LCI workshop
on high performance clustered computing

Linux Clusters Institute: Account Management

Kyle Hutson, System Administrator, Kansas State University

Access Control

- Authentication vs. Authorization
  - Authentication: Am I who I say I am
  - Authorization: What can I access

Authorization

- Who can access what?
- Unix (Posix) accounts
  - User account
    - User identification (uid or username)
    - uidnumber
    - Default group identification number (gidnumber)
    - Password, Gecos, Home directory, Default shell
  - Group entry
    - Group name
    - Group identification number (gidnumber)
    - Password, uid list

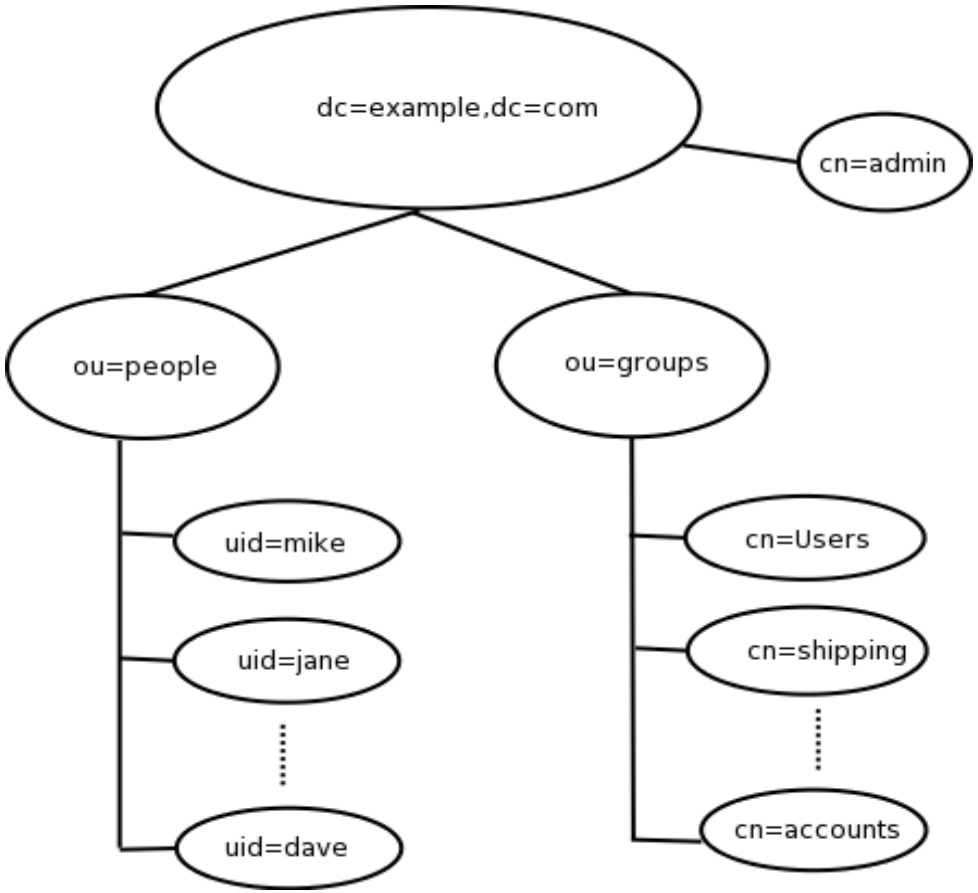
Storing Authorization Info

- Flat files
  - /etc/passwd
    - kylehutson:x:366183:366183:Kyle Hutson:/homes/kylehutson:/bin/bash
  - /etc/shadow
    - kylehutson:*encrypted_password_here*:1::99999:7:::0
  - /etc/group
    - kylehutson_users:*:366183:kylehutson
    - ksu-cis-hpc:*:60010:kylehutson,daveturner,dan,mozes

Centralized Authorization Info

- LDAP (Lightweight Directory Access Protocol)
  - Can be used to store any directory information
    - telephone book, address book, network information, etc.
  - Based on x.500
- Microsoft ADS (LDAP-based)
- NIS

LDAP Structure



Berkeley LDAP Utilities

- ldapadd
- ldapmodify
- ldapdelete
- ldapsearch
- slapcat

LDAP Server Config

- /etc/openldap/slapd.conf
- slapd.conf is now stored in the LDAP directory tree
- slaptest

LDAP Client Config

- /etc/openldap/ldap.conf
- uri ldaps://ldap.test.com:636 ldaps://ldap2.test.com:636
  base dc=YourCompany,dc=com

- sssd (system security services daemon) – Red Hat specific
  - /etc/sssd/sssd.conf
  - [domain/default]
    access_provider = ldap
    ldap_schema = rfc2307bis
    ldap_search_base = dc=YourCompany,dc=com
    ldap_uri = ldaps://ldap.test.com/

Using Authorization Info

- Name Service Switch
  - /etc/nsswitch.conf
  - passwd: files ldap
    shadow: files
    group: files ldap
  - passwd: files sss
    shadow: files sss
    group: files sss
    hosts: files dns

Using Authorization Info

- PAM (Pluggable Authentication Modules)
  - Uses plugins (libraries) to make authentication and authorization decisions.
  - Standardized configuration files in /etc/pam.d/

Resources

- Filesystems
  - Home Directory (typically /home/*username*)
  - You may have your own (/scratch/*username* /archive/*username* /bulk/*username* etc.)
- Permissions
  - `drwxr-x--- 14 jusername username_users 4096 May 16 17:42 mydir`
- Logins
  - /etc/security/access.conf
    - Default is anyone with an account can login
    - - : ALL EXCEPT (adm) jdoe root : ALL

Authentication

- How do I know who you are?
  - Passwords (DES, MD5, SHA)
  - One-time password (OTP)
  - SSH keys
    - ssh-keygen
    - id_rsa.pub --> /home/jdoe/.ssh/authorized_keys
    - Requires shared home directory file system
    - ssh host-based authentication

Authentication

- How do I know who you are?
  - Certificate based
    - PKI (Private Key Infrastructure)
    - CA (Certificate Authorities)
  - OTP (One-time password)

Storing Authentication Info

- Flat files in /etc/shadow
- LDAP
- Kerberos
  - Returns a ticket you can use for future auth

Using Auth Methods

- Service specific
  - Configure each service to use the auth system
  - Gsissh (Globus auth)
- PAM
  - auth required pam_env.so
    auth sufficient pam_unix2.so
    auth sufficient pam_krb5.so use_first_pass
    auth required pam_deny.so

Auth Example

- SSH
  - /etc/ssh/sshd_config

    PubkeyAuthentication yes
    PasswordAuthentication yes
    KerberosAuthentication yes
    UsePam yes

Security

- Passwords or passphrases
  - Minimum length
  - Minimum words in a passphrase
  - How often to change?
  - zxcvbn tests
  - Keep private keys and certs safe – protect with a passphrase
  - 2FA (Two factor authentication)
    - Something you have (OTP, credit card, phone)
    - Something you know (passphrase, PIN)
    - Something you are (fingerprint or other biometric)