```
#get my passwords consistent
#for user in mscott jhalpert dschrute pbeesly abernard plapin shudson
amartin omartinez kmalone dphilbin kkapoor tflenderson mpalmer
cbratton oldo5582; do echo "$user":"$user" | sudo chpasswd; done

#1. limit access with pam

#oldo5582, root, mscott, dschrute must be able to log into all
machines

#to enable pam, see PAM slide 13.

#edit /etc/security/access.conf on A and B
+:root:ALL
+:mscott:ALL
+:oldo5582:ALL
+:dschrute:ALL
-:ALL:ALL

#pbeesly,abernard,kkapoor can log into C and D
+:root:ALL
+:mscott:ALL
+:oldo5582:ALL
+:dschrute:ALL
+:pbeesly:ALL
+:abernard:ALL
+:kkapoor:ALL
-:ALL:ALL

#all users must be able to log into E
+:ALL:ALL

#accounting can log into F
+:root:ALL
+:mscott:ALL
+:oldo5582:ALL
+:dschrute:ALL
+:(accounting):ALL
-:ALL:ALL

#enforce password policy with pam (10 chars, 2 digits, 2 uppercase, 1
otherchar. no length credit for lowercase.)
#/etc/security/pwquality.conf
rm -f /etc/security/pwquality.conf; vi /etc/security/pwquality.conf

minlen = 10
dcredit = -2
ucredit = -2
lcredit = 0
ocredit = -1
```

```
enforcing = 1
retry = 1
```

#do not expire passwords. policy only applies to password changes.

#test stuff

#this took about 4 hours. had to fix some old stuff too.

#script (this does require sshpass, but it was already available on all the redhat machines!)

```
#!/bin/bash

USERS=("mscott" "jhalpert" "dschrute" "pbeesly" "abernard" "plapin"
"shudson" "amartin" "omartinez" "kmalone" "dphilbin" "kkapoor"
"tflenderson" "mpalmer" "cbratton" "oldo5582")
ADMINS=("mscott" "oldo5582" "dschrute") #all machines
WEBADMINS=("pbeesly" "abernard" "kkapoor") #machine c & d
ACCOUNTING=("amartin" "kmalone" "omartinez") #machine f
MACHINES=("100.64.0.11" "100.64.11.2" "100.64.11.3" "100.64.11.4"
"100.64.11.6")
MACHINE_LETTERS=('A' 'B' 'C' 'D' 'F')

machine_num=0
for machine in "${MACHINES[@]}"
do :
  printf "Machine %s\n" "${MACHINE_LETTERS[$machine_num]}"
  for user in "${USERS[@]}"
  do :
    sshpass -p "$user" ssh -o StrictHostKeyChecking=no
"$user@$machine" 'uname -a' &>/dev/null
    ret="$?"
    #a & b, only admins
    if [ "$machine" = "100.64.0.11" ] || [ "$machine" =
"100.64.11.2" ] ; then
      case $ret in
        0)
          if [[ " ${ADMINS[*]} " =~ ${user} ]];
          then
              printf "1 %s can log in\n" "${user}"
          else
              printf "0 %s shouldn't be able to log in\n" "${user}"
          fi
          ;;
        255)
          if [[ " ${ADMINS[*]} " =~ ${user} ]];
          then
              printf "0 %s should be able to log in\n" "${user}"
          else
```

```
              printf "1 %s cannot log in\n" "${user}"
          fi
          ;;
        *)
          echo "other problem"
          ;;
      esac
    fi

    #c & d, admins and webadmins
    if [ "$machine" = "100.64.11.3" ] || [ "$machine" =
"100.64.11.4" ] ; then
      case $ret in
        0)
          if [[ " ${ADMINS[*]} " =~ ${user} ]] || [[ " ${WEBADMINS[*]}
" =~ ${user} ]];
          then
              printf "1 %s can log in\n" "${user}"
          else
              printf "0 %s shouldn't be able to log in\n" "${user}"
          fi
          ;;
        255)
          if [[ " ${ADMINS[*]} " =~ ${user} ]] || [[ " ${WEBADMINS[*]}
" =~ ${user} ]];
          then
              printf "0 %s should be able to log in\n" "${user}"
          else
              printf "1 %s cannot log in\n" "${user}"
          fi
          ;;
        *)
          echo "other problem"
          ;;
      esac
    fi

    #f, admins and accounting
    if [ "$machine" = "100.64.11.6" ] ; then
      case $ret in
        0)
          if [[ " ${ADMINS[*]} " =~ ${user} ]] || [[ " $
{ACCOUNTING[*]} " =~ ${user} ]];
          then
              printf "1 %s can log in\n" "${user}"
          else
              printf "0 %s shouldn't be able to log in\n" "${user}"
          fi
          ;;
        255)
```

```
          if [[ " ${ADMINS[*]} " =~ ${user} ]] || [[ " $
{ACCOUNTING[*]} " =~ ${user} ]];
          then
              printf "0 %s should be able to log in\n" "${user}"
          else
              printf "1 %s cannot log in\n" "${user}"
          fi
          ;;
        *)
          echo "other problem"
          ;;
      esac
    fi
  done
  machine_num=$((machine_num + 1))
done
```