CSE 265:
System and Network Administration

- Sharing System Files
  - Motivation
  - Copying files around
  - NIS: Network Information Service
  - NIS+ and LDAP

Sharing system files

- A typical host has tens or possibly hundreds of configuration files
  - passwd, shadow, group, hosts, services, aliases, printcap
- A typical network has tens or hundreds of hosts
- ➔ The result is too much to configure by hand!
- Solutions
  - Group similarly configured machines and distribute configuration files when they change
  - Use a central server instead of individual config files
    - Possibly slower, but never out of date

Copying files around

- Brute-force copying isn't elegant, but it
  - works on all machines
  - is easy to set up and maintain
  - reliable
  - flexible (such as copying apps and data, too)
  - handles some files that aren't supported otherwise
    - /etc/sendmail.cf, /etc/ntp.conf
- Push vs. pull model of file distribution

Pushing with rdist

- **rdist** distributes files when they are out of date
- Preserves ownership, permissions, timestamps
- Originally used **rsh** mechanism (insecure!)
  - Now **ssh** is typically used
- Looks for a Distfile in current directory
  - specifies options, source files, destination hosts
  - Format:
    - *label: pathnames -> destinations commands*

rdist Distfile

```
# Example Distfile
SYS_FILES = (/etc/passwd /etc/group /etc/mail/aliases)
GET_ALL = (chimchim lollipop barkadon)
GET_SOME = (whammo spiff)

# files -> targets
all: ${SYS_FILES} -> ${GET_ALL}
    notify barb;
    special /etc/mail/aliases “/usr/bin/newaliases”;

some: ${SYS_FILES} -> ${GET_SOME}
    except /etc/mail/aliases;
    notify eddie@spiff;
```

– Copies the three listed files, sends mail to barb@destination with updates or errors

– Need ssh at target, no password

Option #2: rsync

- **rsync** – similar to **rdist**, but doesn't just copy
  - Attempts to transfer only the changes to a file
  - Client can run **rsync** out of **inetd** (no rsh!)
    - Can require a password, restrict access to certain dirs
- Example:

```
# rsync -gopt –password-file=/etc/rsync.pwd /etc/passwd lollipop::sysfiles
```

- Uses /etc/rsyncd.conf

rsync configuration

```
# This is /etc/rsyncd.conf

# sysfiles is just an arbitrary title for the particular module
[sysfiles]
# This is the path you allow files to be pushed to.  It could be just /
path = /etc

# This is the secrets file containing the username/password pair for
# authenticating the module
secrets file = /etc/rsyncd.secrets
# Can be read only if you are pulling files
read only = false
# UID and GID under which the transfer will be done
uid = root
gid = root
# List of hosts that are allowed to connect
hosts allow = master-host
```

- Secrets file is just name:password
  - root access only!

Pulling files

- Simple copy utilities
  - Can use **wget** from ftp or web site (or **ncftp**, etc.)
  - Can use NFS and just **cp**
  - Might want to have script verify contents before installing
- Can use **rsync**
- Need to stagger access to server
  - Can't just use a cron at same time!
  - Wrap with Perl script to randomize

```
#!/usr/bin/perl
sleep rand() * 600; # sleep 0-600s (i.e., 10 minutes)
system(copy_files_down);
```

How programs get to system files

- Many configuration files have routines in standard C library
  - getpwuid, getpwnam, getpwent for passwd
  - Routines are capable of using alternative sources
- In Linux, sources of info are determined by /etc/nsswitch.conf
- nscd: caches many lookup responses
  - cache passwd, group, DNS results
  - /etc/nscd.conf

Sample /etc/nsswitch.conf

```
passwd:     files nis
shadow:     files nis
group:      files nis

#hosts:     db files nisplus nis dns
hosts:      files nis dns

bootparams: nis [NOTFOUND=return] files

netgroup:   files
ethers:     files
netmasks:   files
networks:   files
protocols:  files nisplus
rpc:        files
services:   files nisplus

automount:  files nisplus
aliases:    files nisplus
```

NIS: Network Information Service

- Originally called Sun Yellow Pages
- Shares records (i.e., one line per file)
- Master server maintains authoritative copies of system files, in original locations as before
  - Server process makes contents available over net
  - Server maintains multiple NIS “maps” for lookups
    - e.g., lookup passwd.byname passwd.byuid
- Permits use of slave servers to replicate content
  - File changes on master must be pushed to slaves
  - Clients think they are all servers (no difference)

NIS organization

- Domain
  - A server and its clients constitute an NIS domain
- Netgroups
  - Named sets of users, machines, or networks for easy reference in system files
  - Defined in /etc/netgroup, shared as an NIS map
    - Format: *groupname list-of-members*
    - Member format: (*hostname, username, nisdomainname*)
    - Example: (boulder,-,)
      - Dash/hyphen indicates negation
      - Empty fields match everything

Netgroups

- Larger /etc/netgroup example

```
bobcats          (snake,,) (headrest,,)
servers          (anchor,,) (moet,,) (piper,,) (kirk,,)
anchorclients    (xx,,) (watneys,,) (molson,,)
beers            (anchor,,) (anchor-gateway,,) anchorclients
allhosts  beers bobcats servers
```

- Netgroups can be used in /etc/exports

```
/export/projects    -access=@bobcats
/export/homefiles   -access=@anchorclients,root=@servers
```

- Also in **sudo**
- Netgroups can be used without NIS

NIS

- Client has list of servers in /etc/yp.conf
  - Often supplied by DHCP
- NIS server data files are in /var/yp
  - Subdirectories are NIS domains, e.g.:
    - /var/yp/cssuns/passwd.byname
      /var/yp/cssuns/passwd.byuid
  - Makefile in /var/yp will generate db files from flat (text) files, and run **yppush** to propagate to slaves
- **ypbind** runs on all NIS machines
  - C library contacts local ypbind daemon for every query (if config'd by /etc/nsswitch.conf)

Setting up NIS domain

- NIS must be initialized on all masters and slaves
- On servers (in /var/yp)
  - Set NIS domain name using **domainname**
  - Run **ypinit -m/-s *master***
  - Run **ypserv**
- On slaves, also want **crontab** entries to pull fresh copies
- On clients
  - Set NIS domain (in /etc/sysconfig/network for RHEL/CentOS)
  - Still need /etc/passwd and /etc/group for root without NIS

NIS, NIS+ and LDAP

- NIS: Common, but out of date
- NIS+
  - Extended, “fixed” re-write of NIS with better security
  - Buggy (on Linux), and development has stopped
- LDAP: Lightweight Directory Access Protocol
  - Really, just a database schema
  - Basis for Microsoft Active Directory
  - Can contain admin config data, but more typically contact information (phone, email, address, etc.)
    - Most email clients can use LDAP (e.g., my pine mailer)
  - RHEL/CentOS comes with API, clients and servers from OpenLDAP.org