

# A Directory for Identity Management: Which?



Lyn Waddington  
ICT Support Team  
Oxford University  
[lyn.waddington@ict.ox.ac.uk](mailto:lyn.waddington@ict.ox.ac.uk)

# Agenda

- Which? A comparison of Active Directory and eDirectory
- "Which?" report how to compare?
  - Using the Novell Full Service Directory Model
    - Discovery
    - Security
    - Storage Management
    - Relationship
- What is an identity vault and how does it differ from other directory roles?
- Key Distinguishing Features
- Summary

# Which? A comparison of Active Directory and eDirectory

- as with any comparison different features are important for different functions
- we cover
  - differences between general purpose directory and Identity Vault briefly
  - then focus on the Identity Vault

# Which? report

## How to compare?

- no standard means of comparing LDAP directories.
- MS doesn't have a model listing comparing AD features
- use Novell Full Service Directory Model
  - Discovery
  - Security
  - Storage Management
  - Relationship

# Which? report

## How to compare?

- most of the big differences are under Discovery and Storage Management
- related to how objects are stored, and what they can contain, schema etc.
- Discovery includes how data is searched and published

What is an Identity Vault:  
How does it differ from other  
directory roles?



# General Purpose Directories; are multi-functional

- role includes authentication, authorisation, identification
- people and resources e.g. machines
- many applications leveraging it

# General Purpose Directories; are multi-functional

- need to consider which desktop operating systems in use
- file system access and ACL's
- security objects and how they are stored determines resource management including workstations

# The Identity Vault

## A single purpose directory?

- acts as a data store which other general purpose directories can then leverage
- the vault is populated with authoritative data
- design decisions determine the important functions
- other applications may leverage the Identity (ID) vault including the general directories it feeds
- I advocate single purpose directories as can then tailor design and contents for purpose

# The Identity Vault

## A single purpose directory?

- Identity Manager uses the data to populate other directories according to their purpose
- must have flexibility in how to create, populate and transform data to meet design and purpose of subsidiary directories

# The Identity Vault

## A single purpose directory?

- the directory/data store role is all about object creation and management
  - ability to manage expired objects
  - dynamic creation of objects
  - speed of directory lookups
  - ability of the directory to create and manage groups and other security objects according to logic/rules
  - inheritance
  - role based security and other information

# Key Features making eDirectory the best ID Vault



# Key Features making eDirectory the best ID Vault

- event monitor allows directory events to be noticed in real time
  - AD has a poll technology
- MS say their technology is more redundant as no events can be missed, but?

# Key Features making eDirectory the best ID Vault

- AD itself cannot form the ID vault
  - the data is held solely in a MS SQL database,
  - this has advantage of being searchable via SQL
  - but has the disadvantage that it cannot be leveraged via LDAP
  - therefore in the MS scenario we need to use a separate server ADAM for LDAP applications

# Key Features making eDirectory the best ID Vault

- Disadvantages of SQL server
  - security issues?
  - doesn't provide other services as eDirectory (or AD itself) does
  - non advertising
  - objects are not security objects, no role based services at least not that we can operate on the data store itself
  - cannot authenticate against the database itself, in eDirectory we can run a portal off the ID vault to provide user control and workflow on the ID vault itself

# Other distinguishing features

## Full Services Directory Model

Discovery



# Discovery

- eDirectory is not tied into DNS namespace, this means that we can have a multiheaded tree i.e. two top level O's
- organisation of the directory is more flexible, allowing tree merges and un-merges
- grafting and separation of segments of the tree
- AD only has trusts realm and Domain, users have to exist in multiple locations in order to be able to access resources.

# Discovery

- how we name users can be flexible, we can have multiple users with the same name in different contexts within the same tree
- aliases can also be useful to point back to objects in another container
- AD can not do this more detail on naming conventions in AD here, case sensitive but not enforcing

# Search

- eDirectory is ahead with
  - referrals
  - chaining
  - superior referrals
- because of partitioning and smaller number of attributes stamped on each object, faster searches for eDirectory
- superior referrals, referral and chaining are all configurable
- Active Directory has to search entire forest via Global Catalog every time.

# Search

- Active Directory has made progress in how searches are done and has implemented a number of new LDAP v.3 features;
  - Dynamic objects, with a TTL allow on the fly assignments and creation
  - Groups by LDAP search to compare with Dynamic groups
  - Active Directory groups can persist.

# Publication

- AD uses the global catalog which is like a RW replica, it has to contain the entire contents of the domain
- Edirectory publishes its info in two ways,
  - it can be read through utilities such as console 1 and imanager
  - as an address book through other applications such eguide, the IDM portal, extend etc.

# Other distinguishing features

## Full Services Directory Model

Security



# Security

- both systems have a Public Key Infrastructure (PKI)  
both systems break in certificate authority break. AD is heavily reliant on DNS for certificates
- AD does not store information in the directory unlike eDirectory
- AD bundles in SAML for web based SSO, this is also achieved by Shibboleth, which works well with eDirectory

Other distinguishing features  
Full Services Directory Model

Storage Management



# Distribution

- Partitions in eDirectory allow better distribution and filtered replicas faster searches
- Active Directory has Global catalog roughly equivalent to R/W filtered replica, attributes and searches configurable

# Caching

- Active Directory has no usable search cache
  - cache cleared once change committed
  - may lead to slower searches

# Classification

- Active Directory:
  - Schema classes and attributes can now be declared defunct: not be deleted
  - the Common Name (CN) cannot be changed.
  - supports use of periods in dn's, case aware but not enforcing of user names, important regarding external Kerberos implementations

# Other distinguishing features

## Full Services Directory Model

## Relationship



# Inference

- eDirectory;
  - better at calculating permission through inheritance; Active Directory has to calculate every attribute stamp
  - loses out as doesn't have nested groups,
  - dynamic groups not a security principle and non persistent
  - no dynamic objects with TTL (yet)...

# Inference

- Active Directory:
  - every object a security principle
  - ACL lists inheritance models and calculations and how groups work as a security model affect ldap search speed.
  - effective ACL calculator simplifies how calculations are made:
  - still not able to see which users are member of which group without resorting to ADSI

# Summary



# Summary

- Both Active Directory and eDirectory are enterprise class and for general purpose, less and less to choose between the two.
- For Identity Management eDirectory is the most flexible
  - because it has less structural limitations
  - real time change detection
  - it has a directory not a database as the vault
  - thus the ID vault can itself support applications such as the portal to provide a gui environment to allows users:
    - to manage their information
    - make resource requests
    - white pages and organisational charts

# Summary

- Novell's Identity Manager is more flexible, robust and mature product
  - It offers a user interface to allow user management
  - More built in drivers to connect with other systems
  - Drivers are configurable through GUI environment
  - Virtual environment for testing
- These features are likely to be available in the next Microsoft release of MIIS (Microsoft Identity Integration Server)
- Watch this space...

