Introduction to eDirectory

Johnnie Odom
The School District of Escambia County (ECSD)
and the Technology Transfer Partners (TTP)

Brief Intro

- Designed to Model and Electronically Enable the Individuals, Objects, and Relationships in any Organization
- eDirectory is a X.500-compliant Directory Service
- Originally made by Novell, now by Micro Focus
- Actively developed, used by large organizations world-wide
- Stands on its own and powers other products
- Runs on Linux, Windows, and NetWare (obsolete).
- Can be used in the Cloud but shines in on-Prem

This Session

- Emphasis on Showing
- Will skip install (we assume eDirectory already exists in your environment)
- Explain the usefulness of eDirectory
- Basic usage
- First-Level Troubleshooting
- Simple Internals
- Additional Features and Considerations

Accessing eDirectory

- Main tool is iManager
  - A Tomcat-Based Web Application
  - Can run anywhere and access any eDirectory instance (not just on server where it runs)
    - Login with user, password, and Tree name or DNS name or IP of an eDirectory server.
- LDAP can also be used to access eDirectory
- New web-based admin tool coming soon

What Am I Looking At?

- eDirectory is Hierarchical — structured like a tree.
- A Tree Root is at the top
- Below the Tree Root is usually an Organization (O) object that contains everything else.
- Additional organizational units / containers (OU) divide the tree into sections
    - These allow the tree to represent geographical places, departments, or other divisions that form the hierarchy
- Objects representing individual nouns in the organization (like people, groups, printers, etc.) are under the OUs.
- Objects have attributes that define them.
- The type of attributes an object can have are defined by its Type, which is defined in the eDirectory schema
    - Objects can have more than one type
    - Schema can be heavily modified by design
- Links between objects are handled by an attribute (or even two) linking to another object (and perhaps another on the other object linking back)
- The address or location of an object or container is its DN (Distinguished Name) which uses its common name (CN) and the reverse path of every container the object is under
    - For example: cn=jodom,ou=pensacola,ou=escambia,ou=FL,o=US
      User jodom is in City Pensacola, in County Escambia, in State Florida, in Organization / Country US

Why Is This Useful?

- eDirectory is not just about users and groups
    - Although it does users and groups better than anything else.
- Any real or “organizational fiction” element can be created in eDirectory so that your directory resembles your organization and has all the capabilities and rules of the organization.
- Multiple eDirectory instances can be created for different aspects of your organization (internal employees, external customers, etc.)
- For basic user management, the feature set is very powerful:
    - Universal Password to allow any password format and keep credentials safe.
    - Robust LDAP and other standards support
    - Proprietary X.500 feature implementation accessible through NCP Server and LDAP (superset of LDAP)

Certificate Server

- Since eDirectory implements X.500, it also implements X.509 — the basis for SSL.
- A CA (Certificate Authority) is automatically created when eDirectory is installed.
- eDirectory servers always mint certificates from the CA for LDAP etc.
- Other certificates can be minted from CA
- Certificates can also be imported into eDirectory for use.

eDirectory Rights

- Strong inheritance with effective rights, inherited rights filters, and security equivalence.
- Very granular: Object vs. Property (attribute) rights.
  - Object: Supervisor, Browse, Create, Delete, Rename
  - Property: Supervisor, Compare, Read, Write, Add Self
- Be VERY careful with [Public] rights

Replication

- eDirectory can automatically replicate / copy its data between servers.
- This is not like the relational database model that has primary and secondary databases where writes are handled by primaries only.
- In eDirectory, replicas can be:
  master - Makes some final decisions
  read/write - Can both read and modify data
  read - Read-only
  subordinate - Contains no data, just a placeholder to fetch data from somewhere else
- Replication is a core feature of eDirectory and largely “just works”
- The tree can be partitioned along OU boundaries so that servers can contain different data (i.e. sharing) and servers can hold multiple replicas
  - These days the need for lots of partitions and local replicas is less because machines and networks are so much faster.
  - It is generally good practice to keep 3 copies (replicas) of all data.

Troubleshooting

- iMonitor
  - Examine eDirectory Data, Database, Configuration, and Process on *This* server
  - https://servername:8030
- NDS Trace
  - Available in three versions: iMonitor, dstrace, ndstrace (latter two from CLI)
- ndsrepair
  - Command-Line tool (terrible GUI version also available) to do diagnostics and repair operations
- Backups
  - dsbk for full backups (including roll-forward logs)
  - LDIF export for data-only backups (no passwords or secure objects)

Command-Line

- ndsconfig
  - Configuration and Upgrade. Does not need to be run under normal circumstances
- ndsrepair
  - Primary diagnostic program (very powerful)
  - -E , -N , -T options safe and -R is basic repair (will lock server during repair). Use other flags as directed.
- ndsmanage
  - Bring services up and down
- ndsstat
  - Basic information about running services (always safe to run)
- ndsdump
  - Used only in conjunction with Micro Focus support (dumps database to disk)
- ndslogin
  - Test login
- ndstrace
  - See what is happening in real-time
- ldap
  - Load and unload LDAP
- …. and many others

Some oddities

- eDirectory as a standalone is slightly different than eDirectory on Open Enterprise Server
  - Different ports for iMonitor
  - Some other ports might clash
  - OES has more bells and whistles because its services depend upon eDirectory
- Three different ways of writing DNs
  LDAP Style: cn=alice,ou=thepalace,o=NYC
  eDirectory Style: alice.thepalace.NYC
  Hybrid: cn=alice.ou=thepalace.o=NYC
  (Which one depends upon what you are doing)
- DNs can be relative:
  If already in o=NYC then alice.thepalace
  If somewhere else (like ou=flamingo,o=MIAMI) then start with period:
  .alice.thepalace.NYC

Newer Functionality

- REST API - Wrapper to LDAP calls
- Identity Console - Replacing iManager (and ConsoleOne, and NWAdmin, and dsbrowse …)
- All the FIPS
- Dockerization

Some Nerd Stuff

- eDirectory is based on the FLAIM database, which was originally used by the Church of Latter Day Saints for genealogy databases.
  - Inherits many advantages from FLAIM
    - Other TTP Presentations on FLAIM available.
- eDirectory is larger written in C++ (core) and Java (some utilities)
- eDirectory also powers Identity Manager and Access Manager
- Using iMonitor, it is possible to fine-tune eDirectory and even to make changes directly to the DIB (data store).

Summation

- Yes, eDirectory can handle users and groups via LDAP
- But it can also act as a perfect model for any organization or real-world relationship via hierarchy and schema extensibility.
- Automatic replication
- Extreme on-Prem scalability
- Allows you to own your identities and organization in a way that no other application does.
- Flexible enough to be the core of many internal applications.
- Even more powerful with OES, Access Manager, and Identity Manager.

Additional Help

- Current Documentation (Will Change)
  https://www.netiq.com/documentation/edirectory-92/

- TTP Mailing List
  Join at https://thettp.org
  Login at https://forum.thettp.org

- Micro Focus Community
  https://community.microfocus.com/