hp industry standard servers

february 2003

integration note TC030201IN

tips and tricks for Novell eDirectory

table of contents

abstract

This integration note provides useful tips and tricks to help network administrators, developers, and users plan, design, manage, and optimize Novell eDirectory. Throughout this integration note, tips and tricks are offered in the following areas:

- Novell eDirectory evolution and understanding LDAP
- tips when migrating from NetWare 5.x to NetWare 6.x
- planning, designing, and replicating your eDirectory
- extending your eDirectory schema
- tuning your eDirectory and improving your eDirectory operations
- managing your eDirectory with cross platform tools
- weekly health checklist
- improving your eDirectory operations
- hp manageability and integration with Asset Manager
- metadirectory and other net services solutions such as iFolder and iPrint

Throughout this document, we have gathered several tips from HP engineers, Novell engineers, Novell AppNotes, and Novell Developer Notes.

symbols in text

The following symbols can be found in the text of this document:

CAUTION: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or loss of information.

IMPORTANT: Text set off in this manner presents clarifying information or specific instructions.

Text set off in this manner contains tips that make it easier to perform a certain task.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

introduction

Novell eDirectory is the access point for identity management and organizes, categorizes, and names all resources within a network. It is a highly scalable, high performing, secure directory service that stores and manages millions of objects, such as users, applications, network devices, and data. eDirectory natively supports the directory standard Lightweight Directory Access Protocol (LDAP) version 3 over Secure Socket Layer (SSL).

The bottom line: eDirectory is a full-service directory that simplifies, automates, and protects information while taking full advantage of emerging information and Internet technologies.

Novell eDirectory 8.7 is the newest release of directory services, and includes functional enhancements, extended schema, and new features not previously available. These include web-based utilities, fully RFC-compliant LDAP support, and advanced directory synchronization. Novell eDirectory can co-exist with NDS or eDirectory versions and can be installed in the following heterogeneous and multi-platform networks.

- Novell eDirectory 8.7.x on Windows NT, Windows 2000, NetWare, Solaris, or AIX
- Novell eDirectory 8.6.x on Windows NT, Windows 2000, NetWare, Solaris, or Linux
- NDS eDirectory 8.5.x on Windows NT, Windows 2000, NetWare, Solaris, Linux, or Tru64 UNIX
- NetWare 5.1with Support Pack 1 or later
- NetWare 5 with Support Pack 5 or later, and NDS 8.51 or later
- NetWare 5 with Support Pack 5 or later, and NDS 7.47 or later (but earlier than NDS 8)

To find our more about the latest Novell version of eDirectory, visit www.novell.com/products/edirectory/.

Novell eDirectory evolution

eDirectory is the latest evolution of NDS. Based on version 8, eDirectory is a full service directory that provides for flexible and extensible discovery, rich security tools, an extremely scalable storage engine, and the ability to manage relationships whether internal or external to your organization. eDirectory, the new name for Novell Directory Services, is simply NDS Version 8 on Solaris, Windows NT/2000, Novell NetWare, and Linux.

For the first time, eDirectory is not only cross-platform, but also OS independent, meaning there is no NetWare dependency in the code. For example, you can run a complete Solaris or a complete Windows shop on eDirectory. eDirectory 8.7 allows any LDAP-enabled web browser or application to access information stored in the NDS database. In addition to performance enhancements, it includes an additional container object, called domain, and allows complete auxiliary class support.

Previously, eDirectory version 7.47 supported three auxiliary classes and extended NDS into the Internet and enterprise directory niches with no loss of functionality. eDirectory version 8 was available only for NetWare 5.x servers with Support Pack 1 already installed.

The eDirectory database sometimes is referred to as a DIB Set. DIB is an acronym for Directory Information Base. To determine the size of your DIB Set, do the following:

- On NetWare, download TOOLBOX.NLM from Novell's website. This will allow you to see the SYS: _NETWARE directory on your server.
- On Windows, you can find the DIB Set at \NOVELL\NDS\DIBFiles.
- On Sun Solaris, the DIB Set location may vary depending on the path you specified during the installation.

understanding LDAP

Lightweight Directory Access Protocol (LDAP) has rapidly become a standard, and it is important for anyone developing a directory or directory-based application to provide support for LDAP. To centralize the information of an enterprise, the directory must span the multiple network environments that make up the enterprise, including NetWare, Tru64 UNIX, Windows NT/2000, Linux, and other UNIX flavors.

LDAP client software has become a standard feature of Internet browsers and the standard protocol for accessing directory information. LDAP Services for eDirectory allows for easy publication of your organizations data while still maintaining control of who can access your information.

- LDAP, which is controlled by the Internet Engineering Task Force (IETF), actually started out as a means to simplify access to X.500 compliant directories. For the most current information on LDAP v3 RFC, visit the following IETF websites at www.ietf.org and www.ietf.org/rfc/rfc2251.txt?number=2251.

  There are many tools and utilities available for accessing directory information, three of the most common are:

  - **LDAP search** is probably the most common use of LDAP. An `ldapsearch` searches entries in an LDAP directory server.
    - Netscape Communicator supports searching LDAP directories using LDAP URLs. The URL form of LDAP searches is defined in RFC 2255 available at www.ietf.org under "RFC Pages".
    - In the address window of the browser, type `ldap://[text]` to initiate a directory services search. In general, the form is:
      ```
      ldap://serverdns.domain.name[:port]/cn=ldap,ou=distinguished,o=names[?[attributes][?[scope][?[filter]]]]
      ```
    - For example, you can search for the distinguished names (dn attribute) of all users in an eDirectory tree using: *ldap://172.25.69.248/o=hpq?dn?sub?(objectClass=User)* There is no way to specify a name and password in this format; all searches will be performed using an anonymous bind.
  - **LDAP modify** (`ldapmodify`) opens a connection to an LDAP server, binds, and modifies or adds entries.

- **LDAP delete** (`ldapdelete`) deletes entries from an LDAP directory server. The ldapdelete tool opens a connection to an LDAP server, binds, and deletes one or more entries.

- If an LDAP client cannot bind to LDAP Services for eDirectory, check the following:
  - Is the user entering the correct username and password?
  - Is the user entering an LDAP form of the name?
  - Has the password expired and has the server been reconfigured?

eDirectory version 8 allowed the schema to be extended through LDAP. Beginning with version 8, LDAP support automatically installed when you installed the directory services. You will not see any LDAP-related screens, once the eDirectory Install is finished, you can browse your tree and find the new LDAP Server and Group objects created by the install. The LDAP Install also creates a SAS Server object and a Security container object. If you want secure connections through LDAP clients, you must configure Novell Security Services.

- LDAP support can be disabled and restarted on any server by unloading and reloading NLDAP.NLM on that server.
- If, after installing eDirectory, you have problems performing common LDAP tasks—like class and attribute mappings— it may be because you do not have the LDAP snap-in for ConsoleOne installed. You can install a version of ConsoleOne that already has the LDAP snap-in by running SETUP.EXE that is located in the Sys:public\mgmt\ConsoleOne\1.2\ install directory on your NetWare server.
- LDAP services are highly configurable and allow for changing ports and clear text passwords. If you do not allow clear text passwords, LDAP functionality will be equivalent to an anonymous user.
- eDirectory already has default Class and Attribute Mapping list that converts most of the LDAP class, attribute names to NDS class, and attribute names. Occasionally, you might find an LDAP attribute or class name that is not mapped or is mapped to the wrong NDS attribute or class name. This will cause you some problems. In this situation, you first have to figure out which NDS class or attribute name corresponds with the LDAP class or attribute name and manually reconfigure the mapping for each class or attribute.
- For additional information and helpful tips, visit www.ldapzone.com/ and www.openldap.org/.
- If you need information on eDirectory or configuring the LDAP Server and Group objects, go to the Novell website at www.novell.com/products/nds/ldap.html.

hp LDAP Directory Synchronizer (LDSU)

HP LDAP Directory Synchronizer can synchronize an LDAP directory with virtually any other data source, provide continuous bi-directional synchronization between data sources checks for duplicates, eliminates the need for additional hardware, and deduces development, testing, and maintenance costs.

HP LDAP Directory Synchronizer (LDSU) provides directory data exchange between LDAP-supported directories and virtually any other directory or database. LDSU runs on NetWare eDirectory, Windows 2000/XP/NT, HP-UX, UNIX, OpenVMS, Linux, and Sun Solaris.

To find out more about LDSU or to download LDSU tool, visit http://h18005.www1.hp.com/services/messaging/mg_ldap.html.

tips when migrating from NetWare 5.x to NetWare 6.x and eDirectory

Appropriate planning is required if you are migrating or updating to Novell eDirectory. With eDirectory, you can now manage a billion objects within one tree and you might want to evaluate a server upgrade. To optimize Novell NetWare and eDirectory, evaluate the ProLiant DL and ML series of servers.

Here are some migration tips:

- Verify the following:
  - ability of your backup software to backup and restore eDirectory
  - your bandwidth (increased bandwidth may be necessary for NetWare 6.x)
  - your memory is sufficient
  - eDirectory version is supported
  - time synchronization configuration does not create overhead.

  Note: For more information on backup software, visit Veritas (www.veritas.com/) and Computer Associates (www.computerassociates.com/).
- Verify the ability of the software vendor to sucessfully backup an eDirectory database.
- For recovering from a failed migration, identify if destination server has new name. If it does not, the backup is stored in SYS:\SYSTEM\NUW30\NDSBU. This directory resides on both servers.
- Restore directory services on the source server by doing a NWCONFIG | Directory Options | Restore local NDS information after hardware upgrade. If the destination server does have a new name, take the destination server off of the wire, and remove directory services (`nwconfig -dsremove`).

For the tips below, copy the appropriate DSREPAIR.NLM file to the SYS:\SYSTEM directory of the server that contains the master replica of the Tree partition. Check the latest Novell Support Connection Minimum Patch List on the Novell website: http://support.novell.com/misc/patlst.htm.

- When introducing a NetWare 6.x server into a NetWare 5.x. environment, be sure the network is running eDirectory before proceeding with a migration.
- If you are running a NetWare 4.x server in a mixed environment (with a 6.x cluster), be sure to remove replicas before proceeding with the migration.
- If you are upgrading from NetWare 5.0 or later running NDS 7.47 or later, use PATCHES\DSREPAIR\NW5X\DSREPAIR.NLM.[1]
- If you are upgrading from NetWare 5.0 or later running NDS 8.51 or later, use PATCHES\DSREPAIR\NWNDS8\DSREPAIR. NLM.[1]
- If you are upgrading eDirectory 8.6 on a NetWare 5.1 server, the NetWare 5.1 server must be running NetWare 5.1 SP2a or later.[1]
- Download the latest Support Packs from the website: http://support.novell.com.

Note: NetWare 5.0 or later running NDS 8.11 or 8.17 is not supported.

planning and designing your eDirectory tree

All networks need a solid eDirectory tree design to ensure easy access to the services and applications relying on the directory. The eDirectory tree structure also affects network security and ease of management.

So, keep a few things in mind:

- Keep the design as simple as possible. Novell recommends that you use no more than five levels because flat trees are stable and easier to troubleshoot. A good design provides eDirectory fault tolerance while reducing synchronization traffic, especially across a WAN. (If this traffic crosses WAN links unmanaged, it needlessly increases costs and overloads slow WAN links during high-usage periods.)
- To minimize traffic between remote sites, keep network services, such as eDirectory authentication, file, and print services, local to the remote user if possible.
- In general, do not include dial-up sites in a corporate tree. Create a separate tree for dail-up each site.
- Standardize naming conventions for all objects and enforce the conventions.
- Remember that the first eDirectory server installed on the network holds the master replica by default.

[1] Instructions on the necessary software patches to upgrade to NetWare 6 taken from www.novell.com/documentation/lg/ndsedir86/index.html?page=/documentation/lg/ndsedir86/taoenu/data/a2qqoef.html.

- To communicate properly within a mixed-protocol environment running the Migration Agent, the agent must be loaded on the server with the eDirectory master replica. Otherwise, an IPX server will not be able to connect.
- Do you think you will ever move your servers to another floor or another building? Steer away from tying server names to a specific department. Doing this will eliminate the need to continually rename your servers.
- Login name length should be considered when standardizing the location of users within the tree.

eDirectory Design Rules

Table 1 summarizes additional eDirectory design guidelines for partitions and replicas.

table 1. eDirectory design rules

eDirectory design rules						
eDirectory version	tree size	partition size	subordinate partitions	replicas per partition	non-dedicated server	dedicated server
8.5.x and above	Unlimited (tested to 1 billion objects)	Unlimited (tested to 100 million objects)	Unlimited (tested to 75 partitions)	Unlimited (always have 2 or 3)	50 replicas	150-200 replicas

Below are a few tips from an HP engineer. The tips below may not be applicable for all operating systems on all hardware.

- Create a group for anything that two or more people share in common. Assign the Group the rights that it needs and assign users to those rights.
- Create another emergency Admin account just in case the Admin account is corrupted. Protect the password and audit the account for usage.
- Always be sure to obtain a realiable back-up. Backup your eDirectory by using NWCONFIG.NLM, particularly after doing any large eDirectory changes
- If you have a medium-to-large network and you want to be sure that your master replica is protected, you may want to establish a dedicated eDirectory server. The probability of the server crashing is minimal. Since the master replica is not busy with file serving processes, running databases, or performing web functions, your eDirectory activities will run faster.
- In addition, remember this server must have an eDirectoryTree Name and be the first server installed on the network.

tuning your eDirectory

Tuning your eDirectory is extremely important. Even with the best hardware, unless it is properly tuned, it will not perform to its full potential.

The following settings optimize eDirectory for a variety of uses:

table 2. eDirectory ideal optimization settings for Novell NetWare

ideal optimization settings	
Maximum 4096 Pending TCP Connection Requests	Dirty Directory Cache Delay Time 0
Maximum Number of Internal Directory handles 1000	Enable file compression Off
Maximum Packet Receive Buffers 10000	Immediate purge of deleted files On
Maximum Number of Directory Handles 100	Minimum Packet Receive Buffers 3000
Maximum Record Locks Per Connection 10000	Maximum Number of Directory Handles 100
Maximum Physical Receive Packet Size 2048	Maximum Number of Internal Directory handles 1000
Maximum Record Locks 100000	Maximum Record Locks Per Connection 10000
Maximum Concurrent Disk Cache Writes 2000	Maximum Outstanding NCP Searches 500
Maximum Concurrent Directory Cache Writes 500	Maximum Number of Directory Handles 100
Maximum Directory Cache Buffers 2 GB	

- The biggest setting to affect eDirectory performance is the amount of cache. Up to 50% of available memory can be used for cache. eDirectory operates with a hard limit of 16 MB and 24 MB should be left for the OS. The smallest tested cache size is 0 and the largest is 2 GB.
- Administrators can configure the amount of RAM that will be used as cache. You should try to get as close to a 1:1 ratio of cache to DIB Set as possible. For the best performance, exceed this ratio.

Note: Avoid setting the cache memory size above 40% of the total memory if the server is hosting services or applications other than eDirectory.

To set the cache level, perform the operations detailed in Table 3.

table 3. setting cache levels

platform	location	steps
NetWare	Console screen	Set DSTRACE=!MB<Amount of RAM to use MB>
Windows NT/2000	_NDSDB.INI	Create the _NDSDB.INI file in the \NOVELL\NDS directory Enter the command CACHE=<Amount of RAM to use in MB>
UNIX/Linux	ndstrace screen	Launch ndstrace from the Sun Solaris server or Linux server Enter Set DSTRACE=!MB<Amount of RAM to use in MB>

replicating your eDirectory

A replica is a copy or an instance of a user-defined partition distributed to an eDirectory server. Each server can store more than 65,000 eDirectory replicas; however, only one replica of the same user-defined partition can exist on the same server.

Replication simply means that your network has more than one copy of the Directory, and eDirectory automatically keeps all the copies up-to-date or synchronized. Keeping multiple copies of the directory lets users continue to log into the network and use the remaining resources if servers or network links fail.

- NDS communication uses timestamps to uniquely identify objects and the objects modification time for synchronization purposes. If servers in the tree are not synchronized to the correct local time (or more importantly, to each other) replica synchronization will not be reliable and severe object corruption and data loss can be experienced. To avoid these problems, time must be in sync across all servers in the network.
- Do not copy individual eDirectory files from one server to another. If your network has more than one NDS server, replicate the eDirectory directory.

  IMPORTANT: eDirectory replication is not a file server back-up solution. The replication and synchronization process only replicates information about eDirectory objects, not files and documents.

- If an attribute is missing on all replicas, add the missing attribute using LDAP, ConsoleOne, or iManager (the object will remain unknown) If the object is consistent on some replicas but not others use iMonitor to resend that one object from the consistent replica to the other replicas. As a last resort, remove the object, then recreate it.

  Note: External References are only viewable in iMonitor or DSBrowse.

extending your eDirectory schema

The schema of your Novell eDirectory tree defines the classes of objects that the tree can contain, such as users, groups, and printers and their properties. You can extend the schema of a tree by using ConsoleOne to create a new class or attribute. Schema Manager is an integrated snap-in to ConsoleOne.

Use the Schema Manager to view and customize all aspects of the schema. You can find Schema Manager on the Object menu in eDirectory Manager (NDSMGR32.EXE). Once you are in Schema Manager, a handy wizard will take you through the process step-by-step. The wizard even includes a Help function to answer any questions you have during the process. The "Update Schema" option in the Migration Wizard adds schema updates needed for NetWare 6.

- Start the eDirectory trace screen, type the following at the console prompt: `SET DSTRACE=ON`. The server will respond with the following: DSTrace is set to: `ON`. Use DS Trace for force a schema sync (*S or*SS command) to make sure that all servers are receiving schema updates.
- When creating schema attributes that will access information, consider clients. eDirectory supports a much wider range of names than those supported by other protocols. Typically, you will want to use meaningful names, shorter than 30 characters, comprised of mostly lowercase characters with word boundary uppercase and as few numbers as possible.
- Avoid colliding with existing schema by standardizing a short prefix for all of your attributes and classes which is unique to your organization. If you intend to make your schema available publicly, you should register the prefix with Novell.
- Read and understand the guidelines on schema creation and plan your schema carefully, it can be very time consuming to make changes after the schema is in use.
- Avoid making classes with mandatory attributes whenever possible. These extra mandatory attributes will impose an additional administration overhead on all objects containing them.
- Auxiliary classes can provide useful functionality, but it is important to remember that eDirectory does not restrict their placement. Before creating auxiliary classes that are specific to a particular class, like users, consider how a client should react to that class when it is found on a different class of object.

cross-platform tools to manage your eDirectory

Understanding the practical aspects of your eDirectory tree is vital to successful and proactive directory management. You probably know in order to reduce unnecessary traffic overhead, enhance eDirectory performance, and reduce costs, you need network traffic baseline documentation that will help you understand what objects and processes are generating the traffic.

ConsoleOne

NetWare ConsoleOne is a java-based single point administration tool and provides you with tools to manage eDirectory objects, schema, partitions, replicas and additional NetWare server resources. This tool is compatible with Windows, NetWare, Linux, Solaris, and Tru64 UNIX.

Note: The legacy NetWare Administrator, NDS Manager, and Schema Manager tools run only on Windows systems. ConsoleOne encompasses all functionality of the legacy tools.

- ConsoleOne allows snap-ins from other products to be utilized. Snapins should be installed in the "snapins" subdirectory of ConsoleOne's installation directory. On a Windows OS, the installation directory defaults to "c:\novell\consoleone\1.2\".
- If you have written your own snap-ins, be sure and place them in the correct directory. They will automatically load when ConsoleOne launches.
- Snap-ins load when ConsoleOne is launched and icons appear in the bottom of the splash screen.
- To view exceptions, use the ConsoleOne/WINDEBUG screen. Exceptions for improper loading of will appear in the window.
- Be sure to obtain the latest version of ConsoleOne and note that the directory name does not match the actual version number.

iManager

Novell iManager is similar to ConsoleOne, but is the next generation solution. It is a web-based application for managing, maintaining, and monitoring eDirectory using wired and wireless devices. iManager is based on the eDirectory Management Framework (eMFrame), which is a web application you can use to easily build modular eDirectory management services called plug-ins.[2]

eMBox lets you access all of the eDirectory backend utilities remotely as well as on the server. It also includes web-based access to the new Backup and Restore and Service Manager functionalities. All functions are accessible, either on the local server or remotely, through a command line client. [2]

- For all eDirectory Management Tools (eMTools) to run, such as Backup, DSRepair, DSMerge, Schema Operations, and eDirectory Service Manager, eMBox must be loaded and running on the eDirectory server. [2]
- You can perform tasks for multiple servers from one server or workstation using the eMBox Client. [2]

iMonitor

Novell iMonitor provides cross-platform monitoring and diagnostic capability to all servers in your eDirectory tree. It provides a web-based alternative for many of Novell's traditional server-based eDirectory tools, such as DSBROWSE, DSTRACE, DSDIAG, and the diagnostic features available in DSREPAIR. This tool lets you look at the eDirectory environment in depth on a partition, replica, or server basis. You can also examine what tasks are taking place, when they are happening, what their results are, and how long they are taking.

You can link to the Agent Summary, Agent Information, Agent Configuration, Trace Configuration, DS Repair, Reports, and Search pages from any iMonitor page by using the icons in the navigator frame.

DS Designer

DS Designer is a Windows utility that allows you to see your tree in a nice, easy-to-manage window. It enables you to document your entire tree and all servers with their accompanying IPX or TCP/IP addresses, partitions, and replicas, etc. Using this tool enables you to plan ahead for future tree merges, partition merges, partition creations, replication, moves, and document changes. You can then create reports for existing trees and proposed tree designs. It is then possible to view the results accurately and precisely prior to executing the changes. This allows you to use the DSDIAG.NLM and import that info into DS Designer.

Partition operations, replication, and object manipulation are simulated exactly as they would be executed on a live network. Therefore, all design can be verified, modified, and revised perfectly before changing a live network. DS Designer is available for download from www.netwarefiles.com/.

[2] Information for the iManager heading, such as eMframe and eMbox taken from www.novell.com/documentation/lg/edir87/index.html?page=/documentation/lg/edir87/edir87/data/agabn4a.html and www.novell.com/coolsolutions/nds/features/a_87_features_edir.html.

DSMERGE utility

Use the DSMERGE at the server console to merge the roots of two separate eDirectory trees, rename a tree to verify that all servers in the eDirectory tree are responding properly and have the same tree name. DSMERGE also allows for viewing time synchronization information and displaying the timeserver for all servers in the tree.

To initiate DSMERGE, type `[LOAD][path]DSMERGE` and specify the path to DSMERGE.NLM if it was moved from the default directory of SYS:SYSTEM.

DSREPAIR utility

DSREPAIR is the Novell directory maintenance utility (DSREPAIR.NLM) and is run from the server console or via RCONSOLE. This tool performs three basic functions: corrects any inconsistencies found in the directory database, corrects any partition and replica problems, and reports replica synchronization status. Using the Unattended Full Repair Option automatically performs all possible repair operations that do not require operator assistance. To initiate the DSREPAIR utility, type `LOAD [path] DSREPAIR`. Use the switches in Table 4 to acquire information.

To review replicas, use the DSRepair utility and note that a type `0` is the master.

table 4. DSREPAIR switches

switch	description
D <DIB extension>	Repair the DIB with extension. Defaults to 'NDS' if not specified. The 'NDS' DIB is always closed and locked regardless of the DIB being repaired.
L <log file name>	Specify an alternate location/name for the log file. Default is 'sys:system\dsrepair.log'. The path can be any NetWare volume or dos drive, as in 'a:temp.lg'. Path and filename specified MUST be DOS 8.3 format.
M	Report move inhibit obituaries, this is used to discover if a move has completed or if a partition is reported as BUSY because there are move inhibit obituaries in a replica that have either not completed processing or that are broken.
N [number of days]	Specifies the number of days old that a net-address property is allowed to be on a user class object. It the net-address property is older than the number of days specified, then it is deleted. This resolves a problem where the net-address is never deleted when a connection is terminated, and results in a reduction of allowed connections to the server. The default is 60 days.
P	Mark all unknown class objects as referenced (a referenced object is not synchronized).
U	Unattended mode repair runs the main menu unattended mode operations without user intervention, and unloads when completed. The following options are only available in DSRepair 4.26c or later. They also create a status file called '<log file name>.DSM' by default that contains status information for the DSManager tool. All are short cuts to operations found in the DSRepair command menus.

switch	description
RC	Create a database dump file (sys:system\dsrepair.dib).
RD	Repair local database.
RI	Repair remote server ID's.
RL	Specify an alternate log file. Unlike the L option, the existing file is deleted first instead of appended to.
RM <partition root ID>	Set this server as the master in the replica ring of the specified replica.
RN	Repair network addresses.
RR <partition root ID>	Repair the specified partition root, check remote ID's in the ring.
RVT	Volume object repair followed by trustee check of all trustees on the volume.

DSTRACE utility

In previous versions of NetWare, DSTRACE referred to a group of SET commands available at the server console. DSTRACE commands monitors the status of NDS synchronization process and enables you to view errors that occur during NDS synchronization.

To start the eDirectory trace screen, type the following at the console prompt: `SET DSTRACE=ON`. The server will respond with the following: DSTrace is set to: `ON`.

To use switches type `SET DSTRACE = <switch>` and use the table below.

table 5. DSTRACE switches

DSTRACE switches (flags)	
B	This action instructs eDirectory to schedule the Backlinker background process to begin execution on the source server in one second.
C	This action instructs eDirectory to display the statistics information for the source server's outbound connections to other servers. These statistics do not reflect any information pertaining to the inbound connections that other servers or clients have to the source server.
CT	This action instructs eDirectory to display the source server's outbound connection table, as well as the current statistical information for the table. These statistics do not reflect any information pertaining to the inbound connections that other servers or clients have to the source server.
CI	This action instructs eDirectory to display the source server's outbound connection table, the current statistical information for that table, and the idle information for the entries in that table. These statistics do not reflect any information pertaining to the inbound connections that other servers or clients have to the source server.
CR	This action instructs eDirectory to display the source server's outbound connection table, the current statistical information for that table, and the IPX routing information being used. These statistics do not reflect any information pertaining to the inbound connections that other servers or clients have to the source server.

DSTRACE switches (flags)	
CE	This action instructs eDirectory to display the source server's outbound connection table, the current statistical information for that table, and the WAN Manager expiration information for each connection in the table. These statistics do not reflect any information pertaining to the inbound connections that other servers or clients have to the source server.
C0	This action instructs eDirectory to display the source server's outbound connection table and the current statistical information for that table, and then to reset the statistical information (after being displayed). These statistics do not reflect any information pertaining to the inbound connections that other servers or clients have to the source server.
B	This action instructs eDirectory to schedule the Backlinker background process to begin execution on the source server in one second.

An administrator's work increases with each user account to be managed. A user account is created and maintained for each platform. In enterprises with hundreds of users, the task of account management alone could be quite cumbersome.

Novell announced the availability of eDirectory for Linux and Solaris expanding its leading portfolio of Net services software products across all types of networks and all leading operating systems. It includes a Solaris and Linux package system, which is a collection of tools simplifying the installation of various eDirectory components.

Most UNIX/Linux distributions contain packages that include configuration files, utilities, libraries, daemons, and manual pages. Additionally, eDirectory for Linux enables customers to seamlessly integrate and manage their cross-platform networks.

- You can use `ndssch` utility, to extend the schema on Linux or Solaris systems. The attributes and classes that you specify in the schema file (.SCH) will be used to modify the schema of the tree.
- Use `ndstrace` to initiate limited synchronization processes or view the status of the ndstrace screen.
- Use the `ndsrepair` to correct eDirectory problems, such as bad records, schema mismatches, bad server addresses, and external references.

weekly health check

To maintain eDirectory, check operations once a week for a dynamic directory environment and once a month for a static directory environment on each server. A dynamic directory is one that has partitions added frequently while a static directory is one that rarely adds new partitions.

All versions should be at the latest on their respective operating system platforms and all servers in the tree should be patched to the latest available versions.

- You can verify all DS version that exist in your tree by using the DSREPAIR utility (this includes Unix/Linux and Windows NT/2000 environments).
- If while following the outlined Health Check Procedures you encounter DS errors or if you suspect problems with a server's DS database, the Repair Local Database option within DSREPAIR is a valuable tool to check a server's DS database. **Repair Local Database** checks the integrity of the database and fixes any problems it encounters, as well as reports information that may be useful. **Repair Local Database** does not need to be run at either a specific time or specific interval.
- Use iMonitor to help perform your health checks.

It is recommended that a health check be performed on your tree before executing a major operation, such as moving or deleting large numbers of objects, performing a partition operation, and adding or deleting servers.

Note: All versions should be the latest for their respective operating system platforms. All servers in the tree must be patched to the latest available versions.[3]

Three important areas to be checked weekly on all operating systems are:

- version
- time synchronicity
- replica synchronicity

Step 1- DS versions (DSRepair)

The DS.NLM should be the same version on every NetWare server in the tree (all DS versions 6.x, 7.x, and 8.x) and should be the latest versions available (all servers in the tree need to be patched with the latest available support packs).

Performing a time synchronization check within DSRepair (DSREPAIR.NLM | Time Synchronization) will report the DS.NLM version for each file server in the tree.[3]

NOTE: CD Towers are exceptions to this requirement.

NDS communication uses timestamps to uniquely identify objects and the objects modification time for synchronization purposes. If servers in the tree are not synchronized to the correct local time (or more importantly, to each other), replica synchronization will not be reliable and severe object corruption and data loss can be experienced. To avoid these problems, time must be coordinated across all servers in the network. [3]

[3] Steps for Weekly Heath Check taken from http://support.novell.com/cgi-bin/search/searchtid.cgi?/10060600.htm.

Step 2 - Time synchronization (DSRepair)

Time synchronization is critical for Directory Service functions. This operation can be performed from the "**Available Options**" menu of DSREPAIR.NLM. [3]

NDS servers communicate changes made to objects and partitions boundaries. This step is used to verify that no errors exist when NDS performs synchronization process. To perform this step, a server must have a replica to display the needed NDS trace information. [3]

Step 3 - Replica synchronization (DSTRACE)

A server must have a replica to display any Directory Services trace information. From the file server console prompt, type:

```
SET DSTRACE=ON (this activates the trace screen for Directory
Services transactions)

SET DSTRACE=+S (this makes it so you can see the
synchronization)

SET DSTRACE=*H (this initiates synchronization between file
servers)
```

The Directory Services trace screen can be viewed by selecting Directory Services from the list of Current Screens made available by pressing the two keys **<ctrl> <esc>** simultaneously. [3]

If no errors exist, there will be a line displaying **All processed = YES**. This message will be displayed for each partition contained on this server. [3]

If the information exceeds a single screen, use the following commands:

```
SET TTF=ON (To Trace the Synchronization to a File.
SYS\:SYSTEM\DSTRACE.DBG)

SET DSTRACE=*R (resets the file to 0 bytes)

SET TTF=OFF (once NDS has completed synchronizing
all partitions)
```

You can then map a drive to your server's SYS:SYSTEM directory and bring the DSTRACE.DBG file up in a text editor. Search for "-6" (this will show any NDS errors during synchronization, such as -625), or YES (this will show successful synchronization for a partition). [3]

improving your eDirectory operations

To improve the operations of your eDirectory there are six areas that often causing headaches if not handled properly:

- performing partition operations
- changing server names
- backing up and restoring NDS for planned hardware upgrades
- removing an NDS tree
- removing a server
- recovering from a system crash

Review the headings in the following sections to maintain good operations of eDirectory.

performing partition operations

When partitioning eDirectory, you allow parts of the database to exist on several servers enabling you to optimize network use by distributing the eDirectory data processing and storage load over multiple servers on the network. By default, a single partition is created.

When performing partition operations, remember the following:

- Partition the top of the tree based on the WAN infrastructure. Place fewer partitions at the top of the tree with more at the bottom. You can create containers for each site separated by WAN links (placing each server object in its local container), and then create a partition for each.
- Centralize the partition operation administration. Consider how a partition operation will affect the tree. Partition so that all objects in each partition are at a single location. This ensures that updates to eDirectory can occur on a local server.
- Check replica ring synchronization before performing a partition operation. Place replicas of each partition on servers that are physically close to the workgroup that uses the information in that partition.
- To create fault tolerance, plan for three replicas for each partition if the directory tree has enough servers to support that number. There should be at least two local replicas of the local partition.
- Verify the partition operation on the back end from the master replica. Do not change read/write to master under partition error conditions.

changing server names

Novell eDirectory contains information about server objects, based upon the server name and object ID. Other servers in the eDirectory tree use the server internal IPX address as an external reference. If you change the server name, object ID, or internal address, you can create problems in the eDirectory environment. You could also lose user rights. So, avoid changing the internal IPX or File Server Name.

- If you must change a server name, delete the first server name. eDirectory will take care of the details for you and replicate this information to all the other replicas in the ring. Of course, the larger your tree and the more partitions you have, the longer you will need to wait after deleting the old server name.
- Do a `[SET DSTRACE=*L]` to start the limber process, which verifies the IPX addresses and server names. If you get an *"All Processed = Yes"* response, you can (with confidence) rename the server in your autoexec.ncf file. Do not forget to rename the volumes using NWAdmin. Lastly, down the server and bring it back up.

removing an eDirectory Tree

When data becomes corrupted or damaged, it may become necessary to remove an eDirectory tree.

To remove a corrupted eDirectory tree from a server, type the command `LOAD INSTALL /DSREMOVE` to avoid authenticating to eDirectory. Then, you can remove the tree without the password (it may prompt you, but it will not verify for password).

removing a server

Never disconnect a server from a network or just pull the power plug. A server abruptly removed from the eDirectory tree can generate eDirectory and time synchronization problems.

- If the server has a replica of distributed partitions and participates in time synchronization activities, you must remove the replicas and remove the server from a replica list before you down the server.
- If the server that you are removing has the master replica, you must change the replica type and assign a new master replica. If the server is a single-reference-time server, designate one of the secondary-time servers as a temporary single-reference-time server until it is connected.

backing up and restoring eDirectory for planned hardware upgrades

Before you begin the backup and restore process, be aware of the dependencies other servers currently have on the server you are upgrading. Take into consideration processes such as eDirectory time synchronization. If the server plays a crucial part in the time synchronization of the eDirectory tree you may need to reassign the time server functions and responsibilities to another server before you run INSTALL.NLM.

See the Novell Technical Information Document (TID) 2908156 "Time Synchronization Issues and Definitions" and TID 2911661 "Changing Time Source Type" for additional information. Both documents are available at http://support.novell.com.

- For catastrophic failure/recovery, eDirectory needs to be designed so recovery can take place without using the roll forward logs (one server or a set of servers that contain replicas of the entire tree but do not share replicas). These servers can be used as master copies of the tree and the rest of the servers are restored using replication.
- Use eDirectory Manager to verify the integrity of the tree and the synchronization status of the partitions/replicas that the candidate server contains. Resolve any errors before continuing.

  IMPORTANT: Do not add or remove any replica/partition types during this time, do not uninstall or reinstall any existing servers, and do not install any new servers until the Save and Restore procedure completes.

- It is important that eDirectory partition and replica information remain consistent during the entire upgrade process. If you do not maintain consistency of the tree (including partitions, replicas, placement of replicas, and servers), the INSTALL verification process will return a 601 error (Directory field data not found) during the

Restore phase, and the process will not complete.

- Make sure you also have a current tape backup of the entire server. If the server to be upgraded contains the master replica of your eDirectory tree, you need to move the master replica to another server using DSREPAIR.NLM.
- Use INSTALL.NLM to save eDirectory information a hardware upgrade and to restore eDirectory information after an upgrade. Because other servers in the tree are expecting the server to come back online quickly, you should not plan to take several days to upgrade the server. Complete the upgrade promptly and restore eDirectory information on the server as soon as possible.
- The "Save Local DS Information before Hardware Upgrade"option prepares the eDirectory information on the server before the upgrade and creates a BACKUP.NDS file in the SYS:SYSTEM directory. BACKUP.NDS stores all the NDS information for this server, including replica information. This option also locks and disables the eDirectory database on this server, preventing certain eDirectory operations on this server from taking place. To other servers that normally communicate with this server, the server appears to be down. eDirectory information normally sent to the locked server is held by other servers in the tree. When the server comes back online, this stored information is used to synchronize the eDirectory database to the other servers in the tree.
- When backing up your eDirectory database, the default is A: for copying to a diskette. However, in most cases, the eDirectory database will not fit on a floppy. So, press **F3** to specify a different path. You might want to specify a temporary directory on the local hard drive of your workstation. If you are copying the file to another server, type the second server name and path, and authenticate to the remote server as prompted.
- The "Restore Local DS Information" after Hardware Upgrade option uses BACKUP.NDS to restore NDS information on the server. Before the eDirectory information is restored, INSTALL verifies that the server is in the same relative state as before the upgrade. INSTALL verifies that the server object and authentication keys still exist and that the server still exists in all the replica rings for replicas that were on this server before the upgrade. If you copied BACKUP.NDS to a second server, you might need to re-authenticate as prompted.

IMPORTANT: Remember that these backup and restore tips do not consider the PCI Hot Plug feature on ProLiant servers. With this feature, drives and other hardware can be added, removed, or replaced while the server remains up and running.

recovering from a system crash

When a server crashes, fails, or is taken out of an eDirectory tree without properly removing eDirectory from that server, you need to take several steps to ensure that the remaining network servers can synchronize correctly.

CAUTION: Deleting a server object for a failed server will cause loss of server references unless proper steps have been taken.

If a server fails and needs to be replaced, follow TID # 2920601. The DSMAINT -PSE procedure will retain links to home directories, directory map objects, and eDirectory-aware printing that will be otherwise lost if the server object is just deleted.

- If time is not synchronized, changes cannot properly be made to the directory services tree. See TID 2908867 for time synchronization help.
- If a server goes down permanently or is replaced without removing eDirectory, the replicas it contained will have incorrect replica ring information. You must clean the replica rings; otherwise, each server in each of the replica rings will still think the downed server should be contacted with updates whenever they occur.
- Verify that a master replica exists for each partition. Run DSPEPAIR.
- Always stop and allow eDirectory to complete the synchronization and/or replication process before proceeding with any additional administration tasks.

  Note: You might need to bring the server DOWN before you can delete the server object.

- Clean up the eDirectory Tree (server objects). Run PARTMGR or eDirectory Manager in Windows.
- An undocumented utility that can be useful in managing eDirectory for Windows NT is the NDSConsole (NDSCONS.EXE) copied into the directory that you specified to store NDS information. This utility shuts down NDS or load additional modules.
- NetWare stores eDirectory database files on Volume SYS: However, in a Windows environment, the server stores the NDS database files in an eDirectory installation directory (which can be replicated on multiple servers).

hp manageability and integration with Asset Manager

eDirectory Collection Agent is a solution that simplifies inventory management by automating the collection of hardware asset data for ProLiant servers running in a NetWare environment. This tool enables administrators to view asset information from anywhere on the network using the Novell java-based ConsoleOne application. HP developed NetWare loadable modules (NLMs) retrieve server information collected by HP Management agents.

To download the user guide for the NDS Collection Agent solutions, go to http://h18013.www1.hp.com/products/servers/management/dl_instr.html.

HP has developed a snap-in for ConsoleOne that displays all server hardware data as extensions to server objects within the tree structure. For additional information or to download this tool, visit http://h18013.www1.hp.com/manage/netware_nds.html.

meta-directories and other net services solutions:

A meta-directory is a directory of directories acting as the primary source for information about a network, applications, and users. By synchronizing with the other directories on a network, a meta-directory enables an administrator to make changes to one database. The meta-directory then propagates this information to the other directories.

Major directory vendors have embraced the metadirectory concept, including IBM, Microsoft, Netscape, Novell, and Siemens.

Be aware of the authoritative sources for your system. Certain systems may have authority over specific attributes. Also, determine your company's policies on data flow. This task is critical before starting.

Novell DirXML

One solution for enterprise wide directory integration is DirXML. By using the Extensible Markup Language (XML), administrators create rules to define what information is shared between directories and how it should be shared. It facilitates the movement of data between eDirectory and a given application, database, or directory for synchronizing common data between them.

It is a bidirectional framework enabling administrators to specify data will flow from eDirectory to the application and from the application to eDirectory. FAQs are available at http://www.novell.com/products/edirectory/dirxml/faq.html.

Go to the other tab on your driver set and add both DirXML trace options and set to 3. This action will give you the tracing you need to debug your XSL and XML.

iFolder and iPrint

Novell Net services solutions simply means a consolidation of all network resources, including wireless, forming one highly accessible scaleable secure network regardless of operating systems and personnel location. Two applications in the arsenal are iFolder and iPrint, making access via the Internet a reality.

iFolder is bundled with NetWare 6 and is also available as a separate application. It lets you access files from anywhere, 24/7 and is like having a single, virtual work folder. It offers access from any computer that has Internet access with a web browser. All that is necessary is that local files placed in the iFolder directory for easy access.

iPrint enables users to print to any printer they are authorized to use, no matter where its located or whether it is in front of or behind a firewall. iPrint makes net printing a reality it allows users to find the right printer, automatically receive the right printer driver and, send the print job to that printer.

For information about iPrint, visit www.novell.com/products/netware/printing/. Additional information about iFolder is available at www.novell.com/products/ifolder/.

NetPro Computing Solutions

NetPro Computing, Inc. is the leading provider of software for managing critical eBusiness and enterprise directories, signed a worldwide software distribution agreement with HP designating NetPro as a Solution Provider.

DS Analyzer collects and displays data all the way down to the object level, making it possible for you to establish baselines for network traffic with a few simple steps. You can view such potential eDirectory issues as excessive tree walking, backlinking, replication storms, and extreme hop counts

DS Expert ensures access to business-critical resources by constantly monitoring the directory and alerting administrators to problems that can cause service interruptions. It watches everything from replication latency issues to synchronization errors that can impact the integrity of the directory and prevent user access to vital network services.

Under the terms of this agreement, HP resells the NetPro directory infrastructure management solution to the customers of its consulting organization. NetPro offerings include DS Analyzer™, and DS Expert™.

For more information on these NDS solution products, visit NetPro Computing website at www.netpro.com/products/products.cfm.

summary

Novell eDirectory is the market leader in directory services. HP and Novell have a long tradition of working closely together to create solutions that are highly integrated, quick to deploy, and easy to maintain and manage. HP and Novell have been partners in innovation, pioneering many of the major technology breakthroughs that made high-performance; high-availability networks a reality.

More than a simple marketing partnership, our two companies have actually integrated product development efforts. Novell has HP ProLiant servers and StorageWorks solutions in its lab, testing, optimizing, and developing OS and software packages on them.

for more information

HP also provides information enabling you to stay current on the latest developments and assisting you in making deployment decisions. To learn more about the HP and Novell partnership, visit our website at http://h18000.www1.hp.com/products/servers/software/novell/index.html.

To learn more about ProLiant servers, visit www.hp.com/servers/proliant.

feedback

Help us improve our technical communication. Let us know what you think about the technical information in this document. Your feedback is valuable and will help us structure future communications. Please send your comments to: OSIntegrationFeedback@hp.com.

02/2003

Document Number TC030201IN