



NAME SERVICES IN OPENSOLARIS

Slava Leanovich
Individual Contributor
Sun Microsystems Inc.



NAME SERVICES IN OPENSOLAIRS

Feedback: Viachaslau.Leanovich@Sun.COM

- 1. What Name Services Are**
- 2. LDAP and the Directory**
- 3. Native LDAP Support in Solaris OS**
- 4. Recent Improvements**
- 5. Upcoming Projects**
- 6. Putting All Things Together**
- 7. References**

What Name Services Are ?

- **Databases**

- > passwd
- > hosts
- > ...

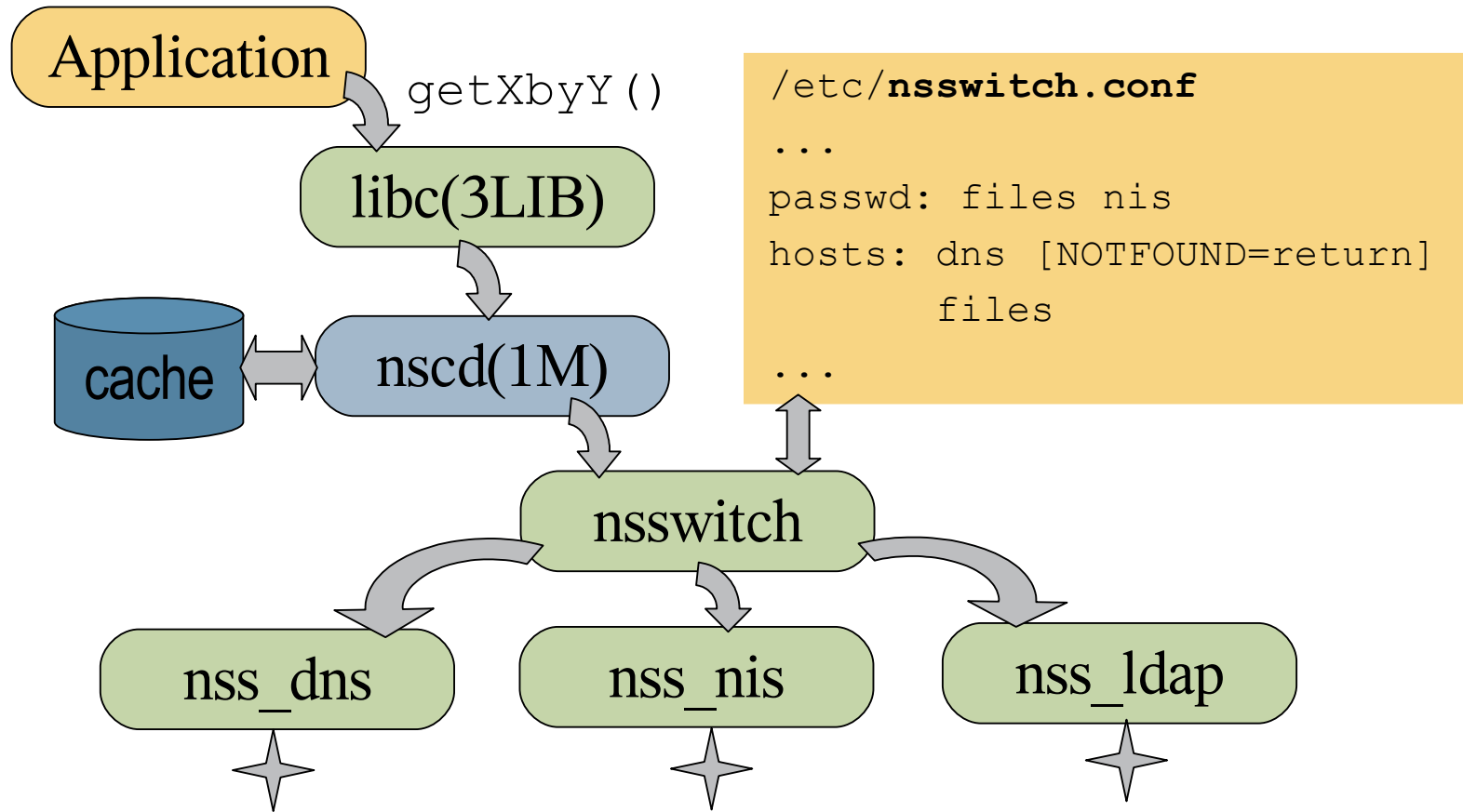
- **Backends**

- > DNS
- > NIS / NIS+
- > LDAP
- > ...

- **Get X by Y**

- > getpwnam()
- > getpwent()
- > getgrnam()
- > gethostbyname()
- > getaddrinfo()
- > getnetbyname()
- > getservbyname()
- > ...

Get X by Y Process



Useful Commands

- DNS

- > nslookup(1M)
- > dig(1M)
- > host(1M)

getent(1M)

- NIS

- > ypinit(1M)
- > ypcat(1)
- > ypmatch(1)

- NIS+

- > nisclient(1M)
- > niscat(1)
- > nisgrep(1)

- LDAP

- > ldapclient(1M)
- > ldaplist(1)
- > ldapsearch(1)

Naming Backends Summary

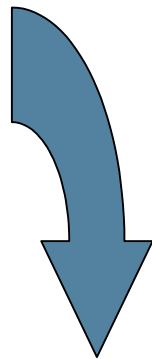
Category	DNS	NIS	NIS+	LDAP
Namespace	Hierarchical	Flat	Hierarchical	Hierarchical
Data Storage	Files	2-column maps	Multi-column tables	Directory (indexed)
Server Names	Master / Slave	Master / Slave	Master / Replica	Master / Replica
Security	None	None	Authentication (Secure RPC)	TLS / SASL (Kerberos)
Transport	TCP/IP	RPC	RPC	TCP/IP
Scale	Global	LAN	LAN	Global

What is LDAP

- RFC **4511** LDAPv3
- RFC **4512** LDAP: Models
- RFC **4513** LDAP: Authentication Methods
- RFC **4514** LDAP: Distinguished Names
- RFC **4515** LDAP: Search Filters
- RFC **4516** LDAP: Uniform Resource Locator
- RFC **4517** LDAP: Syntaxes and Matching Rules
- RFC **4518** LDAP: Internationalized Strings
- RFC **4520** IANA: Considerations for LDAP
- RFC **4522** LDAP: The Binary Encoding Option
- RFC **4523** LDAP X.509 Schema
- RFC **4524** COSINE LDAP/X.500 Schema
- RFC **4525** LDAP Modify-Increment Extension
- RFC **4526** LDAP Absolute True and False Filters
- RFC **4527** LDAP Read Entry Controls
- RFC **4528** LDAP Assertion Control
- RFC **4530** LDAP Entry UUID
- RFC **4531** LDAP Turn Operation
- RFC **4532** LDAP "Who am I?" Operation
- RFC **4533** LDAP Content Synchronization Operation

What is LDAP

X.500 OSI Directory Access Protocol



Simplify

Optimize (fast read queries)

Secure

Lightweight Directory Access Protocol

Directory Information Tree

dn: **ou=people**,
dc=sun,dc=com

dn: **ou=hosts**,
dc=sun,dc=com

dn: **dc=sun,dc=com**
objectClass: nisDomainObject
objectClass: domain
objectClass: top
dc: sun
nisDomain: sun.com

dn: **uid=test_user**,ou=people,
dc=sun,dc=com
objectClass: shadowAccount
objectClass: posixAccount
uid: test_user
uidNumber: 201
userPassword: {crypt}wqpIrejx8/QKQ

• • •

Directory Schema

- Object identifiers (OID)
- Object classes (Structural, Auxiliary)
- Attributes (Mandatory, Optional)
- Matching Rules

```
$ ldapsearch -b "cn=schema" -s base ""  
  
attributeTypes: ( 2.5.4.35 NAME 'userPassword' DESC 'Standard  
LDAP attribute type' EQUALITY octetStringMatch )  
  
objectClasses: ( 2.5.6.6 NAME 'person' DESC 'Standard LDAP  
objectclass' SUP top )  
  
matchingRules: ( 2.5.13.5 NAME 'caseExactMatch' DESC 'Case Exact  
Matching on Directory String [defined in X.520]' )
```

Directory Schema

```
objectClasses: ( 2.5.6.6
```

```
  NAME 'person'
```

```
  DESC 'Standard object'
```

```
  SUP top STRUCTURAL
```

```
  MUST ( sn $ cn )
```

```
  MAY ( description $
```

```
    seeAlso $
```

```
    telephoneNumber $
```

```
    userPassword )
```

```
  X-ORIGIN 'RFC 2256'
```

```
)
```

```
Syntax: (
```

```
  1.3.6.1.4.1.1466.115.121.1.40
```

```
  DESC 'Octet String'
```

```
)
```

```
attributeTypes: ( 2.5.4.35
```

```
  NAME 'userPassword'
```

```
  DESC 'Standard attr type'
```

```
  EQUALITY octetStringMatch
```

```
  ● SYNTAX 1.3.6.1.4.1...
```

```
  X-ORIGIN 'RFC 2256'
```

```
)
```

```
matchingRules: ( 2.5.13.17
```

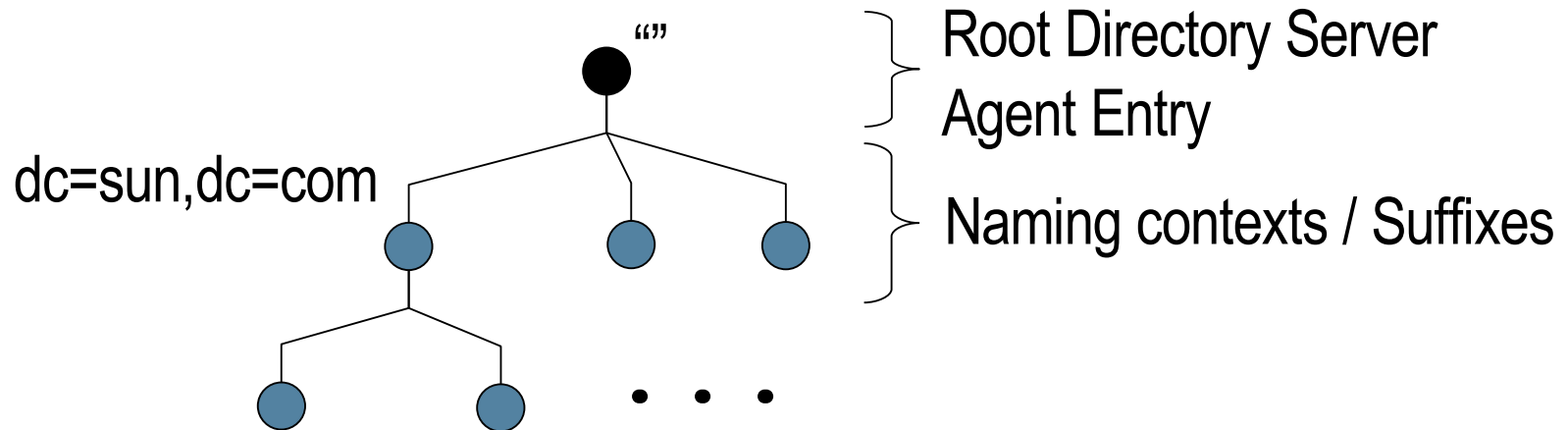
```
  NAME 'octetStringMatch'
```

```
  SYNTAX 1.3.6.1.4.1...
```

```
)
```

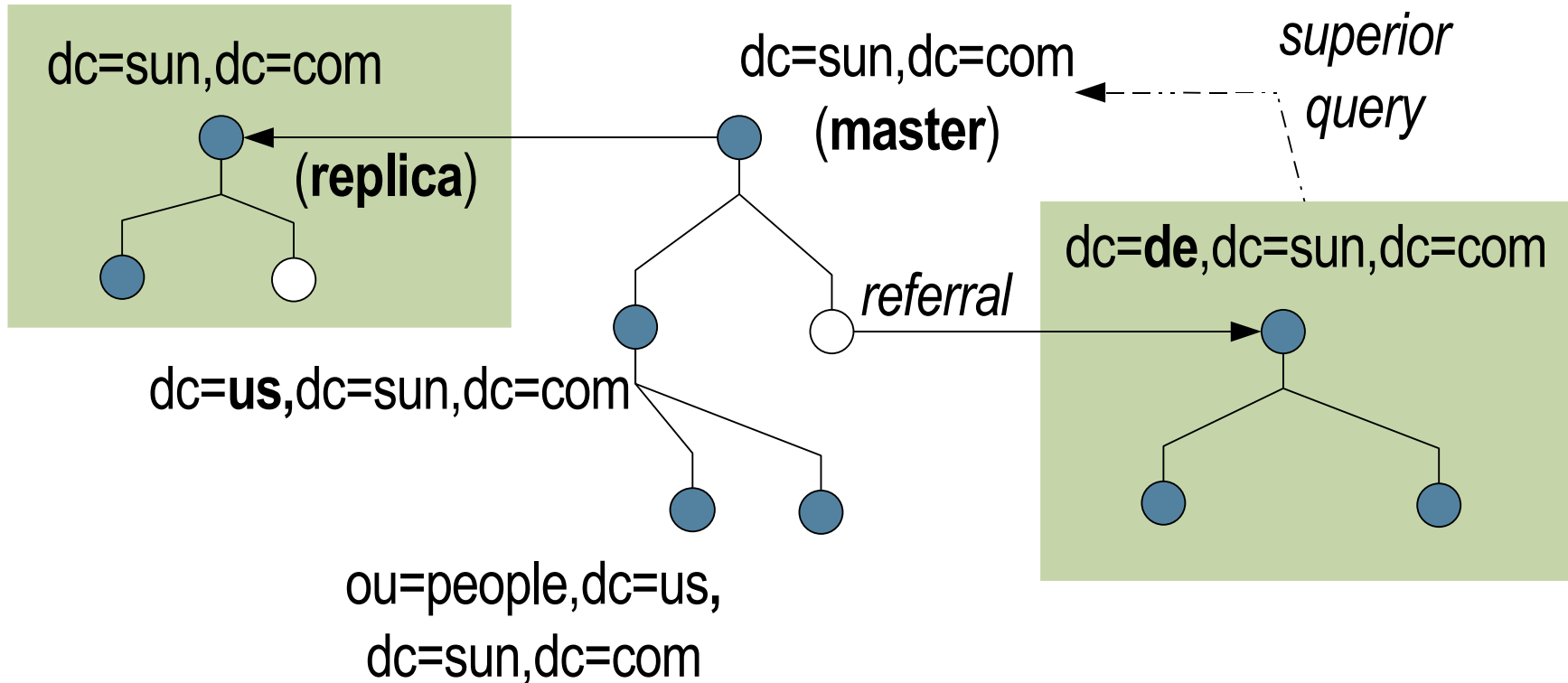


Root Entry

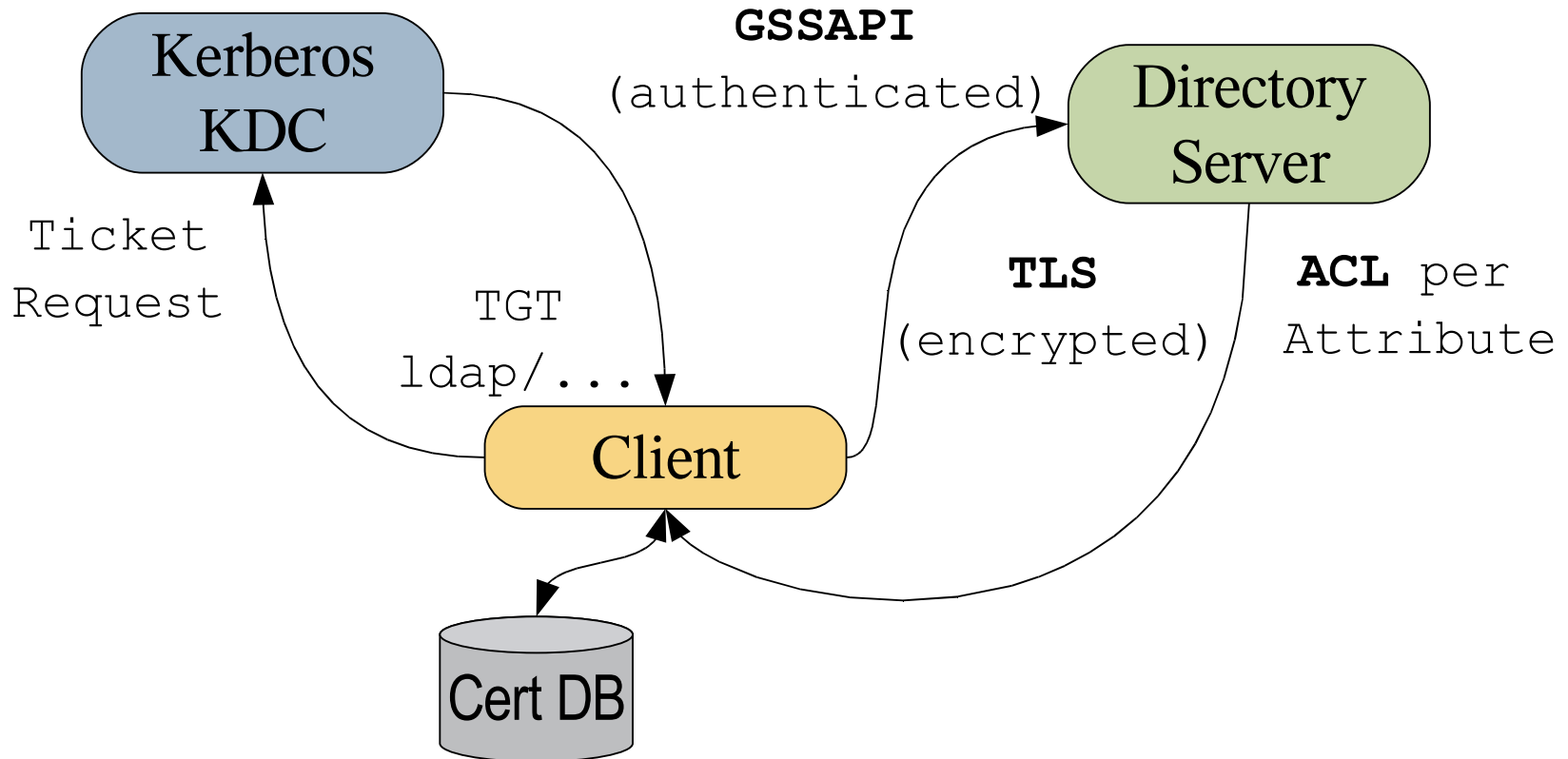


```
$ ldapsearch -b "" -s base ""  
namingContexts: dc=sun,dc=com  
vendorName: Sun Microsystems, Inc.  
supportedExtension: 2.16.840.1.113730.3.5.7  
supportedExtension: 2.16.840.1.113730.3.5.8  
supportedExtension: 1.3.6.1.4.1.4203.1.11.1
```

Distributed Infrastructure



Security



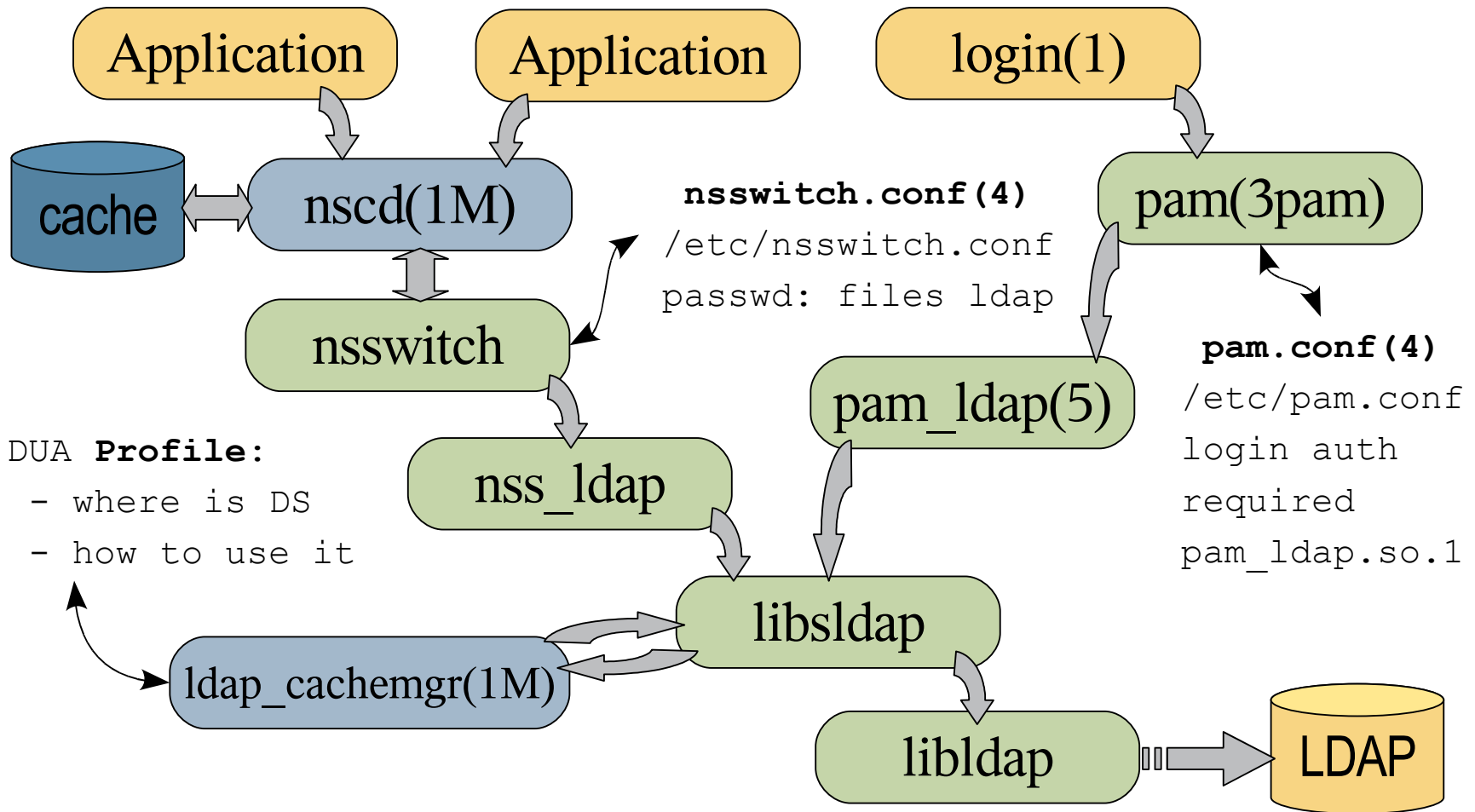
Advantages Summary

- Share naming data with applications
- Good scalability / availability
- Granular security
- Multi platform / vendor

LDAP support in Solaris OS

- Native LDAP Client – `ldap(1)`
- RFC 2307 An Approach for Using LDAP as a Network Information Service
- DUA Profile
 - > <http://www.ietf.org/internet-drafts/draft-joslin-config-schema-17.txt>
- Configuration Cache Manager
- Repository setup – `idsconfig(1M)`

LDAP support in Solaris OS

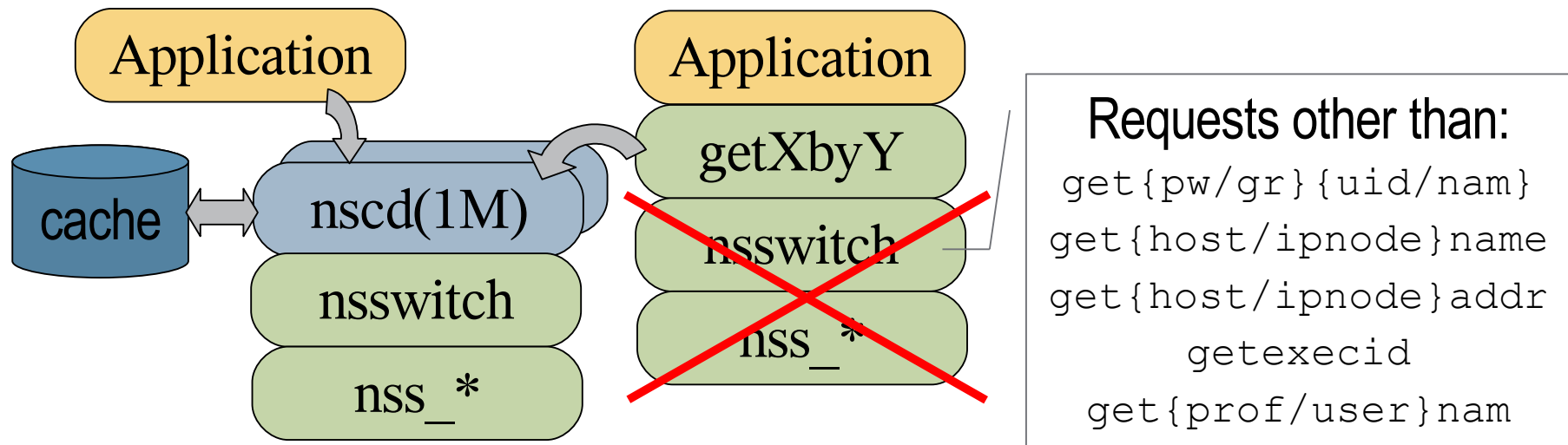


DUA Profile:
 - where is DS
 - how to use it

DUA Profile

```
dn: cn=default,ou=profile,dc=sun,dc=com
cn: default
objectClass: DUAConfigProfile
defaultServerList: 10.18.138.43
defaultSearchBase: dc=sun,dc=com
followReferrals: FALSE
defaultSearchScope: one
searchTimeLimit: 30
bindTimeLimit: 10
profileTTL: 43200
credentialLevel: self
authenticationMethod: tls:sasl/GSSAPI
```

Recent Improvements



- MT scalability
- Self-credentialed lookup
- Per-user cache daemon
- Put X by Y framework
- No more reboots
- SMF integration

Sparks Project

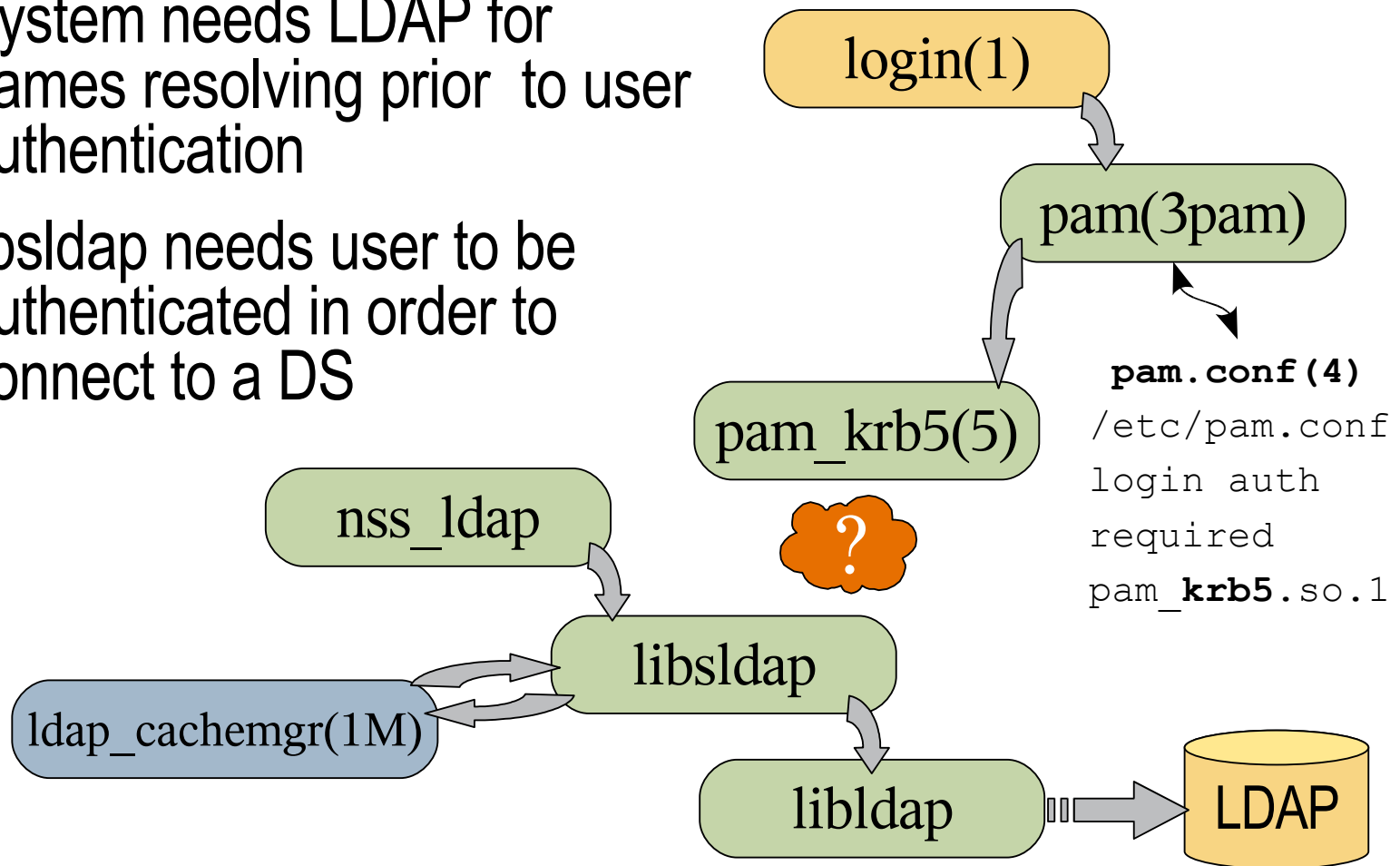
- **Approachability**
- **Interoperability**

<http://opensolaris.org/os/project/sparks>

- MT scalability
- Self-credentialed lookup
- Per-user cache daemon
- Put X by Y framework
- No more reboots
- SMF integration

Kerberized Login — the other piece of puzzle

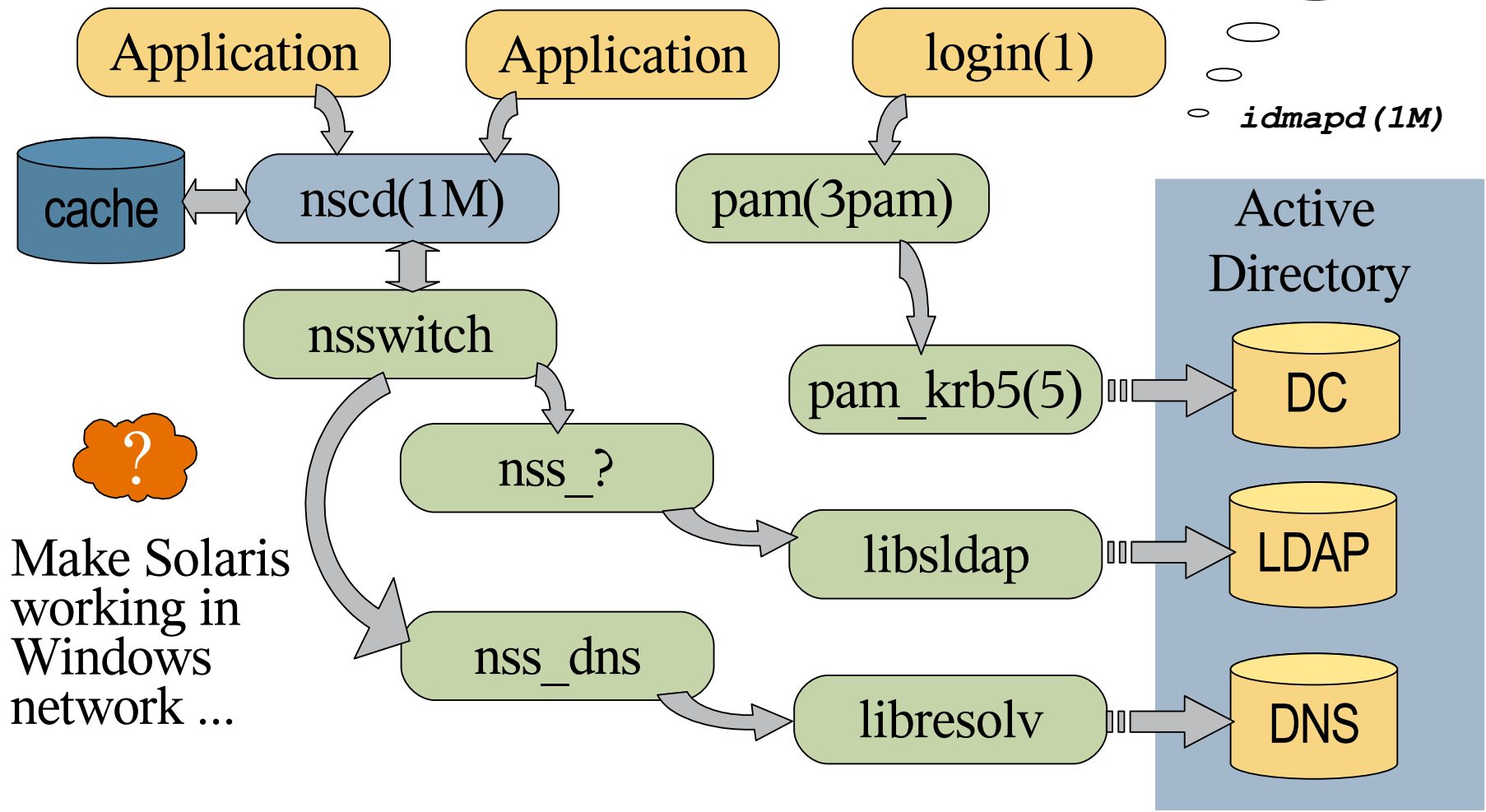
- System needs LDAP for names resolving prior to user authentication
- libldap needs user to be authenticated in order to connect to a DS



Interoperability ?

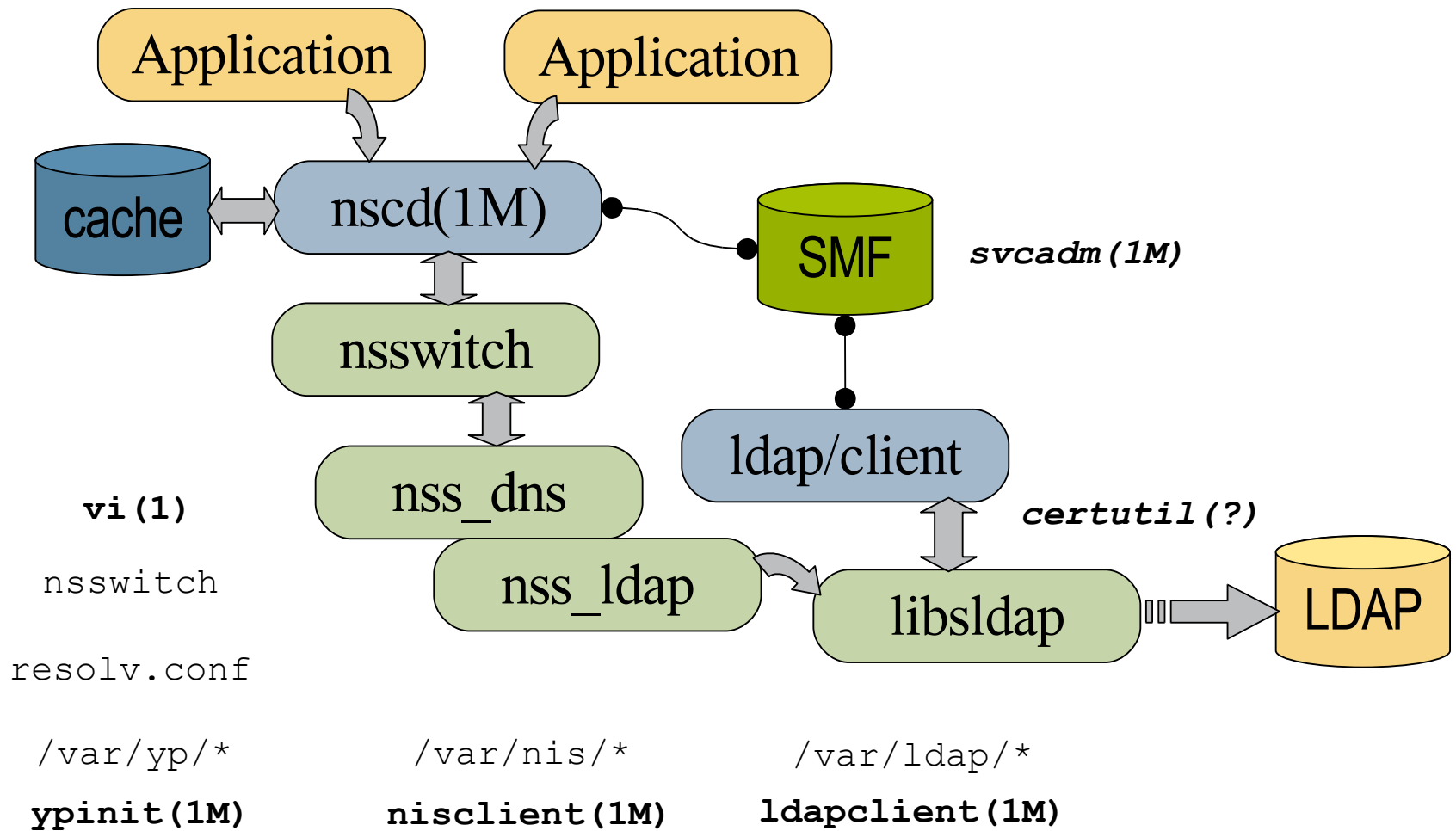
UID - SID

idmapd(1M)

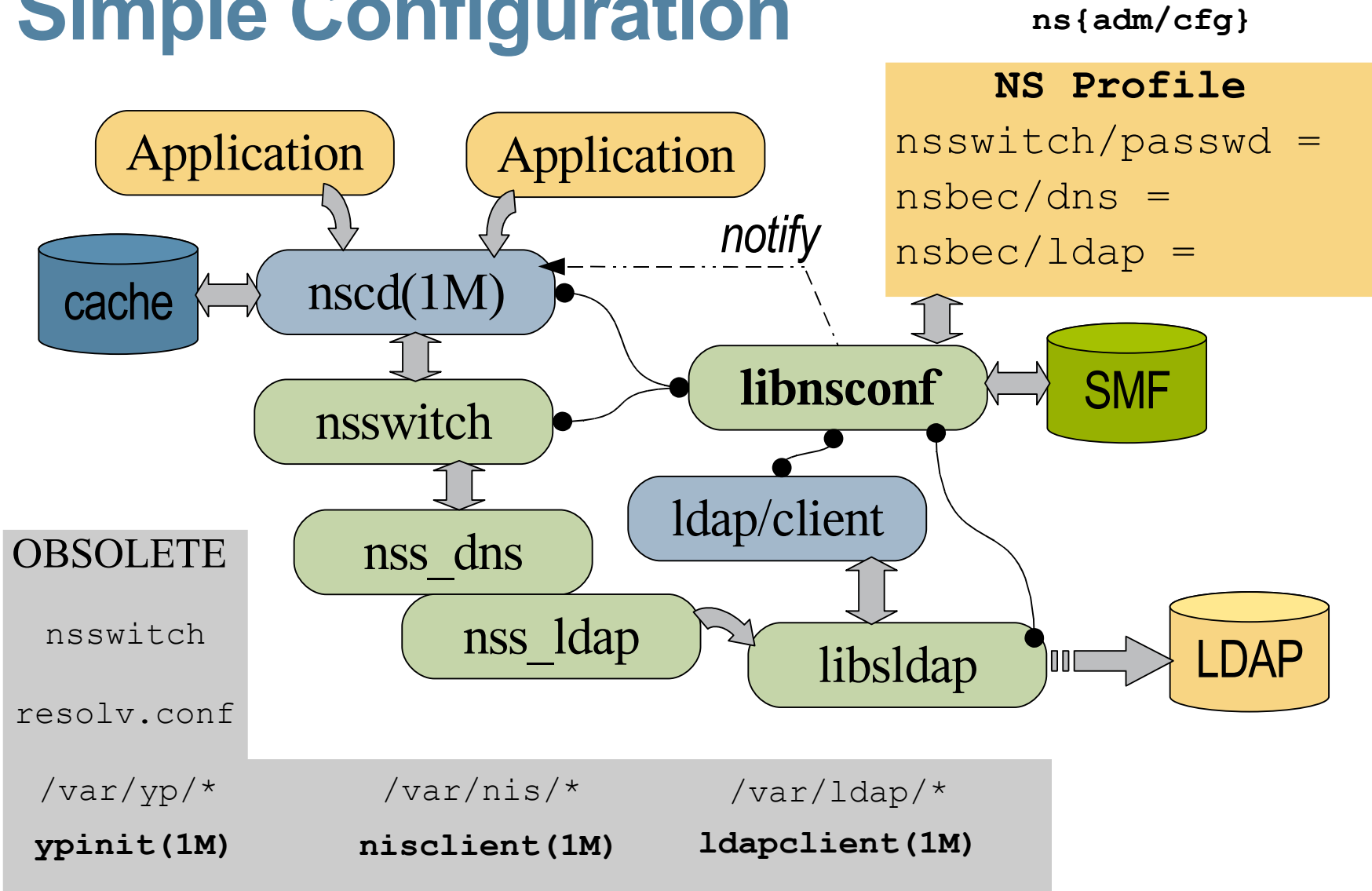


Make Solaris working in Windows network ...

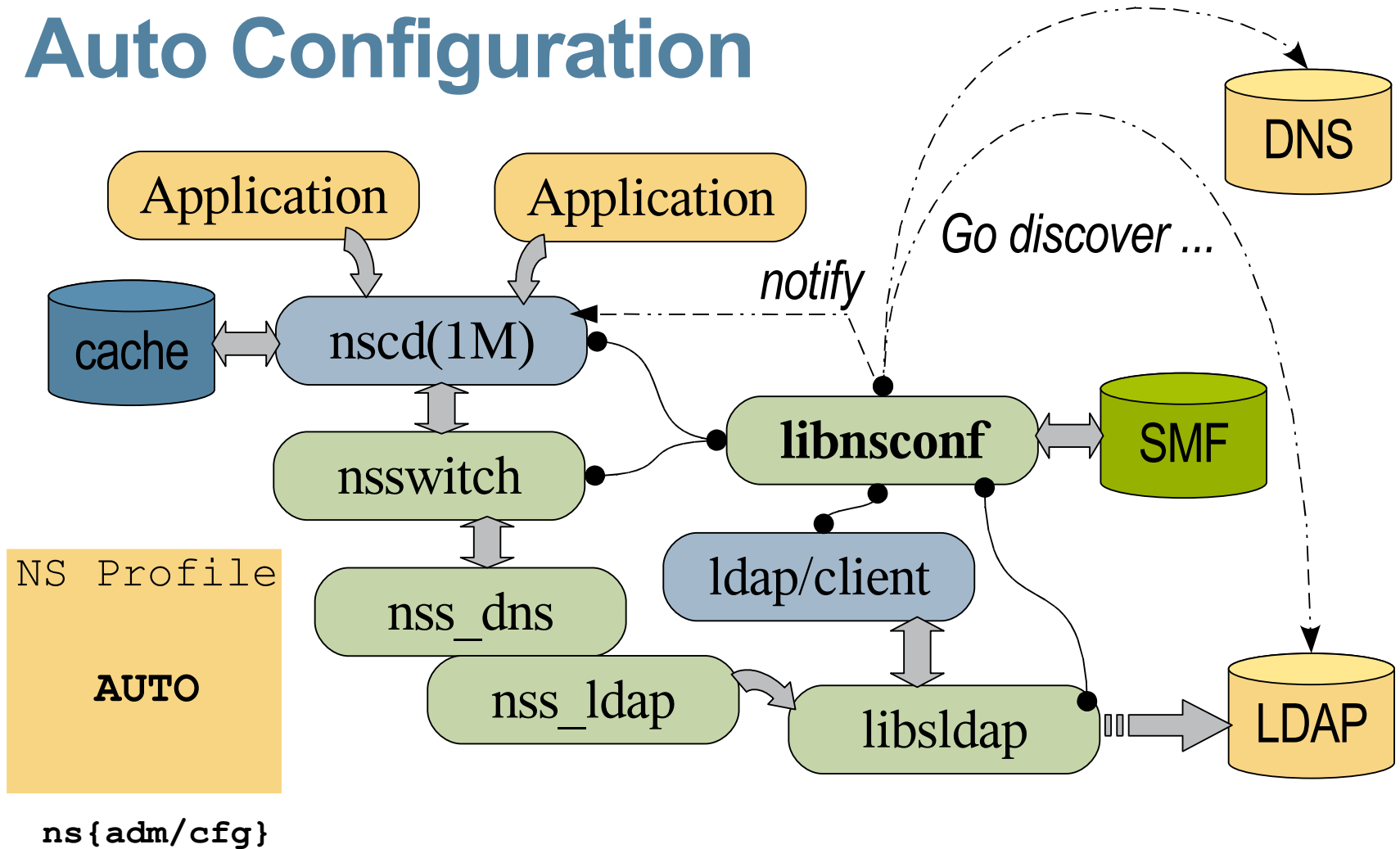
What About Configuration ?



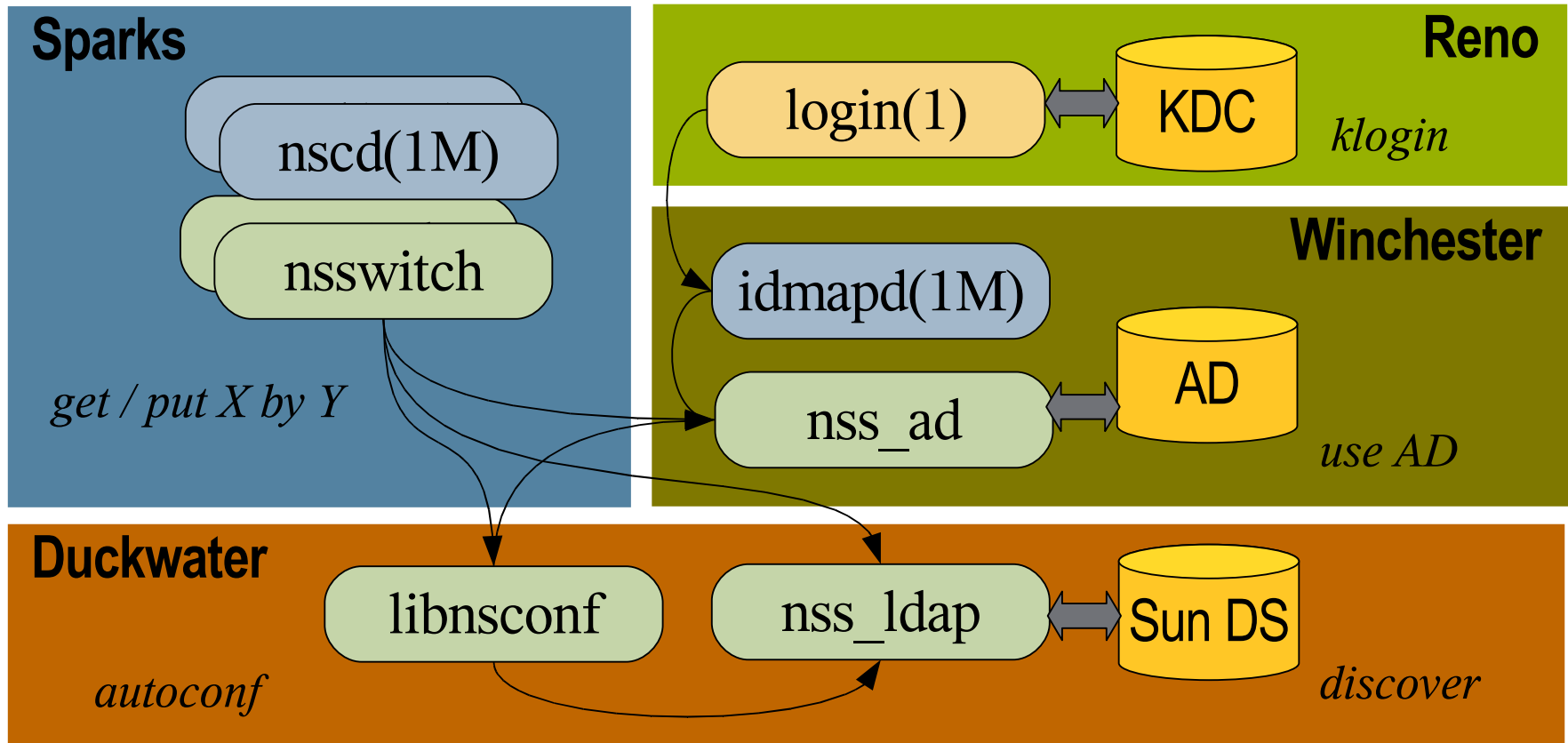
Simple Configuration



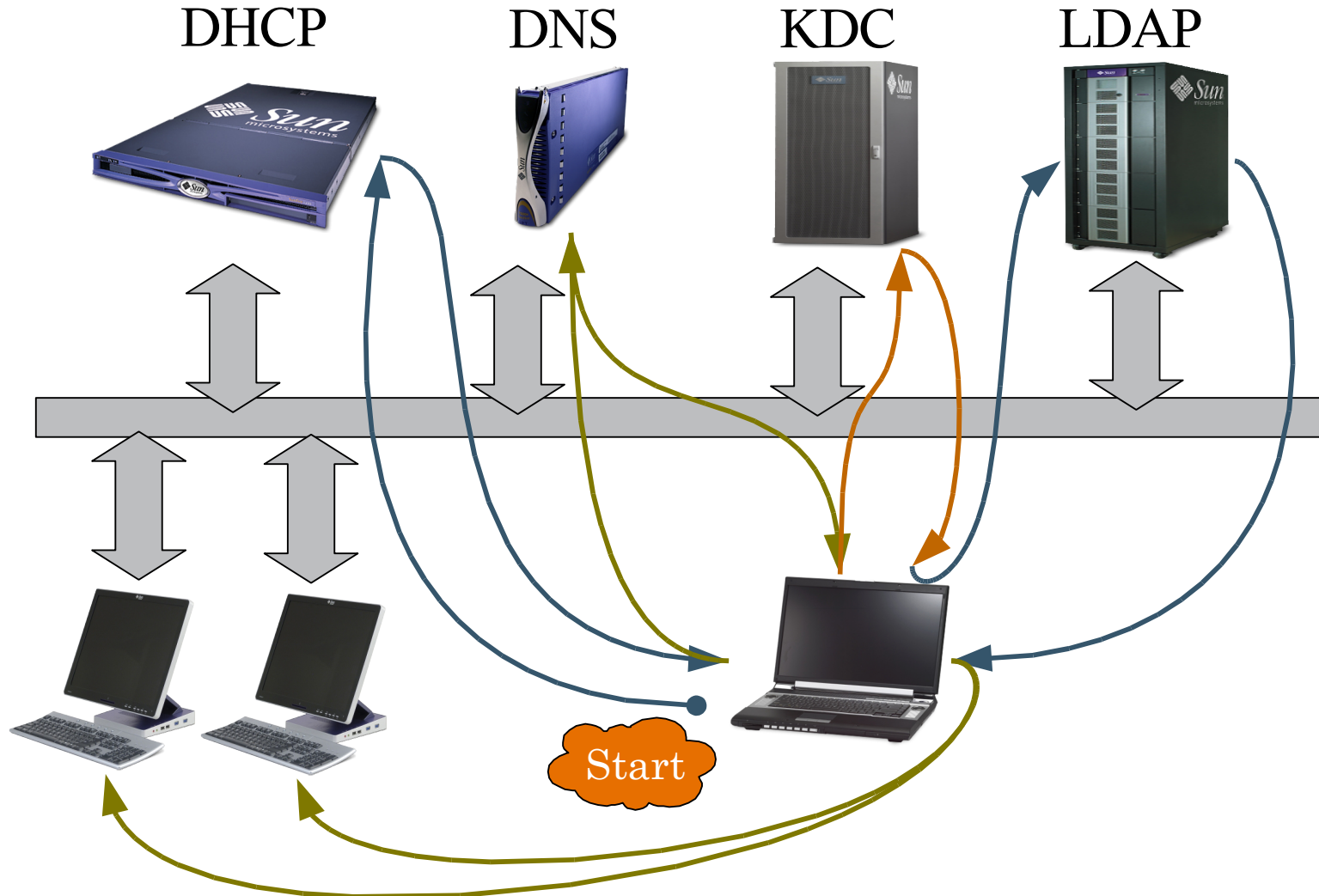
Auto Configuration



The Big Picture



Putting All Things Together ...



References

- <http://opensolaris.org/os/project/sparks>
- <http://opensolaris.org/os/project/reno>
- <http://opensolaris.org/os/project/winchester>
- <http://opensolaris.org/os/project/duckwater>
- www.ietf.org
- System Administration Guide: Naming and Directory Services (DNS, NIS and LDAP)
<http://docs.sun.com/app/docs/doc/816-4556>
- Sun Java(TM) System Directory Server 5.2 2005Q1 Administration Guide
<http://docs.sun.com/source/817-7613/index.html>

Q & A