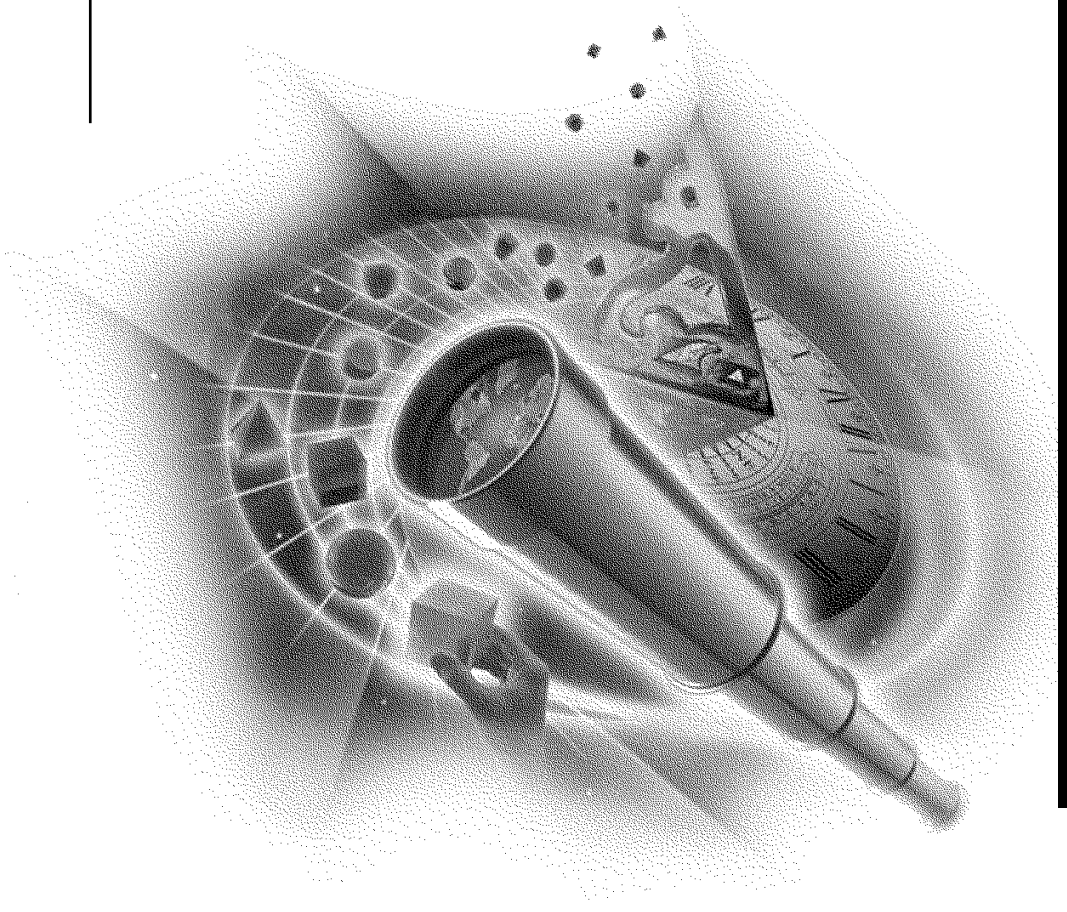
Novell® Directory Services®

Solutions

Guide



Novell®

Legal Notices

Novell, Inc.
1800 South Novell Place
Provo, UT 84606
U.S.A.

www.novell.com

NDS Solutions Guide
October 2000
104-001375-001

Online Documentation: To access the online documentation for this and other Novell products, and to get updates, see www.novell.com/documentation.

Novell Trademarks

BorderManager is a trademark of Novell, Inc.

ConsoleOne is a trademark of Novell, Inc.

NDS is a registered trademark of Novell, Inc., in the United States and other countries.

NetWare is a registered trademark of Novell, Inc., in the United States and other countries.

Novell is a registered trademark of Novell, Inc., in the United States and other countries.

Novell Client is a trademark of Novell, Inc.

Novell Directory Services is a registered trademark of Novell, Inc., in the United States and other countries.

Third-Party Trademarks

All third-party trademarks are the property of their respective owners.

Contents

Solutions Guide

This guide contains example solutions for deploying your directory services. In Chapter 1, “Administering LDAP,” on page 9, JSA Airlines utilizes the full power of NDS eDirectory’s LDAP 3 support. In Chapter 2, “Administering Account Management,” on page 27, Take-a-Break Travel uses Account Management 2.1 to easily manage their mixed-platform network.

1 Administering LDAP

Customer Scenario

JSA Airlines is a medium-sized airline company that offers service between various Western states in the United States. JSA Airlines needs to maintain a secure database with the reservation and credit card information for all passengers. The airline wants this database to be available to 5,000 certified agents for confirming, cancelling, or changing reservations. The agents also need to securely access to the credit card information to charge the customers' purchase prices and late fees.

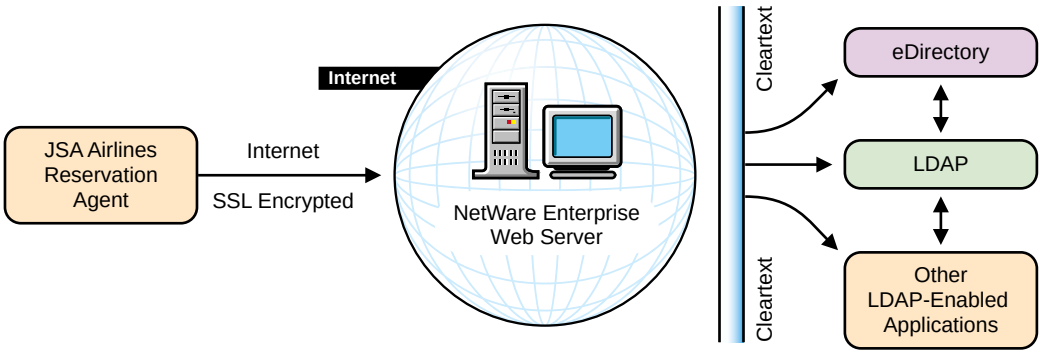
NDS eDirectory Solution

NDS® eDirectory™ with LDAP provides the customized service that JSA Airlines needs to accomplish its business goals. The LDAP compliance of NDS provides the following benefits to JSA Airlines:

- JSA Airlines can connect with various common third-party applications that use LDAP as their directory interface, such as Entrust*, Checkpoint* Firewall, Oblix, Netegrity, Netscape* Web Server, and other applications.
- Reservation agents at the airline can perform search queries for flight reservations. Therefore, each passenger and agent maintains a user identity so that passengers can specify unique information such as credit card information and preferred destinations. However, only certified agents can access this information on the LDAP server.
- JSA Airlines can maintain a secure environment for credit card information through SSL connections that protect data on the wire between the browser and the Web Server, especially passwords and credit card numbers.

The agents need to securely access the credit card information to charge the customers' purchase prices and late fees. To do this, the agents access NetWare Web Manager through an SSL encrypted Internet browser. However, the connection between the NetWare Web Server and the LDAP server relies on clear text passwords for authentication. Since JSA Airlines will only use one machine to maintain the Web Server and the LDAP server, the use of clear text passwords instead of encrypted passwords between the Web Server and the LDAP server does not present a security risk. However, if JSA Airlines expands their operation to include more hardware, then the airline will need to take more security precautions by including a router or a firewall.

Figure 1 The LDAP Solution for JSA Airlines



Requirements

- A Pentium* processor with 512 MB RAM and 2 GB hard disk space that operates as a stand-alone server
- NetWare 5.*x* with NetWare Enterprise Web Server
- NDS eDirectory 8.5

Setting Up the Environment

Installing NetWare and NDS eDirectory

The NetWare Web Server allows reservation agents to access information on the LDAP server through an Internet browser located at airport consoles, travel agencies, or home. From the Web Server, agents can view NDS

eDirectory and locate the passenger information for JSA Airlines on the LDAP server.

1. Install NetWare 5.1, which contains NetWare Enterprise Web Server.

   Select the default installation. For more information, see *NetWare 5.1 Installation Guide* (http://www.novell.com/documentation/lg/nw51/docui/).

2. Upgrade NDS on the Web Server to NDS eDirectory 8.5.

   For more information, see "Installing and Upgrading NDS eDirectory" in *NDS eDirectory Administration Guide.*

   Two new objects are added to the directory tree when NDS eDirectory 8.5 is installed:

   - The LDAP Server object sets up and manages the Novell® LDAP server properties.

     See "Configuring the LDAP Server Object" in *NDS eDirectory Administration Guide* for more information.

   - The LDAP Group object sets up and manages the way LDAP clients access and use the information on the Novell LDAP server.

     See "Configuring the LDAP Group Object" in *NDS eDirectory Administration Guide* for more information.

Setting Up LDAP in ConsoleOne

To access information from other LDAP-enabled applications, if needed, JSA Airlines must set up their users on an LDAP server.

Creating an LDAP User

Create a super user (such as ldapsuperuser) in ConsoleOne™ to use with LDAP, and give the user a password.

The reservation agents connect to the Web Server through an Internet browser where they authenticate as NDS users. However, these agents authenticate as the ldapsuperuser to access the LDAP server information.

Assigning Rights to the LDAP User

Since the JSA Airlines reservation agents need to access flight information and possibly change flight schedules and charge late fees, the users must have

read/write access to passenger information. Consequently, JSA Airlines must give users the proper rights to use the NetWare Web Manager interface and the ability to add users.

Make the ldapsuperuser a trustee of the Organization or Organizational Unit at the level where users are created. Grant the super user Create, Delete, and Write rights to the container.

To do this:

1. In ConsoleOne, select the Organization or Organizational Unit.
2. Right-click Trustees of This Object > click Add Trustees.
3. Select ldapsuperuser > check all entry and property rights > click OK > click Apply.

The ldapproxyuser will be granted all attribute rights, including Compare, Read, and Write rights, and all entry rights, including Browse and Create rights.

Associating the LDAP User to the LDAP Group Object

To associate the ldapsuperuser to the LDAP Group object:

1. In ConsoleOne, right-click the LDAP Group object.
2. Click Properties > the General tab.
3. Click Always Chain > check Allow Clear Text Passwords > click Apply > click OK.

   See "Configuring Chaining and Referrals" on page 22 and "Allowing Clear Text Passwords" on page 17 for more information.

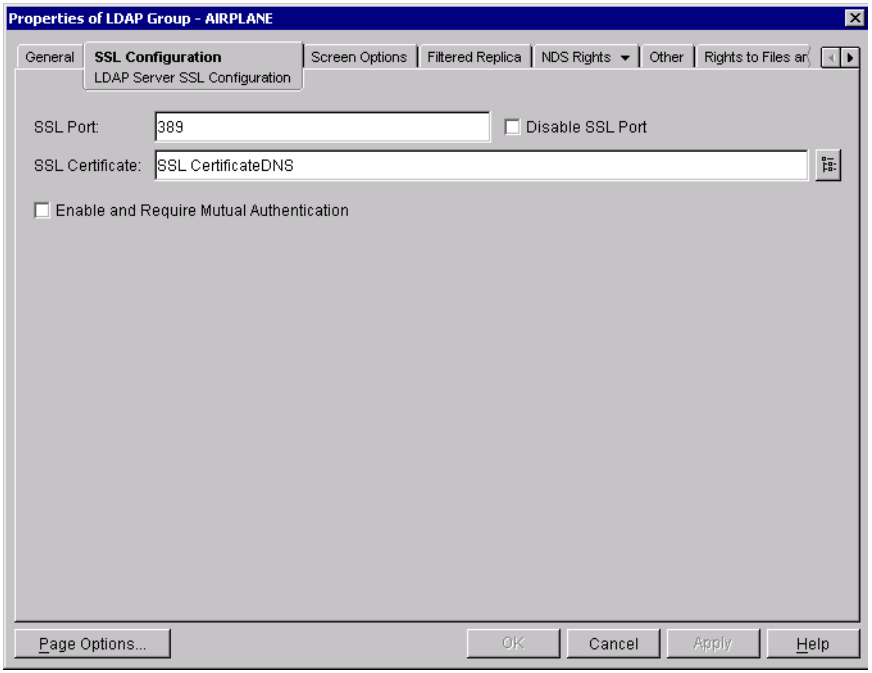
Enabling SSL Connections

Since JSA Airlines uses secure connections to protect credit card information, the company will use LDAP over SSL-encrypted connections. As reservation agents access this information through a secure Internet browser, the SSL encryption protects passwords and secure information through encryption on the wire between the Internet and the NetWare Web Server. However, clear text passwords protect information between the NetWare Web Server and the LDAP server.

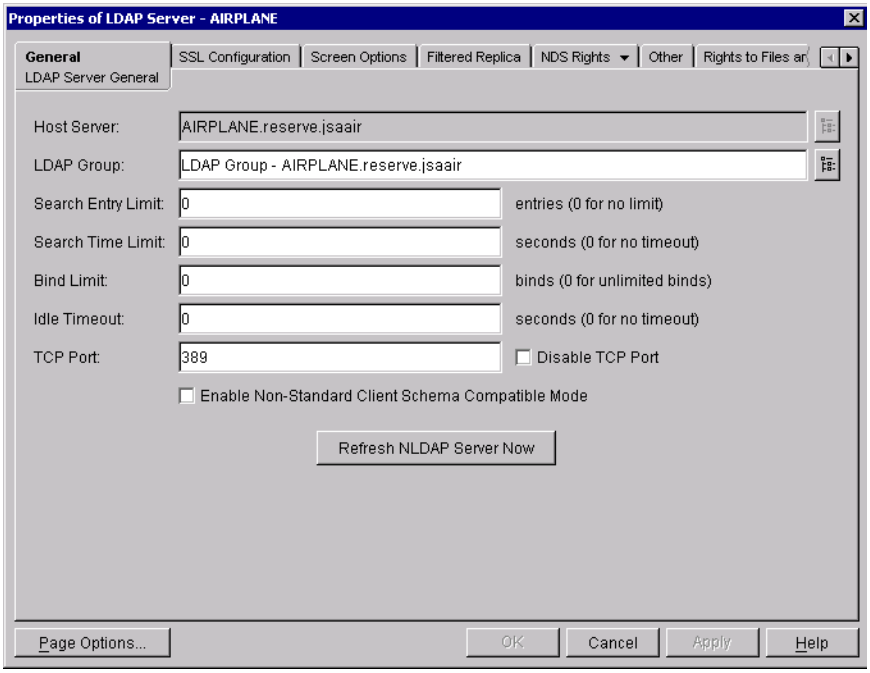
IMPORTANT: SSL connections are maintained from the browser to the Web Server. However, the connection between the Web Server and the LDAP server is non-SSL. Since JSA Airlines maintains the NetWare Web Server and the LDAP

server on the same machine, this does not present a security risk. However, a more complicated configuration would require additional security precautions by including a router or a firewall.

1 Open the LDAP Server object and associate an SSL Certificate, such as SSLCertificateDNS or SSLCertificateIP.



2 Browse to these objects > click Refresh NLDAP Server Now.



Setting Up NetWare Web Manager

Before the agents at JSA Airlines can access the LDAP server to validate passenger accounts, the NetWare Web Server needs to communicate to the LDAP server. The airline will need to configure the Web Server to access the LDAP server for information when agents log in. The LDAP server information, including the server name or IP address, enables the NetWare Web Server to authenticate to NDS eDirectory whenever users log in to the Web Server from a browser. Without this information, the application would need a proprietary database to store this information, but because the passenger information is already in NDS, the company can save the work of re-creating this passenger and password information in a different location.

Perform the following in NetWare Web Manager:

1. Enter https://*server_name_or_IP_address*:2200
2. Log in as Admin > select Global Settings > select LDAP directory server.

   IMPORTANT: The Web Server currently caches information and can access authenticated information for thirty minutes following authentication.
3. Populate the LDAP directory server configuration information.

3a Specify port 389.

The LDAP secure port 636 is currently disabled.

3b In the Base DN field, type the distinguished name, such as ou=reserve, o=jsaair, c=us.

3c In the Bind DN field, type the Bind DN that NetWare Web Manager uses to initially bind or log in to the directory server, such as cn=ldapsuperuser, o=jsaair, c=us.

3d In the Bind Password field, type the password for the ldapsuperuser > click OK > click OK.

4 Restart the Web Server.

4a Type **`nswebdn`** to stop the Web Server at the console prompt.

4b Type **`nsweb`** to start the Web Server.

5 Log in as ldapsuperuser.

After initially binding to the directory server as ldapsuperuser, log in to the Web Server as Admin to administrate the Web Server.

6 Select the Web Server link from the main directory in NetWare Web Manager.

JSA Airlines needs to create an Access Control List (ACL) to change the default from Allow Anyone, which does not require authentication, to Allow All, which only allows authenticated users. Only authenticated agents need to be allowed to access the LDAP server so they can change ticket information and prices accordingly.

7 Create an ACL by performing the following:

7a Click Restrict Access > click Browse > select the EDIR directory.

7b Click Edit > check Access Control Is On > click Submit.

By default, Access Control is off.

7c Click Deny > change Deny to Allow > click Update.

7d Click Anyone > change Anyone to All in the authentication database > click Update > click Save and Apply > click Submit.

Using LDAP Features

Configuring SSL Connections

Because JSA Airlines stores credit card information in the database, it is vital that this information be stored in a secure environment. The SSL protocol uses public/private key technology and X.509 certificates to perform the following tasks:

- Authenticate the Web Server to the client
- Authenticate the client to the Web Server (optional)
- Encrypt the data that flows between the client and the Web Server

The LDAP server uses SSL connections to encrypt the data that flows between the client and the Web Server.

After completing the authentication, the TCP/IP connection is secure. This is accomplished by using secrets and keys passed back and forth during the SSL connection. Another benefit of SSL data transfer is that the protocol ensures that the data integrity is not compromised. In other words, it prevents an intruder from tampering with the data as it is sent between the client and server.

In NDS eDirectory, the certificate authority (CA) and Key Material objects are installed by default when the airline accepts the certificate server. However, JSA Airlines can also configure this information manually.

See "Enabling Secure LDAP Connections" in *NDS eDirectory Administration Guide* for more information.

Importing and Migrating Data

The Novell Import Conversion Export Utility lets JSA Airlines import and export LDIF files and migrate data between LDAP servers. The airline can use this utility to import entries from a file to an LDAP directory and modify the entries in a directory from a file. It also supports schema modifications by allowing the administrator to specify attributes and class definitions in an LDIF file.

For more information, see "Novell Import Conversion Export Utility" in *NDS eDirectory Administration Guide.*

Debugging

Allowing Clear Text Passwords

Setting the clear text password allows JSA Airlines to see the wire protocol in unencrypted form.

The simple form of an LDAP bind is achieved by sending the DN and unencrypted password to the server. However, sending a password over the Internet presents security risks. Consequently, the Novell LDAP server, by default, does not permit this simple bind. The Allow Clear Text Passwords option must first be checked.

If Allow Clear Text Passwords is not checked, the simple bind request fails unless it is made over an SSL connection. If the user attempts a search, the user will bind using the anonymous connection. For more information, see “Configuring SSL Connections” on page 16. If a test environment is used or if security is not an issue, allowing clear text passwords over the normal unsecured TCP connection might be an option.

Screen and File Logging

The Screen Options panel illustrated in the following graphic provides a way for JSA Airlines to control the types of messages output to the Debug Trace screen while the server is processing requests.

JSA Airlines can select all the options, or to decrease traffic, only the ones needed to troubleshoot a particular problem.The following is a list of the screen options settings for the LDAP server and what types of messages they control:

- Critical Error Messages

  Corresponds to messages that are reported when a severe error is encountered. These errors typically signal a condition that causes the server to stop responding.

- Non-Critical Error Messages

  The set of all errors either caused by erroneous user data and requests. These are also the non-critical errors the server encounters that cause an operation to fail.

- Configuration Processing

  Allows messages relating to the server that is updating configuration data. These messages appear when starting or refreshing the LDAP server.

- Informational Messages

  Allows messages that provide useful information but do not signal an error condition. Examples include search time and size limit exceeded and the starting and stopping of operations.

- Search Response Summary

  Sends messages that are related to search results to the trace screen. This is a separate option because the search operation is complex, and generates significant traffic and numerous trace messages. If experiencing a problem with a search, the administrator might need to check just this flag to reduce the amount of messages.

- Messages from LDAP Extended Operations

  Displays informational messages from LDAP extended operations.

- Connection Information

  Displays messages associated with LDAP connections. The amount of information received when this option is checked can be large. This information is typically only useful for connection-related problems.

- Packet Dump or Decoding

  Displays all BER-encoded packets that are received. This generates a tremendous amount of data. This is useful if the client is sending erroneous data.

- Additional connection and operation debugging information on all available messages

  Causes some low-level connection and operation information to be added to each operation. This is useful when many operations flow into the server and a specific operation needs to be tracked.

Tuning for Optimal Performance

After JSA Airlines sets up and implements their NDS eDirectory LDAP environment, they will use the optimal setting for LDAP searches and authentication on a server with two processors and 2 GB of RAM:

Maximum TCP port limit	45000
Maximum pending TCP connection requests	4096
Maximum packet receive buffers	10000
Minimum packet receive buffers	3000
Maximum physical receive packet sizes	2048
Maximum concurrent disk cache writes	2000
Maximum concurrent directory cache writes	500
Maximum directory cache buffers	200000
Maximum number of internal directory handles	100
Maximum number of directory handles	20
DSTRACE	!m*xxxxxx*. Replace *xxxxxx* with the amount of RAM in bytes to use as cache. On Windows* NT*, create a text file named _NDSDB.INI in the NDS directory, then add this line.

Managing the Memory

NDS eDirectory uses memory for the database cache and for directory usage.These are separate allocated memory pools. The directory engine uses memory from available memory pools in the operating system as needed. The database uses a cache pool that is defined by parameters detailed below. Usually, the more database cache given to NDS eDirectory, the better the performance. However, since NDS eDirectory uses available system memory for its buffers, if clients are performing queries that require large data sets to be returned, the size of the database cache might need to be decreased to have enough system memory for the directory to handle building the query responses.

The database engine uses the database cache to hold the most recently accessed blocks. This cache is initially defined with a fixed size of 16 MB. The size of this cache can be changed from the command line in shipping versions of eDirectory 8.5. The following example command will set the eDirectory database cache to 80 million bytes:

```
set dstrace=!mb 80000000
```

A file named _NDSDN.INI in the SYS:_NETWARE directory on a NetWare server can also be defined, or in the directory containing the eDirectory database files on the Windows, Solaris*, and Linux* environments (normally \novell\nds\dbfiles). This text file simply needs to contain a line such as the following:

```
cache=80000000
```

IMPORTANT: Don't add any white space next to the equals (=) sign

The cache in NDS eDirectory 8.5 can be initialized with a hard limit just as with earlier versions. In addition, the upper and lower limits can be set either as hard numbers or as a percentage of available memory. Dynamic allocation control parameters allow the cache size to grow or shrink depending on use. If the proper configuration parameters are set, the database cache dynamically grows or shrinks based on other system resource needs.

Editing the _NDSDB.INI file can manually control database memory usage. The format for .INI file commands is given below:

```
cache=cacheBytes # set_a_hard_memory_limit
```

An alternative format is given in the following table.

cache=*cache options*	Set a hard limit or dynamically adjusting limit. Multiple cache options can be specified in any order, separated by commas. All are optional and are as follows:
DYN or HARD	Dynamic or hard limit.
AVAIL or TOTAL	These only apply for a hard limit. Omit these for a dynamic limit.
%:*percentage*	The percentage of available or total physical memory.
MIN:*bytes*	The minimum number of bytes.

MAX:*bytes*	The maximum number of bytes.
LEAVE:*bytes*	The minimum number of bytes to leave for the OS.
blockcachepercent=*percentage*	The split of cache between block and record cache.

If a hard limit is specified and the administrator wants to define the database cache to use a percentage of the memory, the administrator can select between a percentage of total memory or a percentage of available memory. Dynamic limits always refer to a percentage of available memory. The following command examples are all valid in the _NDSDB.INI file:

The following is an example of a dynamic limit of 75% available memory, a minimum of 16 million bytes, and 32 million bytes for the OS.

```
cache=DYN,%:75,MIN:16000000, LEAVE 32000000
```

The following is an example of a hard limit of 75% total physical memory, a minimum of 18 million bytes, and a maximum of 512 million bytes.

```
cache=HARD, TOTAL,%:75,MIN:18000000, MAX 512000000
```

The following is an example of an old style hard limit of 8 million bytes.

```
cache=8000000
```

The database cache is divided between block cache and record cache. Block cache holds data and index blocks that mirror the storage on the disk. Record cache holds in-memory representations of directory objects and attributes. If updating or adding to the directory, use the block cache setting. If performing mostly reads, use the record cache. It is possible to cause a thrashing condition in both caches if performing numerous sequential updates without allocating cache size properly. Unless specifically changed, the cache is allocated to be 50% block cache and 50% record cache. The blockcachepercent option can be included in the _NDSDB.INI file to specify the percentage of cache allocated to caching data and index blocks. (The default is 50%.) The remaining cache is used for entries.

For example, to designate 60% block cache and 40% record cache, enter the following:

```
blockcachepercent=60
```

Do not select 100% of the cache for either block or record cache and ignore the other cache type. In general, do not allocate more than 75% of your cache memory to one or the other type.

Database cache settings can also be controlled using NDS iMonitor. See "NDS iMonitor" in *NDS eDirectory Administration Guide* for more information.

Configuring Chaining and Referrals

Since JSA Airlines uses only one server, all name resolution options are equivalent. However, if the JSA Airlines expands the network, the airline will need to carefully evaluate what name resolution model to use. In this situation, JSA Airlines could use name resolution out-of-the-box. However, alternate modes of name resolution would enable the administrator to tune NDS to perform more efficiently for the needs of JSA Airlines.

To understand chaining and referrals, an understanding of partitions and replicas is essential.

Partitions and Replicas

A partition is similar to an LDAP naming context and is a portion of the directory hierarchy sectioned off from all the rest and mastered by one or more replicas.

If a user needs information about an object that resides on a different server, the server can either examine the reference object and retrieve the information itself from the other server by chaining, or it can simply return the reference to the client in the form of a referral to tell the client where to get the information itself.

Chaining

Chaining is essentially a server-based name resolution protocol. In the chaining model of name resolution, an LDAP client issues a request to an LDAP server. The LDAP server attempts to find the target entry locally. If the entry cannot be found, the LDAP server accesses another LDAP server with the DN. The second server might not have the entry and might access information from yet another server. The process continues until the first server contacts a server that holds a replica of the entry.

NOTE: Previous versions of LDAP on NDS that supported options for name resolution models used the term traversal instead of chaining in the LDAP administration snap-ins to ConsoleOne and NetWare Administrator. The current

implementation now uses the term chaining in both the server implementation and administration tools.

Once an entry is located in the chaining model, NDS completes the operation. Even if the target entry is on a remote server, NDS conceals this from the client. In this situation, the server to which the client is connected locates the remote server containing the target entry, then authenticates to the remote server using the same identity of the LDAP client. Next, the server acts as proxy for the client and requests that the remote server complete the operation, then reports the result of the operation to the client just as if the entry is stored locally.

Advantages of Chaining	Disadvantages of Chaining
The server hides all name resolution details from the client. The client simply connects to a server, binds, and performs an operation.	If chaining requires establishing connections with several different servers before the target entry is located, or if any of these connections are across slow WAN links, the client can be left without feedback of any kind for an extended period of time, resulting in errors.
The server automatically takes care of re-authentication. Only when NDS locates the server that actually contains the target entry does it create a connection to that server specifically for the LDAP client and authenticate that connection with the client's identity.	In the chaining model, the information describing where an entry is stored is hidden from the client, so it can't be subsequently used by the client. However, the first server might have access to it and be able to use it to increase its efficiency on the client's behalf.

Referrals

Referrals provide clients with a more controlled form of name resolution. In the referral model of name resolution, an LDAP client issues a request to an LDAP server. The server attempts to locate the target entry of the operation locally. If it cannot find the target entry locally, the server uses references to generate a referral to another server with more information about the target entry and returns the referral information to the LDAP client. The LDAP client then establishes a connection to the server specified in the referral and reloads the operation.If the second LDAP server contains the target entry of the operation, the server performs the operation. Otherwise, the server sends a referral back to the client. This continues until the client contacts a server

that has the entry and can perform the desired operation or an LDAP server returns an error indicating that the entry doesn't exist.

Advantages of Referrals	Disadvantages of Referrals
The client is completely in control. At every stage of the name resolution process, the client knows exactly what is occurring and can make better decisions or provide feedback to the user if desired.	If the operation request fails because the desired entry is not stored locally, the work to complete the bind was essentially wasted, since it was not needed. To work around this, the client can do an anonymous base-level search for the target entry of the operation before binding, but this adds additional complexity to the client's job.
Referrals often use network resources more efficiently. If the client uses referrals instead of chaining, it receives the results of the operation from the second server, and the data only needs to be transferred once.	LDAP referrals were not made an official part of the protocol until LDAP 3. LDAP 2 clients don't recognize referrals, or they use an obsolete, non-standard method for recognizing referrals.
Once the client knows where an entry is stored, it can go directly back to the server that has it.	

NDS eDirectory provides three options in the Referral Option box:

- Always Chain (Even to NDS LDAP Servers That Support Referrals)

  This option forces the server to follow referrals for the client. The option also allows the LDAP server to authenticate to the other servers using public and private key pairs. This prevents the client from repeatedly binding to a new server every time it gets a referral.

  This option is ideal if older versions of NDS servers that are not LDAP-compliant exist in the tree. When a server is chaining on the client's behalf, it uses NDAP to connect to the other NDS servers in the tree.

- Refer to NDS LDAP Servers That Support Referrals; Chain to NDS Servers That Don't

  This option attempts to return LDAP referrals if it can, but if it runs into a portion of the tree that is not serviced by an LDAP server, it chains instead. If the tree is comprised of some NDS servers that are not LDAP-compliant, but referrals need to be returned whenever possible, select this option.

- Always Refer (All NDS LDAP Servers in the Tree Must Support Referrals)

  Selecting this option forces the server to always return referrals to LDAP 3 clients and never chain to another server. This works only in an environment where all of the servers are LDAP-compliant and are running versions of LDAP capable of returning referrals.

  This option is ideal if the clients need more control over following a referral. For instance, if the server itself follows referrals on a network that spans the globe, a user might end up waiting hours for a subtree search to complete, because the server has to connect with other servers on the other side of the world.

  The Default Referral field specifies a default referral to be used when Always Refer is selected. This could be used when pointing to a non-NDS LDAP server or an NDS LDAP server in another tree. To specify a default referral, type the URL of the server in this field. Only the host, port, and DN parts of the LDAP URL are used here. When NDS cannot locate a referral to a server that contains an entry, it sends the URL in the Default Referral field as a referral. If nothing is specified in the Default Referral field, then a No Such Object error is sent.

JSA Airlines will use Always Chain, because the airline database relies on LAN connections, and the company does not want the clients to repeatedly re-authenticate. The reservation agents need seamless access to the databases that are all connected centrally.

Managing Indexes

To maximize performance and query time, JSA Airlines indexes information that is frequently accessed.

NDS eDirectory 8.5 can store a tremendous amount of data on a single server. The restrictions in earlier versions of NDS, such as a limit of 5,000 objects in a container, limited containers in a partition, and limited objects held on a single server were removed when NDS eDirectory 8.5 was released.

The more data that can be held on a server, the more time it takes to get a single entry. Many directories have a high performance when enough RAM is available on the directory server to cache the entire content of the directory. However, as directory size grows beyond the capacity of the cache, performance decreases dramatically.

The greatest factor in LDAP search performance in eDirectory is the use of indexes. When an LDAP search filter is analyzed, the directory determines if an index that has been defined on the server can be applied to the search. This significantly improves the performance of queries on a server.

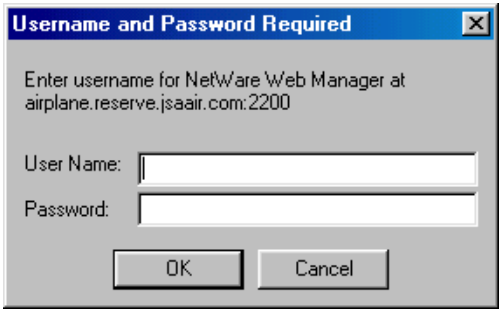
See "Index Manager" in *NDS eDirectory Administration Guide* for more information. Detailed information on handling indexes in eDirectory can be found in How to Supercharge LDAP Searches with eDirectory Indexes (http://developer.novell.com/research/appnotes/2000/july/05/apv.htm).

Combining the LDAP Solution and Users

After setting up this LDAP environment for the NetWare Enterprise Web Server, the reservation agents can access database information from the Internet browsers in their offices or in the airports.

To access the information, the reservation agents need only perform the following:

1. Enter a URL, such as https:reservations.jsair.com, into an Internet browser.
2. Log in as an NDS eDirectory user.



3. Perform a search query and access the data.

2 Administering Account Management

Account Management 2.1 is a directory-enabled application that simplifies the management of user profiles on Windows* NT*, Solaris*, and Linux* networks. This chapter examines how a travel agency implemented Account Management 2.1 to eliminate the complexities of administering a mixed-platform network.

Customer Scenario

Take-a-Break Travel is one of the largest travel agencies in the Western United States, with full-service offices in five states. The agency specializes in vacation packages, cruises, and escorted tours by all methods of travel, including air, train, bus, car, and boat.

Take-a-Break Travel's operating system is a mixed Windows 95/Windows NT* environment with NetWare® servers. The company wants to implement an application that will require the creation of NT domain and NT domain user accounts, but it also needs a solution for how to administer two accounts (one for NetWare and one for NT) for each travel agent in the company.

Table 1 Take-a-Break Travel's Company Make-Up

Number of servers	25% Windows NT 4.0 75% NetWare 5.1 servers running NDS® eDirectory™ 8.5
Number of users corporate-wide	7,500
Number of users logging in concurrently	5,000
Number of containers in a tree	1025

Number of trees	1
Hardware	Compaq* servers, Dell* desktop and laptop workstations

Users at Take-a-Break Travel log in from approximately 90 locations. The company's five major offices are T1-connected. Each user logs in to a local server, then can access resources across a WAN. Some users who travel between offices connect through a BorderManager™ server using the Novell® VPN client.

The travel agency's goal is to simplify the management of customer profiles on its mixed NetWare and Windows NT network. It also wants to leverage the scalability of NDS and thereby eliminate the cost of managing more than one account per user.

Solution

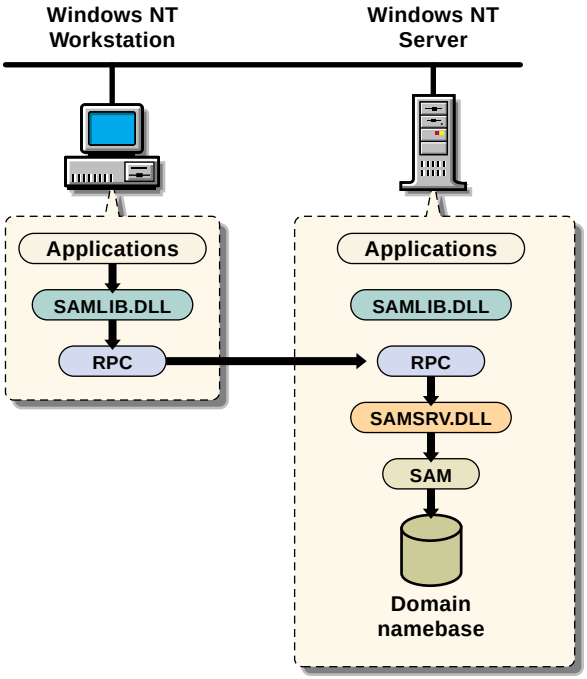
To accomplish these business goals, Take-a-Break Travel should deploy Account Management, which upgrades the Windows NT domain system to a true directory service. The company's travel agents can then access the network with a single login with one password, and full NT application support for its mixed network. The travel agency's administrator should also have a single point of administration for the entire network.

Understanding Account Management

On Windows NT, resources are created and managed in a database called the System Account Manager (SAM). Applications that need information from the Windows NT domain make requests to SAMLIB.DLL. This includes applications running on the NT server or on an NT workstation.

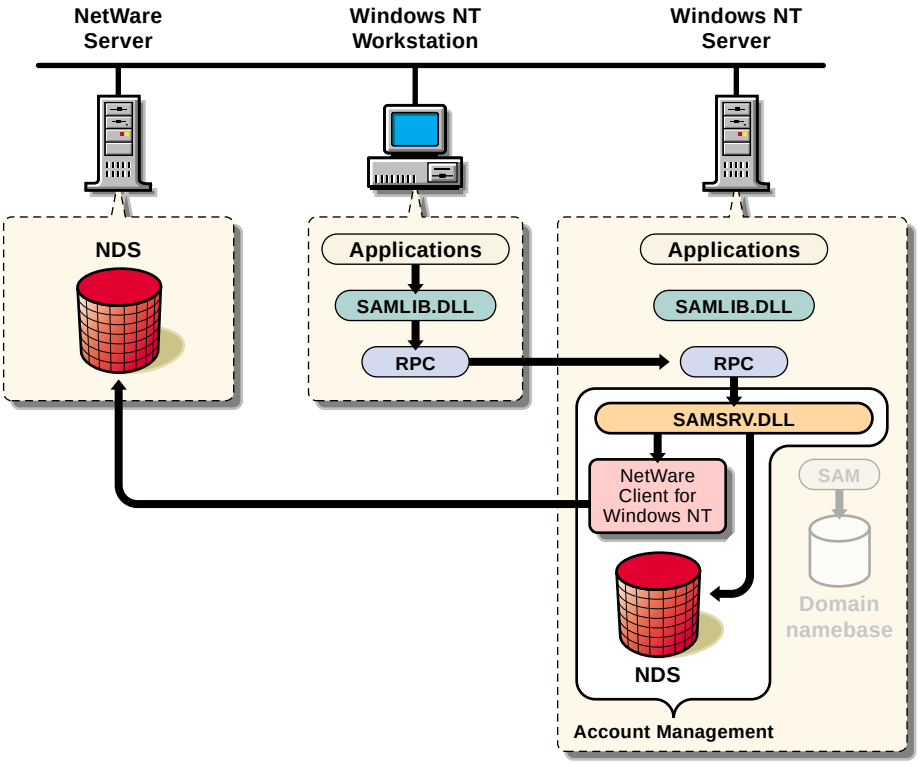
SAMLIB.DLL communicates to SAMSRV.DLL using Remote Procedure Calls (RPCs). For applications being run on the server, this communication is done internally. For requests originating from a workstation, the RPC requests are sent to the server. Once the server RPC receives a request, it is extracted and passed to SAMSRV.DLL. SAMSRV.DLL then accesses the System Accounts Manager where the domain namebase is stored and performs the requested operation. See Figure 2 on page 29.

Figure 2



Account Management relocates Windows NT domains into NDS eDirectory by first replacing the Microsoft* SAMSRV.DLL with an NDS eDirectory-based SAMSRV.DLL. The Domain Object Wizard then relocates the domain. The Domain Object Wizard copies all of the desired domain information into NDS eDirectory. The new SAMSRV.DLL redirects all domain calls, after the product is installed, to NDS eDirectory instead of the domains SAM database. All application requests to the domain namebase are then redirected to NDS eDirectory (which can reside on a NetWare server, an NT server, or both). NDS eDirectory stores the User, Computer, and Group objects that take the place of the objects previously used from the domain. See Figure 3 on page 30.

Figure 3



The advantage of Account Management for Take-a-Break Travel is that all existing applications continue to work without any change. The company can continue to utilize the Windows NT tools to manage accounts in NDS eDirectory. NDS eDirectory containers can scale into hundreds of thousands of objects, unlike NT Domain objects, which are limited to a few thousand.

Since Take-a-Break Travel already has servers installed and has a large number of users and computers defined, Account Management provides a wizard utility that will help the company to easily migrate Windows NT domains into NDS. The wizard enables the company's administrator to navigate through the process of creating the Domain object in NDS, then creating all defined Computer and Group objects. For User objects already existing in the domain, new NDS User objects can be created, or they can be associated with existing NDS User objects, thus simplifying the task of moving the agency's existing domain to NDS.

Take-a-Break Travel can also use ConsoleOne™ to create new domain user members, computers, and groups.

The agency's Windows NT network is installed with a primary domain controller (PDC) and six backup domain controllers (BDCs). The domain namebase is stored on each domain controller in a single master configuration. This means that each domain controller can provide information to requesting entities, but all changes to the domain must be made at the PDC. The PDC then replicates the changes down to each of the BDCs. Account Management moves the domain namebase into NDS where it is referenced by both primary and backup domain controllers. In order for all domain controllers to have access to the domain information stored in NDS, all PDCs and BDCs must have Account Management installed.

Benefits

Account Management will provide the following benefits to Take-a-Break Travel:

- Each office will have access to all pertinent network resources in a seamless manner without compromising security
- The cost of network ownership will be reduced by the simplification of network administration
- Administrators will spend less time managing the company's multi-platform network
- Single NDS User objects will be able to become members of multiple domains if needed

Additional Benefits

Account Management will benefit Take-a-Break Travel with the following new features in Account Management 2.1:

- Domain Cache Management

  Domain Cache Management improves performance and lowers network utilization by updating the domain cache at specific times or time intervals. This feature is enabled from the PDC and BDC Workstation objects located in the Domain object in ConsoleOne. Cache updates can be updated all the time, at certain times, or at certain time intervals. See "Domain Cache Management" in *Account Management 2.1 Administration Guide* for more information.

- Event Logging

  This feature shows whether the user is logged in to the computer with the cached account and logs other critical events such as those relating to SPSENTRY. See "Event Logging" in *Account Management 2.1 Administration Guide* for more information.

- Domain Administration

  Domain Administration allows and disallows user administration from NT User Manager. Using this feature, Take-a-Break Travel's administrator can add NDS users to a domain that he or she does not have rights to. To enable this, the Domain object must have trustee rights to any container that contains users the administrator wants to grant domain rights to. See "Domain Administration" in *Account Management 2.1 Administration Guide* for more information.

- Dial In Information

  The Dial In information associated with users in NT User Manager can be managed from ConsoleOne. Take-a-Break Travel's administrator can grant users permission to use Dial-Up Networking when connecting to the network. User Dial In also lets the administrator set domain-wide permissions or permissions for specific computers. See "Dial In Information" in *Account Management 2.1 Administration Guide* for more information.

- Anonymous Password Change

  This feature manages whether users must log in to their accounts to change their passwords. See "Anonymous Password Change" in *Account Management 2.1 Administration Guide* for more information.

- Password Filter Support

  Password Filter Support allows Take-a-Break Travel's administrator to put a filter in place that enforces certain password characteristics, such as certain length, characters, and numerals.

  Upon installation, the Novell SAMSRV.DLL recognizes if a password filter has been implemented, and uses the filter to provide the boundaries for password changes. Account Management implements password filter support automatically.

Implementation

This section contains the following information about Take-a-Break Travel's implementation of Account Management:

- System Requirements
- Setting Up the Environment
- Installing Account Management

System Requirements

To implement Account Management on Windows NT, Take-a-Break Travel should use the following components:

- ❑ Pentium* 200 computers with 64 MB of RAM and a monitor color palette set to a number higher than 16
- ❑ Administrative rights to the NT server and to all portions of the NDS tree that contain domain-enabled User objects
- ❑ NetWare 5.1 with Support Pack 1 and with NDS eDirectory 8.5
- ❑ Workstations running Novell Client™ for Windows NT 4.71 or later

For more information about recommended system requirements, see "Minimum System Requirements" in *Account Management 2.1 Administration Guide*.

Setting Up the Environment

Before installing Account Management, the administrator for Take-a-Break Travel should complete the following tasks:

- Ensure that NDS versions, synchronization, and replica distribution are appropriate
- Resolve duplicate names
- Determine the location in the tree where Domain objects should be placed
- Update all operating systems to the required service levels

Installing Account Management

At the NT server, Take-a-Break Travel's administrator should log in as Administrator, then run SETUP.EXE from the *Account Management* CD.

The administrator should select from the following components (which can be installed separately or together):

- Integrating Windows NT Domains with NDS
- ConsoleOne

Integrating Windows NT Domains with NDS

Account Management installs the current release of the Novell Client (if necessary) and the Account Management components.

After the server reboots, Take-a-Break Travel's administrator should continue with the following steps, first on the PDCs, then on the BDCs.

1. Log in to the NDS tree as Admin or the equivalent.
2. Log in to the domain as Administrator or a user with administrator privileges.
3. When the Domain Object Wizard launches, Take-a-Break Travel's administrator should follow the online instructions.

   The administrator can move NT domain users to NDS or associate existing NDS users with NT domain users.

   When the Domain Object Wizard finishes running, the NT server reboots.

Installing ConsoleOne

To install ConsoleOne, Take-a-Break Travel's administrator should follow the online instructions in the Installation Wizard. This installs ConsoleOne 1.2d as a management utility and creates a Share called SYS: on the NT server.

Managing Windows NT Accounts

Each Windows NT domain is represented by a Domain object in ConsoleOne. This Domain object, created with the Domain Object Wizard, is a container object that behaves similarly to a Group object in that it not only holds information about the domain and users which are members of the domain, but also contains member objects such as computers and groups, just as an actual

domain. See “Integrating Windows NT Domains with NDS” on page 34 for more information on the Domain Object Wizard.

The Domain object acts as a group with a list of domain members. The computers and groups associated with the domain are represented as objects contained by the NDS eDirectory Domain object. By making User objects members of the domain rather than actually residing within the domain, Take-a-Break Travel’s administrator can place the NDS eDirectory User objects anywhere in the tree and still give users access to specific domains.

Using the NDS for NT snap-in to ConsoleOne, Take-a-Break Travel’s administrator can create Local Group objects, Global Group objects, and Workstation objects. The administrator can also add users to or remove users from Group objects or Domain objects. This means that Take-a-Break Travel’s administrator doesn’t have to learn different applications to manage objects such as Users and Groups.

The following sections contain the steps Take-a-Break Travel’s administrator should take to do the following:

Creating a New Local Group

1. In ConsoleOne, right-click the domain the new local group should be created in.
2. Click New > Object.
3. In the Class list, click NDS for NT Local Group > OK.
4. Specify the group name.
5. (Optional) Check one of the following two check boxes:

Check Box	Description
Define Additional Properties	Lets properties be set for the group being created
Create Another Local Group	Lets another group be created

6 Click OK.

Creating a New Global Group

1 In ConsoleOne, right-click the domain the new global group should be created in.

2 Click New > Object.

3 In the Class list, click NDS for NT Global Group > OK.

4 Specify the group name.

5 (Optional) Check one of the following two check boxes:

Check Box	Description
Define Additional Properties	Lets properties be set for the group being created
Create Another Global Group	Lets another group be created

6 Click OK.

Creating a New Workstation Object

1 In ConsoleOne, right-click the domain where the new Workstation object should be created.

2 Click New > Object.

3 In the Class list, click NDS for NT Workstation > OK.

4 Specify the workstation name.

The workstation name must end with a dollar sign ($). It can be up to 16 characters long including the $.

5 (Optional) Check one of the following two check boxes:

Check Box	Description
Define Additional Properties	Lets properties be set for the workstation being created
Create Another Workstation	Lets another workstation be created

6 Click OK.

Adding an NDS User to an NT Domain

Take-a-Break Travel's administrator can add an NDS user to an NT domain in either of the following ways:

- "Adding an NDS User to an NT Domain through the NDS User Object" on page 37
- "Adding an NDS User to an NT Domain through the Domain Object" on page 38

Adding an NDS User to an NT Domain through the NDS User Object

1 In ConsoleOne, right-click the NDS User object to be added to the domain.

2 Click Properties > Domain Access.

3 Select Group Memberships.

The Add button is enabled but the Delete button is disabled. (The Group Memberships line cannot be deleted.)

4 Click Add.

5 Browse to and select the domain to add the user to.

The administrator can also browse further down and select Local or Global groups. If a Local or Global group is selected, both the group and the domain it belongs to will be added to the user's group memberships. The group called Domain Users will also be added, selected or not, as the user's primary group.

6 Click OK > OK.

Adding an NDS User to an NT Domain through the Domain Object

1. In ConsoleOne, right-click the Domain object to add an NDS User object to.
2. Click Properties > Domain Members.
3. Click Add to browse to and select NDS User objects

   or

   Ctrl-click Add to browse to and select Novell NDS Group objects.
4. Select the NDS User or NDS Group object to be added to the domain.

   If an NDS group is selected, the individual users, not the group itself, are added to the domain.
5. Click OK > OK.

Adding an NDS User to a Local or Global Group

Take-a-Break Travel's administrator can add an NDS user to a Local or Global group in either of the following ways:

- "Adding an NDS User to a Local or Global Group through the NDS User Object" on page 38
- "Adding an NDS User to a Local or Global Group through the Group Object" on page 39

Adding an NDS User to a Local or Global Group through the NDS User Object

1. In ConsoleOne, right-click the NDS User object to add to the Local or Global group.
2. Click Properties > Domain Access.
3. Select a domain

   or

   Select Group Memberships.

   The Add button is enabled but the delete button is disabled. (The Group Memberships line cannot be deleted.)
4. Click Add.

   If you select a domain, then click Add, that domain's Group objects are displayed in the Select Object dialog box.

5 Browse to and select a Local or Global group.

If the user is not a member of the domain the group belongs to, both the group and the domain are added to the user's Group Memberships. The group called Domain Users is also added, selected or not, as the user's primary group.

6 Click OK > OK.

Adding an NDS User to a Local or Global Group through the Group Object

1 In ConsoleOne, right-click the Local or Global group to be added to an NDS User object.

2 Click Properties > Identification > Add.

3 Select the member to be added to the Local or Global group.

Users that are not already members of the domain cannot be added using the browser. The user must first be added to the domain. See "Adding an NDS User to an NT Domain" on page 37.

4 Click OK > OK.

Deleting Users from NT Domains

For information about deleting users from NT domains, see the following sections in *Account Management 2.1 Administration Guide*:

- Deleting an NDS User from an NT Domain
- Deleting an NDS User from an NT Domain through the NDS User Object
- Deleting an NDS User from an NT Domain through the Domain Object
- Deleting an NDS User from a Local or Global Group
- Deleting an NDS User from a Local or Global Group through the User Object
- Deleting an NDS User from a Local or Global Group through the Group Object

Setting a User's Primary Group

To belong to a domain, a user must be a member of at least one group within that domain. The user cannot be deleted from his or her primary group. This primary group is displayed on the Domain Access page in bold. By default, the Domain Users group is set as the primary group.

To set up a user's primary group, Take-a-Break Travel's administrator should do the following:

1. In ConsoleOne, right-click the user whose primary group should change.
2. Click Properties > Domain Access.
3. Select the group to be set as the new primary group.

   When the Group Memberships line, a domain, or a local group is selected, the Set Primary Group button is disabled. Only a global group can be set as the primary group.

   When the current primary group (displayed in bold) is selected, the Set Primary Group button is disabled.
4. Click Set Primary Group > OK.

   The selected group becomes the primary group and is displayed in bold; the group that was previously the primary group is no longer in bold.

Identification

Take-a-Break Travel's administrator can view, enter, or modify information about Domain objects, Groups, and Workstations.

Domain Identification

To view or modify domain identification, Take-a-Break Travel's administrator should do the following:

1. In ConsoleOne, right-click a Domain object.
2. Click Properties > Domain Identification.
3. Select from the following options:

Option	Description
Description	Describes the selected Domain object.
OEM Information	Imports information from NT domains during migration.
Default User Creation Context	Sets the context that locates new users created by NT User Manager. This field is not used by ConsoleOne during the creation process.

4 Click Apply > OK.

Group Identification

To view or modify group identification, Take-a-Break Travel's administrator should do the following:

1 In ConsoleOne, right-click a Local or Global Group object.

2 Click Properties > Identification.

3 Enter or view information about the selected Group object.

Workstation Identification

To view or modify workstation identification, Take-a-Break Travel's administrator should do the following:

1 In ConsoleOne, right-click an NDS for NT Workstation object.

2 Click Properties > Identification.

3 Enter or view the complete name of the workstation and information describing the selected Workstation object.

Enabling Performance Enhancement Settings

To enable performance enhancement settings, Take-a-Break Travel's administrator should do the following:

1 In NT User Manager, right-click a Domain object.

2 Click Properties > Domain Identification.

3 In the Advanced Settings box, select from the following options:

Option	Description
Default User Creation Force Password Sync	Sets the context for new users created by NT User Manager. This field is not used by ConsoleOne during the user creation process. If this check box is checked, NT and NDS passwords are synchronized for users created through NT User Manager.

Option	Description
Use Fast User Display	Speeds up queries for user information in NT User Manager and in ConsoleOne. If this option is checked, NT User Manager displays only the username in the initial list and ConsoleOne displays only the username and context in the initial list. Once a username is selected, additional information is displayed.
On User Added through Snap-in, Enable Administration from NT Tools	Allows new users created in NT User Manager to be managed from NT User Manager.
Users Must Log On in Order to Change Password	Requires users to be logged in to the network to change password security information.

4 Click Apply > OK.

Using the Replica Advisor

User objects that are members of an NT domain can be relocated during or after an NDS for NT installation to any partition. The domain User objects can also be associated with existing NDS User objects in any partition of the NDS tree. This association between Domain and NDS objects occurs when the Domain Object Wizard is run and users are migrated to NDS, eliminating the need for accounts on both NDS and NT for a single user.

The Replica Advisor page of the Domain object shows all the partitions containing the User objects that have membership in the domain. When the partition item is expanded, it lists User objects in that partition.

Another entry displays which partition the Domain object is in. The Domain object and its subordinate groups contain information that is used during login and authentication to resources.

To view a replica, Take-a-Break Travel's administrator should do the following:

1 In ConsoleOne, right-click a Domain object.

2 Click Object > Details.

3 Select the Replica Advisor page.

Partitions that hold Domain, User, and Group objects are shown with the partition symbol.

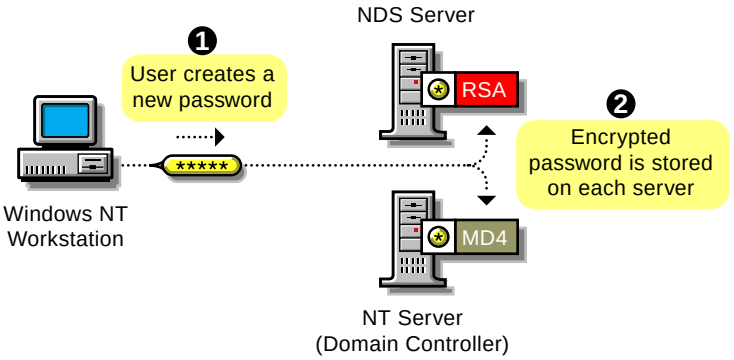
Managing Security on Windows NT

Windows NT uses an MD4 password encryption algorithm, which creates a fixed length hash from the user's password. Such hashes are not very secure. NDS eDirectory, however, uses a public and private key method of encryption called RSA encryption to protect critical information (such as passwords). These public and private keys are created specifically for each user using the password. The public key can be easily shared and passed around. The private key is held securely within NDS eDirectory in a vault associated with the User object.

When a password is initially created at a workstation, it does not cross the wire as clear text. Instead, the Novell Client running on the workstation uses an RSA encryption key received from an NDS server to encrypt the password before it leaves the workstation and hits the wire. That password is received at the server and is entered (in its encrypted form) into NDS.

When a user logs in, the password is used to create a secret token that is sent to NDS eDirectory for verification. If the NDS server accepts that the token has been generated only by the actual user, it allows an authenticated session to be set up. At the same time, the password is also encrypted with the MD4 algorithm and sent to the NT domain controller. This encrypted value is compared to the one stored in the Domain User object. If they match, the user is authenticated to the NT server. This authentication process is secure because the encryption process that is performed on each password is irreversible. See Figure 4 on page 44.

Figure 4 Password Encryption



With Account Management, the respective environments check both passwords. Both passwords, however, are stored in NDS eDirectory. The authentication process is equally secure, since the encryption process performed on each password is still irreversible.

Figure 5 and Figure 6 on page 45 illustrate password checking with and without Account Management.

Figure 5 Password Checking in a Mixed NDS/Domain Network

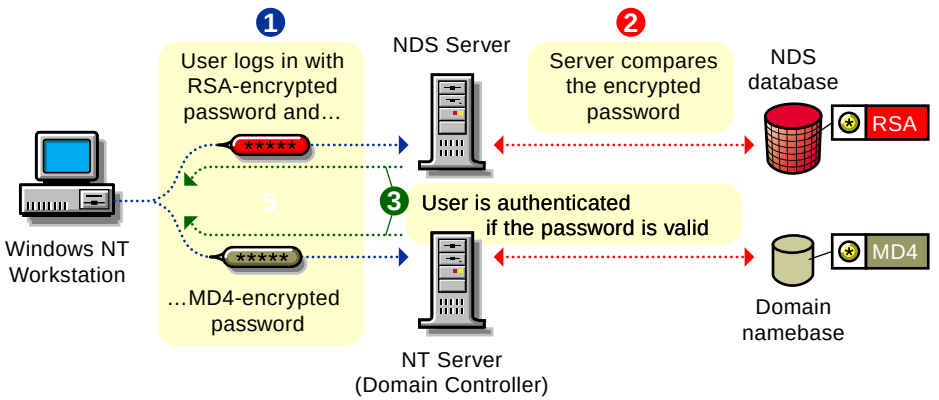
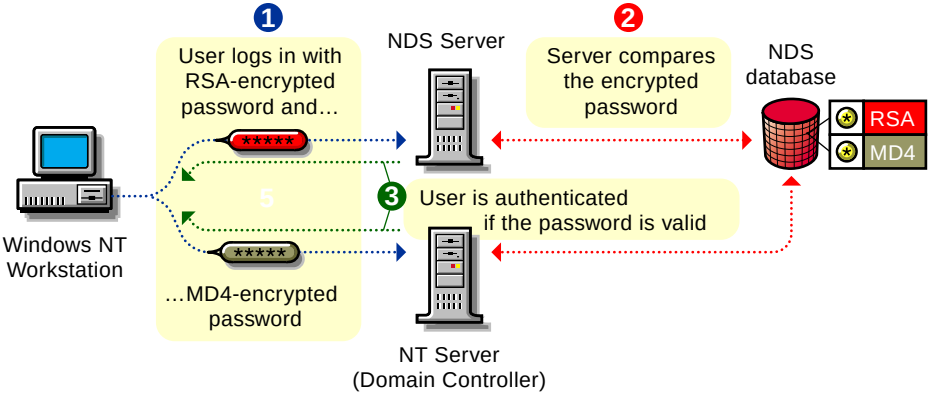


Figure 6 Password Checking with Account Management



Synchronizing a User's NDS and NT Passwords

This procedure lets Take-a-Break Travel synchronize both the NDS and NT passwords. The password change is immediate and cannot be undone by clicking Cancel.

The following are the steps the administrator should follow to synchronize the passwords:

1. In ConsoleOne, right-click the User object for the user whose password should change.
2. Click Properties > Domain Access.

   If the user is not a member of a group or domain, Set Both Passwords is disabled. If groups or domains have been added to the Memberships list, but have not been committed to the NDS database, Set Both Passwords remains disabled. The administrator must first add the user to the domain.
3. Check the Force Password Sync check box > click Apply.
4. Click the Restrictions-Password Restrictions page > Change Passwords.

   Because Take-a-Break's administrator is a system administrator, the Old Password field is disabled. See "Synchronizing a User's NDS and NT Passwords" in *Account Management 2.1 Administration Guide* for steps to follow when the user is not a system administrator.
5. Click OK.

Setting Intruder Detection

Take-a-Break Travel's administrator should do the following to activate or deactivate intruder detection:

1. In ConsoleOne, right-click the domain where intruder detection should be activated or deactivated.
2. Click Properties > Domain-Intruder Detection.
3. Check the Detect Intruders check box to activate intruder detection or uncheck the box to deactivate intruder detection.

   The default limit is seven incorrect login attempts in 30 minutes. Lock Account after Detection is also set automatically with a default interval of 15 minutes.
4. Adjust the default limits and the Intruder Lockout Reset Interval, if necessary.
5. Click OK.