3

CHAPTER THREE

Planning and Implementing an OU Structure

Terms you'll need to understand:

- ✓ Organizational unit (OU)
- ✓ Delegation of control
- ✓ Group Policy
- ✓ Security group
- ✓ Linked policies

Techniques/concepts you'll need to master:

- ✓ Implementing an OU structure
- ✓ Analyzing administrative requirements for an OU
- ✓ Creating an OU
- ✓ Moving objects within an OU hierarchy
- ✓ Delegating permissions for an OU to a user or to a security group
- ✓ Planning an OU structure based on delegation requirements
- ✓ Analyzing the Group Policy requirements for an OU structure

Implementing an Organizational Unit (OU) Structure

One of the primary advantages of Windows Server 2003 and Active Directory over Windows NT is the capability to control administrative powers more discretely. Under Windows NT, the base unit of administrative power was the *domain*. There was no way to grant someone administrative power over a subsection of the domain, such as a sales division or geographical office. This limitation meant that either the administrator was forced to make every required change to user access rights or that administrative power was granted to a larger circle of people.

There were some workarounds to this problem, including the use of master domain/resource domain structures, but even these required careful planning and additional infrastructure to function correctly. Particularly annoying was the fact that competing network operating systems did offer the capability to segregate administrative roles to a particular element of the network.

Fortunately, Active Directory introduces the organizational unit, or OU, to the Windows networking environment. An OU is essentially a container that is a subset of a domain that can contain any Active Directory object. The network administrator can designate control of and access to each OU and the objects it contains. In addition, policies can be designated on the OUs to manage user policies and rights.

Essentially, OUs have two main uses:

- **To allow subadministrators control over a selection of users, computers, or other objects**—These are typically non–domain administrators who have been delegated administrative rights for a specific OU without being granted permissions over the whole domain. Conversely, user accounts and groups with elevated permissions, such as service accounts, can be placed in an OU that has tighter access permissions to make changes than do general user accounts.
- **To control desktop systems through the use of Group Policy objects (GPOs) associated with an OU**—Although we give an overview of using Group Policy with OUs, this topic is covered in more depth in Chapter 5, "Planning a Group Policy Implementation."

We will look at each of these uses in the following sections.

Analyzing the Administrative Requirements for an OU

One of the most common needs for an administrator is the ability to allow others to manage user accounts. In larger companies, for example, it is often practical to allow desktop support personnel to have the ability to reset user passwords rather than having to go through a network administrator. There's always a fine line between maintaining security and delegating power to others. Windows NT offered the capability to grant others the right to change passwords and other limited administrative control, but these rights were applied on a domainwide basis. As a result, organizations were often forced to create complex multidomain environments to handle the varying administration requirements of different divisions.

For example, suppose your company has a group of software developers that needs to administer itself. The individual developers require administrative-level permissions to their source code and development servers. Your company also has a human resources group that must retain its own individual administration because of the confidential nature of the information it possesses, as well as a legal division that also has to administer itself for similar reasons. Plus, you have the main corporate domain that encompasses most everyone else. In the past, with Windows NT, you would be required to have four distinct domains for this scenario, with carefully managed trust relationships in place so everyone could access the corporate domain. But at the same time, you would have to ensure that the corporate domain could not access the other domains, except for some specific exceptions. Sounds like an administrative headache, doesn't it? Well, consider that as the size of the company grew, often so did its domain structure. The result often wasn't pretty.

Windows Server 2003, though, offers the capability to delegate various levels of control to only parts of a domain. This is accomplished through the use of organizational units (OUs). As discussed earlier, an OU is a container that can hold various Active Directory objects, including user accounts, computers, printers, shares, services, and much more. An OU can be thought of conceptually as a subdomain: Administrators of a domain can retain control of the OU, but specific rights can also be granted to other users or groups. It is important to note, though, that unlike a real domain, an OU is not a true security boundary and doesn't function in Active Directory like a domain. The OU is the smallest level of organization that can be administered in Active Directory. Using OUs in Windows Server 2003 with our previous scenario, you would be able to use a single domain for your organization and create OUs for developers, human

resources, and legal to delegate administration of their groups to the appropriate personnel. Because the delegation is within a single domain, the administrative burden of managing trust relationships and duplicating resources is reduced.

EXAM ALERT

The preferred administrative model in Windows Server 2003 is to use OUs whenever possible to delegate administrative authority rather than using additional domains. Administratively, OUs are easier to manage and are a better choice, unless the scenario has specific circumstances why you should use multiple domains.

In the next few sections, we will go through implementing an OU structure on your network, including creating an OU and delegating control of it. The scenario you will be following has the engineering department as somewhat of a separate organization, and it has been decided that the engineering department needs the right to change passwords for the division. Tired of changing passwords for marketing people at 2:00 a.m., the IS department agrees. So, IS will create an OU for engineering and also give someone in engineering the right to change passwords within this OU.

Creating an OU

To give the engineering department the functionality it is asking for, the IS department must first create an OU to contain the user accounts and other objects for the engineering department. All OU implementation and administration is accomplished through the Active Directory Users and Computers snap-in. After the console is started, navigate to the domain that the OU should be located within. From the context menu, choose New, Organizational Unit, as shown in Figure 3.1.

The first property screen for the new OU will ask for a name. This should be something that is descriptive and clearly shows the role of the OU. Enter the name in the field, as shown in Figure 3.2.

Moving Objects Within an OU Hierarchy

After the OU is created, it must be populated. To move users, computers, or other objects to an OU, open the proper folder and highlight the desired objects. From the context menu, select Move, as shown in Figure 3.3. One of the powerful features of this is that you can move multiple objects at the same time by Ctrl+clicking each object prior to right-clicking and clicking Move. In addition to users, groups, computers, and printers, you can also move one OU into another to create a hierarchy. We'll discuss this a bit later in the chapter.

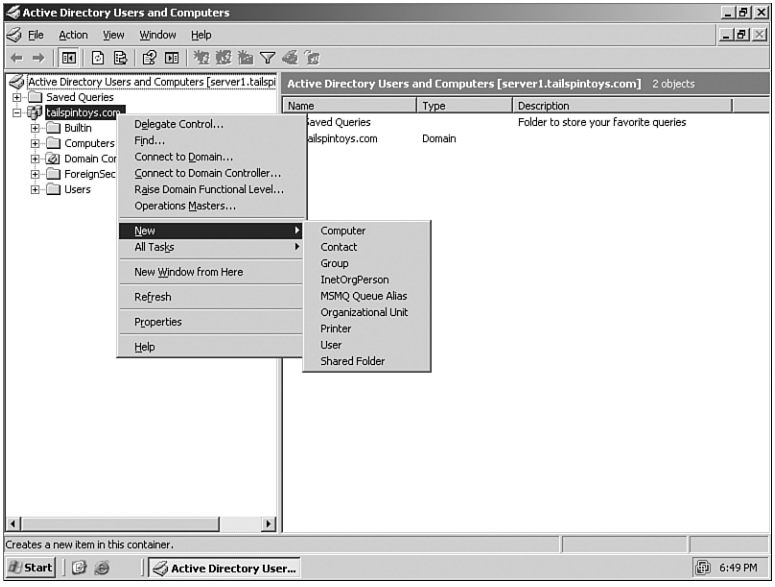

FIGURE 3.1 Creating a new OU.

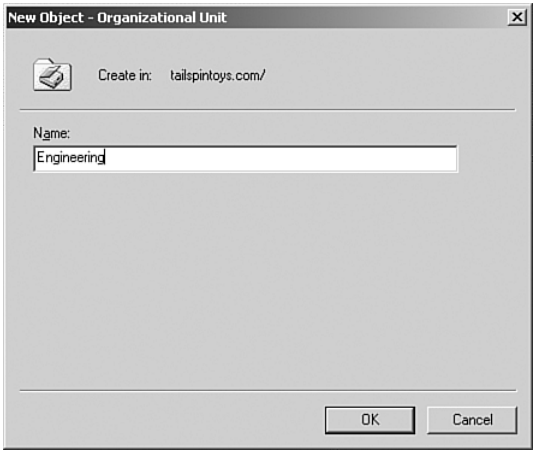

FIGURE 3.2 Enter the name for the OU.

CAUTION

You can also move objects between OUs by dragging and dropping them in Active Directory Users and Computers, but you should use this functionality with great care. It is all too easy to have a slip of the mouse and inadvertently drop objects into the wrong container.

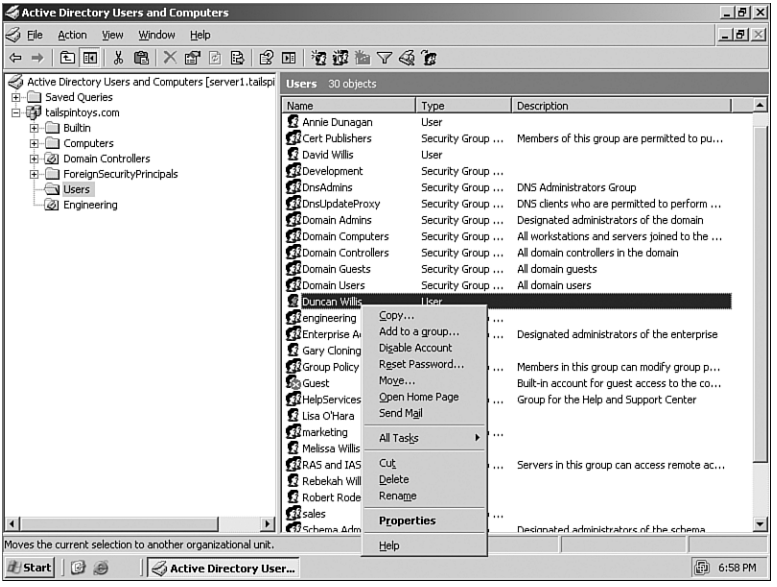

FIGURE 3.3 Moving objects to an OU.

The next step is to select the destination OU for the objects, as shown in Figure 3.4.

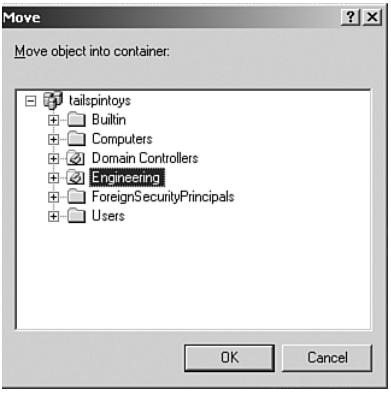

FIGURE 3.4 Selecting the destination OU.

After the various objects are moved into the OU, the contents of that OU can be viewed through the Active Directory Users and Computers console. In Figure 3.5, you see that we placed both the engineering security group and the computers that the engineering group uses into the OU. As a result of these actions, the engineering OU now contains the engineering department objects.

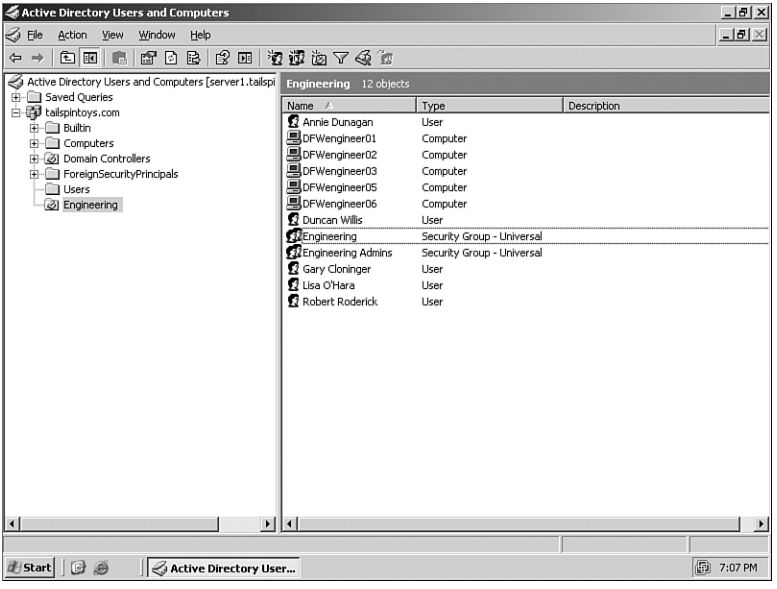

FIGURE 3.5 Viewing the contents of an OU.

Remember that when you move objects, the objects inherit the security settings of the destination. Furthermore, in a complex environment utilizing multiple levels of container nesting and Group Policy, moving objects must be done with care. Chapter 5 covers the tools you can use to accurately predict the results of Group Policy processing without having to actually move the object and see what happens.

Delegating Permissions for an OU to a User or to a Security Group

After the OU is created, it is time to delegate control of the OU to a selected few engineering users. Begin by opening the Active Directory Users and Computers console and selecting the desired OU, as shown in Figure 3.6. From the context menu, select Delegate Control.

This launches the Delegation of Control Wizard, as shown in Figure 3.7. As with most wizards, click Next to pass the startup screen.

The next step, shown in Figure 3.8, is to choose the group and/or users to whom the control is being delegated. In this case, we'll choose a group called Engineering Administrators. This group, which was created earlier, contains the user accounts of the two people trusted to change the passwords.

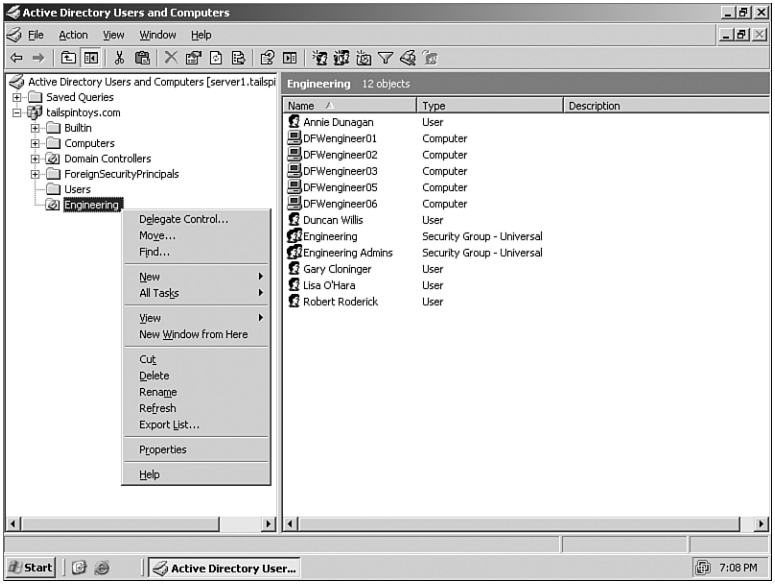

FIGURE 3.6 Delegating control of an OU.

FIGURE 3.7 The Delegation of Control Wizard.

TIP

Permissions should rarely if ever be granted to individual user accounts. It is standard practice to grant permissions to groups rather than users because it simplifies future administration in preventing you from having to change the delegation later if a user leaves the company or if a new employee is added who also needs those permissions. By using groups to delegate permissions, you delegate once and then control who has permission through their group membership. Chapter 4 discusses Users and Groups in more detail.

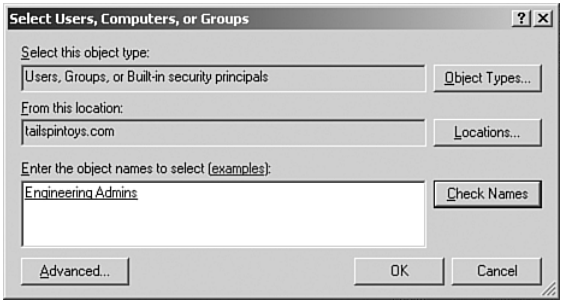

FIGURE 3.8 Select the group or user to whom control will be delegated.

After this selection, choose the rights that the delegates should exercise over the OU. The options you choose here determine the capabilities of the delegated administrators. Selecting the option Reset Passwords on User Accounts will allow the administrators for the OU to reset user passwords. As you can see in Figure 3.9, several other options are available.

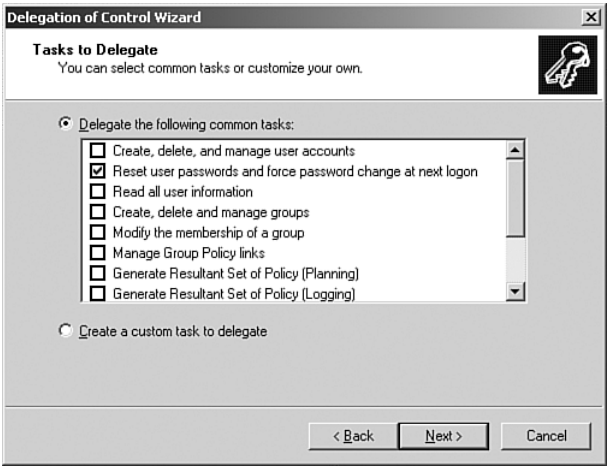

FIGURE 3.9 Assigning permissions.

The last step is merely to confirm the rights granted to the delegates. You should always double-check and verify that the rights granted actually match the intended purpose. Remember, the rights are inherited throughout the OU. If the rights granted are correct, select Finish, as shown in Figure 3.10. Note that if you need to modify the assigned permissions later, you can do so by going to the Security tab in the OU's properties. In addition, by going into the Advanced properties on the Security tab, you can then click the Effective Permissions tab and view the permissions that any user or group has on the object.

FIGURE 3.10 Verifying the delegated rights.

NOTE

The changes made by the delegation of Control Wizard are cumulative. This means that if you run the wizard multiple times and add different permissions for the same user or group, the permissions created would be cumulative rather than having the wizard replace prior permissions every time you run it.

Planning an OU Structure Based on Delegation Requirements

OUs provide a powerful, yet flexible mechanism for administering a Windows Server 2003 domain. As an administrator, when you look to implement an OU structure, you need to analyze your organization for its requirements prior to putting an OU structure in place. One important consideration is with respect to the OU hierarchy. Because you can nest OUs inside of OUs, you have the ability to create a very granular level of administrative control on a group-by-group basis within your organization. Consider the following example.

Your organization consists of 10 sites (sites are discussed in Chapter 7, "Implementing and Managing Active Directory Sites") corresponding to 10 physical locations in North America, Europe, and Asia. The network consists of three domains: na.wwinc.com, europe.wwinc.com, and asia.wwinc.com. The domains are part of the same forest, so they are connected automatically by two-way transitive trusts (trust relationships were discussed in Chapter 2, "Planning and Implementing Forests and Domains"). The Enterprise Admin team resides at your company's headquarters in Dallas, and each member of the Enterprise

Admins group also belongs to the Domain Admins group in each domain. The office in Barcelona is the headquarters for Europe, and that's where the Domain Admins team for europe.wwinc.com resides. The office in Seoul is the headquarters for Asia, and it houses the Domain Admins team for Asia. Each of the seven nonheadquarters physical locations has its own local IT department responsible for its own site.

In this scenario, you want the local IT departments to have administrative permissions for their local offices without granting them permissions at the domain level. In other words, giving them administrative rights should not allow them to administer sites other than their own. This holds true as well for the Domain Admins teams in each country. They should be able to administer their own domains but not other domains. And, finally, the Enterprise Admins team in Dallas should have administrative rights over the entire forest.

In the Windows NT days, this type of complex administrative structure would require creating a multimaster/resource domain model consisting of at least 13 domains (3 master accounts domains and 10 resource domains). Furthermore, you would have to manage a lot of one-way and two-way trust relationships, all manually configured. This would be a messy administrative situation.

Fortunately, with Windows Server 2003 you can use OUs to accomplish your goals. You would start by creating security groups for each IT department. Then you would create OUs for each local site. After that you would delegate administrative permissions for the OUs to the desired security groups (the local IT departments and higher-up IT departments). For example, you create an OU for the Omaha site. You also create all the relevant security groups, including OmahaIT and DallasIT (for North American administration). DallasIT includes the entire Dallas IT department, which has authority over any other site, yet only a subset of DallasIT is in Domain Admins, and only a subset of the na.wwinc.com Domain Admins group is a member of the Enterprise Admins group. After you had done that, you would delegate administrative control of the Omaha OU to OmahaIT and DallasIT (Domain Admins and Enterprise Admins by default have permissions).

Because the Dallas IT group is the highest level of IT in North America, above all the other site-administration groups, you would want to reflect that in your OU structure. Continuing with our example, you can use the nesting ability of Windows Server 2003 OUs to further define the structure. You could then create an OmahaIT OU and nest it inside the Omaha OU. By default, permissions in child objects are inherited from parent objects, so you wouldn't have to explicitly delegate authority to OmahaIT and DallasIT again unless you had disabled propagating permissions. If you had, you would delegate control of that OU to the OmahaIT and DallasIT security groups.

TIP

Inheritance is a double-edged sword. Although it can simplify administration in most cases, it can also be troublesome when you have situations where you do not want permissions to cascade down from higher levels to lower levels. You can turn off inheritance on an OU-by-OU basis, but if you do, you will need to manually specify all permissions. Chapter 5 covers inheritance in more detail.

Continuing, you could create further child OUs in the Omaha OU, one for each department that requires separate administration (or even just for categorizing users and groups). Using a hierarchy of OUs, you could even effectively deal with a situation where a local IT department shouldn't have administrative rights to a certain OU, but the Enterprise Admins group should. For instance, if you had a human resources group in Omaha, you could create an HR OU and remove OmahaIT from having propagated administrative rights (from the Omaha OU), remove DallasIT, remove Domain Admins as well, and delegate administrative control to the HR Administrators security group. The HR Administrators group would have administrative rights to its OU but not to any higher-level OUs (such as Omaha OU), and only the Enterprise Admins security group would still have access.

You could move this philosophy of creating an OU hierarchy across domains as well, resulting in a well-structured administrative hierarchy throughout the organization, encompassing all domains and sites.

Exam Cram Questions

1. Jon is the network administrator for a company that is looking to migrate directly from Windows NT 4 to Windows Server 2003 and Active Directory. The company currently has four domains to support one location because of varying administrative requirements. The CIO has asked Jon for a proposal for the new Windows Server 2003 deployment. What type of structure would be best for him to recommend?

   ❍ **A.** Jon should recommend upgrading each of the four domains in order to maintain their existing structure.

   ❍ **B.** Jon should recommend collapsing the four domains into a single domain and using OUs to create the organizational structure.

   ❍ **C.** Jon should recommend moving all the user accounts into a single account domain for administrative purposes, leaving the other three domains as resource domains.

   ❍ **D.** Jon should recommend upgrading each domain to Windows Server 2003 and using OUs within each domain to define the administrative structure.

2. Which of the following are benefits of using OUs in Windows Server 2003? [Choose the three best answers]

   ☐ **A.** Simplified domain structures

   ☐ **B.** Faster domain logons

   ☐ **C.** More granular permission delegation

   ☐ **D.** The ability to link specific Group Policies to subsets of a domain

3. You are the senior network administrator for a software development company. The Quality Assurance (QA) group has requested the capability to add and remove its own lab computers from the tailspintoys.com domain and to create and manage their own test user accounts on the domain for various testing situations. What steps should you take to grant their request, yet minimize the amount of administrative control they have and prevent them from managing their regular domain user accounts? [Choose the three best answers]

   ☐ **A.** Delegate Create, Delete, and Manage User Accounts and Reset user passwords and force password change at next login to the QA group to the tailspintoys.com domain.

   ☐ **B.** Delegate Create, Delete, and Manage User Accounts and force password change at next login to the QA group to the QA OU.

   ☐ **C.** Create a QA OU.

   ☐ **D.** Move QA users, groups, and computers to the new OU.

   ☐ **E.** Create a QA security group.

4. Brian is teaching a class on Windows Server 2003 administration. A student coming from a Windows NT 4 background just isn't getting the concept of OUs, and he asks Brian why he wouldn't just create the forests and domains necessary to support an organization's administration requirements. What should Brian tell the student? [Choose the three best answers]

   ☐ **A.** OUs provide easier access to network resources than using multiple domains.

   ☐ **B.** Group Policies are easier to manage using OUs than domains.

   ☐ **C.** Complex multidomain models increase the chances of security problems.

   ☐ **D.** The multidomain model is less efficient to administer than OUs.

5. You are an Active Directory consultant who has been hired by a government agency to analyze administrative access in the single domain environment. Because of regulations, the agency requires that not all five network administrators can administer administrator-equivalent accounts (all accounts with administrative access, including the built-in administrator account as well as all service accounts and the domain accounts of the network admins themselves). Instead, only the two admins with top-secret clearances are allowed to administer administrator level accounts. What would you recommend to allow all five admins to administer all 500 or so general accounts and groups, yet restricting administration of admin accounts to the two admins with proper clearance? [Choose the three best answers]

   ☐ **A.** Create a security group for the "super admins."

   ☐ **B.** Create an OU for the managed accounts.

   ☐ **C.** Place all nonadmin accounts in the new OU.

   ☐ **D.** Place all admin accounts in the new OU.

6. Louise is the senior network administrator and has been asked by her CIO to create an OU structure so that the human resources department can administer its own user accounts, and so that the IT department personnel other than Louise don't have permissions to their OU. Louise is the only member of the Enterprise Admins group, other than the domain's administrator account, whose password is known only by Louise and the CIO. Louise creates an HR Admins security group and HR OU, delegates administrative permissions to HR Admins, and removes the IT security group from the permissions list. Later she finds out that another network admin has been resetting user accounts for HR personnel. What has she missed?

   ❍ **A.** She needs to change the password on the domain administrator account because obviously the other network administrator is using that account.

   ❍ **B.** She needs to remove the Domain Admins group from the permissions list.

- ❍ **C.** She needs to create a separate domain for HR to isolate it from the main domain.
- ❍ **D.** She needs to remove the Enterprise Admins group from having permissions to the HR OU.

7. Bill is studying for Windows Server 2003 certification and is practicing on his home lab. He creates an OU using Active Directory Users and Computers and now needs to move his user accounts from the Users container to his new OU. What can he do to get the desired user accounts into the new OU? [Choose the two best answers]

- ☐ **A.** Bill can drag and drop the users between containers.
- ☐ **B.** Bill needs to grant his user account the necessary permissions to move user accounts from one container to another.
- ☐ **C.** Bill needs to select all the desired user accounts and use the Move command from the context menu.
- ☐ **D.** Bill needs to move the desired user account while he is creating the OU.

8. Holly is a network administrator for a Windows Server 2003 network. She wants to configure an HR Admins group to manage the user accounts for the HR department. She creates an HR Admins OU in the HR OU and moves the user accounts for the HR administrators into the OU. Then she delegates control of the HR Admins OU to the individual HR administrators' user accounts. She receives a call a few days later, though, from one of the HR admins, who complains that he can't reset a user's password. What might be wrong?

- ❍ **A.** Holly should have added the HR admins user accounts to the HR OU, not its own OU.
- ❍ **B.** Jeff hasn't logged off and logged back in since the change. He needs to do so to gain his new permissions.
- ❍ **C.** Holly did not delegate permission to the correct OU.
- ❍ **D.** Holly should have delegated permissions to a security group and not individual user accounts.

9. Charles has been asked to give an executive presentation on restructuring his company's Windows NT domains into a single Windows Server 2003 Active Directory domain utilizing OUs. During the presentation, the CEO asks Charles how having a hierarchy of OUs will affect people logging in to the domain and accessing resources compared to the current system. What should Charles tell the CEO?

- ❍ **A.** User accounts will be assigned to the OUs that they need to log on to.
- ❍ **B.** OUs have nothing to do with logging in to the domain.

- ❍ **C.** Because all the OUs will be in the same domain, users will have access to any domain resources.
- ❍ **D.** OUs can trust each other just like domains currently do.

10. Robert is the network administrator for a Windows Server 2003 network. He has delegated the control of the Developers OU to the Developer Admins security group, but after he completes the wizard he realizes he gave permission only to reset passwords and not to create and delete user accounts. What does Robert need to do to fix the problem?

- ☐ **A.** Robert needs to open the properties of the OU and go to the Security tab.
- ☐ **B.** Robert needs to run the Delegation of Control Wizard a second time to grant the desired permissions.
- ☐ **C.** Robert needs to edit the properties of the Developer Admins security group and change the permissions.
- ☐ **D.** Robert needs to remove the Developer Admins security group and re-create it, then run the Delegation of Control Wizard to set the permissions back up.

Answers to Exam Cram Questions

1. **B.** Ideally, Jon will simplify the domain structure and utilize OUs to give himself the benefit of delegated administration that wasn't available in Windows NT 4 (which forced the use of multiple domains). Answer A is incorrect because a new deployment is a perfect time to analyze existing structure and make changes that will be beneficial. Windows NT 4 had limitations that forced the organization into a multidomain environment, but these limitations aren't present in Windows Server 2003. Answer C is incorrect because this is the Windows NT way of structuring things. Answer D is incorrect because although using OUs is desirable, maintaining the four domains adds an unnecessary administrative burden.

2. **A, C, D.** By using OUs, you can simplify your domain structure because you can effectively delegate administrative permissions at the OU level without granting them at the domain level. As a result, you can also apply permissions and policies through Group Policy only to specific OUs without this affecting other OUs or the rest of the domain. Answer B is incorrect because the use of OUs has no impact on logon times.

3. **B, C, E.** Using OUs allows you to effectively limit the scope of administrative privileges, so you would create a QA OU and delegate the ability to create and manage accounts as well as the ability to reset passwords and force password changes. You would create a security group and delegate permissions to it rather than to individual

user accounts. Answer A is incorrect because delegating these permissions at the domain level gives too much access. Answer D is incorrect because the scenario only calls for the QA group to manage their test user accounts and lab machines, not their regular domain accounts. Again, they would have too much administrative control if you moved their regular accounts under their control.

4. **B, C, D.** As the number of domains in your organization increases, so does the number of trust relationships that have to be managed between domains and potentially between forests. The more complex the trust relationship structure, the more likely it is that one domain will be able to connect to another domain that it shouldn't have access to. Also, the use of domains often requires a duplication of administrative effort to configure policies and settings, making it less efficient than using OUs within a smaller number of domains. Group Policies are easier to manage with OUs because you can easily apply different policies to different OUs without this affecting other OUs or the domain. To create domains for every business unit that needs separate permissions or needs to administer itself would be an administrative headache. Answer A is incorrect because access to resources is a permissions issue, and permissions can be granted and managed across domains. From an end-user standpoint, it is no easier or harder to access resources from one domain to another if trusts are in place.

5. **A, B, C, D.** OUs can be used to delegate permissions to tighten control over an OU as well as to grant limited rights to an expanded set of users. In this situation, it makes more sense to create an OU to hold the admin level accounts and delegate authority to it to the two "super admins" than it would be to move 500 or so user accounts and groups to another OU. As a result, answer C is better than answer D because it would involve less administrative effort.

6. **B.** By default, the Enterprise Admins and Domain Admins groups will have administrative rights over any OU that is created in the domain. In this case, another network administrator, who is a member of Domain Admins but not Enterprise Admins, is able to perform account-management tasks on the OU. By removing Domain Admins, Louise will ensure that only Enterprise Admins and HR Admins can perform these tasks. As a result, answer D is incorrect because the scenario states that Enterprise Admins should have rights to the OU. Answer A is incorrect because it isn't necessarily the domain administrator account being used; rather, any member of Domain Admins would currently have administrative rights to the OU. Answer C is incorrect because using an OU is a better choice than using a domain, which is unnecessary to accomplish the goal of the scenario.

7. **A, C.** Active Directory Users and Computers supports dragging and dropping objects from one container to another in Windows Server 2003. Bill could also select all the objects he wants to move (he could do this one at a time as well, but it's less efficient), right-click and choose Move from the context menu, and then select the destination OU when prompted. Answer B is incorrect because this isn't a permissions issue. The console simply doesn't support the method Bill is trying to use. Answer D is incorrect because there is no option to populate an OU during the process of creating it.

8. **C.** Permissions, by default, propagate downward, but they do not propagate upward. As a result, the HR administrators would have administrative permissions to the HR Admins OU, but not to the HR OU. By default, if Holly had delegated control of the HR OU, the HR administrators would also have permissions to the HR Admins OU. Answer A is incorrect because it doesn't matter where the physical accounts are located. Answer B is incorrect because Jeff would not need to log off and on before being able to administer the OU he was delegated control of. Answer D is true in the sense that it is better to apply permissions to groups rather than individual user accounts, but it is incorrect in that there is no requirement to delegate control to a security group.

9. **B.** OUs are a means of organizing Active Directory objects, such as user accounts, for the purpose of delegating administrative control or applying differing policies. The user login process is irrelevant to the use of OUs because users will log in to the domain and access resources that they have been given permission to through security groups. In that respect it is no different from what users currently do. Answer A is incorrect because users don't log on to OUs. Answer C is incorrect because domain resources are still subject to permissions granted to security groups and individual accounts. Answer D is incorrect because OUs are not entities like domains that have trusts between them. An OU in and of itself is simply a container of Active Directory objects, and membership in an OU doesn't by itself grant any type of access to network resources.

10. **A, B.** To make the required changes to the permissions currently granted, it would be best to edit the properties of the OU and go to the Security tab. From there Robert could review the currently assigned permissions and configure new ones as necessary. Answer B would technically work because the changes made by the wizard are cumulative, but it might not be the best answer because when Robert reruns the Delegation of Control Wizard he would be unable to see what security groups and users currently have any privileges on the OU. Furthermore, he couldn't see what permissions had been granted. As a result, it would be difficult to know what permissions he had already granted and needed to grant, which can be done only through the Security tab of the object's properties. Answer C is incorrect because the security is set on the object itself (in this case, the Developers OU), not on the security group. Answer D is incorrect because there is no need to remove and re-create the Developer Admins security group; in fact, this would likely cause more problems than it would solve because the SID associated with the security group would be lost in the process.

Need to Know More?

Honeycutt, Jerry. *Introducing Microsoft Windows Server 2003*. Microsoft Press. Redmond, WA, 2003. ISBN 0-7356-1570-5.

Microsoft Corporation. *Microsoft Windows Server 2003 Resource Kit.* Microsoft Press. Redmond, WA, 2003. ISBN 0-7356-1471-7.

Mulcare, Mike, and Stan Reimer. *Active Directory for Microsoft Windows Server 2003 Technical Reference*. Microsoft Press. Redmond, WA, 2003. ISBN 0-7356-1577-2.