Setup Ubuntu Linux Base Server Bash Script 20 (Dec 2023)

Starting to put together a script to be converted into Puppet or Chef for setup of server using Bonsaiframework approach.

Being revised 5% complete.

If you don't know what you're doing yet, make sure to follow the expanded instructions.

```
#!/bin/bash
# This is not yet ready to use as an automatic script.


#
# MINIMAL SECURITY ON HOST
#


sudo apt-get install fail2ban
#
# MINIMAL SOFTWARE AND UPDATES to copy and past from this script
#

sudo apt-get --assume-yes install ntp
sudo apt-get update
sudo apt-get --assume-yes dist-upgrade
sudo apt-get --assume-yes install man htop

# on super secure system (ie your host container) you might NOT install
sudo apt-get --assume-yes install wget telnet

#
# allow staff to use sudo
#

# allow staff users to have root access through sudo
sudo su - root
cd /etc/sudoers.d/
sudo wget www.bonsaiframework.com/tscripts/01_enable_sudo_for_staff
sudo chmod o-r /etc/sudoers.d/01_enable_sudo_for_staff
exit
#
# SSH for HOST and CONTAINER
#
# install ssh
sudo apt-get --assume-yes install ssh

# If you have slow ssh connection issues this can mean DNS related to
server hosting system is not working properly.
# In cases where you cannot fix this (ie work environment) then disable.
# Only used FROM option in an authorized_keys file and you want to filter
by names and not just IPs.
# echo '# Disable reverse DNS lookup to prevent slow login' | sudo tee -a
/etc/ssh/sshd_config
# echo 'UseDNS no' | sudo tee -a /etc/ssh/sshd_config
```

```
#
# MINIMAL SOFTWARE ON CONTAINER
# Software below is required to run the other scripts ie download keys
#

sudo apt-get --assume-yes install mlocate wget

#
# ACCOUNTS
#



#
# I should add a setp in here to verify that sudo works with the staff
acounts
# Create Staff Users
sudo useradd -d /home/tin.pham -m -g staff -u 2000 -c "Support Tin Pham" -s
/bin/bash tin.pham
sudo usermod -a -G adm tin.pham
sudo passwd tin.pham
sudo su - tin.pham
mkdir ~/.ssh
chmod 700 ~/.ssh
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
cd ~/.ssh
wget www.bonsaiframework.com/tscripts/publicKey.tin.pham
cat publicKey.tin.pham >> authorized_keys
rm publicKey.tin.pham
exit # make sure to leave the user

sudo useradd -d /home/roderick.fongyee -m -g staff -u 2505 -c "Support
Roderick Fongyee" -s /bin/bash roderick.fongyee
sudo usermod -a -G adm roderick.fongyee
sudo passwd roderick.fongyee
sudo su - roderick.fongyee
mkdir ~/.ssh
chmod 700 ~/.ssh
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
cd ~/.ssh
wget www.bonsaiframework.com/tscripts/publicKey.roderick.fongyee
cat publicKey.roderick.fongyee >> authorized_keys
rm publicKey.roderick.fongyee
exit # make sure to leave the user

sudo addgroup --gid 3000 serveradmin
sudo useradd -d /home/serveradmin -m -g serveradmin -u 3000 -c "Admin
catch-all" -s /bin/bash serveradmin
sudo usermod -a -G adm serveradmin
sudo passwd serveradmin
# add public key here if intention is to allow remote login
```

```
sudo su - serveradmin
mkdir ~/.ssh
chmod 700 ~/.ssh
touch ~/.ssh/authorized_keys
chmod 600 ~/.ssh/authorized_keys
cd ~/.ssh
wget www.bonsaiframework.com/tscripts/publicKey.serveradmin
cat publicKey.serveradmin >> authorized_keys
rm publicKey.serveradmin
exit # make sure to leave the user

#
# SECURE SSH
#


# Currently SSH can use keys, but falls back to passwords if keys fail.
# Once you confirm you can log in successfully with keys AND use sudo with
your account
# Only then, disable passwords to protect from brute force.

# Disable ssh user password authentication.
# Note: not necessary for LXD created images as this is already set to be
no
sudo cp /etc/ssh/sshd_config
/etc/ssh/sshd_config.2011-02-12.v0.0.tinpham_about_to_disable_password_aut
h.bck
# We'll edit quickly with sed
cd /etc/ssh/
sudo sed -i.sedautobck 's/#PasswordAuthentication
yes/PasswordAuthentication no/g' /etc/ssh/sshd_config
# Confirm your change worked. If you get nothing back you are good.
cmp -s $_ $_.sedautobck && echo "sed did not work, your files are
identical."

# restart ssh for the change to take effect,
sudo service ssh restart


# Make sure to try starting a new terminal and connecting with a non-ssh
enabled account.
# You will see the error "Permission denied (publickey).
# Your system is now safer.

################ Leave the default account and log into your main account

#
# CLEANUP
#

# Logout and delete default ubuntu account for containers
# Interesting, in a lxc setup, once my main account was created, left and
logged back in, it appeared to automatically delete default ubuntu user.
```

```
# Test this scenario again.
sudo userdel -r ubuntu
sudo userdel -r setupadmin

# Make sure to reboot for any kernel updates to take effect
sudo reboot


# Clean Up
sudo apt-get autoclean # use this if you only want to clean out nolonger
used packages
sudo apt-get clean # clean out all downloaded packages - I usually use this
one
sudo apt-get autoremove # cleans out unused packages

# Setup firewall
```

```
# .... however is following this next add the instructions here
```