z/VM and Linux administration in a no-root environment

Michael MacIsaac
Innovation Data Processing

VM Workshop
June 27, 2015

Abstract

- Many organizations do not allow SSH access to Linux as root. The Linux sudo facility and SSH key-based authentication can be used by system administrators who still need root access. As the number of z/VM and Linux systems increases, configuring sudo and SSH results in more work. This presentation will first suggest a model then show a reference implementation for automating the SSH key configuration, and minimizing the need for sudo. It will additionally show how to allow administrators to securely use Web access.

Outline

- Quotations …
- Introductions
- A short story
- Issues with root logins
- Issues with no-root logins
- Background on sudo and SSH
- Allowing Web access
- Bringing it all together
- Live demo

Quotation

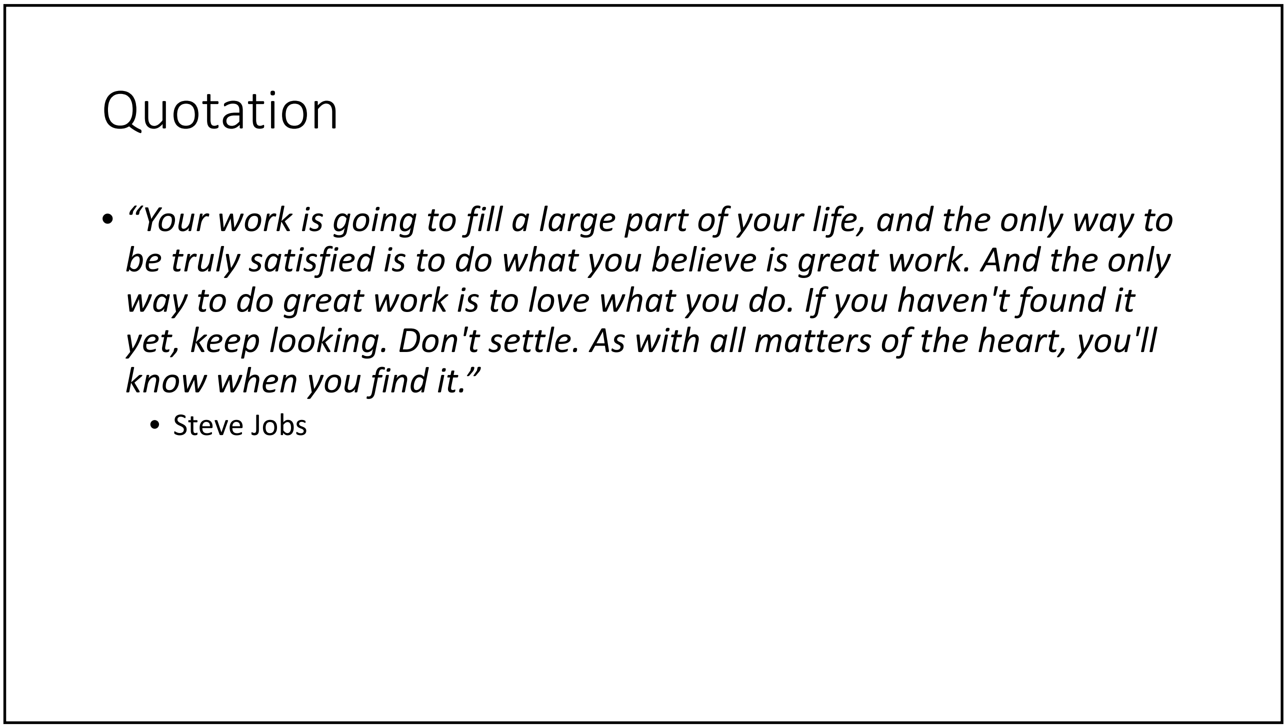
- *“We reject kings, presidents and voting. We believe in rough consensus and running code.”*
    - David Clark, IETF

Introduction

- Who am I?
- Mike MacIsaac
  - 27 years at IBM
  - 1.5 years at Innovation Data Processing
  - 6.5 years writing zoom (previously ‘Mz’)
- Who are you?
  - IBMer
  - Vendor
  - Customer
- Are you allowed to:
  - Login as root?
  - ‘su’ to root?
  - Never be root?
  - Never login to Linux?

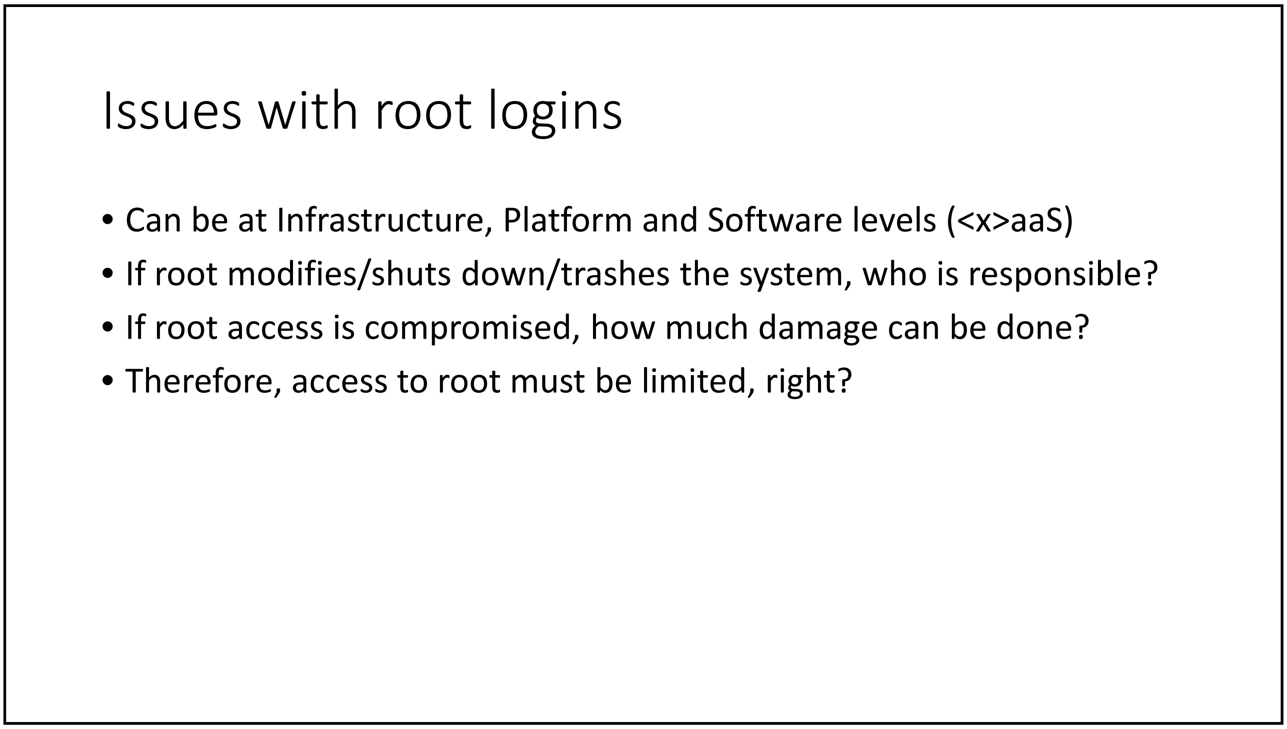
A short story

- Once there was a new hire (and a new manager) …



Quotation

- *“Your work is going to fill a large part of your life, and the only way to be truly satisfied is to do what you believe is great work. And the only way to do great work is to love what you do. If you haven't found it yet, keep looking. Don't settle. As with all matters of the heart, you'll know when you find it.”*
  - Steve Jobs



Issues with root logins

- Can be at Infrastructure, Platform and Software levels (<x>aaS)
- If root modifies/shuts down/trashes the system, who is responsible?
- If root access is compromised, how much damage can be done?
- Therefore, access to root must be limited, right?

Issues with no-root logins (Q)

- How do multiple administrators get R/W access to the same data?
- How do admins invoke privileged (root) commands?
  -
- How are non-admins on a system prevented from sensitive data?

Issues with no-root logins (Q&A)

- How do multiple administrators get R/W access to the same data?
  - Linux groups
- How do admins invoke privileged (root) commands?
  - Sudo su to root (good)
  - Sudo to individual commands (better?)
- How are non-admins on a system prevented from sensitive data?
  - No login access
  - With login access
    - Linux groups and other permissions
    - Linux umask

Linux groups and other permissions

- Example of group and ‘other’ permissions:

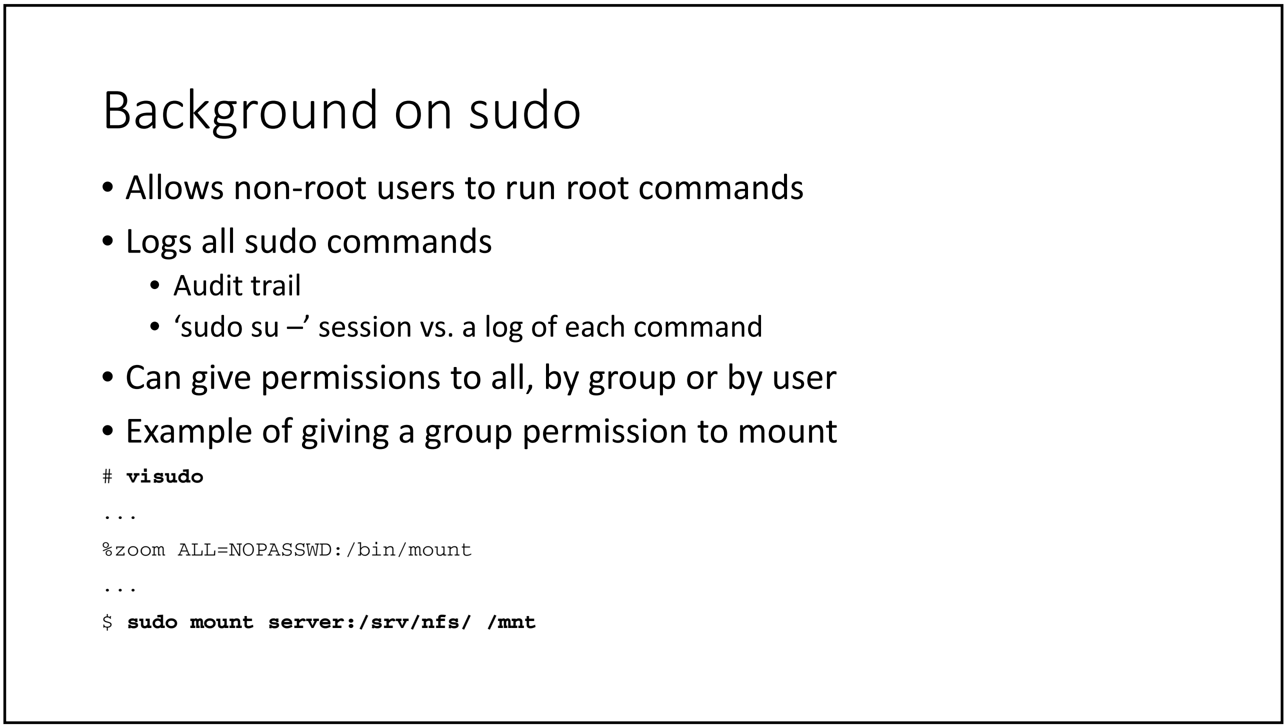
```
# groupadd admins
# cd /srv
# mkdir data
# chmod g+rws,o-rwx data
# chgrp admins data
```

- Example of setting an user’s umask:

```
# su – mike
$ umask 007
$ echo “important data” > /srv/data/foo
```

Quotation

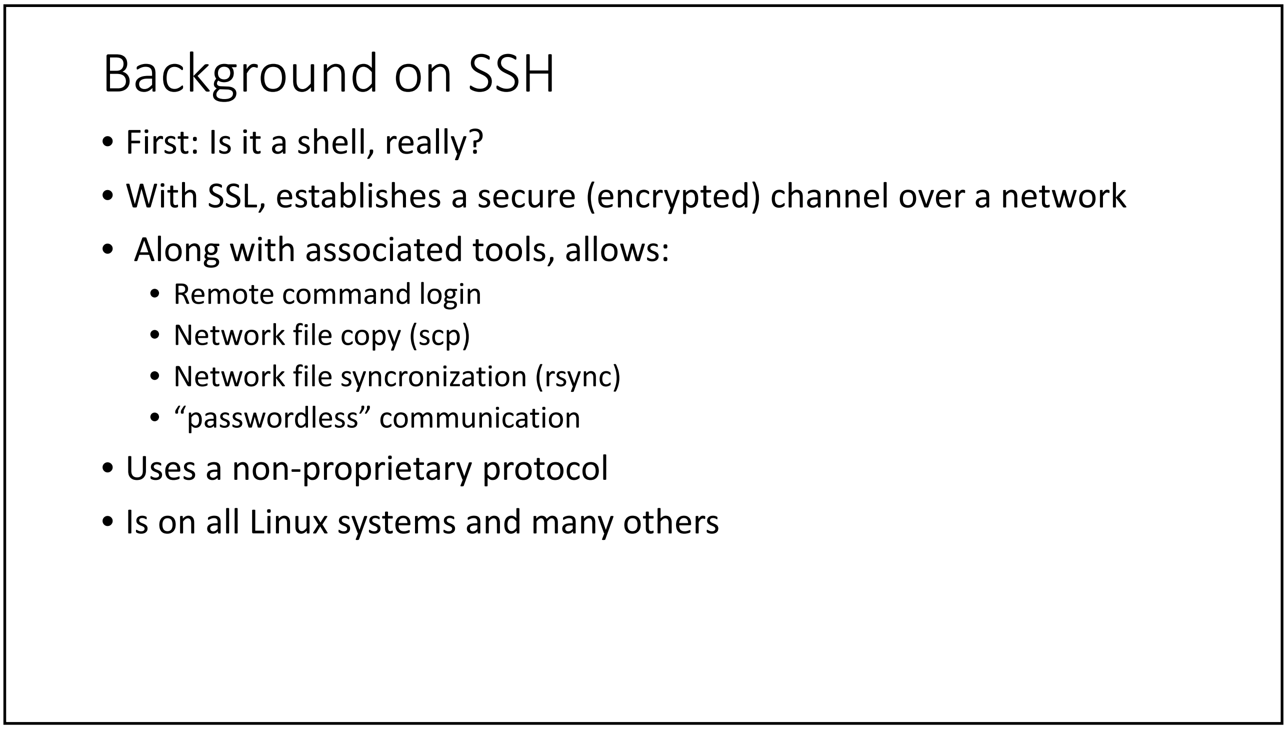
- *“The temptation in systems management software is to try to abstract function and code across platforms. Resist that temptation - it is better to drill down into platform-specifics sooner rather than later.”*
  - Bruce Potter, IBM



Background on sudo

- Allows non-root users to run root commands
- Logs all sudo commands
  - Audit trail
  - ‘sudo su –’ session vs. a log of each command
- Can give permissions to all, by group or by user
- Example of giving a group permission to mount

```
# visudo
...
%zoom ALL=NOPASSWD:/bin/mount
...
$ sudo mount server:/srv/nfs/ /mnt
```



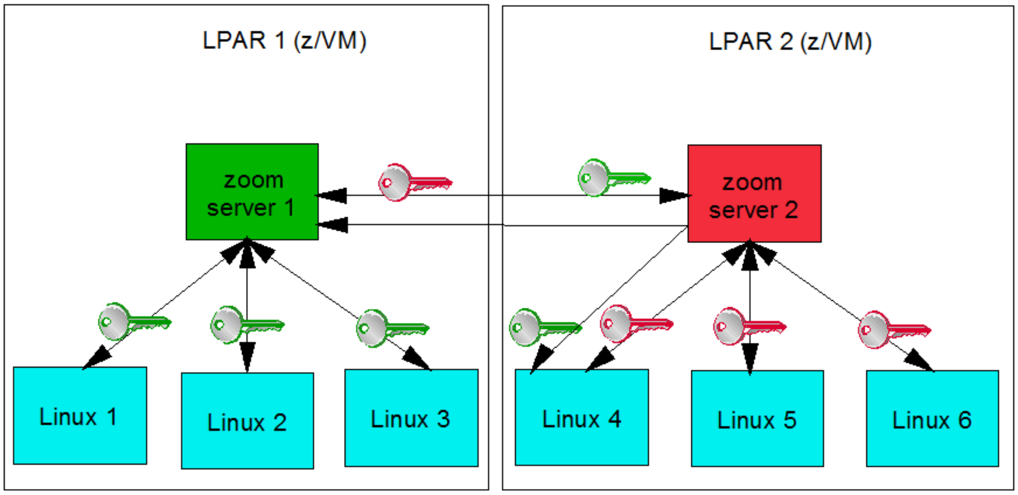
Background on SSH

- First: Is it a shell, really?
- With SSL, establishes a secure (encrypted) channel over a network
- Along with associated tools, allows:
  - Remote command login
  - Network file copy (scp)
  - Network file syncronization (rsync)
  - “passwordless” communication
- Uses a non-proprietary protocol
- Is on all Linux systems and many others

SSH key-based authentication

- Target system lists authorized users
  - Each user must have a .ssh/ directory under their home directory
  - Key files writable only by owner and root
- Source system lists known target hosts

Copying SSH keys



Example bash function

```
function zPushKey
 {
  local node=$1
  local AKfile=authorized_keys
  local sshCmd="/usr/bin/ssh $sshFlags"

  $sshCmd $node "mkdir -p ~/.ssh;
                chmod 700 ~/.ssh;
                cd ~/.ssh;
                touch ~/.ssh/$AKfile;
                chmod 600 ~/.ssh/$AKfile;
                sed -i \"/.*$(hostname)$/d\" ~/.ssh/$AKfile;
                echo \"$(cat ~/.ssh/id_rsa.pub)\" >> ~/.ssh/$AKfile"
 }
```

Quotation

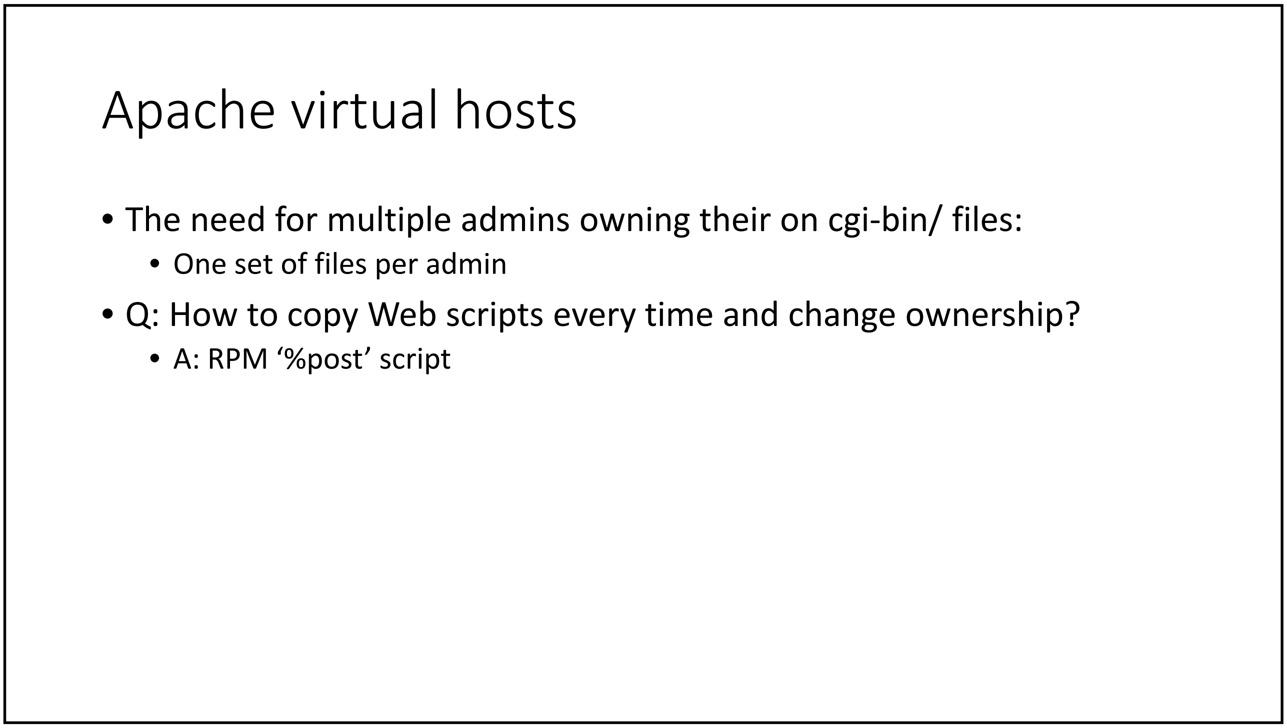
- *“Learn the command line interface first so if something goes wrong, you know how to fix it. Next, learn the GUI - if it makes you more productive, use it.”*
  - Mike MacIsaac

Allowing Web access (Q)

- Does a Web server run as root?
- Can a Web server ‘su’ to another user?
- Can a Web server use LDAP to allow logins?
- Can multiple admins run cgi-bin/ scripts as themselves?

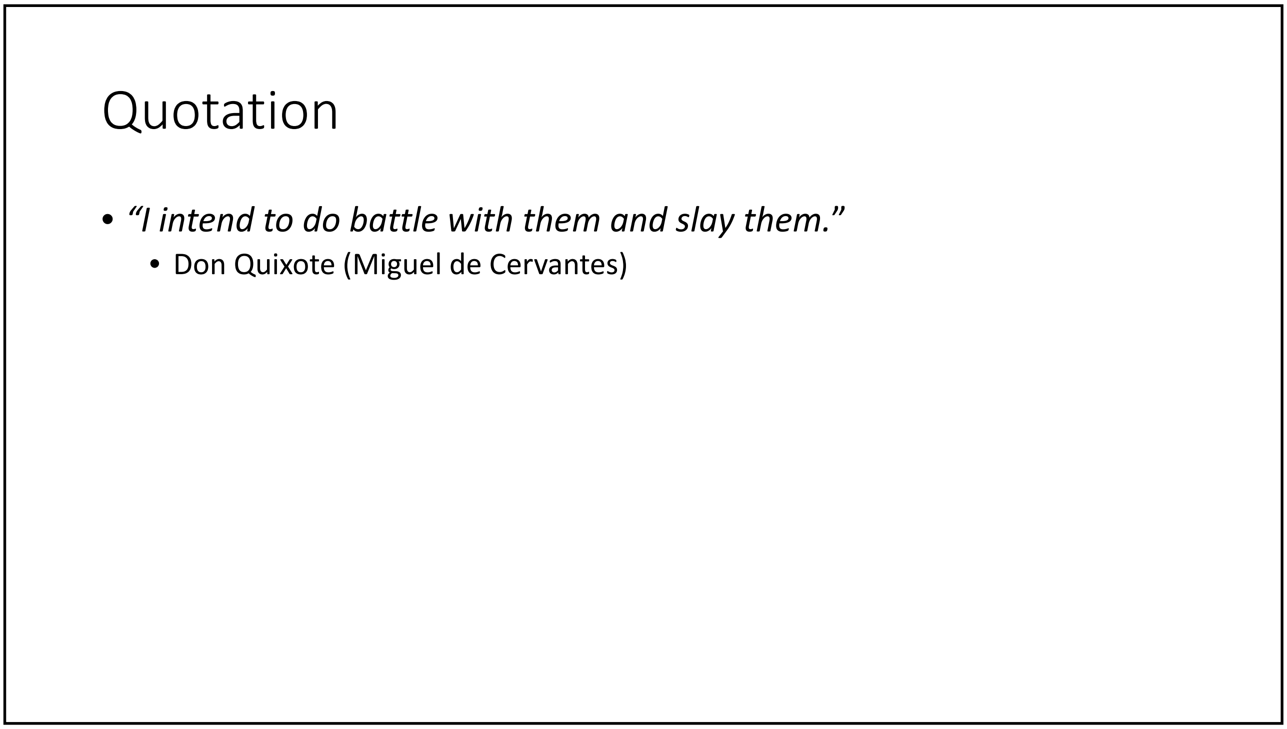
Allowing Web access (Q&A)

- Does a Web server run as root?
  - No
- Can a Web server ‘su’ to another user?
  - Yes, with the Apache **suexec** module
- Can a Web server use LDAP to allow logins?
  - Yes, with the Apache **mod_auth_ldap** module
- Can multiple admins run cgi-bin/ scripts as themselves?
  - Yes, using virtual hosts and **suexec**
  - However, one cgi-bin directory is needed per admin



Apache virtual hosts

- The need for multiple admins owning their on cgi-bin/ files:
  - One set of files per admin
- Q: How to copy Web scripts every time and change ownership?
  - A: RPM ‘%post’ script



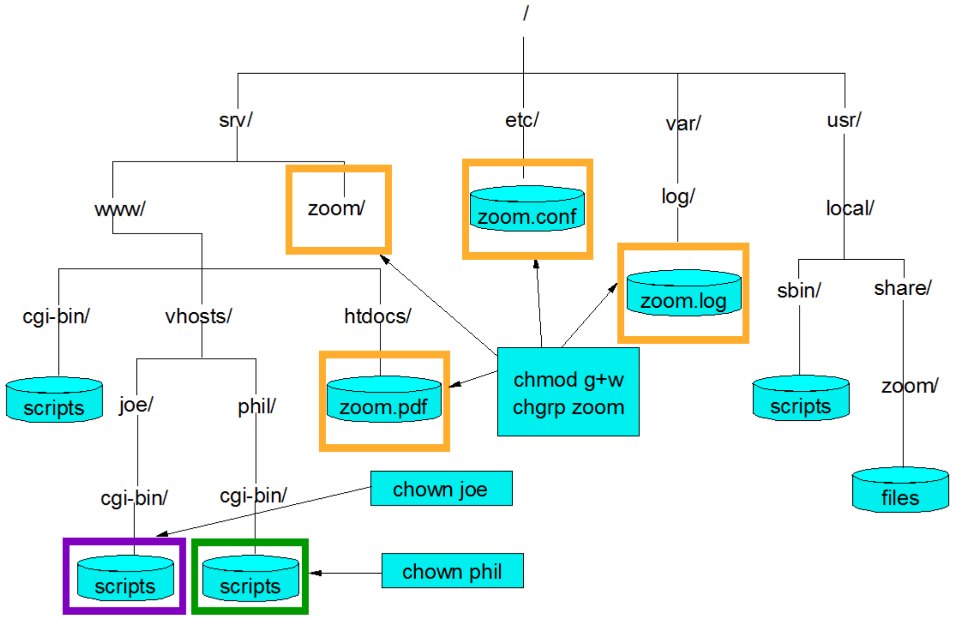
Quotation

- *“I intend to do battle with them and slay them.”*
  - Don Quixote (Miguel de Cervantes)

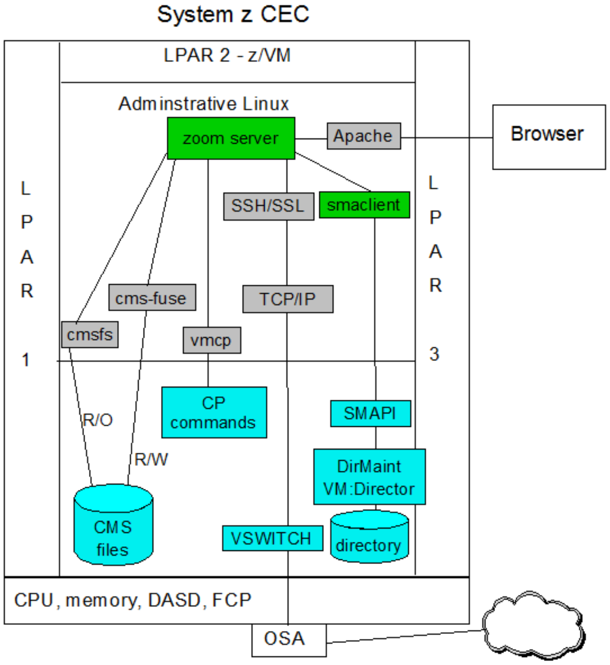
Bringing it all together

- zoom (**z** Systems **o**bject **o**riented **m**anagement)
  - An open-source package for Linux and z/VM
  - Uses TCP/IP, SSH, scp, rsync, sudo, vmcp, SMAPI, smaclient, Apache, …
  - What are the objects?
    - Systems, CECs, LPARs, z/VMs, virtual machines and Linuxes
    - Clients, servers, nodes, clusters and trees
    - Devices, DASDs, FCPs, PAVs, OSAs and CHPIDs
    - Appliances, services and administrators
- CLI is king, GUI (Apache) is a powerful queen
- Added administrators and ‘lazy’ copying of SSH keys
- Uses OVF for appliance capture/deploy
- Performs minimal monitoring
- Complete set of help screens, man pages & a manual

File system hierarchy



Functional hierarchy



Live demo

- *“We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty,* ***Freeware****, and the pursuit of Happiness.”*
    - Thomas Jefferson (***amended by editor for 21st centry*** :))