Linux and LDAP
A SysAdmins dream team

Ryan Matteson
matty91@gmail.com
http://prefetch.net

Presentation Overview

- Tonight I am going to give an overview of LDAP and show you how you can simplify your life by tying your servers into an LDAP directory server
- This presentation assumes a basic understanding of LDAP, but I'll gladly go over the basics if needed
- I love interactive presentations, so ask questions when they pop into your head

The age old problems

- I have 300 machines to manage, each have a different /etc/passwd, /etc/shadow and /etc/group files. I need to change a password for bob on all of the machines. GAK!!!!!!!
- You get a knock on the door Friday afternoon at 4:57pm and are told that an auditor needs one or more accounts disabled immediately. These users have accounts on various machines so your going to stay late to craft a removal script!! GAK!
- You are approached because corporate security needs strong password policies enabled for all users, each login needs to be audited and you need to lock out users from ALL systems after X unsuccessful login attempts. GAK!
- What is an admin to do?

Use LDAP!

- All of the above can be solved by tying your Linux hosts into an LDAP directory
- LDAP allows you to centralize:
  - Accounts
  - Groups
  - Password policies
  - Autofs maps
  - Password operations
  - Anything that makes sense
- Greatly simplifies your life and the life of your users

So what do I need to do to use this awesomeness you speak ok?

- You need to pick a directory server to use:
  - OpenLDAP
  - OpenDS
  - 389 directory server
  - Various other servers
- Once you pick a server you need to create a directory information tree to store all of your accounts, groups, etc.
- Next you need to add your users and groups to the directory server
- And finally you need to configure your Linux servers to use the directory server

Which directory server?

- There is no right choice here, use the one you feel the most comfortable installing (I'll be using the 389 directory server tonight), configuring and supporting (make sure you can get support)
- All of the major directory servers will provide the posixAccount and posixgroup schemas which are needed to make LDAP authentication work
- POSIX schemas you say? These define the user account (uid, gecos, etc.) and group attributes (gid) that map to the fields in /etc/passwd and /etc/shadow

Adding users and groups

- Users and groups need to be created in the directory server's directory information tree (DIT)
- The default pam_ldap.so configuration will check for users in ou=People, and groups in ou=Group under the base search domain
- There are several ways to do this:
  - Graphical interfaces
  - LDAP browsers
  - Pass an LDIF file to ldapadd
  - Perl or python scripts

LDAP user format

- Each user will be part of the posixAccount object class, and will have the following attributes defined:

```
dn: uid=matty,ou=People,dc=prefetch,dc=net
uid: matty
givenName: The
objectClass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetorgperson
objectClass: posixAccount
sn: Matty
cn: Matty
uidNumber: 5000
gidNumber: 100
homeDirectory: /home/mattyldap
loginShell: /bin/bash
gecos: Mattys Account
```

- These attributes map to fields in /etc/passwd

LDAP group format

- Each group will be part of the posixgroup object class, and will have the following attributes defined:

```
dn: cn=servergroup1,ou=Groups, dc=prefetch, dc=net
gidNumber: 6000
objectClass: top
objectClass: groupofuniquenames
objectClass: posixgroup
cn: servergroup1
uniqueMember: uid=mattyldap,ou=People, dc=prefetch, dc=net
```

- These attributes map to fields in /etc/group

Configuring a Linux host to talk to LDAP

- On Fedora and CentOS servers you can enabled ldap authentication with the authconfig-tui utility
- You can also edit the pam configuration files, /etc/ldap.conf and /etc/nsswitch.conf by hand (this is what authconfig-tui does for you)
- You will need to know the following:
  - Base search domain
  - Hostname of the directory server
  - Location of the X.509 certificate (if TLS/SSL enabled)
  - The list of databases you want to manage
- Advanced LDAP configuration (search scope, timeouts, attribute mappings, etc.) can be done through /etc/ldap.conf

Testing connectivity

- You can verify your client is working by running the getent utility with the database you want to see:

  $ **getent passwd | grep mattyldap**

  mattyldap:*:5000:100:Matty Account:/home/mattyldap:/bin/bash

- If you see the account you should be able to login to the server using an SSH client

Debugging problems

- If you are unable to see the user or login you should fire up your favorite pager and take a look at the system and directory server logs
- The system logs will show client and server issues:

  Oct 31 11:10:57 ldap nscd: nss_ldap: failed to bind to LDAP server \
  ldap:/192.168.1.90: ***Can't contact LDAP server***
- The directory server logs will show the operations attempted and if they succeeded or failed

  [01/Nov/2010:20:12:06 -0400] conn=12 op=23 SRCH base="dc=prefetch,dc=net" scope=2 filter="(&(objectClass=posixAccount)(uid=matytldap))" attrs="uid userPassword uidNumber gidNumber cn homeDirectory loginShell gecos description objectClass"

  [01/Nov/2010:20:12:06 -0400] conn=12 op=23 RESULT err=0 tag=101 nentries=0 etime=0

Debugging problems cont.

- If the logs don’t show anything useful, you can utilize ldapsearch or a directory server browser to double check the attributes and account status
- For intermittent problems you can fire up wireshark and use the built-in LDAP protocol decoding to isolate a problem

What about security?

- In an environment that uses centralized authentication based on LDAP, it is critical that you take every measure possible to protect your directory server
  - Harden the OS configuration
  - Configure your firewalls to limit access
  - Limit who can login directory to the directory server
  - Keep up to date with OS updates
  - Use SELinux
  - Audit your logs regularly (there are free auditing tools)
- Enabling SSL/TLS is also essential, and you can use self-signed certificates if cost is an issue

And performance?

- How many people have gotten that call that the system or applications are running slow?
- We don't want LDAP to introduce any additional issues, so you problable want to look into:
  - Using nscd to cache credentials client side
  - Making sure you have the posixuser and posixgroup attributes indexed on the server
  - Sizing your directory server correctly
  - Configuring enough memory to support all of the entries you create
- For more information on monitoring LDAP performance I will refer you to my SysAdmin magazine article *Monitoring OpenLDAP performance*

And availability?

- Once you integrate your servers with LDAP, availability becomes paramount
- Redundancy, redundancy, redundancy
  - Bonded NICs to diversely routed switches
  - RAID protected storage
  - Use multi master replication and read replicas in larger shops
  - Monitor the heck out of your server and make sure your tools are keeping an eye on the logs
  - Back up your database regularly
- Give plenty of thought to how you manage service accounts and root, since a network hiccup will rip those accounts away from the system (I leave these accounts local for just this reason)

And cool stuff?!?

- The LDAP pam module supports global pasword policies, so you can define password policies in one spot and enforce them everywhere (this will make your auditors happy)
- You can use access.conf to limit who can log into your servers by group, so disabling access to systems is as easy as removing a user from a group on the directory server
- You can use the nisMap object class to manage your autofs maps from a single location

Does this actually work?

- I’m a show me person so let me roll up my sleeves and demo all this goodness
- Demo time!
  - Create user and group in 389
  - Configure a CentOS client to talk to the server
  - Display users and groups
  - Access.conf in action

Conclusion

- This talk barely scratched the surface of what LDAP is capable of, and there are tons of great resources available outlining how to tie just about anything into it
- Tying your Linux server into LDAP can greatly reduce the amount of time you spend managing account related tasks
- Go forth and LDAP!

Questions?

References

- Monitoring OpenLDAP server performance:
  http://prefetch.net/articles/monitoringldap.html
- CentOS / 389 directory server documentation
  http://www.centos.org/docs/5/
- Linux LDAP pam module manual page
  http://linux.die.net/man/5/pam_ldap