

How to Secure CENTOS 7.1

Part 1

Motivation

This paper will be a multi-part series on securing CentOS Linux 7.1. This idea has been toiling around my head for almost a year and now is the time to get it into print and share with the community. If you have comments or feedback on how I can represent this better, please email me your ideas to the email address listed on the website (securityhardening.com).

Install the Operating System

There is no reason to go into detail about the OS install. CentOS has good documentation on how to install their OS. Below are a couple of screen shots as to how I installed my test system.



Figure 1

By default, the "Test this media & install CentOS 7" line will be highlighted. If you have performed a hash checksum check of the ISO, then choose the top line, "Install CentOS 7" and press Enter.

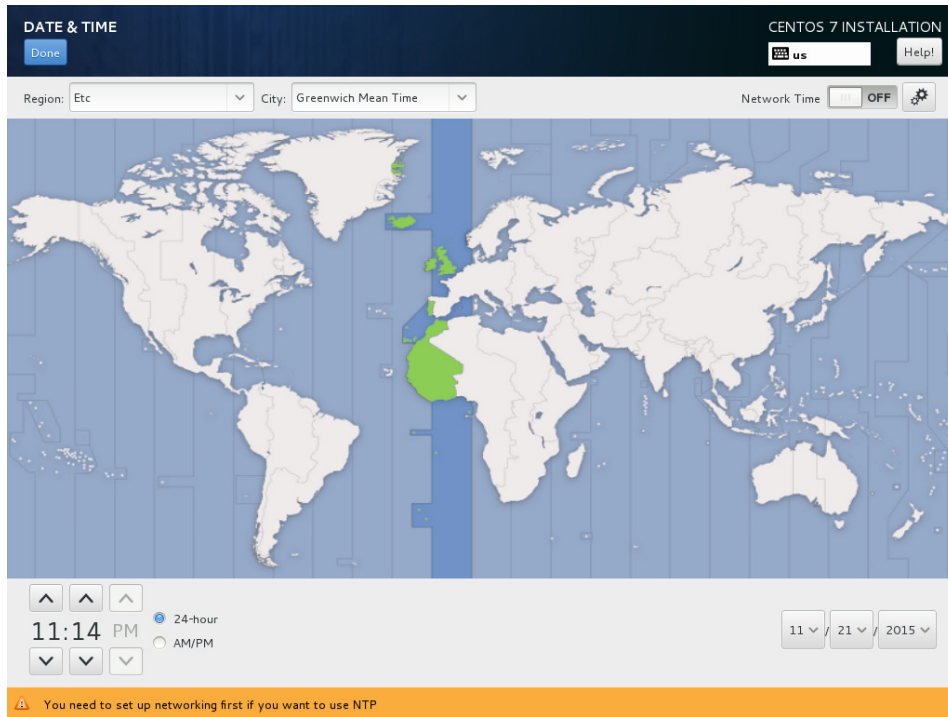


Figure 2

After many years of data center and enterprise solutions, I now always set the timezone to either GMT or UTC. Your applications can be modified for the time to your current location. However, the wave of the future is deploying servers in zones that could be anywhere on the planet in the cloud. This will serve your sanity well.

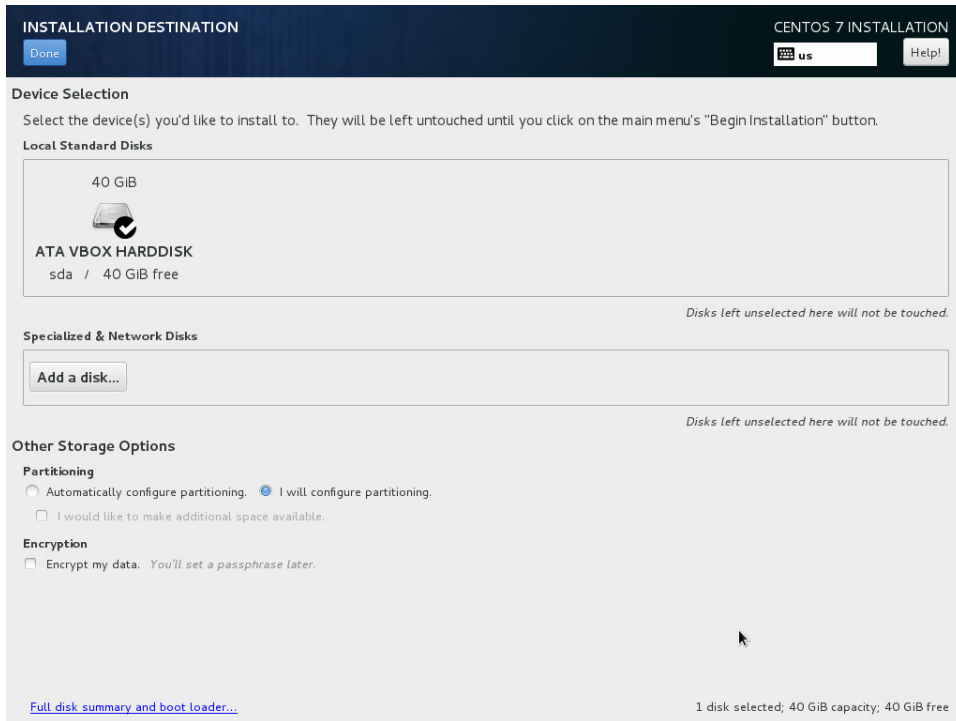


Figure 3

Choose to create your own partitions.

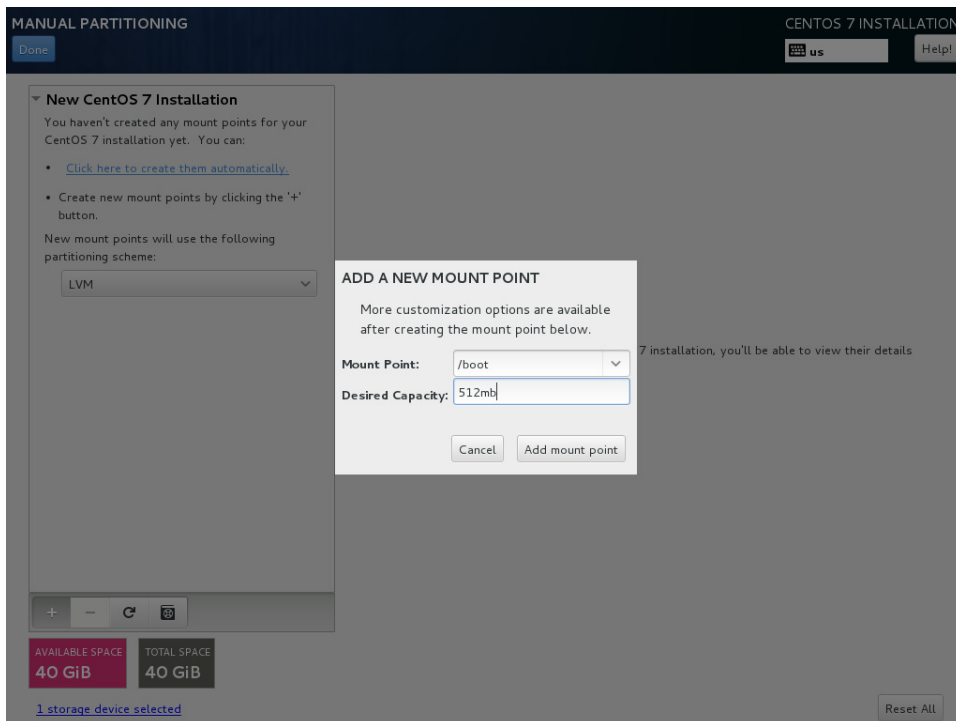


Figure 4

Figure 4, you have to have a boot partition, set around 512 MB for the size.

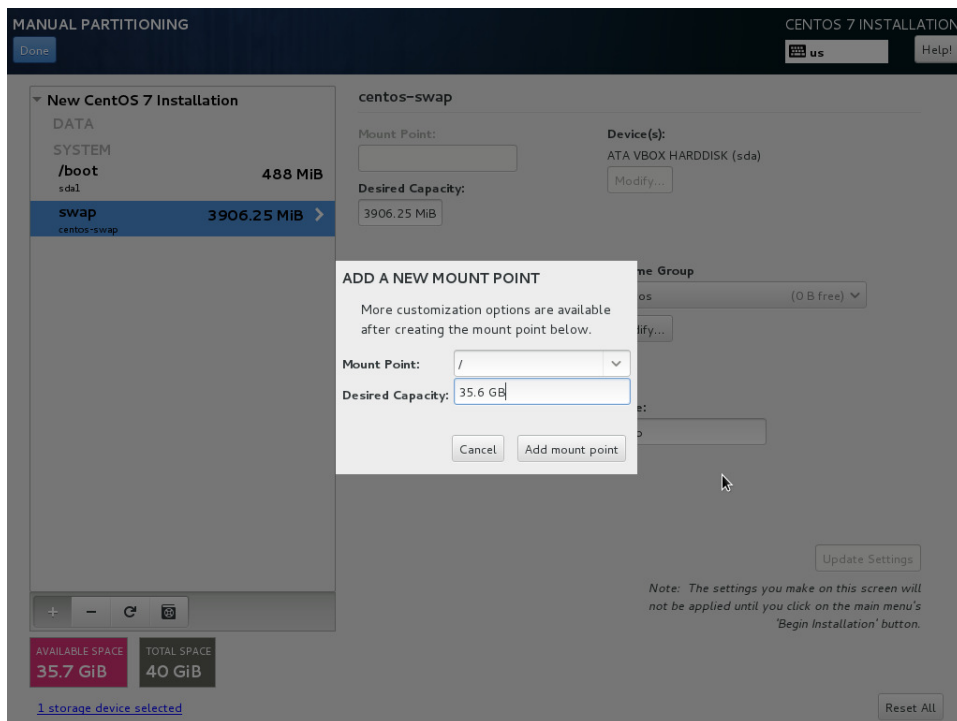


Figure 5

Figure 5, create a swap partition of 4096 MB. Then create a / drive with the rest of the disk space available.

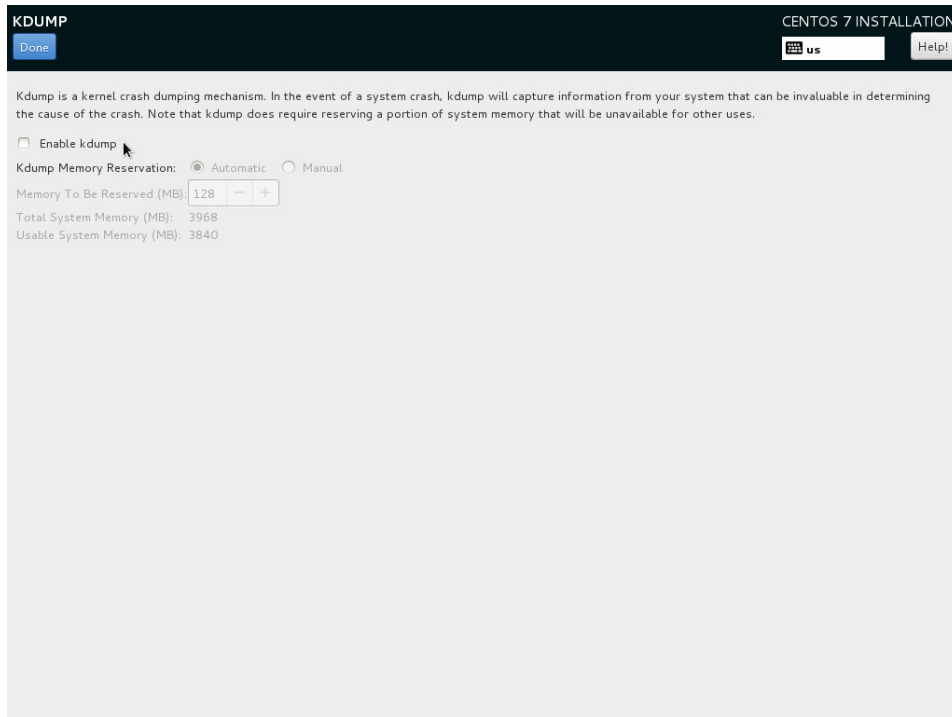


Figure 6

Go into KDUMP and disable kdump. You can re-enable it again in the future if you actually need it to debug kernel level problems.

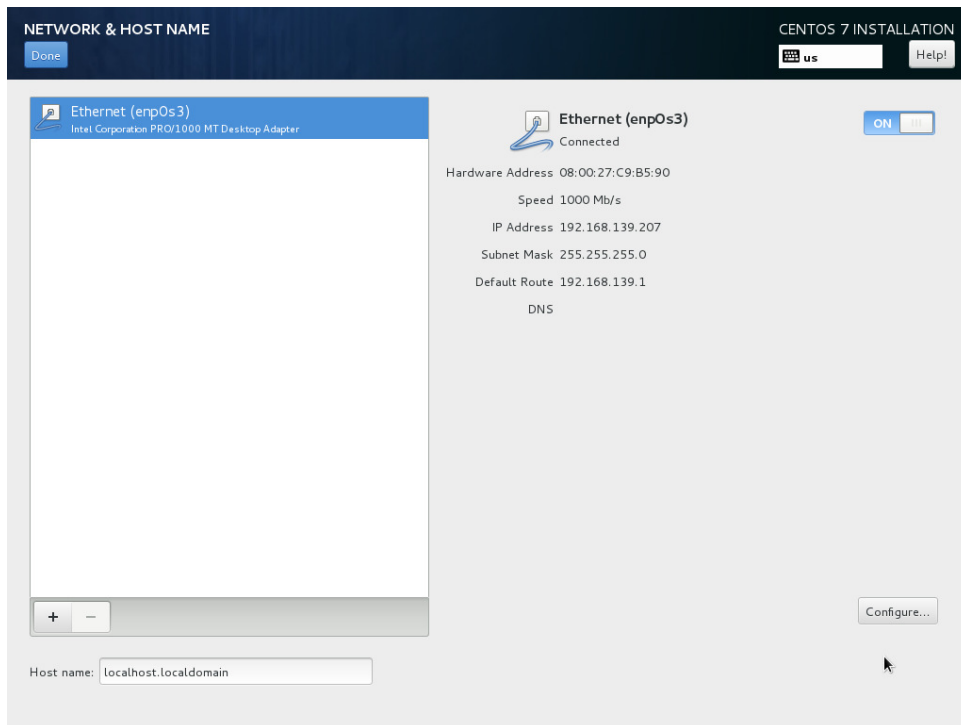


Figure 7

Go into your network settings and set your hostname and configure the interface.

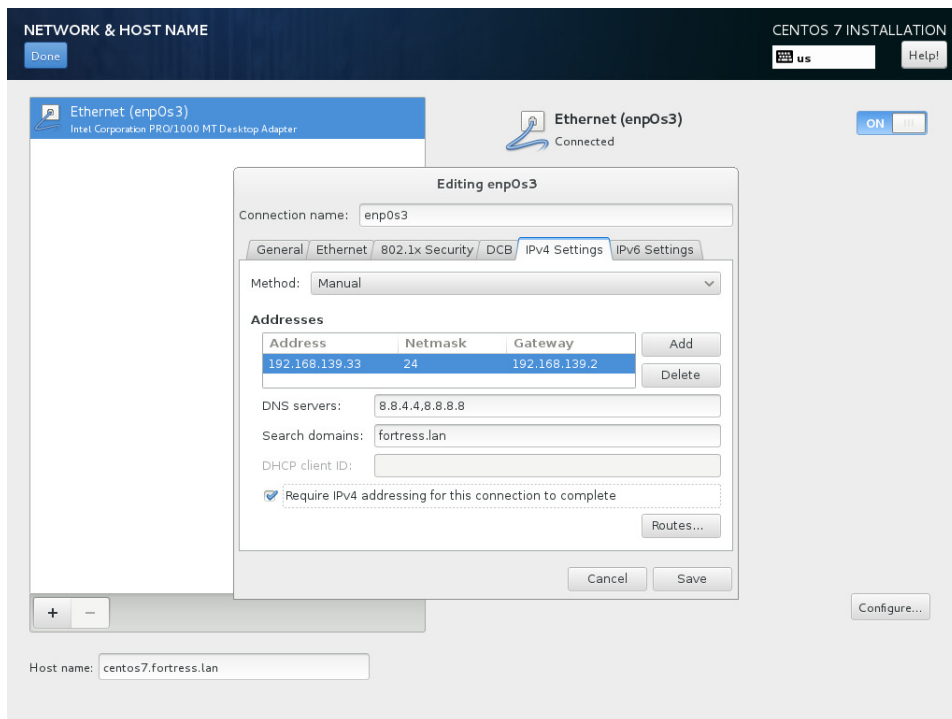


Figure 8

Figure 8, I like to manually set my IP address. This pattern of forcibly setting your IP address will go away in the very near future as the IP protocol, “Software Defined Networks” matures and becomes more prevalent. Reference: <http://www.cisco.com/web/solutions/trends/sdn/index.html>

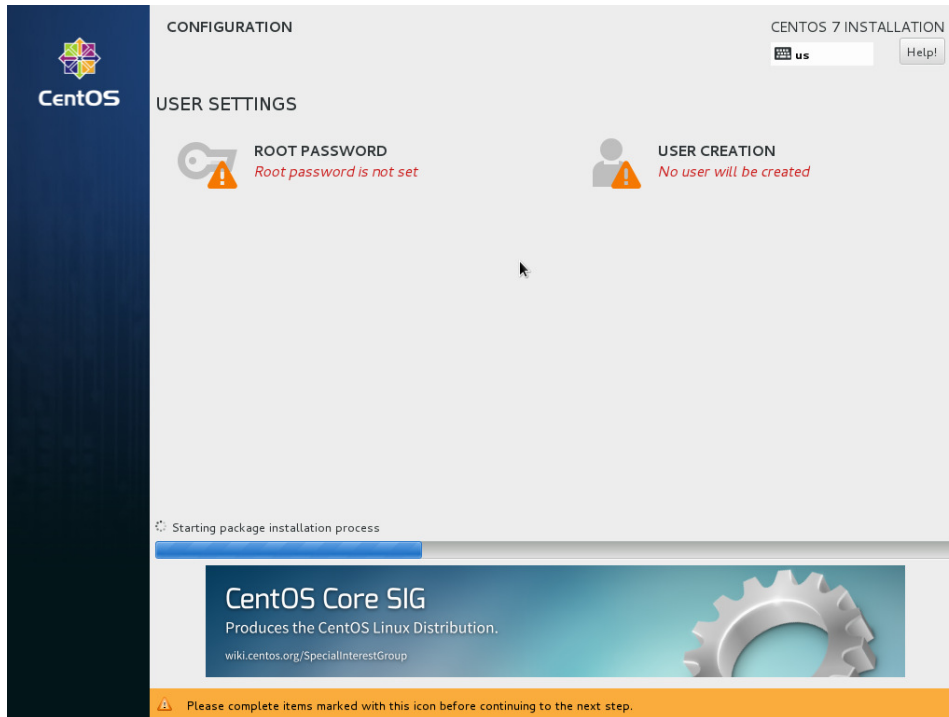


Figure 9

Figure 9, depress the Root Password button and set a solid root password that is greater than 16 characters.

CREATE USER CENTOS 7 INSTALLATION

[Done](#) [Help!](#)

Full name

User name

Tip: Keep your user name shorter than 32 characters and do not use spaces.

Make this user administrator

Require a password to use this account

Password

Weak

Confirm password

[Advanced...](#)

⚠ The password you have provided is weak. You will have to press Done twice to confirm it.

Figure 10

Figure 10, select the User Creation button in Figure 9, and then input your information to create a new account that will also be your primary admin account.

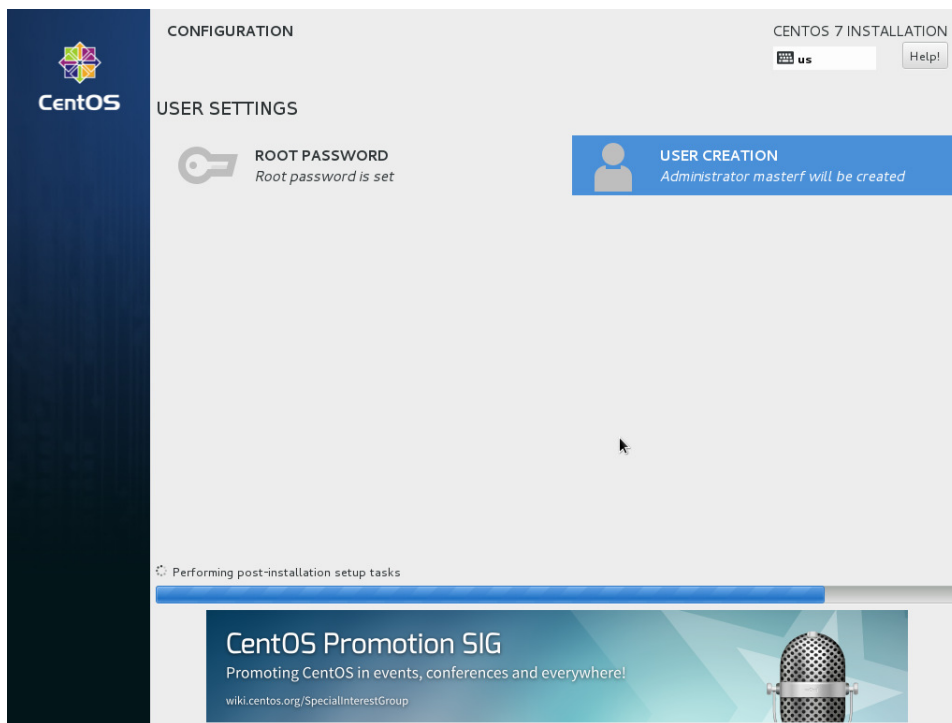


Figure 11

Figure 11, at the end of the install, click on the reboot icon.

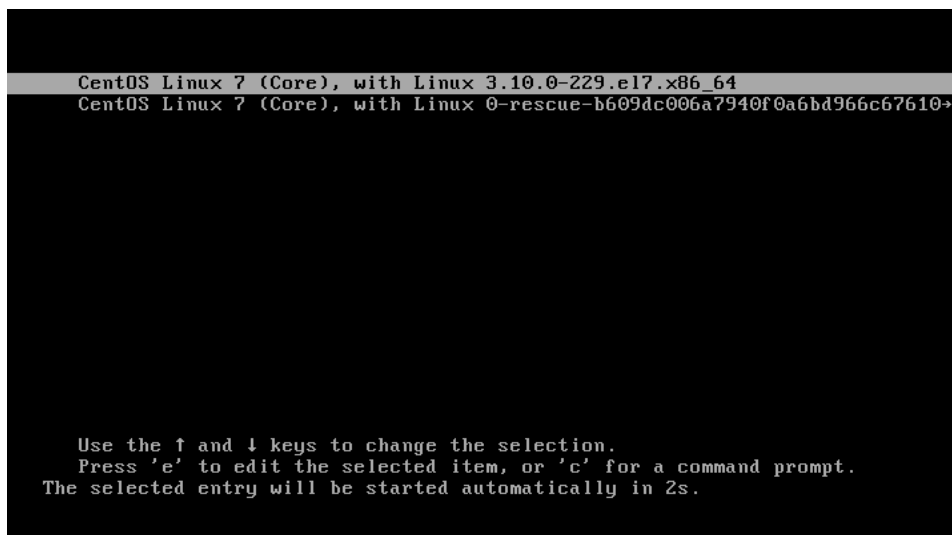


Figure 12

Figure 12, just choose the defaults.

```
CentOS Linux 7 (Core)
Kernel 3.10.0-229.el7.x86_64 on an x86_64

centos7 login: _
```

Figure 13

Figure 13, reboot successful. You are now ready to secure your new installation.

Secure the Boot Loader

Run the command as the root user, `grub2-mkpasswd-pbkdf2`.

This will produce the following output.

```
[root@centos7 aide]# grub2-mkpasswd-pbkdf2
Password:
Reenter password:
PBKDF2 hash of your password is
grub.pbkdf2.sha512.10000.14B9F271C0EF8BB772DAFFD9F05FE49E8B9438BCCD7A1BD3BF26
C012A4D0F7684EA05DB1134809342C34DFA63A59E6334167AB438D4F7EC057D7B95DE9D6F5DD.
85AD355E9F9129E0ADA1F60046C9FC6E87CFE2780C5D5A2572FBAE876A11BBE20F1B4DCC7AF03
CB566ED722C1714B4F9A22BB81D01D84BD52EC1147301F74F2F
[root@centos7 aide]#
```

Copy the password into your buffer and then open `/etc/grub.d/40_custom`. Add the password line.

```
set superusers="masterf"
password_pbkdf2 masterf
grub.pbkdf2.sha512.10000.14B9F271C0EF8BB772DAFFD9F05FE49E8B9438BCCD7A1BD3BF26
C012A4D0F7684EA05DB1134809342C34DFA63A59E6334167AB438D4F7EC057D7B95DE9D6F5DD.
85AD355E9F9129E0ADA1F60046C9FC6E87CFE2780C5D5A2572FBAE876A11BBE20F1B4DCC7AF03
CB566ED722C1714B4F9A22BB81D01D84BD52EC1147301F74F2F
```

A word to the wise, setting the grub password only protects the OS from booting to a different kernel. If a malicious person has physical access to the server, they can boot from a bootable Linux DVD/CD and manipulate the file system any way they choose. Therefore make sure the physical location of the server is secured and depending on the value of the data, only authorized users are capable of booting the system.

Minimize the Boot Sequence

Chkconfig is almost dead, now you get to run systemctl list-unit-files.

```
[root@centos7 aide]# systemctl list-unit-files
UNIT FILE                                STATE
proc-sys-fs-binfmt_misc.automount       static
dev-hugepages.mount                     static
dev-mqueue.mount                         static
proc-sys-fs-binfmt_misc.mount           static
sys-fs-fuse-connections.mount           static
sys-kernel-config.mount                  static
sys-kernel-debug.mount                   static
tmp.mount                                disabled
brandbot.path                            disabled
systemd-ask-password-console.path       static
systemd-ask-password-plymouth.path      static
systemd-ask-password-wall.path          static
session-1.scope                          static
session-2.scope                          static
auditd.service                           enabled
autovt@.service                          disabled
blk-availability.service                 disabled
brandbot.service                         static
console-getty.service                   disabled
console-shell.service                   disabled
cpupower.service                        disabled
crond.service                            enabled
dbus-org.fedoraproject.FirewallD1.service enabled
dbus-org.freedesktop.hostname1.service  static
dbus-org.freedesktop.locale1.service    static
dbus-org.freedesktop.login1.service     static
dbus-org.freedesktop.machine1.service   static
dbus-org.freedesktop.NetworkManager.service enabled
dbus-org.freedesktop.nm-dispatcher.service enabled
dbus-org.freedesktop.timedate1.service  static
dbus.service                             static
debug-shell.service                     disabled
dm-event.service                        disabled
dnsmasq.service                          disabled
dracut-cmdline.service                   static
dracut-initqueue.service                 static
dracut-mount.service                     static
dracut-pre-mount.service                 static
dracut-pre-pivot.service                 static
dracut-pre-trigger.service               static
dracut-pre-udev.service                  static
dracut-shutdown.service                  static
ebtables.service                         disabled
emergency.service                        static
firewalld.service                        enabled
getty@.service                           enabled
halt-local.service                       static
initrd-cleanup.service                   static
initrd-parse-etc.service                 static
initrd-switch-root.service               static
initrd-udevadm-cleanup-db.service        static
```

iprdump.service	disabled
iprinit.service	disabled
iprupdate.service	disabled
irqbalance.service	enabled
kdump.service	disabled
kmod-static-nodes.service	static
lvm2-lvmetad.service	disabled
lvm2-monitor.service	enabled
lvm2-pvscan@.service	static
messagebus.service	static
microcode.service	enabled
NetworkManager-dispatcher.service	enabled
NetworkManager-wait-online.service	disabled
NetworkManager.service	enabled
plymouth-halt.service	disabled
plymouth-kexec.service	disabled
plymouth-poweroff.service	disabled
plymouth-quit-wait.service	disabled
plymouth-quit.service	disabled
plymouth-read-write.service	disabled
plymouth-reboot.service	disabled
plymouth-start.service	disabled
plymouth-switch-root.service	static
polkit.service	static
postfix.service	enabled
quotaon.service	static
rc-local.service	static
rdisc.service	disabled
rdma.service	disabled
rescue.service	static
rhel-autorelabel-mark.service	static
rhel-autorelabel.service	static
rhel-configure.service	static
rhel-dmesg.service	disabled
rhel-domainname.service	disabled
rhel-import-state.service	static
rhel-loadmodules.service	static
rhel-readonly.service	static
rsyslog.service	enabled
serial-getty@.service	disabled
sshd-keygen.service	static
sshd.service	enabled
sshd@.service	static
systemd-ask-password-console.service	static
systemd-ask-password-plymouth.service	static
systemd-ask-password-wall.service	static
systemd-backlight@.service	static
systemd-binfmt.service	static
systemd-fsck-root.service	static
systemd-fsck@.service	static
systemd-halt.service	static
systemd-hibernate.service	static
systemd-hostnamed.service	static
systemd-hybrid-sleep.service	static
systemd-initctl.service	static
systemd-journal-flush.service	static
systemd-journald.service	static

systemd-kexec.service	static
systemd-locale.service	static
systemd-logind.service	static
systemd-machined.service	static
systemd-modules-load.service	static
systemd-nspawn@.service	disabled
systemd-poweroff.service	static
systemd-quotacheck.service	static
systemd-random-seed.service	static
systemd-readahead-collect.service	enabled
systemd-readahead-done.service	static
systemd-readahead-drop.service	enabled
systemd-readahead-replay.service	enabled
systemd-reboot.service	static
systemd-remount-fs.service	static
systemd-shutdown.service	static
systemd-suspend.service	static
systemd-sysctl.service	static
systemd-timedated.service	static
systemd-tmpfiles-clean.service	static
systemd-tmpfiles-setup-dev.service	static
systemd-tmpfiles-setup.service	static
systemd-udev-settle.service	static
systemd-udev-trigger.service	static
systemd-udevd.service	static
systemd-update-utmp-runlevel.service	static
systemd-update-utmp.service	static
systemd-user-sessions.service	static
systemd-vconsole-setup.service	static
tcstd.service	disabled
teamd@.service	static
tuned.service	enabled
wpa_supplicant.service	disabled
-.slice	static
machine.slice	static
system.slice	static
user.slice	static
dbus.socket	static
dm-event.socket	enabled
lvm2-lvmetad.socket	enabled
sshd.socket	disabled
syslog.socket	static
systemd-initctl.socket	static
systemd-journald.socket	static
systemd-shutdown.socket	static
systemd-udev-control.socket	static
systemd-udev-kernel.socket	static
basic.target	static
bluetooth.target	static
cryptsetup.target	static
ctrl-alt-del.target	disabled
default.target	enabled
emergency.target	static
final.target	static
getty.target	static
graphical.target	disabled
halt.target	disabled

hibernate.target	static
hybrid-sleep.target	static
initrd-fs.target	static
initrd-root-fs.target	static
initrd-switch-root.target	static
initrd.target	static
iprutils.target	disabled
kexec.target	disabled
local-fs-pre.target	static
local-fs.target	static
multi-user.target	enabled
network-online.target	static
network.target	static
nss-lookup.target	static
nss-user-lookup.target	static
paths.target	static
poweroff.target	disabled
printer.target	static
reboot.target	disabled
remote-fs-pre.target	static
remote-fs.target	enabled
rescue.target	disabled
rpcbind.target	static
runlevel0.target	disabled
runlevel1.target	disabled
runlevel2.target	disabled
runlevel3.target	disabled
runlevel4.target	disabled
runlevel5.target	disabled
runlevel6.target	disabled
shutdown.target	static
sigpwr.target	static
sleep.target	static
slices.target	static
smartcard.target	static
sockets.target	static
sound.target	static
suspend.target	static
swap.target	static
sysinit.target	static
system-update.target	static
time-sync.target	static
timers.target	static
umount.target	static
systemd-readahead-done.timer	static
systemd-tmpfiles-clean.timer	static

211 unit files listed.

[root@centos7 aide]#

As an administrator, you should be able to determine what services are necessary for your business use. Playing along, let's say you determine that the remote-fs service is not necessary, run the following command:

```
[root@centos7 aide]# systemctl disable remote-fs.target
rm '/etc/systemd/system/multi-user.target.wants/remote-fs.target'
[root@centos7 aide]#
```

Minimize the services down to the smallest amount for the server to run.

Secure the Console and Virtual Terminals

Modify the security file (/etc/securitytty) for the console and make it look like this:

```
[root@centos7 etc]# cat securitytty
console
vc/1
#vc/2
#vc/3
#vc/4
#vc/5
#vc/6
#vc/7
#vc/8
#vc/9
#vc/10
#vc/11
tty1
#tty2
#tty3
#tty4
#tty5
#tty6
#tty7
#tty8
#tty9
#tty10
#tty11
[root@centos7 etc]#
```

For the Virtual Consoles add the rpm vlock the system and use:

To lock the virtual consoles:

```
[root@centos7 ~]# vlock -c
This TTY is now locked.
Please enter the password to unlock.
root's Password:
```

Or as a user account:

```
[masterf@centos7 ~]$ vlock -c
This TTY is now locked.
Please enter the password to unlock.
masterf's Password:
[masterf@centos7 ~]$
```

To lock all virtual consoles:

```
vlock -a
```

Set a Warning Banner

Run these commands to zero out the following files:

```
[root@centos7 etc]# > /etc/issue
```

```
[root@centos7 etc]# > /etc/issue.net  
[root@centos7 etc]# > /etc/motd  
[root@centos7 etc]#
```

Set /etc/issue to look like this:

```
^[c  
\d at \t  
Access to this computer system is for authorized personnel only.  
Unauthorized use or access to this system is regarded as a  
criminal act and is subject to civil and criminal prosecution.  
User activities on this system may be monitored without prior notice.
```

To get the “^[c” symbol set correctly, depress “CTRL+v+[“ then add the lower case c.

Then set /etc/issue.net to look like this:

```
Access to this computer system is for authorized personnel only.  
Unauthorized use or access to this system is regarded as a  
criminal act and is subject to civil and criminal prosecution.  
User activities on this system may be monitored without prior notice.
```

Groups to remove

Here is the default list of groups on a vanilla install (don't remove all of these):

```
root:x:0:  
bin:x:1:  
daemon:x:2:  
sys:x:3:  
adm:x:4:  
tty:x:5:  
disk:x:6:  
lp:x:7:  
mem:x:8:  
kmem:x:9:  
wheel:x:10:masterf  
cdrom:x:11:  
mail:x:12:postfix  
man:x:15:  
dialout:x:18:  
floppy:x:19:  
games:x:20:  
tape:x:30:  
video:x:39:  
ftp:x:50:  
lock:x:54:  
audio:x:63:  
nobody:x:99:  
users:x:100:  
utmp:x:22:  
utempter:x:35:
```



```
avahi-autoipd:x:170:
ssh_keys:x:999:
systemd-journal:x:190:
dbus:x:81:
polkitd:x:998:
tss:x:59:
dip:x:40:
postdrop:x:90:
postfix:x:89:
sshd:x:74:
masterf:x:1000:masterf
vboxsf:x:997:
```

Depending on the server's configuration, a lot of these groups are not needed. I'm going to remove:

dialout, dip, floppy, and tape

Therefore as root, I can run:

```
for X in dialout dip floppy tape; do groupdel $X; done
```

If you get an error, manually delete the group's line out of /etc/group.

Clean out /etc/passwd and /etc/shadow as necessary. You could delete the users first and then you won't get the error messages from groupdel. Your call as to how you wish to perform this. Another thought that I should share is /etc/passwd has a lot of these accounts set with the shell of /sbin/nologin. If you choose to leave these accounts, make sure they have their shells set to nologin. The benefit of having this set is that if an attacker tries to use these accounts, they will log to /var/log/messages with an error (therefore alerting you that someone is trying to break into your system with that or those accounts). Again, the overarching theme for this labor is small is beautiful; hence the focus on removing unneeded accounts and groups.

Securing Passwords

Password complexity and setting rules used to be a pain in the arse. Now days with PAM, this is much less arduous.

New /etc/pam.d/passwd-auth-ac

```
# %%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      required      pam_faillock.so preauth silent audit deny=3 even_deny_root unlock_time=600
auth      sufficient    pam_unix.so nullok try_first_pass
auth      [default=die] pam_faillock.so authfail audit deny=3 even_deny_root unlock_time=600
auth      requisite     pam_succeed_if.so uid >= 1000 quiet_success
auth      required      pam_deny.so

account   required      pam_unix.so
account   required      pam_faillock.so
account   sufficient    pam_localuser.so
account   sufficient    pam_succeed_if.so uid < 1000 quiet
account   required      pam_permit.so

password requisite     pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password sufficient    pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password required      pam_deny.so

session  optional      pam_keyinit.so revoke
session  required    pam_limits.so
-session optional      pam_systemd.so
```

```
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
```

New /etc/pam.d/ system-auth-ac

```
##%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth required pam_env.so
auth required pam_faillock.so preauth silent audit deny=3 even_denied_root unlock_time=600
auth sufficient pam_unix.so nullok try_first_pass
auth [default=die] pam_faillock.so authfail audit deny=3 even_denied_root unlock_time=600
auth requisite pam_succeed_if.so uid >= 1000 quiet_success
auth required pam_deny.so

account required pam_unix.so
account required pam_faillock.so
account sufficient pam_localuser.so
account sufficient pam_succeed_if.so uid < 1000 quiet
account required pam_permit.so

password requisite pam_pwquality.so try_first_pass local_users_only retry=3 authtok_type=
password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password required pam_deny.so

session optional pam_keyinit.so revoke
session required pam_limits.so
-session optional pam_systemd.so
session [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session required pam_unix.so
```

Perform a Google search for “pam_cracklib and syntax”. This will help explain the options I used above if needed. Finally .. PAM rocks!

Modify /etc/login.defs and change the following from:

```
PASS_MAX_DAYS 99999
PASS_MIN_DAYS 0
PASS_MIN_LEN 5
PASS_WARN_AGE 7
```

To (meet your organizations policies):

```
PASS_MAX_DAYS 60
PASS_MIN_DAYS 0
PASS_MIN_LEN 15
PASS_WARN_AGE 7
```

Using AIDE to baseline your system

Install the RPM for AIDE from the install DVD or CDs.

Then run, in order:

```
nice -17 aide --init --config=/etc/aide.conf
cp /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
```

Once the system is set, run a monthly file system integrity check with:

```
nice -17 aide -C --config=/etc/aide.conf
```

The walk away with AIDE is you get free software that performs what tripwire (tripwire.com) used to do in order to monitor your system for file changes. What I like doing is prior to installing third party applications, say something like Oracle Database 11R2 for Linux, I will run AIDE to baseline the system

and then after the application is installed, patched and configured, I run AIDE again to report the delta. It's interesting and solid information to know where all of the files are laying on your file system, especially when you get files in hidden directories that screw up re-installs. Having this knowledge allows you to thoroughly clean out your file system of any crap the vendor conveniently forgot to delete during the uninstall process. Furthermore, the Configuration Management fascists like having the knowledge of what was modified on the filesystem and AIDE affords the sys admin to quickly generate the documentation necessary to satisfy CM's insatiable greed for more documentation. 😊

In the next paper, I will be covering the software firewall, IPTables that comes default on CENTOS 7.1.

If you find any in-accuracies or misrepresentations, please email me so that I can correct my work and keep a better paper online.