PART VI

Migrate to Windows Server 2008

This section deals with moving to the new Windows Server 2008 infrastructure you prepared in the parallel network for virtual service offerings. All systems are go, and now you need to move all of the content from the legacy network to the new parallel network. This means performing the actual migration, as well as preparing your support and operational staff to work in the new environment.

CHAPTER 12

Put the VSO Network into Production

The final technical preparations for the parallel network for virtual service offerings (VSOs) are now done. It is almost ready to go online. Now you need to migrate all users, PCs, data, and services to the parallel network and decommission the legacy environment. It is at the end of this operation that you will have completed your migration to Windows Server 2008 (WS08). You will then move on to the operation of the new network. It is at this stage that you will discover that there are changes in the way you need to administer and operate a native WS08 network.

As you performed all of the operations outlined in the previous chapters, you noticed that several traditional IT tasks have been modified and that new tasks have been added to the operational roster. As you prepare to place the parallel network online and complete the user migration from the legacy network, you realize that there is one final activity you must perform. It is the review of administrative and operational roles within your enterprise network. Once this review is done, your network will be ready for prime time.

These changes will be discussed here. Chapter 13 will take a close look at the administration of Windows Server 2008 networks, outlining specific tasks and how you perform them. But before you get there, you need to populate your new VSO network.

Considerations for the Migration to the Parallel VSO Network

Remember that when you migrate services from your existing network to the parallel VSO network you must perform some form of server rotation. When you select a service to migrate, you should prepare the new virtual servers that will host this service first and ensure that you have a fallback solution in case of service failure. This is the advantage of the parallel VSO network: The legacy network is always available for service fallback if you need it. But if you've done your homework right, you won't. Throughout the process so far, you've carefully prepared native services in WS08 mode, running the latest and greatest features of this powerful operating system (OS). In addition, you've implemented business continuity solutions both for the resource pool and the virtual service offerings to make sure they are always running and always available.

In your considerations for the migration to the parallel VSO network, you'll want to think about the following:

- **The server rotation process** This process will be used to rotate and recover hardware as much as possible as you move to the new network.
- **The migration order** The order in which you will migrate services to the new network.

Both need to be addressed before you can move on.

The Server Rotation Process (Resource Pools)

Chapter 6 introduced the concept of server rotation during the migration of services to VSOs (see Figure 12-1). In the past, this process was relatively simple because you were moving from hardware server to hardware server, but in this case, it is different because hardware and services are now divided into two different infrastructures. Ideally, only 64-bit hardware will be reused and moved to the resource pool, but in most cases, organizations will not be using only 64-bit servers in their legacy network. This means that now is the ideal time to perform a serious server consolidation effort and rationalize as many of these devices as possible.

Keep the following in mind as you move through the server rotation process:

- Get rid of anything beige. Beige servers are usually stand-alone systems that use older hardware architectures, which use a lot of power and generate a ton of heat. If you can, get rid of them all.

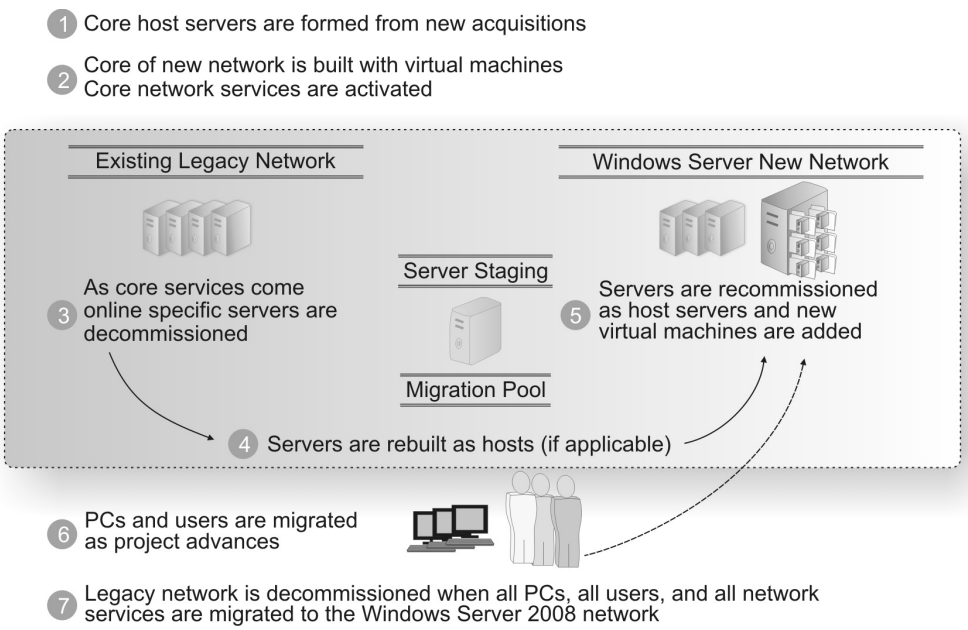

Figure 12-1 The server rotation process

- Recommission anything that is based on x64 hardware. Ideally, these will be rack-mounted or, even better, blade servers you can easily hook up to shared storage. The most important consideration for x64 server re-commissioning as host servers is the nature of the processor(s) it contains. In order to profit from x64 virtualization, the processors must be either Intel VT-enabled processors or AMD-V processors that offer integrated virtualization support.
- Recommission anything that is a recent acquisition. Even if you recommission some 32-bit systems, you can still run virtualization hosting services on them. You just have to run Microsoft Virtual Server (www.microsoft.com/windowsserversystem/virtualserver) instead of Windows Server Hyper-V. And you have to make sure you do so on a full installation of WS08, not Server Core, because Virtual Server requires components of Internet Information Services (IIS) that are not available on Server Core. Use these systems for lower-priority virtual workloads in production. Even better, move them to run testing or development environments in your laboratories. Note that if you deploy Virtual Server through System Center Virtual Machine Manager, you will not need IIS on the system.
- Acquire new hardware when possible. If you have a leasing program, perhaps you can exchange your 32-bit systems for new 64-bit systems, especially the server-in-a-box systems you will need for remote offices.

TIP *For example, cabinet manufacturer Kell Systems offers small-footprint portable server casings that are ideal for the server-in-a-box concept. Find out more at www.kellsystems.com.*

- Make sure you dispose of your unused servers in a proper manner. Several commercial organizations make a business of green server disposal. Look them up on the Internet.
- If you can, cannibalize systems that you will not be retaining for items such as random access memory (RAM) chips, network cards, and hard disk drives. Add them to your resource pool.
- Recommission some more powerful 32-bit servers as either development or administration workstations if you can.
- Make sure all hardware you retain will be part of the resource pool Active Directory Domain Services (ADDS) single-domain forest to ensure tighter security between resource pools and virtual service offerings.
- Make sure you completely wipe disks and all existing data from any systems you decommission. You don't want to have someone rebuild the data on a disk drive because it wasn't wiped properly.

TIP *There are some very good disk-wiping tools on the market. Just search for "disk wiping" on the Internet through your favorite search engine.*

This process will take some time, but you'll find that it is much more malleable and straightforward than resource management has ever been before.

As for the migration itself, we've discussed the preparation of the resource pool servers at length in Chapter 6; proceed with the steps outlined there to prepare enough host servers to start the migration of the VSOs.

TIP *Remember that if your host servers are blades and are connected to shared storage, you can actually rely on copies of the logical units making up the system partition to provision new host servers. This is faster and easier than using an actual deployment tool.*

The Migration Order (Virtual Service Offerings)

When you're ready to move to the new network, you'll have to put together a migration strategy. This strategy must cover four major activities:

- **Security principal migration** Migrating users and computers from the directory service in use in the legacy network to Active Directory Domain Services in the new network.
- **Member server migrations** Migrating all services found on member servers, including file, print, management, collaboration, and more. This also includes special products, such as Exchange, SQL Server, and other services that manage the back office.

TIP *To find out more about Microsoft Exchange Server migration, look up* MCITP Self-Paced Training Kit (Exam 70-238): Deploying Messaging Solutions with Microsoft® Exchange Server 2007*, by Ruest and Ruest, published by MS Press.*

- **PC migrations** Migrating PCs from obsolete operating systems to Windows Vista. This will also involve capturing and restoring user data and preferences or profiles. This portion of the migration may already be done.
- **Custom application migrations** This involves mostly conversions or redevelopment of both rich-client and Web-based in-house applications.

Each of the four stages is a mini-project of its own, and each will require its own resources. You should begin with the security principal migration. If you set up your environment the right way, you will be able to migrate user and computer accounts, as well as groups, at your own pace, giving yourself time to prepare the other aspects of the project. In addition, by using the parallel VSO network approach, you don't affect the current production environment so that users in either network will be able to share applications and services from both networks during the entire length of the migration project.

Next, you'll be able to move to member server migrations. Ideally, you will be able to migrate a service, stabilize the new virtual servers, and then proceed to the client migration. For client migration, you will ideally migrate their PCs to Windows Vista (if it isn't already done) in order to fully profit from the new services infrastructure. As you migrate PCs, you will need to move users to the new service and monitor service performance. It will usually take one to two months of operation before services are fully stabilized. Afterward, you will want to monitor services for growth potential. Meanwhile, you can have your development staff working on upgrades of your key applications, since these will take time and may not be ready until all other migration tasks have been performed.

TIP *If you need to migrate PCs, we strongly recommend you pick up the free e-book* The Definitive Guide to Vista Migration *at www.realtime-nexus.com/dgvm.htm. It provides a wealth of information that may also assist you in the migration of your servers.*

Keep the following considerations in mind as you prepare your migration:

- **Identity servers** You'll begin with the identity servers to perform the security principal migration. Domain controllers (DCs) and Active Directory Domain Services are absolutely essential for the new network to function. Prepare these servers first. Populate enough DCs in the virtual environment to provide a given level of service. If you are a small organization (SORG) with only one site, then you can begin the migration of other services once you have your base production forest infrastructure in place. In very small organizations (about 100 users or fewer), this will mean a single-domain forest and, therefore, two DCs for redundancy. In medium (MORG) to large organizations (LORG), which have at least two sites, you can usually begin the migration of some of your services once you have DCs located in at least two sites. Refer to the recommendations in Chapter 6 for the base requirements for the construction of these DCs.
- **Network infrastructure** Next, you can move to the migration of Dynamic Host Configuration Protocol (DHCP) and Windows Internet Naming Service (WINS)—if you haven't decided to use DNS GlobalNames Zones—because no special client is required for computers to use these services. They work with all versions of Windows. It may be easiest to use a new pool of addresses to do so, however, if you don't want to affect your production systems. Or another good way to perform this migration is to move up to IPv6 in the new network while the legacy network continues to offer IPv4 addresses. Make sure your applications are compatible with IPv6 before you decide to use this strategy. For example, verify network intrusion detection systems, antivirus systems, network analyzers, and so on. Next, create the Windows Deployment Services (WDS) servers because they are required to build PCs. Finally, create your systems management and operational servers so that your management infrastructure will be ready to manage new servers as they are added to the parallel network. The result should be a core network that is ready to deliver services both in a central office to meet the needs of SORGs, MORGs, and LORGs (see Figure 12-2) and remote offices to meet the needs of MORGs and LORGs (see Figure 12-3). And if you followed the advice in Chapter 11, you will already have your core business continuity strategy in place (see Figure 12-4).

TIP *Remember that because VSOs run on virtual machines, you don't really need a tool like WDS to provision them, since all you need to do is copy the files that make up source machines to create a new one. Also see the Application Virtualization: Ending DLL hell once and for all webcast at www.bitpipe.com/detail/RES/1193672482_325.html.*

- **Dedicated Web servers** If you're using single-purpose Web servers, then the dedicated Web servers can be next, since IIS 7 provides backward compatibility for Web applications. Be sure to thoroughly test all applications before putting them into production. There are serious modifications in IIS 7 that may affect application operation. As with network infrastructure servers, no special client is required to operate with IIS.

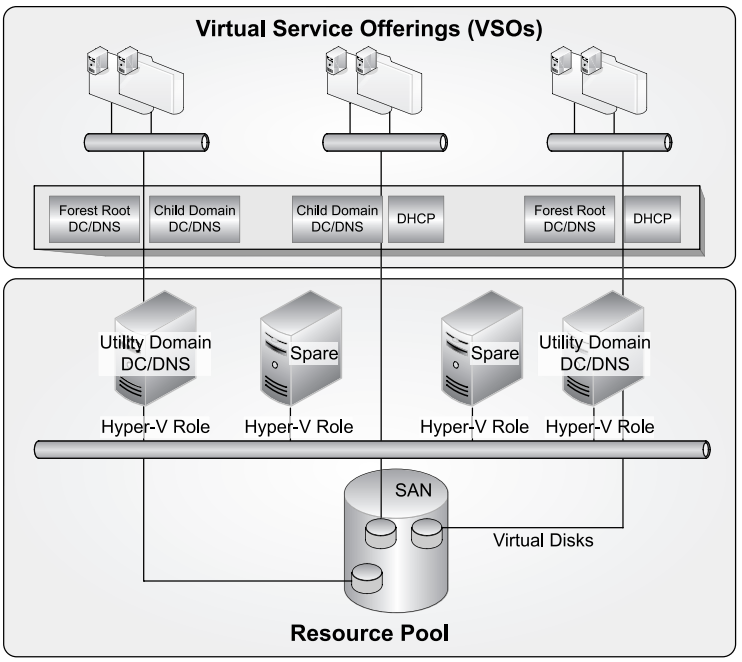

Figure 12-2 The core network for a central office

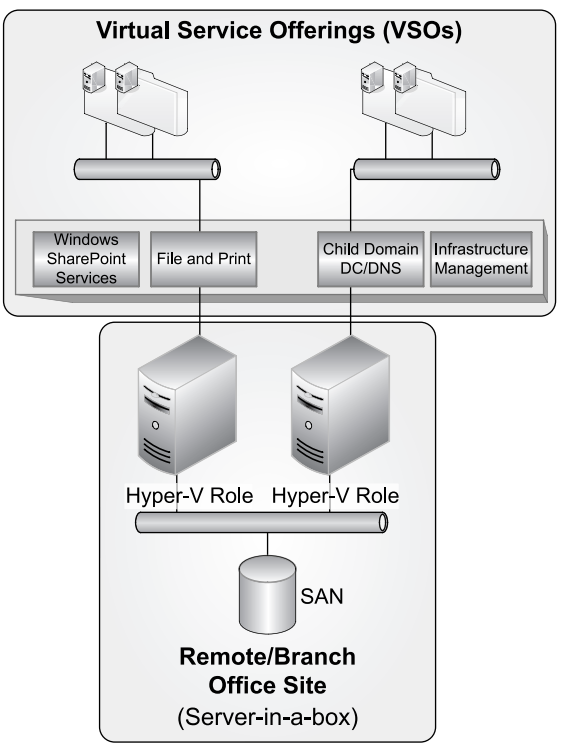

Figure 12-3 Using server-in-a-box for remote offices

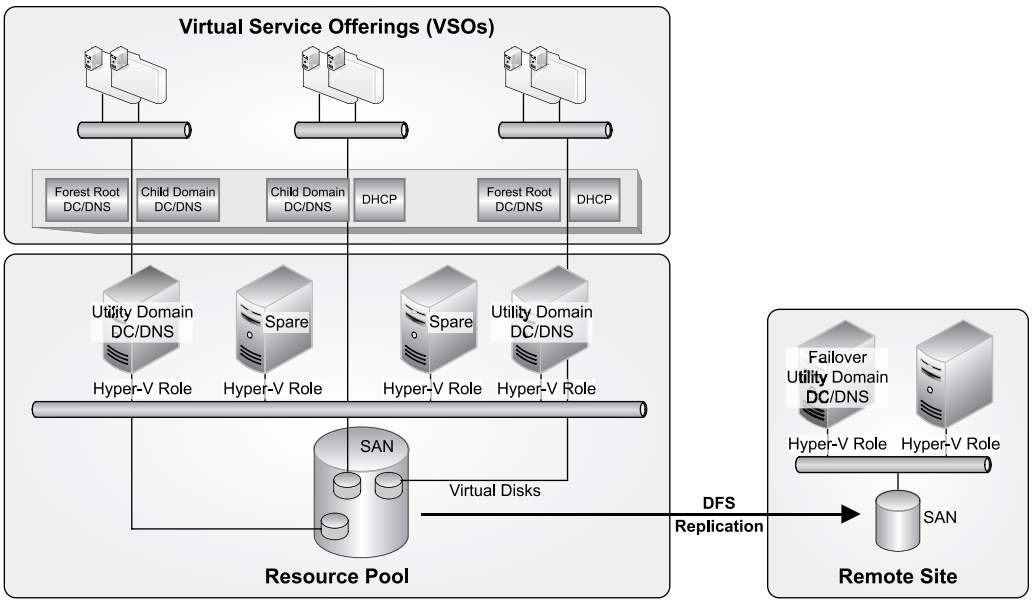

FIGURE 12-4 Business continuity from site to site

- **Application servers** General-purpose IIS servers can also be migrated at the same time as the dedicated Web servers for the same reason. Database servers can also be migrated since, once again, they will operate with existing clients. Corporate application servers can also be migrated since they will also operate with existing clients. Remember to test each component before releasing it to end users.
- **Terminal Services** WS08 Terminal Services (TS) servers can operate through Remote Desktop Web connections through TS Web Access. Clients need to be running the latest version of the Remote Desktop client (RDC). If you want to publish applications to take advantage of RemoteApps, and you want to make them available to existing PCs, then make sure you deploy the latest RDC to each PC.

TIP *You might not need to work with Terminal Services at all if you've decided to move to application virtualization. We strongly suggest you take a look at this operating model, since it is less expensive and more effective than running remote applications through Terminal Services. For more information, see Chapter 6 in* The Definitive Guide to Vista Migration *at www.realtime-nexus.com/dgvm.htm.*

- **File and print services** File services require transfers of large quantities of data to migrate. As such, they should be kept toward the end of your migration or, at the very least, they should be coordinated with PC migrations (servers first, then PCs). Special attention should be paid to file ownership and access rights when files are migrated from the legacy network to the new network. Print services can be moved at the same time. This will decrease the number of printer drivers you need to make available on your systems, since you will only have to deal with updated PC systems.

CAUTION *Keep in mind that you can and should look to the replacement of file services with collaboration services based on Windows SharePoint Services (WSS). WSS provides a richer environment for collaboration than file servers can on their own.*

- **Collaboration services** These services should be kept for last because they are at the basis of network service evolution. WS08 collaboration services extend the capabilities of your network. As such, they require the full capabilities of the new network. You might consider using them, especially the WSS role, instead of working with file servers, replacing the user-oriented file servers altogether with WSS servers.

Remember to create your organizational unit (OU) structure first and pre-stage servers in the directory. Then create the server kernel and follow through with the server role staging process. Then, and only then, can you migrate data and users to the new network.

Begin the Migration to the Parallel VSO Network

Your network is now ready to be launched into the production environment. So far, every operation you followed has been—or should have been—within a laboratory environment. Even the final procedures you'll use for the migration itself must be thoroughly tested before you move to the migration in the new production network. You'll begin by populating the directory in the new network.

Migrate Security Principals

Start by migrating user accounts, PC accounts, and data into the new directory. You'll need to perform the following steps.

- **Create trusts** The first step is to create a two-way trust relationship between the production domain and your legacy domain. This two-way trust serves to support the operation of both networks at the same time. It will need to remain in place until the migration is complete.
- **Nest groups** The second step is to nest the appropriate global groups into the local groups that are required to grant joint access to resources from both domains. For example, if you are migrating a select group of users and the migration cannot be completed all at once, you need to ensure that both sets of users—the ones located in the legacy network and the ones already migrated to the new network—have access to joint resources so that they can continue to work together for the duration of the migration. This approach will need to be extended to all users of shared folders because they must share resources for the duration of your migration.
- **User account migration** Next, you'll need to migrate user accounts from the legacy network to the new environment. Users should be given authority to modify their own personal information through the use of a user data modification web page, as discussed in Chapter 7, so that they can catch any errors in the data. The Active Directory Migration Tool (ADMT) available from Microsoft will provide great help here, since it migrates user accounts, passwords, groups and group memberships, service accounts, computer accounts, and more.

NOTE *This is an excellent opportunity to clean up your legacy directory database as it is imported into the new production domain.*

- **Service account migration** You shouldn't need to migrate service accounts since they have been re-created into the new network as new services have been activated.
- **User data migration** You can then proceed to migrate user data that is located on network shares, such as home directories, or, even better yet, through Folder Redirection Group Policy Objects (GPOs). This is where it is important to use the proper tool for user account migration because each account that is migrated is assigned a new security identifier (SID). This SID is different from the SID used to create the information in the legacy network. This means that it is possible for users to lose access to their data once it has been moved to a new network if you don't manage the migration properly. ADMT can either maintain a SID history when it migrates a user account, giving the account the ability to present a legacy SID when accessing data in the new network, or it can perform SID translation, replacing the legacy SID with the new SID on the object to avoid this problem.
- **PC account migration** Next, you'll need to migrate PCs. If PCs do not need to be restaged (they are already running Windows Vista or, at least, Windows XP), then you can use ADMT to migrate computer accounts and reset security descriptors on each system. If, on the other hand, they are not up to date and need to be staged, you will need to first recover all user data from the system, reinstall the system, join it to the new domain during reinstallation, and then restore user data to the system.

NOTE *Once again, look to* The Definitive Guide for Vista Migration *for more information.*

- **Decommission legacy network** The last step will consist of decommissioning the legacy network. This will be the step that identifies when the migration is complete.

Once these steps are complete, your migration will be finalized and you'll be ready to move on to the administration and optimization of your new network (see Figure 12-5).

NOTE *Using a commercial migration tool avoids many of the migration hassles because it takes all of these situations into account.*

Create Two-Way Trusts

The first step in the security principal migration is to create two-way trusts between the legacy and the new production domains. This is relatively straightforward, but it requires domain administration credentials in both domains. This means creating a trust between the new global child production domain (GCPD) and whichever legacy domain(s) that contain your user accounts.

CAUTION *Make sure your new virtual servers can communicate with the source legacy domains before you proceed with this operation. This may mean changing the properties of your Internet Protocol (IP) connections to include additional Domain Name System (DNS) servers. You should also ping the legacy domain before beginning this operation to make sure the names resolve properly.*

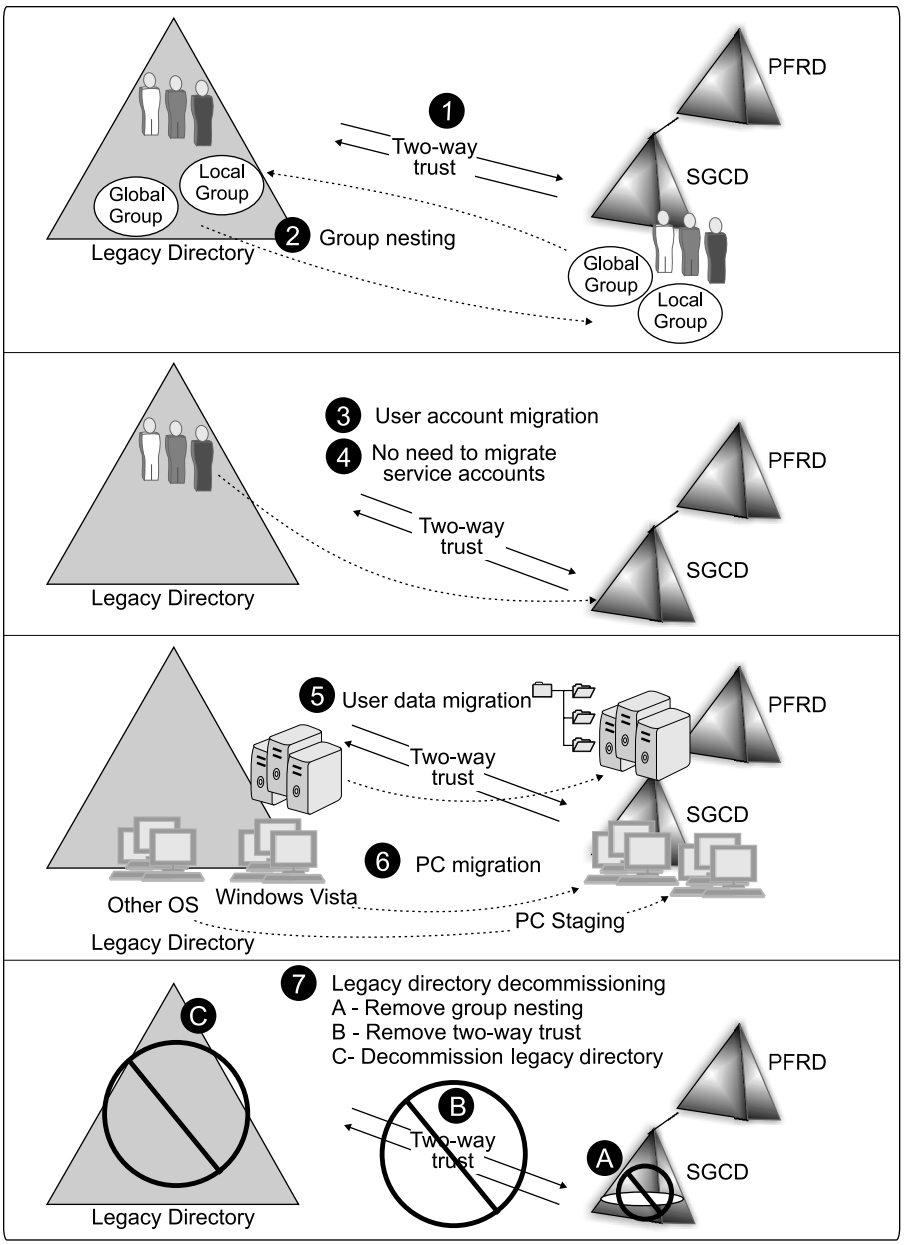

Figure 12-5 The user account, data, and PC account migration process

Trusts are created in the Active Directory Domains and Trusts console. Use the following steps:

1. Perform this operation from within the parallel network. Log on with domain administration credentials. Make sure you have the same level of credentials in the source domains.
2. Launch Start menu | Administrative Tools | Active Directory Domains and Trusts.
3. Expand the forest in the tree pane until you see the GCPD, and right-click the domain name to choose Properties.
4. Move to the Trusts tab.
5. Click New Trust.
6. In the New Trust Wizard, click Next.
7. You can create trusts between domains, forests, or Kerberos V5 realms (UNIX or Linux). In this case, you want a domain-to-domain trust. Type the name of the source domain, and click Next.
8. The system will search for the domain and then produce the appropriate trust creation page. Select Two-Way and click Next (see Figure 12-6).

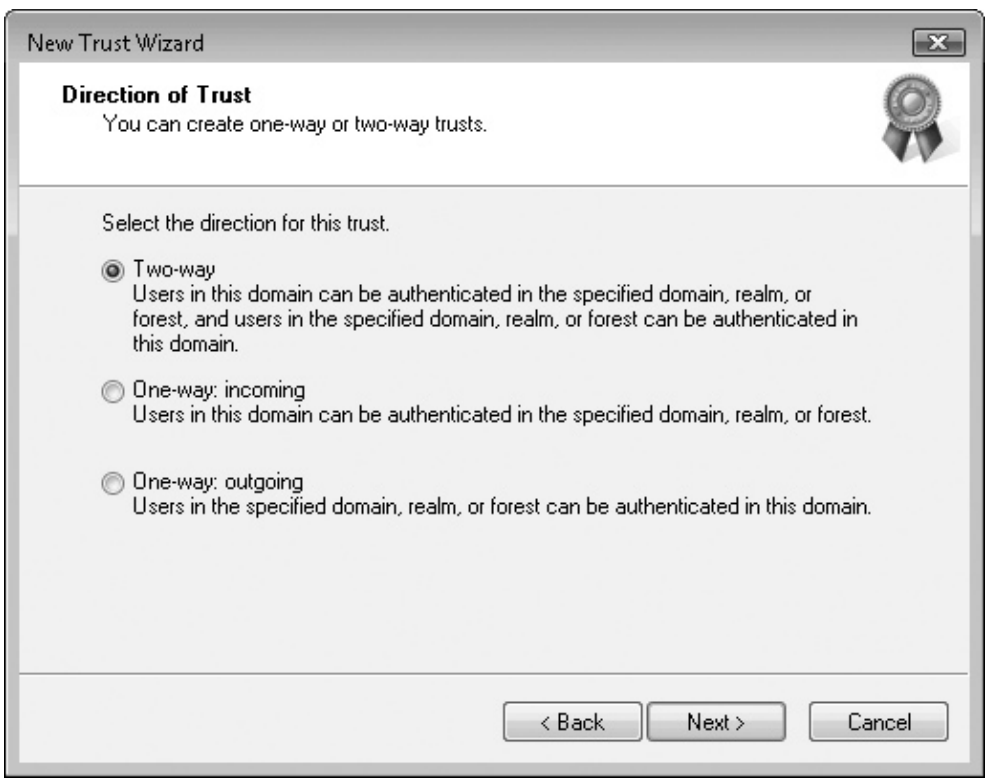

Figure 12-6 Creating a two-way trust

NOTE *You want to use a two-way trust to ensure that operations work for the duration of the migration and that users can access resources that have been migrated as well as those that have not.*

9. In the Sides of Trust dialog box, select Both This Domain And The Specified Domain to create both sides of the trust at once. Click Next.
10. Provide the credentials for the source domain. Remember to include the domain name in your credentials, either through a User Principal Name (UPN) or using domainname\username format. Click Next.
11. Next, specify the scope of authentication for users for the local domain. For a migration, it is best to use domain-wide authentication (see Figure 12-7). Click Next. Repeat for the source domain.
12. Review your selections and click Next to create the trust.
13. Once the trust is created, click Next to configure it.
14. Select Yes, confirm the outgoing trust, and click Next. Select Yes, confirm the incoming trust, and click Next.

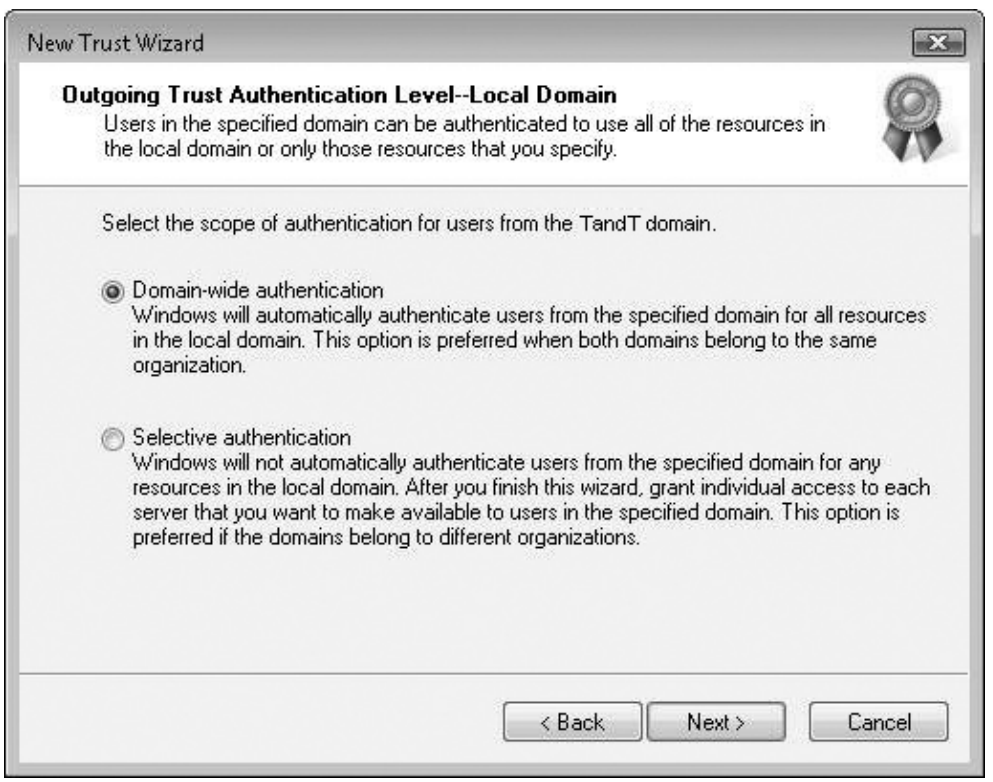

FIGURE 12-7 Selecting authentication levels

15. Click Finish upon confirmation of your trust relationship. A warning dialog box about enabling SID history will be displayed (see Figure 12-8). Click OK. Do not select the Do Not Show This Dialog Box Again check box, because it is useful to have a reminder about turning off SID history when you are done. Click OK again to close the domain Properties dialog box.

Repeat this operation for each source domain you need to link to. Make note of each trust you put in place, because you will need to remove them once you have completed the migration.

Nest Global Groups

The next step is to grant access rights to users in both domains. This will let users from the target domain access resources that are still in the source domain, and users in the source domain can access resources in the target domain; use Server Manager to do so.

You will need to create domain local groups to grant access to members of the source domain to target domain resources. Remember the Account-Global Group-Local Group-Permissions (AGLP) rule (see Figure 12-9); only domain local or local groups can contain objects from other domains in this case.

Keep this in mind as you assign access rights.

1. Go to Server Manager | Roles | Active Directory Domain Services | Active Directory Users and Computers.
2. Locate the container with the groups you want to target. For example, in your new domain, go to the People OU structure.
3. Create appropriate domain local groups.
4. Use the group's Properties dialog box to go to the Members tab, and click Add.
5. In the Select Users, Contacts, Computers, or Groups dialog box, click Locations.
6. Select the source domain, and click OK.
7. Search for the source group in the source domain, and click Add. Click OK when done.

Figure 12-8 SID history warning

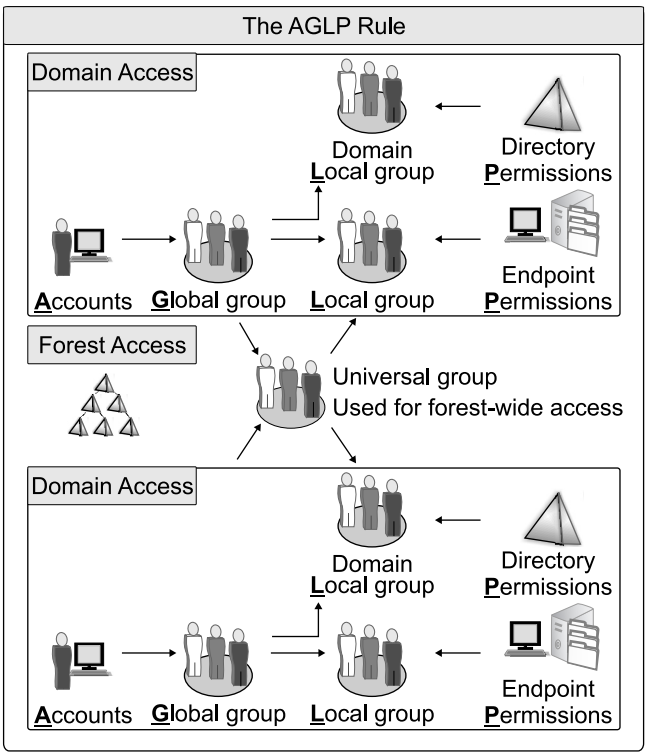

FIGURE 12-9 The AGLP rule

Repeat for each group you need to grant access to. You can also use the `DS` commands to perform this operation through a script. In this case, you'll need the `DSADD` and `DSMOD` commands.

For other resources, you'll need to use member server local groups to grant resource access. You're now ready to move contents from one domain to the other.

Use the Active Directory Migration Tool

The Active Directory Migration Tool (ADMT) offers several features for the support of the parallel network migration approach. It is fairly simple to use. You'll need to download and install it. You don't have to install it on a target server, but you might find it easiest to do so. Remember, you'll need domain administration credentials in both source and target domains. ADMT requires a database for use. It includes a Windows Internal Database, however, so you should be fine.

TIP *Find the ADMT at http://go.microsoft.com/fwlink/?LinkId=75627.*

Once installed, you can launch the ADMT console by moving to Administrative Tools and selecting Active Directory Migration Tool. The operation of the ADMT basically

consists of using the right mouse button to click Active Directory Migration Tool, accessing the context menu, and selecting the appropriate wizard. ADMT offers several wizards:

- User Account Migration
- Group Account Migration
- Computer Migration
- Security Translation
- Reporting
- Service Account Migration
- Exchange Directory Migration
- Password Migration

The operation of the wizards is also straightforward. You need to identify the source domain, the target domain, the objects you want to migrate, the container you want to migrate them to, and then how you want to perform the migration. In addition to performing account or group migration, ADMT supports migration of Exchange objects, such as user mailboxes, distribution lists, and so on.

NOTE *The ADMT can be run in test mode. Choosing this mode allows you to test migration results before actually performing the operation. Simply select Test The Migration Settings And Migrate Later? when you use one of the wizards.*

The best way to use ADMT in the parallel network migration process is to migrate groups of users. When ADMT migrates a group, it can also migrate the users that are contained within it, making it easier for you to determine what to migrate. But before you can move users and computers from one network to another, you need to ensure that the data you will migrate will be filtered and that all obsolete records will be removed. You don't want to input obsolete data into your brand-new WS08 network!

Enable the Password Export Server

In order to migrate user accounts with their passwords, you must enable the Password Export Server (PES). Migrating user accounts with passwords is a lot easier on both users and administrators, because you do not need to provide users with temporary passwords and users do not need to reset their passwords before they log on. You can, however, get them to reset their passwords at first logon as part of a security policy for your new environment.

The PES must be installed on any domain controller in the *source* domain. This DC must support 128-bit encryption—this is supported by most versions of Windows Server from NT on. The tricky part of this installation is that you need to have an encryption key to perform the PES installation. This key must be generated with ADMT, but this time, it must be on the *target* domain.

Make sure you install ADMT on a DC in the target domain. Then generate the key with the following command:

```
admt key /option:create /sourcedomain:SourceDomain /keyfile:KeyFile
/keypassword:*
```

This will prompt you for a password that will not be displayed on the screen. Note that *SourceDomain* is the name of the source domain and *KeyFile* is the name of the file to generate. Place the file on either a very secure file share or a Universal Serial Bus (USB) device to secure it.

You should also create a service account in the target domain. This account needs domain administration rights. Make sure you grant this account local administration rights on the source DC. This account will be used to run the password migration service.

On the source DC, locate the PES installation file. It will be under `%SYSTEMROOT%\ADMT\PES` and is called `PWDMIG.MSI`. Double-click it to launch the installation. Specify the account to run the service under, point to your encryption key file, and provide the password to unlock it and complete the installation.

Once the service is installed, you need to start it. Go to the Services console, locate the Password Export Server service, and start it. It is a good idea to leave it on manual start because this way, you can start it only when you need it. Stop it again once you have performed the migration of the passwords.

Create Domain Data Reports

To filter data from your source domain, you need to use the ADMT Reporting Wizard. This reporting tool can support the creation of several different report types to summarize the results of your migration operations:

- Migrated Users and Groups
- Migrated Computers
- Expired Computers
- Account References
- Name Conflicts

The Expired Computers report lists the computers with expired passwords. The Name Conflicts report does the same with potential objects that will have the same name in the target domain. The Account References report lists the different accounts that have permissions to access resources on a specific computer.

You should try to identify obsolete contents of the original directory before you begin to migrate contents. You can perform this removal in several ways:

- You can remove the objects from the source domain and then migrate the accounts.
- You can create new groups that contain only valid objects in the source domain and migrate objects by using these groups.
- You can move the accounts to a specific OU in the target domain, clean them up, and then move them to their destination OUs.

NOTE *Reports must be generated before you can view them. Many reports are generated from information that is collected from computers throughout your network. This will affect their performance; therefore, you may decide to use dedicated servers for this function. Also, reports are not dynamic; they are point-in-time reports and must be regenerated to get an updated picture.*

The last approach may be your best bet, since the ADMT will allow you to control the way accounts are treated after the migration. In fact, you can ensure that no account is activated until you perform a cleanup operation on the newly migrated accounts.

NOTE *More information on ADMT can be found in the ADMT Migration Guide at www.microsoft.com/downloads/details.aspx?familyid=d99ef770-3bbb-4b9e-a8bc-01e9f7ef7342&displaylang=en.*

Special ADMT Considerations

There are a few items you must keep in mind when using the ADMT. The first is related to the security identifier (SID). As mentioned earlier, all of a user's data is associated with the SID that represents the user at the time the user object is created. All of a user's data will be associated with the user's *legacy* SID. When you transfer this data to the new network, you must use a special technique that will either carry over the user's legacy SID or translate the SID on the object to the user's new SID (the one generated by the new network).

The best way to do this is to ensure that the user's legacy SID is migrated to the new domain (using the appropriate check box in the Account Migration wizards) and then to use SID translation. The latter is performed through the use of the ADMT Security Translation Wizard. But in order for security translation to work properly, you *must make sure that all of a user's data has been migrated to the new network first*; otherwise, you will need to perform the SID translation again once this is done.

It is also important to note that for SID history migration to work, the Password Export Server is required. As mentioned earlier, the PES is installed on a domain controller in the legacy network. It is best to use a dedicated server for this operation because it is resource-intensive. Therefore, you should stage a new domain controller (a backup domain controller—BDC—in Windows NT or simply a DC in Windows 2000 or 2003) and dedicate it to this task. This could be a virtual machine and does not need to be a physical installation.

Your network also needs to meet the following conditions before you can perform password migration or SID translation:

- Auditing must be enabled on the source domain. If it isn't, ADMT will offer to turn it on during the migration.
- Your target domain must be in full functional mode, but this shouldn't be an issue, since it was set to this mode during its creation in Chapter 6.
- If you are migrating from Windows NT, you must also activate legacy access in the target domain by inserting the Everyone group into the Pre-Windows 2000–Compatible Access group.

CAUTION *It is recommended to activate legacy access only for the duration of a migration operation and to deactivate it as soon as the operation is complete because it is a potential security risk. This means that you activate it, perform a user or group migration, and then deactivate it. Do not activate it for the duration of the domain migration because this can last quite a while, depending on your migration strategy and the size of the legacy domain.*

There are other prerequisites you must take care of before performing a migration (such as the service pack level for the source domain machines). ADMT will also require some additional settings, but it can automatically perform the modifications during a migration operation.

You can use the ADMT to perform most of the operations identified previously to support your network migration, including:

- Create a source domain object report for filtering purposes.
- Migrate user accounts, groups, and computer accounts (if the systems are already running Windows Vista or, at the very least, Windows XP).
- Perform security translations to give users access to their data.

The only operation it does not handle is the migration of user data that is stored on network shares. As mentioned before, it is important to migrate user data before you perform security translations.

Use a Commercial Migration Tool

While ADMT offers some powerful features, you may find that it is cumbersome to work with if you have several thousand users to migrate. Several manufacturers have put together some more comprehensive commercial tools in support of migrations from one network environment to another. These tools do not only support directory migrations, but also file server and other migration scenarios.

A good source of information on these migration tools can be found in the article "Server Migration: Moving from Here to There": at http://mcpmag.com/Features/article.asp?EditorialsID=381. While this article is a bit dated and the industry has changed as firms performed mergers and acquisitions, the information itself is still quite valid. In addition, the tools themselves have greatly evolved, making migrations even easier.

Transfer Networked User Data

After the user accounts have been migrated to the new network, but before the security translation has been performed, you must migrate networked user data. This will involve the copying of data found on server shares within the legacy network. It should include public, group, project, and user data. User data should include home directory data, if it was in use within the legacy network.

This operation consists mostly of relocating shared data from one network to the other. In most cases, it will mean moving the data from a specific share on one server to the same share on another server. This may even give you the opportunity to consolidate server processes and regroup file shares on fewer servers. In addition, if you used the practices provided in Chapter 8, you will be now using Distributed File System (DFS) shares instead of mapped drives. You will have to ensure that your migration program includes a user information program showing them how to access the new shares. This user information program should also include the procedure to access personal user data, because this process is now different.

The parallel VSO network should no longer use the home directory concept. It should use redirected folders. There is a catch, though: Redirected user folders are not created until the user has logged on at least once. You cannot simply move the user's home folder files from one server to another, because the user's destination folder won't be created until later.

Because of this, you must devise a special personal user data migration strategy. There are three possibilities:

- First, you can ask all users to move all of their home directory files into their Documents folders on their desktop. Then, when they migrate to the new network and log on for the first time, the contents of their Documents folders will automatically be moved to the new shared folder thanks to the Folder Redirection Group Policy.
- Second, you can migrate data to a holding folder and, using a special one-time logon script, move the files to the user's newly created redirected folder once the user is logged on and the Group Policy has been applied.
- Third, if you need to stage PCs because they are not running Windows Vista, you can add an operation to the profile migration process, since it will be required on all systems. The operation you need to add is similar to the first approach: Script a process that takes all of a user's home directory data and copies it to the Documents folder before performing the profile migration. The data will automatically be redirected at each user's first logon to the new network, and the GPO is applied.

Of these three strategies, the first and third are the best. The first is relatively simple, but it has a flaw: You must rely on operations that are out of your control for the process to complete. It will not work unless you have a well-trained user base and you provide them with excellent instructions. The third works when users' PCs must be staged.

Finally, you may need to migrate roaming user profiles if they were in use in the legacy network. Remember that the new network does not use roaming profiles, but relies on folder redirection instead or, at the very least, uses a combination of both. To migrate roaming profiles, simply turn the feature off in the legacy network (only for users targeted for migration). The profile will return to the local machine. If the machine is already running Windows Vista, the profile will automatically be transformed to folder redirection when the machine is joined to the new domain and the user logs on, because the GPOs will activate folder redirection. If the machine needs to be staged, the profile will be captured through the staging process.

For the actual migration of files from the source domain to the target domain, refer to "Migrate File Servers," later in this chapter.

TIP *For detailed instructions on how to configure roaming profiles with folder redirection in the new VSO domain and use this strategy to migrate user data from the old to the new network, read Chapter 8 of* The Definitive Guide to Vista Migration *at www.realtime-nexus.com/dgvm.htm.*

Migrate Network Infrastructure Servers

Network infrastructure servers do not really require a migration. This category includes services such as DHCP, WINS, WDS, and Windows Server Update Services (WSUS).

It is possible to migrate the databases from previous versions of Windows Server running services such as DHCP and WINS if you have decided to use WINS in the new network. If you are completely happy with your existing DHCP service, you can simply move the DHCP database from the source server to new virtual servers running in the VSO network.

TIP *We strongly recommend that you move to DNS GlobalNames zones instead of using WINS, if it is at all possible in your network. These zones are simpler to work with and profit from all of the powerful features of DNS instead of relying on a legacy service such as WINS.*

However, you must keep in mind that there are several changes to DHCP in Windows Server 2008, changes that may not warrant the migration of your existing database. For example:

- Windows Server 2008 supports DHCPv6, which will work with IPv6 addresses. Your previous DHCP servers will not have this ability, and you will need to re-create the DHCP scopes for this data.
- Windows Server 2008 also changes the nature of the local scope because you need to assign DNS servers to each local scope that also includes a domain controller. DNS is now hosted on each domain controller; therefore, remote site users will rely on their local domain controller for DNS name resolution. Each recovered local scope will need to be updated with this information.
- You may want to update your scopes and begin using new features, such as superscopes, to make scope management simpler.

For these reasons, it may be easier to simply create new scopes in your new VSO network. But if you decide to recover existing scopes, you need to use the following procedure. Remember to rely on the 80-20 rule on your new servers.

1. Export the DHCP server configuration from the source servers.
2. Create an export file for each scope.
3. Import the scopes on the target server(s).
4. Disable the scopes on the source server.
5. Enable the scopes on the new servers.

Then you'll want to modify scopes to meet new requirements generated by the new VSO network.

Other content you can migrate in the network infrastructure server category is the images you use in Windows Deployment Services. Simply create new WDS servers, secure them appropriately, and then copy the images from the old servers to the new servers.

Finally, when it comes to Windows Server Update Services, the only thing you really need to recover is the list of approved updates. WSUS will automatically scan all PCs and servers to determine which updates have been applied to them, so recovering the inventory isn't really required. The best way to effect this migration is to simply install a new version of WSUS in the new VSO network, scan all systems, and make sure you've captured the approved list of updates from the legacy network.

Migrate Web Sites

Microsoft has also made it easier to migrate web sites from previous versions of Internet Information Services (IIS) to IIS version 7. The IIS Migration Tool is a command-line tool that will capture web site information and transfer it to an IIS 7 Web structure. This tool

transfers configuration data, web site content, and application settings to the new server. It can also move only application settings if that is all you need.

This tool will also let you migrate web sites while they are in operation, letting you maintain 24/7 availability of the site as you perform the migration. Configuration data is translated from the metabase format used in previous versions to the new `.CONFIG` file format used in IIS 7. It will also migrate nested applications correctly, letting you migrate even complex web site structures. You can also perform site customizations, such as changing the IP address, port, or host headers of the sites you migrate as you migrate them.

Migrating web sites can be a complex operation, however. Make sure you fully test the web site once you have migrated it to guarantee that all of its functions operate properly on your new Web server infrastructure.

TIP *The IIS Migration Tool can be found at www.microsoft.com/downloads/details.aspx?FamilyID=2aefc3e4-ce97-4f25-ace6-127f933a6cd2&displaylang=en.*

Build Terminal Services Servers

Terminal Services servers do not really require migration, since they host applications that are run on a central platform. Most of the TS servers you will run in your new network, if you choose to run them and not replace them with desktop application virtualization, will be new server installations. They will, however, make it possible for users in both the legacy and the new VSO network to use the applications made available through Terminal Services, because client systems only need to have the updated Remote Desktop Connection client. This client is downloaded automatically to any Windows XP system that relies on software updates from Microsoft. It is also already installed on Windows Vista systems.

Perhaps the best way to make new TS applications available to users, whether they are migrated or not, is through the use of TS Web Access. This lets you place the remote application shortcuts on a web page—something everyone has access to—and provide them with immediate access to applications running on your new Windows Server 2008 infrastructure.

Because of this, you might consider moving these applications as soon as possible. Remember that you will need the cross-domain trusts in place to let users have logon access to the new network from the legacy network.

Migrate File Servers

By their very nature, Windows networks tend to be highly distributed. Somewhere, the industry got the feeling that if you needed more services from Windows, it was easier to simply add a new box to the network than to try to get multiple services to cohabitate on the same server. Well, Microsoft has gone a long way to help dispel this myth, not only by providing valuable information on how servers should scale up, but also by making Windows code faster and more robust. Today, Windows Server 2008 can easily run several thousand printers on one machine or store terabytes of information in a single cluster. That's why many organizations seriously consider server consolidation when it comes to the migration of both file and print services. Not to mention that the more boxes you have, the more complex they are to manage and, particularly, to patch.

The migration of distributed storage in legacy networks to a new disk and shared folder structure must support several activities (see Table 12-1). For example, it must automatically

File Server Migration Activity	Tool Requirements
File migration	Must be supported
Consolidation support	Migrate from many to one
Source operating systems	Any previous version of Windows Server
Target operating systems	Windows Server 2008
File usage analysis before migration	Evaluate different situations, such as duplicate files or unused files
File Re-ACL-ing	Change SID ownership of the files
Password-protected file support	Must support migration of files locked through tools such as Microsoft Office
Encrypting File System support	Required for secure environments
Map to DFS systems	Required to provide consolidation support
Parallel file server support	Provide access to both source and target servers through synchronization
User/PC setting migration	Modify settings on the local PC to remap file shares
Undo capability	Provide a back-out plan in case of failures
Delegation of migration task	Delegate task to other operators
Migration reporting	Report on analysis and task progression
Migration testing	Test a migration only before performing it
Database support	Store information in a database
Scripting or command-line support	Automate procedures

Table 12-1 File Server Migration Activities and Requirements

reassign proper security rights within the target network so that users can continue to access their data. Ideally, the file migration tool you use will either support parallel access to both the source and target servers until the migration is complete or provide a cut-off method to warn users that their files have been migrated. It should also support the verification and modification of access control lists (ACLs) in the target network to remove legacy permissions to the files. In the case of a migration, this means the tool will support SID history, since user accounts acquire new SIDs when moved from a legacy domain to a new directory. Once files are moved and permissions are updated, the migration tool must support the modification of user settings on local PCs. If at all possible, it will perform this task automatically or with little administrative effort. This migration tool must also support special file formats, such as files that include password protection, or, if migrating from more modern networks, files that have been protected with the Encrypting File System (EFS).

In the best migration scenarios, the tool you use should also support the migration of content from a standard file share system to a consolidated DFS system, since DFS has been designed to eliminate the need for mapped drives. Finally, it should help you move from outdated home directories to the more advanced folder redirection supported by Windows Server.

TIP *In the worst-case scenario, you can use NT Backup to back up the file services from your legacy servers and restore them to your new server, then use Microsoft's Security Migration Editor, which is free with Windows Server 2008, to perform SID regeneration on your files. Remember that NT Backup is not available on WS08 and must be downloaded (see Chapter 11).*

Change the Nature of Your File Servers

As mentioned earlier, the role of the file server is changing as organizations move toward better and more efficient collaboration tools. As such, you might find that it is much more practical for you to create SharePoint sites to host shared documents and other data rather than re-creating a very large number of file shares, as you had in your legacy network. If you decide to move to this model, you will not be migrating files from legacy file shares to new file servers, but rather, you will be moving files from legacy file shares to new SharePoint sites that are designed to host more comprehensive collaboration.

There is still room for the file server, however. Users have their own document space on their desktops—a document space that needs protection just as much as centralized file shares. This document space is stored in the user profile. Chapter 7 discussed the use of folder redirection, possibly linked to roaming profiles, to provide a more thorough protection policy for end-user data, as well as providing a better strategy for long-term profile management.

You may, therefore, find that the actual file server migrations you perform are focused more on user and perhaps administrative data than on shared data. If this is the case, then focus on the migration of data to Windows SharePoint Services instead of on file servers.

NOTE *Make sure you communicate the data protection policy to your users. In fact, it might be an excellent idea to use a WSS team site to provide an online users' manual to all end users. This way, they will know exactly what is going on in their new network.*

In fact, the migrations you perform should be mapped out to the new file services you deploy. Chapter 8 outlined how your file services should be structured (see Figure 12-10). These are the shared folders you need to focus on. Table 12-2 outlines how each type of file service should be migrated.

TIP *For instructions on how to create manual DFS shares for file migration, look up Knowledge Base article number 829885 at http://support.microsoft.com/default.aspx?scid=kb%3b%5bLN%5d%3b829885. Microsoft also offers a Solution Accelerator for the consolidation of file and print servers. Solution Accelerators are a set of documentation and tools to provide simpler operation of complex tasks. It can be found at http://go.microsoft.com/fwlink/?linkid=24719&clcid=0x409.*

You'll rarely have the occasion to migrate data when it isn't in use, unless you perform the migration during weekends or during times when your servers are shut down. Even then, it is difficult to find enough time to perform the migration. Most likely, you will be migrating data when users are online and need access to it. This is why running source file servers and target systems in parallel is the ideal situation. Make sure you communicate your plans to end users to limit the number of Help desk calls the migration may generate. If users are left with tasks to perform, then make sure these tasks are clearly outlined and detailed for them in your communications to them.

The first step in any file server migration is to run reports on your existing file shares, but unless you are running Windows Server 2003 R2 on the source servers, you won't have any

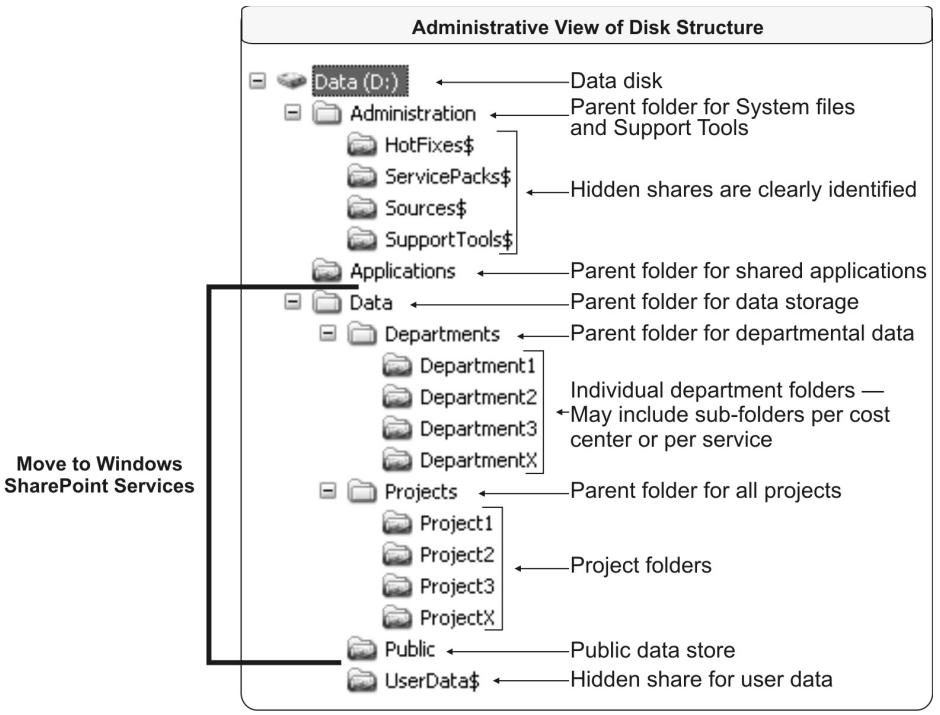

FIGURE 12-10 Mapping file server migrations to disk structures

built-in tools to create these reports. You'll have to manually check files as you migrate them. You can, however, migrate the files and once they are migrated, generate usage reports on the new servers through the File Server Resource Management Reporting feature.

TIP *You can generate reports with third-party file migration tools, or you can get a free or commercial inspection tool. For example, AdvexSoft offers both a free and a paid version of Disk Space Inspector at www.advexsoft.com/disk_space_inspector/disk_space_report.html?gclid=CMPVyoPnxY0CFRAkggod9BlfMQ.*

Once you have an idea of the space requirements—remember that it is always wiser to have more available space on your new servers than on the old ones—you can move to the migration of each file share service to its target technology.

NOTE *In previous versions of Windows Server, Microsoft provided the File Server Migration Toolkit. Unfortunately, this toolkit does not work on Windows Server 2008 and Microsoft has not seen fit to upgrade it for this version of the OS. This leaves you out in the cold as far as free migration tools are concerned. Rely on the migration paths outlined in Table 12-2 to simplify the process. It is unlikely, though, that medium to large organizations will be able to perform this operation without the purchase of migration tools. There are several very good tools on the market. We have worked with the tools from Quest and Metalogix, among others. These tools provide comprehensive features at reasonable cost.*

File Share	Migration Target	Comments
Administrative shares	Hidden shared folders	Move all data from legacy network to new VSO network. A simple copy should do, since there are no special permissions to migrate.
Application shares	File shares with same access rights or RemoteApps	Application shares are simple to migrate, since they rarely have custom permissions. If you choose to migrate them to new file shares, just copy the data and re-create the access control lists. If you choose to migrate them to RemoteApps, then apply new permissions.
Departmental shares, project shares, and public shares	Windows SharePoint Services	To migrate contents from a legacy share to WSS, you can use Windows Explorer to move the data from one location to another. But if you want to automate the process and apply complex access control lists, use a commercial migration tool. See the Migrate SharePoint Sites section in this chapter for more details.
User data	File shares with same access rights	The best way to migrate user data is to perform the migration through a combination of roaming profiles and folder redirection. Using this combination, you can move 100 percent of all user data through an automated process. See the Note in the "Transfer Networked User Data" section of this chapter for instructions on how to perform this operation.

TABLE 12-2 Mapping File Server Migrations

Migrate Print Servers

For printer migration, you must be able to migrate print queues, including printer drivers from one server to another, as well as redirect print queues on client computers. Since Windows Server prefers the use of user-mode drivers over kernel-mode drivers for increased server stability, your migration should convert the driver and block the installation of kernel-mode drivers. You should endeavor to remove any legacy printers requiring kernel-mode drivers from your network, since these can block and hang a print server, even a clustered print server. Finally, you need to publish printers in Active Directory Domain Services and implement Printer Location Tracking to facilitate printer searches in the directory. You will also have to change printer settings on user systems. This can be done either with the Printer Settings GPO or through logon scripts. If you use Printer Location Tracking, you might even be able to get users to change printers themselves.

You can use Microsoft's Print Migrator 3.1 to capture printer information from legacy servers and restore it to new Windows Server 2008 machines. What's nice about this tool is that it will automatically change Line Printer Remote (LPR) ports to the new Transmission Control Protocol/Internet Protocol (TCP/IP) standard port supported by Windows Server. In addition, it will automatically change printer drivers from kernel mode (version 2) to

user mode (version 3) during the transfer. At the very least, you should use this tool to back up all your printer configurations, as it is one of its main functions. This way, you can restore them in the case of an emergency.

TIP *Microsoft Print Migrator can be found at www.microsoft.com/WindowsServer2003/techinfo/overview/printmigrator3.1.mspx.*

Print Migrator is easy to work with. Download the executable, and load it on any server. It doesn't actually require an installation, since the executable is self-contained. Use the following approach:

1. Double-click `PRINTMIG.EXE` to run the Print Migrator.
2. Accept the Run prompt that is presented.
3. Print Migrator automatically lists the printer configuration on the local system (see Figure 12-11).

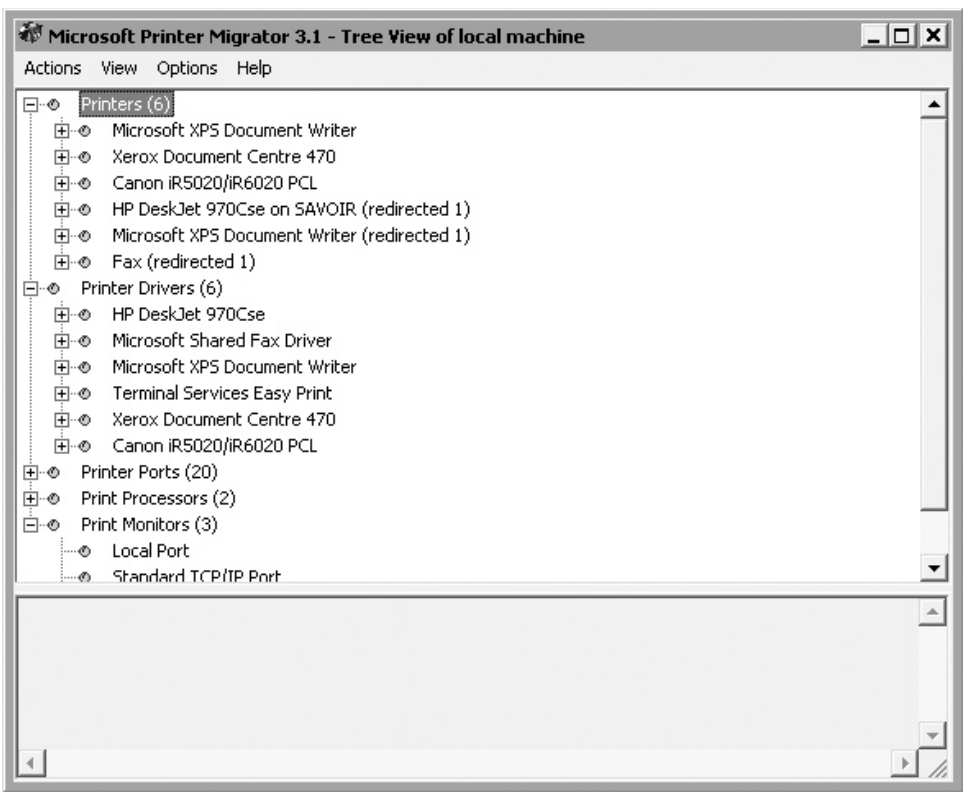

FIGURE 12-11 Using the Print Migrator

4. If you are running the tool on the source print server, move to the Actions menu, and select Backup. Identify the location where you want to save the CAB file—ideally a shared folder—and, optionally, identify the target server for the operation.
5. Click Save and then click OK to perform the backup.

To restore the settings on the target print server, repeat the operation with the Action | Restore command. Here you can select two options:

- Suppress warning popups. These will be captured into the log file even if they are not displayed to you as you run the restore.
- Attempt LPR to SPM conversion. If your old printers used LPR ports, try to convert them to Standard TCP/IP Port Monitor (SPM) for better performance.

Print Migrator can also connect to remote servers and capture their printer settings. Use the View | Target menu item to connect to remote servers.

Finally, printer migration can be automated, since the `PRINTMIG.EXE` program also runs from the command line. Use the following command to identify its options:

```
printmig /?
```

Repeat the operation for every print server in your legacy network. You can actually perform print migration at any time during the migration, since printers in legacy and new networks can run in parallel with no issues.

Migrate SharePoint Sites

Windows SharePoint Services is becoming more and more popular as Microsoft matures the collaboration engine it relies on. Many organizations will already have implemented SharePoint sites in one form or another. For the organizations already using SharePoint systems, the migration path is from one SharePoint system to another. For those who haven't implemented SharePoint systems yet but want to take advantage of this new collaboration paradigm, the migration will most likely be in the form of moving content from file shares to new SharePoint sites.

There are several ways to perform these migrations:

- Migrating an existing site could be as simple as performing a backup on one server and restoring the data on another.
- You can also upgrade database content from older versions of SharePoint to Windows SharePoint Services (WSS) version 3.
- Finally, you can move content from other repositories, such as file shares, to new SharePoint sites.

The tricky part of a migration for SharePoint sites is the back-end database. All SharePoint data is stored in a database. In addition, SharePoint can be run in two modes: stand-alone and server farm. If you run an older version of SharePoint in stand-alone mode, then you are running it with the Windows Microsoft SQL Server Desktop Engine (WMSDE). If you are running a farm, then you are running SQL Server.

If you are migrating from an older stand-alone version, then you will also be moving from WMSDE to the Windows Internal Database (WID). If you are migrating a farm, then it should be simpler, because you will be moving from SQL Server to SQL Server. These latter migrations are often best performed through commercial tools.

TIP *More information on Windows SharePoint Services can be found at the WSS TechCenter at www.microsoft.com/technet/windowsserver/sharepoint/default.mspx.*

Migrate from SharePoint to SharePoint

When you're migrating from SharePoint to SharePoint, you must first run the pre-upgrade scan tool (PUST). PUST will scan your existing site and map out potential upgrade or migration issues, including:

- **Customized content** PUST will scan your sites for any customized content, such as Web parts or site templates, and determine if they can be carried over in the upgrade.
- **Site components** PUST will identify if required components of the site to be migrated are missing from the target site.
- **Orphaned objects** Sites can sometimes have objects that have become orphaned and are no longer linked to the site. PUST will identify these objects and list them for you.

Once it has performed its scan, PUST will provide you with upgrade or migration recommendations and help you determine which migration approach to use.

TIP *Orphaned objects can be recovered before the migration. See Knowledge Base article number 918744 for more information at http://go.microsoft.com/fwlink/?linkid=69958&clcid=0x409.*

Once you have results from PUST, you can move to the migration itself. If you're moving from any version of SharePoint to stand-alone installations of WSS on WS08, then you must perform a WMSDE-to-WID migration since WID is only available on WS08. Basically, you need to perform the following steps:

1. Detach the databases from the WMSDE instance.
2. Copy the databases and attach them to SQL Server (WID).
3. Add the databases to the Web applications, re-creating sites.
4. Review the log files for any issues.

Repeat the operation for each database you need to migrate.

NOTE *Detailed steps for this operation can be found at http://technet2.microsoft.com/windowsserver/WSS/en/library/1f505e96-60e2-41ac-bf5d-9739105f047c1033.mspx?mfr=true.*

Migrate File Content to SharePoint Services

Migrating file content is simpler than migrating SharePoint sites. At its simplest, you can use Windows Explorer to open both the source file share and the target SharePoint site and drag-and-drop the files from one to the other. The problem with this approach is that the

files will not include any metadata content, unless, of course, your users are disciplined and have already added it through the Microsoft Office interface.

The best way to migrate content from a file share to a SharePoint site is through a commercial migration tool. For example, Metalogix (www.metalogix.net) offers FileShare Migration Manager for SharePoint, which migrates any file share content to SharePoint. This product is reasonably priced (as are all Metalogix products) and works through a simple interface. In addition, it lets you analyze content prior to the migration, group content for migrations, and then, once you've begun the migration, you can tag metadata to each file as it is uploaded.

Tagging metadata is important in order to support better content searches when users are looking for information in SharePoint.

NOTE *Metalogix also makes tools to migrate content from Microsoft Content Management Server or other SharePoint Sites to WSS version 3. Check them out, as they provide a much better migration experience than the upgrade process described earlier.*

Decommission the Legacy Network

Once everything has been migrated from the legacy network to the new network, you can proceed with the decommissioning of the legacy network. This process involves the following tasks:

- Begin by removing embedded groups. You only need to do this in the new domain. Remove legacy global groups from your production domain local groups as well as from member server local groups.
- Next, turn off SID history. *You must make sure you have performed Security Translation with the ADMT beforehand!* SID history removal is discussed later in the chapter.
- Next, remove the trust relationships. Once again, you only need to remove trusts from the new production domain. Use the Active Directory Domains and Trusts console to perform this activity.
- Now you can move on to the decommissioning of the legacy domain itself. But before you do so, it is a good idea to perform full backups of the primary domain controller (PDC)—if it is a Windows NT network—or the DCs running Operations Master Roles—if it is Windows 2000 or 2003.
- When the backups are complete, store them in a safe place, then shut down the legacy domain's final domain controller (PDC or main DC).
- If you can recover this server as a new host, you can install Server Core or, if it is a 32-bit server, the Full Installation and join it to your new resource pool domain.

You might consider having a celebration at this stage, because you certainly deserve it! You and your migration team have done a lot of hard work preparing the new network and migrating every legacy resource to the new environment. Congratulations!

But, celebrations aside, it will also be a good idea for you to perform a post-migration review to ensure that you can reuse this process and improve upon it if you ever need it again.

Deactivate SID History

SID history is both a boon and a bane. It is a boon because it automatically provides additional SIDs when a user tries to access a resource from a legacy source. It is a bane because savvy malicious users can add additional SIDS to their own and use them to impersonate credentials they shouldn't have. Therefore, it is important to make sure you remove SID history and deactivate it as soon as you can after the migration and especially after security translation operations have been completed.

TIP *More information on SID history can be found at http://technet2.microsoft.com/windowsserver/en/library/01e5cf71-b317-4967-82a2-75b7b632b7461033.mspx?mfr=true.*

To deactivate SID history, use the following command with enterprise administrator credentials:

```
netdom trust TargetDomain /domain:SourceDomain /quarantine:No
/usero:UserName /password:Password
```

where *TargetDomain* is your new domain, *SourceDomain* is the legacy domain, and *UserName* and *Password* are the enterprise administrator credentials you are using.

CAUTION *Be careful when you perform this operation, as the password appears in plain text on the screen!*

Prepare Your New Support Structure

As you place the new network online, you will begin to realize that a review of administrative and operational roles is also required. In fact, this review of operational roles focuses on the third quadrant of the services lifecycle illustrated in Chapter 3—Production—since the activities of the first two quadrants are now complete (Planning and Preparation and Deployment). The operations outlined in the production quadrant require an updated organizational structure because many of them will be delegated to users with non-administrative privileges.

New and Revised ADDS IT Roles (VSO Network)

One of the areas where IT roles are modified the most is in terms of Active Directory Domain Services management, especially in the new VSO network. If you're migrating from Windows NT to Windows Server 2008, most of these roles are new. If you're already using Windows 2000 or 2003, then you now know that all of these roles are necessary (see Figure 12-12). The responsibilities of each role are outlined in Table 12-3. Once again, depending on the size of your organization, you may combine roles. What is important here is that each function be identified within your IT group. It will also be important to ensure that no unnecessary privileges are given to administrators and operators within ADDS.

All of these roles will need to interact with each other during ongoing operations. A regular roundtable discussion is an excellent way for each of the people filling these roles to get to know each other and begin the communication process. The frequency of these meetings does not need to be especially high. Gauge the number of meetings you need per year according to the objectives you set for your directory. There could be as few as two

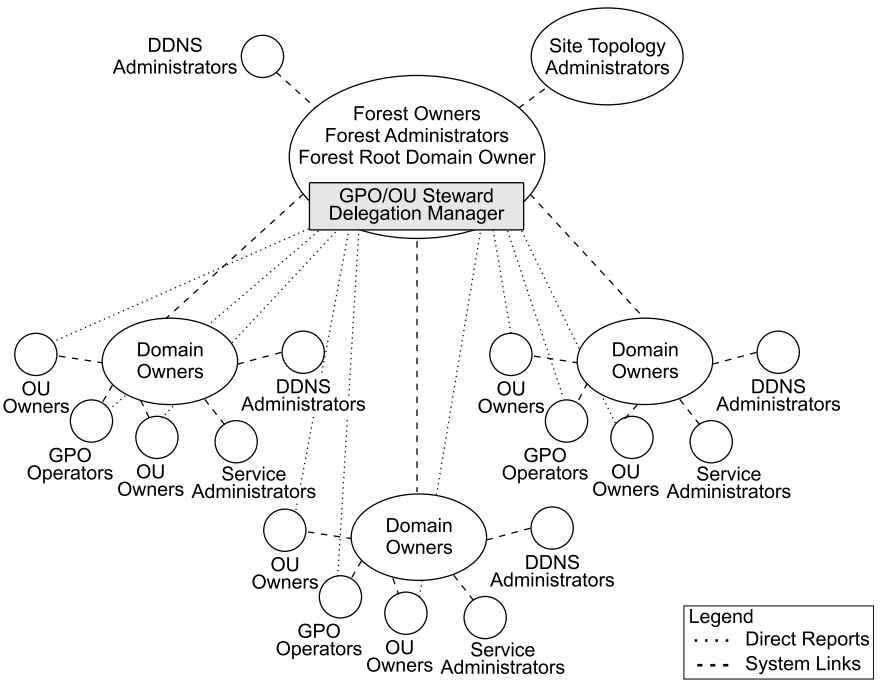

Figure 12-12 ADDS IT role relationships

meetings per year. Depending on the size of your organization, you might restructure your IT group to meet new demands (see Figure 12-13). Also, a shared team site within WSS is a great way to centrally store and protect data about system administration.

Tip *Microsoft offers a complete Active Directory Operations Guide. It is in two parts and is available at http://technet2.microsoft.com/windowsserver/en/library/9c6e4dd4-3877-4100-a8e2-5c60c5e19bb01033.mspx?mfr=true. It also outlines which role should perform which operation.*

New Resource Pool Roles

Since the network is now divided into two portions—resource pools and virtual service offerings—you will need a similar division in your IT roles. At the simplest, your resource pool administration team will consist of at least two people who focus only on resource pool management and administration, allocating appropriate resources on an as-needed basis. In more complex environments, the resource pool team will be divided into roles listed in Table 12-4.

Basically, the resource pool administration team is responsible for all hardware resources and their allocation to provide support for the virtual service offerings. This team is a high-powered team that focuses on Server Core and hardware-level operations. Because of this, they never interact with end users. Instead, they interact with either the Level 3 Help desk technicians from the VSO team or even VSO administrators (see Figure 12-14). It is the VSO Help desk, Levels 1 and 2, that interact with end users, since it is only the VSOs that interact with end users.

Role	Department	Role Type	Responsibilities
Forest Owner	IT Planning and Enterprise Architecture	Service Management	Ensure that all forest standards are maintained within the forest. Responsible for the forest schema. Identify and document new standards.
Forest Administrator	IT Group	Service Management	Ensure that the forest is operating properly. Responsible for the forest configuration. Enforce all forest standards. Responsible for forest root domain administration. Responsible for forest-wide Operation Master roles. Responsible for root domain-centric Operation Master roles. Responsible for the analysis/recommendation of the implementation of operational software that modifies the schema. Responsible for Global Catalog content.
Domain Owner	IT Group/ Training/IS	Service Management	Ensure that all domain standards are maintained within the domain. Identify and document new standards.
Domain Administrator	IT Group	Service Management	Service administrator ensures that the domain is operating properly. Enforce all domain standards. Ensure that all DCs within the domain are sized appropriately. Responsible for domain-centric Operation Master roles.
DDNS Administrator	IT Group	Service Management	Ensure the proper operation of the forest namespace. Administer and manage internal/external DNS exchanges.
Site Topology Administrator	IT Group	Service Management	Monitor and analyze forest replication. Modify site topology to improve forest replication.
Service Administrators	IT Group	Service Management	Responsible for a given service in the domain. Have limited rights in the domain (only to the service they manage).
GPO Operators	IT Group	Service Management	Design and test GPOs for use in production environments. Use the Group Policy Management Console to manage, debug, and modify GPOs. Report to the GPO/OU steward.
Root Domain Owner	IT Planning and Enterprise Architecture	Data Ownership	Responsible for universal administrative groups. Placeholder for the entire forest. Can be the same as the forest owner.

TABLE 12-3 ADDS IT Roles

Role	Department	Role Type	Responsibilities
GPO/OU Steward	IT Planning and Enterprise Architecture	Data Ownership	Responsible for the proper operation of all OUs within the production forest. Must ensure that all OUs are justified and that each has a designated owner. Must maintain the GPO registry (all GPO documentation). Must ensure that all GPOs conform to standards. Must manage the GPO production release process.
OU Owners	Entire Organization	Data Ownership	Responsible for all information delegated within the OU. Must report regularly to the GPO/OU steward.

TABLE 12-3 ADDS IT Roles (*continued*)

Design the Services Administration Plan

The management and administration of Active Directory Domain Services, especially a network operating system (NOS)-centric ADDS, is concentrated mostly on the delegation of specific administrative rights to both service operators and security officers. Chapter 7 identified the requirement for local or regional security officers. If you have decided to delegate specific IT operations related to both the management of PCs and the management of users, you will need to proceed with the delegation of appropriate rights to these officers, as outlined in Chapter 7. In terms of user management especially, you will also need to proceed with the identification of your group managers and give them appropriate rights for the management of their user groups, which was also outlined in Chapter 7.

NOTE *The procedures for creating custom Microsoft Management Console (MMC) consoles and delegating rights, as well as that for creating appropriate administrative groups, are outlined in Chapter 7.*

Finally, you will need to proceed with service management delegation, as outlined in Chapters 8 and 9. Service management activities must be closely related to the Virtual Service Offerings OU structure you designed during the preparation of the parallel VSO network's services. It is also closely tied to the seven core server roles identified in Chapter 3, but additional operations are also required, as you well know—system backup, performance monitoring, security management, problem management, user support, and so on. The core roles to cover here include:

- File and print operators
- Application server operators
- Terminal server operators
- Collaboration server operators
- Infrastructure server operators
- Dedicated Web server operators

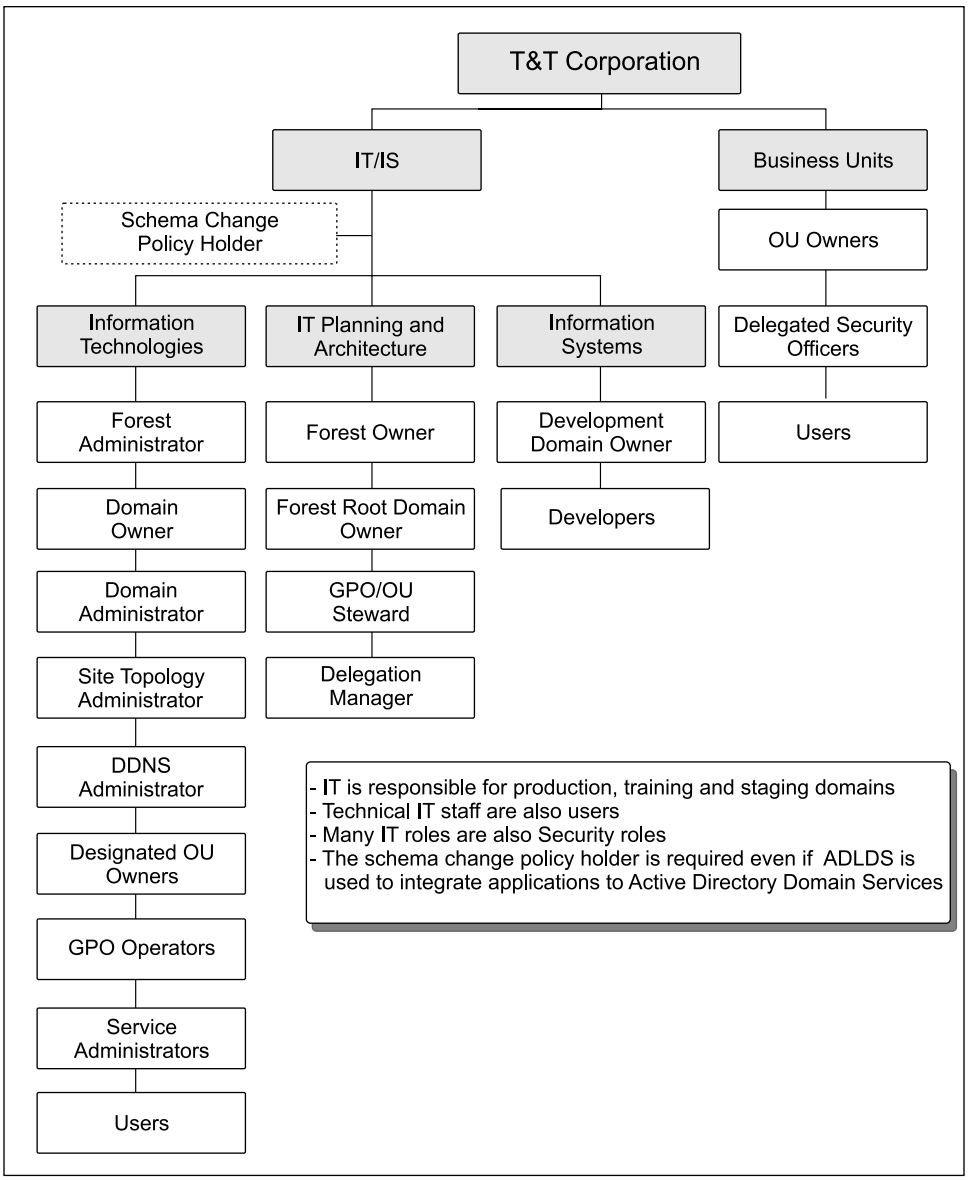

Figure 12-13 The organizational structure of ADDS IT roles at T&T Corporation (VSO network only)

These six operator groups require appropriate rights and delegation of the appropriate OUs. As with the Virtual Service Offerings OU structure, these operational groups may be subdivided into smaller, more focused groups that are responsible for specific technologies. Another role, identity management server operator, is your domain administrator and has already been identified earlier.

Role	Department	Role Type	Responsibilities
Forest Owner and Root Domain Owner	IT Planning and Enterprise Architecture	Service Management	Ensure that all forest standards are maintained within the forest. Responsible for the forest schema. Identify and document new standards. Responsible for universal administrative groups. Operational domain for the entire forest. May be divided roles for the resource pool and VSOs.
Forest Administrator	IT Group	Service Management	Ensure that the forest is operating properly. Responsible for the forest configuration. Enforce all forest standards. Responsible for forest root domain administration. Responsible for forest-wide Operation Master roles. Responsible for root domain-centric Operation Master roles. Responsible for the analysis/recommendation of the implementation of operational software that modifies the schema. Responsible for Global Catalog content. May be divided roles for the resource pool and VSOs.
DDNS Administrator	IT Group	Service Management	Ensure the proper operation of the forest namespace. Administer and manage internal DNS exchanges. Can also manage all resource-pool IP address allocations. May be divided roles for the resource pool and VSOs.
Site Topology Administrator	IT Group	Service Management	Monitor and analyze forest replication. Modify site topology to improve forest replication. Can also manage routing-level IP structure. May be divided roles for the resource pool and VSOs.
Virtual Service Administrators	IT Group	Service Management	Responsible for the virtualization service in the resource pool. Construct and deploy new virtual machines (or guest partitions). May be divided roles for the resource pool and VSOs.
GPO Operators	IT Group	Service Management	Design and test GPOs for use in production environments. Use the Group Policy Management Console to manage, debug, and modify GPOs. Report to the GPO/OU steward.
Resource Pool Administrator	IT Group	Service Management	Responsible for all hardware allocations. Responsible for all hardware staging. Build and run management virtual machines (or parent partitions). Can be the same as the Virtual Service Administrators.

TABLE 12-4 Resource Pool Administration Roles

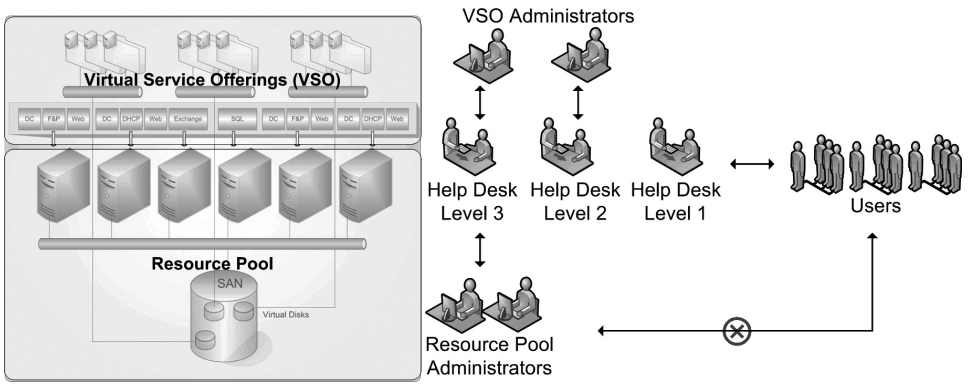

Figure 12-14 The interactions of resource pool administrators, Help desk technicians, virtual service administrators, and end users

Several of the management and administrative activities you need to cover will require special technologies. You need a tool to support application deployment, inventories, and software usage habit analysis. Another tool should support performance and alert management within the network, especially with critical services. But if you have a legacy network, you are most likely already using technologies of this type.

Rely on the WS08 Remote Server Administration Tools

Windows Server 2008 includes a whole series of new and improved management and administration tools. Several are located directly within the operating system and consist of command-line tools. WS08 includes several new command-line tools and over 200 command-line tools in general. In addition, Windows Server 2008 includes an integrated version of PowerShell, the most powerful scripting engine Microsoft has ever released. Both command-line tools and PowerShell are well documented in the WS08 Help Center. In addition, just like previous versions of Windows, WS08 includes the Remote Server Administration Tools (RSAT). These are useful to your administration team.

Chapter 3 outlined the importance of standard operating procedures (SOPs). In many cases, the best SOP is a script or command file because it ensures that the operation is always performed in the same manner. And since technical personnel often prefer not to write documentation, but to create automations and programs, the use of well-documented scripts (documented within the script itself) and a complete script inventory makes it easier to implement an SOP approach.

Tip *Microsoft provides excellent PowerShell scripting support in the TechNet Script Center at www.microsoft.com/technet/scriptcenter/hubs/msh.mspx.*

You should be careful who you give access to the RSAT. They are powerful tools that can cause a security risk if misused. One of the best ways to control their access is to store them on servers only and to use Terminal Services RemoteApps to give access to particular tools. An additional advantage of this approach is that you do not need to create and maintain administrative or operational workstations for your IT staff. Their workstations

can be similar to other power users within your enterprise and focus on productivity tools. Then, when they need to perform an administrative task, they can launch the RemoteApps they need to access the appropriate tool.

This can also help increase security. Since the administrative tools are not on the operators' PCs, they can use their *user* account to perform their daily tasks. Then, when an administrative task is required, they can log in with their *administrative* account in the Terminal Services RemoteApps session. An additional layer of security can be added through the use of smart cards for administrative logons. Since WS08 supports the use of smart cards for administrators, you can ensure that two-factor authentication is required for the performance of all administrative tasks.

TIP *A good reference for administrators of Windows Server 2008 is the Windows Server 2008 Tech Center on Microsoft TechNet at http://technet.microsoft.com/en-us/windowsserver/default.aspx.*

Administration Tools for Resource Pools

As a resource pool administrator, you will be working extensively with the command line, since you will work mostly with Server Core. They will also be using some graphical tools through the use of management virtual machines—machines that are part of the resource pool domain but use the full installation in a virtual instance. This lets you use a graphical interface to manage the Server Core machines that make up your resource pool.

You might also obtain and work with System Center Virtual Machine Manager (SCVMM) because it is completely designed to work with and manage virtual machines, whether they run on Windows Server Hyper-V or through Microsoft Virtual Server. If you end up having a mix of hardware resources—both 32- and 64-bit—because you want to recover existing investments in hardware, SCVMM might just be the best tool to use.

TIP *More information on System Center Virtual Machine Manager can be found at www.microsoft.com/systemcenter/scvmm/default.mspx.*

Resource pool administrators may find themselves working with several additional tools, as listed in Table 12-5.

Administration Tools for Virtual Service Offerings

Like resource pool administrators, if you are a virtual service offerings administrator, you will be working extensively with Windows Server 2008. However, you will have the major advantage of having access to both PowerShell and the Server Manager graphical interface. This will give you a much more powerful management platform, since much more can be done with these tools than with the command line.

VSO administrators may find themselves working with several additional tools, as listed in Table 12-6.

Build a New Approach to Administration

Twenty years ago, when most computers were mainframes or minicomputers, operators and administrators had scheduled, specific tasks they needed to perform on an on-going basis. Each time a task was performed, they had to make note of the time and write their initials in a logbook to demonstrate when the task was performed and by whom.

Role/Feature	Tool	Command-Line
ADCS	Certificate Authority snap-in Certificates snap-in Certificate Templates snap-in Online Responder snap-in PKIView	CertUtil.exe CertReq.exe CertSrv.exe
ADDS	Server Manager	Active Directory Users and Computers Server Manager	Active Directory Sites and Services Active Directory Domains and Trusts	CSVDE Dsadd Dsmod Dsrm Dsmove Dsquery Dsget LDIFDE Ntdsutil
DNS Server	Server Manager	DNS Server	Nslookup
DHCP Server	Server Manager	DHCP Console	Netsh
File Services	Server Manager	DFS Management File Server Resource Manager Server Manager	Storage Reports Mgmt	Netstart, netstop (Macintosh) Dfsradmin.exe Dfsrdiag.exe Dirquota.exe FileScrn.exe StorRept.exe
PowerShell	PowerShell Interface on full installation or administrative workstation	No command
Print Services	Server Manager	Print Services Print MMC	Netstart, netstop (Macintosh) Lpg Lpr Print Prncnfg.vbs Prndrvr.vbs Prnjobs.vbs Prnport.vbs Prnqctl.vbs
Server Core	Local command-line Remote Custom MMC WS-Management and Windows Remote Shell (WinRS) Remote Desktop Remote PowerShell WMI Command (WMIC)	
Terminal Services	Server Manager	Terminal Services Terminal Services Manager Terminal Services Configuration Remote Desktops Console	Tsadmin.exe Tscc.msc Eventvwr.msc quser
Windows Server Hyper-V	Hyper-V Manager	

TABLE 12-5 Additional Administration Tools for Resource Pool Administrators

Role/Feature	Tool
ADCS	Certificate Authority
ADDS	Server Manager	Active Directory Users and Computers Server Manager	Active Directory Sites and Services Active Directory Domains and Trusts
ADFS	IIS Manager Active Directory Federation Services
ADLDS	Server Manager	Active Directory Users and Computers Server Manager	Active Directory Sites and Services Active Directory Domains and Trusts ADSI Edit Ldp.exe Schema management utilities
ADRMS	ADRMS MMC
Application Server	Server Manager	Component Services
DNS Server	Server Manager	DNS Server
DHCP Server	Server Manager	DHCP Console
Fax Server	Fax Service Manager
File Services	Server Manager	DFS Management File Server Resource Manager Server Manager	Quota Management Server Manager	File Screening Management Server Manager	Storage Reports Management
Network Access Protection	NPS MMC HRA MMC NPA Client Management MMC Routing and Remote Access MMC Wireless Network Policies Wired Network Policies
PowerShell	PowerShell Interface
Print Services	Server Manager	Print Services Print MMC
Terminal Services	Terminal Services Manager Server Manager	TS RemoteApp Manager Server Manager	TS Gateway Manager Terminal Services Configuration Terminal Licensing Manager Remote Desktops Terminal Web Access Administration

Table 12-6 Additional Administration Tools for VSO Administrators

Role/Feature	Tool
Web Server (IIS)	IIS 6.0 Manager IIS Manager
Windows Deployment Services	WDS Manager
Windows Server	Local command line WS-Management and Windows Remote Shell (WinRS) Remote Desktop PowerShell Server Manager WMI Command (WMIC)
Windows SharePoint Services	SharePoint 3.0 Central Administration SharePoint Products and Technologies Configuration Wizard

TABLE 12-6 Additional Administration Tools for VSO Administrators (*continued*)

Today, networks are made up of loosely coupled collections of servers and workstations that may or may not include either mainframes or minicomputers. Network or systems administration has become much more complex and covers many more tasks than in those days, but somehow, we've lost something in the transition. Today, most administrators don't keep logbooks any more. Most don't have fixed schedules for administrative activities. Many don't even perform the most basic administrative tasks.

We think it is time to go back to structured systems management. This is why Chapter 13 will provide an extensive list of administrative tasks and their scheduled occurrence based on our past experience. This chapter strives to be different by going straight to the heart of the matter. Each task outlined in the chapter is focused on the task itself. It does not usually include any extensive background information, because it assumes that when you need to perform the task, you do not need an explanation of how something works, but rather an explanation of how to do something because you're right in the middle of it and you want answers fast.

If possible, each task description covers at least three areas:

- The graphical interface
- The command line, if available
- A recommended script, if applicable

The first is how you would approach the task to perform it on one or two servers. In fact, the graphical approach is designed primarily for administrators of small networks that contain fewer than 25 servers. The second is how you would approach a task when you have to perform it on a series of servers. Unfortunately, even though Windows Server 2008 includes a host of new command-line tools, this type of tool is not always available for every task. The advantage of this approach is that it is easy to insert command lines into command files in either CMD or BAT format to run them automatically. Another advantage of the command file is that it can be piped into a text file for automatic record-keeping, making your task even simpler. A third advantage is that it runs on Server Core if the role is supported.

The third method is for extremely large networks, where there are hundreds of servers. Each time a script is applicable to a given task, it is referenced in the task.

The Administrative Task List

The core of Chapter 13 is the administrative task list. The list proposed here has been drawn from a series of different sources, including our own experience as well as our clients' real-life administrative environments. It has, in fact, been validated through discussion and demonstration with several system administrators, as well as several full-day administration courses delivered at Interop (www.interop.com). Much discussion and consultation produced the list you'll find in there.

In addition, the task list has been categorized according to recommended task frequency. Frequencies range from a daily, weekly, monthly, and ad hoc basis. The latter is a category that includes everything from biyearly, yearly, and basically any time because some tasks must be performed, but their timing cannot be predicted.

Wherever possible, tasks that pertain to resource pools and/or virtual service offerings are clearly identified and documented.

NOTE *If you find that the schedule or the task list don't fit your needs, send us a note. Let us know what suits you best, and we'll publish updated information on the companion web site. Write to us at Infos@reso-net.com.*

The System Administrator

As a system administrator, you'll use a variety of tools to perform the activities listed here. Some of the activities will be administrative, some technical. Some will always remain manual, while others will be automated. Some will use Windows Server 2008's graphical interface and others, the command line.

To perform this job, you'll have to be technician, administrator, manager, communicator, operator, user, negotiator, and sometimes, director. You'll also need a significant understanding of the environment you work in and of the technologies that support it. This is why it is so important for you to gain a sound understanding of Windows Server 2008.

Organize Your Task Schedule

The task frequency should help you organize and define an administrative schedule. You can use the Task Management feature in Microsoft Outlook to help manage your administration schedule, especially for weekly, monthly, and bi-annual tasks (see Figure 12-15). You should also include daily tasks in the schedule at first so that you can become familiar with them. It is also a good idea to review all the tasks that are listed as "ad hoc" tasks and determine when you want to perform them.

Basically, daily tasks are performed in the morning of each day. If you can automate them, then they consist mostly of verifying logs rather than actually performing the task. This saves considerable time. Weekly tasks are performed on Tuesday, Wednesday, and Thursday. If you manage your schedule right, you can perform most of these tasks in the mornings along with the daily tasks for those days. Spread out monthly tasks on Mondays and Fridays of each week. This leaves you a bit of time each day to perform ad hoc tasks as they come up.

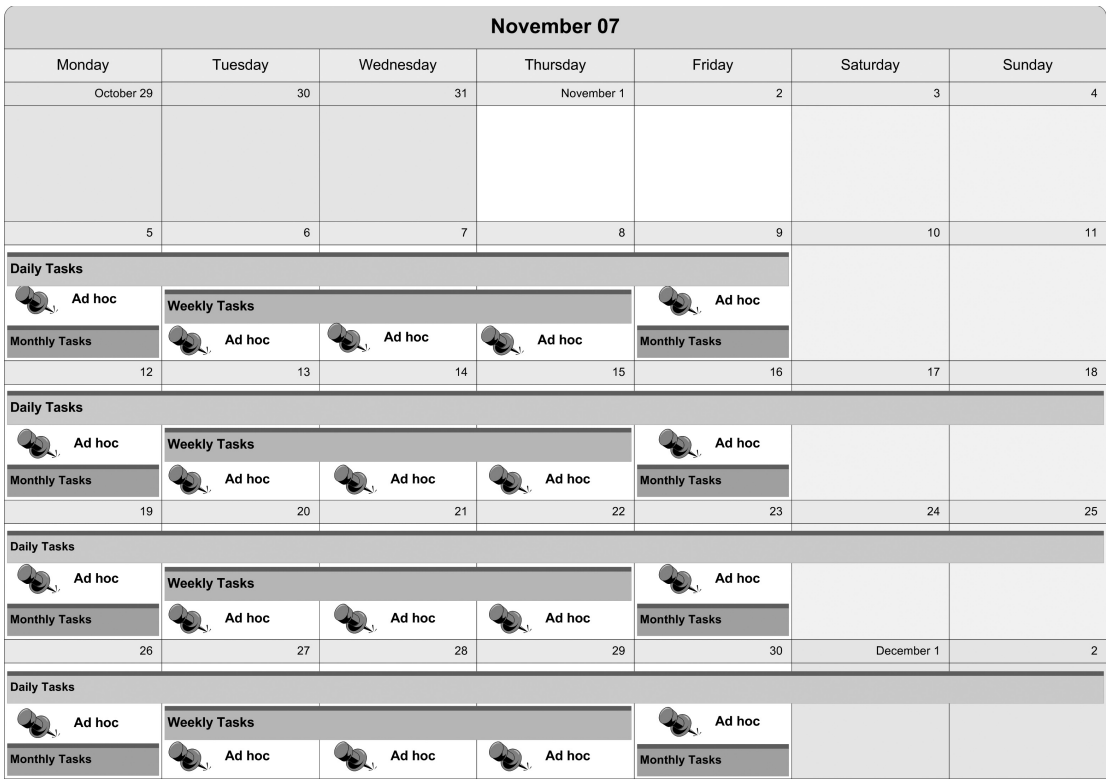

FIGURE 12-15 A sample administrative task schedule

One objective of Chapter 13 is to help save you time. You might consider doing all daily tasks in the morning, then spending the afternoons of the middle of the week performing weekly tasks. Reserve two afternoons of each week for monthly tasks; this way you can spread them out over the course of the month. This should normally leave you time for other or ad hoc tasks. Start out with this type of schedule and refine it as you go.

Now that you've built a powerful new network and implemented the dynamic datacenter, you need to make sure it stays as pristine as when you first built it. That can only happen if you administer it in a structured manner. That is the goal of the task list found in Chapter 13—to help you maintain the network you built based on these first 12 chapters.