realtimepublishers.com™

Tips and Tricks Guide™ To

Active Directory Troubleshooting

NETPRO
The Directory Experts

Don Jones

Introduction

By Sean Daily, Series Editor

Welcome to *The Tips and Tricks Guide to Active Directory Troubleshooting*!

The book you are about to read represents an entirely new modality of book publishing and a major first in the publishing industry. The founding concept behind Realtimepublishers.com is the idea of providing readers with high-quality books about today's most critical IT topics—at no cost to the reader. Although this may sound like a somewhat impossible feat to achieve, it is made possible through the vision and generosity of corporate sponsors such as NetPro, who agree to bear the book's production expenses and host the book on its Web site for the benefit of its Web site visitors.

It should be pointed out that the free nature of these books does not in any way diminish their quality. Without reservation, I can tell you that this book is the equivalent of any similar printed book you might find at your local bookstore (with the notable exception that it won't cost you $30 to $80). In addition to the free nature of the books, this publishing model provides other significant benefits. For example, the electronic nature of this eBook makes events such as chapter updates and additions, or the release of a new edition of the book possible to achieve in a far shorter timeframe than is possible with printed books. Because we publish our titles in "real-time"—that is, as chapters are written or revised by the author—you benefit from receiving the information immediately rather than having to wait months or years to receive a complete product.

Finally, I'd like to note that although it is true that the sponsor's Web site is the exclusive online location of the book, this book is by no means a paid advertisement. Realtimepublishers is an independent publishing company and maintains, by written agreement with the sponsor, 100% editorial control over the content of our titles. However, by hosting this information, NetPro has set itself apart from its competitors by providing real value to its customers and transforming its site into a true technical resource library—not just a place to learn about its company and products. It is my opinion that this system of content delivery is not only of immeasurable value to readers, but represents the future of book publishing.

As series editor, it is my raison d'être to locate and work only with the industry's leading authors and editors, and publish books that help IT personnel, IT managers, and users to do their everyday jobs. To that end, I encourage and welcome your feedback on this or any other book in the Realtimepublishers.com series. If you would like to submit a comment, question, or suggestion, please do so by sending an email to feedback@realtimepublishers.com, leaving feedback on our Web site at www.realtimepublishers.com, or calling us at (707) 539-5280.

Thanks for reading, and enjoy!

Sean Daily

Series Editor

Note to Reader: This book presents tips and tricks for Active Directory troubleshooting topics. For ease of use and for cross referencing, the questions are numbered.

Copyright Statement

Q.1: What do the FSMO roles do?

A: In general, all domain controllers in an Active Directory domain are created equal. That is, they all have the ability to both read from and write to the Active Directory database and are essentially interchangeable. However, certain operations within a domain and forest must be centrally coordinated from a single authoritative source. These operations are handled by only one domain controller within the domain and are divided into five distinct operational categories. These categories are referred to as *Flexible Single Master Operations* (FSMOs).

The term *flexible* refers to the fact that no particular domain controller must handle these operations. Instead, the five FSMO *roles* can be held by any one domain controller; in fact, all five roles can be held by a single domain controller if you desire. When you install the first Active Directory domain in a new forest, the first domain controller you create automatically holds all five roles, and will continue to do so unless you manually move one or more of the roles to another domain controller.

The FSMO Roles

The five FSMO roles are as follows:

- **Schema master**. This role is held by only one domain controller per forest. This role coordinates all changes to the Active Directory schema, and is required in order to process any schema updates. Only the schema master is permitted to replicate schema changes to other domain controllers in a forest.
- **Domain naming master**. This role is held by only one domain controller per forest. This role handles all changes to the forest-wide domain namespace, and is the only role that can process the addition or removal of a domain to or from the forest.
- **RID master**. This role is held by only one domain controller per domain. This role manages the *relative identifier* (RID) pool for the domain (for more information about RIDs, see the sidebar “Relative Identifiers in a Domain”). This role is also responsible for moving objects from one domain to another within a forest.
- **PDC emulator**. This role is held by only one domain controller per domain. This role is the central authority for time synchronization within a domain, and emulates the functionality of a Windows NT 4.0 Primary Domain Controller (PDC). Any NT Backup Domain Controllers (BDCs) in a domain replicate from the PDC emulator. Pre-Windows 2000 (Win2K) clients without the Microsoft Directory Services Client (DSClient) contact the PDC emulator to change user and computer passwords. The PDC emulator is also responsible for processing account lockouts. Finally, any failed logon attempts are first forwarded to the PDC emulator before returning a bad logon message to the client.

> ✎ The PDC emulator is the one FSMO role that your domain cannot live without for very long. This role should be placed on a robust server computer, and you should monitor that computer closely to ensure that the PDC emulator is functioning correctly. Because the PDC emulator processes account lockout, it is a key piece of Active Directory’s security infrastructure.

- **Infrastructure master**. This role is held by only one domain controller per domain. This role updates object *security identifiers* (SIDs) and distinguished names (DNs) in cross-domain object references.

Relative Identifiers in a Domain

All security principals, such as users and computers, in a domain have a unique SID that identifies the principal on access control lists (ACLs) in the domain. SIDs consist of two major portions: the domain SID, which is the same for all SIDs within a domain, and a RID, which is unique for each security principal within a domain. The combination of the domain SID and the RID make the resulting SID completely unique across domains, even though different domains can issue the same RIDs.

The RID master allocates small pools of unique RIDs to each domain controller in a domain. Domain controllers use this pool to assign RIDs when creating new security principals. When a domain controller runs out of available RIDs, the domain controller contacts the RID master to obtain a new pool. Because all RIDs originate from a single source, the RIDS are guaranteed to be unique within the domain.

✎ You might sometimes see references to a sixth FSMO role, the Global Catalog (GC). Although the GC is an extra function that can be assigned to a domain controller, it is not a FSMO. Domains and forests can contain multiple domain controllers acting as a GC server, whereas FSMOs are be definition held by one, and only one, domain controller at a time.

📖 For more information about the FSMO roles, refer to the Microsoft article “Windows 2000 Active Directory FSMO Roles.”

The following list provides some best practices for placing FSMOs:

- In a multiple-domain forest, never place the infrastructure master role on a domain controller that is also a GC server. The infrastructure master’s job is to update cross-domain references, and it does so by looking for references it does not itself possess. Because a GC contains a reference to every object in the entire forest, the infrastructure master will never be without a reference, and will therefore fail to perform its job properly.
- Because the PDC emulator holds such a crucial, central role in Active Directory, you should place the PCD emulator on a domain controller that has the best possible connectivity to other domain controllers in the domain. The PDC emulator in the forest root domain synchronizes time for all other PDC emulators in the forest, and should have a reliable network connection to the domain controllers holding the role in each domain.
- You should place the schema master on a domain controller that is physically collocated with the administrators responsible for maintaining the forest’s schema. This placement will ensure that the administrators have a reliable connection when performing schema updates.

FSMO Failover

Active Directory does not provide automatic failover for the FSMO roles. Some of the roles, such as the schema master, aren't required for Active Directory's day-to-day operations, so automatic failover isn't strictly necessary. However, some roles, such as the PDC emulator, control critical domain operations, and you'll notice pretty quickly if the domain controller containing the role fails. In those cases, you'll have to manually relocate the FSMO role to another domain controller.

For more information about how to move FSMO roles, see Question 8.

Q.2: How do I reset a computer's domain account?

A: Normally, computers' domain accounts are self-maintaining. Computers authenticate to the domain automatically upon startup, and periodically change their domain passwords without your intervention. However, it is possible for a computer's domain account to have problems, which can require you to reset the account.

Resetting a computer's domain account will break the link between the computer and the domain. The computer will have to be joined to a workgroup (thus removing it from the domain), then re-joined to the domain.

Resetting the Account

You can reset a computer account by using either the Microsoft Management Console (MMC) Active Directory Users and Computers snap-in or a command-line utility. To use Active Directory Users and Computers, open Active Directory Users and Computers, and locate the computer's account. By default, Active Directory places computer accounts in the Computers container. However, your organization might place computer accounts in another organizational unit (OU). Right-click the computer account, and select Reset from the context menu.

You can't perform this procedure with a domain controller. Generally, there's no need, as the computer can always contact itself to reset its own password. However, if a domain controller's Active Directory account becomes unsynchronized, you'll have to use DCPromo to remove and reinstall Active Directory.

To use a command-line utility, run

```
dsmod computer computername -reset
```

replacing *computername* with the name of the computer you want to reset.

You must be a Domain Administrator, Enterprise Administrator, or have the appropriate delegated permissions to perform these tasks.

Rejoining the Domain

Once its account is reset, a computer will be unable to authenticate to the domain. Essentially, you've changed the computer's password and have no way to tell it what the new password is. The only solution is for you to remove the computer from the domain, then rejoin it to the domain.

> ✎ A side effect of the computer being unable to authenticate to the domain is that no users will be able to log on to the computer by using domain credentials.

To rejoin the domain on a Windows XP Professional computer (the process for Windows 2000—Win2K—is similar), right-click My Computer, and select Properties from the Context menu. On the Computer Name tab, click Change. Select Workgroup, and click OK to close all dialog boxes. You will need to restart the computer. Return to the Computer Name tab after restarting, and click Change again. Select Domain, provide the appropriate domain name, and click OK. You will need to provide the appropriate user credentials to add the computer back into the domain. After completing these steps, the computer should be able to authenticate to the domain. Restart the computer and ensure that the domain logon problem is resolved.

Q.3: How do I troubleshoot the domain controller location process?

A: Computers that are unable to locate a domain controller for their domain won't be able to log on and won't be able to process user logons. Troubleshooting the domain controller location process is a key part of solving many logon problems.

> 🕮 For more information about how computers locate a domain controller, see Question 4.

Symptoms

Symptoms of a client's inability to locate a domain controller include an inability to log on to the domain and an inability to process user logons. You might also see System and Security event log messages indicating that a domain controller for the appropriate domain could not be found.

Verification

To determine the cause of the problem, follow these steps:

1. Verify that the computer has the correct IP configuration for its subnet, including IP address, DNS server, and default gateway. To do so, open a command-line window and run

   ```
   ipconfig /all
   ```

   to display the configured information. If the configuration is wrong, correct it.
2. Use the Ping utility to verify network connectivity to the configured default gateway, DNS server, and at least one domain controller in the local site. If you cannot verify connectivity, troubleshoot and correct the problem.
3. Run

```
netdiag /v
```

to report on any problems with Windows' networking components. Correct any error conditions that are reported by using Netdiag /fix or by manually correcting the problem.

> ✎ Netdiag is included in the Support Tools on the Windows CD-ROM.

4. Run

   ```
   nltest /dsgetdc:domainname
   ```

   replacing domainname with the name of the domain that you are trying to log on to. This command verifies that a domain controller can be located. Nltest is included in Support Tools.

5. Use the Nslookup tool to verify that DNS contains the proper records to locate a domain controller. If either of the following tests fail to return records with the proper host names and IP addresses, restart your domain controllers to force them to register with DNS (also ensure that DNS is configured to accept dynamic updates and can accept service resource (SRV) records):

   ```
   nslookup fully-qualified-server-name
   ```

   where *fully-qualified-server-name* is the complete DNS name of a known domain controller, such as dc1.mydomain.com

   ```
   nslookup guid._msdcs.rootdomain
   ```

   where *rootdomain* is the complete DNS name of the root domain, such as mydomain.com

6. On your domain controllers, run

   ```
   dcdiag /v
   ```

   to check for many common domain controller problems. Correct any error conditions that are reported.

Corrective Action

Assuming that your client computer has a proper network configuration and is otherwise able to connect to a domain controller (using ping, for example), the problem is most likely in your DNS resource records, or your domain controller is not functioning properly.

If DNS does not contain the proper records, restart a domain controller. Doing so should re-register the domain controller in DNS; if it fails to do so, then either DNS is at fault or that particular domain controller has failed. Verify that other domain controllers can register with DNS. If they cannot, replace your DNS server. If they can, the original domain controller has failed and might need to be removed from the network.

If DNS contains the proper records, but a domain controller continues to not respond to client requests, restart the domain controller. If doing so fails to correct the problem, you will most likely need to demote the domain controller to a member server, then reinstall Active Directory by re-promoting the server.

Note that very few client-side conditions exist other than basic network misconfiguration that prevents a client from locating a domain controller. Most of the problems are in the DNS server or with a domain controller that fails to respond to a client's initial requests.

> 📖 For additional troubleshooting steps that help verify Lightweight Directory Access Protocol (LDAP) connectivity, refer to the Microsoft article "How Domain Controllers Are Located in Windows" for Win2K and "How Domain Controllers Are Located in Windows XP" for Windows XP Professional.

Q.4: How do client computers locate a domain controller?

A: One of the first major tasks a domain member computer has to do when it starts is to locate a domain controller. Generally, this task requires the use of a Domain Name System (DNS) server, which contains records for each domain controller in the domain, and the Locator, a remote procedure call to the computer's local Netlogon service.

Starting Up

When the client computer starts, its Netlogon service starts automatically (in the default configuration). This service implements the DsGetDcName application programming interface (API), which is used to locate a domain controller.

> ✎ In this context, "client computer" is any computer attempting to contact a domain controller. This definition includes member servers.

The client begins by collecting a number of pieces of information that will be used to locate a domain controller. This information includes the client's local IP address, which is used to determine the client's Active Directory site membership, the desired domain name, and a DNS server address.

Finding the Domain Controllers

Netlogon then queries the configured DNS server. Netlogon retrieves the service resource (SRV) records and host (A) records from DNS that correspond to the domain controllers for the desired domain. The general form for the queried SRV records is *_service._protocol.domainname*, where *service* is the domain service, *protocol* is the TCP/IP protocol, and *domainname* is the desired Active Directory fully qualified domain name (FQDN). For example, because Active Directory is a Lightweight Directory Access Protocol (LDAP)-compliant directory service, clients query for _ldap._tcp.*domainname* (or _ldap._tcp.dc._msdcs.*domainname* when locating the nearest domain controller).

Each domain controller in a domain will register its host name with the SRV record, so the client's query results will be a list of domain controller host names. The client also retrieves the associated A records, providing the client with the IP address of every domain controller in the domain. The client then sends an LDAP search query, via the User Datagram Protocol (UDP), to each domain controller. Each domain controller then responds, indicating that it is operational. The Netlogon service caches all of this information so that finding a domain controller in the future won't require a repeat of this initial process. Instead, the service can simply refer to its cache to find another domain controller.

Selecting a Domain Controller

After the client locates a domain controller, the client uses LDAP to access Active Directory on a domain controller, preferably one in the client's own subnet. The domain controller uses the client's IP address to identify the client's Active Directory site. If the domain controller is not in the closest site, then the domain controller returns the name of the client's site, and the client tries to find a domain controller in that site by querying DNS. If the client has already attempted to find a domain controller in that site, then the client will continue using the current, non-optimal domain controller.

Once the client finds a domain controller it likes, it caches that domain controller's information, and the client will continue to use that domain controller for future contacts (unless the domain controller becomes unavailable).

Q.5: How can I manually sync the time of a client computer with the domain?

A: You might need to manually synchronize the time of a client computer within a domain. Note that this need should be the exception rather than the rule; Windows 2000 (Win2K) and later computers in a domain should automatically synchronize time with a domain controller. Manually synchronizing the time will not resolve the underlying time sync issue, but might temporarily resolve any other problems that arise from a lack of proper time sync (such as user and computer logon issues). See the sidebar "Manual Sync as a Troubleshooting Step" for more information about manually synchronizing the time.

📖 For details about how the automatic time sync process works, see Question 7.

Manual Sync as a Troubleshooting Step

One common reason to manually synchronize a computer's time is as a troubleshooting step. For example, if you notice System event log entries from the W32Time service, which indicate that time synchronization failed, you might attempt to manually sync the time as a troubleshooting step.

Typically, failed time synchronization is the result of the computer being unable to contact a domain controller, and you should troubleshoot that problem directly. Once the W32Time service fails to locate a domain controller, it will reduce its activity to location attempts every 16 hours until restarted. You'll see System event log messages to this effect, with Event ID 64, whenever the service is unable to locate a domain controller for a long period of time.

To manually synchronize time, open a command-line window, and run

```
net stop w32time
```

Run

```
w32time -update
```

Run

```
net start w32time
```

Manually verify the synchronization between the client computer and a domain controller. Also check the System event log to ensure that the W32Time service has not logged additional error messages.

Q.6: How can I tell if my PDC Emulator is working?

A: The PDC emulator plays a vital role in the operation of any Active Directory domain. It's responsible for time synchronization, processing account lockouts, and more. If the PDC emulator fails, several key domain functions, including security functions, can stop functioning properly.

Symptoms

If your domain exhibits any of the following symptoms, you need to verify the status of the PDC emulator role:

- Users are unable to log on—This symptom can occur if the domain's time synchronization becomes more than about 5 minutes out of sync. The reason is that the PDC emulator is the central source for time sync; a general lack of domain time synchronization can often be traced to the PDC emulator.

> 🕮 For more information about troubleshooting domain time sync, refer to http://www.Microsoft.com/windows2000/techinfo/reskit/samplechapters/dsbi/dsbi_add_qouy.asp.

- User accounts that should be locked out aren't locked out—The PDC emulator processes account lockouts for the entire domain.
- Pre-Windows 2000 (Win2K) clients are unable to change their passwords—The PDC emulator provides password-change processing for non-Active Directory client computers.
- Windows NT Backup Domain Controllers (BDCs) are not receiving updates to the domain user lists—The PDC emulator is responsible for replicating these updates to down-level domain controllers.

Verification

Some of the symptoms of a PDC emulator failure can be traced to a replication failure, network failure, or other condition unrelated to the PDC emulator. To verify proper operation of the PDC emulator, follow these steps:

- Identify the domain controller that has the PDC emulator role. From the command line of any domain controller, run

  ```
  dsquery server -hasfsmo pdc
  ```

  The command-line utility will report the fully qualified name of the domain controller believed to hold the role. Note that *server* is an actual dsquery parameter and not the name of a particular server on your network.

- Verify network connectivity to the domain controller by using the ping command. Then attempt to connect to the domain controller by using the Active Directory Users and Computer console from another domain controller or client computer. If either of these steps fail, troubleshoot the domain controller for basic network connectivity. Also ensure that all domain controllers in the domain are running the same Windows service pack level.

- Verify that Active Directory replication is working properly. On the domain controller holding the PDC emulator role, run

  ```
  repadmin /showreps servername
  ```

  supplying the server name of the domain controller that holds the PDC emulator role. Any errors indicate a problem with Active Directory replication, which you should resolve.

> ✎ The Repadmin tool is provided as part of the Support Tools, which are available on the Windows Server product CD-ROM.

- Verify that the PDC emulator role is functioning. On the domain controller holding the PDC emulator role, force a user account to lock out (by logging on with a bad password multiple times, for example). Verify that the account appears locked out in Active Directory Users and Computers on the domain controller. If not, the PDC emulator has failed. If the account locks out, verify that the locked out status replicates to other domain controllers in the domain. If it does not replicate to some domain controllers, troubleshoot for Active Directory replication failure. If it does not replicate to any domain controllers, the PDC emulator role might have failed.

> ✎ You will need to be familiar with your domain's account lockout policy in order to effect an account lockout. Note that disabling an account is not the same as the account being locked out, and will not be handled the same by the PDC emulator.

Corrective Action

If you determine that the PDC emulator has failed, try these corrective actions:

- If the domain controller believed by Active Directory to hold the PDC emulator role no longer exists, seize the role on another domain controller in the domain.
- If the domain controller containing the PDC emulator role is still functioning, restart it. Re-verify the proper function of the PDC emulator. If it is still not working properly, attempt to transfer the PDC emulator role to another domain controller. If you cannot, remove the domain controller from the network and seize the PDC emulator role on another domain controller.
- If the domain controller that holds the PDC emulator role has failed, seize the PDC emulator role on another domain controller. Remove the original domain controller from the network and do not reconnect it until it has been repaired and demoted to member server status in the domain.

> 📖 For steps about transferring or seizing the PDC emulator role, refer to Question 8.

Q.7: How does domain time sync work?

A: Active Directory domains rely on synchronized time for a number of key operations. For example, all Kerberos messages passed between domain members and domain controllers have a maximum default lifetime of 5 minutes. This limitation is intended to make the messages useless to attackers who might capture the messages on the network; by the time the attacker is able to decrypt and modify the packet (if the attacker is able to do so at all), the message will be useless.

> ✎ Active Directory replication is not especially time-sensitive and only uses timestamps as a tiebreaker in certain circumstances.

If time synchronization fails, the operations that depend upon it can also fail. For example, suppose a client computer has a local time of 10:00am, and its closest domain controller has a local time of 10:06am. Kerberos packets time-stamped by the client will be considered out of date by the domain controller even if those packets arrive immediately. The domain controller will reject the logon attempt, and the client will display a generic logon failure message—making it a difficult problem to detect without careful detective work. Understanding how the time sync process works is important to keeping the process running smoothly and solving any problems that occur.

The Components

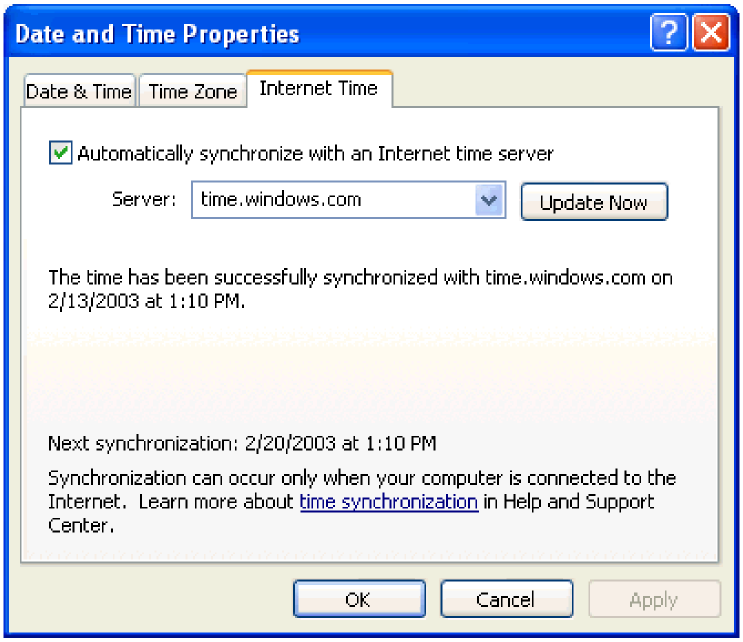
Windows 2000 (Win2K) and later include the Windows Time (W32Time) service, which is configured as a standard Windows background service to start automatically and to log on as the special LocalSystem account. This service is a Microsoft implementation of a Request for Comment (RFC)-compliant Simple Network Time Protocol (SNTP) client and server.

For more information about SNTP, refer to the Internet Engineering Task Force (IETF) RFC 2030.

The Windows Time service originally provided in the Windows NT resource kit is not compatible with W32Time. However, Microsoft makes an NT-compatible W32Time service, which allows NT computers to participate in Active Directory domain time sync. Obtain the updated service from Microsoft.

Non-Member Computers

Computers that aren't members of a domain don't automatically synchronize time. However, because the W32Time service is a standard SNTP client, you can configure it to synchronize with any available SNTP server. To do so, simply double-click the clock in the computer's taskbar, and select the Internet Time tab, which Figure 7.1 shows.



☑ Automatically synchronize with an Internet time server

Server: time.windows.com

The time has been successfully synchronized with time.windows.com on 2/13/2003 at 1:10 PM.

Next synchronization: 2/20/2003 at 1:10 PM

Synchronization can occur only when your computer is connected to the Internet. Learn more about time synchronization in Help and Support Center.

Figure 7.1: Manually configuring time sync.

As Figure 7.1 shows, Windows XP Professional includes a number of preconfigured Internet time servers, including one made available by Microsoft. Other time sources include the official United States government time server at http://www.time.gov.

Obviously, time sync can only occur when the computer is connected to the Internet, so it works best if your computer utilizes an always-on broadband connection. However, Windows will automatically detect a network connection—such as a dial-up connection—and attempt time sync when necessary. By default, Windows attempts to sync about every 8 days.

> ✎ Windows doesn't synchronize the system date only the time. Furthermore, Windows won't synchronize the time if the date isn't correctly set.

Member Computers

Within a domain, time synchronization is a good deal more complex because there are so many computers that need to be in sync with one another. At the top of the time sync authority list is the domain controller that holds the PDC emulator role in the forest root domain. That domain controller is considered the most authoritative source for time information in the entire forest, and the time sync process attempts to bring all other domain clocks into sync with that domain controller.

All domain controllers within a domain attempt to synchronize time. If possible, they try to find a reliable time service in their parent domain. If unavailable, they'll try for a reliable time service in their own domain. Generally, the reliable time service is held by the domain controller that holds the PDC emulator role for the domain. This query process of determining a reliable time service is a bit complex, and I'll cover it in more detail next.

All domain controllers holding the PDC emulator role will try to sync time with the PDC emulator of their parent domain. This behavior creates an easy-to-understand hierarchy of time sync leading up to the forest root domain's PDC emulator.

All client computers synchronize time with the domain controller that authenticates them to the domain. The key, then, is in how domain controllers (other than those holding the PDC emulator role) decide which computer to synchronize time with.

Domain Controllers

Domain controllers will nearly always select their parent domain's PDC emulator as their time source. However, if that computer is unavailable or does not respond promptly, they will attempt to instead synchronize with their own domain's PDC emulator. Each domain controller's selection is based upon an initial query; if, for example, the parent domain's PDC emulator doesn't quickly respond to the initial query, the domain controller will be more likely to choose the PDC emulator from its own domain.

The entire time sync process for domain controllers ranks time sources by *stratum.* Stratum one is an external time source, such as the US Naval Observatory (which I'll discuss in the next section). The forest root PDC emulator represents stratum two. All domain controllers accessing time from the forest root PDC emulator are stratum three, and any domain controllers that get their time from *them* (the domain controllers accessing time from the forest root PDC emulator) are in stratum four, and so forth. Each stratum is progressively less accurate due to network latency, local clock inaccuracies, and so forth.

Windows includes the ReliableTimeSource registry entry, which optimizes time synchronization. When set to 1 on a domain controller, the Netlogon service on that domain controller broadcasts an announcement that the domain controller is a reliable time service. Other domain controllers will prefer a reliable time service if one is available. Generally, this registry entry should only be set to 1 when the computer is in stratum two (synchronizing with an external time source).

When a domain controller starts, it will attempt to locate a time source:

- In the same site
- Marked as a reliable time source (stratum two)
- In the parent domain (which by definition will be in a higher stratum)
- That is a PDC emulator

These attributes are ranked from most important to least important, and result in a selection preference something like the following order (from most preferred to least preferred):

- Parent domain controller, same site, marked as reliable
- Local domain controller, same site, marked as reliable
- Parent domain controller, same site, not marked as reliable
- Local PDC emulator, same site, not marked as reliable
- Parent domain controller, not the same site, marked as reliable
- Local domain controller, not the same site, marked as reliable
- Parent domain controller, not the same site, not marked as reliable
- Local PDC emulator, not the same site, not marked as reliable

This list can enable you to determine which time source a domain controller will attempt to select. Keep in mind that if such a source is available but is too busy to respond to a domain controller's initial query, the domain controller will try to find the next preferred source on the list.

> ✎ Computers will never choose themselves to sync with. They'll move on to the next preferred source on the list, if necessary.

The Forest Root PDC Emulator

The PDC emulator in the forest root domain does not attempt to synchronize time with anyone; it considers itself authoritative by default. For the best time synchronization, however, you should configure this domain controller to synchronize with an authoritative, Internet-based time source. To do so, open a command-line window on the domain controller. Run

```
net time /setsntp:server
```

replacing *server* with the fully qualified name of an authoritative time source.

The US Naval Observatory is considered the United States' official source of time. The observatory maintains a cesium-based atomic clock that is the most accurate timepiece in the world. This clock is connected to several Internet-based time servers that can be used by the public (including ntp2.usno.navy.mil and tock.usno.navy.mil). Note that the SNTP protocol uses UDP port 123 by default, so your domain controller will need access to the Internet on that port in order to sync time.

☞ If your network spans multiple time zones, you should always configure your forest root PDC emulator to synchronize with an authoritative outside time source. Doing so will ensure that your entire network receives authoritative time, and that time-dependent network operations will work as smoothly as possible.

🕮 For Microsoft's documentation about configuring a time source, see the Microsoft articles "How to Configure an Authoritative Time Server in Windows 2000" and "How to Configure an Authoritative Time Server in Windows XP."

Adjusting Time

When computers sync time, they don't necessarily make an instant, radical adjustment to their local clocks. Doing so could disrupt other processes, so the time sync process takes a more gradual approach.

First, the W32Time service exchanges network packets with its selected time source to determine network latency. Doing so provides an internal adjustment based on how much time is required for time sync packets to physically cross the network, and is measured in nanoseconds.

Next, the service examines the target time provided by its times source. If the target time is ahead of the current local time, the service immediately adjusts the local time to the target time. A slow local clock can be a major problem for Kerberos and other operations, so any other potential disruptions by the sudden shift in time are considered secondary concerns.

✎ The actual formula used to calculate target time is specified in RFC 1769, and is LocalClockOffset = ((ReceiveTimestamp – OriginateTimestamp) + (TransmitTimestamp – DestinationTimestamp)) / 2, which accounts for network latency.

If the target time is behind the current local time, the local time is slowed until it equals the target time. Effectively, local time will begin to pass more slowly until the target time catches up. However, if the local time and target time are more than 3 minutes out of sync, the local clock is immediately adjusted to match the target time.

Time sync normally occurs about every 45 minutes by default. Once time sync has successfully completed at least three times, the period is extended to 8 hours, and remains at that setting so long as each attempt to sync is successful. If any attempt fails, time sync reverts back to 45 minutes.

✎ Sync periods are more frequent than 8 days for computers that use the Kerberos protocol because time is so important to this protocol.

Q.8: How do I move FSMO roles from one domain controller to another?

A: On occasion, you might need to transfer one or more Flexible Single Master Operation (FSMO) roles from one Active Directory domain controller to another. Perhaps the domain controller holding the FSMO has failed, or you simply need to relocate the FSMO role to optimize Active Directory performance.

📖 For information about how the FSMO roles work and what they do, see Question 1.

There are two means of transferring FSMO roles: *seizing* and what I'll refer to as a *peaceable* transfer. In a peaceable transfer, which Microsoft documentation simply refers to as a *transfer,* the domain controller already holding the FSMO role is online and functioning perfectly, and you're usually transferring the role to optimize domain performance. This situation is ideal, and I prefer to accomplish the transfer through the various Active Directory consoles. However, if the domain controller holding the FSMO has failed, you might need to seize the role from a different domain controller, which I prefer to accomplish with command-line tools.

💣 Seizing a FSMO role can result in problems if the original domain controller is ever returned to service. I'll discuss these concerns in more detail for each FSMO role.

Transferring the Schema Master Role

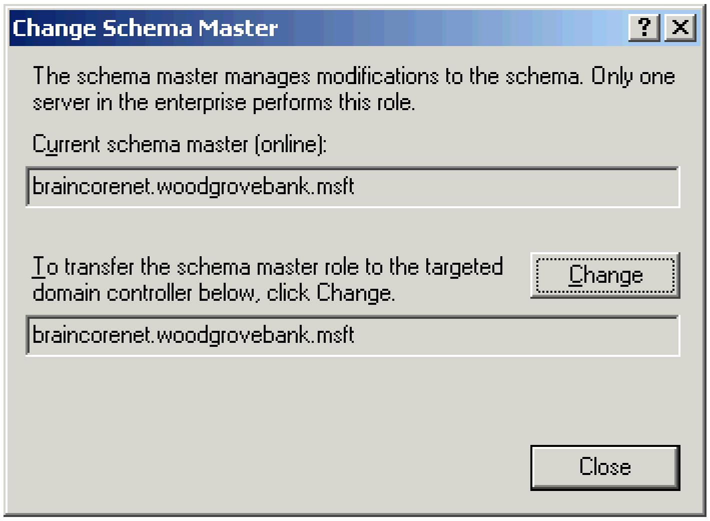
You accomplish a peaceable transfer of the schema master by using the Schema console. By default, Windows does not provide a preconfigured Schema console or even make the console snap-in available for your use. Follow these steps to gain access to the Schema console:

1. Open a command prompt window.
2. Change to the \Windows\System32 folder.
3. Run

   ```
   regsvr32 schmmgmt.dll
   ```

   to register the Schema snap-in.
4. Close the command prompt window.
5. Open a blank Microsoft Management Console (MMC) window.
6. From the File menu, choose Add/Remove Snap-In.
7. Click Add.
8. Locate Active Directory Schema in the list, and double-click it.
9. Click Close, then click OK.

To transfer the schema master, right-click Active Directory Schema, and select Operations Master from the pop-up menu. You'll see the Change Schema Master dialog box, which Figure 8.1 shows.



Change Schema Master

The schema master manages modifications to the schema. Only one server in the enterprise performs this role.

Current schema master (online):

braincorenet.woodgrovebank.msft

To transfer the schema master role to the targeted domain controller below, click Change.

braincorenet.woodgrovebank.msft

Figure 8.1: Changing the schema master role.

Click Change, and select the domain controller that you want to hold the schema master role.

To seize the schema master role:

1. Open a command prompt window.
2. Run Ntdsutil.
3. At the Ntdsutil command prompt, enter

   ```
   roles
   ```

4. Enter

   ```
   connections
   ```

5. Enter

   ```
   connect to server servername
   ```

   providing the fully qualified name of the domain controller that you want to seize the schema master role.

6. Enter

   ```
   qui
   ```

7. Enter

   ```
   seize schema master
   ```

After you seize the schema master, do not return the original schema master domain controller to the network. Doing so will result in an authority conflict. If you are able to repair the original domain controller, first demote it to a member server while it is disconnected from the network, reconnect it, then reinstall Active Directory using DCPromo.

Transferring the Domain Naming Master Role

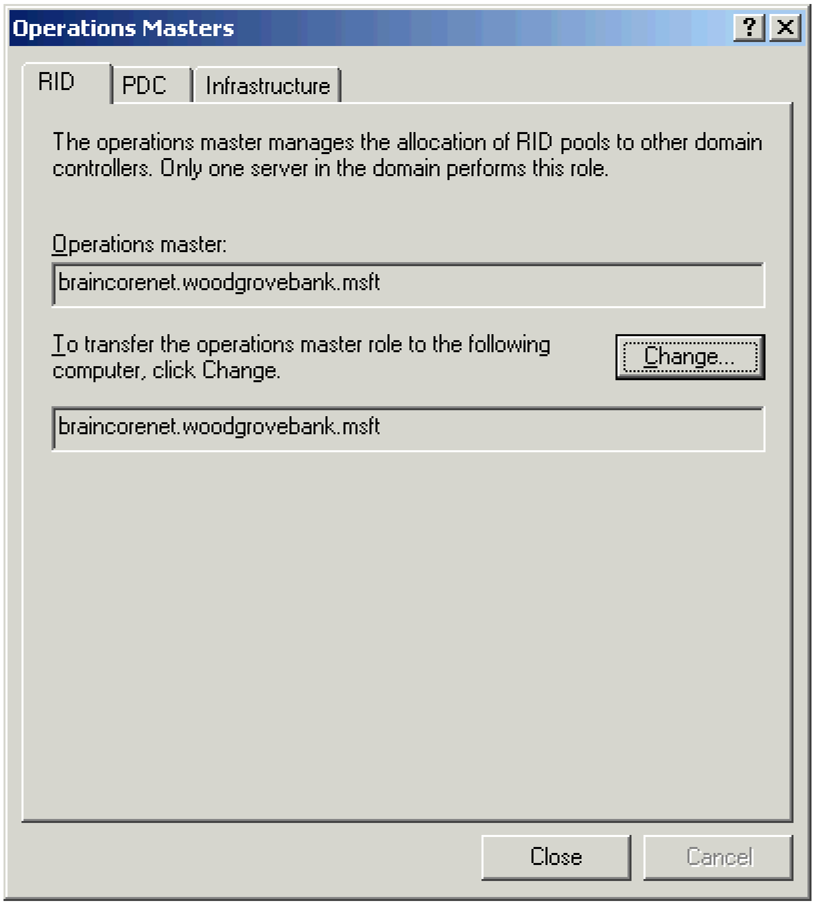
The process of transferring the domain naming master role involves basically the same steps as transferring the schema master does. However, rather than using the schema console, you'll use the Active Directory Domains and Trusts console on the domain controller that currently holds the role. Simply right-click Active Directory Domains and Trusts in the console, and select Operations Masters from the pop-up menu.

Seizing this role requires the use of the Ntdsutil command-line utility. Run the utility as described for seizing the schema master role, but enter seize domain naming master at the appropriate prompt.

If you are forced to seize the domain naming master role, do not return the original domain controller to the network until it has been demoted to member server status.

Transferring the RID Master, Infrastructure Master, or PDC Emulator Roles

Transferring the RID master, infrastructure master, or PDC emulator roles involves basically the same steps as transferring the schema master role. However, rather than using the schema console, you'll use the Active Directory Users and Computers console, which is configured by default on every domain controller. Simply right-click the appropriate domain in the console, and select Operations Masters from the pop-up menu. You'll see a dialog box similar to the one that Figure 8.2 shows, which provides a separate tab for transferring each of the three domain-specific roles.



The operations master manages the allocation of RID pools to other domain controllers. Only one server in the domain performs this role.

Operations master:

braincorenet.woodgrovebank.msft

To transfer the operations master role to the following computer, click Change.

braincorenet.woodgrovebank.msft

Figure 8.2: Transferring the domain-specific FSMO roles.

Seizing these roles also requires the use of the Ntdsutil command-line utility. Run the utility as described for seizing the schema master role, but enter the appropriate seize command at the appropriate prompt:

- To seize the PDC emulator role, use seize PDC.
- To seize the infrastructure master role, use seize infrastructure master.
- To seize the RID master role, use seize rid master.

> If you are forced to seize any of these roles, do not return the original domain controller that held the role to the network until that domain controller has been demoted to member server status. Although this step isn't strictly necessary with the PDC emulator role (the original holder of the role will generally "let go" when it comes back online), I prefer safe over sorry and always demote the original holder before returning it to the network.

Q.9: I have users who can't log on to the domain for some reason. How do I find the cause of the problem?

A: A number of different problems can lead to users (or computers) being unable to authenticate to the domain. To easily resolve these problems, you need an ordered troubleshooting methodology that simply moves from one possibility to another until you arrive at the actual root cause of the problem.

Symptoms

The symptoms of this problem are obvious: Users can't log on to the domain. However, keep in mind that an underlying problem might be that the user's client computer might not be logging onto the domain either. Client computers that are domain members maintain their own security account in the domain, and must authenticate to the domain before they are able to log on a user account. Normally, client computers attempt to authenticate to the domain as soon as Windows starts. Log on locally and check the System and Security event logs for error messages that indicate that the computer was unable to authenticate.

> I'll assume that you've already attempted to reset the user's domain password, checked the Caps Lock key, and the other common culprits of logon problems. For the sake of this discussion, I'm assuming that the user's domain password isn't the problem.

Verification

First, ensure that the computer is authenticating to the domain. You can use the Nltest utility from the Support Tools package on the Windows CD-ROM to verify authentication. If authentication isn't working, use the same verification steps presented here, but focus on the computer's domain account rather than the user's account.

Can the Domain Controller Be Found?

First, verify that the computer is able to locate a domain controller. Check the System event log of the client computer for messages indicating that a domain controller couldn't be found. If error message are present, troubleshoot the domain controller location process.

> For more information about how to do so, see Question 3 and Question 4.

You can also force the domain controller location process to run by using the Nltest support tool and running

```
Nltest /dsgetdc:domain
```

on a client computer (replacing *domain* with the appropriate domain name). If Nltest fails to locate a domain controller, you've found your logon problem.

Is Time Synchronized?

By default, Windows' Kerberos authentication protocol allows for a 5-minute difference between the clocks of client computers and domain controllers. Kerberos messages are time-stamped at their source and cannot be more than 5 minutes old when they arrive at their destination. If your computers are not time-synchronized correctly, packets might be considered old by the destination even if they arrive almost immediately.

💣 You can configure your domain security policies to allow a longer period of time difference. However, doing so makes your network more vulnerable, as it gives attackers additional time to decrypt and re-use Kerberos messages captured from the network. Rather than extending the Kerberos time tolerance, you should correct the time synchronization problem.

Checking time synchronization is easy: Simply check the clocks on the client computer and a domain controller. If they are more than a minute or two off, troubleshoot time synchronization problems.

📖 For information about how to troubleshoot time sync problems, see Question 7, and check out Question 5 for steps on manually correcting a time sync problem.

Is the Computer Account Valid in the Domain?

Use Active Directory Users and Computers to verify that the computer's domain account isn't locked out or disabled. Also, a computer account that has been cloned from one domain to another can cause problems until the original source account is deleted. If event log messages on the client computer continue to indicate logon problems, you might need to reset the computer's domain account.

📖 For step-by-step instructions, see Question 2.

Corrective Action

Corrective action for logon problems will be determined by the root cause of the problem:

- If the client computer is unable to locate a domain controller, troubleshoot and resolve that problem.
- If the client computer's time is out of sync with the domain, troubleshoot and resolve that problem or manually synchronize the time. Note that a manual synchronization will not permanently resolve the problem.
- If the client computer's domain account isn't working, resolve that problem. Doing so might require you to re-enable the account or even reset it.