Prior to adoption of LDAP, RCF/ACF had exclusively used NIS as a directory service.

- 7 slow, aging NIS servers for ~2000 node RHIC Linux cluster and miscellaneous systems.
- 3 NIS servers for ~400 node USATLAS Linux cluster.
- 37 NFS servers, each operating as a NIS slave.

Upgrade of Linux farms provided an opportunity to eliminate NIS and switch to LDAP.
Problems with NIS

- Insecure
- Not scalable
  - Flat namespace – no subdomains
  - Max size of 1024 bytes per record
  - UNIX-only
- Not extensible – inability to add new data fields.
  - Demands of GRID applications like GUMS.
- Continued support?
Lightweight Directory Access Protocol

- Central repository used to store and manage directory information.
- Can be used for authorization.
- Data is stored in a directory information tree (DIT).
Why use LDAP as a directory service?

LDAP Features

- Centralized administration and information.
- ACIs (Access Control Instructions)
- Referrals
- Dereferencing
- Security
- Customization and extensibility
- Directory integration
Why choose OpenLDAP?

• Platform independent (Linux, BSD, Solaris, Windows)
• Open source
• Rich feature set

Competitors
• SUN Java System Directory Server (SunOne)
• Microsoft Active Directory
• Novell eDirectory
OpenLDAP components

- slapd – stand-alone LDAP daemon
- slurpd – stand-alone LDAP replication daemon

Database back-ends
- BerkeleyDB (bdb, hdb)
- LDBM (a neutral interface for bdb, gdb,mdbm, ndbm)
OpenLDAP components

More backends

- ldap and meta
- Relay
- SQL
- dnssrv
- Monitor
- Perl and shell

Overlays (many)

- Proxy cache (pcache)
- accesslog
Access Control

Access Control Instructions (ACIs)

- ACIs are hierarchical.
- Access control of information at container, object, and attribute levels.

Examples:

access to *
  by * read
  by anonymous auth

access to dn.subtree= “nisMapEntry=netgroup.byhost,dc=rcf,dc=bnl,dc=gov”
  attrs = @nisMap
  by dn= “uid=rpetkus,dc=rcf,dc=bnl,c=gov” write

access to dn.regex= “uid=globus([^,]+),ou=People,dc=usatlas,dc=bnl,dc=gov”
  by domain=server1.usatlas.bnl.gov
  by dn= “uid=globusadmin,cn=usatlas.bnl.gov,cn=digest-md5,cn=auth” write
• NIS → LDAP Translation
• Nice, stable solution for legacy systems that do not have LDAP client support.
• As with NIS, there is still a 1024 byte limit per record.
• Commercial software
Performance Tuning

• Indexing increases performance dramatically

Situation where indexing would be beneficial:

Many slapd log messages stating:

bdb_equality_candidates: (nisNetgroupTriple) index param failed.

Add to slapd.conf and reindex database using “slapindex”:

Index nisNetgroupTriple pres,sub,eq

• DB_CONFIG : At a minimum, set_cachesize should be increased from the default 256 kb. Use “db_stat -M” to check the efficiency of the db cache.

• Cachesize: Set the amount of entries to be stored in memory.

• Logging: Use sparingly for debugging.

• Increase thread count.
Performance Tuning

• Increase file descriptor limit.
  • Can hard-set by defining FD_SETSIZE in slapd/daemon.c (OR)
  • Increase 1024 fd Linux default
    # /etc/security/limits.conf
    * hard nofile 8192
    # /etc/pam.d/other
    session required pam_limits.so
  • Increase 256 fd Solaris default by recompiling OpenLDAP 64-bit and setting limit with ulimit

• TCP tuning for TIME_WAIT reuse and recycling.
• conn_max_pending and conn_max_pending_auth
  – Set the queue size for incoming requests.
Performance Tuning

Hardware considerations

- Ample memory for large caches.
- Separate hard disk for database logging to prevent thrashing. Useful if heavy writes are expected.
High Performance and Fault Tolerance

LDAP load balancing

- DNS round robin
- LDAP proxy server using meta or ldap backend.
- Software load balancing: LVS and Ultra Monkey.
- Hardware load balancing (layer 4-7 switches): F5, Radware, Cisco CSS.
Load Balancing Solutions

Robert Petkus – OpenLDAP Configuration and Tuning in the Enterprise
OpenLDAP Issues / Qualms

- Dereferencing is slow.
- No server-side sorting of search results (RFC 2891)
- Single-master replication. No multiple or floating master replication.
- Logging is expensive.
General Issues

**nss_ldap**
- Statically compiled applications crash if nscd is not running and LDAP is used as a name service.
  - nss_ldap has added dependencies extending beyond glibc proper.
  - Required a recompilation of Condor.

**pam_ldap**
- Differing behavior on Solaris and Linux.
Solaris-specific Issues

OpenLDAP client:

• ldap_cachemgr, while handy for configuration consolidation, introduces a point of failure.
• Need to include extra schemas for ldap_cachemgr to function properly.
• Hard limit of 1000 entries in pagesize request.

OpenLDAP server:

• 256 file descriptor limitation.
• Non-blocking port crash (ITS 3567). How select() is mapped to poll() in Solaris?
Conclusions

- Linux client – server functionality is great.
- OpenLDAP as a drop-in replacement for NIS on Solaris clients is achievable but problematic.
- Strong, active development.
- Many useful backends and overlays available.
- Large-scale deployments will benefit from hardware load balancing.