Solaris

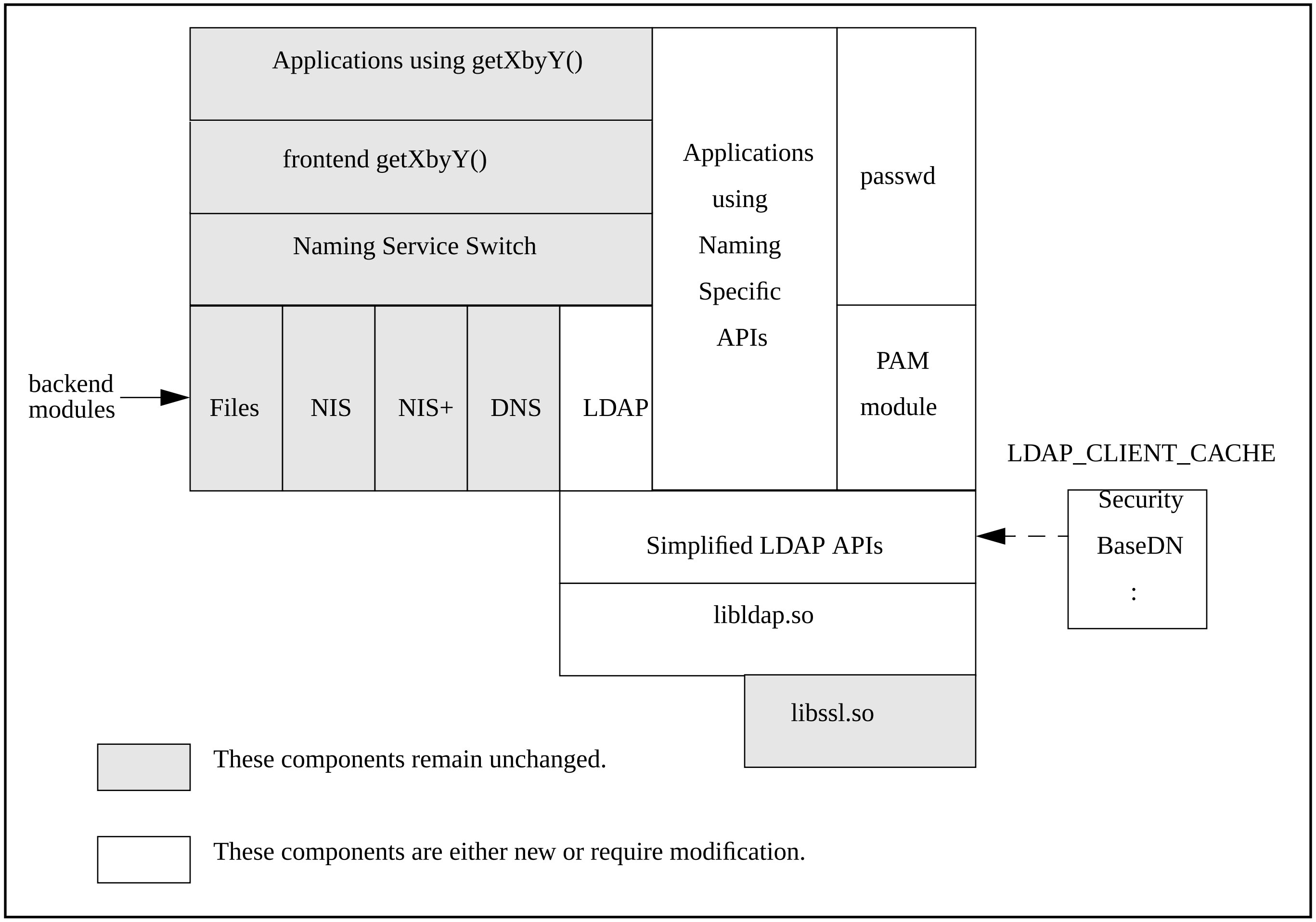
LDAP Naming Service

Roberto Tam

LDAP Naming Service

- Solaris LDAP naming clients
- POSIX Standard getXbyY() API support
- LDAP-aware Solaris Application/Utilities
  (sendmail, automounter, login/passwd, keyserv)
- Compliant with RFC2307
- LDAP v3

Solaris Naming Switch Architecture



Applications using getXbyY()

frontend getXbyY()

Naming Service Switch

backend modules

Files

NIS

NIS+

DNS

LDAP

Applications using Naming Specific APIs

passwd

PAM module

LDAP_CLIENT_CACHE

Security
BaseDN
:

Simplified LDAP APIs

libldap.so

libssl.so

▨ These components remain unchanged.

□ These components are either new or require modification.

Client Setup

- Install or ldapclient
- Client Profiles
- LDAP_CLIENT_CACHE file
- Manual Configuration

ldapclient

Using Client Profile define on the server:

```
ldapclient -P <profile_name> [ -x ] [ -v ] <LDAP_server_addr>
```

Example:

```
ldapclient -P engineering 129.100.100.1
```

ldapclient (cont)

Manual Configuration:

```
ldapclient -i | -m [ -x ] [ -v ]
    [ -a none | simple | cram_md5 ]
    [ -b <baseDN> ] [ -B <alternate-search-dn> ]
    [ -D <Binding_DN> ] [ -w <client_password> ]
    [ -c <certificate_path> ]  [ -r <search_dereference> ]
    [ -t <transport_layer_security> ] [ -E <TTL> ]
    [ -p <server_preference> ] [ -o <timeout-value> ]
     [ -s base | one | sub ] <LDAP_server_addr>+
```

LDAP_CLIENT_CACHE

Domain related info:

```
NS_LDAP_SERVERS=129.100.100.1
NS_LDAP_SEARCH_BASEDN="dc=eng,dc=sun,dc=com"
NS_LDAP_BINDDN="cn=client,dc=eng,dc=sun,dc=com"
NS_LDAP_EXP=#####
```

LDAP_CLIENT_CACHE(cont)

Client related info:

```
NS_LDAP_BINDDN="cn=client,dc=eng,dc=sun,dc=com"
NS_LDAP_BINDPASSWD=xyxyxy
NS_LDAP_AUTH=SIMPLE
NS_LDAP_TRANSPORT_SEC=SSL
NS_LDAP_SEARCH_DEREF_P=NS_LDAP_DEREF_ALWAYS
NS_LDAP_CERT_PATH=/some/file/path
NS_LDAP_SEARCH_DN=(passwd:ou=people,dc=sun,dc=com)
NS_LDAP_CACHE_VERSION=Version1.0
NS_LDAP_SEARCH_SCOPE=NS_LDAP_SCOPE_SUBTREE
NS_LDAP_SEARCH_TIME=30
NS_LDAP_SERVER_PREF=129.100.100,129.100.200.1
NS_LDAP_PREF_ONLY=FALSE
```

Server Setup

Server side:

- Client Profiles
- RFC 2307 Schema
- DIT Layout
- ACLs
- dsimport tool and mapping file
- transition from existing SunDS

Client Profile Schema

```
( oid nnn
  NAME ’clientProfile’
  SUP top
  STRUCTURAL
  DESC ’Native LDAP client profile objectClass’
  MUST cn, LDAPServers, searchBaseDN
  MAY  bindDN, bindPassword, authMethod,
          transportSecurity, searchDereference, certificatePath,
          dataSearchDN, searchScope, searchTimeLimit,
          preferredServer, preferredServerOnly, ExpirationTime
)
```

RFC 2307 Bis Draft

- Extending Luke Howard’s NIS Schema
- Changes:
  - Naming attributes: ipServiceProtocol, ipHostNumber, ipNetworkNumber
  - Object classes: ipNetwork, ipHost
- Additions:
  - Attributes: nisPublikey, nisSecretkey, nisDomain
  - Object class: nisKeyObject, nisDomainObject

DIT Layout

NIS Map	Object Class	Naming Context	getXbyY
passwd	posixAccount shadowAccount	ou=People,dc=..	getpw*() getsp*()
group	posixGroup	ou=Group,dc=..	getgr*()
services	ipService	ou=Services,dc=..	getserv*()
protocols	ipProtocol	ou=Protocols,dc=..	getproto*()
rpc	oncRpc	ou=Rpc,dc=..	getrpc*()
hosts ipnodes	ipHost	ou=Hosts,dc=..	gethost*() getipnode*()
ethers	ieee802Device	ou=Ethers,dc=..	ether_*()
bootparams	bootableDevice	ou=Ethers,dc=..	
networks netmasks	ipNetwork	ou=Networks,dc=..	getnet*()
netgroup	nisNetgroup	ou=Netgroup,dc=..	getnetgr*()
generic	nisObject	nisMapName=..,dc=..	

ACLs

- pam_unix
  - all NIS attributes must be readable by everyone.
- pam_ldap
  - userPassword can be compared by everyone but only writable by owner. No read is allowed.
  - remaining NIS attributes must be readable by everyone.

dsimport Tool

- New Mapping File: files.mapping
- Compound RDNs
  - hosts entries: cn=hostA+ipHostNumber=129.100.100.1
  - services entries: cn=fs+ipserviceprotocol=tcp
- Case Sensitive Automounter RDNs
  - cn=%My%Home,nismapname=auto_home,dc=..

SunDS Transition

- RFC 2307 to RFC2307Bis
- SunDS 1.0 & 3.1 to SunDS 3.2
- Bundling SunDS into Solaris

Open Issues

- RFC2307Bis Draft
- LDAP C-api Draft RFC
- LDAP Authentication Draft RFC
- Hiearchical Namespace
- SLP support
- Connectionless LDAP APIs
- Sendmail Schema