Directory Replication: from Gigabit LAN to HF Radio

Steve Kille – CEO

October 2011

Some Thoughts on Replication

- One Slide for each section of the paper
  - Key conclusions/points
  - More detail in the paper and URLs
- Leave time to show how it works in practice
- And a few retrospective slides at the end

LDAP & Replication

- LDAP is generally used to share information based on standard schema (people; accounts; PKI etc)
- (High) Replication of this data is often very important
  - For reasons we all understand (performance; locality; reliability)
- There are wide range of approaches

X.500 DISP

- X.500 DISP (Directory Information Shadowing Protocol)
- The only open standard for directory replication
- Good functionality
- A protocol that deserves to be used much more than it is

Strong Authentication for Replication

- Strong Authentication (X.509 PKI) is sometimes sensible for client authentication (e.g., with smart cards)
- It should always be used for server to server authentication
  - Good security and administration characteristics
- Too many organizations avoid it, because it is seen as “scary technology”

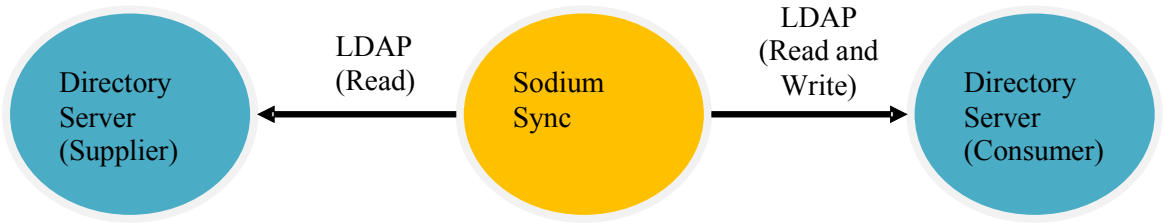
Single Master vs Multi-Master

- Pros and Cons
- Single Master is best for many directory deployments

Disaster Recovery

- Off site disaster recovery is key for some mission critical directory deployments
- Straightforward with multi-master (no special product support needed)
- Straightforward with single master (but you need product support)

LDAP Synchronization



- Replication can be achieved between LDAP servers without any special protocol support
  - And enhanced easily (e.g., Changelog)
- Isode's Sodium Sync product gives server independent replication
- Plus flexible transformation and filtering

Filtered Replication & Security Labels

- Filtered Replication good for sharing selected information
- Security Labels (military and intelligence) are a good way to control replication
  - For example labelling an item “UK Top Secret, Releasable to NATO Countries” vs “UK Top Secret, Releasable to US and Germany” can give flexible data oriented control

Directory Replication by Email

- Seems a crazy idea, but useful for:
  - Messaging-only organizational boundaries
  - Where there are no special or optimized directory protocols:
    - Data Diode
    - HF Radio and other Constrained Networks

“Show Me” Time

- X.500 DISP Replication (and how it can be easy to set up)
- Strong Authentication (for replication): it’s easy and there is no excuse not to use it
- Failover for Disaster Recovery
- Sodium Sync for LDAP replication (and briefly replication by email)
- Security Label based access control (if there is time)

Hindsight on X.500 and LDAP

- The goal was a global directory
- This role has been taken by DNS
  - Which I don't think is the best outcome
- Things could have been different if two things had been done early on with LDAP and X.500

Change 1: Use Domain/Email Names

- Typed attributes are great for data and search
- They suck for naming: awkward for real users
- DC= was too little and too late

Change 2: Sort Top Level Replication

- Today's talk has been all about "leaf" replication
- Top level replication is key to a very large distributed directory
  - getEDB should have been the start, not a dead-end

Questions?

- LDAP has a nice niche, but it could have been much much more