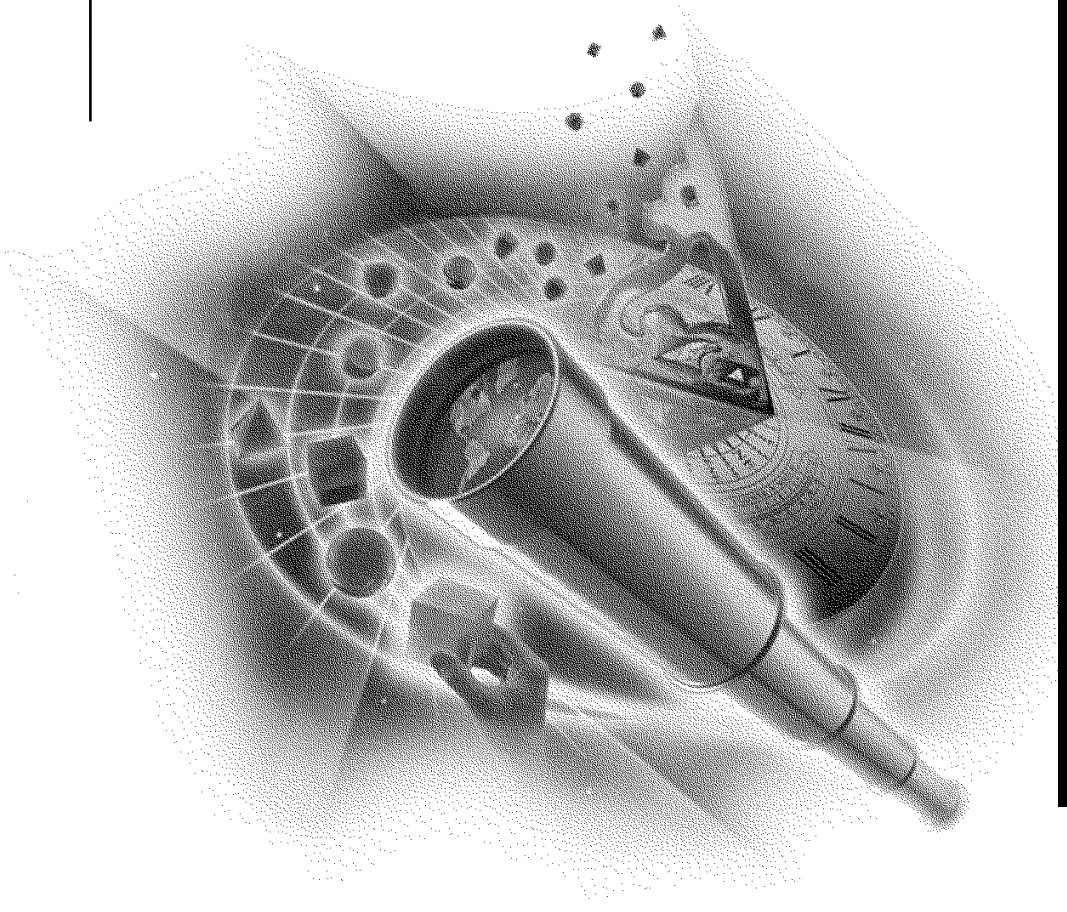
LDAP Configuration



NDS™ 7

Novell®

Legal Notices

Novell, Inc.
122 East 1700 South
Provo, UT 84606
U.S.A.

www.novell.com

LDAP Configuration
January 2000
104-001268-001

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

Novell Trademarks

For a list of Novell trademarks, see the final appendix of this book.

Third-Party Trademarks

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

Contents

LDAP Configuration . . . 7

1 Understanding . . . 9

Understanding LDAP Services for NDS . . . 9
What's New in Version 3.0 . . . 10
LDAP Version 3 Features in NetWare 5 . . . 10
Other NetWare 5 LDAP Features . . . 12
Understanding Lightweight Directory Access Protocol (LDAP) . . . 12
Understanding NDS Rights . . . 13
[Public] User (Anonymous Bind) . . . 13
Proxy User (Proxy User Anonymous Bind) . . . 14
NDS User (NDS User Bind) . . . 15
Understanding Secure Sockets Layer (SSL) Protocol . . . 16
Overview . . . 16
Key Material Object . . . 16
SSL Configuration . . . 17
Understanding Class and Attribute Mappings . . . 18
Understanding Auxiliary Class Support . . . 18
Understanding LDAP vs. NDS Syntax . . . 19
Commas . . . 20
Typeful Names Only . . . 20
Escape Character . . . 20
Multiple Naming Attributes . . . 20

2 Setting Up . . . 23

Installing LDAP Services for NDS . . . 23
Configuring the LDAP Server Object . . . 23
Configure and LDAP Server Object . . . 24
Configuring the LDAP Group Object . . . 24
Property Pages . . . 24
Configure an LDAP Group Object . . . 25
Configuring the User Object . . . 25
Configure the User Object . . . 25
Assigning NDS Rights for LDAP Clients . . . 25
Setting Up Access Control Lists (ACL) . . . 27
Overview . . . 27
ACL Processing Order . . . 27
Setting Up an LDAP Client . . . 28

Setting Up a Test Server Configuration 28
Configure LDAP Services for NDS for Testing Client Communications 29
Using LDAP in a Wide Area Network Environment 30

3 Troubleshooting 33

Determining Why LDAP Clients Cannot Bind to LDAP Services for NDS 33
Determining Why the Server Isn't Using a New Configuration 33
Determining Why Question Marks Appear in NetWare Administrator 34

A Novell Trademarks 35

LDAP Configuration

The Lightweight Directory Access Protocol (LDAP) in NetWare® 5 is configured and managed using LDAP Services for NDS™, a snap-in to the NetWare Administrator utility (nwadmn32.exe). LDAP Services for NDS 3.0 is a server application that allows LDAP clients to access read and write information stored in NDS. With LDAP Services for NDS, all your NDS data is available and you define the directory information that is accessible to LDAP clients and the clients that can access the directory. You can also give different clients different levels of directory access or access the directory over a secure connection. These security mechanisms allow you to make some types of directory information available to the public, other types available to your organization, and certain types available only to specified groups or individuals.

1 Understanding

This section gives overview information of LDAP Services for NDS™ 3.0.

Understanding LDAP Services for NDS

LDAP Services for NDS is a NetWare® server application (nldap.nlm) that allows LDAP clients to access information stored in NDS.

With LDAP Services for NDS, you define the directory information you want to make accessible and grant the rights to the LDAP clients that you want to have access to the directory. Using the NetWare Administrator utility, you can specify all the attributes of the LDAP clients and set all security information in one place.

You can give different clients different levels of directory access, or you can access the directory over a secure connection. These security mechanisms allow you to make some types of directory information available to the public, other types available to your organization, and certain types available only to specified groups or individuals.

The directory features available to LDAP clients depend on the features built in to the LDAP server and the LDAP client. For example, LDAP Services for NDS allows LDAP clients to read and write data in the NDS database if the client has the necessary permissions. Some clients have the capability to read and write data; others can only read directory data.

Some typical client features allow clients to do one or more of the following:

- Look up information about a specific person, such as an e-mail address or phone number
- Look up information for all people with a given last name, or a last name that begins with a certain letter

- Look up information about any NDS object or entry
- Retrieve a name, e-mail address, business phone number, and home phone number
- Retrieve company name and city name
- Retrieve any information in the NDS database

What's New in Version 3.0

LDAP Version 3 Features in NetWare 5

RootDSE Request

NetWare 5 includes support for a RootDSE request from a v3 client. The RootDSE request allows the client to discover what features are available from the LDAP server (authentication mechanisms, controls, schema). In NetWare 5, the RootDSE object is Read-only. If the RootDSE were writable, then it would be possible to extend the NDS schema through a write operation on the RootDSE object.

Auxiliary Classes

There is support for the auxiliary classes currently required by Netscape and Entrust in NetWare 5. A more flexible auxiliary classes mechanism is pending support of this feature in NDS itself.

LDAP v3 Bind Request

NetWare 5 LDAP supports a clients bind request that includes v3 in the version field. Simple authentication is the only supported authentication mechanism in NetWare 5 LDAP.

LDAP v3 Implied Bind

NetWare 5 LDAP will perform an implied bind if a request from a client is received without a prior explicit bind request. For instance, if a server sees a search request from a client that has not issued a bind request, it will perform a bind for this client as an anonymous user and proceed with the search request.

SASL Authentication

LDAP v3 requires simple authentication (username and password) and recommends protected and strong mechanisms as defined in X.500. Any authentication mechanism in LDAP v3 other than simple is handled through SASL. NetWare 5 LDAP supports the required simple mechanism and fails other mechanisms (through SASL) as specified in the LDAP v3 spec.

Controls

LDAP v3 specifies that a client can request or demand controls on a search request (sorted, paged, etc). Supported controls are contained in a RootDSE response. If a client requests a control, it can be ignored by the server (which is done in NetWare 5). If a client demands a control (termed 'critical control') and the server cannot handle it, then it must return a failure (which is done in NetWare 5). LDAP does not support any controls in NetWare 5.

Extended Requests

Supported extended requests in LDAP v3 are reported through RootDSE (there currently aren't any). Any unsupported extended requests must return a failure (which is done in NetWare 5).

Internationalization

The NetWare 5 LDAP supports international characters in UTF-8 format, as specified by the LDAP spec. UTF-8 is basically an ASCII-safe transformation of Unicode.

Modify DN

LDAP v2 supported a ModifyRDN operation, which could only rename an object within its existing container. LDAP v3 supports ModifyDN, which can move an object to a new container. ModifyDN in supported in NetWare 5.

Referrals

In LDAP v3, referrals were returned to clients by forcing them into an error field in the protocol. LDAP v3 provides for a new, more explicit method of returning referrals. The new mechanism is supported in NetWare 5. However, the referral that is returned is not a true NDS referral to an NDS server that contains the information requested. Instead, the user can enter, via NetWare Administrator, a single-server URL that will be returned in all referrals from

this server. If LDAP URLs were included in the NDS replica set information, then true NDS referrals could be returned via LDAP.

Other NetWare 5 LDAP Features

SSL

NetWare 5 LDAP supports LDAP access over an SSL encrypted channel.

Dclient Interface

LDAP uses the Dclient interface to NDS. This allows for multiple parallel connections, rather than serializing requests as the 1.0 version did. It also provides faster NDS access.

Catalog Services Integration

LDAP can be configured to access NDS data from a catalog. This provides significantly faster access, especially in a tree that is geographically widely distributed or a tree that is structurally flat with large numbers of objects per container. LDAP can be configured to use catalog data only, to use live NDS data only, or to use the catalog first and fall back to NDS for data not contained in the catalog.

Configuration Stored in NDS

LDAP now stores its configuration data in NDS rather than in a separate config file. Configuration can be updated at any time using NetWare Administrator.

Understanding Lightweight Directory Access Protocol (LDAP)

Widespread acceptance and implementation of Internet and intranet technologies have made networks much larger and more complex than in the past. These larger networks, in turn, have created a greater need for a comprehensive directory service and a standard method for accessing information located in the directory.

The Lightweight Directory Access Protocol (LDAP) is a developing Internet communications protocol that allows client applications to access directory information. It is based on the X.500 Directory Access Protocol (DAP) but is

less complex than a traditional client and can be used with any other directory service that follows the X.500 standard.

The most popular current use of LDAP is for allowing clients to access directory services that store and publish telephone numbers and e-mail addresses.

For more information about LDAP, refer to the following:

- The University of Michigan (http://www.umich.edu/~dirsvcs/ldap/ldap.html)
- Critical Angle Inc. (http://www.critical-angle.com/ldapworld/index.html)

Understanding NDS Rights

LDAP Services for NDS allows LDAP clients to access data in NDS directories. All LDAP clients bind, or connect, to NDS as one of the following types of users:

- [Public] user
- Proxy user
- NDS user

Login restrictions and password restrictions will still apply; however, any restrictions will be relative to where LDAP is running. Time and address restrictions are honored, but address restrictions are relative to where the NDS login occurred--in this case, the LDAP server. Also, as LDAP does not support grace logins, it is possible to log in to NetWare and yet not be able to bind to LDAP.

[Public] User (Anonymous Bind)

An anonymous bind is a bind that does not contain a username or password. If an LDAP client binds to LDAP Services for NDS and the service is not configured to use a proxy user, the user is authenticated to NDS as user [Public]. User [Public] is a nonauthenticated NDS user. By default, user [Public] is assigned the Browse right to the objects and attributes in the NDS tree. The default Browse right for user [Public] allows users to browse NDS objects but blocks user access to object attributes. The default [Public] rights are typically too limited for most LDAP clients. Although you can change the

[Public] rights, this will give these rights to all users. Because of this, use of the Proxy User Anonymous bind is suggested.

To enable user [Public] access to object attributes, you must make user [Public] a trustee of the appropriate container or containers and assign the appropriate object and attribute rights.

NOTE: Rights to specific attributes currently cannot be inherited in NDS. If you want to grant Read and Search rights to a particular attribute, you must do so for all NDS objects to be accessed, not just a parent object. The rights assigned to user [Public] are available to anyone who accesses NDS. This access can be set up through LDAP Services for NDS or through any NetWare utility, such as NetWare Administrator.

Proxy User (Proxy User Anonymous Bind)

A proxy user anonymous bind is an anonymous bind that is linked to a normal NDS username. If an LDAP client binds to LDAP Services for NDS anonymously and the service is configured to use a proxy user, the user is authenticated to NDS as the proxy user, whose name is configured in LDAP Services for NDS and in NDS.

To implement proxy user anonymous binds, you must create the Proxy User object in NDS and assign the appropriate rights to that user. Assign the Proxy User Read and Search rights to all objects and attributes in each subtree where access is needed. Use LDAP Access Control Lists (ACL) to restrict access as necessary. You also need to enable the proxy user in LDAP Services for NDS by specifying the same proxy username.

The key concepts of proxy user anonymous binds are as follows:

- All LDAP client access through anonymous binds is assigned through the Proxy User object.
- The proxy user cannot have a password or any password restrictions (such as password change intervals), because LDAP clients do not supply passwords during anonymous binds. You should not force the password to expire or allow the proxy user to change passwords. You may want to limit the locations from which the user can log in by setting address restrictions for the Proxy User object through the Network Address Restrictions page of NetWare Administrator.
- The Proxy User object must be created in NDS and assigned rights to the NDS objects you want to publish. The default user rights provide Read access to a limited set of objects and attributes. Assign the Proxy User Read and Search rights to all objects and attributes in each subtree where access is needed. Use LDAP ACLs to restrict access as necessary.

- The Proxy User object must be enabled on the General page of the LDAP Group object that configures LDAP Services for NDS. Because of this, there is only one Proxy User object for all servers in an LDAP group.
- You can configure Access Control Lists (ACL) in the LDAP Group object to add access controls for the proxy user. For example, you can create an Access Control List that allows the proxy user access through one IP address or a group of IP addresses.

NDS User (NDS User Bind)

An NDS user bind is a bind that an LDAP client makes using a complete NDS username and password. The NDS user bind is authenticated in NDS, and the LDAP client is allowed access to any information the NDS user is allowed to access.

When LDAP Services for NDS is installed, NDS user bind requests using cleartext (unencrypted) passwords are refused by default. Cleartext passwords and NDS usernames entered by LDAP clients on non-Secure Socket Layer (SSL) connections are vulnerable to capture by network monitoring equipment. Anyone who captures an NDS username and password has immediate access through an LDAP or NDS client to all the NDS objects to which the captured username has access. NDS user binds should only be used on LDAP servers that are configured to use SSL.

NOTE: Even though cleartext passwords are not accepted by default, this does not prevent users from trying to bind with their usernames and passwords. On an unsecured connection, all attempted binds expose the username and password to eavesdropping, whether or not the bind is successful. However, not allowing cleartext passwords for NDS user binds discourages users from using their names and passwords, because this method of binding will be unsuccessful.

To support NDS user binds on non-SSL connections, you must allow cleartext passwords within the LDAP Group object.

The key concepts of NDS user binds are as follows:

- NDS user binds are authenticated to NDS using the username and password entered at the LDAP client.
- On non-SSL connections, the NDS password is transmitted in cleartext on the path between the LDAP client and LDAP Services for NDS.
- Any NDS username and password used for LDAP client access can also be used for NetWare client access to NDS.

- To support NDS user binds on non-SSL connections, you must allow cleartext passwords. To enable this feature, check the Allow Cleartext Passwords check box on the LDAP Group object using NetWare Administrator for Windows* 95* or NetWare Administrator for Windows NT*.
- If cleartext passwords are not enabled, all NDS bind requests that include a username or password on non-SSL connections are rejected.
- If an NDS user password has expired, NDS bind requests for that user are rejected.

The type of bind with which the user authenticates has a direct effect on the content the LDAP client can access. LDAP clients access a directory by building a request and sending it to the directory. When an LDAP client sends a request through LDAP Services for NDS, NDS completes the request for only those attributes to which the LDAP client has the appropriate access rights. For example, if the LDAP client requests an attribute value (which requires the Read right) and the username is granted only the Compare right to that attribute, the request is rejected.

Understanding Secure Sockets Layer (SSL) Protocol

Overview

LDAP Services for NDS supports the Secure Sockets Layer (SSL) protocol to ensure that the connection over which data is transmitted is secure and private.

SSL is a protocol that establishes and maintains secure communication between SSL-enabled servers and clients across the Internet. To ensure message integrity, SSL uses a hashing algorithm. To ensure message privacy, SSL provides for the creation and use of encrypted communications channels. To prevent message forgery, SSL allows the server and, optionally, the client to authenticate each other during the establishment of the secure connection. This release of LDAP does not ask the LDAP client to authenticate itself.

Key Material Object

To implement the authentication and encryption processes, SSL uses a cryptographic mechanism called public keys. To establish a secure connection, the server and the client exchange their public keys to establish a session key. The session key will be used to encrypt the data for the life of the connection. A subsequent LDAP connection over SSL will result in the generation of a new session key that is different from the previous one.

Digital certificates, digital IDs, digital passports, or public key certificates are critical for verifying the identity of the contacted server. They are similar to an employee badge that identifies the wearer as an employee of a company.

Each LDAP server requires a digital certificate to implement SSL. Digital certificates are issued by a certification authority (CA). Certificates are stored in a new NDS object, the Key Material object. Use Novell® PKI Services, a snap-in of the NetWare Administrator utility (nwadmn32.exe), to request, manage, and store certificates in NDS. Refer to the Novell PKI Services help system for details on setting up a certificate on a server. You can access Novell PKI Services help by selecting the Help button from any Key Material object page.

In order for the LDAP server to use a specific certificate for LDAP SSL connectivity once it is stored in NDS, you must indicate the Key Material object containing the certificate on the LDAP Server General Page in NetWare Administrator.

NOTE: The Key Material object must be in the same container as the NetWare Server object that will use it.

SSL Configuration

Although SSL can be configured on both the client and server to ensure the identity of both parties, clients do not require digital certificates to communicate securely. As the LDAP server listens for SSL connections on a special port, all the client needs to do is initiate the connection over that port.

NOTE: When you make changes to your LDAP Services for NDS configuration using NetWare Administrator, many of the changes take effect dynamically without having to restart the LDAP server. However, most SSL configuration changes require a restart. Note the following:

- If SSL is disabled, you can enable it without restarting the LDAP server, and the enabling will occur dynamically.
- If SSL is enabled and you disable it, you must restart the LDAP server in order for the disabling to take effect.
- If you make any configuration changes to the SSL port or the SSL certificate, you must restart the LDAP server for the changes to take effect.

To restart the LDAP Server, type the following at the NetWare server console prompt:

```
UNLOAD NLDAP
LOAD NLDAP
```

Understanding Class and Attribute Mappings

A class is a type of object in a Directory, such as a user, a server, or a group. An attribute is a Directory element that defines additional information about a specific object. For example, a User object attribute might be a user's surname or phone number. In NetWare Administrator, classes are called object types or classes and attributes are called properties.

A schema is a set of rules that defines the classes and attributes allowed in a Directory and the structure of a Directory (where the classes can be in relationship to one another). Because the schemas of the LDAP directory and the NDS Directory are different, mapping of LDAP classes and attributes to the appropriate NDS objects and attributes is necessary. These mappings define the name conversion from the LDAP schema to the NDS schema.

LDAP Services for NDS provides default mappings. In many cases, the correspondence between the LDAP classes and attributes and the NDS object types and properties is logical and intuitive. However, depending on your implementation needs, you might want to reconfigure the class and attribute mapping.

In most instances, the LDAP class to NDS object type mapping is a one-to-one relationship. However, the LDAP schema supports a feature called auxiliary class support that allows an object to be associated with more than one class.

Understanding Auxiliary Class Support

The LDAP directory schema is different from the NDS directory schema. In an NDS directory, an object has a base class. The base class is part of a class hierarchy. The base class is a subclass of other classes and inherits the classes for which it is subclassed. Only a single base class can be associated with the object. The object can contain or inherit only the attributes associated with that class.

In NDS, to add more functionality (attributes) to the object, you must extend the class by adding more attributes to the class definition. In an LDAP

directory, standard classes are static and cannot be extended. However, the LDAP schema allows an object to belong to more than one class and to inherit attributes from more than one class. This association of multiple classes is called auxiliary class support.

Although the NDS schema does not allow multiple class associations, LDAP Services for NDS can emulate auxiliary class support for the following selected subset of LDAP classes:

- strongAuthenticationUser
- certificationAuthority

LDAP Services for NDS extends the NDS schema to allow User objects to have an auxiliary class of strongAuthenticationUser and Organization or Organizational Unit objects to have an auxiliary class of certificationAuthority. To emulate auxiliary class support for other NDS object classes, use the NDS Manager™ utility to extend the schema for the NDS object class with the appropriate LDAP class. For example, an optional attribute called LDAP UserCertificate could be added with NDS Manager to a group object that would map to the LDAP User Certificate. Future versions of NDS will more fully support auxiliary classes.

The strongAuthenticationUser and certificationAuthority auxiliary classes provide security features. They can be used to support a Public Key Infrastructure to maintain and store the digital keys necessary for secure applications such as secure e-mail and electronic commerce. For example, the strongAuthenticationUser class contains a User Certificate attribute. This attribute holds the user's public key. This public key can be accessed and used to encrypt data and initiate a secure session with the user.

NOTE: Although the mappings for these object classes don't appear in the NetWare Administrator LDAP Group object Class Map page, you cannot remap these object classes.

Understanding LDAP vs. NDS Syntax

LDAP and NDS use different syntaxes. Some important differences are:

- Commas
- Typeful names only
- Escape character
- Multiple naming attributes

Commas

LDAP uses commas as delimiters rather than periods. For example, a distinguished, or complete, name in NDS looks like this: CN=JANEB.OU=MKTG.O=EMA. Using LDAP syntax, the same distinguished name would be CN=JANEB,OU=MKTG,O=EMA.

Some additional examples of LDAP distinguished names include:

CN=Bill Williams,OU=PR,O=Bella Notte Corp

CN=Susan Jones,OU=Humanities,O=University College London,C=GB

Typeful Names Only

NDS uses both typeless (.JOHN.MARKETING.ABCCORP) and typeful (CN=JOHN.OU=MARKETING.O=ABCCORP) names. LDAP uses only typeful names with commas as the delimiters (CN=JOHN,OU=MARKETING,O=ABCCORP).

Escape Character

The backslash (\) is used in LDAP distinguished names as an escape character. If you use the plus (+) character or the comma (,) character, you can escape them with a single backslash character. Some examples include

CN=Pralines\+Cream,OU=Flavors,O=MFG (CN is Pralines+Cream)

CN=D. Cardinal,O=Lionel\,Turner and Kaye,C=US (O is Lionel, Turner and Kaye)

Multiple Naming Attributes

Objects can be defined with multiple naming attributes in the schema. In both LDAP and NDS, the user object has two: CN and OU. The plus symbol (+) separates the naming attributes in the distinguished name. If the attributes are not explicitly labeled, the schema determines which string goes with which attribute (the first would be CN, the second is OU for NDS and LDAP). You may reorder them in a distinguished name if you manually label each portion.

For example, here are two relative distinguished names:

Sammy (CN is Sammy)

Sammy+Lisa (CN is Sammy, the OU is Lisa)

Both relative distinguished names (Sammy and Sammy+Lisa) can exist in the same context because they must be referenced by two completely different relative distinguished names.

2 Setting Up

This sections gives instructions on how to set up and configure LDAP Services for NDS™ 3.0.

Installing LDAP Services for NDS

LDAP Services for NDS is installed using the NetWare® 5 installation program. Refer to the NetWare 5 installation instructions for futher information.

The LDAP Services for NDS NetWare Loadable Module™ (nldap.nlm) can also be loaded and unloaded at the NetWare server console.

If you uninstall LDAP Services for NDS with the intention of reinstalling it again later, you should wait a significant period of time before attempting the reinstall. Since the schema needs to resychronize across the tree, the time period you wait should be commenserate with the size of the NDS tree.

Configuring the LDAP Server Object

The LDAP Server object stores configuration data for one LDAP Services for NDS server. During installation, an LDAP Server object named LDAP Server *servername* (where *servername* is the name of the server on which LDAP Services for NDS is installed) is created. The object is created in the same container as the NetWare Server object on which the product is installed.

NOTE: Each LDAP Server object configures one LDAP Services for NDS server. Do not assign the same LDAP Server object to more than one LDAP Services for NDS server. If you assign the LDAP Server object to another server, it is no longer assigned to the previous server.

The LDAP Server object contains five property pages from which you set configuration options:

- General Page
- Log File Options Page
- Screen Log Options
- Catalog Usage Page
- Catalog Schedule Page

Configure and LDAP Server Object

1. Launch NetWare Administrator (nwadmn32.exe).
2. Select the object.
3. Configure the property pages.
4. Click OK.

Configuring the LDAP Group Object

The LDAP Group object stores configuration data that can be applied to a single LDAP server or a group of LDAP servers. If you plan to implement the same configuration on multiple servers, the best way is to configure one LDAP Group object and assign it to each of the LDAP Services for NDS servers from the LDAP Server General Page.

The LDAP Group configures the class and attribute mappings and security policies on the server. This greatly simplifies configuration changes, because one configuration change can be applied instantly to multiple LDAP servers.

During installation, an LDAP Group object named LDAP Group is created in the same container as the NetWare Server on which object the product is installed.

Property Pages

The LDAP Group object has five property pages in NetWare Administrator from which you set configuration options:

- General Page
- Server List Page
- Access Control Page

- Attribute Map Page
- Class Map Page

Configure an LDAP Group Object

1. Launch NetWare Administrator (nwadmn32.exe).
2. Select the object.
3. Configure the property pages.
4. Click OK.

Configuring the User Object

LDAP Services for NDS extends the User object to include a new E-mail Address page where you can specify an Internet e-mail address for the user.

The Internet e-mail address is not required for LDAP server operation. If an address is specified, that address will be delivered to the LDAP client when a user's e-mail address is requested.

LDAP Services for NDS uses the following property page:

- E-mail Address Page

Configure the User Object

1. Launch NetWare Administrator (nwadmn32.exe).
2. Select the User object in NetWare Administrator.
3. Select the E-mail Address page for the User object.
4. Add, modify, or remove the address.

Assigning NDS Rights for LDAP Clients

To assign NDS rights for LDAP clients:

1. Determine which type of username the LDAP clients will use to access NDS:
   - [Public] (anonymous bind)
   - Proxy user (proxy user anonymous bind)
   - NDS user (NDS user bind)

2. If users will use one Proxy user or multiple NDS usernames to access LDAP, create these usernames in NDS.
3. Assign the appropriate NDS rights to the usernames that LDAP clients will use.

The default rights that most users receive provide limited rights to the user's own object. To provide access to other objects and their attributes, you must change the rights assigned in NDS.

If the NDS rights assignment options do not provide the exact access level you want, you can implement additional controls using the optional LDAP Access Control List (ACL) feature.

When an LDAP client requests access to an NDS object and attribute, NDS accepts or rejects the request based on the LDAP client's NDS identity. The identity is set at bind time. Use the following tables to determine the NDS rights the LDAP client needs to complete the various types of LDAP client requests.

LDAP Object Access Requested	*NDS Object Rights Required*
Search	Browse
Add	Create
Delete	Delete
LDAP Attribute Access Requested	*NDS Attribute Rights Required*
Compare	Compare
Search	Compare
Read	Read
Write	Write

NOTE: NDS does not allow objects to inherit individual attribute rights from containers. One way to assign inheritable individual attribute rights is to use the LDAP Access Control List feature.

Also, those operations that require NDS Supervisor rights are currently not available through LDAP.

Setting Up Access Control Lists (ACL)

Overview

An Access Control List (ACL) is an optional feature of LDAP Services for NDS that allows you to create an additional layer of security between LDAP clients and NDS. You can use ACLs to implement LDAP client access restrictions for all LDAP servers in an LDAP Group object.

An ACL accomplishes the following:

- Creates container object attribute-level access controls that are inherited by the objects the container contains.
- Controls access based on criteria that NDS does not use (such as IP addresses).
- Implements more restrictive rights to NDS when accessed via LDAP (such as Read-only or publishing just names and e-mail addresses).

Each ACL contains the following components:

- Access To List
- Access By List

To create an ACL, use NetWare Administrator (nwadmn32.exe) to configure the LDAP Group object Access Control page.

ACL Processing Order

The order of the ACLs in the list is important. When LDAP Services for NDS receives a client request, it searches the ACL list and uses the first ACL that specifies the requested attributes in the Access To List. LDAP Services for NDS then searches Access By List and uses the first entry that includes the LDAP client user. If no ACL is found, full NDS rights are given.

For example, suppose that you specified two ACLs, one for Organizational Unit Acme and one for User object Jim within Acme. Now suppose that the ACLs appear in the following order:

o=Acme, c=us

cn=Jim, o=Acme, c=us

In this example, the ACL for Jim would never be processed because Jim is part of the Acme organization. Every request for Jim would be processed by the ACL for Acme because Jim is part of Acme. To provide separate controls for

user object Jim, you need to move this object above Organizational Unit object Acme in the ACL list.

Now consider an example of the processing order used in the Access By List. Suppose that the Access By List contains two entries, one for Jeff and one for his group, TeamT. Jeff is a member of TeamT and the entries appear in the following order with the indicated access level:

.*,ou=TeamT, o=Acme, c=us (Read access)

Jeff, ou=TeamT, o=Acme, c=us (Write access)

In this example, Jeff has Read access to the objects in the Access To List because he is recognized as part of the TeamT group. To give Jeff the intended level of access, you need to move the entry for Jeff above the entry for TeamT in the Access By List.

To change the ACL processing order, use NetWare Administrator (nwadmn32.exe) to configure the LDAP Group object Access Control page.

Setting Up an LDAP Client

LDAP clients use TCP/IP to communicate with LDAP Services for NDS. NetWare client software is not required. Novell® does not develop or release LDAP client software. However, many third-party LDAP client applications are readily available.

1. On the client workstation, install a network board, the network cabling, and TCP/IP software.
2. Install the client software.
3. Configure the server connection in the client software.
4. Bind to the server.
5. Complete an LDAP request and review the results.

Setting Up a Test Server Configuration

After installation and startup, LDAP Services for NDS is ready to process client requests for NDS information. However, your NDS tree might not be set up to support LDAP requests. For example, your LDAP clients cannot access phone numbers if the phone numbers are not in NDS. Also, LDAP clients cannot read the phone numbers if they do not have the appropriate NDS rights.

The following configuration procedure creates a test organization within the NDS tree and gives LDAP clients unlimited Read access to this organization. Use this procedure to help you learn how to use LDAP Services for NDS. As you become more familiar with the product, you can reconfigure your server to present the directory data you want to publish to selected clients.

Configure LDAP Services for NDS for Testing Client Communications

1. Install LDAP Services for NDS.
2. At the administration workstation, log in to the directory and start NetWare Administrator (nwadmn32.exe).
3. If you have a container that you can make public, select that container. Otherwise, create a test container somewhere in the tree.
4. Create several users in the test container and assign values to the following properties:
   - Last name
   - Given name
   - Middle initial
   - Title
   - Location
   - E-mail address
   - Telephone
5. In the test container, create a user named LDAP_Proxy.

   This user will be given permission to read all the data in the test container.
6. Select the Password Restrictions page for the LDAP proxy user and clear the check box for Allow User to Change Password. Do not assign a password to this user.
7. Make the LDAP proxy user a trustee of the test container with the NDS Browse object right and Read and Compare rights to all properties.

   NOTE: If you allow NDS user binds, these users will typically not have sufficient rights to read and compare most attributes, even though all attributes and classes in the container that are mapped are readable by LDAP.

8. Open the LDAP Group object and configure the following:

   8a. Click the browse button for the Proxy Username text box, and select the LDAP proxy user you created. This maps all anonymous LDAP requests to the proxy username for NDS authentication.

   8b. Click the browse button for the Suffix text box, and select the test container. This limits access by the LDAP proxy user to the test container. Note the complete name of this container. LDAP clients need this name to configure their connections.

   8c. Select the Server List page and verify that your LDAP Services for NDS server appears in the list. If it isn't there, click Add and use the browse button to locate the LDAP Server object.

9. Click OK. LDAP Services for NDS will automatically load in the new configuration.

10. To prepare for client configuration, record the following information:

    - Server IP address or DNS name:
    - Test container distinguished name:

      NOTE: The LDAP distinguished name has no preceding period and uses commas to separate the components. For example, the NDS distinguished name ou=test.c=usa must be entered at an LDAP client as follows: ou=test, c=usa.

Using LDAP in a Wide Area Network Environment

In order to reduce network traffic when using a wide area network (WAN), you can specify exact times when you want to refresh LDAP objects in NDS.

Type one of the following at the NetWare 5 server console:

- LDAP REFRESH = 'date' 'time' 'interval'

  This command refreshes the LDAP objects at a specified date and time. Use the following syntax:

  Date format: mm:dd:yyyy (If zeros are entered for all date fields, then the current date will be used.)

  Time format: hh:mm:ss (If zeros are entered for all time fields, then the current time will be used.)

  Interval format: minutes greater than or equal to 1. Default is 30 seconds. If zero is entered, 30 seconds is used.

- LDAP REFRESH IMMEDIATE

  This command refreshes the LDAP objects immediately. If you have already set the LDAP REFRESH command, the set interval will be saved.

- LDAP REFRESH

  This command displays the time and interval of the next scheduled refresh.

- LDAP HELP

  This command displays help information at the server console.

3 Troubleshooting

This section gives troubleshooting information for LDAP Services for NDS™ 3.0.

Determining Why LDAP Clients Cannot Bind to LDAP Services for NDS

If an LDAP client cannot bind to LDAP Services for NDS, check the following:

- Is the user entering the correct username and password?
- Is the user entering an LDAP form of the name?
- Has the Allow Cleartext Passwords option been set?
- Has the password expired?
- Has the server been reconfigured?

Determining Why the Server Isn't Using a New Configuration

Processing LDAP Server configuration updates can be affected by currently bound LDAP clients.

Configuration changes are updated dynamically. The LDAP server checks for configuration changes periodically (every two minutes). When a change is detected, new clients cannot bind to the LDAP server during the reconfiguration process.

The LDAP server stops processing new LDAP requests for any clients currently bound and waits for any active LDAP requests to complete before updating the configuration.

Determining Why Question Marks Appear in NetWare Administrator

If the LDAP Services for NDS objects appear as question marks in NetWare® Administrator, one of the following has happened:

- Your copy of NetWare Administrator has not been extended to understand LDAP Services for NDS objects. Use nwadmn32.exe on a NetWare 5 server.
- Your copy of NetWare Administrator cannot be extended to support LDAP Services for NDS.

A Novell Trademarks

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

Advanced NetWare is a trademark of Novell, Inc.

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

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppNotes is a registered service mark of Novell, Inc. in the United States and other countries.

AppTester is a registered service mark of Novell, Inc. in the United States and other countries.

BrainShare is a registered service mark of Novell, Inc. in the United States and other countries.

C-Worthy is a trademark of Novell, Inc.

C3PO is a trademark of Novell, Inc.

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

Certified NetWare Administrator in Japanese and CNA-J are service marks of Novell, Inc.

Certified NetWare Engineer in Japanese and CNE-J are service marks of Novell, Inc.

Certified NetWare Instructor in Japanese and CNI-J are service marks of Novell, Inc.

Certified Novell Administrator and CNA are service marks of Novell, Inc.

Certified Novell Engineer is a trademark and CNE is a registered service mark of Novell, Inc. in the United States and other countries.

Certified Novell Salesperson is a trademark of Novell, Inc.

Client 32 is a trademark of Novell, Inc.

LAN WorkGroup is a trademark of Novell, Inc.

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

LAN WorkShop is a trademark of Novell, Inc.

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

LANalyzer Agent is a trademark of Novell, Inc.

Link Support Layer and LSL are trademarks of Novell, Inc.

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

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

Media Support Module and MSM are trademarks of Novell, Inc.

Mirrored Server Link and MSL are trademarks of Novell, Inc.

Mobile IPX is a trademark of Novell, Inc.

Multiple Link Interface and MLI are trademarks of Novell, Inc.

Multiple Link Interface Driver and MLID are trademarks of Novell, Inc.

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

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

Natural Language Interface for Help is a trademark of Novell, Inc.

NDS Manager is a trademark of Novell, Inc.

NE/2 is a trademark of Novell, Inc.

NE/2-32 is a trademark of Novell, Inc.

NE/2T is a trademark of Novell, Inc.

NE1000 is a trademark of Novell, Inc.

NE1500T is a trademark of Novell, Inc.

NE2000 is a trademark of Novell, Inc.

NE2000T is a trademark of Novell, Inc.

NE2100 is a trademark of Novell, Inc.

NE3200 is a trademark of Novell, Inc.

NE32HUB is a trademark of Novell, Inc.

NEST Autoroute is a trademark of Novell, Inc.

NetExplorer is a trademark of Novell, Inc.

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

NetSync is a trademark of Novell, Inc.

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

NetWare 3270 CUT Workstation is a trademark of Novell, Inc.

NetWare 3270 LAN Workstation is a trademark of Novell, Inc.

NetWare 386 is a trademark of Novell, Inc.

NetWare Access Server is a trademark of Novell, Inc.

NetWare Access Services is a trademark of Novell, Inc.

NetWare Application Manager is a trademark of Novell, Inc.

NetWare Application Notes is a trademark of Novell, Inc.

NetWare Asynchronous Communication Services and NACS are trademarks of Novell, Inc.

NetWare Asynchronous Services Interface and NASI are trademarks of Novell, Inc.

NetWare Aware is a trademark of Novell, Inc.

NetWare Basic MHS is a trademark of Novell, Inc.

NetWare BranchLink Router is a trademark of Novell, Inc.

NetWare Care is a trademark of Novell, Inc.

NetWare Communication Services Manager is a trademark of Novell, Inc.

NetWare Connect is a registered trademark of Novell, Inc. in the United States.

NetWare Core Protocol and NCP are trademarks of Novell, Inc.

NetWare Distributed Management Services is a trademark of Novell, Inc.

NetWare Document Management Services is a trademark of Novell, Inc.

NetWare DOS Requester and NDR are trademarks of Novell, Inc.

NetWare Enterprise Router is a trademark of Novell, Inc.

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

NetWare Global Messaging and NGM are trademarks of Novell, Inc.

NetWare Global MHS is a trademark of Novell, Inc.

NetWare HostPrint is a registered trademark of Novell, Inc. in the United States.

NetWare IPX Router is a trademark of Novell, Inc.

NetWare LANalyzer Agent is a trademark of Novell, Inc.

NetWare Link Services Protocol and NLSP are trademarks of Novell, Inc.

NetWare Link/ATM is a trademark of Novell, Inc.

NetWare Link/Frame Relay is a trademark of Novell, Inc.

NetWare Link/PPP is a trademark of Novell, Inc.

NetWare Link/X.25 is a trademark of Novell, Inc.

NetWare Loadable Module and NLM are trademarks of Novell, Inc.

NetWare LU6.2 is trademark of Novell, Inc.

NetWare Management Agent is a trademark of Novell, Inc.

NetWare Management System and NMS are trademarks of Novell, Inc.

NetWare Message Handling Service and NetWare MHS are trademarks of Novell, Inc.

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

NetWare Mirrored Server Link and NMSL are trademarks of Novell, Inc.

NetWare Mobile is a trademark of Novell, Inc.

NetWare Mobile IPX is a trademark of Novell, Inc.

NetWare MultiProtocol Router and NetWare MPR are trademarks of Novell, Inc.

NetWare MultiProtocol Router Plus is a trademark of Novell, Inc.

NetWare Name Service is trademark of Novell, Inc.

NetWare Navigator is a trademark of Novell, Inc.

NetWare Peripheral Architecture is a trademark of Novell, Inc.

NetWare Print Server is a trademark of Novell, Inc.

NetWare Ready is a trademark of Novell, Inc.

NetWare Requester is a trademark of Novell, Inc.

NetWare Runtime is a trademark of Novell, Inc.

NetWare RX-Net is a trademark of Novell, Inc.

NetWare SFT is a trademark of Novell, Inc.

NetWare SFT III is a trademark of Novell, Inc.

NetWare SNA Gateway is a trademark of Novell, Inc.

NetWare SNA Links is a trademark of Novell, Inc.

NetWare SQL is a trademark of Novell, Inc.

NetWare Storage Management Services and NetWare SMS are trademarks of Novell, Inc.

NetWare Telephony Services is a trademark of Novell, Inc.

NetWare Tools is a trademark of Novell, Inc.

NetWare UAM is a trademark of Novell, Inc.

NetWare WAN Links is a trademark of Novell, Inc.

NetWare/IP is a trademark of Novell, Inc.

Novell Gold Partner is a service mark of Novell, Inc.

Novell Labs is a trademark of Novell, Inc.

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

Novell NE/2 is a trademark of Novell, Inc.

Novell NE/2-32 is a trademark of Novell, Inc.

Novell NE3200 is a trademark of Novell, Inc.

Novell Network Registry is a service mark of Novell, Inc.

Novell Platinum Partner is a service mark of Novell, Inc.

Novell Press is a trademark of Novell, Inc.

Novell Press Logo (teeth logo) is a registered trademark of Novell, Inc. in the United States and other countries.

Novell Replication Services is a trademark of Novell, Inc.

Novell Research Reports is a trademark of Novell, Inc.

Novell RX-Net/2 is a trademark of Novell, Inc.

Novell Service Partner is a trademark of Novell, Inc.

Novell Storage Services is a trademark of Novell, Inc.

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

Novell Technical Services and NTS are service marks of Novell, Inc.

Novell Technology Institute and NTI are registered service marks of Novell, Inc. in the United States and other countries.

Novell Virtual Terminal and NVT are trademarks of Novell, Inc.

Novell Web Server is a trademark of Novell, Inc.

Novell World Wide is a trademark of Novell, Inc.

NSE Online is a service mark of Novell, Inc.

NTR2000 is a trademark of Novell, Inc.

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

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

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

Open Data-Link Interface and ODI are trademarks of Novell, Inc.

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

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

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

Storage Management Services and SMS are trademarks of Novell, Inc.

Technical Support Alliance and TSA are collective marks of Novell, Inc.

The Fastest Way to Find the Right Word is a registered trademark of Novell, Inc. in the United States and other countries.

The Novell Network Symbol is a trademark of Novell, Inc.

Topology Specific Module and TSM are trademarks of Novell, Inc.

Transaction Tracking System and TTS are trademarks of Novell, Inc.

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

Virtual Loadable Module and VLM are trademarks of Novell, Inc.

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

Yes, It Runs with NetWare (logo) is a trademark of Novell, Inc.

Yes, NetWare Tested and Approved (logo) is a trademark of Novell, Inc.

ZENworks is a trademark of Novell, Inc.