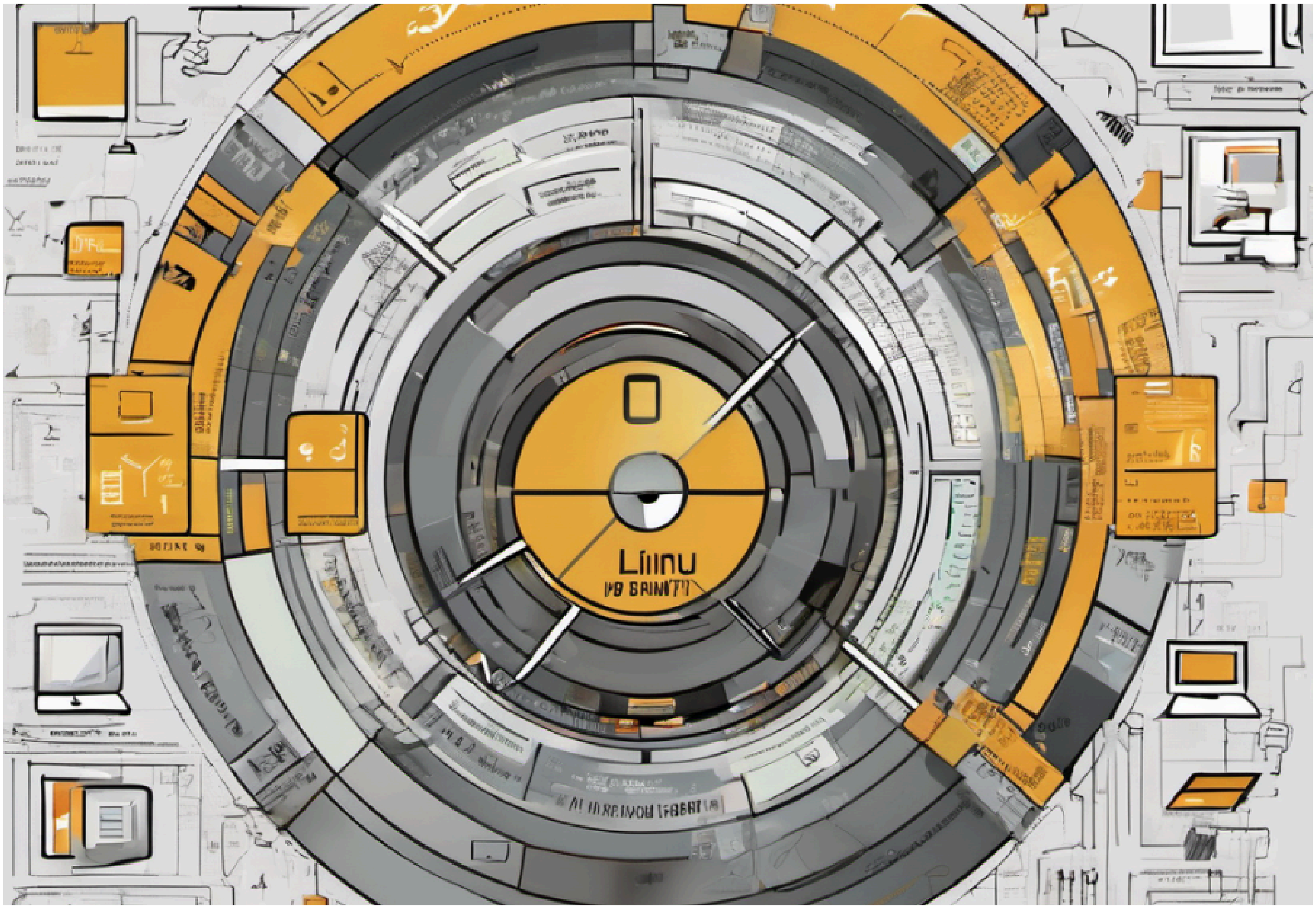
tech by K

EXPLORING TECHNOLOGY, ONE BLOG AT A TIME.

Step-by-Step Guide to Hardening RHEL with CIS Recommended Partition Setup

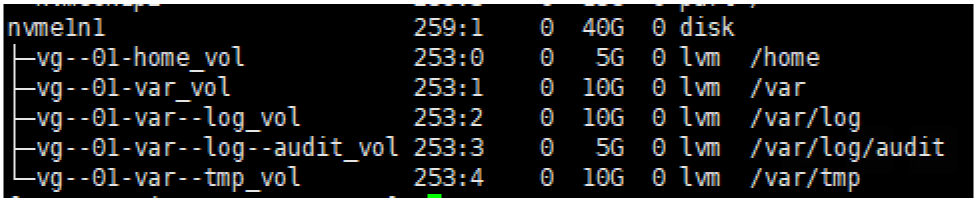
by kaushaldevin / March 3, 2024



Introduction

CIS (Center for Internet Security) hardening refers to a set of best practices and security configurations developed by the Center for Internet Security to secure computer systems and networks. These guidelines are designed to reduce vulnerabilities and improve the overall security posture of an organization’s IT infrastructure.

For Red Hat Enterprise Linux (RHEL), CIS provides a benchmark document that outlines recommended security settings and configurations. These settings cover various aspects of the operating system, including user authentication, file system permissions, network configuration, and system services. One such recommendation is to have a proper CIS partitioning structure as shown in Figure01.



```
nvme1n1                        259:1    0  40G  0 disk
├─vg--01-home_vol              253:0    0   5G  0 lvm  /home
├─vg--01-var_vol               253:1    0  10G  0 lvm  /var
├─vg--01-var--log_vol          253:2    0  10G  0 lvm  /var/log
├─vg--01-var--log--audit_vol   253:3    0   5G  0 lvm  /var/log/audit
└─vg--01-var--tmp_vol          253:4    0  10G  0 lvm  /var/tmp
```

Figure 01: Proper CIS partition structure

However, let's say these requirements are to be applied to an existing system. And you only have an attached /root partition. Then, it is going to be a significant challenge. In this article, I'll explain step by step how to manually create CIS recommended partition structure. As a bonus step, I've included how to create a /tmp partition with noexec permissions according to CIS guidelines within RHEL flavors.

Disclaimer:

⚠️ **Caution**: **Potentially Dangerous Procedure** ⚠️

> *The procedure described herein carries a risk of data loss and/or system damage. The author provides these instructions for* ***informational purposes only*** *and assumes* ***no responsibility for any adverse consequences*** *resulting from the execution of these steps. It is essential to exercise caution and understand the potential risks involved before proceeding. By following the steps outlined in this article, you acknowledge and accept the responsibility for any outcomes, including data loss and/or system damage. Please proceed only if you are fully aware of the risks and prepared to accept the consequences.*

Prerequisites:

- Take a snapshot of the existing VMs/partitions.
- Make sure to back up all your important data.
- Attach a 40GB disk to the VM. If it's AWS, then can attach a 40GB EBS to the instance.
- The following steps were tested on RHEL 8 system.
- Please understand this is a very risky procedure and re-read the above disclaimer.

Execution procedure:

As you can see within the above Figure 01, there should be 5 separate CIS partitions.

1. /var
2. /var/log
3. /var/log/audit
4. /var/tmp
5. /home

You could start from either of them. The riskiest partitions are /home and /var.

Let's assume you have a 40GB disk attached to your VM and first create the LVMs.

Identify the New VM Disk: Before proceeding, it's crucial to identify the new VM disk that is being attached. This step ensures that you're performing the following operations on the correct disk. It is highly advisable and recommended to restart the VM after attaching the new disk. For example, in this case, the new disk is identified as "nvme1n1".

Partition the Disk using parted: Use the parted utility to partition the disk. First, label the disk with GPT (GUID Partition Table) using the mklabel command. Then, create a primary partition with the mkpart command, specifying the file system type (in this case, "ext4") and the size of the partition. Finally, enable LVM (Logical Volume Manager) on the partition using the set command.

```
parted /dev/nvme1n1
(parted) mklabel gpt
mkpart primary ext4 1MiB 39.9GiB
set 1 lvm on
(parted) quit
```

Initialize Physical Volume (PV): Use the `pvcreate` command to initialize the partition created in the previous step as a physical volume for use with LVM.

```
pvcreate /dev/nvme1n1p1
```

Create Volume Group (VG): Create a volume group using the `vgcreate` command, specifying the name of the volume group ("vg_kda_cis") and the physical volume created earlier.

```
vgcreate vg_kda_cis /dev/nvme1n1p1
```

Create Logical Volumes (LV): Use the `lvcreate` command to create logical volumes within the volume group. Specify the size of each logical volume (“lv_kda_home”, “lv_kda_var”, etc.) using the `-L` option.

```
lvcreate -L 5G -n lv_kda_home vg_kda_cis
lvcreate -L 10G -n lv_kda_var vg_kda_cis
lvcreate -L 10G -n lv_kda_var_log vg_kda_cis
lvcreate -L 5G -n lv_kda_var_log_audit vg_kda_cis
lvcreate -L 9.89G -n lv_kda_var_tmp vg_kda_cis
```

Format Logical Volumes: Format each logical volume with the desired file system using the `mkfs.ext4` command. This step prepares the logical volumes for use by creating an ext4 file system on each volume.

```
mkfs.ext4 /dev/vg_kda_cis/lv_kda_home
mkfs.ext4 /dev/vg_kda_cis/lv_kda_var
mkfs.ext4 /dev/vg_kda_cis/lv_kda_var_log
mkfs.ext4 /dev/vg_kda_cis/lv_kda_var_log_audit
mkfs.ext4 /dev/vg_kda_cis/lv_kda_var_tmp
```

So, now you would have the required partition structure. The next step would be to move the existing data from the / partition to the newly created LVMs.

a. For /var partition

1. **Create a Temporary Directory and Mount the Existing /var Directory:**

```
mkdir /var1
mount /dev/mapper/vg_kda_cis-lv_kda_var /var1
```

2. Copy Contents of /var to the Temporary Directory:

```
cd /var
cp -dpRx * /var1/
```

3. Unmount the Temporary Directory and Re-Mount /var and remove the temporary directory:

```
umount /var1
cd ..
```

```
mount /dev/mapper/vg_kda_cis-lv_kda_var /var
rm -rf /var1
```

4. Update the /etc/fstab entry so that the /var directory is mounted correctly even after a restart.

```
cat /proc/mounts | grep /var
```

blkid command would provide the UUID.

The format would be:

```
UUID=<"UUID without quotes"> /var ext4 defaults 0 0
```

```
UUID=421d52ac-a173-4d18-bee1-889caf83100a /var ext4 defaults,nodev,noexec,nosuid
0 0
```

Can verify with teh following command.

```
mount -a
```

When you execute `mount -a`, it will attempt to mount any filesystems specified in `/etc/fstab` that are not currently mounted.

5. Set SELinux Contexts for /var:

The following command would restore the SELinux contexts recursively for the /var directory and subdirectories. This is very important step, that you should follow.

```
restorecon -vvFR /var
```

6. Modify GRUB configurarions to reflect the new lvm and rebuild GRUB

eg:

```
GRUB_CMDLINE_LINUX="console=ttyS0,115200n8 console=tty0 net.ifnames=0
rd.blacklist=nouveau nvme_core.io_timeout=4294967295 crashkernel=auto
rd.lvm.lv=vg_kda_cis/lv_kda_var audit=1 audit_backlog_limit=8192"
```

Rebuild grub:

```
grub2-mkconfig -o /boot/grub2/grub.cfg
```

7. Backup and rebuild initramfs.

```
cp /boot/initramfs-$(uname -r).img /boot/initramfs-$(uname -r).img.$(date +%m-
%d-%H%M%S).bak
dracut -v -f /boot/initramfs-$(uname -r).img $(uname -r)
```

8. Reboot the VM with the reboot command.

```
reboot
```

Make sure the VM properly boots after the restart. If any of the above steps had any issues, it would not properly boot. Then, the next logical step would be to recove the VM from the earlier taekn snapshot.

b. For /var/log partition

Since most of the steps in the next partition would include similar steps as above, I will not go into detailed descriptions.

1. **Create temporary dirctory and copy the content and mount the partition properly and finally remove the temporary directory.**
   ```
   mkdir /var/log2
   mount /dev/mapper/vg_kda_cis-lv_kda_var_log /var/log2
   cd /var/log
   cp -dpRx * /var/log2
   umount /var/log2
   cd ..
   mount /dev/mapper/vg_kda_cis-lv_kda_var_log /var/log
   rm -r /var/log2
   ```
2. **Update the /etc/fstab with relevant entry.**
   eg:
   ```
   UUID=982ec633-7e2c-4682-92ef-7e4131d32065 /var/log ext4
   defaults,nodev,noexec,nosuid 0 0
   ```
3. **Set SELinux Contexts for /var/log:**
   The following command would restore the SELinux contexts recursively for the /var directory and subdirectories. This is very important step, that you should follow.
   ```
   restorecon -vvFR /var/log
   ```
4. **Reboot the system using the reboot command.**
   ```
   reboot
   ```

c. For /var/log/audit partition

The difference here would be that the auditd service could be running. Therefore, better to stop the running service first.

1. **Stop the auditd service.**
   service auditd stop

2. **Copy the content.**
   ```
   cd /var/log/audit/
   rm -rf /var/log/audit/*
   chmod 700 /var/log/audit
   ```

3. **Set SELinux Contexts for /var/log/audit:**
   The following command would restore the SELinux contexts recursively for the /var directory and subdirectories. This is very important step, that you should follow.
   ```
   restorecon -vvFR /var/log/audit
   ```

4. **Start the auditd service and check the service status.**
   ```
   service auditd start
   service auditd status
   ```

5. **If all of the above steps are okay, next update the /etc/fstab entry.**
   eg:
   ```
   UUID=a7d86ae4-a794-40d6-894b-ebb55527e7eb /var/log/audit ext4 defaults,nodev,noexec,nosuid 0 0
   ```

6. **Finally reboot the system with reboot command.**
   ```
   reboot
   ```

d. For /home partition

This is also similar to the previous steps. Only issue would be that we have to be extra cautious due to /home directory having the .ssh directory. If something goes wrong, you would loose SSH access to the VM.

1. **Create a temporary directory and copy content.**
   ```
   mkdir /tmp/home
   cp -rp /home /tmp/home/
   ```

```
du -ksch /tmp/home/*
cd /home/
rm -rf /home/*
mount /dev/vg_kda_cis/lv_kda_home /home
cp -rp /tmp/home/home/* /home/
```

2. **Update the SELinux contexts.**

   The current values could be found with the ls -Z /home command.

   ```
   ls -Z /home
   restorecon -vvFR /home
   ```

3. **Update the /etc/fstab entry**

   eg:

   ```
   UUID=798ad27c-533c-41ec-9170-9da7d96a28ca /home ext4
   defaults,grpquota,nodev,nosuid,usrquota 0 0
   ```

4. **Reboot the VM with the reboot command.**

   ```
   reboot
   ```

Make sure the VM properly reboots.

e. For /var/tmp partition

1. **Create a temporary directory and copy the content and mount partition.**

   ```
   mkdir -p /tmp/var/tmp
   cd /var/tmp
   cp -rp * /tmp/var/tmp/
   rm -rf /var/tmp/*
   mount /dev/vg_kda_cis/lv_kda_var_tmp /var/tmp
   ```

2. **Set the sticky bit.**

   ```
   chmod 1777 /var/tmp
   ```

3. **Update the SELinux contexts.**

   ```
   ls -Z /var/tmp
   restorecon -vvFR /var/tmp
   ```

4. **Update the /etc/fstab entry**

   eg:

   ```
   UUID=08c972b4-6cca-4278-b9a1-78fe72f01c11 /var/tmp ext4
   defaults,nodev,noexec,nosuid 0 0
   ```

5. **Restart the VM with the reboot command.**

```
reboot
```

f. /tmp partition.

This is a bonus tip !🎁
CIS partioning require us to make sure /tmp is a seperate partition and does not have noexec for the partition.
Following commands would achieve that.

1. Make sure tmp is mounted as tmpfs and separate partition

```
systemctl enable tmp.mount
systemctl start tmp.mount
```

2. Next, edit /etc/systemd/system/local-fs.target.wants/tmp.mount

Add noexec to the “Options” list.

```
Options=mode=1777,strictatime,nosuid,nodev,noexec
```

That’s it! 🎊

By following the above steps you would be able to manually setup the CIS partitioning within your RedHat environment. In fact, most of these commands would even work within other Linux flavors as well. However, please note that I have not tested those and is not encouranging you to try. 👋

References:

- https://access.redhat.com/solutions/4126441

Tags: CIS HARDENING MANUAL PARTITIONING REDHAT RHEL RHEL8 TMPFS

Leave a Reply

Your email address will not be published. Required fields are marked *

Name *

Email *

Website

Comment *

☐ Save my name, email, and website in this browser for the next time I comment.

Post Comment

Search

Search

Recent Posts

Step-by-Step Guide to Hardening RHEL with CIS Recommended Partition Setup

License Renewal Journey: Lessons from the DMT

Enabling VoWiFi and VoLTE on Pixel devices – Sri Lanka

How I converted to an eSIM Online [Dialog]

Fixing Flickering lines on Displays: A Home Remedy

Recent Comments

kaushaldevin on WannaCry: The Ransomeware

Bob Hairstyles on WannaCry: The Ransomeware

kaushaldevin on WannaCry: The Ransomeware

kaushaldevin on Enabling VoWiFi and VoLTE on Pixel devices – Sri Lanka

I Fashion Styles on Story of the gorgeous …!!!

Neve | Powered by WordPress