

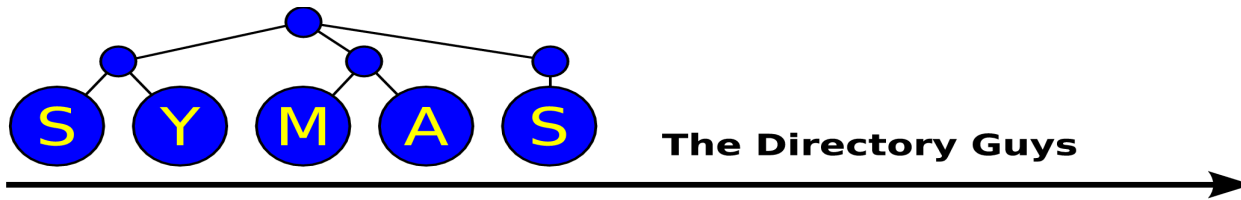
The Directory Guys

Unified Authentication Service in OpenLDAP

Howard Chu

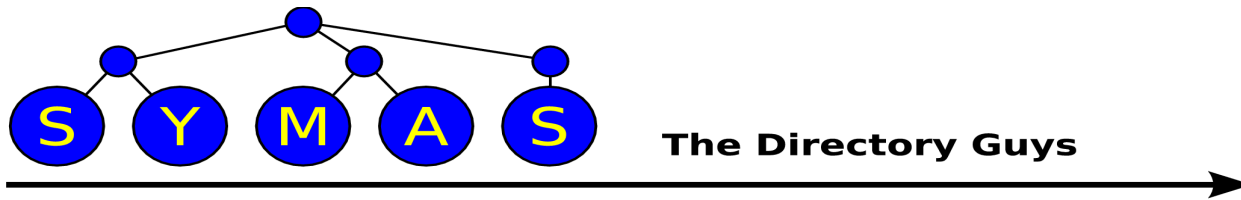
CTO, Symas Corp. hyc@symas.com

Chief Architect, OpenLDAP hyc@openldap.org



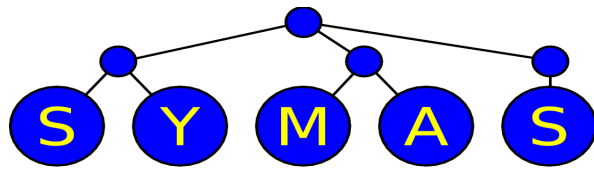
OpenLDAP Project

- Open source code project
- Founded 1998
- Three core team members
- A dozen or so contributors
- Feature releases every 12-18 months
- Maintenance releases roughly monthly



A Word About Symas

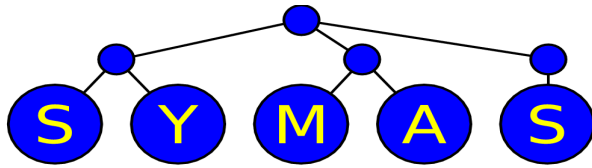
- Founded 1999
- Founders from Enterprise Software world
 - *platinum* Technology (Locus Computing)
 - IBM
- Howard joined OpenLDAP in 1999
 - One of the Core Team members
 - Appointed Chief Architect January 2007



The Directory Guys

Topics

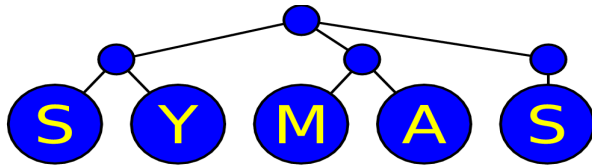
- Overview
- POSIX and LDAP
- Problems with the Existing Options
- Steps to Solutions
- Future Directions



The Directory Guys

Overview

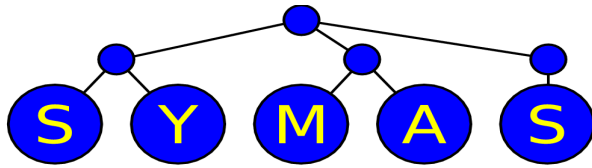
- LDAP directories have long been used for authentication in computing systems.
- Proprietary solutions have been very tightly integrated with their respective OS platforms.
- Despite having roots in the same technologies upon which these proprietary services are built, the Linux / Open Source world hasn't had directory services tightly integrated into their OS infrastructure.



The Directory Guys

Overview

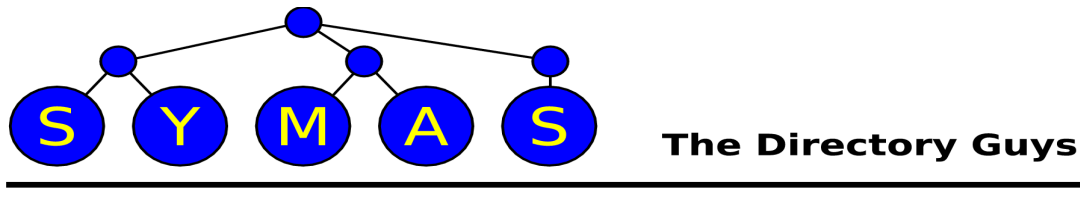
- The existing solutions for Linux are pretty bad.
 - deployment and administration are basically no better than ad hoc; you must munge individual files on every machine to effect configuration changes across a network.
- The move towards cluster, cloud, and other large-scale system designs makes the need for scalable distributed OS security management even more urgent.
- It's not hard to do better. Recent work in the OpenLDAP Project addresses these issues and more.



The Directory Guys

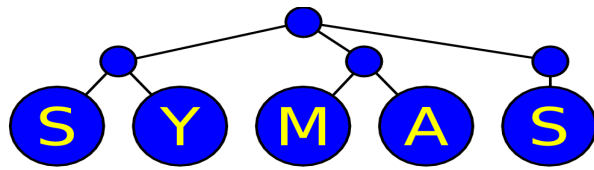
POSIX and LDAP

- RFC2307, March 1998, Luke Howard
 - Basically defined an LDAP schema for presenting Sun NIS map information
 - NIS maps were used for a variety of common POSIX system tables, including users, groups, IP services, ports, protocols, hosts, and networks, etc.
 - Implemented in `nss_ldap` module, using the Name Service Switch, integral to a platform's C library
 - Could be used for authentication, if the LDAP entry's `userPassword` was stored using a POSIX-compatible `{crypt}` hash
 - Current version RFC2307bis-02 being edited by Howard Chu



POSIX and LDAP...

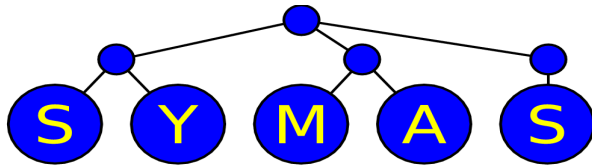
- nss_ldap was nice, but has some problems when used on its own
 - Standard POSIX utilities couldn't be used to update table data stored in LDAP
 - Requirement for {crypt} password hashes is too restrictive, and providing client access to hashes is a security risk



The Directory Guys

POSIX and LDAP...

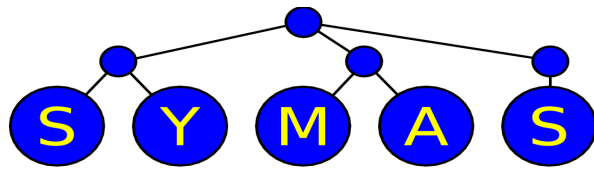
- Enter pam_ldap, Pluggable Authentication Mechanism
 - Can delegate authentication to the LDAP server, thus lifting the constraints on the storage mechanisms used for credentials
 - Can handle password modification, using the PasswordModify exop



The Directory Guys

Problems with pam_ldap/nss_ldap

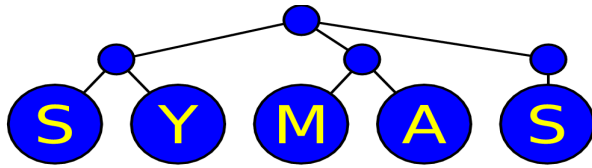
- Config file issues
 - All configuration comes from an ldap.conf file that must reside on every client machine - minor changes in directory layout / schema / whatever require major effort to propagate / synchronize on each dependent machine
 - The config file is confusingly named and documented
 - The file must be world-readable. Even if no secrets are present, intimate details of the server configuration are exposed, encouraging their misuse by application developers



The Directory Guys

Problems with pam_ldap/nss_ldap

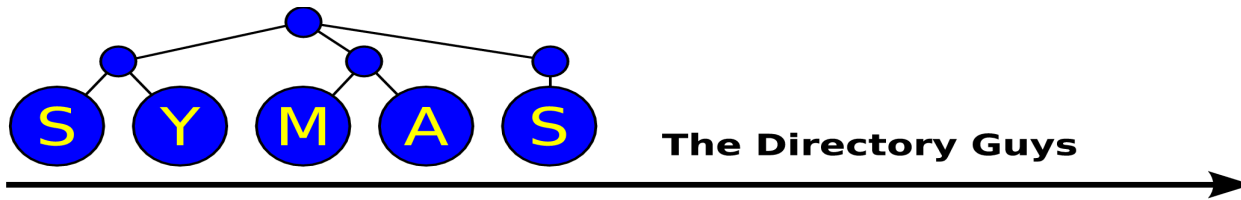
- Runtime issues
 - Both are implemented as shared libraries linked directly to libldap, thus polluting the namespace of essentially every process on the system
 - Library version dependency nightmare
 - threaded vs non-threaded library issues
 - Library initialization / deinit issues



The Directory Guys

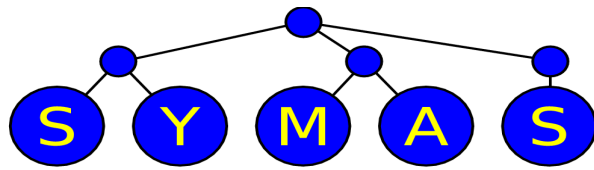
Problems with pam_ldap/nss_ldap

- Operational issues
 - Requires live access to an LDAP server - provides no fallback in case of network or server outages
 - Additional modules can be used to provide caching of tables and credentials, but those mechanisms are also known to be flawed
 - Provides limited, inflexible mechanisms for login authorization control



Obvious Solutions

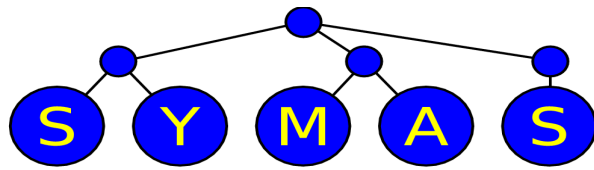
- Insert a stub between the pam/nss API and the actual LDAP client code
 - The LDAP client runs as a separate process
 - The pam/nss code communicates to the client via a Unix Domain socket
 - Isolates all processes from the actual LDAP API
 - Hides all LDAP configuration in a file private to the client process
 - First implemented in nss-ldapd by Arthur de Jong, October 2006



The Directory Guys

Obvious Solutions

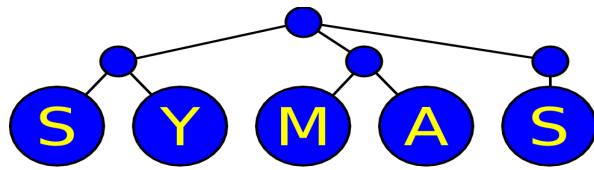
- nss-ldapd brings a major improvement to system stability, but still has shortcomings
 - still no fallback solution for network / server outages
 - doesn't address PAM
 - LDAP client is fairly sparse in features
 - Only supports Linux



The Directory Guys

nssov Overlay

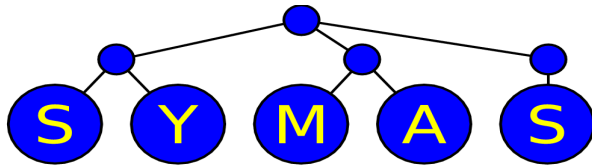
- Uses the same stub library as nss-ldapd
 - brings the listener directly into slapd
 - immediately brings benefits of improved manageability
 - provides total immunity to network / server outages using either replication or proxying with local caching
- First released in OpenLDAP 2.4.11, July 2008



The Directory Guys

nssov Overlay

- Current version also implements PAM as of 2.4.17, July 2009
 - PAM support has also been contributed back to nss-ldapd
- Provides fine-grained login authorization control using the slapd ACL engine
 - Authorization checked using an LDAP Compare operation



The Directory Guys

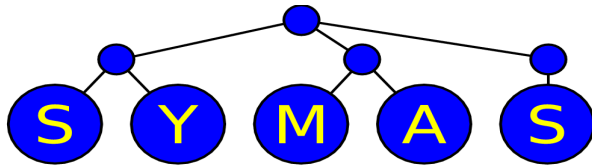
PAM Authorization

- Example host entry

```
dn: cn=hostX,ou=hosts,dc=example,dc=com
objectClass: ipHost
objectClass: authorizedServiceObject
cn: hostX
ipHostNumber: 192.168.1.127
authorizedService: sshd
authorizedService: ftp
```

- Sample Access Control rule

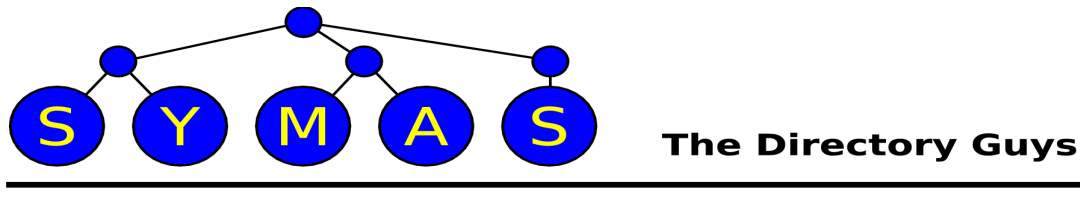
```
access to dn.subtree=ou=hosts,dc=example,dc=com
  attrs=authorizedService val.exact=sshd
  by group.exact="cn=admins,ou=groups,dc=example,dc=com" write
  by peername.ip=198.207.56.0%255.255.255.0 read
  by * none
```



The Directory Guys

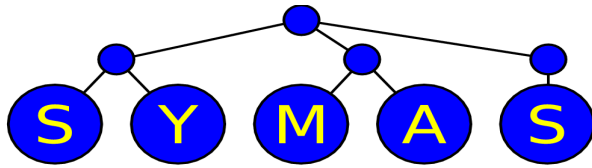
ProxyCache Enhancements

- "Offline" mode - suspends cache expiration while the remote server is unreachable
- Time To Refresh - cached entries that have been referenced and aren't expired are automatically re-fetched after a certain age
- Bind caching - credentials used in a Simple Bind are hashed and stored for satisfying subsequent Bind requests
- Cached credentials have a separately configured Refresh period



ProxyCache + nssov

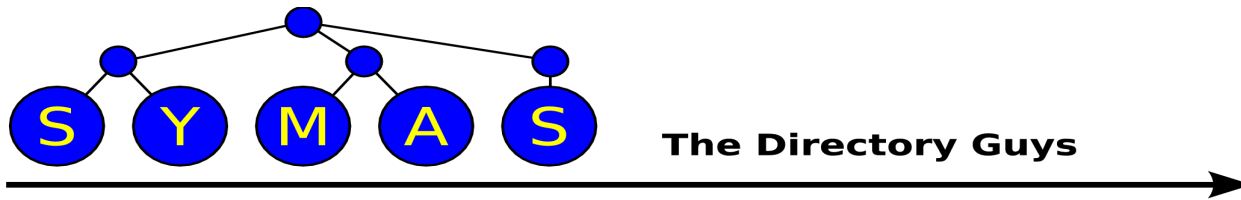
- Seamless authentication + authorization
- Configuration managed centrally, only a stub is exposed
 - actual configuration can be distributed via syncrepl, for painless automatic maintenance
- Multiple options for availability / disconnected operation, using syncrepl or proxy + cache
- Natural integration with LDAP Password Policy



The Directory Guys

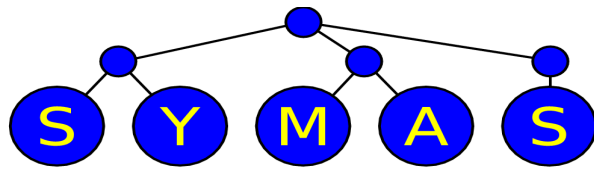
Password Policy

- Spec was intended to enable other applications to leverage the policy in LDAP
- No other applications have managed to do so yet
- Current draft version 10 being edited by Howard Chu and Ludovic Poitou
- Various additions and clarifications, with changes explicitly aimed at supporting policy usage in Kerberos and SASL



Kerberos

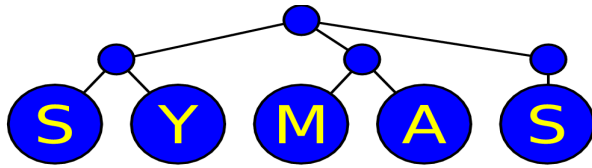
- KDC Information Model draft published by the IETF Kerberos Working Group
- KDC LDAP Schema draft being written by Howard Chu
 - Unified schema for both MIT and Heimdal KDCs
 - Replaces MIT password policy elements with LDAP password policy schema



The Directory Guys

Certificate Authority

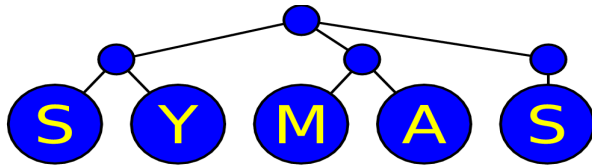
- Simplified, automated certificate generation
 - Automatically issued to the currently bound user's DN and stored in their entry - no need for certificate request objects
 - Certs can be generated with short lifetimes for single-use or short-time usage - analogous to Kerberos tickets
 - Implemented in an overlay, triggered by a search request on the user's entry and userCertificate attribute with magic filter parameters



The Directory Guys

Certificate Authority

```
ldapsearch -x -H ldap://my-server -ZZ  
-D cn=someone,dc=example,dc=com  
-w goodpassword  
-b cn=someone,dc=example,dc=com  
-s base  
((&(startDate=200909212245Z)  
  (endDate=200909212300Z))  
  userCertificate userKey
```



The Directory Guys

Certificate Authority

```
ldapsearch -x -H ldap://my-server -ZZ
```

```
-D cn=manager,dc=example,dc=com
```

```
-w secretpassword
```

```
-e authzid=cn=hostX,ou=hosts,dc=example,dc=com
```

```
-b cn=hostX,ou=hosts,dc=example,dc=com
```

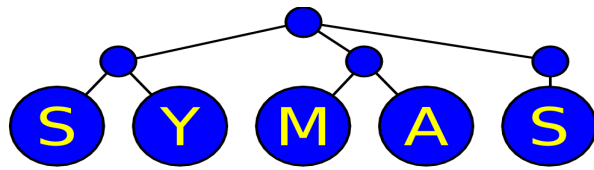
```
-s base
```

```
(&(startDate=200909211800Z)
```

```
(endDate=201109211800Z)
```

```
(subjectAltName=DNS:bighost))
```

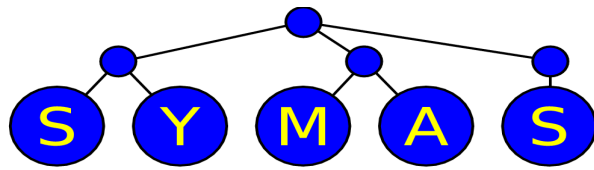
```
userCertificate userKey
```



The Directory Guys

Future Directions

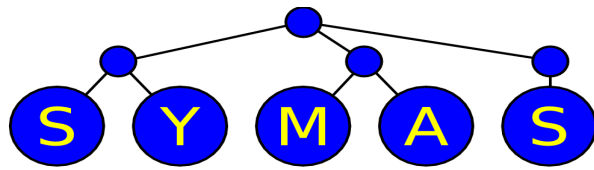
- Porting underway to support Solaris in nssov
- "pinpoint replication": allow replication of individual attributes onto target entries, leaving other attributes intact
 - provides greater flexibility when using replication to distribute cn=config changes



The Directory Guys

Future Directions

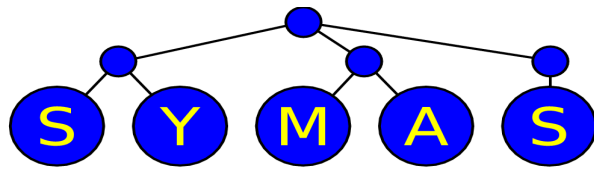
- Further integration work with MIT and Heimdal Kerberos projects
- Implement Password Policy checking for Kerberos and SASL authentication
- (Notice that a lot of future work is peripheral to OpenLDAP. We've succeeded in building our core functionality and are bugging other projects now while still managing to avoid writing an OpenLDAP GUI...)



The Directory Guys

Conclusion

- LDAP is a powerful tool, but even in its most visible use, it has been poorly utilized until recently
- Done properly it really can make sysadmin's lives easier, not harder
- The current OpenLDAP release provides features that go a long way toward banishing the problems of LDAP deployments of the past



The Directory Guys

Conclusion

- The majority of the OpenLDAP Project's existence has been focused inward, striving to improve our base technology to bring it to world class status
- While there's still deep-internals work being planned, our focus is shifting outward to bring better utilization of LDAP to a wider world