LDAP as a Service

REALITY CHECK & WISH LISTS

ALL VIEWS AND COMMENTS EXPRESSED HERE ARE MINE AND NOT THAT OF MY EMPLOYER

Let LDAP be ! and All was Light(weight)DAP"

- "Some colleagues and I created a similar protocol called DIXIE, which people liked. Soon after that, I was approached by some people in the IETF community to create a standardized version of DIXIE, and, with the help of a couple of colleagues, that's how LDAP was born.“
  - **Tim Howes**

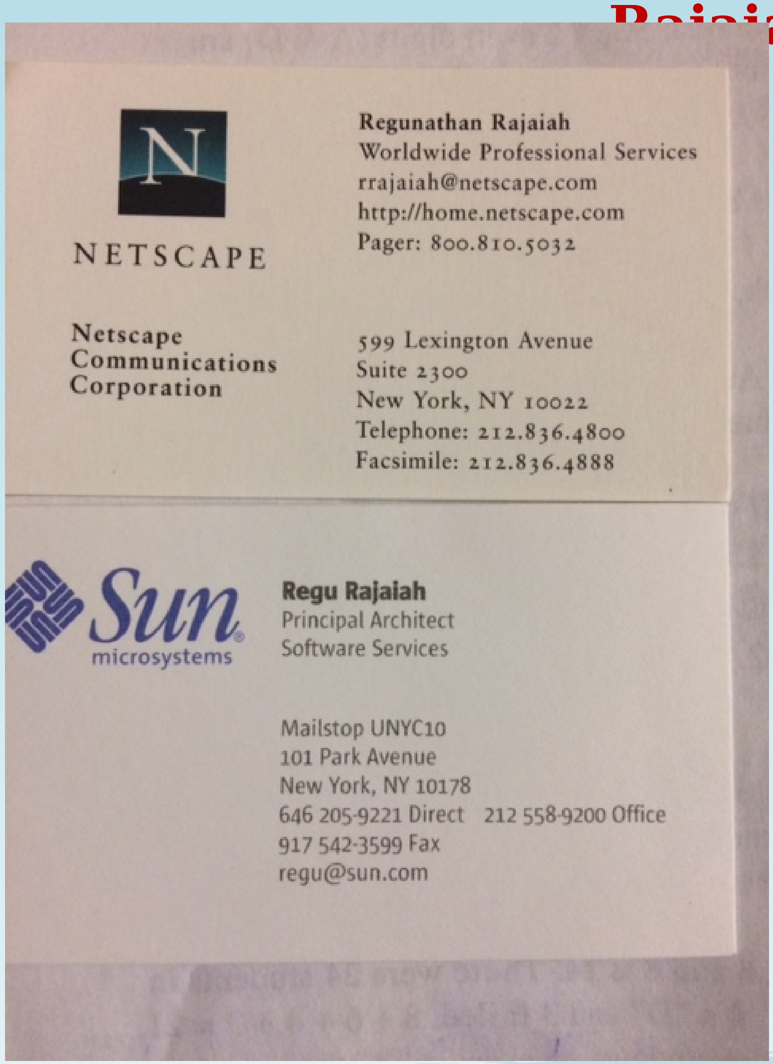
    https://jumpcloud.com/blog/tim-howes-interview-origins-ldap/

What is on Tap?

- ldapWHOAMI
- Landscape
  - Vendor pitch
- Reality Check
  - Few standards and many not so!
- Wish lists
- Q & some A

ldapwhoami

```
ldapwhoami -x -D "cn=Regu Rajaiah,dc=ldapconn,dc=com" -W
```



NETSCAPE

Regunathan Rajaiah
Worldwide Professional Services
rrajaiah@netscape.com
http://home.netscape.com
Pager: 800.810.5032

Netscape
Communications
Corporation

599 Lexington Avenue
Suite 2300
New York, NY 10022
Telephone: 212.836.4800
Facsimile: 212.836.4888

Sun
microsystems

Regu Rajaiah
Principal Architect
Software Services

Mailstop UNYC10
101 Park Avenue
New York, NY 10178
646 205-9221 Direct 212 558-9200 Office
917 542-3599 Fax
regu@sun.com

Millions of entries

Large number of static groups

Feature

Bug

Billions of searches

Sev 1 / Sev 2

RCA / ETA ??

Regu Rajaiah
Vice President

citigroup

Citigroup Technology, Inc.

Regunathan Rajaiah
Vice President

Morgan Stanley

LDAP servers - landscape

Vendor	Product	Lang
Oracle	ODSEE	C
Oracle	OUD	Java
Open source	OpenLDAP	C
Open source	Apache DS	Java
Ping	Ping DS	Java
ForgeRock	OpenDJ	Java
IBM	IBM security directory server	C
CA	eTrust	C
Microsoft	AD	C
Redhat	Fedora-389	C

LDAP vendor pitch

MATCH / OUTPERFORM ODSEE

MIGRATE FROM ODSEE

“Are you still relying on a legacy directory server like Oracle/Sun Directory Server Enterprise Edition (DSEE)? “- Pingidentity

“As the legacy Sun product has reached its end of life, many companies are looking at migrating from Sun Directory Server Enterprise Edition [SunDSEE] to ….” - ForgeRock

Reality check

I’m not strange, weird, off, nor crazy, my reality is just different from yours.
– The Cheshire Cat

Standards	**Not so so**
Lightweight Directory Access Protocol (v3)	Access control
The String Representation of Standard Attribute Syntaxes	Replication
A String Representation of Distinguished Names	Large static groups
LDAP Data Interchange Format (LDIF)	Password Policy
LDAP Password Modify Extended Operation	Operational attributes
Lightweight Directory Access Protocol (LDAP): Syntaxes and Matching Rules	Referential integrity
	Attribute uniqueness

Reality check

Standards	**Not so so**
	Extended operations
	Server side controls
	Retro changelog
	GSSAPI-Mapping
	Logging
	VLV
	Pass through authentication

LDAP Wish lists

Installme.txt

- Reduce per instance foot print
  - Binaries , libs on shared file system [SFS]
  - All DB files too ?
  - Links to file on SFS
- Non root installs
- JRE bundles
  - Modify lib/security/….
- Upgrade /Migrate woes
  - Think large deployments
  - Big Bang not an option

I BIND therefore I am

- Bind with any unique attribute
  - Uid,mail,any other custom attribute
- AD implementation
  - “accepts several forms of name in the name field of the Bind Request. Each name form is tried in turn”
  - https://msdn.microsoft.com/en-us/library/cc223499.aspx
- Use case
  - RDN: emplid=100001,ou=emp,.....
  - Client apps have access to uid, or mail like attributes
  - One less search

BIND

GSSAPI Mappings

- Role mapping with regular expressions

- No per entry ,static definition of principal

BIND

- u:
- dn:

- Configurable Service principal
  - No hard coding of “ldap/…….”

- minssf encryption support

SRCH and you will find

- Scoping * search
  - Search for * , get only attr1,attr2,.....attrn
  - ACI on * search
  - Helps to track attribute usage

- Virtual attribute for group size

- Robust ‘ismemberof ‘ implementation

- Group search with uid , login name …etc
  - Use case
    - uniquemember: emplid=100001,ou=emp, ...
    - Client apps have access to uid, or mail like attributes
    - One less search

SRCH and you will find

- Query Execution Plan
  - Estimates on etimes, no of entries looked into
  - Number of entries in result set
  - Index suggestions
  - Helps to track attribute usage

- Search filters to support
  - All attributes of a specific OC or combinations

- Unindexed search override for groupdn

- Ability to reindex system indexes
  - ancestor , parentid
- Reindex on one host / Copy to other hosts
- Index files on SFS

SRCH

Groups

- Large static groups [MV attributes / large value set]
  - >N members ?
  - Internal representation
    - Optimized ?
  - Modification/ Deletion write traffic
    - Replication
    - Tombstone
  - Referential integrity triggered

- Reverse group lookups
  - All the groups XXX is member of ?
- Tracking group usage
  - When was a group last used ??

Groups

Access control

- ACI regression scripts
  - Permissions before/after ACI change
  - ACI syntax validation CLI
- Restrict attributes of specific OC [targetoc
  - All attributes of a specific OC or combinations
- Deny specific operations based on conn method [Non SSL/SSL]
- Public attributes
  - If attrX belongs to publicattrs OC , read
    - If not deny
- ACI rules in QEP
- ACI dry run

Access control

- ACI on subtypes
  - GDPR [manager;UK, manager:USA]
- ACI eval on Boolean filter
  - (|(telephonenumber=1234567890)(cell=1234567890)(homephome=1234567890))
  - BIND DN can read telephonenumber,cell but not homephone

- ACI on log level setting
- IP addresses mapping / wild cards / masking

Password Policy

- Global account lockout
  - Password policy attributes
    - Replicated
    - Not replicated
    - Read only consumers

Password policy

- Multiple password policies
- Admin override

- Assign password policy to groups
  - No COS

- Operational attributes
- Biggest migration challenge

Log Analytics

- Compatible with ODSEE logging

- BIND DN only on tag=97 err=0
  - Log analytics “slow” to correlate operations by BIND DN
  - Conn the glue
  - BIND DN on all operations ?

Log analytcis

- Debug levels / options – leak data ?

- Customizable logs to separate
  - PA operations
  - High etimes
  - Specific filters, attributes

Log Analytics

- Audit logs
    - Parsing , correlation scripts
    - Undo ldifs from audit
    - Data classification
        - Hide/show attributes

Log analytcis

- Encrypt / Sign audit logs
    - Tamper proof

- Modification origin host:port:DN:timestamp
    - Replication overloading this data

Replication

- Mutual host authentication
  - Kerberos

- Alerts on changelog size

- Different set of replicas with “days” lag
  - 1 day
  - 2 days

Replication

- Proactive check of changelog db health [cli]

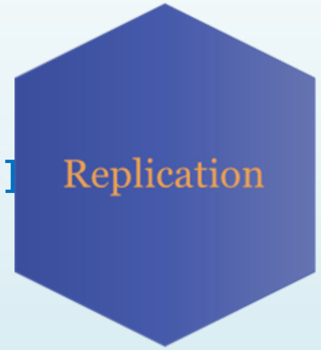
- Reinitialize entire topology
- Steps to deco master / hub from topology

  - CLEANRUV Ludo ?

Replication

- Replicated operations
  - Log originating instance:port
  - Log operation complete time on originating instance:port

- CLI tool to trace a mod op in time & server



Replication

- All Masters topology
  - Client app mod operations on any of the masters
  - Ordering of replication
    - Specially DEL

- More granular replication debugging

- Document firewall ports

Retro changelog

- Changelog access over LDAP

- Global / consistent change number
- HA

- Granular ACIs on changelog
- Configurable list of attributes to log/not to log

- Indexing guidelines on retro
- Health check scripts
- Enable / Disable implications

- Export / Import retro changelog

Retro
change
log

Multi Tenancy

- Single instance
  - Multiple listeners

- Config.ldif
  - Common config
  - Tenant specific

Multi
tenancy

- Schema
  - Common schema [..config/ldif/schema/common]
  - Tenant specific [..config/ldif/schema/$tenant$]

- ACIs
  - Common ACI [Suffix]
  - Tenant specific

Fries, Chocolate, Waffles

- Most of the enterprise features are vendor proprietary
- Make your own wish lists
- Product / wish list analysis

Fries, Chocolate, Waffles

- “World was created in seven days”
  - No migration to worry about

- What is in your wish list ?

@luvcrypto
regu.rajaiah@gmail.com