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

Michael MacIsaac
MVMUA
Poughkeepsie, NY
July 21, 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 (zoom) for automating the SSH key configuration, and minimizing the need for sudo. It will also show a model for secure Web access to the same set of tools.

Outline

- Overview
- Quotations by famous and not-so-famous people …
- Issues with root logins
- Issues with no-root logins
- Background on sudo and SSH
- Allowing Web access
- Bringing it all together
- Live demo

Overview

- z/VM meeting – Why Linux content?
  - Related: *"CMS in the 21st century"* thread on IBMVM (July 7-12)
- What is the business value?
  - Automation
  - Reference implementation
- Linux vs. z/VM in zoom:
  - "The zoom package was designed and written to perform the ***majority of systems management from Linux*** because there is a rich set of tooling and support for Linux worldwide, with many programmers working to improve the operating system. While z/VM has an older heritage, it does not have near the support structure that Linux does. Of course z/VM skills will always be needed, but if much of the day-to-day system administration can be performed by those more comfortable with Linux, fewer z/VM resources will be needed in the organization."

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

- Is at Platform and Software levels, possibly Infrastructure (<x>aaS)
  - Iaas – a z/VM virtual machine (new cmd name: zannihilateclient? ☺)
  - Paas – a VM with Linux (or other OS)
  - Saas – Linux with application
- 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 Linux administrators get R/W access to 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 (acceptable?)
  - 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

System access truth table

User type	Can access system?	System data R/O	System data R/W, operations
Cannot SSH to hosts	No	No	No
Can SSH, not in admin group	Yes	No	No
In admin group	Yes	Yes	No
A zoom administrator	All systems, w/o passwords	Yes	Yes

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 synchronization (rsync)
  - “passwordless” communication (aka “key-based authentication”)
- Uses a non-proprietary protocol
- Is on all Linux systems and many others

Background on SSH keys

- Types
  - DSA – Digital Signature Algorithm
    - Key size must be exactly 1024 bits as specified by FIPS 186-2.
  - RSA – Rivest, Shamir, Adleman
    - Minimum key size is 768 bits and the default is 2048 bits
  - Other
    - SLES 12 has a new default?

SSH key-based authentication

- Each system has a public/private key
  - 'Host key'
- Target system lists authorized users
  - Each user must have a .ssh/ directory under their home directory ('user key')
    - Public key
    - Private key
    - Known_hosts file
    - Authorized_keys file
  - For example:

```
mike@lab152:~ # ls -ld .ssh
drwx------ 2 mike zoom 4096 Jul 20 07:36 .ssh/
mike@lab152:~ # ls -l .ssh
total 16
-rw------- 1 mike zoom  393 Jul 20 07:36 authorized_keys
-rw------- 1 mike zoom 1675 Jul 20 07:36 id_rsa
-rw-r----- 1 mike zoom  393 Jul 20 07:36 id_rsa.pub
-rw-r--r-- 1 mike zoom 1212 Jul 20 07:36 known_hosts
```

Two SSH key files

```
mike@lab152:~/.ssh # cat known_hosts
```

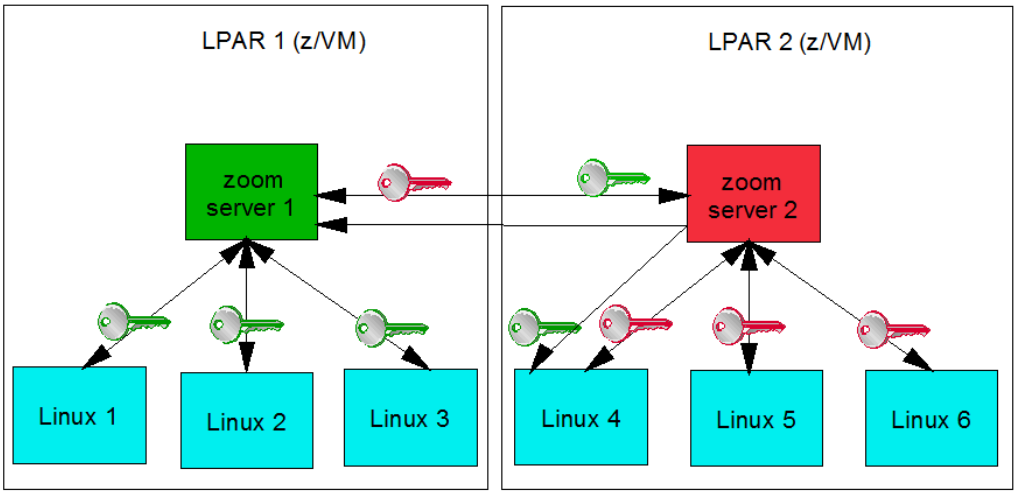
```
lab152,192.168.250.152 ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQDZ0t15xGuY9I3NnxRHcN/fEuTQQ2PA1keWLsyExtP+tIUTwXPXuiFy
hJjCZ6oytmut5S+X9ZZFi8Uz+MnHYxG4wp55JJmLE5wPrHstNFeZHJoTMZlupgiWRB11UenNaAfRR9HLqWS8
qc5YpAuG0Mzi/N0Aeu6PjeSknsf/pDAik6JopSO5S7k9SPLYOgVSq533JxMDWyDRBpcRKh4xZU/VtCz0ZJ+6
s60uecwPWWC8FP2571P007+PRyEYVMnijG336tj2KfFaB76UXT/jJBVJbGX5G9G5BofoxOlsYZAejuAhsAUe
B2nf514Kq5M4yYtE2Tp1b9UVWGO4GaXRsiAR
```

```
mike@lab152:~/.ssh # cat authorized_keys
```

```
ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQCjVH3qeWA/1+HSj/t/DrR6ZU4UPIMJ4iuY5FPZZ28xt5iCE2CwJtfj
DWRugdpPplchrstD5Sqz7ipsOIbKi3QIEMeQJUwwqwyPRHb1ZCVxAMnETTNKrRhbv0WsWgSbW7WkRpeQ8vCq
hdQqnpK8DmbRYJlSMzcMkG0u2ngZxcK1nLTd7x8HPW4bFpPWq1+GS1pAinNTBWtp+ZkVxQBsSh032czt8l7V
BD+/NizckYjYPQ2eq/1DLxqp5JKMWF/eu9Dz2Jkl2FaJrnP3L3u5OdF0Okefjo4W7J7yFTF3Bvh28pirLiRf
hcvL+7OBQLPwD0GC6XwWnhdq7f6P0g4vwluB mike@lab152
```

Copying SSH keys in zoom

- 'Lazy' key copying:



- New 'Full' key copying (added July 2015)

SSH variables in zoom

- Variables in zoom related to security and SSH

```
# variables releated to permissions SSH key-based authentication
adminGroup="zoom"               # the Linux group for zoom administrators
AKfile=authorized_keys          # file name relative to ~/.ssh/ directory
HKfile="/etc/ssh/ssh_host_rsa_key.pub" # hosts' fully qualified public key file
rootSSH="yes"                   # is the root user allowed to scp/ssh/rsync?
sshFlags="-o HostKeyAlgorithms=ssh-rsa" # flags passed with ssh commands
sshKeyPush="full"               # 'full' for all keys 'lazy' for this server
umask="007"                     # user/group: R/W, other: none
```

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

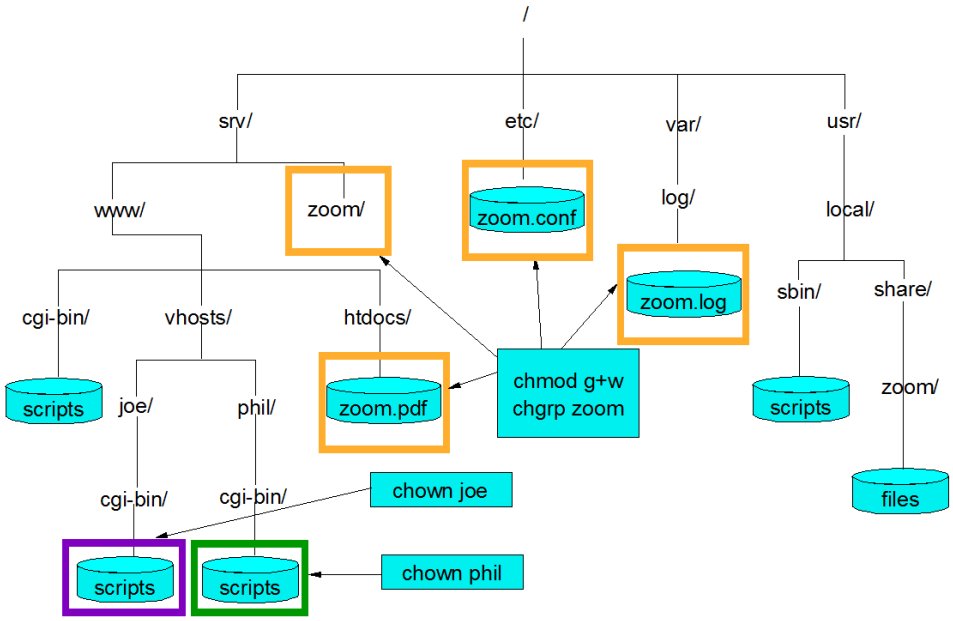
Quotation

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

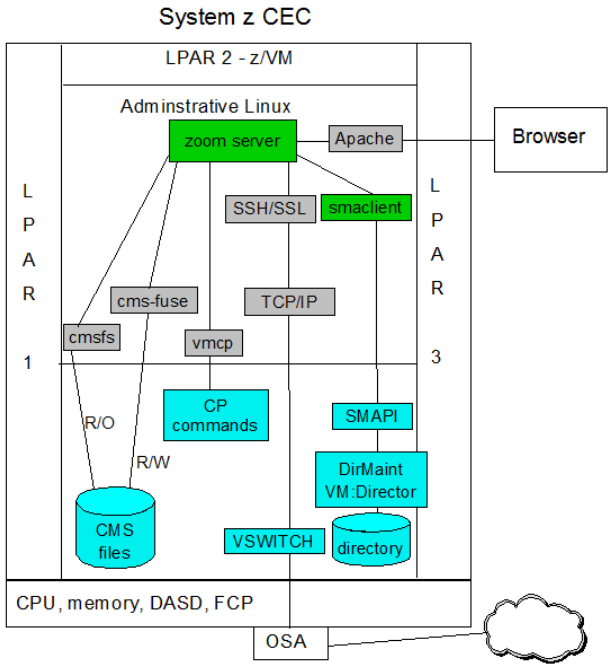
Bringing it all together

- 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
- Added 'full' copying of SSH keys (July 2015)

File system hierarchy



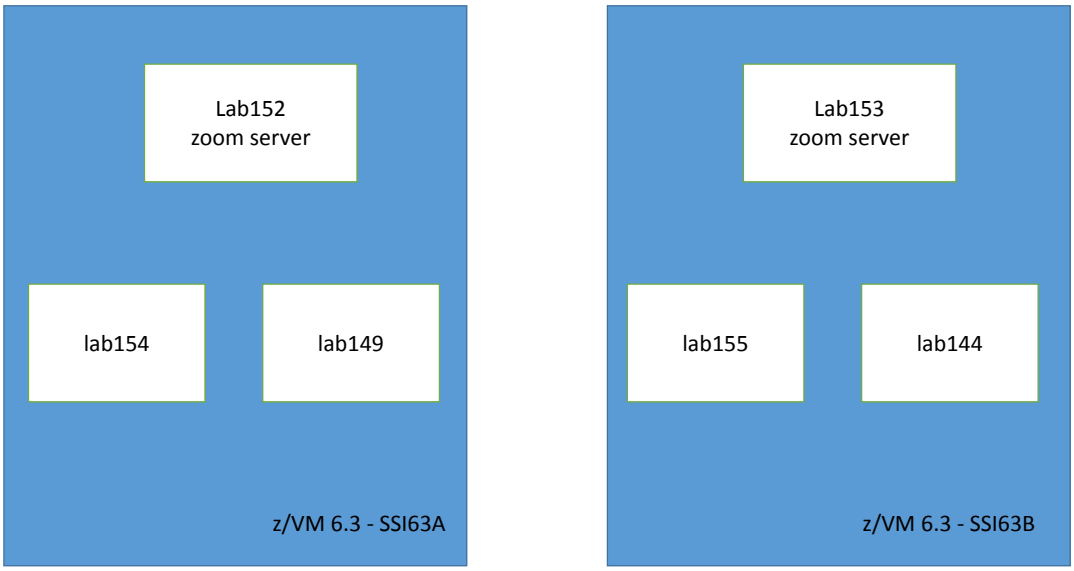
Functional hierarchy



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*** :))

Live demo - zoom no-root SSH key-based authentication



Video and download

- Short 5 minute YouTube video:
  - https://www.youtube.com/watch?v=p19-08aJUEA
- Download the code
  - https://sites.google.com/site/mike99mac/home
    - README.txt
    - Zoom.pdf – the Cookbook
    - Zoom.tgz – the code in tar format
    - Zoom-1-16.s390x.rpm – the code in RPM format

Questions?

- Or discussion?