Network Administration And Support

Terms you'll need to understand:

- √ User accounts
- √ Passwords
- √ Event auditing
- √ Local groups
- √ Global groups
- √ Trust relationships
- √ Emergency Repair Disk (ERD)
- √ Registry
- √ Performance Monitor
- √ Network Monitor
- √ System management

Techniques you'll need to master:

- √ Setting up users and groups
- √ Making sure your network is secure
- √ Monitoring network performance

Not all of network administration is about hardware installation and troubleshooting. Once you've got the hardware in place and prepared to do its thing, you still need to ensure that the network is performing as expected, and that people can get to the resources they need, without getting to (or tampering with) resources they don't. In this chapter, we discuss the important points of network administration.

Managing Networked Accounts

The main task of network management is pretty basic: Make sure all users can access what they need, but can't get to what they don't or shouldn't. Okay, so this simple concept isn't always easy. We'll use Windows NT Server's User Manager For Domains as a framework for this subject, but the main idea is much the same no matter what tools you're using.

Managing User Accounts

There are three main points to managing user accounts. You must ensure that:

- Users have only the rights they need.
- Their accounts are secure.
- You know what those users are doing, within predetermined limits.

Creating User Accounts

The first step in managing user accounts is, of course, to create an account. Windows NT Server comes with two predefined accounts: an Administrator account for management duties and a Guest account for those who don't have an official account. However, it's unlikely that you'll want to use either of these for regular users. One account is too powerful for the average user, and the other is only useful if more than one person knows its password, which makes this option extremely insecure.

Before you begin creating accounts, however, you've got some decisions to make regarding the following:

- Passwords Should the user be able to change the password? How often should that password be changed? How many letters should it be? How often should users be able to reuse passwords? Should failed attempts to log on lead to lockouts?
- Logon hours Should users be restricted to logging on during certain hours of the day or only on certain days?

- Auditing Should user actions (logon, logoff, object access, and policy changes) be tracked? To what degree?

Passwords

For security reasons, it's best that users change passwords regularly. However, you will want to limit the frequency to some extent so users don't forget their passwords. If a user does lose track of his current password, it's fairly simple to fix with the User Manager For Domains—just open that user's account information, assign a new password, and then change the settings so that the user must change the password when signing on. More important, if you've adjusted passwords so that they may not be reused too frequently, it does you no good if an enterprising user just cycles through eight passwords to use "GoFish" again for the tenth time. Which brings up another point—Windows NT passwords are case sensitive, so you should take advantage of this fact to make them harder to guess. You should also include numbers in your passwords to make them less susceptible to dictionary attacks (password guessing programs that run through an entire dictionary to guess a password). But you shouldn't make passwords so difficult to guess that users start writing them down on sticky notes attached to their monitors.

What about account lockouts? It may seem unfriendly to lock out a user after a certain number of failed logon attempts. However, it foils automatic logon programs and good guessers if further attempts are refused after the specified number of attempts. Although it is an inconvenience, a valid user who has forgotten the password will have to find the network administrator to log on.

How long should passwords be? Theoretically, Windows NT can handle passwords up to 128 characters long, but dialog boxes won't accept more than 14 characters. Longer is generally better, especially because a minimum letter count avoids users using one space as their password (and pressing the spacebar once to gain access). We recommend a minimum of eight characters for password length.

Logon Hours

What about restricting logon hours? This isn't always necessary, and in some companies, it might even be undesirable. But in a tightly regulated office, it's another handy way of making sure that intruders can't break in and log on after working hours. However, the opportunities for a hacker to

steal a password are limited if an account is locked when the account's owner is out of the office and unlocked only when he or she is in.

Using Windows NT, you can restrict logon hours by day of the week, hours of the day, or both. What happens if a user is logged on past his or her logon hours? This depends on the OS the user has. If it's Windows NT Workstation, and you have checked the option to break the connection when logon hours are over, then he or she will be forcibly disconnected. If it's another operating system, such as Windows 98, the user simply won't be able to log back on if disconnected.

With Windows NT, you can set logon hours individually, so you don't have to set everyone's account to the same schedule.

Auditing

One way to keep track of what's happening on the network (or, more accurately, on the server) is to configure the server so that certain actions such as object accesses, changes to the security information, logons and logoffs, and the like, are recorded for later review.

How much you audit depends on how much information you can usefully store. Although you could conceivably log every activity on the network, you'd probably end up storing so much information that you couldn't use it. Often, it's enough to record failures so that you know what people were unsuccessful at. Of course, if you have reason to suspect unauthorized access, then it's time to start recording successes as well.

Setting User Rights

A more specific matter that you need to consider is which user rights you should assign. Windows NT Server and Windows NT Workstation both come with predefined groups to which you can assign users and to give them a set of rights without having to handpick them. For example, Windows NT Server comes with the predefined local groups described in Table 8.1.

The Replicator group is not included in this list because it's not a user group; rather, it is used for the Replicator service to dynamically replicate specified folders across the network.

Table 8.1 Windows NT's built-in groups.

Group	Rights
Administrators	Complete control over the computer and domain.
Account Operators	May administer user and group accounts for the local domain.
Backup Operators	Can back up and restore files to which they normally do not have access.
Guests	Permitted guest access to domain resources.
Print Operators	May add, delete, and manage domain printers.
Server Operators	May administer domain servers.

In addition to the local groups are some global groups (groups meant to be used in more than one domain): Domain Administrators, Domain Users, and Domain Guests. These groups are essentially the same as the local groups with similar names, with some caveats about group membership that we'll explain in the following section on group accounts.

Using predefined groups like these makes it easy to assign rights to new user accounts, but you're not limited to these options. Rather, you have the choice of assigning extra rights on an individual basis (for example, if necessary, you could add the right to create printers to Carla's account—although Carla is a member of the Users group and ordinarily would not have such a right). Another choice is to assign a user to more than one group, like Users and Print Operators. Just remember that rights are cumulative: In cases where rights conflict (that is, one group has the right to do something but another group does not), the most restrictive right (i.e., No Access) takes precedence.

In addition to the groups to which you can assign users, there are some other groups to which users are automatically added, and which you cannot delete. These groups are described in Table 8.2.

Table 8.2 Groups in Windows NT that cannot be deleted and have users automatically assigned.

Group	Membership
Everyone	Everyone currently logged on to the domain.
Interactive	Everyone logged on to the domain locally.
Network	Everyone logged on to the domain via the network.

It's very important to remember the existence of these groups. For example, all members of the group Everyone have Full Control access to objects by default—they can add to, delete from, and change them. Sometimes, this is exactly what you want, but do recall that the Everyone group includes everyone from the network administrator to the intern who started last week. Be aware of who's got what rights on your network.

Managing Group Accounts

You can, of course, add and delete rights for groups just as you can for users. You can even create entirely new groups to provide exactly the rights that you need, or add groups to other groups (subject to the restrictions explained in the following section). Once your network expands beyond a single domain, however, you can use groups to make other domains accessible to your users.

Global Groups And Local Groups

It's impossible to talk about managing group accounts in a Windows NT context without getting into the concept of global and local groups. The concept is at first difficult to grasp, but quickly becomes second nature.

Global groups are those intended for use in more than one domain. Their membership may include individual users.

Local groups are those intended for use in the local domain. Their membership may include individual users and global groups.

Trust Relationships

One reason you would want to add a global group to a local one is for cross-domain communication. As you know, Windows NT Server networks are organized into administrative units, called domains, for security reasons and to manage from a central point the resources and accounts for that portion of the network. By default, the resources for one domain are not accessible to those whose accounts are in another domain. This is all very well and good, but sometimes it's desirable to let members of one domain access resources on another.

That's where trust relationships come into play. With them, you can establish "trust" (one-way or two-way) between domains so that their members may use the resources of a domain to which they don't belong. A domain must first "permit" another domain to trust it before the trust is actually established. For two domains to trust each other—that is, for

the members of both domains to be able to use each other's resources—a two-way trust must be established, with each domain trusting the other as a separate action.

What do local and global groups have to do with all this? To establish the trust, you have to give the members of Domain A an account on Domain B. There are three ways of doing this:

- Method 1 Add each user individually to Domain B's user-account database.
- Method 2 Add each user's Domain A account to a global group on Domain A, and give that group rights on Domain B.
- Method 3 Add the Domain A user accounts to a global group, and then add that group to a local group on Domain B.

Although the reasons why the third method is the easiest choice are probably pretty clear, let's walk quickly through the decision process. The first method works, but it's slow and it's a pain, and if you ever add new users to Domain A, you have to remember to add them to Domain B as well; the account databases are not shared, and Domain B's will not be updated to reflect the changes.

The second method makes a little more sense, because you don't have to make as many changes, but you're still taking an unnecessary step.

The third method, on the other hand, is the simplest way from an administrative standpoint. Add the users of Domain A to Domain Users (a global group) and then add that group to the Users group on Domain B. Any changes to the membership of Domain A will immediately be reflected in Domain B (as long as the accounts in question are part of the global group).

Dealing With Changes To Users And Groups

Every time you make a change to a user account or group account under Windows NT, that change is reflected in the Registry database and recorded in the two hive files that make up the security information of the Registry: Security and SAM. Therefore, it is extremely important to back up the contents of the Registry, preferably during your daily server backup. Although you could technically re-create all the account information for your domain if you had to, it's much easier to keep backups so that you don't.

As you know, one important aspect of disaster recovery for Windows NT is making sure that changes are reflected in the Emergency Repair Disk (ERD) that you can use to restore your installation if necessary. When you do so with the RDISK utility, it's important to be sure to include the /S switch to the command when you run it, and to include the security hives as well as the other ones. By default, this information is not saved when you update the Repair directory and ERD.

Managing Network Performance

At this point, then, your network users are all set to go. It's not yet time to relax, however, because you've still got to worry about the performance those users will see. In this section, we'll talk about network performance, including what you're looking for and how you can use Windows NT and other tools to get that information.

Network Performance Characteristics

Just what are you looking for when it comes to monitoring your network? Obviously, you want to be sure that the cables are in one piece and the network cards aren't conflicting with anything. But beyond the bare minimum of making sure the hardware works, what is there to monitor?

- Data read from and written to the server each second
- Connections currently maintained to other servers
- Errors in accessing data
- The number of files network users have opened
- Queued commands
- The number of collisions per second on an Ethernet network

Data Reads And Writes

The number of bytes read from and written to the server provides a useful measure of how busy the server is, particularly if this count increases over time. You can also count the amount of data that cannot be read or written. This is because (on a Windows NT network) the server will attempt to take large data streams as streams of raw data, not as sets of packets. If the server refuses to accept many such streams of raw data, it's a possible indication of memory problems on the server, because a certain buffer is needed to accept the stream.

Queued Commands

The number of commands that are awaiting execution is one measure of how busy a server is. This number should never be too high—not much more than the number of network cards in the server; otherwise, it will represent a bottleneck.

Collisions Per Second

Only one node on an Ethernet segment can broadcast at a time. When more than one attempts to do so, there is a collision of the two packets, and you must resend them both. Although the time to resend is fairly short for the first failed attempt, it increases exponentially for further failed attempts (and the chance of a repeated collision is fairly good for the first couple of retries); this slows down network transmission. High collision rates are not a good thing.

The rate of collisions per second can actually tell you something about your network's physical topology. One of the main causes of network collisions is a cable segment is too long for the nodes to hear that another node is already transmitting. Nodes normally "listen" to determine if other nodes are transmitting before they transmit their data. However, the nodes can only "hear" over a certain distance, so a high rate of collisions may indicate that you need to include a repeater in your network segment. Even if it's not a matter of a segment being too long, a high rate of network collisions indicates a problem somewhere in the segment, and you must track it down.

The propagation delay problem that causes excess collisions is not usually that severe. The main cause of collisions is when high utilization rates mean that random backoff and retry on retransmissions induces further collisions. Also, collisions and utilization have nothing to do with each other, except that as the "knee" of the utilization curve is crossed (between 56 and 60 percent for Ethernet) collisions go up enormously, and eventually swamp real traffic.

Security Errors

Although there may be innocent explanations, high rates of failed logons, failed access to objects, and failed changes to security settings may all indicate a security risk on the network. Perhaps a hacker is attempting to break into the system or a user is trying to access objects to which he or she has been denied access. Either way, it's something to watch, and it's a good idea to set up auditing so you can see who's causing the errors. This is also a good time to drag out the protocol analyzer to see where the errors are coming from, in case someone is being spoofed.

Server Sessions

You can tell a bit about server activity by observing the rate at which connections to the server are made and how those connections are broken, whether by a normal logoff, by an error, or by a server timeout. The last two cases may indicate that the server is overloaded and is either refusing connections or can't service them quickly enough. More RAM in the server may do the trick, or you may need to update other hardware.

Monitoring Network Performance

You need to monitor network performance, but how do you do it? If you're running Windows NT Server, you already have three tools that you can use to monitor your system: the Event Viewer, the Performance Monitor, and the Network Monitor.

The Event Viewer

From the User Manager For Domains, you can choose to audit certain events. When you do so, the event logs are stored within the Event Viewer, which is part of the basic set of Windows NT administrative tools. The Event Viewer maintains three logs: one for security information, one for system information, and one for events generated by applications.

Of the three logs, the first two are the most important to our current discussion. The Security log records security events based on the filters you set up in the User Manager For Domains, so it's the most useful for getting information about failed attempts to log on or access data. The System log records events logged by Windows NT system components, and therefore is the most useful for nuts-and-bolts information about how your network is running, and whether all the hardware is working properly. For example, if you've recently installed a new network card and it's not working, you can check the System log of the Event Viewer to see whether an interrupt conflict has been recorded. In addition, the System log notes when services are stopped and started, so you can be sure that all necessary services are running.

The Performance Monitor

Unlike the Event Viewer, which records individual events, the Performance Monitor is best for recording and viewing trends. For the purposes of monitoring your network, you'll be most interested in collecting data for the following objects:

- Logical or physical disk on the server
- Network interface

- Any of the protocol counters (there are several)
- Redirector
- Server
- Server work queues

However, because running the Performance Monitor takes up resources that you'll probably want to save for servicing client requests, it's a good idea to monitor the server remotely, from a Windows NT Server machine that's not as busy. This will increase network traffic, but the performance hit won't be as bad as the strain on memory would be from running the Performance Monitor from the server.

The Network Monitor

Unlike the Event Viewer and Performance Monitor, the Network Monitor is not automatically installed during Windows NT setup; you must install it separately as a network service. Once it is installed, it becomes a fairly capable software-based protocol analyzer. As such, it monitors the network data stream and records the source address, destination address, headers, and data for each packet. Network Monitor can only capture as many frames as there's room for in physical memory (and it always leaves 8 MB free for other programs). Therefore, it's best to prepare some kind of filter to ensure that you get all the data you need without crowding it out with data you don't. You can filter data packets based on the transport protocol used to transmit them, by source and destination address, or by data pattern, looking for specific ASCII or hexadecimal streams in the data at a certain point in the data.

For security reasons, Network Monitor detects other installed instances of Network Monitor agents on the network, showing the name of the computer on which they are running, the name of the person logged in, what the agents are doing at the moment, the adapter address, and the version number. Some instances of Network Monitor may not be detected if there's a router between your part of the network and the Network Monitor, if the router does not support multicasting, but if the monitor can see you, you can see it.

Total System Management

The network is a major bottleneck when it comes to network performance, but it's not the only one. In addition to thinking about network conditions, you should also consider what's happening on the server side, particularly when it comes to hard disk space and the amount of available memory.

Hard Disk

Of the three tools that come with Windows NT Server, the Performance Monitor is most useful when it comes to monitoring disk information on a Windows NT network. You'll be looking at the following:

- Remaining disk space
- Speed at which requests are serviced (both in terms of throughput and the amount of data being transferred)
- How often the disk is busy (both in terms of how often it's running and the average number of requests queued)

When monitoring disks, notice whether you're monitoring the physical disk object or the logical disk object; each may represent something different. Also, notice that not all counters will add up to 100 percent even if you do measure on a percentage basis. This is because the readings for multiple logical disks may very likely add up to more than 100 percent for the entire physical disk. Sometimes, you need to average the results among disks.

To use the disk-performance counters, you must first run DISKPERF from the command prompt. Otherwise, they'll all register as zero.

Memory Use

The other big issue with servers is the amount of memory they have to service the requests that come in. Windows NT is designed to page data out of memory when the data is not in use, or when it needs the memory for other, more recently used data. If it needs the data, it lets a page fault occur to get the data back in memory. However, if the server has to page too much data, installing more memory would be a good idea.

There are two kinds of page faults. Soft page faults occur when data is removed from a program's working set (the set of data that the process is actively using) and is moved to another area in physical memory. Thus, when that data is needed, it's a very fast operation to get it back into the working set. Hard page faults—when the data has gone unused for so long or there's such a shortage of physical memory that program data is actually stored on the hard disk—are another matter entirely. Reading data from disk takes quite a while longer than reading it from memory does, so if too many hard page faults occur, response time slows considerably. Thus, the best measure of memory shortages is the rate at which hard page faults occur.

Maintaining Network History

Both the Performance Monitor and the Event Viewer are able to prepare log data that you can use to keep long-term records of network performance and events. You can use this data to determine trends or notice when a new problem arises. Just as with any other troubleshooting techniques, you can't recognize a problem if you don't know what the solution looks like.

Be a little selective about the data you retain. One of the principal errors most beginning network administrators make is being too enthusiastic about archiving data, recording every burp and hiccup on the network and servers. The end result, of course, is that when the time comes to review this material there's an impossible amount of data to wade through and the history becomes useless.

Practice Questions

Question 1

What user accounts are already built into Windows NT? [Check all correct answers]

- ❑ a. Administrator
- ❑ b. Replicator
- ❑ c. Backup Operator
- ❑ d. Guest

Answers a and d are correct. The Administrator and Guest user accounts are built into Windows NT. Answers b and c are incorrect: Replicator and Backup Operator are not user accounts built into Windows NT.

Question 2

Which of the following are logs maintained by Event Viewer? [Check all correct answers]

- ❑ a. Security information
- ❑ b. Network information
- ❑ c. System information
- ❑ d. Application events

Answers a, c, and d are all correct. The Event Viewer maintains logs for security, system information, and events generated by applications. Answer b is incorrect; Event Viewer does not maintain a network information log.

Question 3

Where are user accounts created?

- ❍ a. Server Manager
- ❍ b. Network Monitor
- ❍ c. User Manager For Domains
- ❍ d. System Administrator

Answer c is correct. User accounts are created and maintained by the User Manager For Domains. Neither Server Manager nor Network Monitor are capable of creating user accounts. Therefore, answers a and b are incorrect. There is no tool called System Administrator. Therefore, answer d is also incorrect.

Question 4

Which of the following need to be considered before you begin creating user accounts? [Check all correct answers]

- ❑ a. Passwords
- ❑ b. Logon hours
- ❑ c. Groups
- ❑ d. Auditing

All of the answers are correct. You should consider password length and duration, what time of day users are allowed to log on, what groups they will belong to, and what type of auditing needs to take place on user accounts.

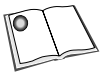
Question 5

Which of the following can you track using Network Monitor? [Check all correct answers]

- ❑ a. Data packets based on the transport protocol
- ❑ b. Source and destination addresses
- ❑ c. Data patterns
- ❑ d. Disk reads and writes

Answers a, b, and c are all correct. You can filter data packets based on the transport protocol used to transmit them, by source and destination address, or by data pattern, looking for specific ASCII or hexadecimal streams in the data at a certain point in the data. You would use Performance Monitor to track disk reads and writes. Therefore, answer d is incorrect.

Need To Know More?



Heywood, Drew: *Inside Windows NT Server 2nd Edition*. New Riders, Indianapolis, IN, 1995. ISBN 1-56205-860-6. Chapter 16, "Windows NT Server and NetWare," explains the salient software, communications issues, and connectivity concerns that are likely to appear on the test.

Minasi, Mark and Peter Dyson: *Mastering Windows NT Server 4, 5th Edition*. Sybex Network Press, Alameda, CA, 1997. ISBN 0-7821-2163-2. This book provides a good overview of Windows NT network-management tools and how to use them effectively.

Zacker, Craig, Paul Doyle, et al.: *Upgrading and Repairing Networks*. Que Books, Indianapolis, IN, 1996. ISBN 0-7897-0181-2. Chapter 30 discusses network management.

Search the TechNet CD (or its online version through www.microsoft.com) using the keywords "network performance," "user accounts," and "group accounts." The Windows NT *Concepts and Planning Manual* also includes useful information on network management and using the tools listed here.