

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.

```
mes-vaavco01. [REDACTED] login:  
root  
Password:  
Account locked due to 43 failed logins  
Login incorrect  
  
-
```

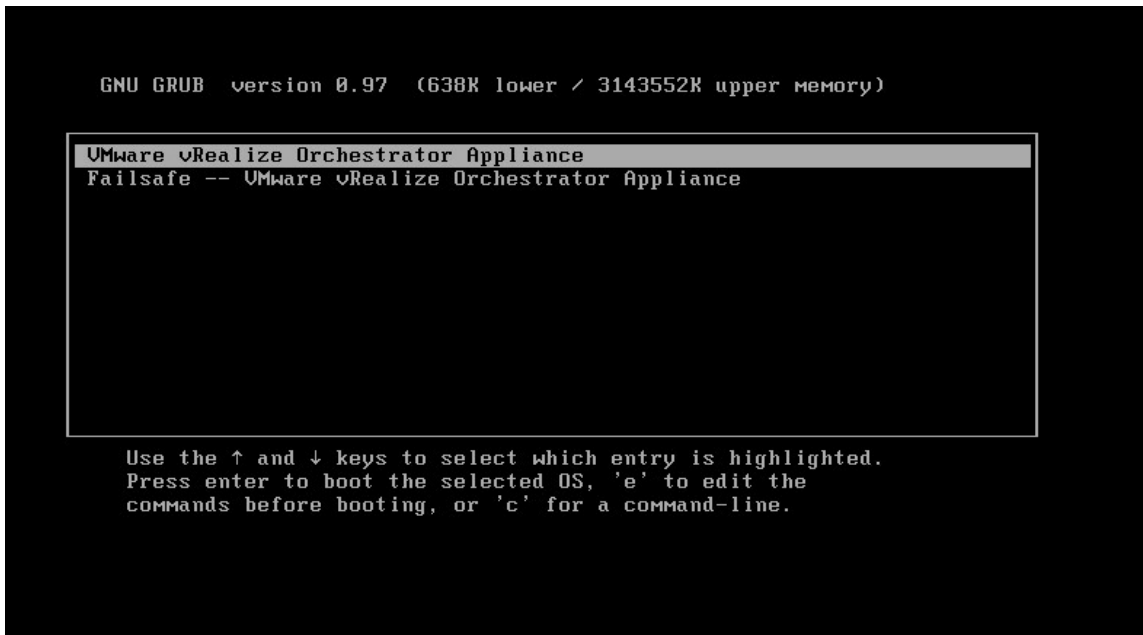
As you can see account was locked due to 43 failed logins, account will not unlock itself after a day.

Pre-Requisites:

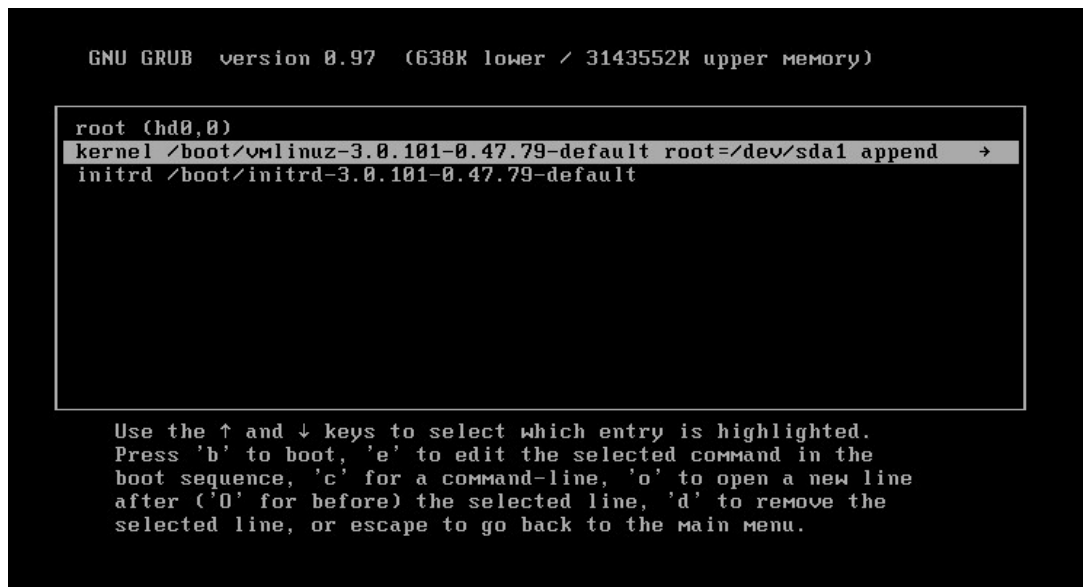
- Need console access to the vRO server. SSH will not work (I am clueless of why so many post are telling to login using ssh when the account is locked. I am missing something)

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.

```
[ Minimal BASH-like line editing is supported. For the first word, TAB
  lists possible command completions. Anywhere else TAB lists the possible
  completions of a device/filename. ESC at any time exits. ]
```

```
<exec=on nousb audit=1 init=/bin/bash_
```

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

```
GNU GRUB version 0.97 (638K lower / 3143552K upper memory)
```

```
root (hd0,0)
kernel /boot/vmlinuz-3.0.101-0.47.79-default root=/dev/sda1 append →
initrd /boot/initrd-3.0.101-0.47.79-default
```

```
Use the ↑ and ↓ keys to select which entry is highlighted.
Press 'b' to boot, 'e' to edit the selected command in the
boot sequence, 'c' for a command-line, 'o' to open a new line
after ('O' for before) the selected line, 'd' to remove the
selected line, or escape to go back to the main menu.
```

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

```

[ 2.630083] sd 0:0:1:0: [sdb] Cache data unavailable
[ 2.630138] sd 0:0:1:0: [sdb] Assuming drive cache: write through
[ 2.630801] sdb: sdb1 sdb2
[ 2.631017] sd 0:0:1:0: [sdb] Cache data unavailable
[ 2.631073] sd 0:0:1:0: [sdb] Assuming drive cache: write through
[ 2.631135] sd 0:0:1:0: [sdb] Attached SCSI disk
[ 2.641606] sda: sda1 sda2
[ 2.641775] sd 0:0:0:0: [sda] Cache data unavailable
[ 2.641828] sd 0:0:0:0: [sda] Assuming drive cache: write through
[ 2.641885] sd 0:0:0:0: [sda] Attached SCSI disk
mount: devpts already mounted or /dev/pts busy
mount: according to mtab, devpts is already mounted on /dev/pts
Boot logging started on /dev/tty1(/dev/console) at Thu Mar 2 13:16:03 2017
Waiting for device /dev/sda1 to appear: ok
fsck from util-linux 2.19.1
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a -C0 /dev/sda1
/dev/sda1: recovering journal
/dev/sda1: clean, 42453/294336 files, 624569/1176576 blocks
fsck succeeded. Mounting root device read-write.
Mounting root /dev/sda1
mount -o rw,acl,user_xattr -t ext3 /dev/sda1 /root
[ 3.624602] kjournald starting. Commit interval 15 seconds
[ 3.625320] EXT3-fs (sda1): using internal journal
[ 3.625456] EXT3-fs (sda1): mounted filesystem with ordered data mode
(none):/ # _

```

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.

```

[ 2.630801] sdb: sdb1 sdb2
[ 2.631017] sd 0:0:1:0: [sdb] Cache data unavailable
[ 2.631073] sd 0:0:1:0: [sdb] Assuming drive cache: write through
[ 2.631135] sd 0:0:1:0: [sdb] Attached SCSI disk
[ 2.641606] sda: sda1 sda2
[ 2.641775] sd 0:0:0:0: [sda] Cache data unavailable
[ 2.641828] sd 0:0:0:0: [sda] Assuming drive cache: write through
[ 2.641885] sd 0:0:0:0: [sda] Attached SCSI disk
mount: devpts already mounted or /dev/pts busy
mount: according to mtab, devpts is already mounted on /dev/pts
Boot logging started on /dev/tty1(/dev/console) at Thu Mar 2 13:16:03 2017
Waiting for device /dev/sda1 to appear: ok
fsck from util-linux 2.19.1
[/sbin/fsck.ext3 (1) -- /] fsck.ext3 -a -C0 /dev/sda1
/dev/sda1: recovering journal
/dev/sda1: clean, 42453/294336 files, 624569/1176576 blocks
fsck succeeded. Mounting root device read-write.
Mounting root /dev/sda1
mount -o rw,acl,user_xattr -t ext3 /dev/sda1 /root
[ 3.624602] kjournald starting. Commit interval 15 seconds
[ 3.625320] EXT3-fs (sda1): using internal journal
[ 3.625456] EXT3-fs (sda1): mounted filesystem with ordered data mode
(none):/ # pam_tally --user root --reset
User root      (0)      had 0
(none):/ # _

```

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.

```
##PAM-1.0
#
# This file is autogenerated by pam-config. All changes
# will be overwritten.
#
# Authentication-related modules common to all services
#
# This file is included from other service-specific PAM config files,
# and should contain a list of the authentication modules that define
# the central authentication scheme for use on the system
# (e.g., /etc/shadow, LDAP, Kerberos, etc.). The default is to use the
# traditional Unix authentication mechanisms.
#
auth    required      pam_env.so
auth    required      pam_unix2.so
auth    optional      pam_faildelay.so
#auth   required      pam_tally2.so deny=3 onerr=fail even_deny_root unlock_t
me=86400 root_unlock_time=300
~
~
~
~
~
~
"/etc/pam.d/common-auth" 17L, 663C          17,1          All
```

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.