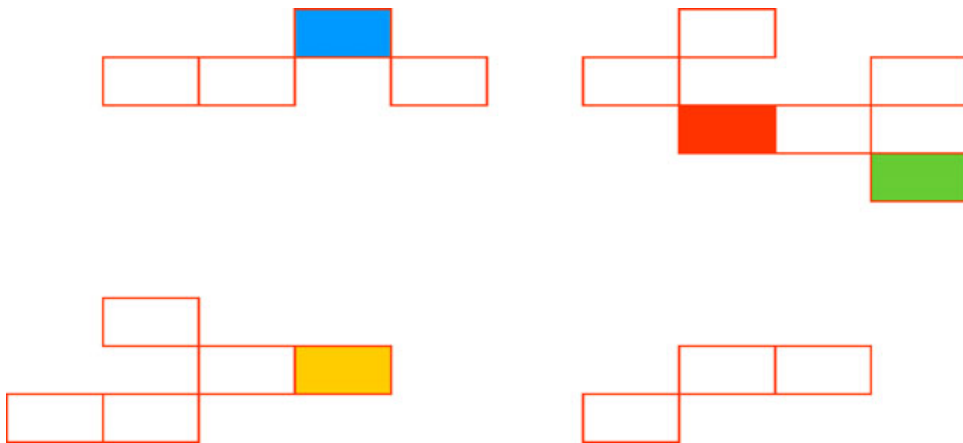
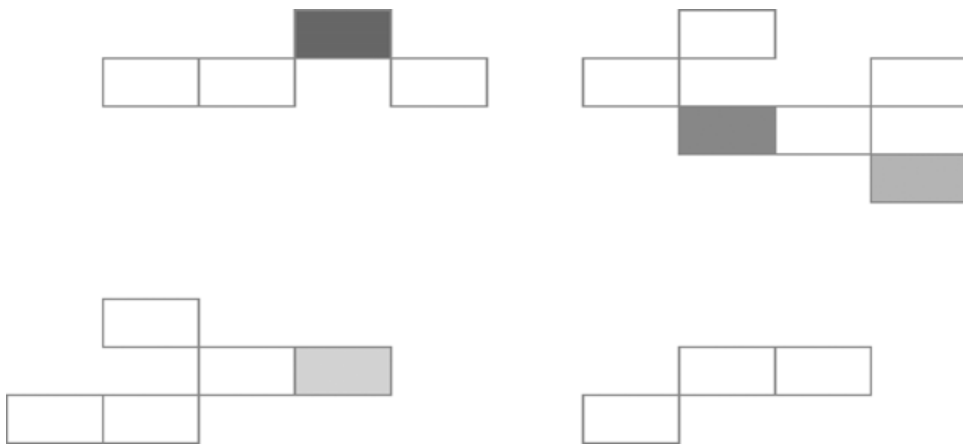


Understanding and Troubleshooting Directory Access



Paul Bowden, Michele Martin,
Scott Roberts

Understanding and Troubleshooting Directory Access



**Paul Bowden, Michele Martin,
Scott Roberts**

Copyright

The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication. Because Microsoft must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

Unless otherwise noted, the example companies, organizations, products, domain names, e-mail addresses, logos, people, places and events depicted herein are fictitious, and no association with any real company, organization, product, domain name, email address, logo, person, place or event is intended or should be inferred.

© 2002 Microsoft Corporation. All rights reserved.

Microsoft, Active Directory, MSDN, Outlook, Windows, and Windows NT are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Writers: Paul Bowden, Michele Martin, Scott Roberts

Technical Reviewers: Tom Larson, Rafiq El Alami, Vladimir Grebenik

Project Editor: Megan Bradley

Designer: Kristie Smith

Published: November 2002

Applies To: Exchange 2000 Server SP3

Table of Contents

Introduction	1
Chapter 1	
Understanding How Directory Access Works	3
What Is DSAccess?	3
What Is DSProxy?	5
What Is the Categorizer?	5
How DSAccess Discovers the Active Directory Topology	6
How DSAccess Assigns Active Directory Server Roles	9
How DSProxy Performs Outlook Address Book Lookups	14
How the Categorizer Works	23
Chapter 2	
Directory Access in Large Active Directory Environments	25
Calculating Active Directory Load	25
Event Logging	26
Server Failures and Their Effect on Exchange 2000	28
Server Promotion and Its Effect on Exchange 2000	35
Server Demotion and Its Effect on Exchange 2000	40
Manual Topology Definition	42
Static Port Mappings	48
DSAccess Cache	49
DSAccess in a Perimeter Network	49
Chapter 3	
Directory Access Troubleshooting Checklist	53
Step 1. Look for Errors in the Event Logs	53
Step 2. Monitor Performance Counters	56
Step 3. Check that DNS is Configured Properly	58
Step 4. Verify the Configuration of Active Directory Sites	58

Step 5. Verify the Correct Operation of the Domain	59
Step 6. Look at the DSAccess Roles.....	59
Step 7. Verify the Health of Each Active Directory Server	59

Appendix A

Sample Registry File.....	63
----------------------------------	-----------

Appendix B

Common RPC and LDAP Error Codes	65
--	-----------

RPC Error Codes.....	65
LDAP Error Codes.....	65

Additional Resources

Microsoft Knowledge Base.....	71
-------------------------------	----



Introduction

This document discusses the interaction between Microsoft® Exchange Server 2000 and Microsoft Active Directory® directory service. Unlike earlier versions of Exchange, Exchange 2000 does not have its own directory service; instead it relies entirely on Active Directory for configuration and user information.

In large companies, Active Directory designs can be complex. Understanding how Exchange 2000 interacts with Active Directory domain controllers and global catalog servers will help you design a high-performance, reliable Exchange 2000 service.

This paper discusses three Exchange 2000 directory access components:

- Directory Service Access (DSAccess)
- Directory Service Proxy (DSProxy)
- Categorizer

These components perform separate tasks, but they depend on each other. If DSAccess has difficulty communicating with Active Directory, DSProxy and the Categorizer will have the same difficulty.

2 Understanding and Troubleshooting Directory Access

The goal of this document is to enable Active Directory and Exchange 2000 designers to make the best possible decisions when deploying servers, and to help administrators troubleshoot any directory access problems that occur. To fully understand the concepts in this document, you should have a working knowledge of Active Directory and Exchange 2000.

Caution This document contains information about changing settings in the registry. Using Registry Editor incorrectly can cause serious problems that may require you to reinstall your operating system. Microsoft cannot guarantee that problems resulting from the incorrect use of Registry Editor can be solved. Before editing the registry, back up any valuable data. Use Registry Editor at your own risk.

For information about how to edit the registry, see the “Changing Keys and Values” Help topic in Registry Editor (Regedit.exe), or the “Add and Delete Information in the Registry” and “Edit Registry Data” Help topics in Regedt32.exe. Note that you should back up the registry before you edit it. If you are running Microsoft Windows NT® or Microsoft Windows® 2000, you should also update your Emergency Repair Disk (ERD).

1

Understanding How Directory Access Works

This section describes each of the Exchange 2000 directory access components and explains how the core technology works in a stable Active Directory environment.

What Is DSAccess?

DSAccess is a core component of Exchange 2000 that is implemented as a DLL file named DSACCESS.DLL. The purpose of DSAccess is to control how other Exchange components access Active Directory. DSAccess discovers the Active Directory topology, detects domain controllers and global catalog servers, and maintains a list of valid directory servers that are suitable for use by Exchange components. If the status of a domain controller or global catalog server changes, DSAccess updates its list. In addition, DSAccess contains a memory cache, which reduces the load on Active Directory by reducing the number of Lightweight Directory Access Protocol (LDAP) requests that individual components must send to Active Directory servers.

The core components of Exchange 2000 require access to the directory. Therefore, they rely on DSAccess to provide a current list of Active Directory servers. For example, the message transfer agent (MTA) routes LDAP queries through the DSAccess layer to Active Directory. The store process uses DSAccess to obtain configuration information from Active Directory in order to connect to databases. The transport process uses DSAccess to obtain information about the connector arrangement in order to route messages. If each of these Exchange 2000 components had a separate mechanism for performing Active Directory lookups, Exchange 2000 would become disjointed and less scalable. In Exchange 2000, DSAccess is the centralized mechanism that determines the Active Directory topology, opens the appropriate LDAP connections, and works around server failures.

The following table (Table 1) contains a list of components that depend on DSAccess.

Table 1 Components that depend on DSAccess

Component	Dependency on DSAccess
Exchange Metabase Update (DS2MB)	Directory changes tracked by update sequence number (USN)
Exchange Routing (RESVC)	User and configuration lookups
SMTP Categorizer (SMTP CAT)	List of global catalog servers in the topology
Directory Service Proxy (DSProxy)	List of global catalog servers in the topology
Exchange Information Store	User and configuration lookups
WebDAV	User and configuration lookups
Message transfer agent (MTA)	User and configuration lookups
Instant Messenger	User and configuration lookups

What Is DSProxy?

DSProxy is the Exchange 2000 component that provides an address book service to Microsoft Outlook® clients. DSProxy is implemented as a DLL file named DSPROXY.DLL. DSProxy has two functions:

- To emulate a Messaging Application Programming Interface (MAPI) address book service, and proxy requests to an Active Directory server
- To provide a referral mechanism so that Outlook clients can directly contact Active Directory servers

Although its name implies that it provides proxy services only, DSProxy provides both proxy and referral services. MAPI clients running Outlook 2002 Service Release 1 (SR-1) and earlier versions (including Outlook 2000, Outlook 98, Outlook 97, and the Exchange 5.0 client) use the proxy functionality. These earlier clients were designed with the assumption that each Exchange server contains a directory service. This is no longer true in Exchange 2000. Therefore, DSProxy emulates a directory service so that these earlier clients can continue to function. In actuality, however, the Exchange 2000 server forwards the requests to Active Directory.

Later versions of Outlook, such as Outlook 2000 (SR-2 and later) and Outlook 2002, are designed with the assumption that Exchange 2000 does not have its own directory service. After DSProxy refers one of these later clients to a global catalog server, the client communicates directly with Active Directory.

DSProxy obtains its list of working global catalog servers from DSAccess, but it does not route its queries through DSAccess. This is because DSProxy uses the Name Service Provider Interface (NSPI) to submit MAPI address book lookups. DSAccess handles only LDAP queries.

What Is the Categorizer?

The Categorizer is a component of the Exchange 2000 transport process. When a message is submitted to the transport process, the Categorizer uses the header information on the message to query Active Directory for information about how and where the message must be delivered. For example, from a Simple Mail Transfer Protocol (SMTP) address such as someone@example.com, the Categorizer identifies the Exchange 2000 server that contains the users mailbox and determines how to route the message to the server. The Categorizer also expands distribution lists and applies per-user limits to messages.

The Categorizer relies on DSAccess for the list of Active Directory servers that it should use for lookups; however, like DSProxy, it uses its own mechanism to read information from Active Directory after it has the server list.

How DSAccess Discovers the Active Directory Topology

Understanding how Exchange 2000 discovers the Active Directory topology is key to designing a reliable system. DSAccess relies on a well-designed Active Directory Site structure. As you will see later in this document, if the Active Directory Sites have been poorly configured, Exchange 2000 will not work properly. For example, if your site link costs are not set properly, the Exchange 2000 server may bind to a domain controller over a WAN connection, rather than a LAN connection. Not only will the server perform poorly, but Outlook will perform poorly and experience errors.

Exchange 2000 also requires a well-designed Domain Name System (DNS) implementation. If DNS has been poorly configured, Exchange 2000 will not work.

The key to optimal Active Directory access is identifying which domain controllers and global catalog servers are available at the lowest network cost. This section provides a high level overview of the discovery process DSAccess uses to accomplish this goal.

Note The discovery process described in this section was introduced in Exchange 2000 Service Pack 2 (SP2). In earlier versions of Exchange, DSAccess used remote procedure calls (RPCs) to locate Active Directory servers. In SP2, DSAccess no longer used RPCs to locate Active Directory servers during the discovery process. Eliminating the use of RPCs enables DSAccess to operate in perimeter networks where RPC traffic across the internal firewall is prohibited.

Discovery Process

Upon startup, DSAccess uses a discovery process to identify the network topology and assess the availability of directory servers. Every 15 minutes thereafter, DSAccess uses an almost identical process to rediscover the topology and check for any changes in server availability.

Note If you have hard coded the domain controllers you want DSAccess to use, DSAccess will skip the discovery process and check server suitability only.

The following list outlines the discovery process, noting differences between initial discovery and rediscovery:

1. DSAccess opens an LDAP connection to a randomly chosen domain controller from the local domain. This server is referred to as the “bootstrap” server.
2. DSAccess conducts an LDAP search to identify local domain controllers and global catalog servers. DSAccess determines server suitability and assigns server roles.
3. DSAccess conducts an LDAP search to determine if one or more secondary sites are connected to the local site. If secondary sites exist, DSAccess sorts the **siteLink** objects for each site from lowest cost to highest cost. (Administrators preassign these numeric costs to reflect the relative bandwidth between sites. Messages are routed between sites according to lowest cost.) DSAccess places the lowest cost sites in a secondary topology list.
4. DSAccess conducts an LDAP search to identify the domain controllers and global catalog servers that are located in the secondary topology sites.
5. DSAccess identifies the full topology and compiles a list of working domain controllers and a list of working global catalog servers.

Note By default, DSAccess initialization during startup must finish within one minute; otherwise, DSAccess stops. One minute is usually long enough for DSAccess to initialize. If initialization takes longer, there might be a problem with the network or topology configuration. Although you can extend the time-out parameter by setting a registry key, you should first determine why initialization is taking longer than expected. (The registry key that extends the time-out parameter is located under **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\MSExchangeDSAccess\TopoCreateTimeoutSecs.**)

Determining Server Suitability

Exchange components rely on DSAccess to identify Active Directory servers and determine whether domain controllers and global catalog servers are suitable for use. During both initial discovery and ongoing rediscovery, DSAccess determines server suitability and then logs the results of suitability checks in event 2080 in the application log (for more information about event 2080, see “Directory Access Troubleshooting Checklist” later in this document).

DSAccess uses the following criteria to determine server suitability:

- **Reachability** Depending on the type of server object (domain controller or global catalog server), DSAccess must be able to reach the server over the network through either the domain controller port 389 or the global catalog server port 3268.
- **Access rights** DSAccess reads the security descriptor of the configuration naming context object (**ConfigNC**) on the server. If the security descriptor cannot be read, the server is not suitable.
- **Domain preparation** The directory server must be located in a domain in which DomainPrep has been run.
- **Synchronization** DSAccess checks whether the server is synchronized.
- **NetLogon** DSAccess sends a DSGetDcName RPC to the directory server to test its general suitability. If the directory server is not synchronized, is out of disk space, or is experiencing other problems, it will not advertise itself as a directory server.

Important In a perimeter network where RPC traffic is not allowed, the NetLogon check cannot occur. However, the NetLogon check will continue to issue RPCs until it fails, which can take a long time. Because repeated NetLogon checks decrease performance, you should stop DSAccess from issuing NetLogon checks by creating the **DisableNetLogonCheck** registry key. For more information, see “Directory Access in Perimeter Networks” later in this document.

- **DNS priority and weight** Each domain controller and global catalog server has a Service (SRV) resource record, which contains both a priority value and a weight value. The administrator preassigns these values to reflect how servers should be load balanced. DSAccess uses only the weight value to determine which server the client should prefer; therefore, administrators can use the priority value to control Active Directory load generated by logons, and the weight value to control Active Directory load generated by Exchange. A higher weight results in a higher probability that DSAccess will choose a server. DSAccess treats a weight of 0 the same it treats a weight of 1. If DSAccess cannot read the weight, it uses a default weight of 100.
- **FSMO primary domain controller role owner** If your topology contains Windows NT servers, the flexible single master operation (FSMO) primary domain controller (also known as a PDC) server will experience heavy loads. To avoid performance problems, you should exclude FSMO primary domain controller servers from DSAccess by setting the **MinUserDc** registry key. (For more information, see “Excluding the FSMO Primary Domain Controller Role” later in this document.)

- **Critical data** The server must contain a minimum set of critical data. For example, the local Exchange server object must be present in the Exchange configuration container.
- **Residential site** DSAccess prefers local Active Directory servers to servers located in other sites.

How DSAccess Assigns Active Directory Server Roles

As described in the previous section, during the discovery process DSAccess identifies all of the servers that are suitable for use by Exchange components. From this list of servers, DSAccess identifies servers that fulfill three key roles:

- **Configuration domain controller** The single domain controller that reads and writes information in the configuration naming context in Active Directory. DSAccess chooses a domain controller or global catalog server to act as the configuration domain controller.
- **Working domain controllers** Up to ten domain controllers that perform Active Directory lookups for objects in the local domain.
- **Working global catalog servers** Up to ten global catalog servers that perform forest-wide queries.

The following sections describe how DSAccess identifies the servers that fulfill these Active Directory roles.

Identifying the Configuration Domain Controller

The configuration domain controller is a single computer that DSAccess chooses to serve as the reference point for Active Directory information. The Active Directory server can be either a domain controller or global catalog server, but it must be a high-performance server that is located on the same local area network as the Exchange 2000 server.

Because there is latency during replication, DSAccess chooses a single server to perform the role of configuration domain controller instead of load balancing among the available Active Directory servers.

Requirements for the configuration domain controller role under normal conditions are as follows:

- The server must be located in a domain in which DomainPrep has been run.
- The server must be located in the same Active Directory Site as the Exchange 2000 server.
- The server must be a domain controller (or global catalog server).

DSAccess uses the selected configuration domain controller for eight hours, after which DSAccess randomly chooses a new configuration domain controller. The following conditions also force DSAccess to choose a new configuration domain controller:

- The Exchange 2000 server restarts.
- The configuration domain controller fails or shuts down.

You can use System Manager to determine which server DSAccess has selected to perform the role of configuration domain controller (Figure 1).

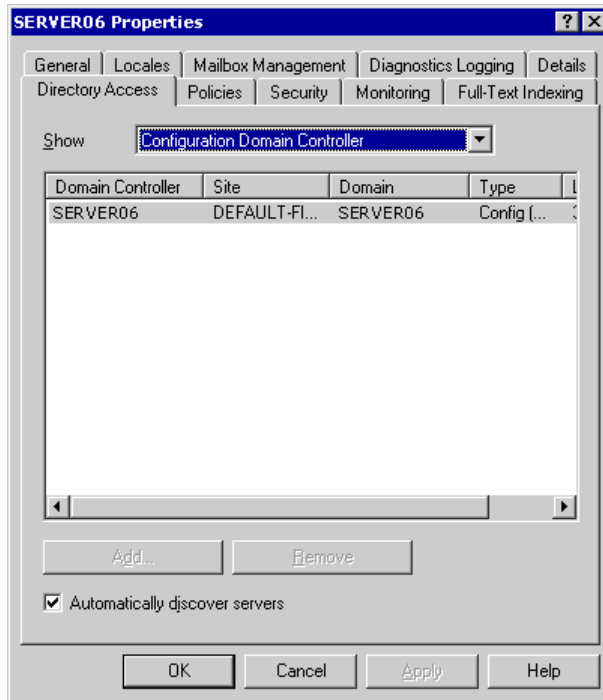


Figure 1 Viewing the configuration domain controller in System Manager

Identifying Working Domain Controllers

DSAccess compiles a list of working domain controllers that Exchange components can use to read nonconfiguration data about the domain. As long as there are no replication issues, all working domain controllers should be up to date. Therefore, DSAccess uses a sequential, round robin mechanism, as well as the individual server response time and the number of outstanding requests, to distribute the requests against multiple domain controllers.

The working domain controller list is composed of up to ten Active Directory servers that meet the following criteria:

- The server must be located in a domain in which DomainPrep has been run.
- The server must be in the same Active Directory Site as the Exchange 2000 server.
- The server must be a domain controller (or global catalog server).
- The server must pass suitability checks.

If the Active Directory site spans domains, the list will contain servers from multiple domains.

In practice, the servers on the working domain controller list are seldom used because they can only provide information about objects in the domains in which they are located. DSAccess tries to use servers from this set whenever possible, but most queries for user information can only be serviced by a global catalog server.

Identifying Working Global Catalog Servers

The working global catalog server list is similar to the working domain controller list. This list can contain up to ten global catalog servers. DSAccess uses a sequential, round robin mechanism, as well as the individual server response time and the number of outstanding requests, to distribute load among these servers.

The working global catalog server list is composed of Active Directory servers that meet the following criteria:

- The server must be located in a domain in which DomainPrep has been run.
- The server must be in the same Active Directory Site as the Exchange 2000 server.
- The server must be a global catalog server.
- The server must pass suitability checks.

If the Active Directory site spans domains, the list will contain servers from multiple domains.

How to View Server Roles

You can view the roles that DSAccess has assigned to specific servers in the application log or System Manager in the following ways, depending on your version of Exchange:

- In Exchange 2000 SP2 and later, the application log lists information about the servers in your topology under event 2080, which reports server roles and suitability. Exchange generates this event only if the MExchangeDSAccess topology logging level is set to **Minimum** or greater. (For more information about changing the logging level and interpreting event 2080, see “Directory Access Troubleshooting Checklist” later in this document.)
- In Exchange 2000 SP2 and later, use System Manager to view the roles DSAccess has assigned to servers. In the server’s **Properties**, click the **Directory Access** tab.

It is extremely important that you review the servers that are assigned the role of working global catalog server, because these servers have the greatest impact on Outlook (MAPI) clients. Only global catalog servers support the NSPI facility, which is required to perform MAPI address book lookups. If DSAccess detects inappropriate global catalog servers, user response times will be affected.

Examples of How DSAccess Assigns Server Roles

The following examples depict different Active Directory configurations and show how DSAccess assigns server roles in each case.

Example 1 – Simple single domain topology

Figure 2 depicts a single Active Directory forest with a single Active Directory domain. The topology consists of two Active Directory sites.

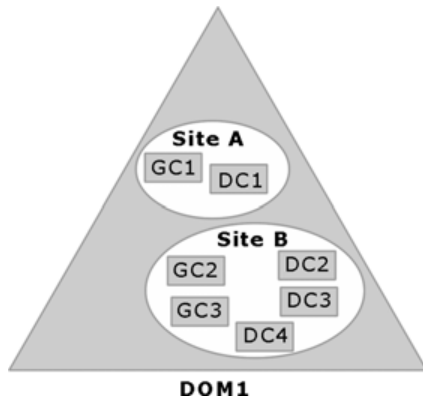


Figure 2 One domain with two sites

If an Exchange 2000 server is placed in Site A, DSAccess detects the following topology:

- **Configuration domain controller role** – DC1, GC1
- **Working domain controller list** – DC1, GC1
- **Working global catalog server list** – GC1

If an Exchange 2000 server is placed in Site B, DSAccess detects the following topology:

- **Configuration domain controller role** –DC2, DC3, DC4, GC2, GC3
- **Working domain controller list** – DC2, DC3, DC4, GC2, GC3
- **Working global catalog server list** – GC2, GC3

Example 2 – Complex topology

Figure 3 depicts a more complex topology. There are two Active Directory domains in the forest, and there are two Active Directory sites. However, Site A spans both domains.

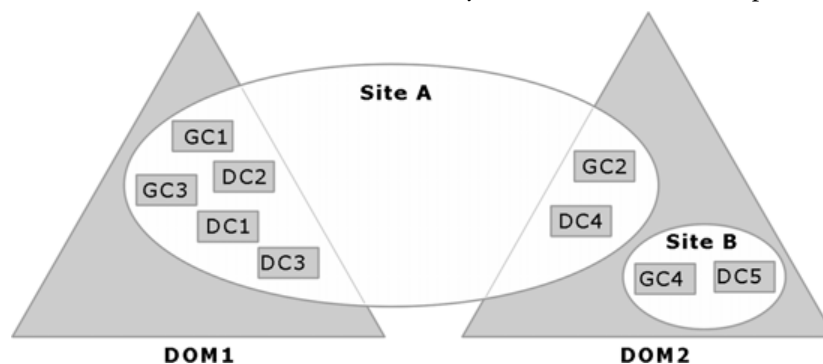


Figure 3 Two domains with a site spanning both domains

If an Exchange 2000 server is installed in the Domain 1 and placed in Site A, DSAccess detects the following topology:

- **Configuration domain controller role** –DC1, DC2, DC3, DC4, GC1, GC2, GC3
- **Working domain controller list** – DC1, DC2, DC3, DC4, GC1, GC2, GC3
- **Working global catalog server list** – GC1, GC3, GC2

If an Exchange 2000 server is installed in Domain 2 and placed in Site A, DSAccess detects the following topology:

- **Configuration domain controller role** – DC1, DC2, DC3, DC4, GC1, GC2, GC3
- **Working domain controller list** – DC1, DC2, DC3, DC4, GC1, GC2, GC3
- **Working global catalog server list** – GC2, GC1, GC3

If an Exchange 2000 server is installed in Domain 2 and placed in Site B, DSAccess detects the following topology:

- **Configuration domain controller role** – DC5, GC4
- **Working domain controller list** – DC5, GC4
- **Working global catalog server list** – GC4

How DSProxy Performs Outlook Address Book Lookups

DSProxy is responsible for ensuring that MAPI clients such as Outlook can perform name resolution. MAPI clients use the Name Service Provider Interface (NSPI) instead of Lightweight Directory Access Protocol (LDAP) to resolve names, because LDAP is not a good protocol for displaying cursor-based address books (such as the Exchange global address list).

NSPI was introduced with the Exchange 4.0 directory service and is still used in Exchange 5.0 and 5.5. Although Exchange 2000 does not include its own directory service, the DSProxy process emulates NSPI and forwards requests to Active Directory servers. DSProxy does not convert NSPI requests into LDAP or any other protocol; it works by simply forwarding the NSPI request that it receives from the client. Therefore, global catalog servers also natively support NSPI. Domain controllers do not support NSPI because they contain directory information for only the local domain and not the entire directory. Keep Outlook clients in mind when designing an Active Directory topology, especially when you are considering placing domain controllers and global catalog servers in separate physical locations.

DSProxy Initialization

After DSAccess builds the list of working global catalog servers, DSAccess forwards the list to DSProxy. In turn, DSProxy removes global catalog servers that are in nonlocal domains. DSProxy dynamically adds and removes servers as required. The resulting server list that DSProxy uses consists of up to ten global catalog servers from the same Active Directory Site and domain as the Exchange 2000 server.

To monitor DSProxy activity, in System Manager, set the NSPI Proxy diagnostics logging level to **Maximum** (Figure 4).

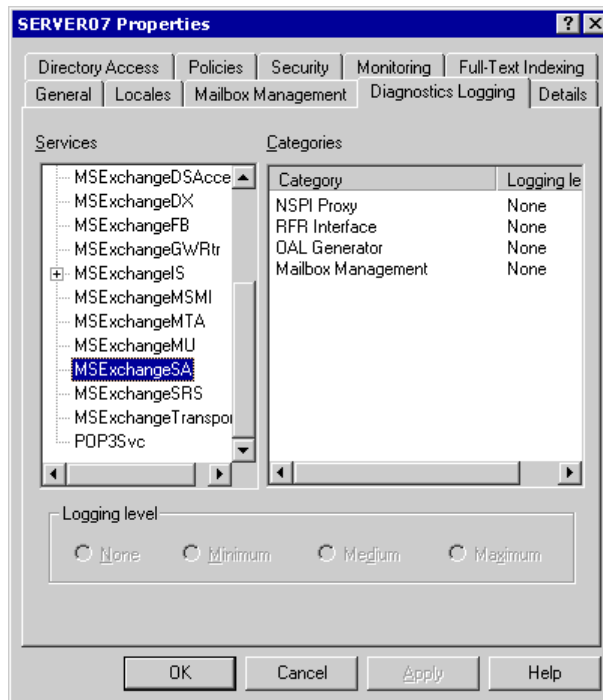


Figure 4 Setting the DSProxy logging level in System Manager

A logging level of **Maximum** is recommended for NSPI Proxy because lower logging levels do not provide much information. Unlike other Exchange 2000 components, a setting of **Maximum** for NSPI Proxy will not overwhelm the event logs with information.

As mentioned earlier, DSProxy has two functions: proxying NSPI requests for older MAPI clients and providing a MAPI referral service (RFR) for newer clients. After you set the logging level to **Maximum** and restart System Attendant, a number of events will appear in the event log:

- MSExchangeSA – General – 9006
Microsoft Exchange System Attendant is loading 'DSPROXY.DLL'.
- MSExchangeSA – General – 9007
Microsoft Exchange System Attendant is initializing 'DSPROXY.DLL'.
- MSExchangeSA – NSPI Proxy – 9027
The NSPI Proxy service is starting.
- MSExchangeSA – NSPI Proxy – 9061

NSPI Proxy created a listening socket on network transport Tcp/Ip. NSPI Proxy will be able to proxy requests made on this transport.

- MExchangeSA – NSPI Proxy – 9058

NSPI Proxy successfully connected to the NSPI Service on server <server> at endpoint 1026 on RPC protocol sequence ncacn_ip_tcp.

- MExchangeSA – RFR Interface – 9058

NSPI Proxy successfully connected to the NSPI Service on server <server> at endpoint 1026 on RPC protocol sequence ncacn_ip_tcp.

- MExchangeSA – NSPI Proxy – 9141

NSPI Proxy's list of targets has been updated. Clients on transport Tcp/Ip will be load balanced amongst the active servers in this list: <servers>

- MExchangeSA – RFR Interface – 9148

Referral Interface's list of targets has been updated. Clients will be referred to a Global Catalog from the following list: <servers>.

- MExchangeSA – RFR Interface – 9069

The Directory Service Referral interface (RFRI) is starting.

- MExchangeSA – RFR Interface – 9075

The Directory Service Referral interface (RFRI) is available on 6 RPC protocol sequence(s). The bindings are listed here: <bindings>

- MExchangeSA – RFR Interface – 9070

The Directory Service Referral interface (RFRI) started successfully.

- MExchangeSA – NSPI Proxy – 9036

The NSPI Proxy started 1 worker thread(s) and 1 listener thread(s) to handle client requests and server responses.

- MExchangeSA – NSPI Proxy – 9028

NSPI Proxy service started successfully.

- MExchangeSA – NSPI Proxy – 9045

NSPI Proxy worker thread (ID: 0x588) is starting.

- MExchangeSA – NSPI Proxy – 9051

NSPI Proxy listener thread (ID: 0x584) is starting. Listening on network transport Tcp/Ip.

DSPProxy Scalability

The startup events show that DSPProxy begins with one worker thread and one listener thread. The NSPI Proxy service is designed to be highly scalable. For every 512 connected clients, DSPProxy creates one additional worker thread. Because additional threads consume a small number of additional resources, you can scale each Exchange 2000 server to many thousands of simultaneous clients. For best performance, you should use newer versions of Outlook (Outlook 2000 or Outlook 2002) that can use the referral service and communicate directly with global catalog servers, rather than communicating through the proxy service.

When Outlook clients send NSPI requests to the directory service, the overhead is insignificant. For example, when resolving a list of names in the **To** field, NSPI generates one RPC request and one RPC response packet. Due to the efficient cursor mechanisms of NSPI, scrolling through the global address list generates only a few packets on the network. Therefore, DSPProxy and NSPI scalability is not a concern.

Unlike DSAccess, DSPProxy does not cache NSPI responses, so each lookup requires a request to and response from the server. Later versions of Outlook include a client-side cache, which reduces the number of requests.

DSPProxy Load Balancing

Although NSPI is a very efficient process, the DSPProxy process uses a load balancing mechanism to ensure that client requests are divided equally among all available global catalog servers.

When a MAPI client contacts NSPI Proxy, the IP address of the requesting client is hashed against the number of available global catalog servers. DSPProxy uses the result to either proxy or refer the client to one of the global catalog servers. This load balancing method enables the client to contact the same global catalog server, thus ensuring consistency. The Directory Service Referral interface (RFRI) uses a different load balancing mechanism; when a client connects to RFRI, global catalog servers are returned in round robin fashion.

Differences Among Outlook Versions

Different versions of Outlook use different methods for connecting to and interacting with Active Directory servers. Table 2 summarizes these differences.

Table 2 How different versions of Outlook interact with Active Directory

Version	Initial connection	General connection	Global catalog server refresh	Dynamic global catalog server failover	Global catalog server locator
Outlook 2002	NSPI	RFR	Yes – Startup, failure, and reconnect	Yes – Fully dynamic within 30 seconds	Client or server (default)
Outlook 2000 SR-2	NSPI	RFR	Yes - Startup	No – Restart required	Server only
Outlook 2000	NSPI	RFR	Yes - Failure	No – Restart required	Server only
Outlook 98	NSPI	NSPI	N/A	No – Restart required	N/A
Outlook 97	NSPI	NSPI	N/A	No – Restart required	N/A
Exchange 5.0	NSPI	NSPI	N/A	No – Restart required	N/A

As shown in Table 2, the various versions of Outlook differ from each other in the following areas:

- **Initial connection** Refers to the method used to communicate with the directory service when a client first logs on with a new profile.
- **General connections** Refers to the mechanism used to contact the directory service when a client logs on after the initial connection.

- **Global catalog server refresh** Indicates whether the client periodically asks for a new referral from the Exchange 2000 server. For example, in the original release of Outlook 2000, a referral is only refreshed if the global catalog server becomes unreachable. In Outlook 2002 Service Pack 2, the referral is refreshed each time Outlook is started. This change prevents Outlook 2000 from continually binding to an inappropriate global catalog server.
- **Dynamic global catalog server failover** Indicates whether the client is capable of dynamically failing over to a different global catalog server if the existing server is unreachable.
- **Global catalog server locator** Indicates whether Outlook contacts the global catalog server based on a server referral, or whether the client can automatically detect the closest global catalog server.

When any MAPI client initially connects to Exchange with a new profile, the client-side address book provider (ESMABP32.DLL) only knows the name of the Exchange server. During the first session, even the latest versions of Outlook use NSPI Proxy. However, while logging out the client will ask for an address book referral, which is stored in the MAPI profile under the following registry key.

Location	HKEY_CURRENT_USER\Software\Microsoft\Windows NT \CurrentVersion\Windows Messaging Subsystem \Profiles\Outlook\dca740c8c042101ab4b908002b2fe182
Name	001e6602
Type	REG_SZ (string)
Value	Fully qualified domain name (FQDN) of the global catalog server

Outlook 2002

Outlook 2002 incorporates many new features and is extremely robust when Active Directory issues occur. If the global catalog server that Outlook is using fails during a client session, Outlook displays a dialog box indicating that it is waiting for a response from the server (Figure 5).

Tip If the server name shown in the **Requesting data...** dialog box is in the FQDN format, Outlook is waiting for a response from the directory service. If you see a short server name, Outlook is waiting for either the mailbox server or public folder server to respond.



Figure 5 Delay while requesting data

If Outlook does not receive a response from the global catalog server within 30 seconds, the client requests a new referral from DSProxy. The referral is saved in the MAPI profile and Outlook dynamically connects to the new global catalog server. The user does not encounter any error messages during failover.

Outlook 2002 refreshes its global catalog referral whenever the client is restarted or a failure occurs. Additionally, if Outlook loses its connection to the Exchange 2000 server, it requests a new referral.

If you turn on diagnostics logging for the RFR Interface category on the Exchange 2000 server, you will see a 9073 event each time the RFR interface generates a referral (Figure 6).

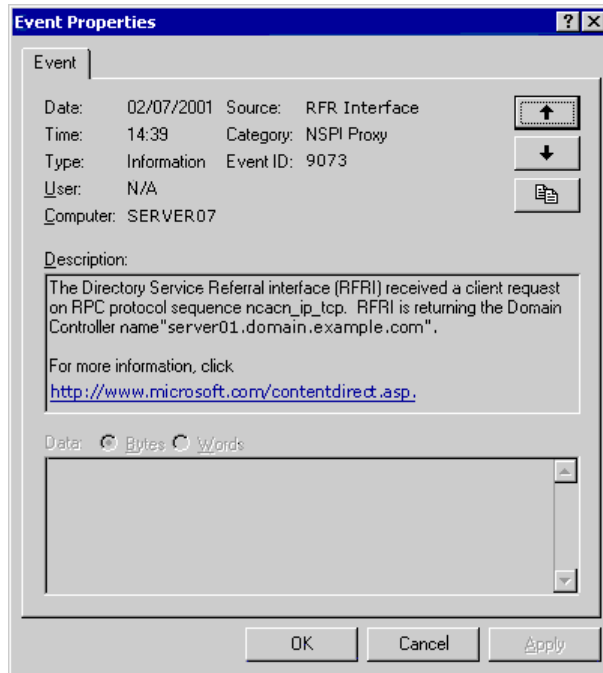


Figure 6 New referral event

By default, Outlook 2002 requests a global catalog referral from DSProxy. This strategy works well in many scenarios. Under some circumstances, however, you may want to configure the client to use a specific global catalog server. For example, the Outlook client and the Exchange server may be separated by a WAN (Figure 7).

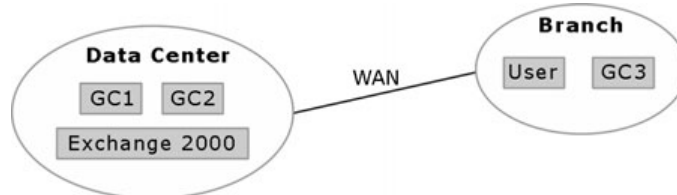


Figure 7 WAN separating Outlook and Exchange server

In Figure 7, the Exchange 2000 topology is centralized with all Exchange 2000 servers located at the data center of the company. Users are located in branch offices, and log on to their mailboxes over the WAN. By default, Outlook receives a referral to either GC1 or GC2. This is because DSProxy identifies the global catalog servers that are closest to the

server running DSProxy, rather than the global catalog servers that are closest to the client. In this example, the Active Directory designers have chosen to implement a global catalog server at the branch office so that logon traffic is kept local.

Although the default referral works, you can optimize traffic patterns by configuring the following registry key so that the client uses the closest global catalog server.

Location	HKEY_CURRENT_USER\Software\Microsoft\Exchange\Exchange Provider
Name	closest GC
Type	REG_DWORD
Value	0x00000001

In other topologies, you may want to force Outlook to communicate with a specific global catalog server. Although you can manually change the registry parameter in the MAPI profile, it will be overridden the next time the client computer starts. To force Outlook 2002 to use a predefined global catalog and override settings in the MAPI profile, set the following special registry key.

Location	HKEY_CURRENT_USER\Software\Microsoft\Exchange\Exchange Provider
Name	DS Server
Type	REG_SZ (string)
Value	<i><FQDN of the global catalog server></i>

With either of the previous registry settings, if the specified global catalog server fails, Outlook will request a new referral from DSProxy. When configuring the client to select the global catalog server, you should remember the following:

- The global catalog server chosen by the client may be out of date or may not be fully functional. If the global catalog server is having problems but still responds to NSPI requests, Outlook may not fail over to DSProxy for a new referral.
- In multiple-domain environments, the global catalog server chosen by the client may not be in the same domain as Active Directory group objects. Therefore, users may not be able to update group membership, because the local global catalog server has a read-only copy of the group.

How the Categorizer Works

The Categorizer, which is a component of the transport and routing engine, is responsible for performing Active Directory lookups. Its primary task is to use header information (such as **From** and **To**) to resolve addresses by using the directory. The Categorizer looks at all user information (for example, per-recipient limits), and instructs the routing engine on how to deliver the message. The Categorizer is also responsible for expanding distribution lists.

Because the Categorizer performs forest-wide lookups, it only uses global catalog servers. Like DSProxy, the Categorizer obtains the list of working global catalog servers from DSAccess, filters out the servers from nonlocal domains, and uses the remaining servers. However, the Categorizer does not by default open connections to all global catalog servers. To conserve resources, the Categorizer opens an LDAP connection to one global catalog server and uses this server for lookups. If there are more than 14 messages waiting in the “Messages Awaiting Directory Lookup” queue (also known as the PreCatQ), the Categorizer opens an LDAP connection to a second global catalog server if one is available. If the PreCatQ continues to build, the Categorizer opens additional connections to other global catalog servers on the list.

2

Directory Access in Large Active Directory Environments

The first part of this document describes the core technology behind directory access. The information presented so far describes how directory access works in a small, stable Active Directory environment. However, real life scenarios are much more complex. In large companies, the Active Directory environment changes daily, and you should understand the impact of those changes on Exchange 2000.

Unfortunately, some of the operations performed in your environment are out of your control. For example, you probably do not have control over who installs hotfixes on domain controllers or when global catalog servers are restarted. Therefore, you must have a clear set of operational procedures to ensure that the messaging system is not affected by changes made to the underlying platform.

Calculating Active Directory Load

The Microsoft Exchange 2000 & DS Topology Calculator at <http://go.microsoft.com/fwlink/?linkid=1716> is a tool that can help you determine the load on your Active Directory servers based on the following:

- Your Exchange 2000 topology
- Server resources
- Numbers of users
- Protocols
- The amount of mail flowing through your organization

The calculator is especially useful for determining minimum hardware requirements.

Event Logging

Event logging is an important tool for understanding how DSAccess works. There are five categories under which DSAccess logs events in the Event Viewer Application Log. By default, the logging level for each category is set to “None,” but it is recommended that you enable logging by selecting a higher logging level for each category. Table 3 describes the types of events that are generated under the various logging levels.

► **To enable DSAccess logging**

1. Start System Manager. (On the Start menu, point to Programs, point to Microsoft Exchange, and then click System Manager.)
2. In the console tree, double-click Servers, right-click a server, and then click Properties.
3. Click the **Diagnostics Logging** tab.
4. Click **MSExchangeDSAccess**. You can configure the five categories described in Table 3.

The following table summarizes the types of log entries that are generated under each category and logging level.

Table 3 Diagnostics logging categories for DSAccess

Category	Logging level	Types of log entries generated
General	None	Start-Stop Service
	Minimum	Other system-wide events
Cache	None	Cache errors
	Medium	Informational messages about cache records
Topology	None	Connection errors General discovery errors Site-specific suitability failures Information about initial topology discovery
	Minimum	Information about server status and suitability changes Regular topology discovery information and lists of Active Directory servers being used Going outside of site and returning into the site DNS warnings
	Medium	Information about LDAP retries
Config	None	Errors in DSAccess registry settings
	Minimum	Information about using servers specified in the registry
LDAP	Medium	Failed LDAP calls with return codes LDAP limit exceeded error

Server Failures and Their Effect on Exchange 2000

DSAccess, DSProxy, and the Categorizer have been designed to be fault tolerant of failures in the network and Active Directory. When there is more than one domain controller and global catalog server available, all of the components on the Exchange server will fail over to another server and continue running. If you are using Exchange 2000 SP2 or later, DSAccess chooses failover domain controllers and global catalog servers based on site link costs. If the clients are using Outlook 2002, the clients will also fail over without interruption to service.

During failover, DSAccess:

- Chooses failover domain controllers and global catalog servers based on site link costs.
- Load balances all available domain controllers and global catalog servers in the failover site.
- Predetects the failover resources, and keeps the list up to date so that failover is quick.
- Polls the site that failed every five minutes, to determine whether it can fail back to that site.
- Fails back to the site when in-site resources become available.

You should understand the difference between “hard” and “soft” failures. A hard failure occurs when a server is taken offline, catastrophically fails, or is generally unreachable. DSAccess handles hard failures well, especially in environments where multiple Active Directory servers are present. Soft failures occur when an Active Directory server is reachable and responding, but for some reason is not responding in a timely manner to requests sent by the Exchange 2000 server. In these cases, DSAccess does not attempt to fail over, but instead logs errors in the application log.

Configuration Domain Controller Failures

When a hard failure occurs on the server acting as the configuration domain controller, DSAccess attempts to locate another suitable domain controller. If one is available, service is not interrupted, and no errors are logged. However, DSAccess marks the domain controller as down and tracks its progress through a series of ping attempts. If DSAccess determines that the server is again available, it marks it as available, but it does not attempt to fail back to the original configuration domain controller role. If the domain controller is both a working global catalog server as well as the configuration domain controller, failures are handled differently, as described in the following section.

Working Global Catalog Server Failures

When a hard failure occurs on a global catalog server, DSAccess marks this global catalog server as down and redistributes the requests among the remaining global catalogs on the working list. DSAccess tracks the progress of the failed global catalog server and reinstates it into the working global catalog server list when it becomes available. Because both DSAccess and DSProxy automatically round robin requests to global catalog servers under normal conditions, the failure of a global catalog server should not affect server operations.

If the global catalog server had outstanding DSAccess requests when it failed, a small number of errors are logged in the application log. However, the occurrence of these errors should be short lived. If an error message recurs, either the Active Directory servers are going through a series of hard failures, or more likely, soft failures are occurring.

In the case of a hard failure, DSAccess always reissues all outstanding requests to another working global catalog server if one is available. Therefore, if the Active Directory topology has sufficient resources, end-user operations on the server (such as mail delivery) are not affected.

A hard global catalog server failure can severely impact Outlook clients. Outlook 2000 clients (and earlier versions) may stop responding if the user attempts to browse the global address list or perform name resolution. However, access to messages and folders is unaffected. Outlook eventually times out and displays an error message indicating that there are network problems with contacting the Exchange server. Earlier versions of Outlook do not differentiate between store and directory service problems; one error message covers both failure scenarios.

While the global catalog server is in a down or failed state, Outlook 2000 (and earlier versions) does not function. This is because the Outlook cache still contains the universally unique identifier (UUID) that is assigned to each NSPI directory service. Therefore, failing over to a different global catalog server requires that the UUID cache be flushed. In Outlook 2000 and earlier Outlook versions, the UUID cache is flushed only when the user quits Outlook. To solve this issue, the user must either restart Outlook or wait for the global catalog server to become active again.

Outlook 2002 can dynamically flush the UUID cache while the client is running. Outlook 2002 contains a time-out period which, when exceeded, causes the client to fail over to a different global catalog server without requiring a restart.

When a global catalog failure occurs, DSAccess provides the modified list of available global catalog servers to DSProxy. If DSProxy diagnostics logging is set to **Maximum**, you will see new events in the application log. Figure 8 shows an example of the event that indicates that the target list for NSPI Proxy has changed.



Figure 8 Target list change event for NSPI Proxy

Both NSPI Proxy and the RFR interface update their target lists. NSPI Proxy generates event 9141 (Figure 8), and the RFR interface generates event 9148.

Hard Failures

If DSAccess cannot identify suitable domain controllers or global catalog servers due to hard failures, DSAccess is unable to continue servicing Exchange components. Depending on the environment and type of failure, different error messages are reported.

For example, if the only global catalog server fails but a domain controller is still available, some operations will succeed. DSAccess will log event 2103 and DSProxy will report errors such as event 9057 (Figure 9).

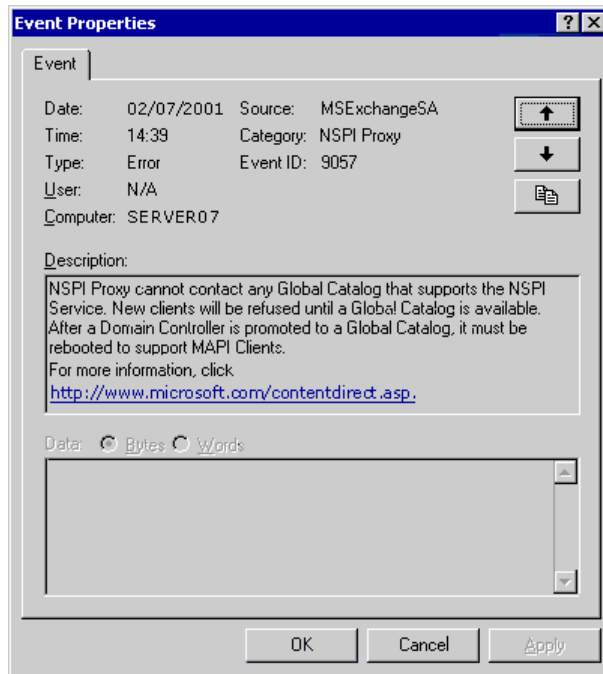


Figure 9 Global catalog server failure event for NSPI Proxy

Upon global catalog server failure, the Categorizer stops processing messages and the messages back up in the client's Outbox or the "Messages awaiting directory lookup" queue. Under most conditions users are unable to perform directory lookups. However, if the global catalog server becomes available within a relatively short period of time (usually within a few minutes), service resumes and messages move through the queue.

A more critical problem occurs if the configuration domain controller server fails and there are no suitable domain controllers to take over this role. DSAccess logs critical errors, which have an event identifier of 2102 in the application log.

If the configuration domain controller outage is brief (for example, if the outage occurs while a network cable is moved from one port in the hub to another), DSAccess continues service. However, if the configuration domain controller is down for more than a few seconds, other Exchange 2000 services will begin timing out and reporting errors. For example, more error messages will be generated by the store and transport (Figure 10).

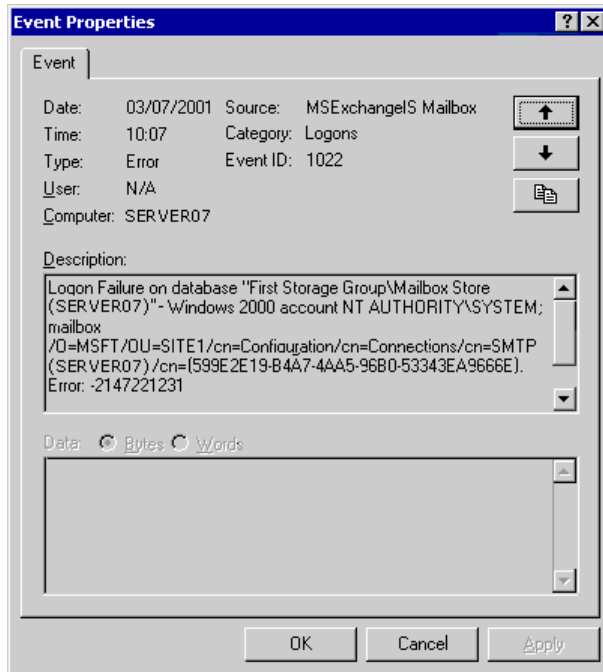


Figure 10 Logon failure generated by the store process

Soft Failures

Soft failures are more difficult to resolve than hard failures. A domain controller may appear to be up and running because it responds to port 389 requests, but it may be experiencing serious problems. Soft failures can also occur on the network; for example, bad cables and hubs can cause transient network failures and routers can drop packets. Additionally, firewalls or network address translation (NAT) servers can introduce problems.

In all soft failure cases, DSAccess generates error messages in the application log. If errors appear once or twice and then disappear, a transient error has occurred and has been resolved. If an error is continuously logged at a frequent interval (such as every 60 or 120 seconds), you should investigate the problem.

The following examples describe some of the error messages that occur when servers fail.

Example 1

In the application log, you see the following entry:

```
Event Type:          Warning
Event Source:        MExchangeDSAccess
Event Category:      None
Event ID:            2389
Date:                mm/dd/yyyy
Time:                hh:dd:ss
User:                N/A
Computer:            PATLAB06
Description:
Process STORE.EXE" (PID=2136). A search request to Directory Server
patlab02.partlab.exinternals.com did not return a result within 120
seconds and is being abandoned. The search will be retried if
possible. The search that failed has the following characteristics:
Base DN=<GUID=89DD2250-B777-43A9-8455-09170C9A0A23>,
Filter=(objectclass=*) , Scope=0.
```

This warning indicates that DSAccess has sent an LDAP request to the named directory server, but no response was received after 120 seconds. If you see this error appear and then disappear, the cause is most likely one of the following:

- The named domain controller is temporarily overloaded or overworked.
- A transient error occurred on the network.

As the warning states, DSAccess will retry the operation. If after another 120 seconds the error reappears, the cause is most likely one of the following:

- The named domain controller is severely overloaded or overworked.
- A general problem exists on the network (for example, connections are failing).
- The directory server cannot find a route back to the Exchange 2000 server.
- A firewall or NAT is not allowing the return connection to succeed.

Example 2

In the application log, you see the following entry:

```
Event Type:          Error
Event Source:        MExchangeSA
Event Category:     General
Event ID:           9154
Date:               mm/dd/yyyy
Time:               hh:dd:ss
User:               N/A
Computer:           PATLAB06
Description:
DSACCESS returned an error '0x8007203a' on DS notification.
Microsoft Exchange System Attendant will re-set DS notification
later.
```

Whenever you see hex error codes in directory-related errors, they normally correspond to LDAP errors. For example, 0x8007203a means LDAP_SERVER_DOWN. Understanding the translation of the hex error code can help you understand why the error occurred. For more information about common LDAP error codes and their meanings, see Appendix B.

Example 3

In the application log, you see the following entry:

```
Event Type:          Error
Event Source:        MExchangeSA
Event Category:     None
Event ID:           2075
Date:               mm/dd/yyyy
Time:               hh:dd:ss
User:               N/A
Computer:           PATLAB06
Description:
Process STORE.EXE" (PID=1720). DsBind failed.
dir.svc.exinternals.com, hr=0x800706bb, deltaT=125. The operation
will be retried.
```

This error indicates an RPC problem rather than an LDAP problem. The translation is `RPC_S_SERVER_TOO_BUSY`. This error message can be returned for several reasons; for example, the domain controller or global catalog server may be overloaded. However, there may be other causes:

- The date and time in the Exchange server differ from the date and time in the Active Directory server by more than 60 seconds.
- The server is experiencing Kerberos authentication problems.

When this error occurs, the system attendant retries the operation within one second. After four attempts, the operation is abandoned. If you do not see four of these errors within the same short time period (within 10 seconds), the operation was retried and considered a success.

For more information about troubleshooting directory access problems, see “Directory Access Troubleshooting Checklist” later in this document.

Server Promotion and Its Effect on Exchange 2000

As your user population grows, you may need to install additional domain controllers and global catalog servers, which you can do by promoting servers to these roles. You should carefully manage server promotion to ensure that Exchange does not attempt to use the services of the newly promoted servers until they are ready for use.

All Windows 2000 servers are initially installed as member servers. To promote the member to a domain controller, use the Active Directory Installation Wizard. After the computer is promoted to a domain controller, you can promote it to a global catalog server by using the Active Directory Sites and Services snap-in.

Promoting a Member Server to a Domain Controller

It is extremely important for Exchange 2000 servers to use Active Directory servers that have the latest directory information. When you use the Active Directory Installation Wizard to promote a Windows 2000 member server to a domain controller, other domain controllers in the domain replicate the schema and configuration naming contexts to the new domain controller. One of the final tasks performed by the wizard is the replication of the domain naming context. It is possible to instruct the wizard to perform this replication at a later time by using the **Finish Replication Later** button (as shown in Figure 11). However, this could mean that when the new domain controller is restarted, it will not have the latest domain information.

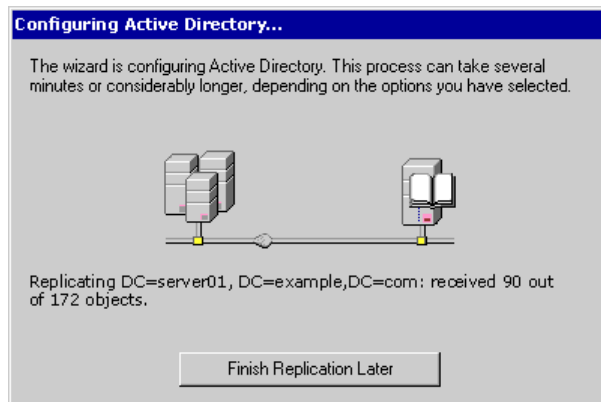


Figure 11 The Finish Replication Later button

Delaying replication has implications for Exchange. DSAccess detects the new domain controller and attempts to use the computer. If the new domain controller does not yet contain information about all of the users in the domain, Exchange may fail to find the information that it requires. Fortunately, Exchange 2000 typically uses global catalog servers instead of domain controllers to perform user lookups. However, as a best practice, when you are promoting a server to a domain controller role, always allow the Active Directory Installation Wizard to complete the replication of the domain naming context.

Note During promotion, you may see many 1153 events in the Directory Service event log. This event indicates that an Exchange-related class (for example, **msExch**) has an invalid super class and inheritance has been disregarded. These errors are harmless and can be ignored.

When the Active Directory Installation Wizard is finished, you will be asked to restart the server. After the server restarts, it will advertise itself in DNS. DSProxy will dynamically pick up the topology change and begin using the new domain controller.

Promoting a Domain Controller to a Global Catalog Server

You can promote a domain controller to a global catalog server by using the Active Directory Sites and Services snap-in. Select the **Global Catalog** checkbox in the server's **NTDS Settings Properties** (see Figure 12).

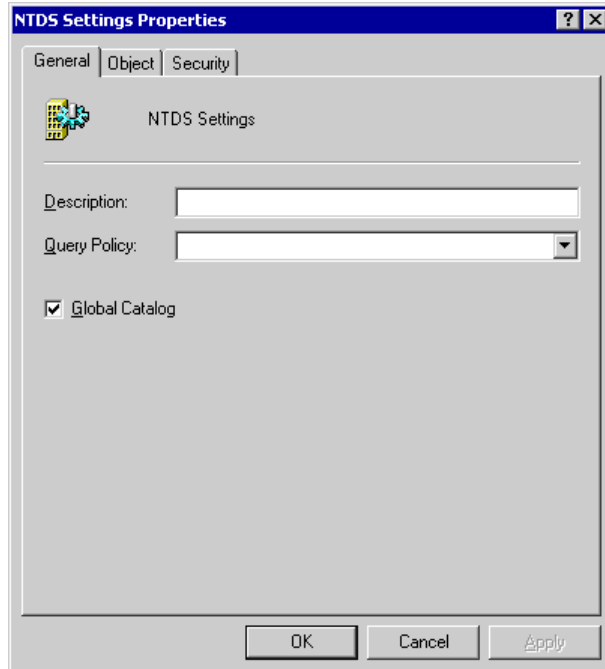


Figure 12 Global catalog server option in the NTDS Settings Properties

Although the process is simple, without proper planning promoting a server to a global catalog server can negatively impact Exchange. This causes the following problems:

- NSPI is not enabled. The server must be restarted in order to enable NSPI.

Note NSPI is only supported on global catalog servers; domain controllers do not support NSPI and are never used for Outlook address book lookups.

- The global catalog server may advertise itself before replication is complete.

After promotion, there is no automatic prompt to restart the server; however, promoting the server immediately places SRV records in DNS. Because new SRV records exist, the system attendant attempts to use the new global catalog server, but it detects that NSPI is disabled. As a result, the event shown in Figure 13 appears in the application log.

Users are not affected by this situation, because NSPI Proxy and RFR interface simply refuse to allow clients to communicate with the server. However, you should restart the server to enable NSPI and allow use of the server. You should wait until replication has completed before you restart the server; otherwise, DSProxy will use the server for address book lookups, but the address books will be incomplete.

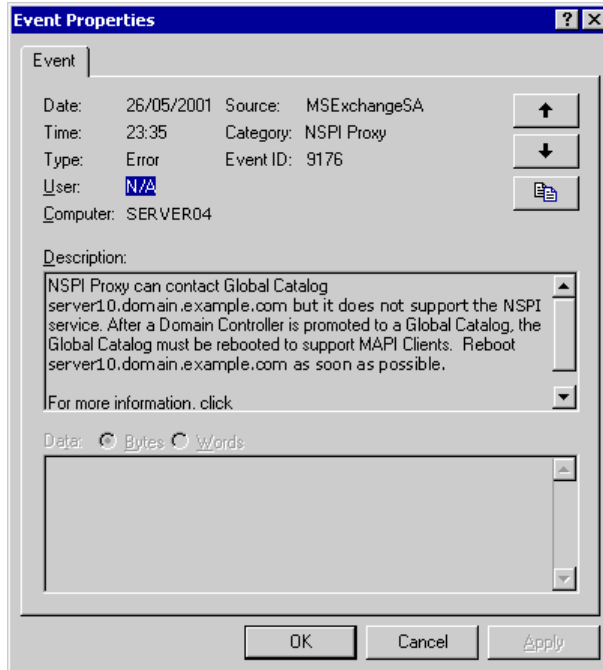


Figure 13 NSPI error resulting from failure to restart

After promotion, DSAccess places the server into its list of working global catalog servers. Because replication may not have completed, the new server may not contain all of the information about the forest.

DSAccess sends the new working global catalog list to the Categorizer. In large, complex environments, it is possible for the Categorizer to reference global catalog servers that have not finished replicating. The result is sporadic nondelivery messages. The effect may be random because the Categorizer may choose to reference a different global catalog server when the user clicks **Send Again**. However, this is not a big problem, because the Categorizer waits one hour after it receives a new working global catalog server list from DSAccess before it uses new servers on the list.

The best practice is to promote the domain controller to a global catalog server, prevent it from advertising itself as a global catalog server, and avoid restarting the server until all the partial naming contexts have replicated. This is possible if you are running Windows 2000 with Service Pack 2.

► **The correct process for promoting a domain controller to a global catalog server in an Exchange 2000 environment is as follows.**

1. On the domain controller to be promoted, create the following registry key.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters
Name	Global Catalog Partition Occupancy
Type	REG_DWORD
Value	0x00000006

This registry key tells the promotion process that it must complete the full replication of all naming contexts before the server advertises itself. By default, promotion runs at partition occupancy level 4, which only requires the naming contexts found within the local Active Directory site to be fully replicated before the server advertises itself.

2. Stop the NetLogon service on the server to be promoted. This will prevent the server from advertising itself after replication has completed and the 1119 event is reported in the Directory Service log.
3. Check the box in the Active Directory Sites and Services snap-in to start the promotion process.
4. Monitor the Directory Service log for the 1119 event. This event signifies that promotion has met the level set in the **Global Catalog Partition Occupancy** registry key.
5. Restart the server.

After the server restarts, NSPI is enabled and the server advertises itself in DNS. DSPProxy detects the new server within 15 minutes. Because you have set the partition occupancy level to 6 and the server has been restarted, the new global catalog server is fully operational and is valid for use by Exchange 2000 and Outlook.

Because of the load balancing mechanism used by DSProxy, the RFR interface service will start using the new global catalog server after the server restarts, but NSPI Proxy will not proxy clients to the server until the Exchange 2000 server restarts. If NSPI Proxy did not have this behavior, Outlook clients would be proxied to the new global catalog server during an Outlook session. This would cause the client to stop responding because of the UUID change. This problem does not affect the RFR interface because clients that do not support dynamic UUID changes only ask for referrals at startup.

Note After promotion, you may see a 1110 event in the Directory Service log. The event indicates that you can set a registry key called **Global Catalog Delay Advertisement** to control the length of time before the newly promoted global catalog server is advertised in DNS. You should not use this registry key to control advertising, because it is ignored if the value exceeds 300 seconds (5 minutes).

Server Demotion and Its Effect on Exchange 2000

Windows 2000 allows administrators to demote Active Directory servers. Although this is a rare occurrence in most topologies, it is possible to demote a global catalog server to a domain controller, and a domain controller to a member server. As with promotion, the demotion process must be carefully planned and executed to ensure that Exchange 2000 is not affected.

Demoting a Global Catalog Server to a Domain Controller

When a global catalog server is demoted to a domain controller, it stops responding to LDAP connections on port 3268 and removes its SRV records from DNS. DSAccess detects that the server is no longer a global catalog and removes it from the working global catalog server list. However, NSPI cannot be automatically disabled on the demoted server, so Outlook continues to use the server. DSProxy receives the modified working global catalog list and the RFR interface updates itself so that it no longer sends referrals to the demoted server. However, NSPI Proxy continues to use the demoted server.

A problem can occur if you do not restart the demoted server, because after the directory database purges the remote naming contexts, NSPI reports information about the local domain only and not the forest. However, restarting the demoted server causes Outlook clients to stop responding. To solve this problem for Outlook 2000 clients (and earlier versions), restart the clients. No action is necessary for Outlook 2002 clients; these clients automatically fail over to a different global catalog server.

► **To mitigate the issues associated with demoting a global catalog server to a domain controller, do the following:**

1. A week before the demotion is due to occur, hard code the RFR interface to a defined group of global catalog servers. (For more information, see “Manually Controlling RFR and NSPI Proxy Servers” later in this document.) Ensure that the global catalog server to be demoted does not appear on the list.

Note All Outlook 2002 and Outlook 2000 Service Release 2 (SR-2) clients will ask the Exchange 2000 server for a new referral upon restart of the client. The server will refer the clients to one of the global catalogs on your defined list.

2. After a week has elapsed, demote the global catalog server during a quiet time (for example, in the evening). Immediately restart the demoted server to disable NSPI.
3. After the demoted server restarts, monitor the event log to verify that Exchange 2000 servers are not reporting the server as a global catalog server. If the demoted computer is still reported as a global catalog server, wait 15 minutes and view the event log again. If the server continues to appear in the working global catalog server list, verify that the global catalog server’s SRV records have been removed from the DNS server. Then run IPCONFIG /FLUSHDNS and IPCONFIG /REGISTERDNS on each Exchange 2000 server. (For more information, see Microsoft Knowledge Base article Q305967 at <http://go.microsoft.com/fwlink/?LinkId=3052&ID=305967>, “How to Clear Bad Information in Active Directory-Integrated DNS”.)
4. If your organization contains Outlook 2000 clients (or earlier versions), restart the clients after the demotion has taken place.

Note If you are only running Outlook 2002 clients, you do not need to hard code the RFR list, because the clients will dynamically fail over to another global catalog server. Simply demote the server at a time when there is little activity on the server, and then immediately restart it.

Demoting a Domain Controller to a Member Server

You can use the Active Directory Installation Wizard to demote a domain controller to a member server. After demotion starts, SRV records are removed from DNS and the server no longer responds to port 389 connections.

Because Outlook users do not connect to domain controllers, only the Exchange 2000 processes are affected by the demotion. DSAccess still reports the server as an available domain controller while the wizard runs. As long as there are other suitable domain controllers in the Active Directory Site, DSAccess fails over and binds to a different server. It is common to see 2075 errors from DSAccess in the application log during demotion. These errors indicate that DSAccess had problems communicating with the domain controller while it was being demoted. However, DSAccess will have found another domain controller to handle its query.

After the demotion process is complete, DSAccess removes the domain controller from its list of working domain controllers.

Demoting a Global Catalog to a Member Server

Using the Active Directory Installation Wizard, it is possible to demote a global catalog server directly to a member server (assuming that other servers exist in the environment). If you are attempting to perform this operation, combine the best practices of demoting a global catalog server to a domain controller and a domain controller to a member server, as detailed in the previous sections.

Manual Topology Definition

In most scenarios, DSAccess does a good job of detecting the Active Directory topology and load balancing requests against the available servers. However, DSAccess does not handle all of the problems associated with large, complex topologies. DSAccess chooses Active Directory servers based on whether a server:

- Is located in the local Active Directory Site.
- Responds on either the domain controller port 389 or the global catalog server port 3268.
- Returns an LDAP response within 2 seconds.

Specifically, DSAccess does not detect the following issues or conditions:

- The number of network hops between servers
- Slow replication or replication failures
- Transient errors
- If a server is semioperational
- If a server is under-powered (unless it exceeds a 2 second response)
- If a server is over-worked (unless it exceeds a 2 second response)
- If a server is performing FSMO roles (other than the primary domain controller role)

- If a server's weighting in DNS is misconfigured
- The number of outstanding LDAP requests on the domain controller from other sources
- If network connections are poor but still allow the transfer of packets

If problems occur with Active Directory servers, Exchange reports errors. In some cases the Exchange services may fail to start, or Exchange may fail to connect to databases, or (in extreme cases) messages may fail to be delivered. For information about what to do if any of your Active Directory servers are experiencing problems, see "Directory Access Troubleshooting Checklist" later in this document.

If Exchange performance suffers because of Active Directory issues, you can temporarily hard code DSAccess to communicate with a predefined set of domain controllers and global catalog servers. This will give you time to fix the Active Directory problem while Exchange is running. After you fix the problem, you should remove the hard-coded settings and allow DSAccess to use automatic topology detection.

Hard Coding Active Directory Servers

It is not necessary to hard code Active Directory servers for use by DSAccess unless you are troubleshooting a specific problem or there is another reason to use specific servers. If you decide it is necessary to hard code servers for use by DSAccess, you can either specify servers in System Manager or set registry keys.

If the domain controllers or global catalog servers you have hard coded are not available, DSAccess does not attempt to discover other servers. In contrast, the configuration domain controller registry key indicates a preferred server. If the preferred configuration domain controller fails, DSAccess attempts to choose a suitable server that can act as the configuration domain controller from the list of working domain controllers. If you have hard coded the list of domain controllers, DSAccess attempts to choose a configuration domain controller from the hard coded list.

In Exchange 2000 Server SP2 and later, right-click a server, click **Properties**, and then use the **Directory Access** tab to view and configure Directory Access information for any server running Exchange SP2 or later in your topology. You can add servers to or remove servers from the topology list.

Note If your topology contains Exchange 2000 and SP1 servers, you can only view a partial current topology list. If you try to select a server running Exchange 2000 or Exchange 2000 SP1, only the names of the domain controllers that Directory Access uses are listed, and you cannot manually configure the servers because **Add** and **Remove** are not available.

In Exchange 2000 SP1 and earlier versions, you can specify servers in the registry by creating certain registry keys. Because DSAccess detects registry key changes immediately, it is best to create a registry import file. For a sample registry file that hard codes DSAccess parameter settings, see Appendix A. You can include multiple domain controllers and global catalog servers in the registry file. After you set these registry keys, DSAccess dynamically detects the specified servers. In addition, Outlook 2002 dynamically detects the specified servers and begins using them. However, if other MAPI clients are currently using a global catalog server that is not one of the servers you specified in the registry keys, you must restart the MAPI clients.

Note When hard coding servers, make sure that the fully qualified domain names (FQDNs) you enter are spelled correctly.

The following tables show the registry keys to create to specify servers.

Working domain controller registry keys

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Profiles\Default\ <i><unique key></i>
Name	IsGC
Type	REG_DWORD
Value	0x0

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Profiles\Default\ <i><unique key></i>
Name	HostName
Type	REG_SZ
Value	<i><FQDN of the server></i>

Working global catalog server registry keys

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Profiles\Default\ <i><unique key></i>
Name	IsGC
Type	REG_DWORD
Value	0x1

Working global catalog server registry keys (continued)

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Profiles\Default\ <unique key><="" td=""> </unique>
Name	HostName
Type	REG_SZ
Value	<FQDN of the server>

Configuration domain controller registry key

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Instance0
Name	ConfigDCHostName
Type	REG_SZ
Value	<FQDN of the server>

Deciding Which Servers to Use

When hard coding servers for DSAccess, use the following list to help you decide which Active Directory servers to use:

- Avoid Active Directory servers that are known to have problems.
- Avoid Active Directory servers that have been problematic in the past.
- Avoid Active Directory servers that are reporting errors in the Directory Service log.
- Use Active Directory servers that have good processing power and plenty of memory.
- Use Active Directory servers that are on the same hub or in the same rack as the Exchange 2000 server.
- For additional fault tolerance, hard code more than one server.

After you have hard coded servers, use the event logs or System Manager (when running Exchange 2000 SP2 or later) to verify that the correct servers are being used. Inform your operations team of the hard-coded servers and, if you contact Microsoft Product Support Services, tell them that you have hard coded the DSAccess list. Finally, fix the problem with Active Directory as soon as possible so that you can remove the hard coding.

Manually Controlling RFR and NSPI Proxy Servers

If you want DSAccess to perform automatic topology detection but you want to control the NSPI Proxy and RFR interface services, you can implement registry parameters.

In some scenarios, you may want to force all Outlook clients, regardless of version, to use NSPI Proxy. You may need to do this if a firewall exists between your user and the Exchange 2000 server. Instead of allowing the Exchange server to send a referral to the client and opening a new server/port through the firewall, you can force the client to use the NSPI Proxy service on the Exchange 2000 server by setting the following registry key.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeSA\Parameters
Name	No RFR Service
Type	REG_DWORD
Value	0x00000001

Specifying the MAPI client proxy service server

To specify the server that should be used for MAPI client proxy service, set the following registry key.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeSA\Parameters
Name	NSPI Target Server
Type	REG_SZ or REG_MULTI_SZ
Value	<FQDN of the server>

Specifying the MAPI client referral service server

If you want to specify the server that should be used for MAPI client referral service, set the following registry key.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeSA\Parameters
Name	RFR Target Server
Type	REG_SZ or REG_MULTI_SZ
Value	<FQDN of the server>

Excluding the FSMO Primary Domain Controller Role

The primary domain controller role is the only Active Directory flexible single master operation (FSMO) role that DSAccess detects. In Windows NT, a primary domain controller handled all directory changes. In contrast, in Active Directory, multiple domain controllers can handle directory changes. To enable compatibility with Windows NT, Active Directory must provide a server in each domain that can emulate the primary domain controller role.

If your topology contains Windows NT servers, the server performing the primary domain controller role experiences heavy loads. To avoid performance problems, you should exclude FSMO primary domain controller servers from DSAccess.

To exclude a FSMO primary domain controller server from detection by DSAccess, create the **MinUserDC** registry key (listed in the following table). Set the value to the number of domain controllers and global catalog servers that are required to support your user load. For example, if four global catalog servers must be available at all times, set the **MinUserDC** value on all Exchange servers to 4. As long as more than four global catalog servers are available, DSAccess will avoid the primary domain controller. If at some point all but three global catalog servers are down, DSAccess will be forced to use the primary domain controller.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Profiles\Default
Name	MinUserDC
Type	REG_DWORD
Value	1-10 (depending on the minimum number of domain controllers and global catalog servers required to support user load)

If you do not have Windows NT servers in your topology, you do not need to set this registry key.

Static Port Mappings

In scenarios where firewalls are present between Outlook clients and the Exchange 2000 server, you may need to statically map the listening port for NSPI Proxy and the RFR interface process. When DSProxy initializes, it chooses a random port between 1024 and 5000. To statically map DSProxy, create the following registry keys.

Important You must specify different port numbers for **TCP/IP NSPI port** and **TCP/IP port**.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeSA\Parameters
Name	TCP/IP NSPI port
Type	REG_DWORD
Value	Port number to be assigned to NSPI Proxy

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeSA\Parameters
Name	TCP/IP port
Type	REG_DWORD
Value	Port number to be assigned to the RFR interface (must be a different port than the TCP/IP NSPI port)

If you need to statically map the NSPI port on a global catalog server, you can create the following registry key.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\NTDS\Parameters
Name	TCP/IP port
Type	REG_DWORD
Value	Port number to be assigned to the Active Directory NSPI

In addition to these directory service static mappings, you will also need to statically map the port for the Information Store. For more information about statically mapping ports in Exchange 2000, see Microsoft Knowledge Base article Q270836 at <http://go.microsoft.com/fwlink/?LinkId=3052&ID=270836>, “XCLN: Exchange 2000 Static Port Mappings”.

DSAccess Cache

In Exchange 2000 SP2, the following values for configuration data were changed:

- Time-to-live value
- Maximum number of entries in the cache
- Maximum amount of memory that can be used by entries in the cache

In earlier versions of Exchange 2000, configuration and user data had the same “time-to-live” value. The time-to-live value specifies the length of time information must be cached. In Exchange 2000 and Exchange 2000 SP1, configuration data and user data both shared a time-to-live value of 5 minutes. Because configuration data changes less often than user data, configuration data is assigned a time-to-live value of 15 minutes in SP2 and later. User data still has a value of 5 minutes.

In addition, the maximum number of entries in the cache and the maximum amount of memory that can be used by entries in the cache were the same for both configuration and user data in earlier versions of Exchange 2000. In Exchange 2000 SP2 and later, configuration and user data now have separate values. Each type of data now has its own unlimited value for the maximum number of entries in the cache, and its own 25 MB limit for the maximum amount of memory that can be used by data. (Previously, configuration and user data shared a single limit of 50 MB.)

DSAccess in a Perimeter Network

Changes to DSAccess in Exchange 2000 SP2 made deployment easier in perimeter networks (also known as DMZs, demilitarized zones, and screened subnets).

Hard Coding Active Directory Servers

Exchange 2000 SP2 and later eliminates remote procedure calls (RPCs) in the DSAccess component. Because DSAccess now uses Lightweight Directory Access Protocol (LDAP) to locate available domain controllers and global catalog servers, deployment is improved for perimeter networks.

In earlier versions of Exchange 2000, if DSAccess was deployed in a perimeter network, the list of Active Directory servers had to be manually configured because DSAccess discovery methods depended upon RPCs. The discovery methods have been changed to use non-RPC Microsoft Windows implementation of LDAP (wLDAP) calls exclusively. Therefore, hard coding Active Directory servers is no longer required.

Stopping The NetLogon Check

DSAccess skips the NetLogon check during initial topology discovery, but runs the NetLogon check every 15 minutes during ongoing discovery. The check determines whether the NetLogon service is running.

In a perimeter network where RPC traffic is not allowed, the NetLogon check cannot occur; however, the NetLogon check will continue to issue RPCs until it fails, which can take a long time. Because repeated NetLogon checks decrease performance, you should stop DSAccess from issuing NetLogon checks by creating the following registry key.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Profiles\Default
Name	DisableNetLogonCheck
Type	REG_DWORD
Value	1

For more information, see Microsoft Knowledge Base article Q320228, "XGEN: The 'DisableNetLogonCheck' Registry Value and How to Use It" at <http://go.microsoft.com/fwlink/?LinkId=3052&ID=320228>.

Stopping The Directory Access Ping (LDAP ICMP Keep Alive)

By default, DSAccess uses Internet Control Message Protocol (ICMP) to ping each server that it connects to, in order to determine if the server is available. In a perimeter network, ICMP is typically blocked between the Exchange 2000 server and the domain controllers. This situation causes DSAccess to respond as if every domain controller is unavailable. DSAccess then discards old topologies and frequently performs new topology discoveries, which affects server performance. You can turn off the ICMP ping by creating the following registry key.

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MExchangeDSAccess
Name	LdapKeepaliveSecs
Type	REG_DWORD
Value	0

Microsoft only supports conditions in which the **LdapKeepaliveSecs** registry key is either set to 0 or not present in the registry. For more information about the **LdapKeepaliveSecs** registry key, see Microsoft Knowledge Base article Q320529, "XADM: Using DSAccess in a Perimeter Network Firewall Scenario Requires a Registry Key Setting" at <http://go.microsoft.com/fwlink/?LinkId=3052&ID=320529> .

3

Directory Access Troubleshooting Checklist

Troubleshooting directory access problems requires experience and knowledge. Use the following steps as a guide. Depending upon the scenario, troubleshooting may differ.

Step 1. Look for Errors in the Event Logs

To begin troubleshooting, analyze any errors that appear in the event logs on the Exchange 2000 server. You should look at the system log for general service problems, and at the application log for Exchange-specific errors.

Example: Event 2080

- ▶ **Event 2080 is a DSAccess event that helps you diagnose most topology-related problems. To enable DSAccess topology logging, do the following**
 1. In System Manager, navigate to the server.
 2. Right-click the server, and then click **Properties**.
 3. On the **Diagnostics Logging** tab, click **MSExchangeDSAccess**.
 4. Under **Category**, click **Topology**, and then set **Logging level** to **Minimum** or higher.

Event 2080 reports certain characteristics of your Active Directory servers, including the roles a server is capable of fulfilling, whether the server is reachable, and so forth. The following is an example of event 2080 text. Table 4 describes how server characteristics are represented in the event text.

```
Event Type: Information
Event Source: MExchangeDSAccess
Event Category: Topology
Event ID: 2080
Computer: MyMachine

Description:
Process MAD.EXE (PID=1304). DSAccess has discovered the following
servers with the following characteristics:
(Server name | Roles | Reachability | Synchronized | GC capable |
PDC | SACL right | Critical Data | Netlogon)
In-site:
EXGGHH01.ParentDomain.extest.microsoft.com CDG 7 7 1 1 1 1 7
Out-of-site:
```

Table 4 Server characteristics reported in event 2080

Characteristic	Description
Server name	Shows the actual Active Directory server name.
Roles	Shows whether or not the particular server can be used as a configuration domain controller (C), a domain controller (D), or a global catalog server (G). An abbreviation means the server can be used, and a hyphen (-) means the server cannot be used.
Reachability	Shows whether the server is reachable through a TCP/IP connection. These are bit flags, where 0x1 means the server is reachable as a global catalog server (port 3268), 0x2 as a domain controller (port 389), 0x4 as a configuration domain controller (port 389). In the previous example, "7" means that the server is reachable as all three types (0x1 0x2 0x4 = 0x7).

Table 4 Server characteristics reported in event 2080 (continued)

Characteristic	Description
Synchronized	Shows whether the “isSynchronized” flag set on the rootDSE of the server is TRUE. These values are the same bit flags used in Reachability.
GC capable	Boolean. Specifies whether the server is a global catalog server.
PDC	Boolean. Specifies whether the server is a primary domain controller for its domain.
SACL right	Boolean. Specifies whether DSAccess has the necessary permissions to read the Security Access Control List (SACL) (part of the nTSecurityDescriptor) for the configuration naming context.
Critical Data	Boolean. States whether DSAccess found this Exchange server in the Exchange configuration container.
NetLogon	Shows whether the server is running the NetLogon service. These are bit flags, where 0x1 means the server is reachable as a global catalog server (port 3268), 0x2 as a domain controller (port 389), 0x4 as a configuration domain controller (port 389). In the previous example, “7” means that the server is reachable as all three types (0x1 0x2 0x4 = 0x7).

► **To analyze event 2080, do the following:**

1. Begin by looking at the **Roles** column. There should be at least one server that can act as the configuration domain controller (C), one that can act as a domain controller (D), and one that act as a global catalog server (G). If servers are not available for these roles, check your topology. Do you have at least one domain controller and one global catalog server in either the same site as your Exchange server or the closest connected sites (in other words, sites with the lowest siteLink cost)?
2. Next, look at the **Reachability** column. If the server is a domain controller but not a global catalog server (Roles column shows “CD”), this number should be 6 (0x2 | 0x4), signifying that the server's DC port (389) is reachable through TCP/IP. If the server is a global catalog server (Roles column shows “CDG”), this number should be 7 (0x1 | 0x2 | 0x4), signifying that the server's domain controller port (389) and global catalog server port (3268) are reachable through TCP/IP. If you see other numbers here (especially 0), the Exchange server is having trouble connecting to the server.
3. Look at the **SACL right** column. DSAccess does not use a server if it does not have permission to read the SACL on the nTSecurityDescriptor attribute for the configuration naming context. You must have at least one server that satisfies each role (C, D, or G), is reachable for that role (the appropriate bit flag in the **Reachability** column), and reports 1 in the **SACL right** column. If you do not have these servers, ensure that the domain has been prepared with DOMAINPREP and Recipient Update Service has been configured for the domain.

Note The right that determines whether the DSAccess can read the server's SACL is the Manage Auditing and Security Log right (**SeSecurityPrivilege**). All domain controllers should receive this right from the group policy for Exchange Enterprise Servers. You can run the POLICYTEST tool (found in the \support\utils\i386 folder on the Exchange 2000 CD) to verify that all domain controllers have the **SeSecurityPrivilege** right.

Step 2. Monitor Performance Counters

DSAccess performance counters indicate whether DSAccess is performing as expected, and warn you about processing delays and latencies that require your attention.

Example: Mail is not delivering locally or is slow

In the Windows 2000 Performance Logs and Alerts snap-in, DSAccess has two performance counters under the **MSExchangeDsaccessProcesses** performance object: **Ldap Search Time** and **Ldap Read Time**. If an increase in these counters coincides with a drop in message delivery rate, the slowdown is occurring in Active Directory.

Note that these same counters exist for every process that runs DSAccess. Although it is interesting to compare them, you can focus on the store process initially. By examining the **Process ID** counter (also under the **MSExchangeDsaccessProcesses** performance object) you can find out which process ID corresponds to which instance. There is also a set of various **Searches/sec** counters that can be informative.

If performance counter rates drop and performance times spike, and you suspect that Active Directory is sluggish, the configuration domain controller may not be performing well. Changing the configuration domain controller may cure some of these problems. In Exchange 2000 SP2 and later, you can use System Manager (on the **Directory Access** tab in the server's **Properties**) to select the configuration domain controller.

You may also be able to speed up mail delivery by increasing the DSAccess cache size, especially if the server stores mailboxes for a large number of users. The default user and configuration cache size is 25 MB. If the server has sufficient RAM, performance may increase if you set the user cache size to 90 MB and the configuration cache size to 5 MB. In addition, the cache hit and miss performance counters under the **MSExchangeDSAccess Cache** performance object are useful for determining an optimal cache size. Use the following registry keys to set cache sizes (values are in KB).

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Instance0
Name	MaxMemoryUser
Type	REG_DWORD
Value	90000

Location	HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\MSExchangeDSAccess\Instance0
Name	MaxMemoryConfig
Type	REG_DWORD
Value	5000

Step 3. Check that DNS is Configured Properly

The majority of Exchange 2000 directory access problems are caused by DNS and name resolution problems. Therefore, DNS is the first component you should verify. Symptoms of DNS trouble include failures in starting Exchange 2000 services and setup failure.

1. To view the IP address entered into the DNS field on the TCP/IP stack of the Exchange 2000 server, run **ipconfig /all** at the command prompt. Verify that the address is correct.
2. Ping the IP address of the DNS server to see if it responds.
3. In the console of the DNS server, verify that the server's IP address is correct.
4. Open the DNS Manager snap-in to verify that the Host record of the Exchange 2000 server exists.
5. Verify that the `_msdcs`, `_sites`, `_tcp`, and `_udp` keys exist in the DNS database. If they do not exist, verify that the DNS IP address has been correctly entered on the TCP/IP stack of the DNS server.

Step 4. Verify the Configuration of Active Directory Sites

If DNS appears to be configured correctly, you should turn your attention to the configuration of the sites in Active Directory. If the Exchange 2000 server cannot determine which site it belongs to, directory access will fail. The most common problem occurs when the Active Directory administrator renames the 'Default-First-Site-Name' and forgets to create subnets.

1. Install the Windows 2000 Support Tools (found in the `\support` folder on the Windows 2000 compact disc) on the Exchange 2000 server.
2. Run `NLTEST /DSGETSITENAME`. If a valid site name is returned, the Exchange 2000 server can determine which site it belongs to.
3. Run `NLTEST /DSGETDC:<domain-name>`. If valid information is returned, the Exchange 2000 server can communicate with the local domain controller.

Step 5. Verify the Correct Operation of the Domain

If the Exchange 2000 server can communicate with the local domain controller, you should verify that the domain is healthy and capable of running Exchange servers:

1. Run the DCDIAG tool (part of the Windows 2000 Support Tools). This tool verifies that the domain is healthy and all normal Active Directory operations can run successfully.
2. Run the POLICYTEST tool (found in the \support\utils\i386 folder on the Exchange 2000 CD). This tool verifies that all domain controllers have the Exchange-specific parts of the Group policy. Each domain controller should return **SeSecurityPrivilege**. If one or more domain controllers returns an error, you should rerun `SETUP /DomainPrep` in the domain. The most common symptom of this problem is failure to connect to Exchange 2000 databases.

Step 6. Look at the DSAccess Roles

If you have verified the previous five steps, DSAccess should be up and running. You should now interrogate the Exchange 2000 server to determine which Active Directory computers it is communicating with and verify their health:

- View the DSAccess server roles in System Manager (Exchange 2000 SP2 or later versions) or in event 2080 in the application log. Verify that each server on the working domain controller and working global catalog list reports itself as suitable. If one or more servers fail to meet this criterion, investigate the server.

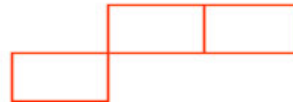
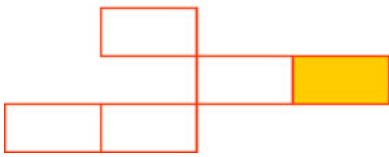
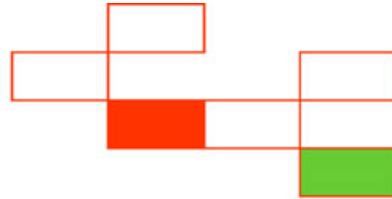
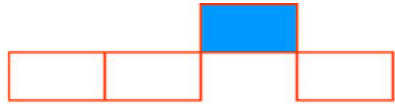
Step 7. Verify the Health of Each Active Directory Server

Examine the health of the Active Directory servers reported in event 2080 in the application log:

1. Ping each reported server by FQDN to verify that it responds.
2. Use an LDAP viewer such as LDP (ldp.exe), a support tool included with Microsoft Windows 2000, to verify that all reported domain controllers are responding to port 389 connections.
3. Use an LDAP viewer such as LDP (ldp.exe) to verify that all reported global catalog servers are responding to both port 389 and 3268 connections.
4. Check the CPU utilization on each reported Active Directory server. This attribute indicates whether the server is overloaded

5. Check the amount of memory installed in each Active Directory server to ensure that there are no discrepancies.
6. Check the date and time on each reported Active Directory server to verify that it matches the other domain controllers (within 60 seconds). Also, verify this information against the date and time reported by the Exchange 2000 server. Clocks that are not synchronized are a common cause of DSAccess errors.
7. Check for errors in the event logs of each domain controller. In the system log, see if the server is having general problems, and check for NetLogon events. In the directory service log, see if the server is having replication problems.

Appendixes



A

Sample Registry File

```
Windows Registry Editor Version 5.00

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\MSExchangeDSAccess\Instance0]
    "ConfigDCHostName"    = "configdc.microsoft.com"

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\MSExchangeDSAccess\Profiles\Default\UserDC1]
    "IsGC"                = dword:00
    "HostName"            = "firstDC.microsoft.com"

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\MSExchangeDSAccess\Profiles\Default\UserDC2]
    "IsGC"                = dword:00
    "HostName"            = "secondDC.microsoft.com"

[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\MSExchangeDSAccess\Profiles\Default\UserDC3]
    "IsGC"                = dword:00
    "HostName"            = "thirdDC.microsoft.com"
```

```
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\MSExchangeDSAccess\Profiles\Default\UserGC1]
```

```
"IsGC" = dword:01
```

```
"HostName" = "firstGC.microsoft.com"
```

```
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\MSExchangeDSAccess\Profiles\Default\UserGC2]
```

```
"IsGC" = dword:01
```

```
"HostName" = "secondGC.microsoft.com"
```

```
[HKEY_LOCAL_MACHINE\system\currentcontrolset\services\MSExchangeDSAccess\Profiles\Default\UserGC3]
```

```
"IsGC" = dword:01
```

```
"HostName" = "thirdGC.microsoft.com"
```

B

Common RPC and LDAP Error Codes

RPC Error Codes

```
0x800706bb = RPC_S_SERVER_TOO_BUSY  
0x800706d9 = EPT_S_NOT_REGISTERED
```

LDAP Error Codes

The following table (Table 5) lists LDAP error codes their corresponding Win32 messages. LDAP error codes may also appear in the format 0x800409xy, where the variables x and y indicate the reason for the error. For more information, go to the MSDN[®] Library <http://go.microsoft.com/fwlink/?LinkId=10149>.

Table 5 LDAP error codes

ADSI error value	LDAP message	Win32 message	Description
0L	LDAP_SUCCESS	NO_ERROR	The operation succeeded.
0x80070005L	LDAP_INSUFFICIENT_RIGHTS	ERROR_ACCESS_DENIED	The user has insufficient access rights.
0x80070008L	LDAP_NO_MEMORY	ERROR_NOT_ENOUGH_MEMORY	The system is out of memory.

Table 5 LDAP error codes (continued)

ADSI error value	LDAP message	Win32 message	Description
0x8007001fL	LDAP_OTHER	ERROR_GEN_FAILURE	An unknown error occurred.
0x800700eaL	LDAP_PARTIAL_RESULTS	ERROR_MORE_DATA	Partial results and referrals were received.
0x800700eaL	LDAP_MORE_RESULTS_TO_RETURN	ERROR_MORE_DATA	More results are to be returned.
0x800704c7L	LDAP_USER_CANCELLED	ERROR_CANCELLED	The user has cancelled the operation.
0x800704c9L	LDAP_CONNECT_ERROR	ERROR_CONNECTION_REFUSED	The server cannot establish the connection.
0x8007052eL	LDAP_INVALID_CREDENTIALS	ERROR_LOGON_FAILURE	The supplied credential is invalid.
0x800705b4L	LDAP_TIMEOUT	ERROR_TIMEOUT	The search was timed out.
0x80071392L	LDAP_ALREADY_EXISTS	ERROR_OBJECT_ALREADY_EXISTS	The object already exists.
0x8007200aL	LDAP_NO_SUCH_ATTRIBUTE	ERROR_DS_NO_ATTRIBUTE_OR_VALUE	Requested attribute does not exist.
0x8007200bL	LDAP_INVALID_SYNTAX	ERROR_DS_INVALID_ATTRIBUTE_SYNTAX	The syntax is invalid.
0x8007200cL	LDAP_UNDEFINED_TYPE	ERROR_DS_ATTRIBUTE_TYPE_UNDEFINED	Type is not defined.
0x8007200dL	LDAP_ATTRIBUTE_OR_VALUE_EXISTS	ERROR_DS_ATTRIBUTE_OR_VALUE_EXISTS	The attribute exists or the value has been assigned.
0x8007200eL	LDAP_BUSY	ERROR_DS_BUSY	The server is busy.

Table 5 LDAP error codes (continued)

ADSI error value	LDAP message	Win32 message	Description
0x8007200fL	LDAP_UNAVAILABLE	ERROR_DS_UNAVAIL ABLE	The server is not available.
0x80072014L	LDAP_OBJECT_CLASS_VIOLATION	ERROR_DS_OBJ_CLASS_VIOLATION	There was an object class violation.
0x80072015L	LDAP_NOT_ALLOWED_ON_NONLEAF	ERROR_DS_CANT_ON_NON_LEAF	Operation is not allowed on a non-leaf object.
0x80072016L	LDAP_NOT_ALLOWED_ON_RDN	ERROR_DS_CANT_ON_RDN	Operation is not allowed on the relative distinguished name (RDN).
0x80072017L	LDAP_NO_OBJECT_CLASS_MODS	ERROR_DS_CANT_MOD_OBJ_CLASS	Cannot modify object class.
0x80072020L	LDAP_OPERATIONS_ERROR	ERROR_DS_OPERATIONS_ERROR	An operations error occurred.
0x80072021L	LDAP_PROTOCOL_ERROR	ERROR_DS_PROTOCOL_ERROR	A protocol error occurred.
0x80072022L	LDAP_TIMELIMIT_EXCEEDED	ERROR_DS_TIMELIMIT_EXCEEDED	The time limit has been exceeded.
0x80072023L	LDAP_SIZELIMIT_EXCEEDED	ERROR_DS_SIZELIMIT_EXCEEDED	The size limit has been exceeded.
0x80072024L	LDAP_ADMIN_LIMIT_EXCEEDED	ERROR_DS_ADMIN_LIMIT_EXCEEDED	The administration limit on the server has been exceeded.
0x80072025L	LDAP_COMPARE_FALSE	ERROR_DS_COMPARE_FALSE	Compare yielded FALSE.
0x80072026L	LDAP_COMPARE_TRUE	ERROR_DS_COMPARE_TRUE	Compare yielded TRUE.
0x80072027L	LDAP_AUTH_METHOD_NOT_SUPPORTED	ERROR_DS_AUTH_METHOD_NOT_SUPPORTED	The authentication method is not supported.

Table 5 LDAP error codes (continued)

ADSI error value	LDAP message	Win32 message	Description
0x80072028L	LDAP_STRONG_AUTH_REQUIRED	ERROR_DS_STRONG_AUTH_REQUIRED	Strong authentication is required.
0x80072029L	LDAP_INAPPROPRIATE_AUTH	ERROR_DS_INAPPROPRIATE_AUTH	The authentication is inappropriate.
0x8007202aL	LDAP_AUTH_UNKNOWN	ERROR_DS_AUTH_UNKNOWN	An unknown authentication error occurred.
0x8007202bL	LDAP_REFERRAL	ERROR_DS_REFERRAL	The server returned a referral.
0x8007202cL	LDAP_UNAVAILABLE_CRIT_EXTENSION	ERROR_DS_UNAVAILABLE_CRIT_EXTENSION	A critical extension is unavailable.
0x8007202dL	LDAP_CONFIDENTIALITY_REQUIRED	ERROR_DS_CONFIDENTIALITY_REQUIRED	Confidentiality is required.
0x8007202eL	LDAP_INAPPROPRIATE_MATCHING	ERROR_DS_INAPPROPRIATE_MATCHING	There was an inappropriate matching.
0x8007202fL	LDAP_CONSTRAINT_VIOLATION	ERROR_DS_CONSTRAINT_VIOLATION	There was a constraint violation.
0x80072030L	LDAP_NO_SUCH_OBJECT	ERROR_DS_NO_SUCH_OBJECT	The object does not exist.
0x80072031L	LDAP_ALIAS_PROBLEM	ERROR_DS_ALIAS_PROBLEM	The alias is invalid.
0x80072032L	LDAP_INVALID_DN_SYNTAX	ERROR_DS_INVALID_DN_SYNTAX	The distinguished name has an invalid syntax.
0x80072033L	LDAP_IS_LEAF	ERROR_DS_IS_LEAF	The object is a leaf.
0x80072034L	LDAP_ALIAS_DEREF_PROBLEM	ERROR_DS_ALIAS_DEREF_PROBLEM	Cannot dereference the alias.

Table 5 LDAP error codes (continued)

ADSI error value	LDAP message	Win32 message	Description
0x80072035L	LDAP_UNWILLING_TO_PERFORM	ERROR_DS_UNWILLING_TO_PERFORM	The server is unable to perform the request.
0x80072036L	LDAP_LOOP_DETECT	ERROR_DS_LOOP_DETECT	A loop was detected.
0x80072037L	LDAP_NAMING_VIOLATION	ERROR_DS_NAMING_VIOLATION	There was a naming violation.
0x80072038L	LDAP_RESULTS_TOO_LARGE	ERROR_DS_OBJECT_RESULTS_TOO_LARGE	The results returned are too large.
0x80072039L	LDAP_AFFECTS_MULTIPLE_DSAS	ERROR_DS_AFFECTS_MULTIPLE_DSAS	Multiple directory service agents are affected.
0x8007203aL	LDAP_SERVER_DOWN	ERROR_DS_SERVER_DOWN	Cannot contact the LDAP server.
0x8007203bL	LDAP_LOCAL_ERROR	ERROR_DS_LOCAL_ERROR	A local error occurred.
0x8007203cL	LDAP_ENCODING_ERROR	ERROR_DS_ENCODING_ERROR	An encoding error occurred.
0x8007203dL	LDAP_DECODING_ERROR	ERROR_DS_DECODING_ERROR	A decoding error occurred.
0x8007203eL	LDAP_FILTER_ERROR	ERROR_DS_FILTER_UNKNOWN	The search filter is bad.
0x8007203fL	LDAP_PARAM_ERROR	ERROR_DS_PARAM_ERROR	A bad parameter was passed to a routine.
0x80072040L	LDAP_NOT_SUPPORTED	ERROR_DS_NOT_SUPPORTED	The feature is not supported.
0x80072041L	LDAP_NO_RESULTS_RETURNED	ERROR_DS_NO_RESULTS_RETURNED	Results are not returned.

Table 5 LDAP error codes (continued)

ADSI error value	LDAP message	Win32 message	Description
0x80072042L	LDAP_CONTROL_NOT_FOUND	ERROR_DS_CONTROL_NOT_FOUND	The control was not found.
0x80072043L	LDAP_CLIENT_LOOP	ERROR_DS_CLIENT_LOOP	A client loop was detected.
0x80072044L	LDAP_REFERRAL_LIMIT_EXCEEDED	ERROR_DS_REFERRAL_LIMIT_EXCEEDED	The referral limit has been exceeded.

Additional Resources

Microsoft Exchange 2000 Web Site

<http://www.microsoft.com/exchange>

Microsoft Developer Network Web Site

<http://msdn.microsoft.com>

Microsoft Knowledge Base

The following Microsoft Knowledge Base articles are available on the Web at

<http://support.microsoft.com/>:

- Q305967, How to Clear Bad Information in Active Directory-Integrated DNS (<http://go.microsoft.com/fwlink/?LinkId=3052&ID=305967>)
- Q270836, XCLN: Exchange 2000 Static Port Mappings (<http://go.microsoft.com/fwlink/?LinkId=3052&ID=270836>)
- Q320228, XGEN: The “DisableNetLogonCheck” Registry Value and How to Use It (<http://go.microsoft.com/fwlink/?LinkId=3052&ID=320228>)
- Q320529, XADM: Using DSAccess in a Perimeter Network Firewall Scenario Requires a Registry Key Setting (<http://go.microsoft.com/fwlink/?LinkId=3052&ID=320529>)

For more information: <http://www.microsoft.com/exchange/>

Does this paper help you? Give us your feedback. On a scale of 1 (poor) to 5 (excellent), how do you rate this paper?

<mailto:exchdocs@microsoft.com?subject=Feedback: Understanding and Troubleshooting Directory Access>