

LDAP in a Linux Environment

Smoot Carl-Mitchell
smoot@tic.com

Server Environment

- 11 servers
- 12-16 virtual servers under VMware
- Linux RedHat Enterprise Linux

Motivation for LDAP

- Individual password files on all servers
- No naming standard for uids
- No group naming standard for access control
- Difficult user administration

Requirements

- Centralized authentication store
- Fault tolerant
- Easy administration
- Web authentication
- Per machine authorization

Required Software

- OpenLDAP
- OpenSSL
- nss_ldap
- pam_ldap
- mod_ldap

Architecture

- 2 load balanced read-only servers
- backend master server (update master)
- replication from backend to front-end

Schema Design

- core – base LDAP object classes
- nis – emulates Sun's NIS
- inetorgperson – useful objects for people
- sudo – integration of sudo authorization

users and groups

- dc=com,dc=subimo,ou=People
- dc=com,dc=subimo,ou=Group
- standard object set for authenticating users
- replacement for /etc/passwd and /etc/group

People entry

- uid=smoot (unique RN)
- cn=Smoot Carl-Mitchell
- sn=Carl-Mitchell

- plus a bunch of other attributes

Certificates

- private signing certificate
- LDAP server certificate
- used to support encryption on LDAP ports
 - 389 – TLS
 - 636 - SSL

Administrative Tools

- Jxplorer
- phpLDAPadmin
- adduser (geared towards Linux systems)

OpenLDAP Server Configuration

- `/etc/openldap/slapd.conf`
- `/etc/openldap/ldap.conf`

/etc/openldap/ldap.conf

```
BASE                dc=subimo,dc=com
HOST                prod1.subimo.com prod2.subimo.com
PORT                389
TLS_REQCERT        never
SASL_SECPROPS      none
```

/etc/openldap/slapd.conf

```
# Master SLAPD server configuration.
loglevel          0
include           /etc/openldap/schema/core.schema
include           /etc/openldap/schema/cosine.schema
include           /etc/openldap/schema/inetorgperson.schema
include           /etc/openldap/schema/nis.schema
include           /etc/openldap/schema/evolutionperson.schema
include           /etc/openldap/schema/sudo.schema
include           /etc/openldap/schema/samba.schema

pidfile           /var/run/slapd.pid
argsfile          /var/run/slapd.args

# Create a replication log in /var/lib/ldap for use by slurpd.
repllogfile       /var/lib/ldap/master-slapd.repllog

# Timeout idle connections after an hour.
# This a hidden master and is not subject to a lot of query traffic.
# idletimeout     3600

# TLS Configuration
TLSCipherSuite    HIGH:MEDIUM:+SSLv2:+SSLv3:RSA:+TLSv1
TLSCertificateFile /usr/share/ssl/certs/ldap.pem
TLSCertificateKeyFile /usr/share/ssl/certs/ldap.pem
TLSCACertificateFile /usr/share/ssl/certs/ca-bundle.crt
TLSVerifyClient   never
# Password hashing - Use the Linux crypt with MD5 extensions
password-hash     {CRYPT}
password-crypt-salt-format $1$%.8s
```

/etc/openldap/slapd.conf

```
access to dn="" by * read
access to dn.sub="ou=Customers,dc=subimo,dc=com"
    by dn.base="uid=ldaproot,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=customerroot,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=ldapnobody,ou=people,dc=subimo,dc=com" read
    by anonymous auth
    by * read
access to attrs=uid,uidNumber,gidNumber,homeDirectory,loginShell
    by dn.base="uid=ldaproot,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=ldapnobody,ou=people,dc=subimo,dc=com" read
    by anonymous auth
    by * read
access to attrs=shadowLastChange,shadowMax,shadowWarning,ShadowExpire,shadowFlag,shadowInactive,shadowMi
    by dn.base="uid=ldaproot,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=ldapnobody,ou=people,dc=subimo,dc=com" read
    by anonymous auth
    by * read
access to attrs=userPassword,sambaLMPassWord,sambaNTPassWord
    by dn.base="uid=ldaproot,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=ldapnobody,ou=people,dc=subimo,dc=com" read
    by self write
    by anonymous auth
access to *
    by dn.base="uid=ldaproot,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=ldapnobody,ou=people,dc=subimo,dc=com" read
    by self write
    by anonymous auth
    by * read
```

/etc/openldap/slapd.conf

```
database      bdb
suffix        "dc=subimo,dc=com"
rootdn        "cn=Manager,dc=subimo,dc=com"
rootpw        {SSHA}Xe9pDmpQT/iVJO6hW1VUfHQlduvcZn9B
directory     /var/lib/ldap
index objectClass,uid,uidNumber,gidNumber,memberUid eq
index cn,mail,surname,givenname eq,subinitial
```

NSS and PAM Configuration

- `/etc/ldap.conf`
- `/etc/ldap.secret`
- `/etc/pam.d/system-auth`
- `/etc/nsswitch.conf`

/etc/ldap.conf

```
# Connection info
host prod1.subimo.com prod2.subimo.com
port 389
timelimit 30
bind_timelimit 30
idle_timelimit 3600
# Directory parameters
base dc=subimo,dc=com
ldap_version 3
scope sub
# Credentials
binddn uid=ldapnobody,ou=people,dc=subimo,dc=com
bindpw *****
rootbinddn uid=ldaproot,ou=people,dc=subimo,dc=com
# Password in /etc/ldap.secret
# Access control
pam_login_attribute uid
pam_groupdn cn=vm.subimo.com,ou=accessGroups,dc=subimo,dc=com
pam_member_attribute uniqueMember
pam_min_uid 100
# SSL
ssl start_tls
tls_checkpeer off
tls_ciphers TLSv1
# Sudo
sudoers_base ou=SUDOers,dc=subimo,dc=com
sudoers_debug 0
# Password changes
#pam_password_prohibit_message Change your password with an LDAP browser.
pam_password exop
```

/etc/pam.d/system-auth

```
auth          required      /lib/security/pam_env.so
auth          sufficient    /lib/security/pam_unix.so likeauth nullok
auth          sufficient    /lib/security/pam_ldap.so use_first_pass
auth          required      /lib/security/pam_deny.so

account       required      /lib/security/pam_unix.so
account       [default=bad success=ok user_unknown=ignore
service_err=ignore system_err=ignore authinfo_unavail=ignore]
/lib/security/pam_ldap.so

password      required      /lib/security/pam_cracklib.so retry=3 type=
password      sufficient    /lib/security/pam_unix.so nullok use_authtok
md5 shadow
password      sufficient    /lib/security/pam_ldap.so use_authtok
password      required      /lib/security/pam_deny.so

session       required      /lib/security/pam_limits.so
session       required      /lib/security/pam_unix.so
session       optional     /lib/security/pam_ldap.so
session       required      /lib/security/pam_mkhomedir.so umask=0066
skel=/etc/skel
```

/etc/nsswitch.conf

```
passwd:      files ldap
shadow:      files ldap
group:       files ldap
```

Replication

- Change requests sent to centralized master
- Changes replicated on load balanced server pair
- Requires setting up slurpd

Replication Configuration

```
# Slave
updatedn          uid=ldapreplica,ou=people,dc=subimo,dc=com
updateref         ldaps://vm.subimo.com:636

access to dn="" by * read
access to attrs=userPassword,sambaLMPasssword,sambaNTPasssword
    by dn.base="uid=ldaproot,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=ldapreplica,ou=people,dc=subimo,dc=com" write
    by * auth
access to *
    by dn.base="uid=ldaproot,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=ldapreplica,ou=people,dc=subimo,dc=com" write
    by dn.base="uid=ldapnobody,ou=people,dc=subimo,dc=com" read
    by anonymous auth
    by * read
```

Replication Configuration

```
# Master
replica uri=ldaps://prod1.subimo.com:636
bindmethod=simple
binddn="uid=ldapreplica,ou=people,dc=subimo,dc=com"
credentials=*****
replica uri=ldaps://prod2.subimo.com:636
bindmethod=simple
binddn="uid=ldapreplica,ou=people,dc=subimo,dc=com"
credentials=*****
```

LDAP Authorization

- Per machine via pam_ldap hooks
- dc=com,dc=subimo,ou=accessGroups
- authenticate user
- authorization per machine
- can include specific users

Unix Group Usage

- admin – sudo rights on all servers
- devels – limited to development environments – give full sudo rights

sudo

- added sudo.schema extensions
- dc=com,dc=subimo,ou=SUDOers,
cn=<group_name>

NSCD

- caching daemon
- improves performance
- implemented, but not needed in current environment

Hints and Tidbits

- proof of concept on VMware
- custom built RPMs for RedHat
- work around netgroup limitations

Experience

- no restarts except for certificate reloads on client facing servers
- extremely robust – it just runs
- centralized admin has saved many hours of routine administration
- extended LDAP tree to other authentication requirements