

# UNIX LDAP Clients

Or, how I got our Linux/UNIX systems to use an  
LDAP client to authenticate against Novell's  
eDirectory

# OUTLINE

1. Introduction – statement of problem
2. General Discussion of Directories
3. UNIX LDAP clients connecting to eDirectory
4. Some useful client configuration options
5. Conclusion + other resources

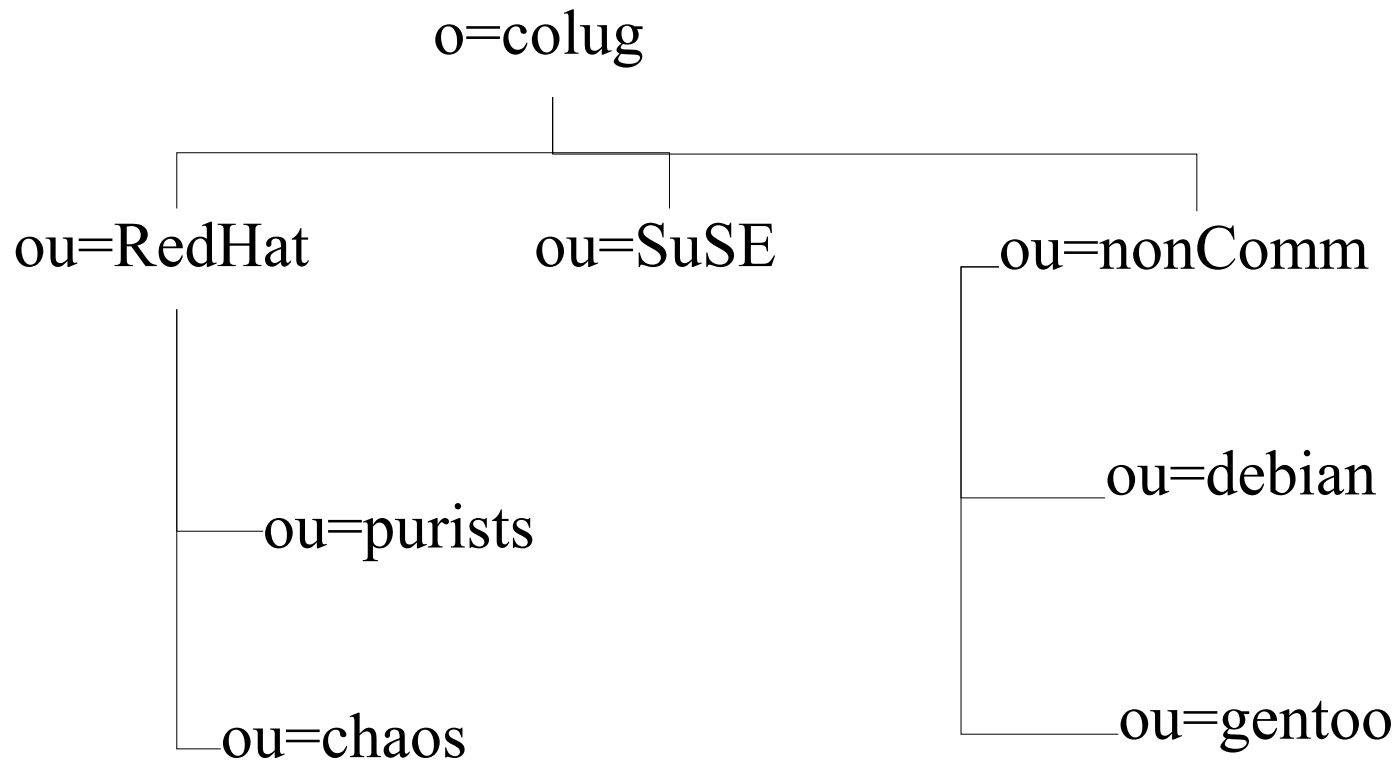
# Introduction

- Previous system support assignments
- OS environment prior to 2002
  - Hard core NetWare (300 + servers)
  - Windows for specific applications (IIS)
  - No UNIX in-house, handled by DAS
- First AIX purchase Q4 2002
- 60 + UNIX/Linux today, more in the wings

# Directories, part 1

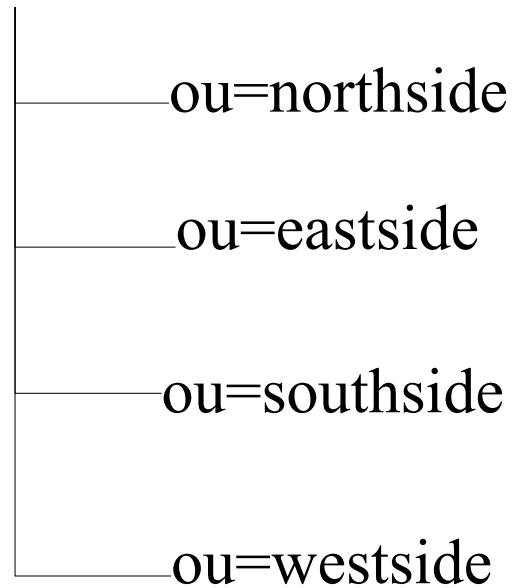
- Consolidate user accounts across multiple platforms
- Examples:
  - flat file: NIS
  - hierarchical: NT Domains/AD
  - flexible: NDS/eDirectory

# Directories, part 2



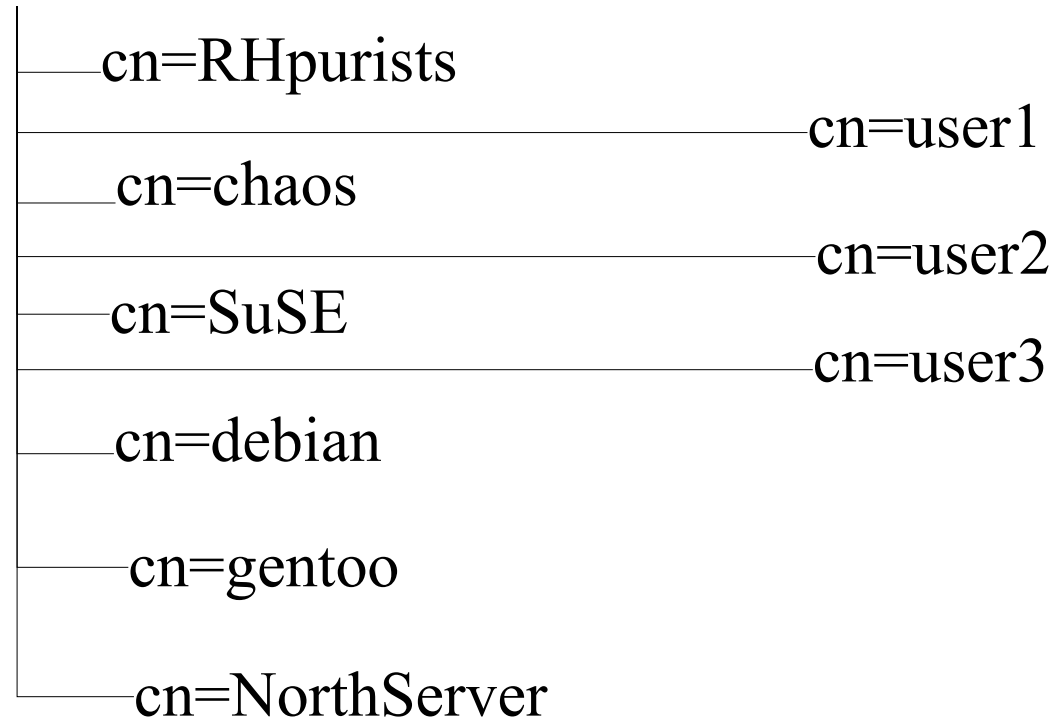
# Directories, part 3

o=colug



# Directories, part 4

ou=northside



# Linux LDAP client, part 1

- OpenLDAP comes with Linux
- Newer versions (/etc/ldap.conf) documented for NDS
  - “some option is obsolete, for NDS now use:”
- Must extend user and group objects with LAM (Linux Account Management) to have uid and gid
- Set up SSL/TLS within the LDAP Server object

# Linux LDAP client, part 2

- LDAP Group – Server Name
  - Under class mappings, associate the following eDirectory classes to the same-named LDAP classes:
    - posixAccount
    - posixGroup
    - shadowAccount
- Prior to OES, must manually track uid/gid numbers.

# UNIX LDAP client, part 1

- AIX requires use of PAM for authentication, which is not set up by default.
  - Not yet implemented in our environment
- Solaris comes with PAM support built in, and an LDAP client
  - I have yet to see anyone claim to have gotten the native LDAP client to work with eDirectory

# UNIX LDAP client, part 2

- Download, compile, and install PADL software
  - [http://www.novell.com/coolsolutions/nds/features/trenches/tr\\_solaris\\_8\\_ldap\\_auth\\_edir.html](http://www.novell.com/coolsolutions/nds/features/trenches/tr_solaris_8_ldap_auth_edir.html)
  - For Solaris 9, must compile OpenLDAP client with Sun's make, not GNU make (assert.h error)
  - Just copied the files to Solaris 10
- Other options discussed under Linux client

# Client Configuration Options

- `ssl starttls` vx. `ssl on`
- `host` vs. `uri://`
- `scope sub`
- `pam_groupdn` `cn=groupname,ou=some,o=colug`
- `pam_min_uid >0`
- `base` `ou=some,o=colug`

# Client Configuration, part 2

- `nss_base_passwd`
- `nss_base_shadow`
- `nss_base_group`
- `pam_mkhome.so skel=/etc/skel umask=022`
  - in pam configuration
  - session optional
- Full Name should map to `gecos` (LDAP attribute)

# Conclusion/Resources

- Everyone says it is easy, but the only good documentation comes from people who have worked through the issues, not from the vendors who want you to use their products
- Novell documentation is inadequate

# Resources

- [http://www.novell.com/coolsolutions/nds/features/trenches/tr\\_solaris\\_8\\_ldap\\_auth\\_edir.html](http://www.novell.com/coolsolutions/nds/features/trenches/tr_solaris_8_ldap_auth_edir.html)
  - Really resolves the Solaris client to Novell LDAP server issues
- <http://www.openldap.org>
- <http://www.padl.org>
- <http://www.kingsmountain.com/ldapRoadmap.shtml>
  - good general resource, lots of links to other LDAP sites
- <http://www.novell.com/documentation>
  - provides general guidance on configuration of Novell's eDirectory
- [http://support.novell.com/search/kb\\_index.jsp](http://support.novell.com/search/kb_index.jsp)
  - search the KnowledgeBase, led me to the first link above