eDirectory™ on Linux

Frank Moore
ATT Engineer/Instructor
Novell, Inc.

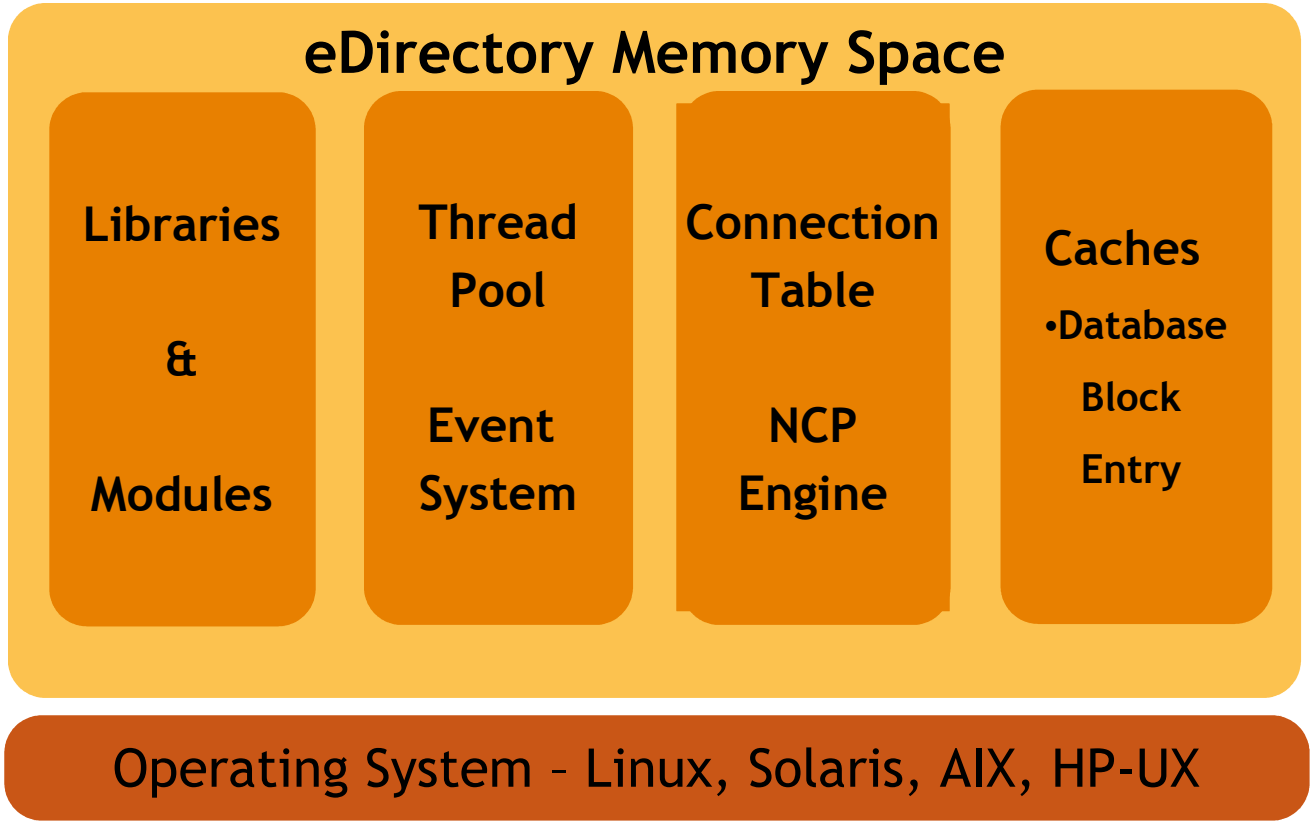
Rick Killpack
World Wide Support / eDirectory
Novell, Inc.

Novell®

Agenda

1. Implementing eDirectory on Linux
2. Managing the ndsd process
3. Installing eDirectory on Linux
4. Monitoring eDirectory with SNMP
5. Managing and Monitoring with iMonitor
6. eDirectory command line utilities
7. Log files
8. Linux Authentication to eDirectory
9. Linux Client Configuration

Implementing eDirectory on
Linux Model



Novell.

Implementing eDirectory on
Linux Specifications

4 GB of Addressable memory for the process

- Requires kernel tweaking to get to 4 GB
- Otherwise limited to 2.8 GB to 3.6 GB

Runs in the User memory space

Works well in multi-processor environments

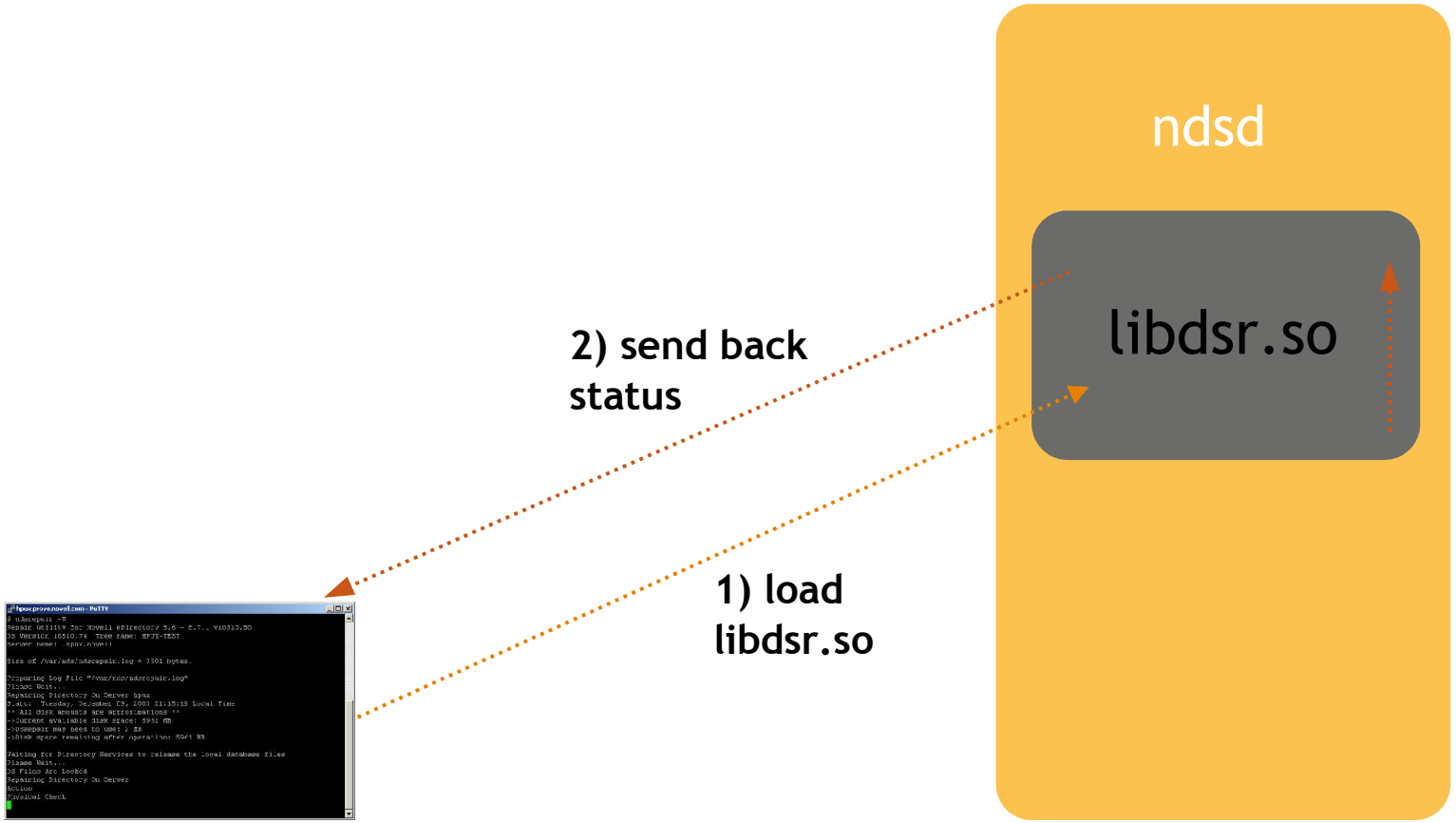
Run as root

eDirectory admin can:

- Relocate DIBS
- Relocate Logs

Most utilities are wrappers to libraries

Implementing eDirectory on Linux
Utilities Execution



ndsrepair -U

Implementing eDirectory on Linux
Location of Components

Configuration

/etc

Dib

/var/nds/dib

Logs

/var/nds

Libraries

/usr/lib

/usr/lib/nds-modules

Binaries

/usr/bin

usr/sbin

Novell.

Implementing eDirectory on Linux
Configuration Files

/etc/nds.conf

- Primary configuration file for ndsd

/user/lib/nds-modules/ndsmodules.conf

- Configures how modules are loaded on startup
- Configures what modules are loaded
- To troubleshoot remark them out and load 1 at a time

/etc/ndsimon.conf and ndsimonhealth.conf

- Allows for customization of iMonitor

/etc/nici.cfg

- Contains the nici configuration, version, strength, etc…

Implementing eDirectory on
Linux OES Default Ports

Service	Port
NCP	524
SLP	427
LDAP	389
Secure LDAP	636
HTTPSTK (imon, iconsole)	8028
Secure HTTPSTK	8030

- Locate the current httpstk ports --> ndsconfig get | grep http
- locate the NCP ports --> ndsconfig get | grep tcp
- Locate the LDAP ports --> ldapconfig get | grep -i port

Managing the ndsd process
Starting and Stopping

The service script for both Linux and Solaris:

- Starting: /etc/rc.d/init.d/ndsd start
- Stopping: /etc/rc.d/init.d/ndsd stop

It is recommended not to start and stop ndsd manually

- Use the scripts !!!

Managing the ndsd process
Monitoring ndsd

```
# ps -eaxf |grep ndsd
    root      5067     1  0 00:54 ?        00:00:00 /usr/sbin/ndsd
    root      5070  5067  0 00:54 ?        00:00:00 /usr/sbin/ndsd
    root      5071  5070  0 00:54 ?        00:00:00 /usr/sbin/ndsd
    root      5072  5070  0 00:54 ?        00:00:00 /usr/sbin/ndsd
    root      5074  5070  0 00:54 ?        00:00:00 /usr/sbin/ndsd
    root      5075  5070  0 00:54 ?        00:00:01 /usr/sbin/ndsd
```

These threads are Light Weight Processes (LWPs)

- Reduces switching overhead
- You see as multiple ndsd's running on same machine
- Can use pstree to see as structure view
  - E.G. pstree `cat /var/nds/ndsd.pid`
- Use top to make sure ndsd not hogging system resources

Novell.

Installing eDirectory on Linux
Considerations

Memory

Disk space for DIBs, libraries, binaries and logs

CPU speed and number of CPUs

File System Types

I/O channel

Platforms

Time Synchronization

Communications using SLP and hosts.nds

SNMP for monitoring activity

Novell.

Installing eDirectory on Linux
Considerations

Memory
- 128 - 256 MB minimum.
- 2 GB just for eDirectory usually works best.

Disk space
- Full installation ~ 300 MB
- Approximately 74 MB for every 50,000 objects

CPU speed
- 200 Mhz min. (Intel only for Linux)
- => 400 Mhz recommended.

Note: See the README and the Documentation for Details!

Installing eDirectory on Linux
Considerations

File System Types

- The file system must be on a local bus !!!
- eDirectory is not supported on NFS mount
  - DIB corruption can occur
- It does work with many file systems
  - reiserFs, ext2, ext3
- SANs are supported through a local bus

Platforms

- eDirectory is only built for x86 architecture
  - Other platforms will not work
  - For example: IBM S/390 or Power PC

Installing eDirectory on Linux
Considerations

Time Synchronization

- Important thing is that it is synchronized
- If use NTP
  - nptdate <time_source>
    - Must be run when ntpd is not running
  - ntpq –p
    - Use to test ntp configuration
  - /etc/ntp.conf
    - Syntax
      - Server 127.127.Xtype.0 prefer
      - Fudge 127.127.XType.0 stratum 0
    - Local hardware clock
      - Server 127.127.1.0
    - Remote IP NTP time source
      - Server clock.via.net
    - Ports
      - 123 for tcp/udp

Installing eDirectory on Linux
Considerations

Communications

- SLP
  - Can use existing SLP on system or it installs NovellSLP
    - OpenSLP - Uses TCP
    - Novell SLP – Uses UDP
  - Configuration in /etc/slp.conf
  - Ports 427 tcp/udp
  - The "smart switch /stupid router" problem
    - Newer switches placed between hosts and routers will not route to hosts. See specific switch documentation.

Installing eDirectory on Linux
Considerations

Communications

- /etc/hosts.nds
  - Used to resolve tree names to server referrals.
  - It is a static lookup table used by eDirectory applications to look up eDirectory partitions and servers.
  - If a tree or server is not available in the file, then the lookup is performed through SLP.
  - Can be used to avoid SLP multicast delays when a SLP Directory Agent (DA) is not present in the network.

Installing eDirectory on Linux
Considerations

Sample /etc/hosts.nds

```
## Master of tree partition
Partition ----------- Server DNS or IP
CORP.                 server1.corp.com
## R/W of tree partition
CORP.                 server2.corp.com

## Master of novell partition
novell.CORP.                 server2.corp.com
## R/W of tree partition
novell.CORP.                 server1.corp.com

## Server name --------- Internet address
NCPserver1                 server1.corp.com
NCPserver2                 server2.corp.com
```


Novell.

Installing eDirectory on Linux
Procedure

1. Download & extract tarball
   - # tar -zxvf eDir_873_linux.tgz
2. Change to the install directory
   - # cd ./Linux/setup
3. Install the binaries
   - # ./nds-install
4. Configure an instance of eDirectory
   - # ndsconfig add -t MyTree -n Novell -a admin.Novell ...

Installing eDirectory on Linux
Procedure

If adding to an existing tree

- Test in a lab
- Understand the process
  - nds-install does not run ndsconfig
- Run a health-check on the environment
  - Check in iMonitor
    - Maximum Ring Delta
    - Health Options (Green Lights)
    - Time Sync

Installing eDirectory on Linux
Procedure

Installation FAQ's

- What if the the installation fails finding my existing eDirectory environment (tree)?
  - Check SLP environment, daemon running, configured
  - If using /etc/hosts.nds file then create it before the installation.
  - Run ndsconfig with the (-p server_address) to specify a server that holds a partition of the tree.
- What if eDirectory fails when getting schema?
  - Is a firewall running on one of the eDirectory servers?
    - Many Linux installations default to having a firewall.
  - Check: iptables -L

Monitoring eDirectory with SNMP
Overview

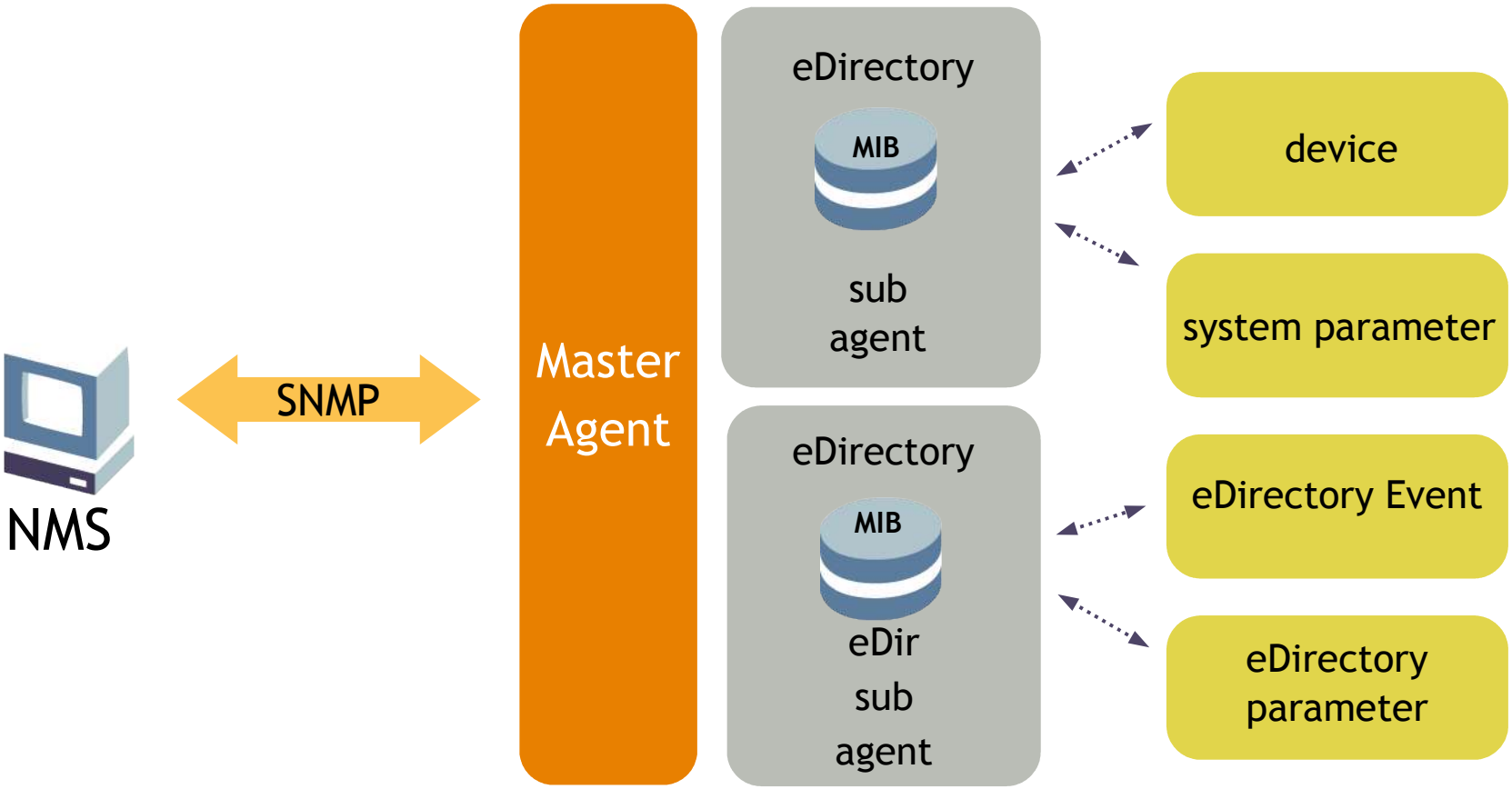
eDirectory has a monitoring MIB

eDirectory events published as SNMP traps

- Can be configured dynamically
- Standard SNMP
- 119 traps
- Provides following statistics
  - Protocols – ndap and ldap
  - Cache - Usage and configuration
  - Server interactions for last 'N' active interactions

Can be used with any 3rd party monitoring console

Monitoring eDirectory with SNMP
Overview



Monitoring eDirectory with SNMP
Installing and Configuring

Supported SNMP Packages

- Use ncd-snmp-4.2.1-7.rpm or later on Linux
- Install package using YaST or rpm tools

Configuring the Master Agent

1. Create SNMP group object
   - Syntax: ndsconfig add –m <modulename> -a <userFDN>
   - Example: ndsconfig add –m snmp –a admin.novell
2. Configure snmp.conf
   - Enter host name
     - trapsink myserver public
   - Add the line
     - master agentx
3. Starting the Master Agent
   - /usr/sbin/snmpd

Novell.

Monitoring eDirectory with SNMP
Installing and Configuring

Configuring the Subagent

1. Configure /etc/ndssnmp/ndssnmp.conf
   - If make changes must restart subagent
   - SERVER hostname/ipaddr
     - Only locally installed eDirectory server supported
     - Required command
2. Starting the Subagent
   - /usr/sbin/snmpd

Novell.

Monitoring eDirectory with SNMP
Installing and Configuring

Dynamic configuration

- Anytime after directory service running
- ndssnmpconfig –h [hostname[:port]] –p password –a userFDN –c command
  - Enable and disable traps
  - Set a time interval for individual traps
  - Set a default time interval
  - List all traps enabled for failure operations
  - List traps that meet certain criteria
  - Reconfigure from ndstrap.cfg

Monitoring eDirectory with SNMP
Modules

Subagent module is NOVLsubag

- Installed as part of eDirectory installation
- Configure using /etc/ndssnmp/ndssnmp.cfg
  - Must give path of trusted root certificate file SSLKEY
- Only monitors server on same machine
  - Limits additional network traffic
- Works with master agent available with OS
  - SNMP version subject to version of OS supports
- Requires user credentials

Monitoring eDirectory with SNMP
Modules

Trap module is NOVLsnmp

- Configure traps using SNMPGroup object
- Use iManager or ndssnmpcfg utility to setup
- Can be configured to send on failures
- Can be configured to send only once in time interval
- Configuration can be shared by multiple servers

Monitoring eDirectory with SNMP
Sample trap

Trap number 51

```
ndsChangePassword    TRAP-TYPE
                     ENTERPRISE  ndsMIB
                     VARIABLES
                          {
                               ndsTrapTime,
                               ndsEventType,
                               ndsResult,
                               ndsPerpetratorName,
                               ndsTransportAddress,
                               ndsProcessID,
                               ndsVerbNumber,
                               ndsEntryName,
                               ndsServerName2
                          }
                     DESCRIPTION
                         "Changing Password"
                     ::= 51
```


Novell.

Monitoring eDirectory with SNMP

Configuring with iManager

Novell iManager

Novell.

User: Admin.novell.SNMP-DEMO.

Roles and Tasks

- Dynamic Group Management
- eDirectory Administration
- eDirectory Maintenance Utilities
- Group Management
- Help Desk Management
- LDAP Management
- NMAS Management
- Partition and Replica Management
- Novell Certificate Server Management
- Rights Management
- Schema Management
- Server Management
- SNMP Management
  - SNMP Overview
  - Create Object
  - Delete Object
- User Management
- WAN Traffic Management

Simple Network Management Protocol: SNMP Group - SERV1.novell

General

General | Traps

	Active	Description	Error Enabled	Interval (seconds)	EOID
27	☐	ndsPurgeStart	☐	5	1.3.6.1.4.1.23.2.98.4
28	☐	ndsPurgeEnd	☐	5	1.3.6.1.4.1.23.2.98.4
29	☑	ndsLimberDone	☑	0	1.3.6.1.4.1.23.2.98.4
30	☐	ndsPartitionSplitDone	☐	5	1.3.6.1.4.1.23.2.98.4
31	☑	ndsSyncServerOutStart	☑	0	1.3.6.1.4.1.23.2.98.4
32	☑	ndsSyncServerOutEnd	☑	0	1.3.6.1.4.1.23.2.98.4
33	☑	ndsSyncPartitionStart	☑	0	1.3.6.1.4.1.23.2.98.4
34	☑	ndsSyncPartitionEnd	☑	0	1.3.6.1.4.1.23.2.98.4
35	☐	ndsMoveTreeStart	☐	5	1.3.6.1.4.1.23.2.98.4
36	☐	ndsMoveTreeEnd	☐	5	1.3.6.1.4.1.23.2.98.4
37	☐	ndsJoinPartitionDone	☐	5	1.3.6.1.4.1.23.2.98.4

OK | Cancel | Apply

Novell.

Monitoring eDirectory with iMonitor
Overview

Tool for diagnosing and monitoring eDirectory

Architecture with 3 components

- NDS Information Gathering Agent
  - Queries eDirectory to retrieve raw data
- HTTP Stack
  - No additional web server needed
- HTML Emitter
  - Presents data to browser

Monitoring eDirectory with iMonitor
Overview

Modes of Operation

- Proxy mode
  - Gather data from server and eDir versions not running iMonitor
  - Do not get all features, some are server-centric
  - Single point of access for remote monitoring
  - Only get server centric information where iMonitor installed
- Direct mode
  - Information displayed is for server being accessed
  - Get all features, including
    - DSTrace
    - DSRepair
    - Background Process Schedule

Monitoring eDirectory with iMonitor
Configuration

NDSIMON

- /usr/lib/imon/ndsimon.conf
- Configure file locations for documentation, traces, etc
- Set HTTP port
- Trace file size
- NIC address assignments
- Timeouts for interactive connections
- Maximum number of concurrent trace files

NDSIMONHEALTH

- /usr/lib/imon/ndsimon.conf
- Configure settings for Agent Health page
- Set reporting levels and ranges
- Set server reporting levels

Monitoring eDirectory with iMonitor
Configuration

Can also test configurations on a temporary basis

- http://<servername>:<port>/ndsimon/config/set?parameter=value

Can list available paramters

- http://<servername>:<port>/ndsimon/config/get

Options available

- Send entry to Replicas
- Mutate Entry
- Remove Entry
- Timestamp Entry
- Reset Schema
- Request Schema

Warning: Use with caution, may cause damage to tree

eDirectory command line utilities
ndsconfig

get/set eDirectory parameters

- Can configure location of DIBs using nds.conf
  - n4u.nds.dibdir – defines location of DIBs
    - Default: /var/nds/dib
  - n4u.server.configdir – defines location of nds.conf
    - Default: /etc
  - n4u.server.vardir – defines location of logs
    - Default: /var/nds
  - n4u.server.libdir – defines location of eDir library
    - Default: /usr/lib
- Better to use ndsconfig than to manually edit nds.conf

eDirectory command line utilities
ndsconfig

Can recover eDirectory Services

- ndsconfig add -m [module]
  - See man ndsconfig for details
  - Create LDAP objects
  - Create SNMP Group object
  - Create SAS Server Certificates (KMOs)
  - Create HTTP object for iMonitor
  - Create NMAS objects.

eDirectory command line utilities
ndsrepair

Check and repair eDirectory

- Check synchronization
  - bash# ndsrepair –E
- Single Object Repair
  - bash# ndsrepair –J [entry_id]
- Checking Obituaries
  - bash# ndsrepair -C -Ad -A

    Found: 0 total obituaries in this DIB,

    0 Unprocessed obits, 0 Purgeable obits,

    0 OK_To_Purge obits, 0 Notified obits

    Total errors: 0
- Check eDirectory time sync
  - bash# ndsrepair –T
- Problems?: Start will all options set to off.
  - bash# ndsrepair -R -l yes -u no -m no -f no -d no -t no -i no -o no -r no -v no -c no

eDirectory command line utilities
ndstrace

Run in command mode or use iMonitor

- Run in commnad line mode
  - bash# ndstrace -l [>> output.log]
- Modules Loaded
  - bash# ndstrace -c modules
  - bash# ndstrace -c “load ndsclone”
- Connections
  - bash# ndstrace -c connections
- Threads
  - bash# ndstrace -c threads

eDirectory command line utilities
ldapconfig

Can administer LDAP server

- View all LDAP server attributes
  - bash# ldapconfig get –a admin.novell –w password
- Change LDAP server attributes to change behavior
  - Can alter logging level on dstrace screen
  - bash# ldapconfig set “LDAP Screen Level”=“all” –a admin.novell –w password
- Can refresh LDAP server
  - bash# ldapconfig –R –a admin.novell –w password

eDirectory command line utilities
ndsindex

Can create, list, delete, suspend, resume indexes

- Installed by default into /usr/ldaptools/bin
  - `bash# ./ndsindex [command] [options] [index]`
- Uses LDAP to manipulate indexDefinition on NCP server object
  - This means LDAP must be working correctly
  - Once modifies indexDefinition kicks off limber process

eDirectory command line utilities
ndsindex

To list CN index

- `./ndsindex list -D cn=admin,o=novell -w password -s cn=SVR01,o=novell CN`
- Result:

```
- Index Version: 0
  Index Name: CN
  Index State: Online
  Index Rule: Value
  Index Type: Added on attribute creation
  Index State Value: Added from server
  NDS Attribute: CN
```


Novell.

eDirectory command line utilities
ndsindex

To add a VALUE index to the uid attribute:

- `bash# /usr/ldaptools/bin/ndsindex add -D cn=admin,o=novell -w novell -s cn=SVR01,o=novell "uid;uid;VALUE“`
- Result
  - Index(es) addition successful.

eDirectory command line utilities
ndsindex

To suspend the uid attribute index:

- `bash# /usr/ldaptools/bin/ndsindex suspend -D cn=admin,o=novell -w novell -s cn=SVR01,o=novell uid`
- Result
  - Index(es) suspension successful.
- `bash# /usr/ldaptools/bin/ndsindex list -D cn=admin,o=novell -w novell -s cn=SVR01,o=novell uid`
- Result
  - Index Version: 0
    Index Name: uid
    Index State: Suspended
    Index Rule: Value
    Index Type: User defined
    Index State Value: Added from server
    NDS Attribute: uid

eDirectory command line utilities
Log files

ndsd.log

- Log file for the ndsd process.
- Typically found in the "/var/nds" directory.
- Can be changed with n4u.server.vardir directive.
- FIRST PLACE TO CHECK WHEN SOMETHING GOES WRONG!
- Stores initialization, security information, and errors.
- Check the log after installs and errors

eDirectory command line utilities
Log files

schema.log

- Log of schema changes to eDirectory by various utilities.
  - ndsconfig upgrade will extend the schema and write the changes to this log.

ndsrepair.log

- Log of ndsrepair activity run from the CLI
- Alternate log file can be specified
  - # ndsrepair -F

eDirectory command line utilities
Log files

ndstrace.log *(NOTE: These commands work after typing ndstrace at a terminal).*

- Set the log file size:
  - set ndstrace=*M<size_in_bytes>
- Reset Log file:
  - set ndstrace=*R
- Log the CLI output to a file
  - svr1:/var/nds # ndstrace; ndstrace file on

    or
  - svr1:/var/nds # ndstrace -l > /pub/dstrace_example.log &

eDirectory command line utilities
Log files

syslog (/var/log/messages)

- Check for kernel errors such as
  - Bad memory
  - Out of disk space
  - Bad NIC
  - Port conflicts

eDirectory command line utilities
Log files

Log support tips

- Search for errors in the logs and then search support.novell.com
- Search for errors in iMonitor
- Search for signals
  - Signals are “software interrupts”
  - SIGPIPE (13) – There was a broken pipe in IPC
  - SIGTERM (15), SIGINT (2) – Shuts down the service
  - SIGABRT (6) – Causes a core dump of the process

Linux Authentication to eDirectory

Recommendations

Use LDAP APIs for cross-platform services that require accessing eDirectory objects and attributes.

Use PAM-ldap for native Linux applications for Linux authentication and authorization.

- Configured by default in OES

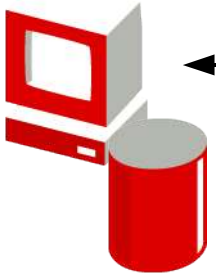
Use DirXML® (Novell Nsure® Identity Manager 2) when the applications are not directory-enabled, PAM-enabled or cannot be customized.

Novell.

Linux Authentication to eDirectory
Overview

User credentials

Credentials validated
User's Unix profile forwarded
User is accepted for login
User's SHOME



User credentials

Multiuser login enabled

eDirectory
LDAP/S Enabled

Schema extended
for Unix profile
uid
gid
login shell
...

Linux Client
pam_ldap enabled
/etc/password
only system users are stored locally

Linux Authentication to eDirectory

- “Meet all prerequisite requirements.” on page 9
- Extend schema in eDirectory with rfc2307 schema.
- Create a Group Object in eDirectory that will contain the PAM enabled users.
- Add a gid value to the gidNumber attribute to the new group.
- Add a distinctive uidNumber, gidNumber, loginShell and homeDirectory values for each user in eDirectory.
- Configure home directories for each user on the SuSE 9.2 or RedHat 9 workstation and assign appropriate rights so that the users can access them.
- Enable PAM authentication on the Linux workstations.
- Configure the pam.conf file on the SuSE 9.2 or RedHat 9 workstation.
- Configure the ldap.conf file on the SuSE 9.2 or RedHat 9 workstation.
- Configure the nsswitch.conf file on the SuSE 9.2 or RedHat 9 workstation.

Novell®

Novell