 5.5 SP3 or higher to support LDAP writes and paged results.

Exchange servers that do not form the endpoint of a CA can run earlier versions of Exchange, but you should try to run the same version on all servers to minimize potential compatibility issues and increase flexibility.

The ADC uses three types of CAs:

- **Recipient.** This CA maps the attributes of User, Group, and Contact objects in Active Directory with Recipient, Distribution List, and Custom Recipient objects in the legacy Exchange directory service.

- **Public Folder.** This CA maps legacy public folders with Public Folder objects in Active Directory to permit Exchange 2003 to accept e-mail on behalf of the public folders.
- **Configuration.** This CA maps some of the objects in the legacy Configuration container with objects in the Exchange 2003 Organization container in Active Directory. You cannot create this CA manually. Exchange Setup configures the CA as part of installing the first server in each legacy site.

Because each site forms a separate naming context in the legacy Exchange directory service, you must create a separate User and Public Folder CA for each site. The Connection Agreement Wizard in Exchange 2003 automates this process. You can use the same ADC for multiple sites. Consider installing multiple ADCs if you have large geographical separations or so many sites that you would overload a single ADC server.

ADC Mailbox Mapping

To build a mental picture of the way the ADC operates, it helps to understand the function of certain critical attributes that tell the ADC how to select objects and which e-mail parameters to copy between the objects.

Let's assume that you do an in-place upgrade of an NT4 domain to Active Directory. This transfers user account information from the PDC's SAM into Active Directory, including the users' original SIDs and passwords. As shown in Figure 12.2, a user's SID provides the initial link between the user's domain account and the user's legacy Exchange mailbox. Legacy Exchange stores this SID in the Primary Windows NT Account attribute. Active Directory stores the SID in an attribute called ObjectSID.

Initial ADC Attribute Copy

When you configure a Recipient Connection Agreement, the ADC makes an LDAP connection between the two directory services and, for each recipient object in the legacy Exchange directory service, it reads the Primary Windows NT Account attribute and then searches for a user object in Active Directory with a matching ObjectSID attribute.

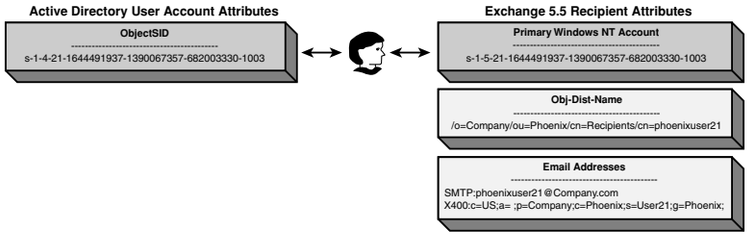

Figure 12.2 Initial linkage of user object in Active Directory to legacy mailbox via user SID.

Once the ADC makes this match, it copies the e-mail attributes from legacy Exchange to the Active Directory object. Figure 12.3 shows a few of the copied attributes. An ADC Policy object in Active Directory determines which attributes to copy and maps the legacy Exchange attribute names to their Active Directory equivalents.

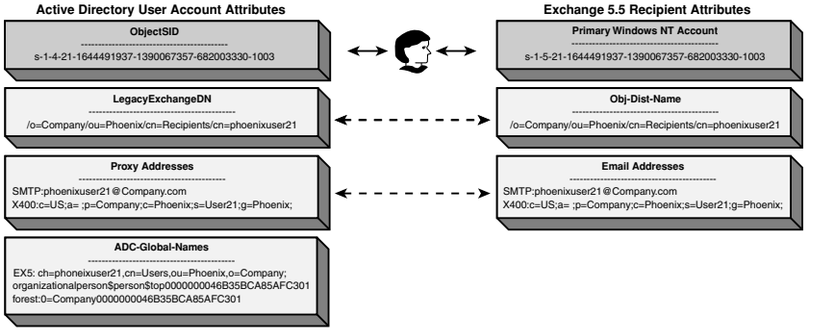

Figure 12.3 Following initial ADC replication, e-mail attributes copied to Active Directory object and ADC-Global-Names created.

ADC-Global-Names Attribute Creation

In addition to copying attributes from legacy Exchange, the ADC assigns a new attribute called ADC-Global-Names to the Active Directory object. This permits the ADC to store detailed matching information that simplifies subsequent searches and reduces the LDAP traffic required to perform object mapping. The initial content of the ADC-Global-Names attribute includes two elements:

- **EX5.** This element contains the Distinguished Name and object class of the legacy Exchange object along with a timestamp of the last update and a set of flags that control the update methods used by the ADC.
- **Forest.** This element contains the Distinguished Name of the Active Directory forest along with an update timestamp and some flags.

The next time the Connection Agreement runs, the ADC looks for User objects that have an ADC-Global-Names attribute, uses the EX5 element to locate the complementary object in legacy Exchange, and then replicates any updated e-mail attributes to the legacy object. This transaction also replicates the ADC-Global-Names attribute.

After this replication, as shown in Figure 12.4, the ADC then adds two elements to the legacy Exchange copy of ADC-Global-Names:

- **NT5.** This element contains the Globally Unique Identifier (GUID) of the legacy Exchange organization along with an update timestamp and some flags.
- **FOREST.** This element contains the GUID of the Configuration container in Active Directory along with an update timestamp and some flags.

The next time the Connection Agreement runs, these new elements replicate from legacy Exchange to Active Directory. At this point, the ADC can match users to mailbox owners based solely on their ADC-Global-Names attributes and no longer needs their SIDs.

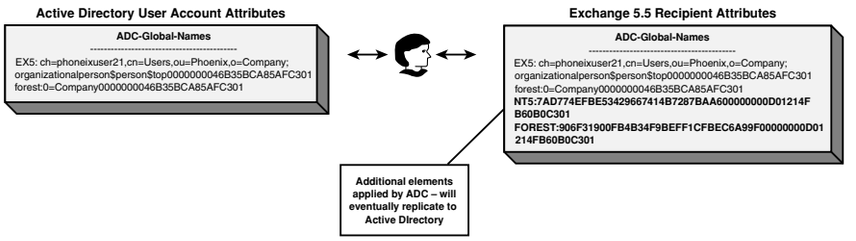

Figure 12.4 Following replication back to legacy Exchange, the ADC-Global-Names provides all mapping information needed to keep objects in sync.

NT Account Migrations

Not all transitions from NT to Active Directory involve an in-place upgrade of the PDC, though. Many organizations create a pristine Active Directory domain and then use a utility such as the Active Directory Migration Tool (ADMT), or a third-party migration utility, to move user, group, and computer account information into the Active Directory domain.

Unlike an in-place upgrade, which retains the users' original domain SIDs, a migration creates new user accounts with new SIDs. It also saves the original NT domain SIDs into a special Active Directory attribute called SIDHistory.

When a user authenticates in the Active Directory domain, the SIDHistory value gets included in the user's access token. Essentially, this gives the user two account identities: the new Active Directory account, represented by the ObjectSID attribute, and the old NT account, represented by the SIDHistory attribute.

In a migration involving Exchange, first create the user accounts in Active Directory using the migration utility of your choice, and then install and run the ADC to populate these objects with e-mail attributes. As shown in Figure 12.5, the ADC starts off by matching a mailbox owner's SID with a SID stored in SIDHistory. Once the ADC completes this initial match and copies the e-mail attributes, it can then use ADC-Global-Names to permanently link the two objects.

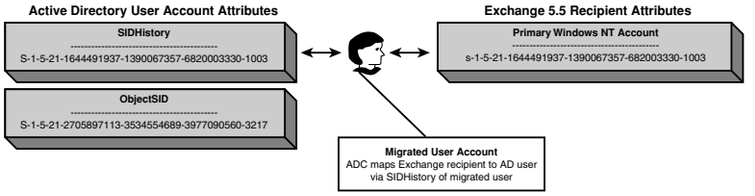

Figure 12.5 Migrated user maps to legacy Exchange mailbox via SIDHistory attribute.

Invalid User Accounts

The ADC matching process might seem straightforward, but if you read between the lines, you'll see that the ADC makes a couple of critical assumptions:

- **Valid mailbox owner.** Every mailbox in the legacy Exchange directory service has an owner that exists in Active Directory.
- **Unique mailbox owner.** No two mailboxes have the same owner.

One or both of these assumptions might prove invalid in a production environment. For example, although it's unusual to have a mailbox with no owner, it's possible for someone to create a mailbox and deliberately not put an entry in the Primary Windows NT Account field. Or the mailbox owner might be assigned to a group, something not supported by Active Directory. Missing owners can also occur in domain migrations, where an NT account might not successfully copy to Active Directory for one reason or another. Keep in mind that a mailbox can be assigned only to a single user.

If a legacy mailbox owner does not exist as a user object in Active Directory, the ADC creates a *disabled* user object to represent the recipient. As shown in Figure 12.6, this disabled user object has no legacy NT domain SID, so the ADC creates an attribute called msExchangeMasterAccountSID and populates it with the user's legacy SID. It then uses this attribute as the initial match between the disabled user object and the legacy mailbox owner so it can populate the object with e-mail attributes and set up the ADC-Global-Names link.

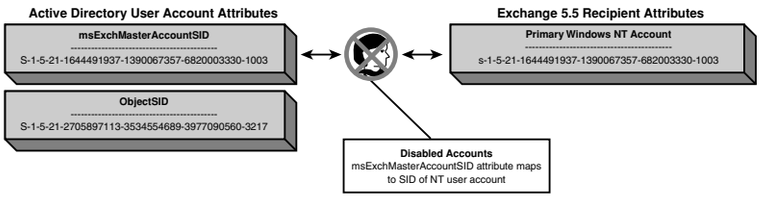

Figure 12.6 ADC creates a disabled user object when confronted with a legacy Exchange mailbox without a direct match in Active Directory.

Don't Enable the Disabled User Objects

A disabled user object created by the ADC acts solely as a placeholder. It has no authentication functions. As shown in Figure 12.7, the disabled object has a scrambled logon name and no User Principal Name (UPN), indicating that it should not be used for logon purposes. (You can't see it in the user interface, but the account also gets a randomly generated complex password.)

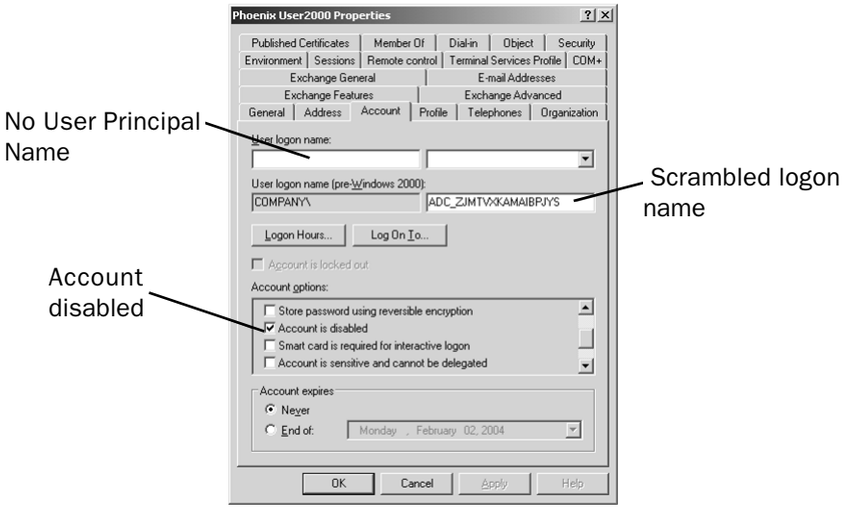

Figure 12.7 Disabled mailbox created by ADC not intended for authentication purposes. It's simply a placeholder for a resource mailbox.

If you do a thorough job of migrating user accounts from each NT domain to Active Directory, you should not see any disabled user accounts after installing the ADC. If you *do* get a disabled user account, don't simply change the logon name and enable the account. Determine why the legacy mailbox did not have a valid owner, correct the condition, and then delete the disabled user account and let the ADC find the correct object. Microsoft Knowledge-Base article 316047 discusses the various negative effects of enabling a disabled ADC placeholder account and offers several workarounds.

Multiple Mailbox Owners

Another common ADC matching issue involves so-called resource mailboxes. These mailboxes don't represent users. Instead, they represent conference rooms, projectors, audio equipment, laptop computers, and so forth. By creating mailboxes for these items, you can use the free/busy information in Outlook calendars to schedule access to the resources.

Resource mailboxes tend to have the same owner. For example, a single admin assistant in an office might own all the resource mailboxes for the conference rooms and audio-visual equipment. This presents a problem for the ADC, because Exchange 2003 permits users to have only one mailbox. You can resolve this problem using an ADC feature called NTDSNoMatch. Here's how it works.

Consider a user who has ownership of a primary mailbox and several resource mailboxes. The ADC Tools has a Resource Mailbox Wizard that looks for multiple mailboxes owned by the same user. It presents these mailboxes in a tree with the suggested primary mailbox shown in bold, as shown in Figure 12.8.

The wizard determines its candidate for the primary mailbox by matching the mailbox alias to the user name. If the wizard makes a mistake, you can highlight the actual primary mailbox and click Set as Primary. (The Resource Mailbox Wizard in the ADC Tools replaces the NTDSNoMatch utility described in Microsoft Knowledge-Base article 274173.)

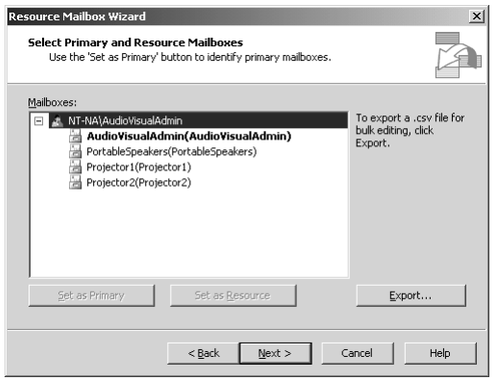

Figure 12.8 Primary mailbox can be mapped to user account separately from resource mailboxes using Resource Mailbox Wizard in ADC Tools.

The wizard takes the settings you configure in the tree and marks each resource mailbox by placing the word NTDSNoMatch in Custom Attribute 10 of the mailbox object in legacy Exchange. Figure 12.9 shows an example.

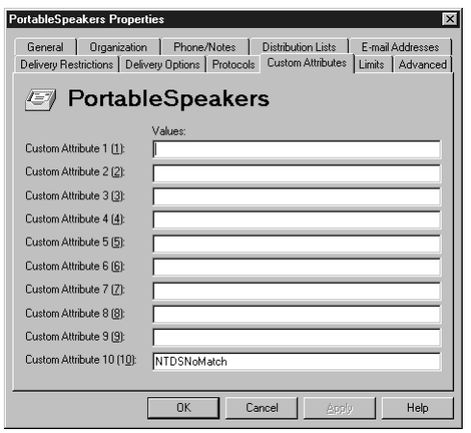

Figure 12.9 Resource mailboxes marked with NTDSNoMatch entry in Custom Attribute 10 of legacy Exchange object.

When the ADC runs the Recipient Connection Agreement the first time, it copies the e-mail attributes from the primary mailbox to the matching user object in Active Directory. It then creates disabled user accounts for each resource mailbox and places the original owner on the permission list for those mailboxes, so the original owner retains the ability to open the mailboxes, even though they are now owned by the disabled user accounts.

Active Directory Account Cleanup Wizard

If you should accidentally or deliberately use the ADC to create a set of disabled user accounts in Active Directory prior to migrating users from one or more legacy domains, you can recover full functionality in two stages.

- First, migrate user accounts using ADMT or a third-party migration tool. Because the migrated accounts have actual logon names, not the scrambled logon names assigned by the ADC, the migration succeeds so long as you don't target the new user objects to the same container that holds the disabled user objects.
- Second, use the Active Directory Account Cleanup Wizard that accompanies the ADC to merge the e-mail attributes from the disabled user objects to the actual user objects and then delete the disabled objects.

The AD Account Cleanup Wizard is installed along with Exchange 2003 and can be accessed via the Start menu using the path **Start | All Programs | Microsoft Exchange | Deployment**. Run the Active Directory Cleanup Wizard as follows:

1. At the initial welcome screen, click **Next**. The Identify Merging Accounts window opens, as shown in Figure 12.10.

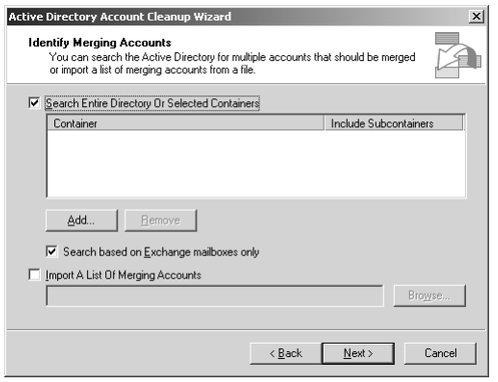

Figure 12.10 AD Cleanup Wizard showing Identify Merging Accounts window where you select a search container for the cleanup.

2. Leave the **Search Entire Directory or Selected Containers** option selected along with the **Search Based on Exchange Mailboxes Only**.
3. Click **Next**. After a period of searching, the Review Merging Accounts window opens to display the list of disabled accounts that match enabled accounts. Figure 12.11 shows an example.

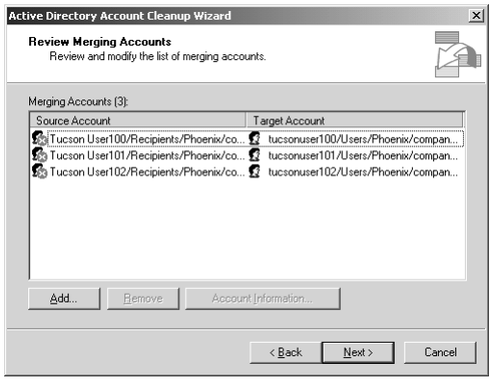

Figure 12.11 Review Merging Accounts window gives side-by-side comparison of disabled user object and live user object.

4. Click **Next**. The Begin Merging Accounts window opens, as shown in Figure 12.12.

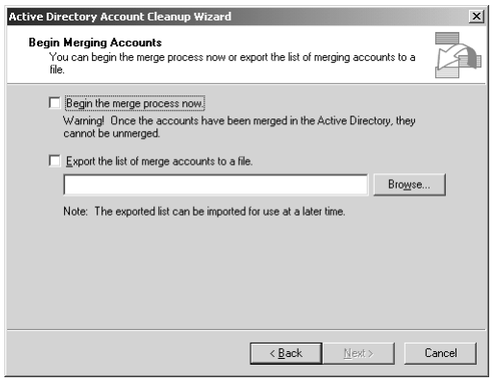

Figure 12.12 Begin Merging Accounts window provides options to do the merge or save to a file.

5. Check the **Begin the Merge Process Now** box.
6. Click **Next** to begin the merge. Acknowledge the warning that pops up.
7. Once the merge has completed, a Summary window opens. If you see any errors, follow up by checking the Adclean.log file in the \Exchsrvr\bin folder.

Now check the Recipients folder that originally held the disabled user accounts and verify that the accounts have disappeared. You might need to press F5 to refresh the display. Check the Properties window of a user account to verify the presence of the Exchange tabs and that the Exchange information looks correct.

As a recap, you should not need to use the Active Directory Cleanup Wizard if you perform the migration steps in the proper order (migrate and then install the ADC.) If you have a few accounts that did not migrate the first time, you can use the Active Directory Cleanup Wizard to merge the e-mail attributes and avoid a remigration. You can also run Adclean.exe from the command line. The utility has several switches. See Microsoft Knowledge-Base article 270655 for details.

ADC and Distribution Lists

Exchange 2003 uses Distribution groups and Security groups in Active Directory to represent distribution lists. When the ADC encounters a

distribution list in the legacy Exchange directory service, it creates a Universal Distribution Group in Active Directory.

The ADC creates Universal groups so that the members can get mail from any user in any domain in the forest. Universal group membership replicates in the Global Catalog so that membership expansion works correctly.

The ADC creates Distribution groups rather than Security groups just in case the target domain has not been upgraded to Windows 2000 Native functional level or higher. Distribution groups have an SID, but they cannot be used on Access Control Lists (ACLs) for security objects such as NTFS files and folders, Registry keys, and Active Directory objects. Creating Universal groups also avoids conflict with Windows administrators, who might not want a pile of new Security groups to appear in Active Directory following the e-mail migration.

Automatic Security Group Upgrades

Populating Active Directory with Universal Distribution Groups can lead to a problem, though. Legacy Exchange allows distribution lists to control access to resources such as public folders and user mailboxes.

In Exchange 2003, MAPI permissions on a public folder correspond to Access Control Entries (ACEs) on an ACL for the folder. Figure 12.13 shows a comparison of the MAPI permissions and ACEs for an example public folder. The example shows that a group called TucsonDistro1 appears on the MAPI permission list with the Author role, and that Exchange converts this to a set of ALLOW and DENY entries for two ACEs in the ACL for the folder.

It's this correlation of MAPI permissions to ACL entries that causes a problem when the ADC creates a Universal Distribution Group. If the distribution list represented by that group appears on the MAPI permissions of a public folder, then the Exchange 2003 Information Store can't create an Access Control Entry for the group to put on the ACL for the folder.

Exchange 2003 resolves this in the same way that your mother resolved arguments with you. It doesn't take no for an answer. If the Information Store sees that a Universal Distribution Group has been placed on the MAPI permissions for a public folder or user mailbox, it automatically promotes the group to a Universal Security Group and then puts the SID of the group in the ACL.

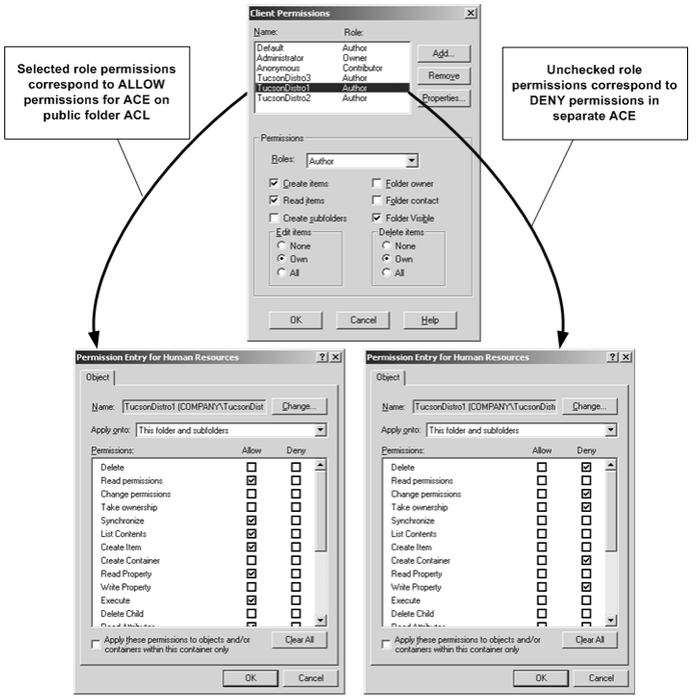

Figure 12.13 MAPI role corresponds to a set of Allow and Deny permissions in standard Windows ACL.

Distribution List Membership

When the ADC creates a new Universal Distribution Group, it populates the group with members based on the membership of the legacy Exchange distribution list.

For example, if the legacy Exchange directory service contains a distribution list called South Park that holds a recipient named Kenney, the ADC creates a Universal Distribution Group called South Park and links the group's Member attribute to the Kenney object.

If a distribution list contains an invalid recipient—for example, if someone deletes the Kenny object from Active Directory (the b#*$%ds)—the ADC would create a disabled user account to represent the recipient and then would create the Universal Distribution Group with a link between the Member attribute and the disabled account.

Subsequent changes to the group membership in Active Directory replicate to legacy Exchange as a change to the distribution list members.

If you permanently delete the newly created Kenny account from Active Directory and remove him from the membership of the South Park group, then the ADC removes him from the legacy distribution list, as well.

Forest and Domain Preparation

The first major stage of the deployment involves modifying the Active Directory schema and creating the top-level containers in the Configuration naming context. This is done as part of installing the ADC. Figure 12.14 shows the Exchange organization objects following the installation of the ADC and before installing the first Exchange server.

The Forestprep and Domainprep steps can be run anytime in advance of actually starting the upgrade and installing the ADC. You can also run the deployment tools several times in preparation for deploying the ADC.

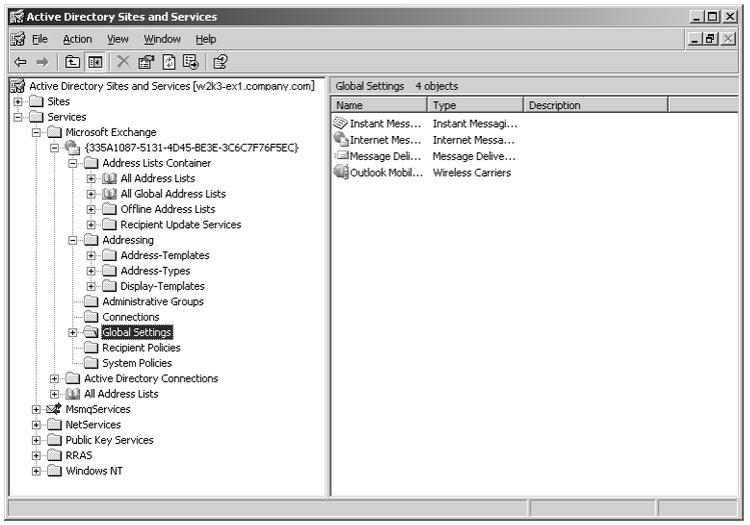

Figure 12.14 The ADC will create Organization placeholders but does not populate servers or connections until the first Exchange 2003 server is installed.

This method for preparing the organization avoids the necessity for running ADC Setup with an account that has both full administrator rights in the legacy Exchange organization and Enterprise Admin permissions in the Active Directory forest. Many enterprises do not permit combining these two functions into a single administrator. This issue is independent of installing the ADC, and becomes a factor only because the ADC requires Forestprep and Domainprep.

ADC Setup Permissions

The account you use to install the first ADC must meet the following requirements:

- **Belong to the Enterprise Admins group.** This allows Setup to modify the Configuration naming context.
- **Belong to the Schema Admins group.** This allows Setup to modify the schema.
- **Belong to the Domain Admins group in the domain where the ADC resides.** This allows Setup to create the Exchange Services group in the domain and to write to the Registry of the server hosting the ADC service.

Installing subsequent ADCs requires Domain Admin rights only in the domain that hosts the server.

Because ADC Setup performs all the necessary schema modifications for Exchange 2003, installing the first Exchange 2003 server after installing the ADC requires Domain Admin permissions only in the domain hosting the server along with Exchange Full Administrator permissions in the Exchange organization.

Subsequent Exchange 2003 server installations requires Exchange Full Administrator permissions only in the Administrative Group (legacy site) containing the server.

ADC Server Selection

The Exchange 2003 ADC service can run on Windows 2000 SP3+, Windows Server 2003 Standard, or Enterprise Edition as long as the server belongs to the same forest as the Exchange 2003 organization. The service communicates with Active Directory, but it does not need to run on a domain controller.

If you have a large organization with many Exchange sites, you should dedicate a server exclusively to running the ADC so that it can handle connections to the various sites without interruption. If you have a medium-sized organization with a few sites, you can run the ADC service on a domain controller or directly on the Exchange 2003 server.

If possible, install the ADC server in the forest root domain where administrators have full rights to the Configuration naming context and the schema.

If you cannot install the ADC server in the forest root domain, before you install the ADC, extend the schema in the forest root domain using **setup /schemaonly** while logged on as an Enterprise Admin and a member of Schema Admin group. This step is not included in the Exchange 2003 prescriptive checklist.

If you choose to deploy Exchange 2003 in the midst of a migration to Exchange 2000, either upgrade your existing Exchange 2000 ADC or install an Exchange 2003 ADC on a Windows Server 2003 server; then create new connection agreements and tear down the old ones.

ADC Service Account Selection

During ADC Setup, you must designate a service account for the ADC that it can use when connecting to a legacy Exchange server. The service account you designate during Setup becomes the Logon Account for the service, as shown in Figure 12.15.

You should not use the domain Administrator account for the ADC service account. It's too likely that you'll forget you did this and change the password. Also, most security experts agree that the domain Administrator account should be avoided as a service account to minimize the impact of a successful penetration. Instead, use the following criteria to select the service account:

- If the ADC server belongs to the same domain as the legacy Exchange servers (for example, after performing an in-place upgrade), then you can use the same service account as that used by the legacy Exchange servers. (And if that's the domain Administrator account, well, shame on you.)

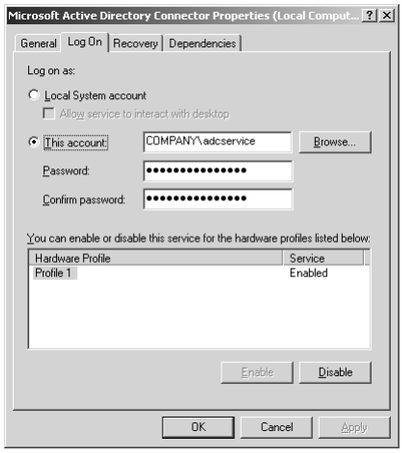

Figure 12.15 ADC requires a service account with access to legacy Exchange directory service.

- If the ADC resides in a different domain than the legacy Exchange servers, create a new account in Active Directory and grant this account Service Account Admin permissions on the Organization, Site, and Configuration containers in each legacy Exchange site.

On the Active Directory side, ADC Setup creates a group called Exchange Services with Full Control access rights to the Exchange organization. It makes the ADC service account a member of this group.

Domain Prerequisites

Windows 2000 introduced the concept of a "mode change" to differentiate between a domain that can support NT BDCs (Mixed mode) and one that has full functionality (Native mode). Windows Server 2003 extends the mode concept to include backward compatibility with Windows 2000 but the term is now "functionality level." The highest functional level is *Windows Server 2003*. This functional level enables certain critical features helpful for Exchange 2003 operation, such as replicating individual members of groups and reducing the replication interval within a site from five minutes to five seconds.

Exchange 2003 does not require a functional level of Windows Server 2003, but it does require at least one domain to be set at the functional level of Windows 2000 Compatible. This enables Universal Security Groups.

If you are consolidating multiple NT4 domains into a single Active Directory domain, you must have a trust between each NT4 domain, the Active Directory forest root domain, and each domain hosting users with mailboxes on NT4 Exchange servers.

You'll also need to perform a few operations in each domain that hosts mail-enabled objects:

- **Name Resolution.** Verify proper DNS name resolution at each server you intend to use for ADC and Exchange 2003. It's important that the servers find domain controller and Global Catalog servers. You should also verify proper WINS registration for Exchange server candidates. Legacy Exchange servers and downlevel Exchange clients use WINS to locate Exchange services. WINS has a couple of other minor functions, as well. See **hellomate.typepad.com/exchange/2004/03/exchange_200x_r.html** for details.
- **ADC Staging OU.** You'll need an OU to act as a repository for groups and contacts created by the ADC when it replicates distribution lists and custom recipients along with disabled user accounts representing resource mailboxes. In the examples, I'll call this OU the ADC_Staging_Area.
- **Verify Trusts.** The trust relationships between the Active Directory domains and any downlevel domains must be intact. Use Nltest from the Windows Server 2003 Support Tools to verify the trust.
- **Global Catalog locations.** You should have at least one Global Catalog server in each site that has an Exchange 2003 server. Microsoft recommends a 4-to-1 ratio for the number of processors in your Exchange servers to the number of Global Catalog servers. For example, if you have two 4-way Exchange servers in the same site, you should have two Global Catalog servers. If you have a single domain, enable the Global Catalog on all domain controllers. This does not increase the size of the Active Directory file. It merely ensures that the server listens on TCP port 3268 for LDAP queries directed at the Global Catalog.

- **Active Directory Replication topology.** Identify each Active Directory bridgehead server and map out the inter-site replication links. This helps you diagnose replication problems that might occur when you upgrade the Schema. Also, Exchange 2003 depends on Active Directory replication to inform other Exchange servers about configuration changes, so you want to document your configuration and get proactive about monitoring for critical events.
- **Remove Internet Explorer Enhanced Security.** ADC Setup (and Exchange 2003 Setup) make extensive use of Internet files (.html, .hta, and so forth). This can cause you a bit of irritation because Windows Server 2003 has a feature called Internet Explorer Enhanced Security that forces to you accept the location for each of the screens launched by the wizard. Do yourself a favor and remove this feature from the server, at least for the duration of the ADC and Exchange setup.

You can run Exchange Setup without going through the prescriptive checklist and the deployment tools. Run Setup from the \Setup\I386 folder on the CD.

To remove the Internet Explorer Enhance Security feature:

1. Launch **Control Panel**.
2. Open the **Add/Remove Programs** applet.
3. Click **Add/Remove Windows Components**.
4. Uncheck the **Internet Explorer Enhanced Security Configuration** option, shown in Figure 12.16.
5. Click **Next** to accept the change.

When you've finished installing the ADC and/or Exchange on the server, feel free to install the Internet Explorer Enhanced Security Configuration service again. It does not interfere with Exchange operations, and it prevents other administrators from using your Exchange server to browse the Internet and possibly download something that performs an unfortunate activity on your server.

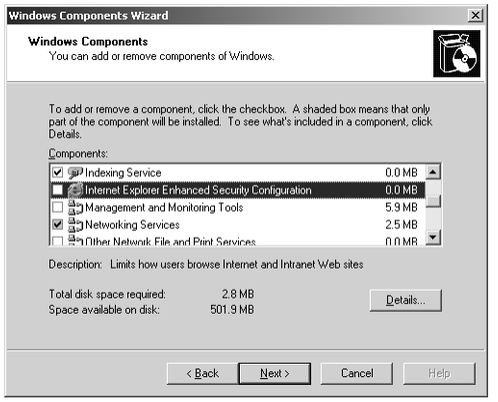

Figure 12.16 Simplify ADC and Exchange Setup by removing Internet Explorer Enhanced Security Configuration for the duration of the Internet Explorer Enhanced Security Configuration service installation.

ADC Installation

I recommend installing the ADC using the prescriptive checklist in Exchange Server 2003 Setup rather than using the ADC Setup directly. Following the prescriptive checklist ensures that you run all the preliminary tests to validate your configuration and the operation of your infrastructure. You can also take full advantage of the ADC Tools and the Connection Agreement Wizard.

The checklist appears as part of the standard Exchange and ADC Setup. Figure 12.17 shows an example of the checklist.

You'll need to install the Windows Server 2003 Support Tools prior to starting the ADC installation so that you have the Dcdiag and Netdiag utilities available. These are required components of the prescriptive checklist.

You can do the installation in an admin-mode remote desktop session, if that's your normal way of managing your servers. In Windows Server 2003, you might want to connect directly to the console by running mstsc /console. This puts a warning message on the regular console display to warn your colleagues if they select the server with a KVM switch.

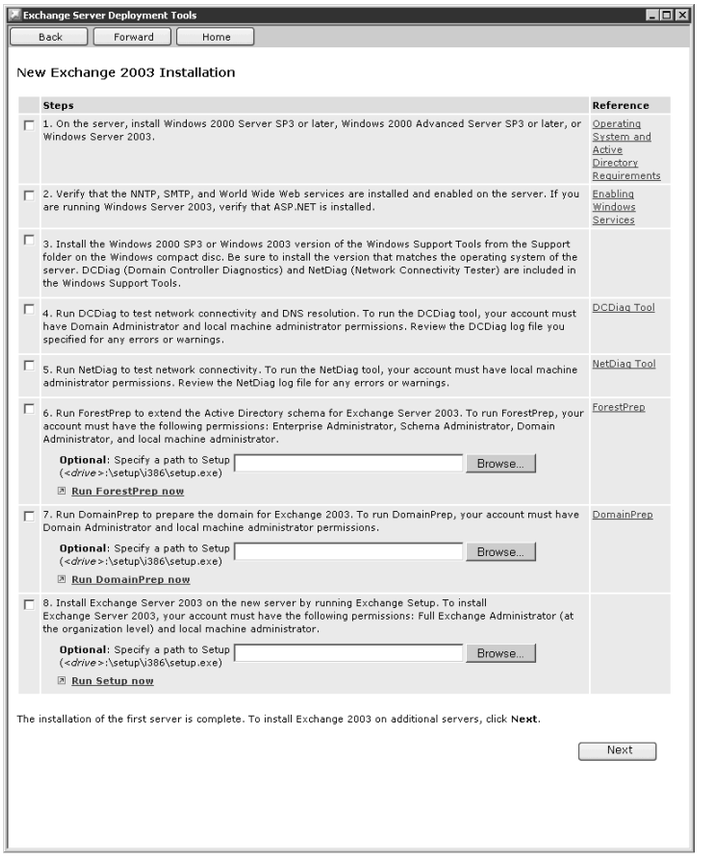

Figure 12.17 Component Selection window showing ForestPrep selected under Action if all prerequisites are met.

The prescriptive checklist prompts you to run Forestprep to modify the Active Directory schema. If you do not use the checklist, the ADC Setup Wizard updates the schema using its own files. The end result is the same. Unlike Exchange 2000, the ADC in Exchange Server 2003 performs the same schema modifications as the Exchange server setup.

This section does not contain a step-by-step procedure for installing the ADC. That's provided by the prescriptive checklist. It gives you an overview the of the more important elements of the checklist along with pointers about the information you'll need to enter, and it shows you what a clean set of deployment log entries would look like.

1. To start the ADC installation, insert the Exchange Server 2003 CD and launch Setup from the root of the CD.
2. At the main welcome screen, under the **Deployment** column, select **Exchange Deployment Tools**. The Welcome to the Exchange Server Deployment Tools window opens.
3. Click **Deploy**, the first Exchange 2003 Server option. The Deploy the First Exchange 2003 Server window opens.
4. Select the **Coexistence with Exchange 5.5** option. This opens the prescriptive checklist. Follow the numbered items in the checklist. Make sure you specify the log file location on a handy local folder so you can review the logs frequently during the process.

Initial Testing

The first major item on the prescriptive checklist runs a comprehensive suite of tests called DSScopeScan. This suite includes the following tests (detailed a little later in this section):

- **DSConfigSum.** This test reports the total number of sites and the number of servers in each site.
- **DSObjectSum.** This utility reports the total number of public folders, distribution lists, distribution lists with hidden membership, and custom recipients.
- **UserCount.** This test reports the total number of recipients (users) in the organization, broken down by site.
- **VerCheck.** This test verifies that you have the right Exchange version and service pack level on your Exchange servers.

You must specify the name of an Exchange 5.5 SP3 (or higher) server, an Active Directory domain controller, and a location for the deployment log files. If you enter an incorrect path for the log files, each element of DSScopeScan errors out and you'll see that the log folder holds no files. If this happens, simply correct the entry for the path and run the tool again.

The main log file for the deployment is Exdeploy.log. It shows the result of each test performed by DSScopeScan. (The other deployment tools have their own detailed logs with summaries appended to Exdeploy.log.) For example, if your logon account does not have sufficient

legacy Exchange permissions, you get an error message like this in the Exdeploy.log file:

```
Warning: Either you do not have permission to view
➥hidden objects in the Exchange 5.5 directory, or the
➥directory is not Exchange 5.5 SP1 or later. Returned
➥information may be inaccurate.
```

A file called Exdeploy-Progress.log gives a blow-by-blow account of the installation, useful only if something entirely unexpected and strange goes wrong. Be sure to resolve all error messages prior to continuing. New messages append to the end of each log, so you won't lose any diagnostic information by running DSScopeScan over and over. See Appendix C, "Detailed Deployment Log Contents," for details on the expected content of the individual logs.

After you have resolved any errors that came up in DSScopeScan, go to the next page of the prescriptive checklist.

ForestPrep

The next major step in the prescriptive checklist runs Forestprep. This modifies the Active Directory schema to include new attributes and classes used by Exchange and also installs the top-level objects for a placeholder organization tree in the Configuration naming context in the Active Directory forest.

Clicking ForestPrep in the prescriptive checklist launches Exchange Setup, which takes you through an End-User License Agreement (EULA) window to the Component Selection window shown in Figure 12.18.

If you properly completed all prerequisites, the Action column automatically fills in with the word Forestprep. If the Action column remains empty, you neglected to fulfill one of the prerequisites. To see what you missed, manually select Forestprep in the Action column. An error window will appear describing what you forgot to do.

During ForestPrep, you'll get prompted for the name of the Microsoft Exchange Server Administrator Account, as shown in Figure 12.19. This account gets Exchange Full Administrator privileges in the skeleton Organization container created by ForestPrep. Enter the domain name and the name of the account that you want to act as the initial Exchange administrator.

When ForestPrep completes, return to the prescriptive checklist.

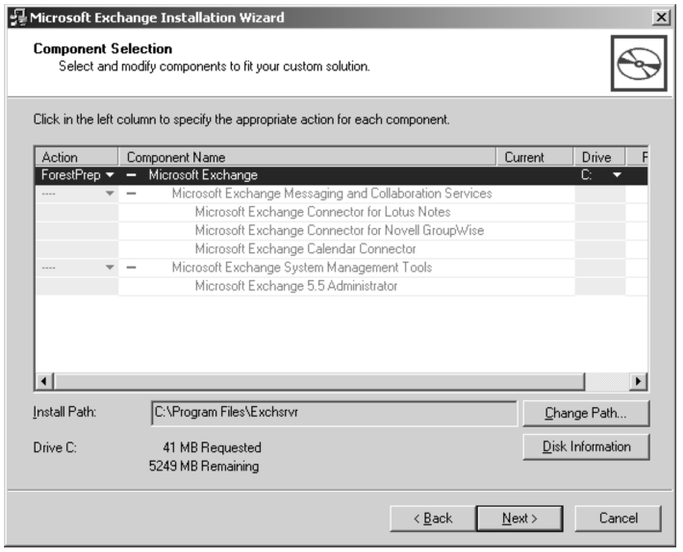

Figure 12.18 Component Selection window showing ForestPrep selected under Action, if all prerequisites are met.

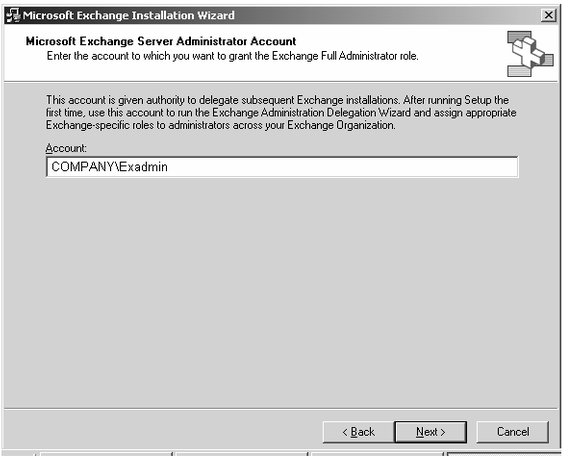

Figure 12.19 Exchange Server administrator account given Exchange Full Administrator role in organization.

DomainPrep

The next step in the prescriptive checklist runs DomainPrep. This creates objects in the Active Directory domain that represent Exchange service accounts, public folders, and groups that represent Exchange servers in the domain and the enterprise.

When you click on DomainPrep, Exchange Setup launches and takes you through a EULA window to the Component Selection window. This time the Action column is filled in with word DomainPrep.

If the Action column remains empty, you neglected to fulfill one of the prerequisites. To see what you missed, manually select DomainPrep, and an error window appears describing what you forgot to do.

During DomainPrep, a warning message appears informing you that the domain has been identified as insecure for mail-enabled groups. The default configuration of Active Directory in Windows Server 2003 places the Authenticated Users group in the Pre-Windows 2000 Compatible Access group. This group has Read permissions for group membership. This does not override the Deny Read permissions used to hide group membership, but Setup doesn't seem to know that. Click OK to acknowledge the message.

When DomainPrep finishes, return to the prescriptive checklist.

Verification Tests

At this point, let's take a breather and figure out where we stand. As part of the preparation steps to installing the ADC, you've updated the schema, made significant changes to the Global Catalog, and added quite a few objects to the Domain naming context. You want to make sure that all these changes fully propagate to all domain controllers and Global Catalog servers in the enterprise before you proceed. For this purpose, the next step of the prescriptive checklist presents a tool called OrgPrepCheck. This tool runs two tests, Orgcheck and Polcheck.

- **OrgCheck.** This test verifies that Setup created the proper Exchange objects in the Configuration naming context and Domain naming context. For example, it verifies that the Exchange Domain Servers group, Exchange Enterprise Servers group, and Exchange Services group exist. It also verifies that the schema changes have fully propagated and that it can find a Global Catalog server in the same site as the ADC server.

- **PolCheck.** This test queries each domain controller in the domain to determine if the Exchange Enterprise Servers group has been given the Manage Auditing and Security Logs privilege. If this has not yet occurred, then the Domainprep changes have not yet replicated to that domain controller, or an error prevented the changes from applying. You can use Active Directory Sites and Services to force replication to the affected domain then run OrgPrepCheck again.

A successful run of these two tests indicate that the schema changes have fully replicated and that every domain has been properly updated to include the necessary Exchange objects. You're ready to proceed to the next step in the prescriptive checklist.

ADC Setup

You're now ready for the meat and potatoes part of the ADC installation. Click the Run ADC Setup Now option in the prescriptive checklist to launch ADC Setup. (You can run Forestprep and Domainprep on a different server than where you install the ADC.)

1. At the welcome window, click **Next**. A EULA window opens.
2. Click **Next**. The Component Selection window opens, as shown in Figure 12.20. Select both options to install the ADC and the ADC Management components.

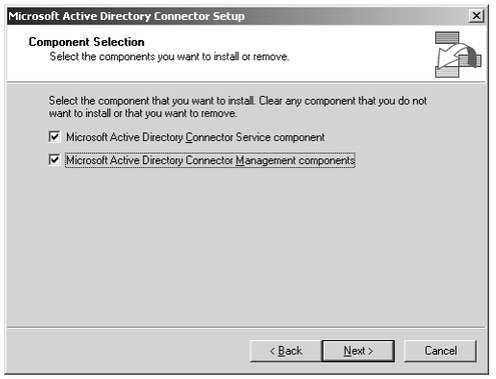

Figure 12.20 Component Selection window permits installing the ADC and the ADC Tools, or just the tools.

3. Click **Next**. The Install Location window opens. Enter a path for the ADC executable files. The ADC does not use a database, but it does store error logs in this location.
4. Click **Next**. Setup installs the ADC and keeps you notified via a status window. At the completion of ADC Setup, return to the prescriptive checklist. This could take quite a while. Go grab a sandwich and come back in a half hour or so.

ADC Tools

The next step in the prescriptive checklist prompts you to open the ADC management console and select the ADC Tools option, as shown in Figure 12.21.

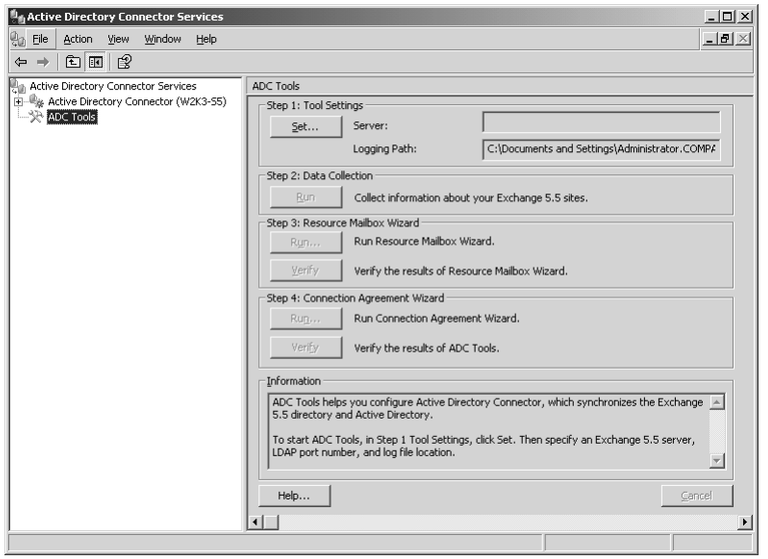

Figure 12.21 ADC Tools simplify the process of testing prerequisites and installing Connection Agreements.

The ADC Tools consists of a suite of utilities designed to report on inconsistencies in the legacy Exchange directory service, to automate the process of marking resource mailboxes with NTDSNoMatch, and to automate the process of creating Recipient and Public Folder Connection Agreements. The user interface divides these chores into four steps:

- **Step 1: Tool Settings.** In this step, you specify the name of the Exchange 5.5 server to use for data collection and a location for the ADC logs.
- **Step 2: Data Collection.** This step runs a suite of utilities that scans both Active Directory and the legacy Exchange directory service to find parameters that will be synchronized by the ADC.
- **Step 3: Resource Mailbox Wizard.** This step determines if the same user owns multiple mailboxes and gives you the opportunity to identify the user's primary mailbox so that the other mailboxes can be designated as resource mailboxes and given new, disabled accounts in Active Directory.
- **Step 4: Connection Agreement Wizard.** This step creates Connection Agreements that define the replication endpoints of the ADC and determine how attributes will be mapped between the endpoints.

The ADC reads and writes to the legacy Exchange directory service using LDAP. The server must be running Exchange 5.5 SP3 or higher so that it supports LDAP writes and LDAP queries that use paged results.

Step 1: Tool Settings

Click Set. The Tool Settings window opens. Here you specify the name of an Exchange 5.5 server to use for data collection. You do not necessarily need to select the server you will use for Connection Agreements, but you could. Select a location for the ADC logs. The default location puts the files in your user profile.

Step 2: Data Collection

Click Run to query the Exchange 5.5 server and collect information about the Exchange organization. ADC Tools performs a series of four tests that check for objects and attributes in legacy Exchange and Active Directory. These tests also build XML database files used by later steps for resource mailbox marking.

Resource Mailbox Scan

This test looks for mailboxes that have the same owner. If it finds them, it puts an entry in the ADCTools.log file similar to the following:

```
Pass 1 of 4: Resource Mailbox Scan 01/09/2004 13:37:35
Warning: The Data Collection tool found objects that must be marked as
➥resource mailboxes before they can be replicated to Active Directory.
➥Running the Resource Mailbox Wizard in Step 3 will resolve these issues.
```

Active Directory Connector Object Replication Check

This test verifies that each mailbox owner has a match to an Active Directory user object. If it finds unmatched objects, it identifies them in the ADCTools.log file. Here's a sample listing:

```
Pass 2 of 4: Active Directory Connector Object Replication Check
➥01/09/2004 13:37:48
Matched 'cn=PhoenixUser1,cn=Recipients,ou=Phoenix,o=Company' to
'cn=Phoenix User1,ou=Phoenix,dc=Company,dc=com' based on SID.
Could not find match to 'cn=PhoenixUser2,cn=Recipients,ou=Phoenix,
➥o=Company'.
Could not find match to 'cn=phoenixuser3,cn=Recipients,ou=Phoenix,
➥o=Company'.

Warning: The Data Collection tool found objects that are not replicated
➥from the Exchange 5.5 directory to Active Directory. Running the
➥Connection Agreement Wizard in Step 4 will resolve these issues.
```

The log might reassure you that the Connection Agreement Wizard will resolve replication issues for the matched entries, but you should not proceed until you resolve any unmatched entries. You do not want the ADC to create disabled user accounts in Active Directory for any mailboxes other than resource mailboxes. The presence of other unmatched objects indicates a possible error in the user account migration, if you migrated from a separate NT domain, or user accounts that someone deleted without deleting the mailboxes.

Active Directory Object Replication Scan

This test looks for mail-enabled objects in Active Directory that do not have corresponding recipient objects in legacy Exchange. You have not yet run a Connection Agreement, so this test does not find any invalid entries. Here's a sample listing:

```
Pass 3 of 4: Active Directory Object Replication Scan 06/09/2003 13:38:17
No mail enabled objects found in Active Directory.
Active Directory Object Replication Scan completed.  No unreplicated
➥objects found.
```

If you run this test once you've deployed Exchange 2003 servers, you might get an error such as this:

```
Warning: The Data Collection tool found mail-enabled users,
➥contacts, or groups that are not replicated from Active
➥Directory to the Exchange 5.5 directory. Running the
➥Connection Agreement wizard in Step 4 will resolve these
➥issues.
```

This error indicates that you created a mail-enabled object in Active Directory, but the ADC has not yet replicated that object to the legacy Exchange directory service. Resolve this by determining why the CA has not replicated the object. The most likely cause involves a failure of the CA to locate the two endpoint servers.

Active Directory Unmarked Resource Mailbox Scan

This test checks for potential resource mailboxes that do not have an NTDSNoMatch entry. Since you have not yet run the ADC or deployed Exchange 2003 servers, this check comes up clean. If you run the test after you have been operating awhile, you might get an error about mismatched accounts. This indicates that the ADC cannot match a potential resource mailbox to a disabled user account. The most likely cause involves a failure to properly mark the primary and resource mailboxes assigned to the same owner in legacy Exchange. Correct the problem and repeat the test.

Step 3: Resource Mailbox wizard

The next step in the ADC Tools identifies and marks resource mailboxes using the Resource Mailbox Wizard. Larger enterprises might have hundreds of these resource mailboxes. You can use the bulk edit capabilities to create .csv files for doing the mailbox marking.

1. Click **Run** to start the Resource Mailbox Wizard. The Welcome window opens.
2. Click **Next**. The Select Primary and Resource Mailboxes window opens, shown in Figure 12.22. This window lists owners of multiple mailboxes along with the mailboxes they own. The wizard makes a guess about the primary mailbox based on the user's account name and mailbox alias. It indicates the primary mailbox in bold.

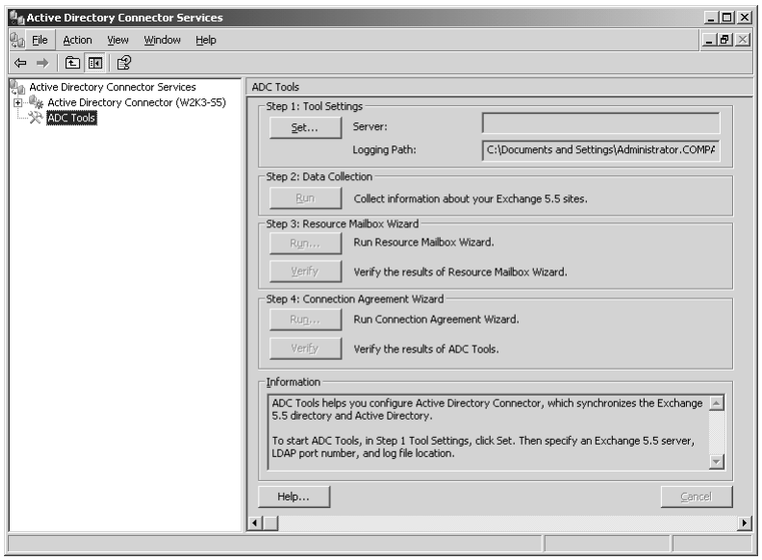

Figure 12.22 Resource Mailbox Wizard searches out mailboxes with the same owner and allows you to specify which mailbox is the user's primary mailbox and designates the remainder as resource mailboxes.

3. If the wizard guesses wrong about the primary mailbox, highlight the true primary mailbox and click **Set as Primary**. The other mailboxes automatically shift to resource mailboxes.
4. Click **Next**. The Site Credentials window opens, as shown in Figure 12.23.

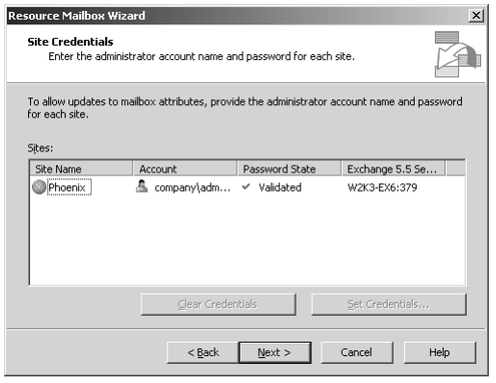

Figure 12.23 Site Credentials window validates the account you select to install the ADC.

5. Click **Set Credentials** and browse for an account that has administrative permissions in the legacy Exchange organization. Use the Exchange service account, because you know it has Service Account Admin permissions. If the Password State column indicates Validated, you know you entered the correct password, but that does not guarantee that the account has sufficient admin permissions.
6. Click **Next**. A Summary window opens. Verify that all settings are correct.
7. Click **Next**. This applies the changes.
8. Click **Finish** to return to the ADC Tools window.
9. In the ADC Tools window, click **Verify** to test that each resource mailbox has been marked with NTDSNoMatch.

Step 4: Connection Agreement wizard

You've arrived at the point where you'll create Connection Agreements that replicate the e-mail attributes to the Active Directory objects. The Connection Agreement Wizard asks you a few questions then sets up sufficient Recipient and Public Folder CAs to connect each site to Active Directory.

1. Click **Run** to start the CA Wizard.
2. At the main welcome window, click **Next** to open the Staging Area window, shown in Figure 12.24.

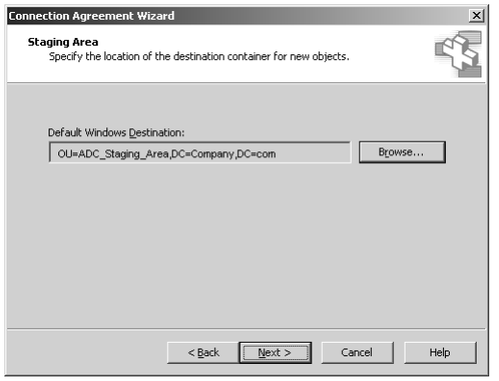

Figure 12.24 Staging Area allows you to enter the OU in Active Directory where Distribution Groups, Contacts, and disabled User accounts will be created.

3. Browse to the **ADC_Staging_Area** OU (or whatever OU you created to act as the repository for group and contact objects replicated from legacy Exchange).
4. Click **Next**. The Site Connections window opens (Figure 12.25). The **Two-Way Connections** pane of the window should list every legacy site. If you don't see a site, stop and determine the problem. Replication failure at the legacy Exchange server used by the ADC can cause this problem.

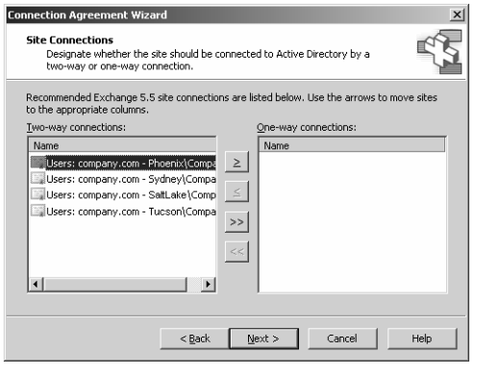

Figure 12.25 Site Connections shows the Connection Agreements suggested by the Connection Agreement Wizard.

5. Click **Next**. The Site Credentials window opens, shown in Figure 12.26. Use the **Set Credentials** button to enter the name and password for an account with Service Account Admin permissions in each site. In the example, each site uses the **company\exservice** account.
6. Click **Next**. The Domain Credentials window opens. Enter a set of administrator credentials for each domain in the Active Directory forest.
7. Click **Next**. The Connection Agreement Selection window opens, shown in Figure 12.27. Leave all the entries checked.
8. Click **Next** to get a summary window.
9. Click **Next** again to build the Connection Agreements.
10. When the CA Wizard has completed its tasks, check the final window for reported errors.
11. Click **Finish** to return to the ADC Tools interface.

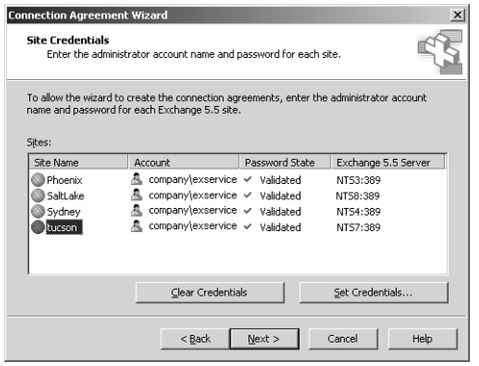

Figure 12.26 Site Credentials window validates the account you provide to install the Connection Agreements.

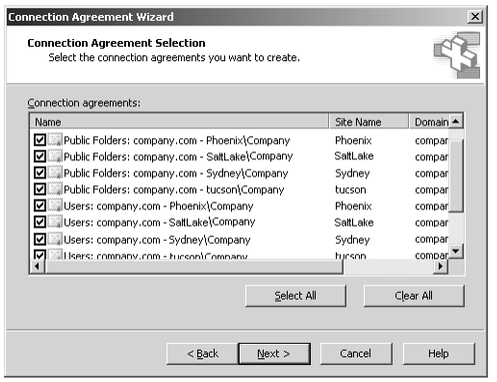

Figure 12.27 Connection Agreement Selection window allows you to not install one or more Connection Agreements suggested by the wizard.

12. Click **Verify** to initialize the Connection Agreements. This verifies that all necessary updates were applied to both directory services.
13. In the ADC Services console, select the Active Directory Connector icon and press F5 to refresh the display. The listing now includes the Connection Agreements created by the wizard, as shown in Figure 12.28.

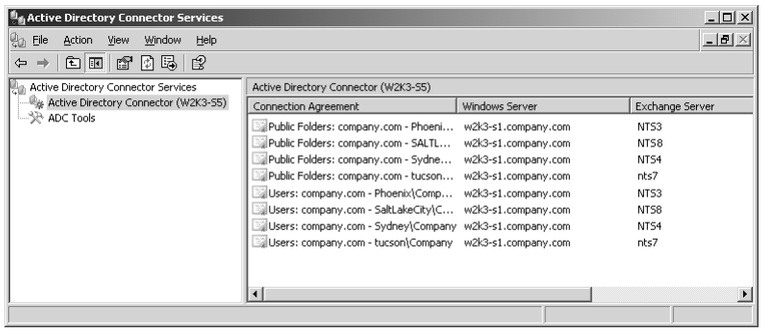

Figure 12.28 ADC Services console showing Connection Agreements created by the wizard and their endpoint servers.

Final Checks

At this point, now that you've completed installing the ADC, you should check a few Active Directory users to make sure the Exchange attributes appear in their properties using the Active Directory Users and Computers console. Also, check the staging area to make sure you have objects representing the legacy distribution lists and custom recipients. Figure 12.29 shows an example.

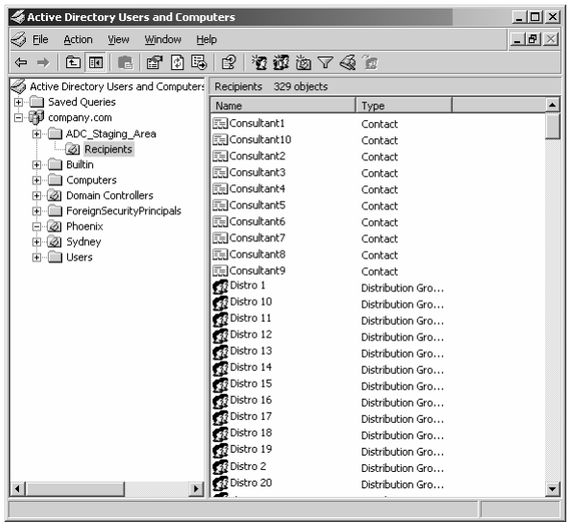

Figure 12.29 Active Directory Users and Computers showing the Universal Distribution Groups and Contacts created by the ADC.

Once you get an Exchange 2003 server up and running, you can familiarize yourself with the operation of a Connection Agreement by creating mailbox-enabled users, mail-enabled groups, and contacts; then using the ADC to replicate them to the legacy Exchange directory service.

At this point, you've finished the ADC installation and you're ready to proceed with installing the first Exchange 2003 server. Ordinarily, at a major milestone such as this, you would want to do some verification testing. But you can't do a thorough test of the ADC until you have all the Connection Agreements, and this won't happen until you install the first Exchange 2003 server. For that reason, you'll find a section on verifying CA operation in the next section.

Connection Agreement Properties

Although the Connection Agreement Wizard does a lot to simplify the creation of CAs, you'll find it useful to get familiar with the properties of the various types of CAs. You might need to modify the settings of a CA created by the CA Wizard. Or you might need to create a custom CA without the help of the wizard. You might also need to troubleshoot the operation of a CA, and that can get very tedious if you don't know how they operate with various settings.

Recipient Connection Agreements

Open the Properties window for one of the User CAs created by the wizard. Figure 12.30 shows the General tab.

The wizard creates two-way connection agreements, meaning that changes made to either directory service replicate to the other service. This ensures that you have full synchronization throughout the migration.

These settings are stored in Active Directory, so if you want another ADC server to take over the replication duties, you can select a different server using the **Select a Server to Run** option.

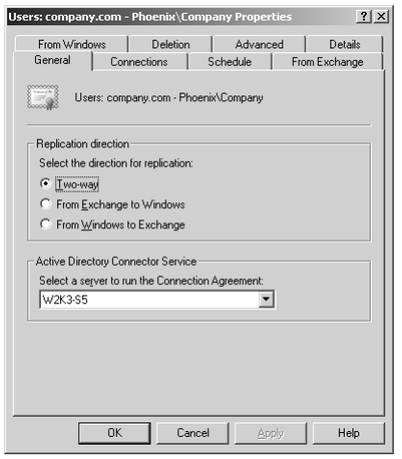

Figure 12.30 Connection Agreement properties showing the agreement type and the name of the ADC server.

Connection Settings

Select the Connections tab, shown in Figure 12.31. This tab allows you to select the endpoint server for each side of the Connection Agreement and the credentials used to access the directory service on that server.

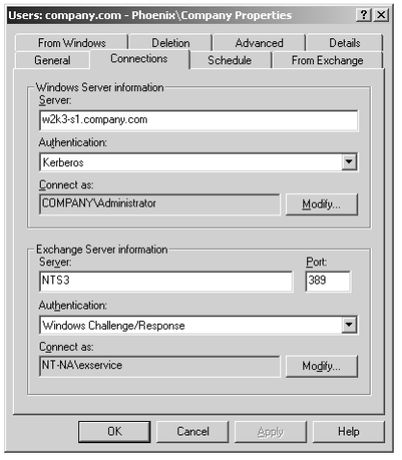

Figure 12.31 Connections tab showing the two-endpoint servers in the Connection Agreement and the credentials used to make the connection.

If you decommission the legacy Exchange server acting as the endpoint to the Connection Agreement, use this tab to specify another legacy server. As you'll see in the next section, Exchange 2003 has a service called the Site Replication Service that maintains a replica of the legacy Exchange directory service on an Exchange 2003 server. You can point a CA at this SRS service rather than at a legacy Exchange server. The only caveat is that SRS listens at TCP port 379 rather than TCP port 389, the standard LDAP port.

If you change the password on either of the accounts used to access Active Directory or legacy Exchange, use this tab to change the passwords stored in the Connection Agreement. Failure to do so will be reported to the Application event log.

Schedule Settings

Select the Schedule tab, shown in Figure 12.32. The default setting for CA replication is **Always**. This replicates a change as it occurs.

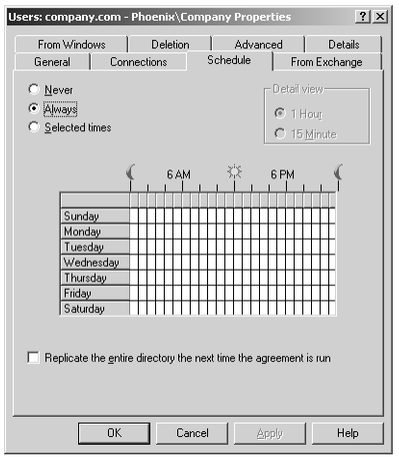

Figure 12.32 Schedule tab permits throttling back on replication to accommodate network restrictions, if any.

If immediate replication overloads a slow connection, you can elect to replicate periodically, such as hourly or every 15 minutes throughout a given window. Under general circumstances, you won't change the default setting.

"From Exchange" Settings

Select the From Exchange tab, shown in Figure 12.33. Note that the CA replicates all changes from a given legacy site into the staging area OU you created in Active Directory. You should only see Universal Distribution Groups, contacts, and disabled user accounts for resource mailboxes in this OU. The ADC locates a user object in the OU where it resides.

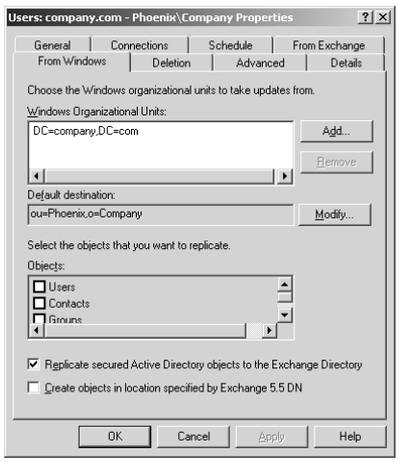

Figure 12.33 From Exchange shows the source, target containers, and the object types that will be copied from legacy Exchange to Active Directory.

"From Windows" Settings

Select the From Windows tab, shown in Figure 12.34. This side of the CA works a little differently. The CA takes changes made to mail-enabled objects anywhere in the domain and replicates them to objects in the legacy site container.

If you think about it for a moment, this configuration might cause a problem. After all, the CA wizard creates several CAs, one for each legacy site. Each of these CAs pulls changes from the entire domain. This could lead to a situation where you mail-enabled an object in Active Directory, and the overlapping CAs each created a corresponding object in its own legacy site OU.

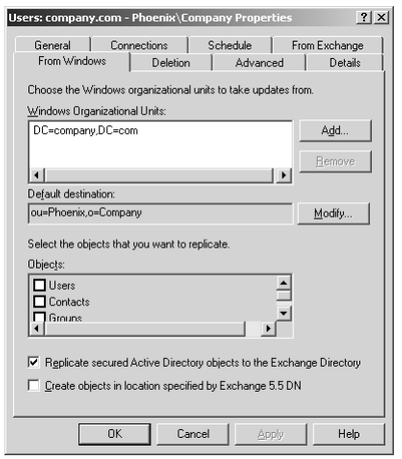

Figure 12.34 From Windows specifies the source and target containers for the Connection Agreement, but does not indicate the type of objects. This is determined by a custom filter that cannot be seen in the user interface.

To avoid this, Microsoft does a little magic trick. In the From Windows tab, take a look at the Objects field. The ADC uses this field to configure a filter in the Connection Agreement to search only for objects of the specified class. If you were to configure a CA manually and check each of the object types, the ADC would create a filter to search for all objects of the User, Group, and Contact class.

Notice in the Connection Agreement created by the CA Wizard that the Objects field contains a gray background, and none of the checkboxes have checks. Instead of using a standard filter, the CA Wizard inserts a custom filter into the CA that limits the search to objects in the same site as the Exchange server that forms the endpoint of the Connection Agreement. This search restriction prevents overlapping CAs from creating multiple objects in their own site OU based on a single mail-enabled Active Directory object.

Just in case you're interested in the full details, here's how the custom filter created by the CA Wizard works. It's good to know this information if you ever want to create a CA without the aid of the CA Wizard.

continues

Each mail-enabled object in Active Directory has an attribute called LegacyExchangeDN. As you might expect, this attribute corresponds to the Distinguished Name of the object in the legacy Exchange directory service.

The syntax of the LegacyExchangeDN attribute uses X.821 format rather than X.500 format, so an example would look like this: `/o=Company/ou=Phoenix/cn=phoenixuser100`.

When a user gets a mailbox, the Exchange Task Wizard determines the site of the user's home server and constructs a LegacyExchangeDN entry that corresponds to that site. For example, if you were to take a user with the logon name sydneyuser50 and give that user a mailbox on an Exchange server in Sydney, the LegacyExchangeDN attribute would look like this: `/o=Company/ou=Sydney/cn=sydneyuser50`.

When the CA Wizard creates a Connection Agreement, the wizard modifies the Active Directory search filter in the CA to look only for objects with a legacyExchangeDN that specifies the same site as the Exchange server acting as the endpoint of the CA. For example, if the Exchange server resides in the Phoenix site, then the CA search filter would look for LegacyExchangeDN entries equal to `/o=Company/ou=Phoenix/cn=*`.

Advanced Settings

Select the Advanced tab, shown in Figure 12.35. The wizard configured the CA as a Primary CA for the Windows domain but not for the Exchange organization. Only a Primary CA can create new objects or delete existing objects. By preventing the CA from creating new objects in the legacy Exchange directory service, you avoid potential update loops in which changes to the same object would replicate back and forth between multiple sites.

The Advanced properties also tell the CA to create a disabled user account in Active Directory if it cannot match a mailbox owner to an Active Directory user. The other options include creating a *new* user object or a new *contact* object. These options have only limited utility, and you should not select them unless instructed by Microsoft Product Support Services in the event that you require their help to resolve a problem.

The Paged Results entry defines how many items the ADC will obtain in a single LDAP query. In Exchange 2003, Microsoft recommends leaving this setting at the default of 20 unless specifically instructed to use a higher number by a support technician or Microsoft consulting engineer. (The Exchange 2000 ADC Deployment Guide recommends raising this value to 99, but that does not apply to Exchange 2003.)

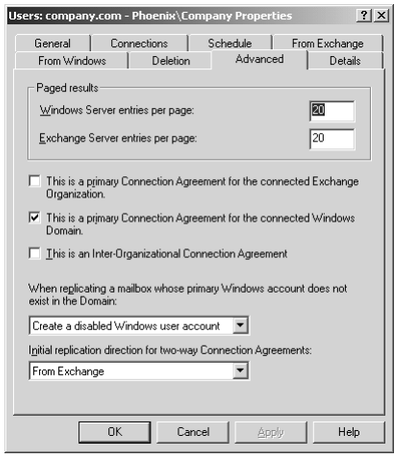

Figure 12.35 Advanced tab shows that each CA is a Primary only on the Windows side and that an unmatched mailbox in legacy Exchange will create a disabled user account.

Deletion Settings

Select the Deletion tab, shown in Figure 12.36. The default configuration deletes objects in one directory service when the corresponding object gets deleted from the other directory service.

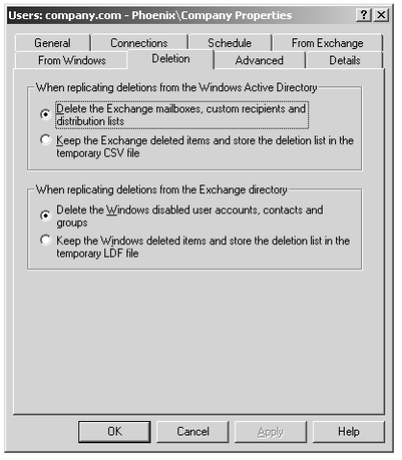

Figure 12.36 Deletion tab shows that deleted objects in each directory service will cause action on the part of the other directory service, by default. The alternative is to save the action in a flat file for later application.

Replicating object deletions between the two directory services can get a little complex, depending upon the object type and directory service from where you delete it.

Object Deletions Originating in Active Directory

If you delete a mailbox-enabled user, a mail-enabled group, or a contact in Active Directory, the object doesn't actually get deleted. Instead, the system strips off all but the most essential attributes, moves the object to a hidden container called Deleted Objects, and sets an attribute on the object called IsDeleted to TRUE.

The search criteria on the Connection Agreements created by the CA Wizard include a filter to look for objects with the IsDeleted attribute set to TRUE. When the ADC finds such an object, it instructs the legacy Exchange directory service to delete the corresponding object.

Mail Attribute Deletions Originating in Active Directory

If you use the Exchange Task Wizard in Active Directory Users and Computers to revert a mailbox-enabled user, a mail-enabled group, or a contact back to a standard object (the task name is **Remove Exchange Attributes**), the wizard strips most of the e-mail attributes from the object and then sets the value for the LegacyExchangeDN attribute to ADCDisabledMail.

The search criteria on the Connection Agreements created by the CA Wizard include a filter to look for objects that have the LegacyExchangeDN attribute set to ADCDisabledMail. When the ADC finds such an object, it instructs the legacy Exchange directory service to delete the corresponding object.

Object Deletions Originating in Legacy Exchange

On the legacy Exchange side, the action varies depending on whether the mailbox belongs to a real user or a disabled user linked to a resource mailbox.

- If you delete a resource mailbox, the ADC deletes the corresponding disabled user object in Active Directory.
- If you delete a standard mailbox, the ADC strips the e-mail attributes from the corresponding Active Directory object and sets the LegacyExchangeDN attribute to ADCDisabledMailByADC.

The search criteria on Connection Agreements created by the CA Wizard include a filter to look for objects that have the LegacyExchangeDN attribute set to ADCDisabledMailByADC. When the ADC finds such an object, it turns right around and attempts to delete the corresponding object from legacy Exchange, even though the object is already gone. This might seem redundant, but that's what happens.

Points to Remember about Object Deletions and the ADC

Here's a quick synopsis of the way the ADC handles object and attribute deletions:

- If you delete a mailbox-enabled user in Active Directory, the ADC deletes the corresponding mailbox in legacy Exchange.
- If you delete a mail-enabled group or contact in Active Directory, the ADC deletes the corresponding distribution list or custom recipient in legacy Exchange.
- If you remove the e-mail attributes from users, groups, or contacts in Active Directory, the ADC deletes the corresponding mailbox, distribution list, or custom recipient in legacy Exchange.
- If you delete a mailbox in legacy Exchange, the ADC strips the e-mail attributes from the corresponding user object in Active Directory.
- If you delete a distribution list or custom recipient in legacy Exchange, the ADC strips the e-mail attributes from the corresponding group or contact in Active Directory.

Configuration Connection Agreements

Consider the legacy Exchange directory service replication topology diagrammed in Figure 12.37. Within each site, the Exchange servers send directory service updates directly to each other using Remote Procedure Calls (RPCs). Between sites, the bridgehead servers convert the directory service updates into messages that they send to other bridgeheads.
When you start the migration to Exchange 2003, you introduce a new actor: the ADC server. You've already seen how the Connection Agreements created by the ADC keep recipients and public folders in sync between legacy Exchange and Active Directory. But that's not the whole story.

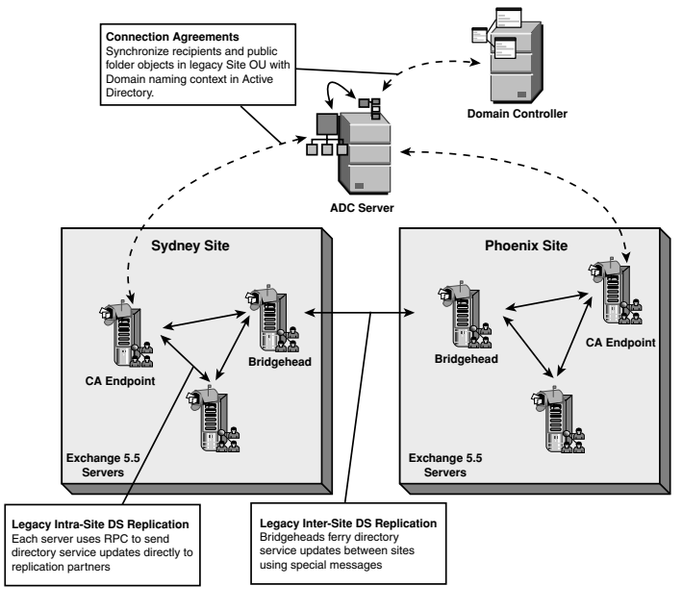

Figure 12.37 Configuration Connection Agreement connects the legacy Configuration containers in each site with the Exchange Organization container in Active Directory.

Exchange 5.x stores server information in a Configuration container in the legacy Exchange directory service. Each Exchange server in a site knows about the other servers in the site by looking in this Configuration container. The legacy servers in a site won't know that you installed an Exchange 2003 server until they see the server's information in the legacy Configuration container. That's the job of the Configuration Connection Agreement, which is created automatically when you install the first Exchange 2003 server in the site.

Configuration CA Function

When you install an Exchange 2003 server, Setup creates objects under the Exchange organization container in Active Directory that represent the following functions:

- Exchange server itself, including its operational settings
- Site addressing
- Connectors
- MTA and transport protocols

- Private and public mailbox storage parameters
- Recipient Policies
- Site (Administrative Group) configuration parameters
- Encryption and secure messaging parameters

The ADC synchronizes these objects with the legacy Exchange Configuration container using a Configuration Connection Agreement. The Configuration CA also connects the legacy Configuration container to the Recipient Policies container in Active Directory so that the ADC can update addressing policies. This is how Exchange 2003 finds out about the SMTP, X.400, and other proxy addresses currently used by legacy Exchange.

Configuration CA Endpoints

During your migration from legacy Exchange to Exchange 2003, you'll be decommissioning legacy servers. At some point, a given site might not have any remaining legacy servers, but the Exchange 5.x servers in other sites must still replicate the legacy Configuration partition so they can calculate message routing.

You could leave a legacy server in each site until you're just about ready to finish your migration, but to help smooth the transition, an Exchange 2003 server pretends to be a legacy Exchange server so it can replicate the Configuration container to the other legacy servers. That's the job of the SRS. An upcoming section in this chapter titled "Site Replication Service Configuration" details the operation of the SRS.

Public Folder Connection Agreements

Legacy Exchange public folders also act like standard recipients in that they can receive mail and belong to distribution lists. Active Directory represents mail-enabled public folders with a special object called Public Folder.

A Public Folder Connection Agreement in the ADC populates Active Directory with one Public Folder object for each public folder in the Public Folder Hierarchy. If you have 10,000 public folders in legacy Exchange, you'll end up with 10,000 Public Folder objects in Active Directory.

Public Folder CAs created by the Connection Agreement Wizard resemble Recipient CAs. Here are the differences:

- Both CA types define a two-way connection agreement with an Exchange server as the endpoint on one side of the CA and Active Directory on the other side.
- Both CA types limit the CA so that only the Windows side acts as a Primary CA.
- Both CA types have a default schedule of Always.

Their primary difference lies in the type of object included in the search criteria. A Public Folder CA searches only for objects of the Public Folder class in Active Directory and for public folders in legacy Exchange.

The target container in Active Directory is also different. A Public Folder CA points at the Microsoft Exchange System Objects container, as shown in Figure 12.38.

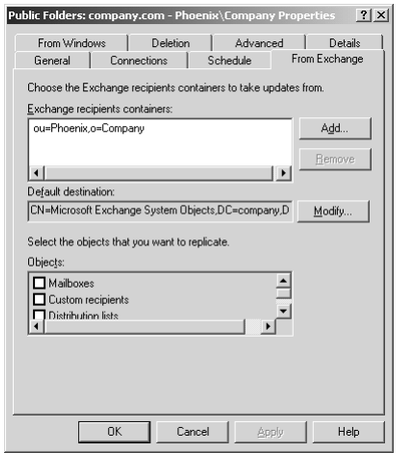

Figure 12.38 Public Folder Connection Agreement properties showing that the destination is the Microsoft Exchange System Objects container so that Public Folder objects can be created to correspond with mail-enabled MAPI public folders.

When the ADC runs the Public Folder CA for the first time, the Microsoft Exchange System Objects container fills with objects representing public folders. Figure 12.39 shows the Microsoft Exchange System Objects container after the initial replication. (Select View | Advanced view in the console to see the container.)

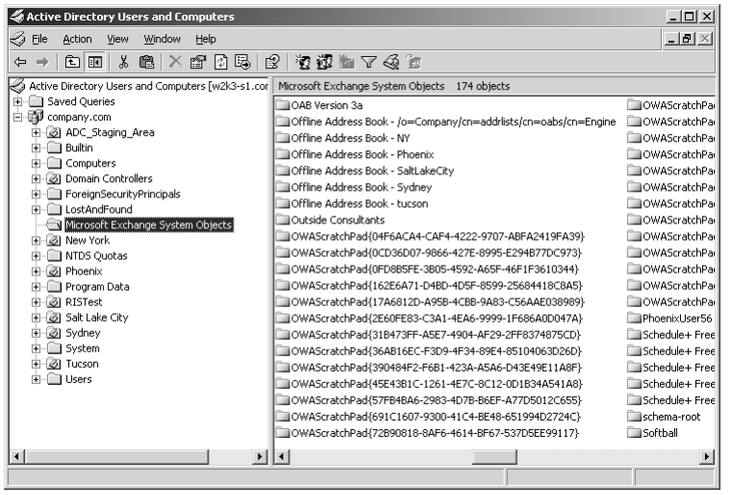

Figure 12.39 Active Directory Users and Computers console showing Public Folder objects created by Public Folder CA.

Initial Exchange 2003 Server Installation

You can't directly upgrade an existing Exchange 5.5 server to Exchange 2003. Once you've installed the ADC, select a site and install an Exchange 2003 server in that site. For best results, select the site that acts as the hub of your current organization.

The steps to install the first Exchange 2003 server in an existing legacy Exchange organization do not differ much from those that install an Exchange 2003 server in a pristine organization. Refer to Chapter 1, "Installing an Exchange 2003 Server," for the detailed installation steps.

The Exchange 2003 prescriptive checklist includes provisions for installing the first Exchange 2003 server in an existing legacy Exchange organization. Don't forget the prerequisite services on the server:

- NNTP (Nntpsvc)
- SMTP (Smtpsvc)
- WWW (W3svc)
- IIS Admin (Iisadmin)

Once you've installed the Exchange 2003 server, you should do some provisional testing to ensure that your migration infrastructure operates satisfactorily.

The primary differences in the installation of an Exchange 2003 server in a legacy organization occur in the background. Setup does the following:

- Replaces the placeholder name on the Organization object in Active Directory with the name of the legacy Exchange organization.
- Installs a Configuration Connection Agreement in the ADC that links the legacy Configuration container to the Organization container in Active Directory.
- Enables and starts the Site Replication Service (covered later in this chapter).

A short time after Setup completes, the Recipient Update Service places the newly installed Exchange server into the Exchange Domain Servers group.

Drum roll. Cymbals clash. You did it. You installed the first Exchange 2003 server in the legacy organization. You have a lot of work ahead of you, but for right now, you should test the system to make sure everything works right so far.

Connection Agreement Testing

Now that you have a live Exchange 2003 server, you can test the Connection Agreements created by the ADC. Here's a list of experiments you should perform to familiarize yourself with the ADC operation. For the sake of getting the most experience possible from the experiments, check the Application Log on the ADC server during each experiment to see the events that occur as objects replicate back and forth between legacy Exchange and Active Directory.

- **Create a new mailbox-enabled user** and verify that the ADC creates a mailbox in legacy Exchange with an owner whose name matches the new user. You might want to use the LDAP Browser (LDP) to see how the ADC-Global-Names attribute gets fleshed out as the attributes replicate back and forth between Active Directory and the legacy Exchange directory service.

- **Create a new mail-enabled group** and verify that the ADC creates a distribution list in legacy Exchange.
- **Add members to a mail-enabled group** in Active Directory and then see if they appear in the legacy distribution list.
- **Connect to a legacy mailbox with Outlook** to make sure you have access permission via SIDHistory (if applicable) and to make sure you can add members to distribution lists and send mail to the members. Verify that the members appear in the group in Active Directory.
- **Create a new mail-enabled contact** and verify that the ADC creates a custom recipient in legacy Exchange. Check the legacy attributes to verify that the e-mail address you gave the contact appears in the custom recipient.
- **Create a new mailbox in legacy Exchange** using Admin and give the mailbox an owner from Active Directory who does not already have a mailbox. Verify that the ADC populates the user account with e-mail attributes so that the account now shows as a mailbox-enabled user.
- **Delete a mailbox in legacy Exchange** and verify that the ADC removes the e-mail attributes from the corresponding user in Active Directory. Do this for a user with a mailbox on the legacy Exchange server and for a user with a mailbox on the Exchange 2003 server. Note that the Exchange 2003 mailbox does not actually get deleted when you delete the mailbox in legacy Exchange. Instead, run the Mailbox Cleanup Wizard to see that the mailbox gets a big red X and that you can link it to the same or another user. See Chapter 5, "Managing Recipients and Distribution Lists," for details.
- **Delete a distribution list and a contact in legacy Exchange** and verify that the ADC strips e-mail attributes from the corresponding objects in Active Directory. Note that the Active Directory objects themselves remain and that the membership of a group remains intact.
- **Place a Universal Distribution Group on a public folder permission list** and verify that it gets promoted to a Universal Security Group in a few minutes. The Exchange Information Store service performs this upgrade, so you might want to check the Event Log for MsExchangeIS events.

- **Create a new public folder** using Outlook or ESM, and verify that the ADC creates a corresponding Public Folder object in the Microsoft Exchange System Objects container in the domain.
- **Delete a public folder** and verify that the ADC removes the Public Folder object from the domain.
- **Replicate public folder content** by including the new Exchange server in the replication list for each public folder using the steps outlined in Chapter 10, "Managing Public Folders." You'll eventually decommission the legacy server so you want to move all public folders and system folders to Exchange 2003 servers.
- **Verify that Schedule + Free Busy replicates to the new server** by opening a new user and creating an appointment and then opening another user and verifying that the appointment appears in the availability columns.

The final set of ADC tests involve the Configuration Connection Agreement created when you installed the first Exchange 2003 server in the site.

- **Legacy Exchange.** Launch Admin at a legacy Exchange server in the same site as the new Exchange 2003 server and verify that the new server appears in the Configuration container.
- **Active Directory.** Launch ESM and drill down to the Administrative Group representing the legacy site and verify that you have black-and-white icons representing the legacy Exchange servers.

If you don't see this information, force the CA to replicate by right-clicking the CA object and selecting Replicate Now from the flyout menu. Check the Event Log to make sure there aren't any errors. If you experience any issues, you can use the Diagnostics Logging tab in the properties window for a server in ESM to assist in troubleshooting (or to overwhelm you with information).

Site Replication Service Configuration

When you install the first Exchange 2003 server in a site, the Exchange Setup program initializes the SRS. This service maintains a copy of the legacy Exchange directory service that it can replicate with legacy servers in the site, as shown in Figure 12.40.

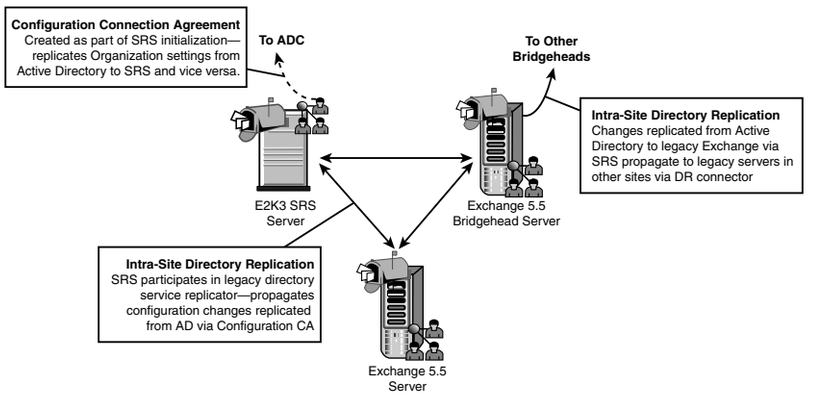

Figure 12.40 Site Replication Service allows Exchange 2003 server to participate in legacy Exchange directory service replication to simplify Connection Agreement connections.

SRS acts as an endpoint for the Configuration Connection Agreement created in the ADC by Exchange Setup. This allows SRS to funnel organizational changes made in Active Directory into the legacy Exchange directory service, where they propagate to the legacy servers via standard directory service replication.

It's important to keep in mind that the SRS **does not** replicate directly to Active Directory. You still need the ADC to move data to and from Active Directory and the legacy Exchange directory service. The SRS simply makes it possible to home the Exchange side of a Connection Agreement to an Exchange 2003 server.

You should manually change the endpoints of Recipient and Public Folder CAs to point at SRS rather than a legacy Exchange server. In this way, you can decommission your legacy servers without losing synchronization with Active Directory.

SRS does not run as a clustered resource. Because the first Exchange 2003 server in a site must run SRS, you cannot install the first Exchange 2003 server in a site on a cluster. Install at least one standalone Exchange 2003 server to act as SRS and then install Exchange on the cluster. (This was also true for Exchange 2000.)

Managing the SRS Directory

You cannot manage the content of the SRS directory directly from Exchange System Manager. It's a legacy directory service, so you need a copy of Admin, the legacy Exchange administration utility.

You can use Admin from another Exchange server or you can install it on your Exchange 2003 server (or management workstation) using an Exchange Setup option. Figure 12.41 shows the option.

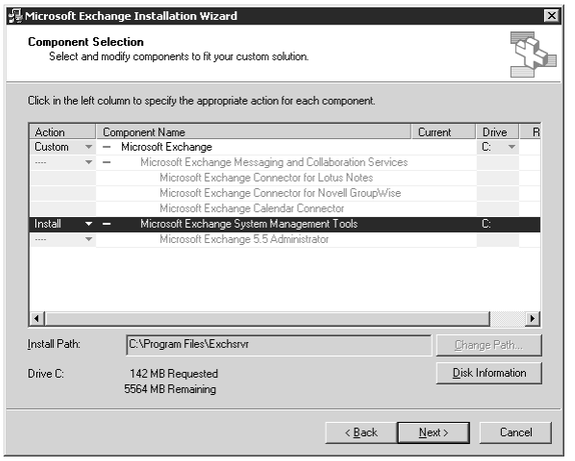

Figure 12.41 Installing the legacy Admin tool on an Exchange 2003 server allows you to manage an SRS databases and legacy Exchange servers.

Installing the legacy Admin tool also comes in handy because you can manage other legacy servers in addition to the SRS server. You do not need to run SRS to load the Admin tool.

Configuring New SRS Servers

Exchange Setup installs SRS on every Exchange 2003 server, but only initializes the service on the first Exchange 2003 server in a legacy site. You can see the servers running SRS in ESM by drilling down to Tools | Site Replication Services. Figure 12.42 shows an example.

You can use ESM to start SRS on additional servers if you want to transfer Connection Agreement endpoints to another Exchange 2003 server. You must run ESM on the console of the server where you want to initialize SRS (or in a remote desktop session connected to the server).

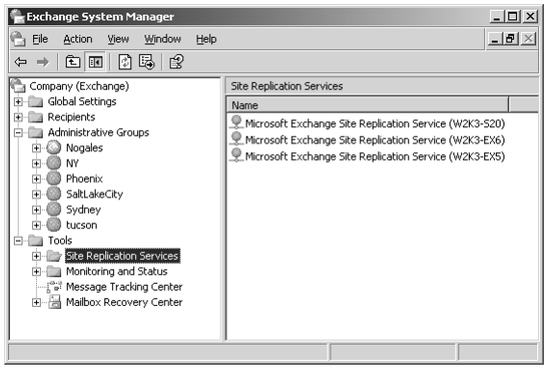

Figure 12.42 ESM showing SRS servers. Each site with a legacy Exchange server and an Exchange 2003 server must have an SRS server.

1. Right-click the **Site Replication Services** icon and select **New | Site Replication Service** from the flyout menu.
2. A popup window asks if you are sure you want to start the service. Click **Yes** to acknowledge.
3. The Initial SRS Replication window opens, offering you a choice of which legacy server or SRS server to replicate from during the initial population of the local directory service database. Figure 12.43 shows an example. Select a server and click **OK**. The Site Replication Service logon window opens, as shown in Figure 12.44.

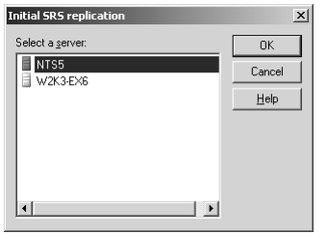

Figure 12.43 When creating a new SRS server, you can select the legacy server or the SRS server from which to pull initial replication.

4. Enter the password for the Exchange service account used by the SRS.

Figure 12.44 SRS logon window allows you to enter the credentials of the legacy Exchange service account.

Exchange now starts SRS on the server, initializes the legacy directory service database, and joins the replication topology of the site. You can now rehome Connection Agreements to the server as described in the next section.

Changing Connection Agreement Endpoints

When the CA Wizard first creates the Recipient and Public Folder Connection Agreements, it selects a legacy Exchange server in each site to act as the endpoint for the CA. To keep from changing the CA endpoints from one legacy server to the next as you decommission them, rehome the CA endpoints to an SRS server and be done with it.

Change the endpoint of a CA using the Properties window for the Connection Agreement in the ADC Services console.

1. Select the Connections tab.
2. Change the server name in the **Exchange Server Information** field from the legacy Exchange server to the Fully Qualified Domain Name (FQDN) of the SRS server in that site.
3. **Important.** Change the port number from **389** to **379**. The SRS service listens for LDAP queries on port 379. This permits SRS to coexist with Active Directory if you run Exchange 2003 on a domain controller.
4. When prompted that the change requires a full replication, click **OK** to acknowledge.
5. Verify that the Connection Agreement operates correctly by making a small change in Active Directory and then manually running the CA to see if the change replicates to legacy Exchange.

Completing the Migration

At this point, you've installed the ADC and your first Exchange 2003 server. You've replicated the public and system folders to the new server and verified that each of the Connection Agreements works.

You can now install additional Exchange 2003 servers in this and other sites and start laying out your new messaging infrastructure. This involves creating new Routing groups, moving mailboxes, moving connectors, decommissioning legacy servers, and shifting to Exchange Native mode.

Create Routing Groups

Each legacy site forms a separate Routing group in Exchange 2003, so as soon as you install an Exchange 2003 server in a second site, you should create a Routing Group connector between them and remove the legacy Site connector. This has several benefits.

- You stop routing messages through the slow, cumbersome MTA on the legacy Exchange bridgeheads.
- You reduce your reliance on the error-prone Gateway Address Routing Table (GWART) and move toward using the Link State Table exclusively for message routing.
- Once you get multiple Exchange 2003 servers in each site, you can take advantage of fault tolerant message routing and reduce your reliance on a single bridgehead.

To replace the legacy Site connectors, just install a Routing Group connector between sites, select the Exchange 2003 as the bridgeheads, verify that messages flow between those two bridgeheads, and then remove the Site connectors using legacy Exchange Admin.

Do a final verification that mail sent from a user with a legacy Exchange home server in one site arrives in the mailbox of a user with a legacy Exchange mailbox in another site. This assures you that the legacy servers and the new servers all understand the new topology.

For safety's sake, once you have replaced sufficient Site connectors so that you don't need to worry about routing loops, you should start putting multiple routes between Routing groups to assure fault tolerance in case one network connection should go down.

For details on creating Routing Group connectors, and for details on SMTP routing and the operation of Link State tables, see Chapter 8.

Identify Legacy Exchange Services

It's important to map out the legacy services so you have a good idea how to transfer their functionality to Exchange 2003 as you migrate. Be on the lookout for servers hosting the following features:

- **Internet Mail Service (IMS).** To retain access to Internet e-mail, make it a top priority to transfer your Internet mail from any legacy Exchange IMS servers to Exchange 2003 servers acting as bridgeheads for an SMTP connector. To assure continuity of service, leave the existing IMS connection in place with a high cost until you verify that the new SMTP connector works in all situations. See Chapter 8, "Message Routing," for details.
- **SNADS, PROFS, and ccMail connectors.** Exchange 2003 does not support these connectors. Leave a legacy Exchange server in place to host the connectors while you find some other method to connect to these services or convince users to abandon them.
- **Third-party fax connectors.** Verify that the vendor of the fax connector supplies an Exchange 2003 version and test it in your lab.
- **Routing Calculation Server.** While you retain legacy Exchange servers in an organization, you need to provide them with routing information via the GWART. Only one legacy server in a site calculates the GWART. You can select the calculation server using the legacy Admin utility. Drill down to the Configuration container for the site and open the Properties window for the Site Addressing object. Figure 12.45 shows an example. Select an Exchange 2003 server from the dropdown list. Any Exchange 2003 server can perform this function. It does not need to run SRS.

Before using an Exchange 2003 server to calculate the GWART, transfer all Internet mail routing to Exchange 2003 servers. When Exchange 2003 calculates the GWART, it removes the @ sign from the address scope. Legacy Exchange IMS requires this @ sign to work properly.

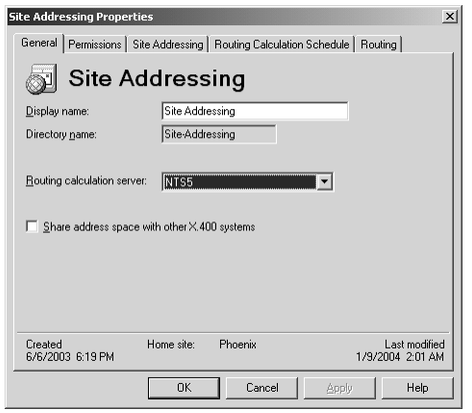

Figure 12.45 You can use legacy Admin to select a different routing calculation server when the time comes to decommission the server.

- **Bridgehead servers.** Before decommissioning a legacy server that acts as a bridgehead for a Site connector or a Directory Service connector, evaluate whether you still need the connector. In most circumstances, once you have Exchange 2003 servers in all sites, you do not want legacy Exchange servers to act as bridgeheads.
- **Address Book Views.** You cannot migrate legacy Address Book Views to Active Directory. Create custom address lists with LDAP queries that mimic the selection criteria used for a particular Address Book View.
- **Key Management Server (KMS).** If you have deployed secure messaging in your legacy Exchange organization, you'll have at least one legacy Exchange server acting as the KMS. Exchange 2003 does not have a KMS function. That's because Windows Server 2003 Certification Authorities can store private keys, so you do not need a KMS. See the Microsoft white paper titled, "Key Archival and Management in Windows Server 2003" (download from `http://snipurl.com/5z3s`) for instructions on transferring the KMS database to a Windows Server 2003 CA.

Complete Mailbox Moves

During the initial testing of your first Exchange 2003 server, you moved a few user mailboxes from the legacy servers to the new server. Now that

you have installed sufficient Exchange 2003 servers to handle your user population, continue moving mailboxes until all users have their mailboxes on new Exchange 2003 servers.

ESM can move four mailboxes at a time, so this portion of the migration should not take long unless you have users with extremely large mailboxes. See Chapter 7, "Managing Storage and Mailboxes," for details.

Shift to Exchange Native Mode

Once you have decommissioned all your legacy servers, you can shift the Exchange organization to Native mode. This exposes the following additional features:

- **Move mailboxes between Administrative Groups**. In Native mode, you can move a user's mailbox from an Exchange server in one AG to an Exchange server in another AG, so long as you have Exchange Administrator permissions on both AGs.
- **Consolidate Administrative Groups**. Once you're in Native mode, you can create Administrative Groups that make sense from an IT operational perspective instead of the site-centric model in legacy Exchange. The only drawback is that you cannot move servers from one Administrative Group to another. You'll have to install a server in the new Administrative Group, move mailboxes and connectors to this server, and then decommission and reuse the old server. This is called a "swing" transfer. Native mode also allows you to have Routing Group boundaries that do not follow the boundaries of Administrative Groups.
- **Create Query-Based Distribution Groups**. The Native mode organization permits you to mail-enable a QDG so you can take advantage of the dynamic group membership features inherent in QDG operation.
- **8BITMIME on Exchange 2003 Bridgehead Servers**. If two bridgehead servers in a Native mode organization run Exchange 2003, then they use 8BITMIME for data transfers. This improves bandwidth utilization by nearly 15 percent, all other things being equal.
- **Automatic Zombie removal**. When Exchange 2003 evaluates trustees in an Access Control List, if it finds an entry referring to

an account that no longer exists, it removes the entry from the ACL. This eventually eliminates any performance issues arising from zombie entries on public folder permissions.

- **Mailbox-enable InetOrgPerson objects**. If you need to create instances of the InetOrgPerson class to use as User objects for compatibility with NDS or PeopleSoft or iPlanet, you can mail-enable and mailbox-enable those objects once the organization is in Native mode.

You cannot reverse the shift to Exchange Native mode. Once you save the configuration change, you can no longer introduce legacy Exchange servers into your organization.

Shifting to Native mode toggles the *msExchMixedMode* attribute in the Organization object to FALSE. Don't try using a utility to toggle it back to TRUE because other configuration changes are made in the background once an Exchange server sees the Native mode flag.

Native Mode Prerequisites

You must decommission all legacy Exchange servers in the organization before shifting to Native mode. This involves removing (de-installing) Exchange from the servers. If you have servers that no longer function, you can delete the associated objects from Active Directory using Exchange System Manager. (You might need to remove the objects from the SRS using Admin, as well.)

You must also remove Site Replication Service from your organization by shutting down the service using ESM at each SRS server. SRS maintains a copy of the legacy Directory Service, so from the perspective of Exchange, an Exchange 2003 server running SRS represents a legacy server.

Performing the Shift

When you're ready to do the shift, launch ESM and open the Properties window for the Organization object at the top of the tree. Figure 12.46 shows an example.

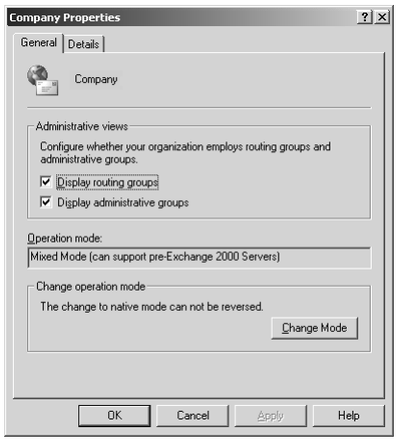

Figure 12.46 The Organization properties window showing the Change Mode button, which will be available only if all prerequisites are met to shift to Exchange Native mode.

If you have done all the necessary prerequisites to make the change to Native mode, the Change Mode button will be available. Click the button, acknowledge the warning, click OK and you're done.

Yes, it's true.

You're done.

At least for now.

Looking Forward

No doubt about it, this chapter contains the hardest work you'll probably ever do as an Exchange administrator. Completing the migration to Exchange 2003 makes you feel like you're soaring at 30,000 feet with nothing around you but blue sky, blue horizons, and, if you're an *X-Files* fan, a blue space alien who wants to take snapshots of your eyeballs. If it makes you feel any better, the steps you followed in this chapter are much simpler than an upgrade from Exchange 5.5 to Exchange 2000.

Still, you have earned the right to relax a while, but don't rest on your laurels quite yet. You need to make sure that your system doesn't become a nest for viruses and spam, and you need to make sure you have a good backup process in place so you can soar up there above the clouds without worrying that a simple deleted mailbox item will send you plummeting back to Earth.