Summary:
After successfully resolving the storage issue on the file server, you've discussed a plan with Michael Scott to create employee accounts on all production machines. Michael also asked you to create a few directories on Machine E that can be used to share important, super secret, confidential files. One directory needs to be dedicated to managers, another to sales, and a third to accounting.

Michael has given you an organizational chart (see below) listing the names and titles of the employees at our branch of Dunder Mifflin.

Rationale

Forcing users to log in with their own credentials reduces the risk of having the root password compromised or of them inadvertently harming the system. It also provides accountability because actions on a machine can be traced back to a specific user. Users can be restricted to specific commands.

Managing user accounts on a single machine is easy but it can be challenging to ensure consistency of account information among multiple machines. Several tools such as ldap and kerberos are designed to centralize account data, but these advanced topics are beyond the scope of the lab.

How can we distribute account information?

As discussed in class the commands passwd, useradd/del/mod, and groupadd/del/mod simply modify the files /etc/passwd, /etc/shadow, and /etc/group. One simple way to distribute account information is to use rdist, rsync, or scp (secure copy) to routinely copy these files from a 'master' machine to the rest. However, this entails some security risks.

Simply copying files is ok for new unix/linux system administrators, but there are better ways. One slightly better way is to script the passwd, useradd/del/mod, and groupadd/del/mod commands.

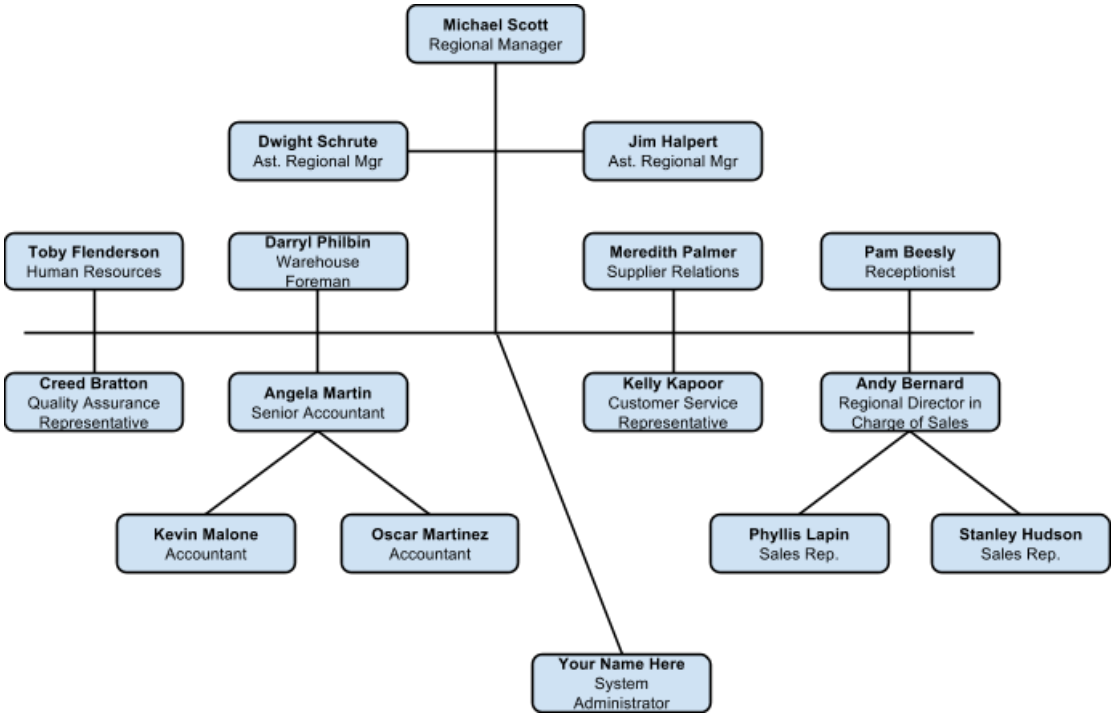
Another method is to either use a central authentication and authorization system such as LDAP + Kerberos, or a configuration management tool such as puppet. Either method enables administrators to avoid the tedious task of repeating the same commands several times, or hacking together a bunch of bash scripts.

Learn and use puppet for this lab. Aside from the introduction in class there are a few good resources online such as this basic introduction, or you can pick up a good book on the subject.

Prerequisites

Please finish the required reading before starting the lab. You are strongly encouraged to experiment with the commands involved on your own virtual machine before trying this on the production machines.

Dunder Mifflin Organizational Chart



Dunder Mifflin Network Topology & Configuration

D-M currently has the following CentOS Linux machines:

1. A gateway (machine A) handles dhcp, ip_forwarding, and network/port address translation (nat/pat).
2. A file server (machine E) stores company files centrally.
3. An http server (machine B) hosts the corporate website.
4. An ftp server (machine C) updates prices and accepts batch orders.
5. A dns server (machine D) maps between domain names and IP addresses.

Submission Requirements

1. Please submit your lab notes including any puppet manifest(s) you used to create users.
2. Set up accounts on all machines for all D-M employees and yourself. Each user should have a username of the form first-initial last-name, password, unique uid, unique gid, /path/to/login/shell, and /path/to/home/directory/. The grading script is very strict about user names. usernames must be all lowercase with no punctuation. Account data must be the same on all machines. The Gecos field does not matter.
3. Home directories must exist for all users. All home directories on all machines must be initialized with the contents of /etc/skel/ and owned by the appropriate user and user-private-group.
4. Create secondary groups for managers, sales, and accounting. The grading script checks for these exact names. Add the appropriate users to these groups based on the org chart.
5. Create a shared directory under /home/ on the file server (machine E) for each secondary group you created, with permissions such that only the user owner and members of the group owner can read, write, and execute files. New files and folders created under these shared directories must inherit the group id of the parent directory, not that of the process that creates them.

6. Use exact names for users mscott, dschrute, jhalpert, pbeesly, abernard, amartin, kkapoor, omartinez, dphilbin, tflenderson, kmalone, plapin, shudson, mpalmer, cbratton.