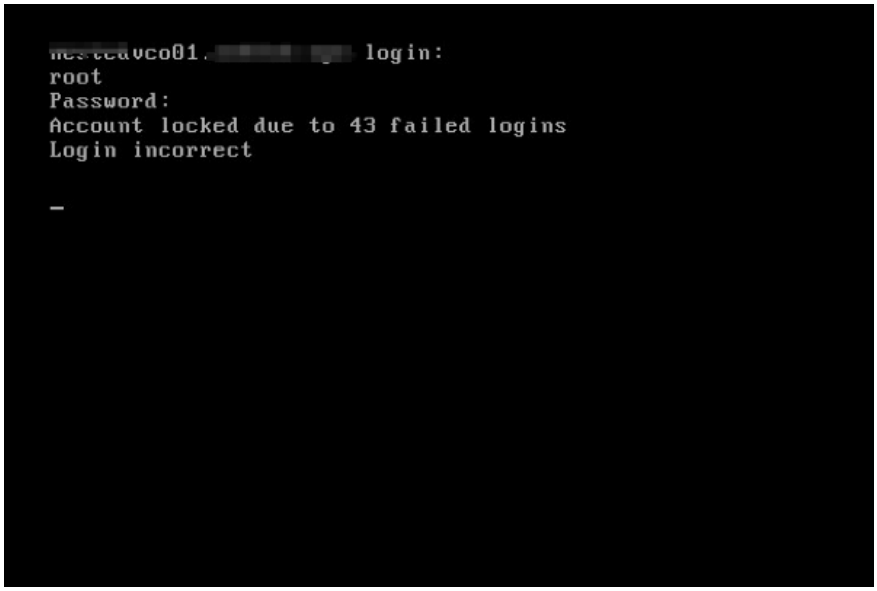
Reset root password

vRealize Orchestrator 7.# - Unlocking vRO Root Account after too many failed login attempts

Recently I tried to access one of my many vRO Server and noticed the root account was locked out due to too many tries. If you are here because of root account lockout, this post will walk you through unlocking root account and resetting password.

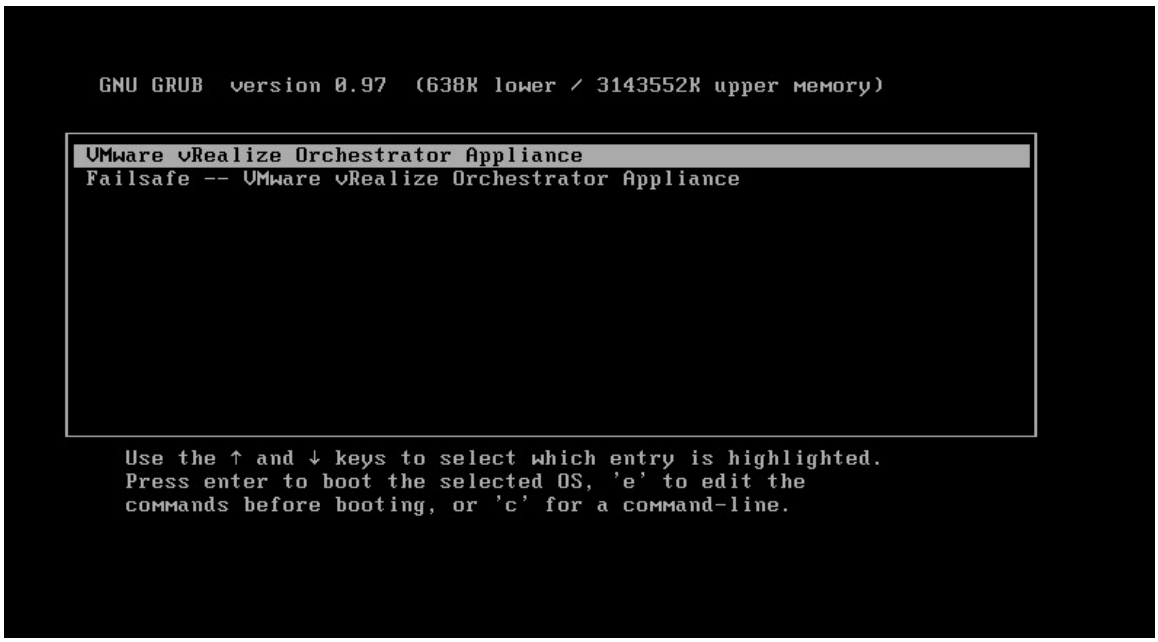


As you can see account was locked due to 43 failed logins, account will not unlock itself after a day.

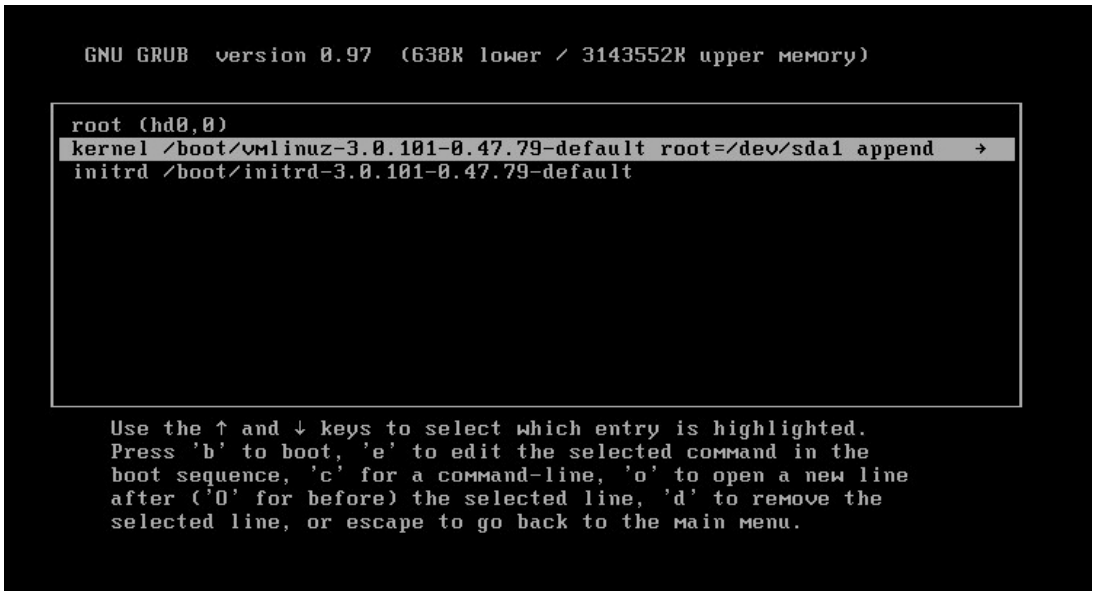
Pre-Requesites:
- Need console access to the vRO server. SSH will not work (I am clueless of why so many post are telling to login using ssh when the account is locked. I am missing something)

Step 1 - Gain access vRO server root shell via Console

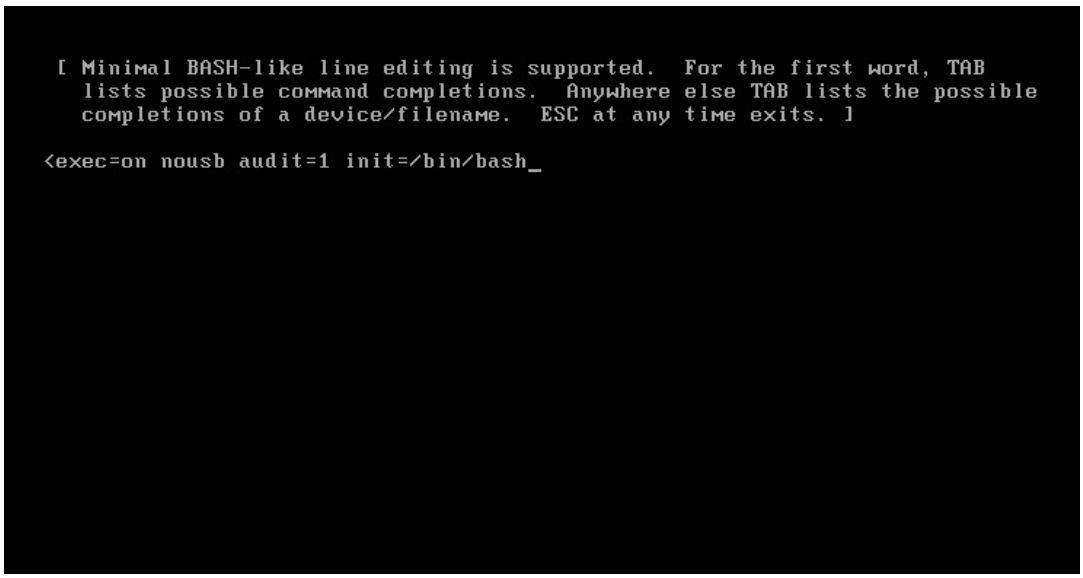
1 - Access the vRO server via vSphere Console and reboot server. When the GRUB bootloaders appears, press spacebar to disable autoboot.



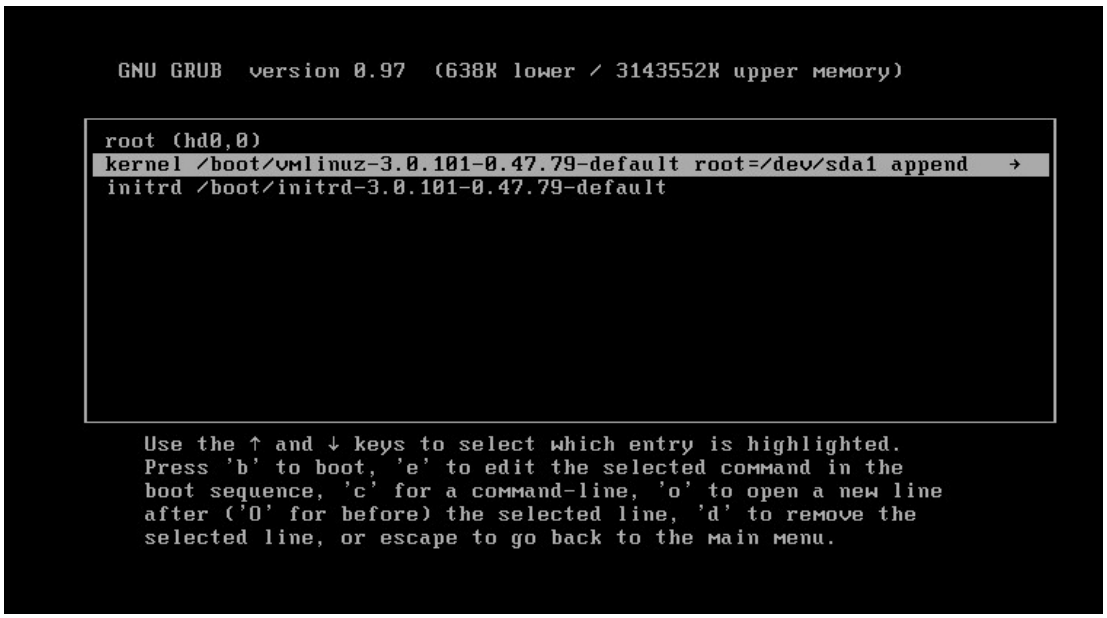
2 - Select VMware vRealize Orchestrator Appliance and type ?e? to edit the boot commands. Then move down to the second line showing kernel boot parameter and type ?e? again.



3 - Append the **init=/bin/bash** to the kernel options.



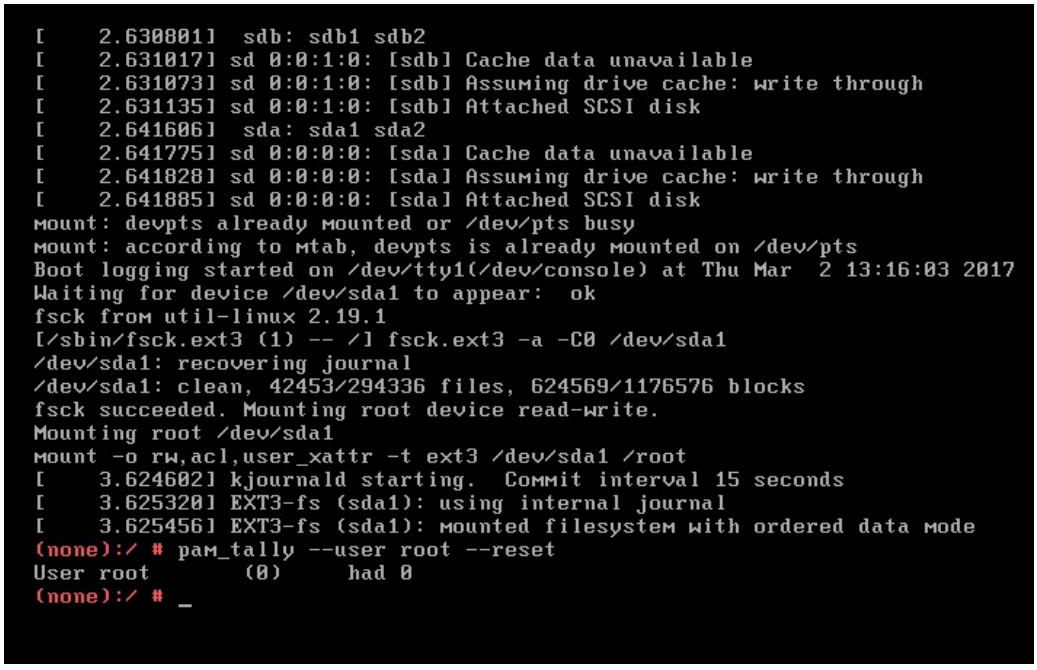
4 - Hit Enter and the GRUB menu will appear again. This time hit ?b? to start the boot process.



5 - Now you should be in the shell - ready to issue commans to unlock or reset password.

Step 2 - Unlock and Reset vRO ?root? account

1 - To unlock account use type following command: **# pam_tally - -user root - -reset** (double dashes together) . Same command can be used to unlock any other account.

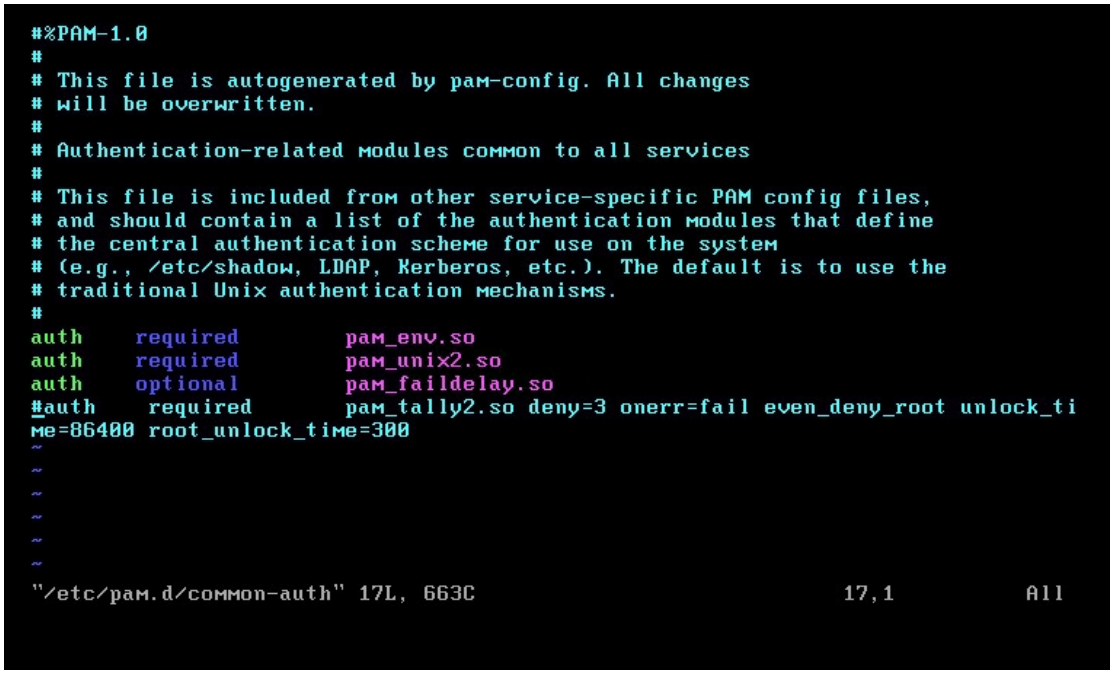


2 - If you cannot remember the password change password by using passwd command: # passwd root
Enter your new password twice.
3 - Reboot the appliance by running reboot command.
Note: If reboot not working issue following commands:
mkfifo /dev/initct
reboot -f

Step 3 - Disable automated lockout policy (optional)

I find this extremely annoying specially in my DEV environment so disabling the lock out possible comes in handy. to do so modify the **/etc/pam.d/common-auth** file.

1 - Use vi or any preferred editor to modify the **common-auth** file. Comment out the line where ?pam_tally2.so deny=3?.? as shown in picture.



2 - Save file. If using **vi** editor. Esc then type **:wq!**

3 - Reboot the appliance by running reboot command.
Note: If reboot not working issue following commands:
mkfifo /dev/initct
reboot -f
This should should take care of vRO ?root? account lockouts.