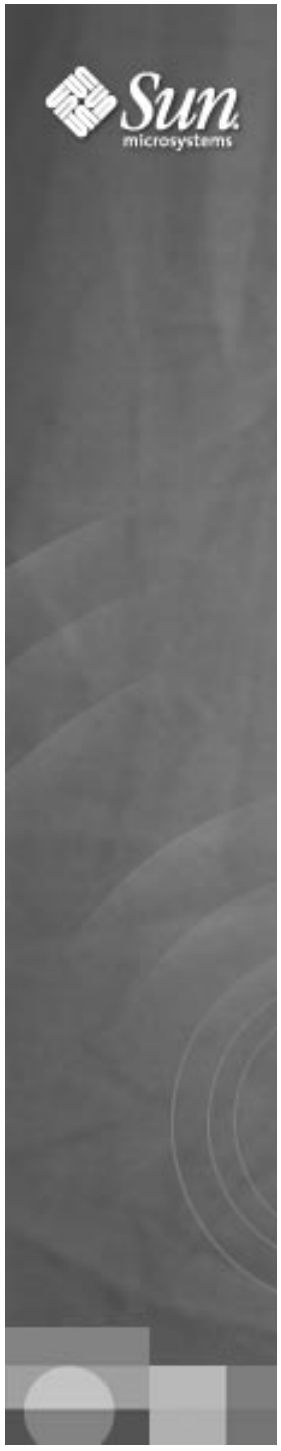
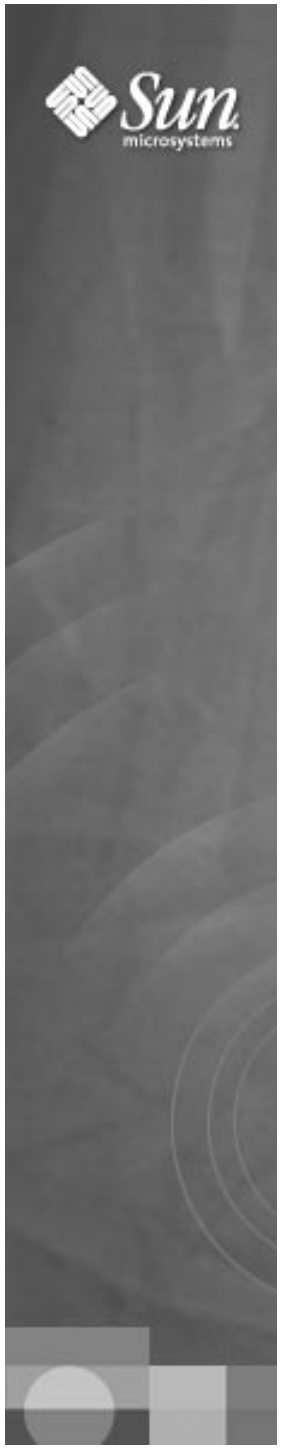


LDAP

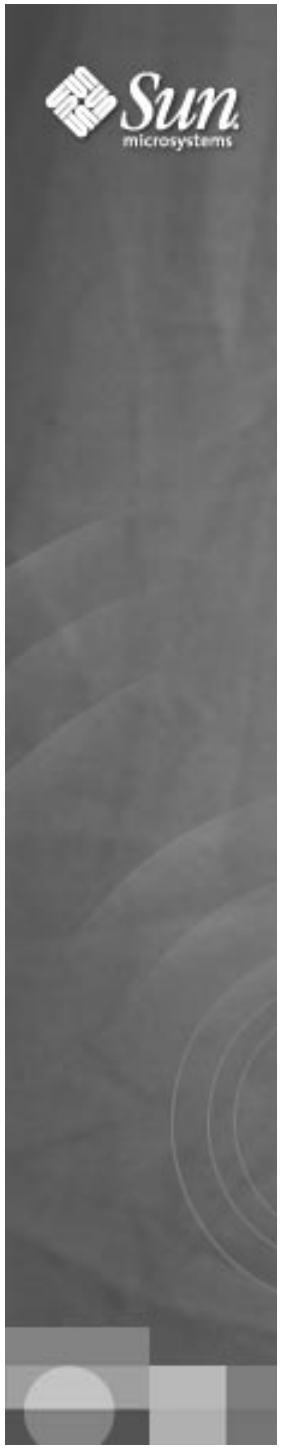
Lightweight Directory Access Protocol

Morteza Ansari
Naming and Directories Group



Overview

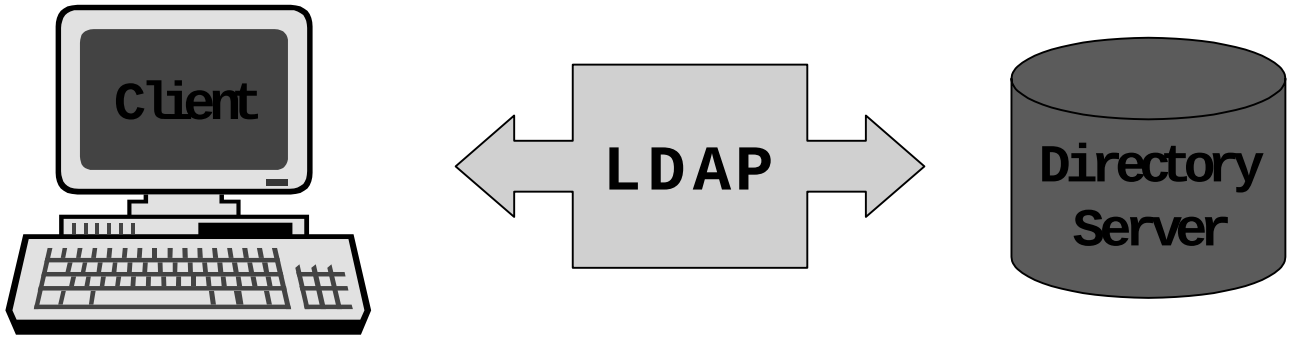
- LDAP?
- LDAP in Solaris
- Q&A



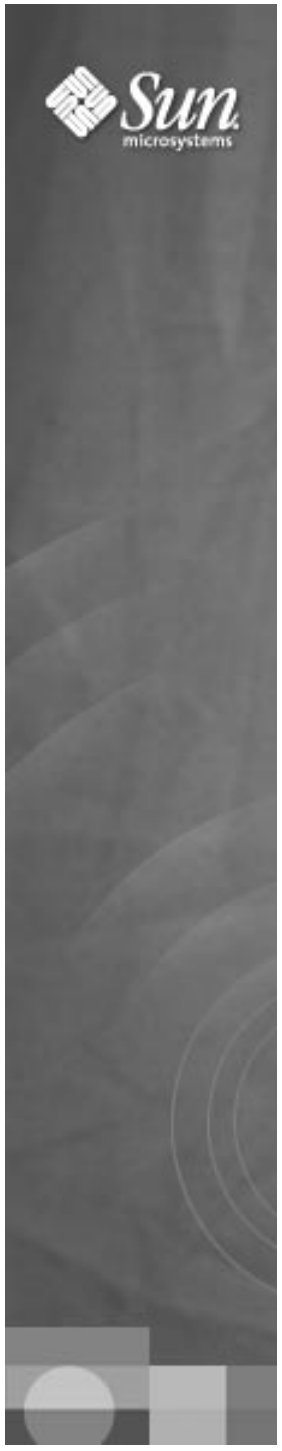
What Is LDAP?

- LDAP
  - History
  - X.500 vs. LDAP
  - Data model
  - Advantages/disadvantages
- Latest from IETF
- Issues

LDAP



Provides a lightweight industry standard protocol to retrieve and manage information stored in a directory

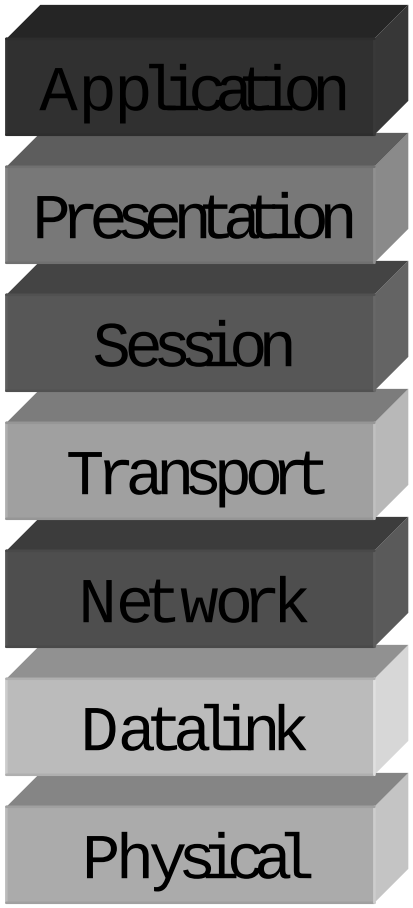


LDAP

- Access Protocol
- Extensible Add, Delete, Modify, and Search operations
- Key features:
  - Lightweight
  - Open standard
  - Runs over TCP/IP
  - Hierarchical directory structure

LDAP History

- University of Michigan
- X.500 roots
- LDAPv1
- LDAPv2
- LDAPv3

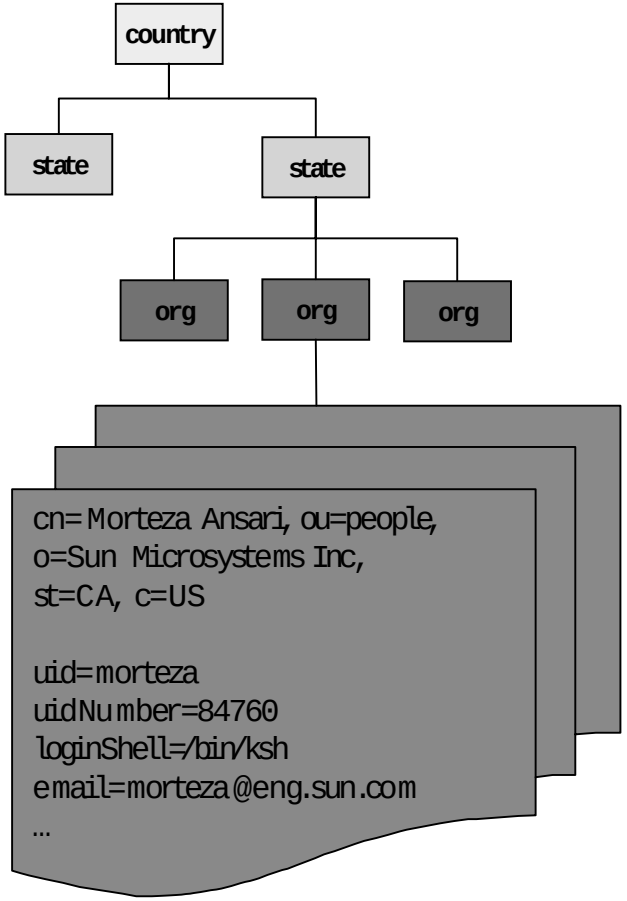


X.500 vs. LDAP

	X.500	LDAPv1	LDAPv2	LDAPv3
Client to Server	OSI	TCP/IP	TCP/IP	TCP/IP
Server to Server	OSI	X.500 OSI	None	TCP/IP (replication only)*
Security	Password Strong	Password	Password	Password Strong*
Not found action	Servers chain requests	Servers chain requests	Dumb referrals	Referrals
Schema	Fixed	Fixed	Fixed	Dynamic

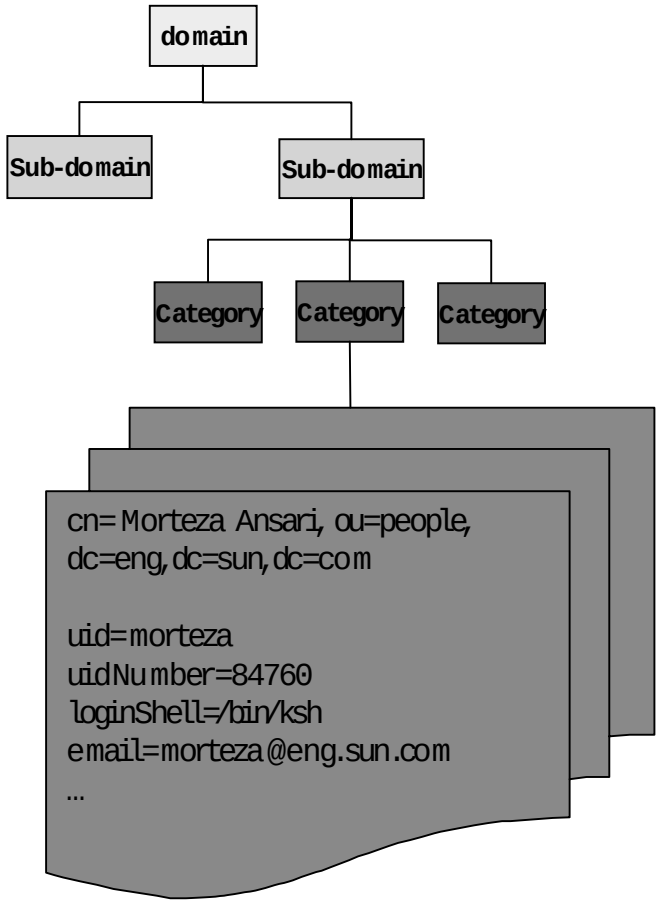
Hierarchical Directory Structure

- Similar directory information structure as X.500
- Entries are distinguished by an unique name (DN), that identifies the entry within DIT



Hierarchical Directory Structure

- Similar directory information structure as X.500
- Entries are distinguished by an unique name (DN), that identifies the entry within DIT



Advantages of LDAP

- Open standard
- Available on virtually all operating systems
- Database and vendor independent
- Relatively simple to LDAP-enable applications

Disadvantages of LDAP

- Slowly becoming a "Heavyweight" protocol!
- No official entity for registering Schemas
- Access control & replication is vendor specific
- Clients tend to get more and more complex

Latest from IETF

- LDAP Authentication is approved

  draft-ietf-ldapext-authmeth-04.txt
  draft-ietf-ldapext-ldapv3-tls-06.txt
  draft-leach-digest-sasl-05.txt

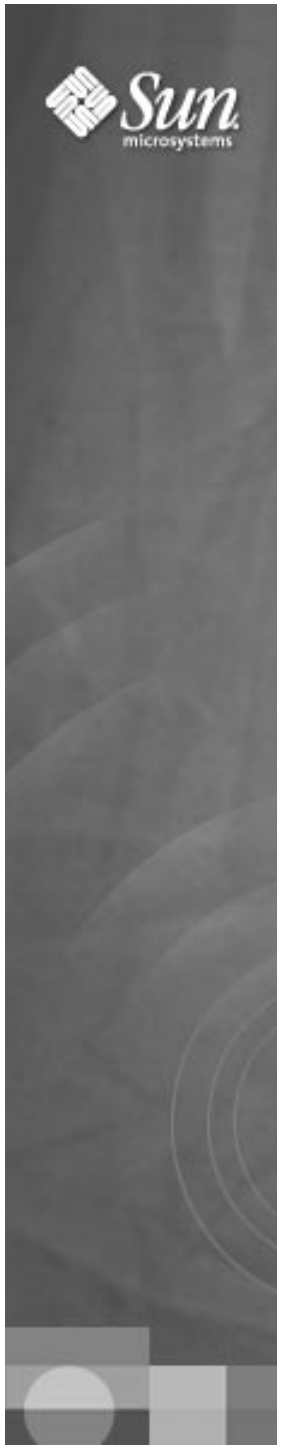
- C-API is close to RFC status
- Access control is expected to reach RFC status later this year
- Replication work is coming along, but is still long ways off

Other Industry Efforts

- Directory Interoperability Forum
  - Sun/AOL alliance, IBM, ISOCOR, Lotus, Novell, and Oracle
  - Promote a common set of APIs and SDKs
  - Accelerate acceptance of standards
  - Provide interoperability, conformance, and certification of directories (through Open Group)
  - Still missing Microsoft

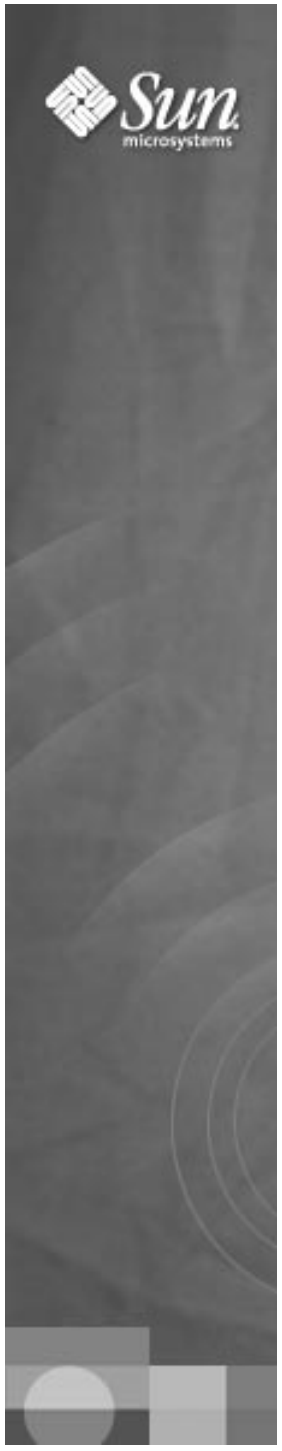
Other Industry Efforts

- Directory Services Markup Language (DSML) Alliance
  - Bowstreet, IBM, Lotus, Microsoft, Novell, Oracle, and Sun/Netscape
  - Use XML to describe directory content and structure



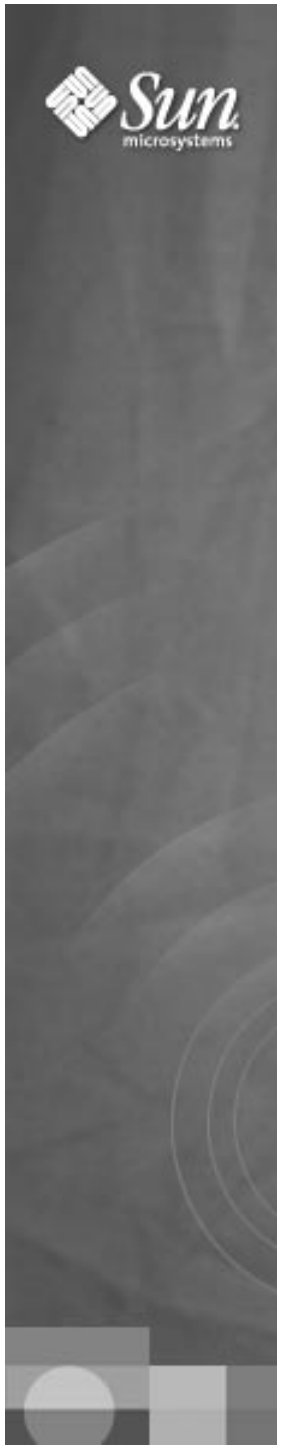
Overview

- What is LDAP
- LDAP in Solaris
- Q & A



LDAP in Solaris

- LDAP library (C-API)
- LDAP Naming Service
- PAM LDAP module
- Others



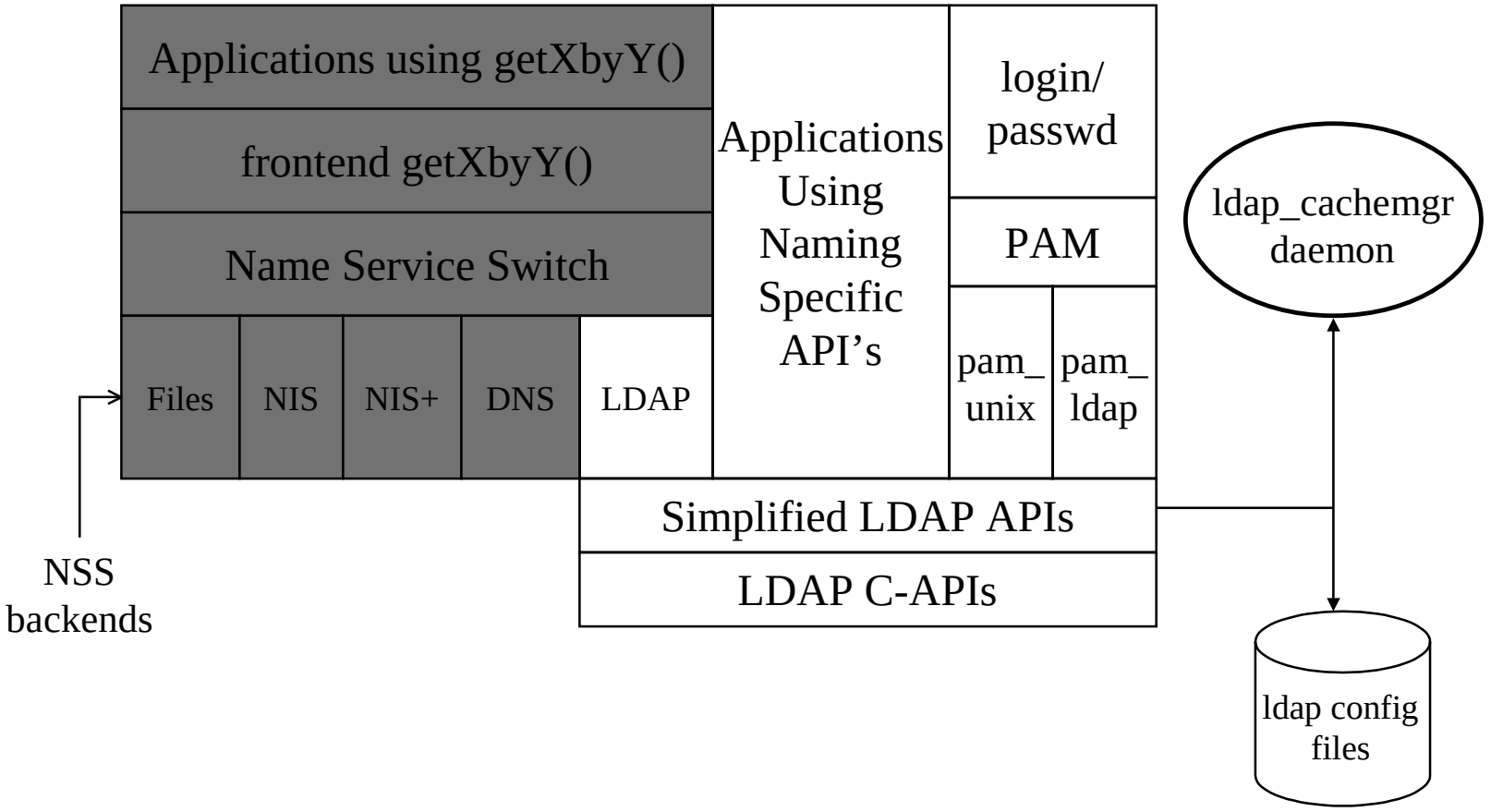
LDAP C-API

- Based on University of Michigan source
- draft-ietf-ldapext-ldap-c-api-04.txt
- Minimal security
  - SIMPLE
  - CRAM-MD5

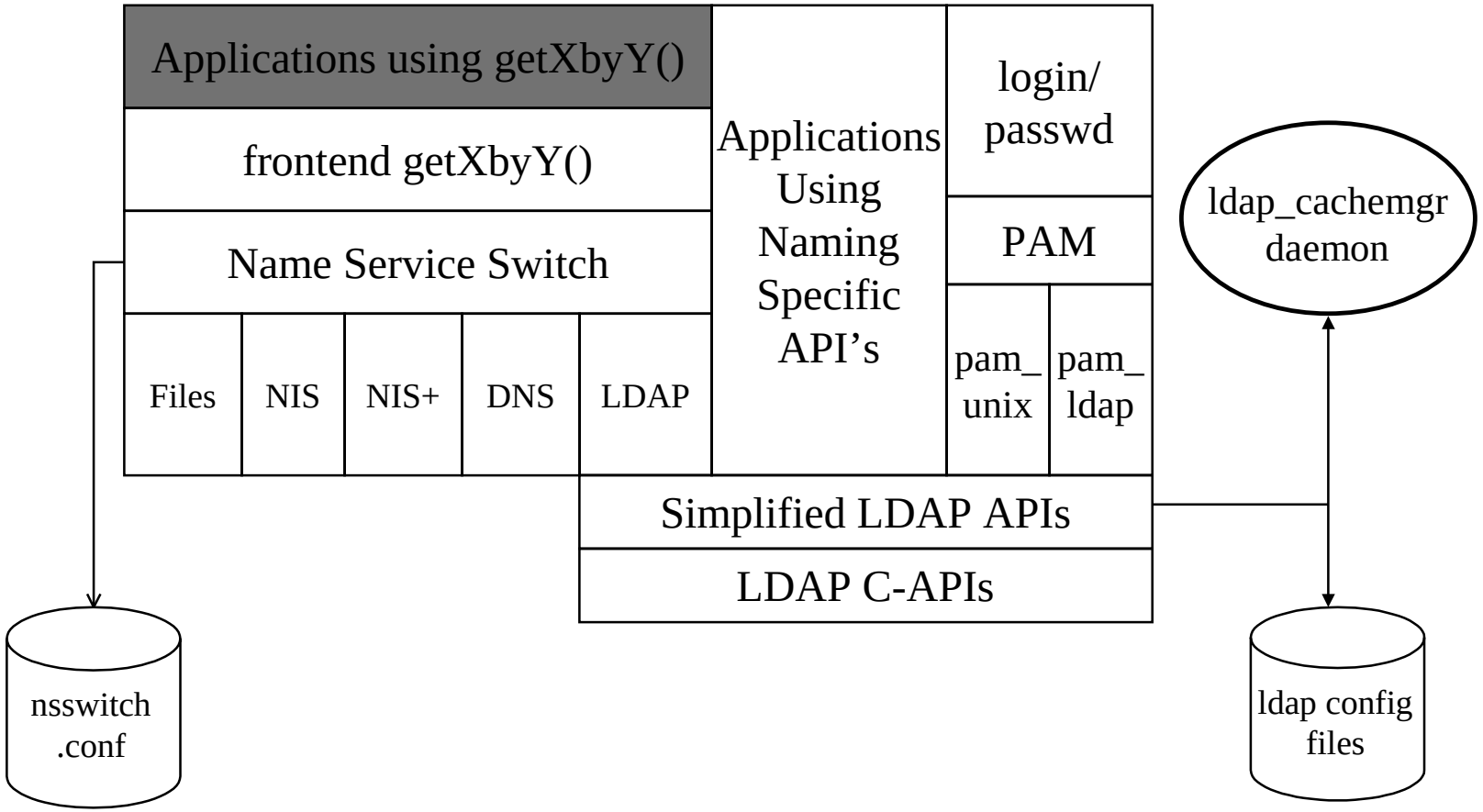
LDAP Naming Service

- Use LDAP as the directory for storing Network Information Services
- Reduce redundant data
- Simplify administration
- Data sharing among apps & OS's
- Common authentication

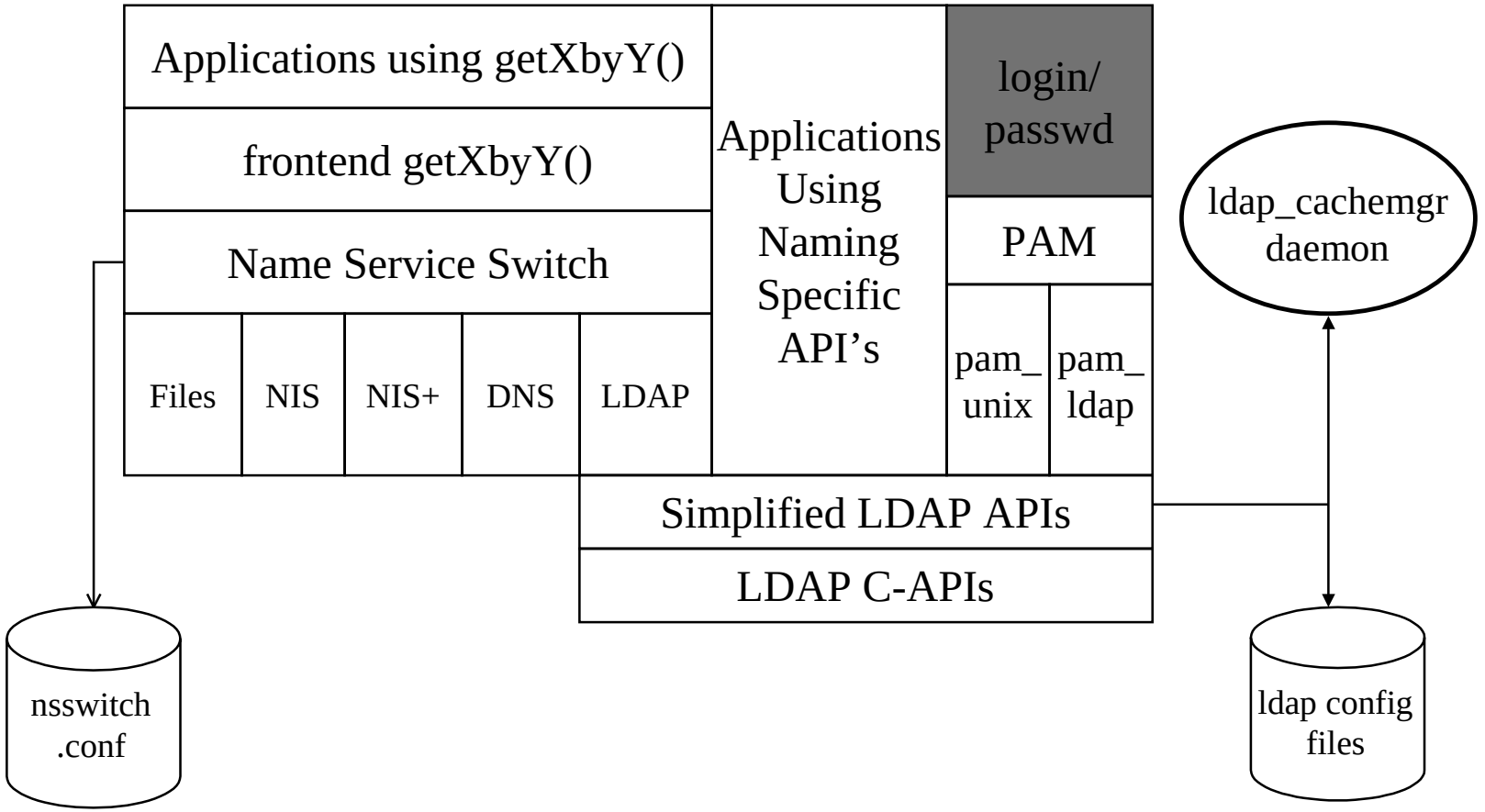
LDAP Naming Service



LDAP Naming Service



PAM LDAP


Applications using getXbyY()
frontend getXbyY()
Name Service Switch
Files
NIS
NIS+
DNS
LDAP
Applications Using Naming Specific API's
login/ passwd
PAM
pam_ unix
pam_ ldap
ldap_cachemgr daemon
Simplified LDAP APIs
LDAP C-APIs
nsswitch .conf
ldap config files

PAM LDAP

- Schema
  - rfc2307 (rfc 2307bis draft)
  - Automount tables in nisMap/nisObject OC
  - SolarisNamingProfile
- Client configurations (profiles) are stored in LDAP and are cached locally

DIT Layout

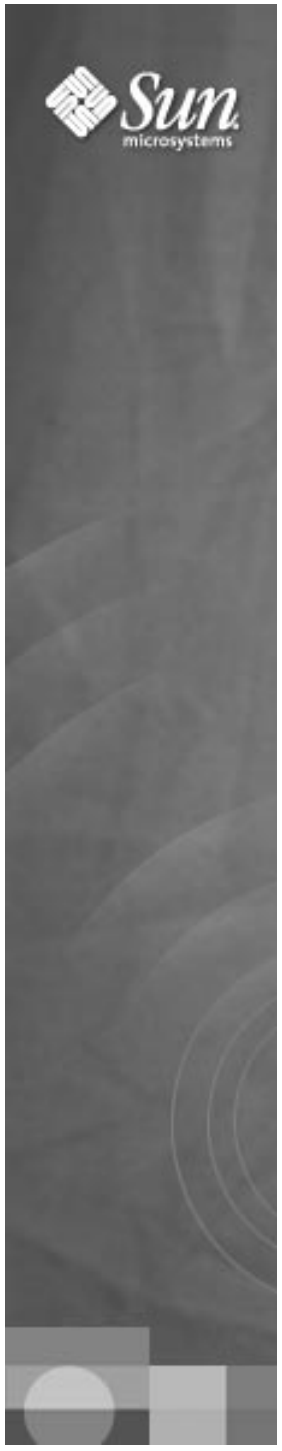
NIS map	object class	naming context	getXbyY()
passwd	posixAccount shadowAccount	ou=people, ...	getpw*() getsp*()
group	posixGroup	ou=group, ...	getgr*()
services	ipService	ou=services, ...	getserv*()
protocols	ipProtocol	ou=protocols, ...	getproto*()
rpc	oncRpc	ou=rpc, ...	getrpc*()
hosts ipnodes	ipHost	ou=hosts, ...	gethost*() getipnode*()
ethers	ieee802Device	ou=ethers, ...	ether_*()
bootparams	bootableDevice	ou=ethers, ...	
networks netmasks	ipNetwork	ou=networks, ...	getetgr*()
netgroup	nisNetwork	ou=netgroup, ...	getetgr*()
generic	nisObject	nisMapName=*,...	

New Commands

- ldap_gen_profile
- ldapclient
- ldaplist
- ldap_cachemgr

References

- http://www.directoryforum.org
- http://www.dsml.org
- http://www.umich.edu/~dirsvcs/ldap
- IETF:
  - LDAP Extension working group
    http://www.ietf.org/html.charters/ldapext-charter.html
  - LDAP Duplication/Replication/Update WG
    http://www.ietf.org/html.charters/ldup-charter.html



References

- Programming Directory-Enabled Applications with LDAP

  By: Tim Howes, Mark Smith

- Understanding and Deploying LDAP Directory Services

  By: Time Howes, Mark Smith, & Gordon Good