|  |
| --- |
| HCSC |
| On-Premises Linux VM OS Upgrade – RHEL 7 to RHEL 8 |
| **STANDARD OPERATING PROCEDURE** |

|  |  |
| --- | --- |
| **Project Name** | HCSC UNIX |
| **Customer Name** | HCSC |
| **Customer Project Manager Name** | Todd Anders |
| **HCL Project Manager Name** | Amarjeet Singh |
| **SOP Name & Number** | DC-UNIX-15 |
| **Creation Date** | 08/31/2023 |

Table of Contents

[1. Introduction 2](#_Toc511048688)

[2. Purpose & Scope 2](#_Toc511048689)

[3. Standard Operating Procedure Summary 2](#_Toc511048690)

[4. Abbreviations Used 3](#_Toc511048691)

[5. Revision History 3](#_Toc511048692)

[6. SOP Approval – HCSC Two in a Box / Validator 3](#_Toc511048693)

[7. Procedure 4](#_Toc511048696)

[o Paperwork: 4](#_Toc511048697)

[o Technical Steps: 5](#_Toc511048698)

# Introduction

HCL is entrusted to Upgrade Linux servers from RHEL 7 to RHEL 8 in HCSC Datacenter. This document captures the process and technical steps for upgrading the Linux Virtual Machines in On-Premises Datacenter.

# Purpose & Scope

The purpose and scope of this document is to document overall process and present the technical steps for On-Premises Linux VM OS Upgrade from RHEL 7 to RHEL 8.

# Standard Operating Procedure Summary

|  |  |
| --- | --- |
| Application Name & Number | Linux OS Upgrade SOP |
| SOP Name | SOP – On-Premises Linux VM OS Upgrade – RHEL7 to RHEL8 |
| Current Version | 1.0 |
| Date Created | 31-Aug-2023 |
| Last Updated By | Richard Davis |
| Date Last Updated | 31-Aug-2023 |
| HCSC - Approved By |  |
| HCL – Approved By |  |
| Approved On |  |

# Abbreviations Used

|  |  |
| --- | --- |
| Term | Term Definition |
| OS | Operating System |
| RHEL | Redhat Enterprise Linux |

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| Version No. | Date | Author/Reviewer | Change Description |
| 1.0 | 08/31/2023 | Niranjan Kumar/Richard Davis |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# 

# SOP Approval – HCSC Two in a Box / Validator

|  |  |  |  |
| --- | --- | --- | --- |
| **Name** | **Company** | **Email-ID** | **Primary / Secondary** |
| Richard Davis | HCSC | richard\_davis@bcbsil.com | Primary |
| Niranjan Kumar | HCL | [niranjan\_kumar@bcbsil.com](mailto:niranjan_kumar@bcbsil.com) | Primary |
| Bill Mesik | HCSC | william\_mesik@bcbsil.com | Secondary |
| Ashish Verma | HCL | [Ashish\_Verma@bcbsil.com](mailto:Ashish_Verma@bcbsil.com) | Secondary |

# Procedure

* **Paperwork:**

|  |
| --- |
| * Open the share point link to download ‘Linux RHEL Upgrades for HCL to process’ spreadsheet:   <https://myfyi.sharepoint.com/:x:/r/teams/DistrComp/_layouts/15/Doc.aspx?sourcedoc=%7B2B6CE346-A3A1-44D0-874C-8BCC7E9B3593%7D&file=Linux%20RHEL%20Upgrades%20for%20HCL%20to%20process.xlsx&action=default&mobileredirect=true>     * All RHEL 7 server approved for OS Upgrade is placed in sheet with tab named ‘HCL Master - To Be Upgraded’. |
| * Create Change in AYS for approved servers as per the downtime approval in Column ‘J’ in the sheet. * Update the Sheet with Change Number in Column ‘K’. * Once the Change is approved, send formal communication to the Project and Application team with Change details and Implementation Window. * Get an acknowledgement from Application Team after the application is brought down. * **Technical Steps:** |
| * STEP 1:  1. Take VM Snapshot. Snapshot is required for quick recovery if the upgrade fails. |
| 1. Enter relevant information in Description and click ‘CREATE’ button. |
| 1. Click on the Snapshots Menu to verify the snapshot is created. |
|  |
| 1. Additionally check into Task Console to verify snapshot is created. |
|  |
|  |

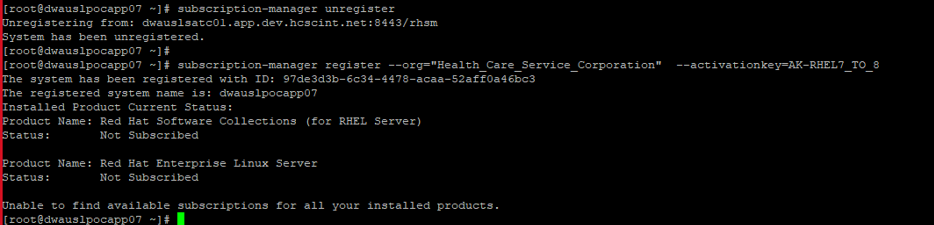
* STEP 2:

1. Set the host Content View to the leapp upgrade.

**Local CLI**

# subscription-manager unregister

# subscription-manager register --org="Health\_Care\_Service\_Corporation" --activationkey=AK-RHEL7\_TO\_8

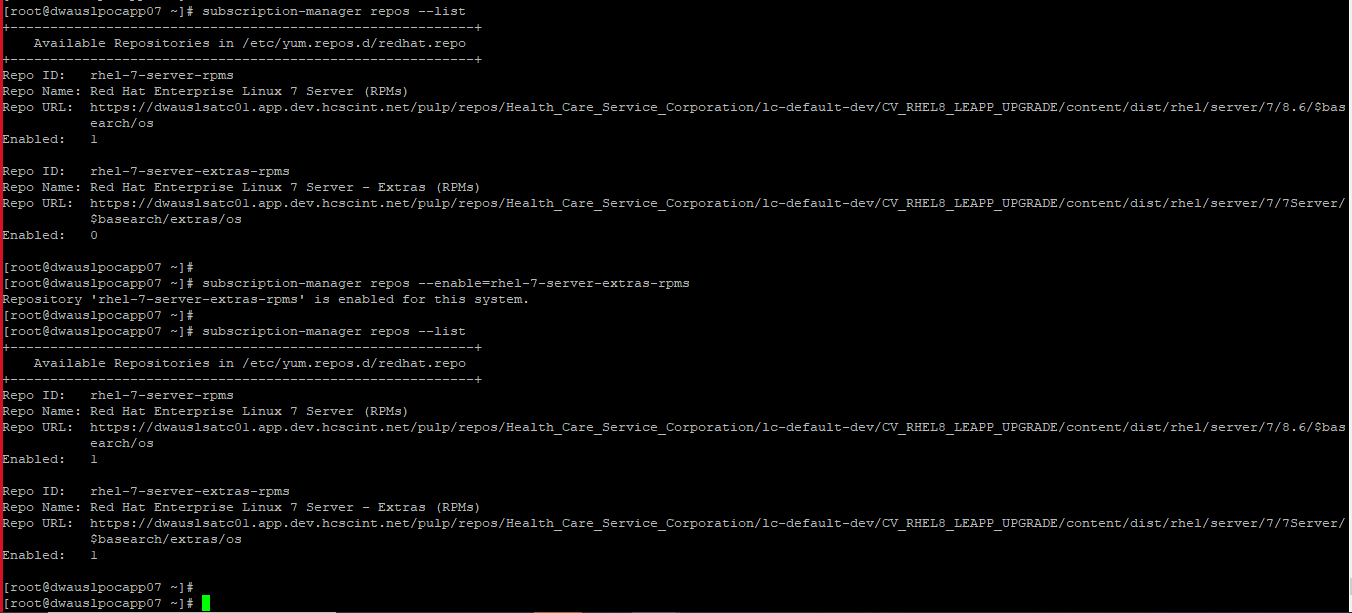


1. Verify the Yum Repositories. Enable the disabled repo.

# subscription-manager repos –list

# subscription-manager repos --enable=rhel-7-server-extras-rpms

# subscription-manager repos --list

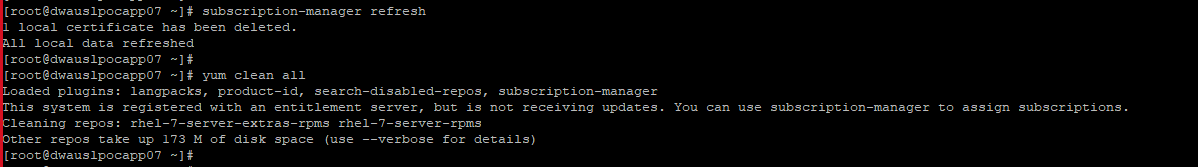


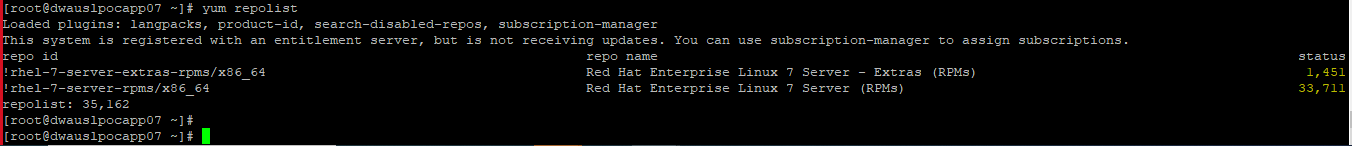
1. Pull the latest entitlement data from the satellite server.

# subscription-manager refresh

# yum clean all

# yum repolist



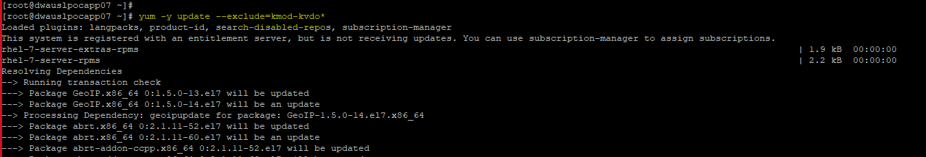


* STEP 3:

1. Patch the server to the latest kernel level of RHEL 7.9. Exclude any rpm package if yum update is failing due to some of its dependency and reboot the server. If the server is already patched to latest kernel level of RHEL 7.9, then just reboot the server.

# yum -y update --exclude=kmod-kvdo\*

# shutdown -r now

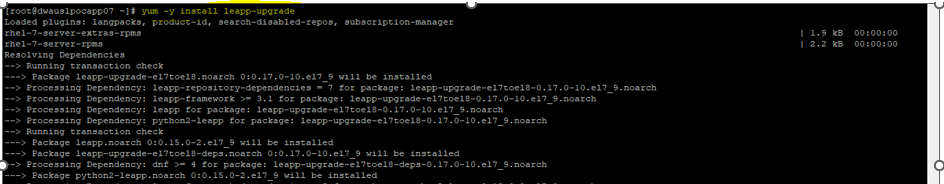




* STEP 4:

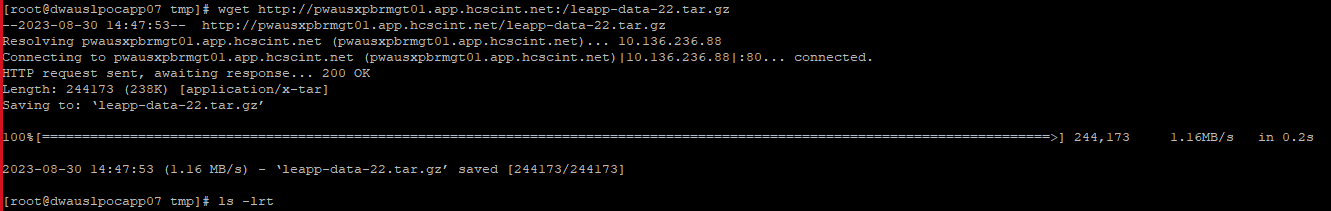
1. Install leapp upgrade software.

# yum -y install leapp-upgrade



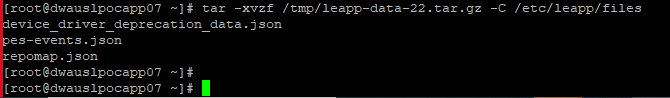
1. Download the leapp meta data archive file, currently leapp-data-22.tar.gz, in /tmp

# wget http://pwausxpbrmgt01.app.hcscint.net:/leapp-data-22.tar.gz



1. Extract the tar zip leapp meta data file to /etc/leapp/files

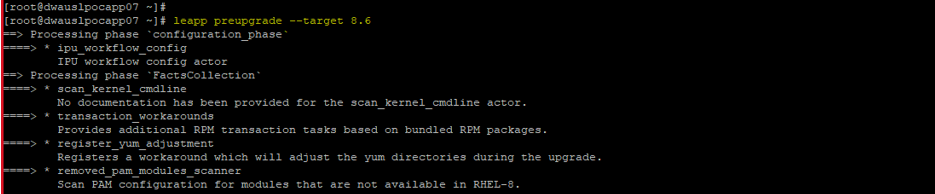
# tar -xvzf /tmp/leapp-data-22.tar.gz -C /etc/leapp/files

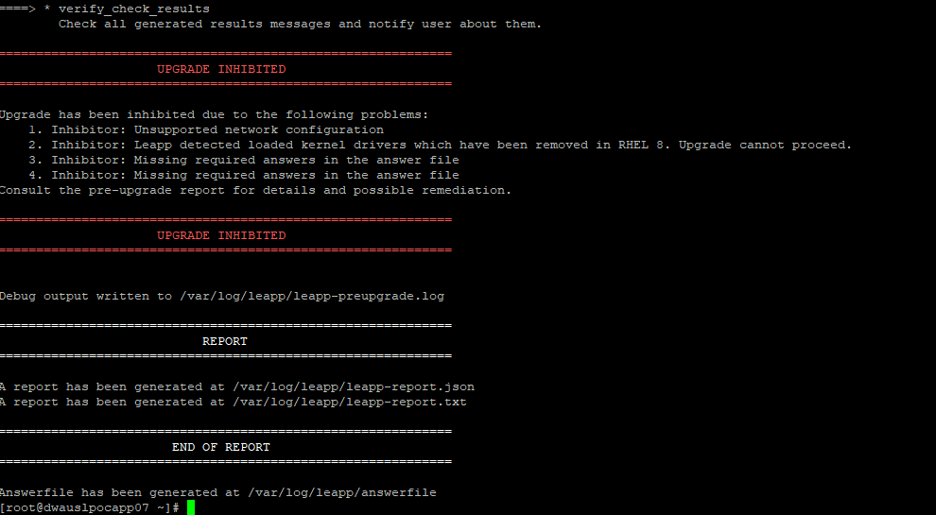


* STEP 5:

1. Run leapp preupgrade and generate upgrade report

# leapp preupgrade --target 8.6

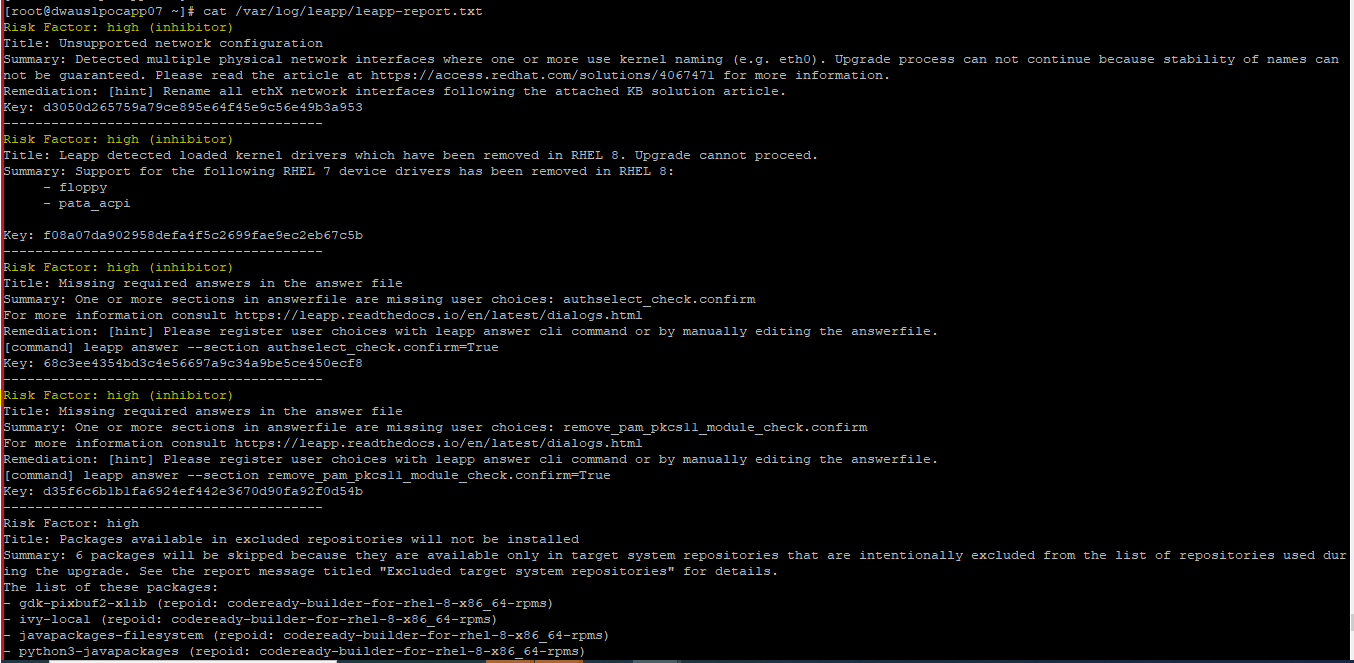




* STEP 6:

1. View the file generated at /var/log/leapp/leapp-report.txt. Review and correct "Risk Factor: high (inhibitor)"

# cat /var/log/leapp/leapp-report.txt



1. Correct Ethernet Interface Names. Rename ethX interfaces to emX

# ls -lrt /etc/sysconfig/network-scripts/ifcfg-\*

# mv /etc/sysconfig/network-scripts/ifcfg-eth0 /etc/sysconfig/network-scripts/ifcfg-em0

# mv /etc/sysconfig/network-scripts/ifcfg-eth1 /etc/sysconfig/network-scripts/ifcfg-em1

# cat /etc/sysconfig/network-scripts/ifcfg-em0

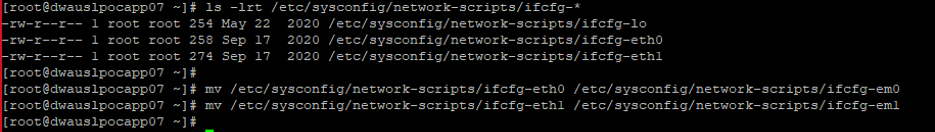
# vi /etc/sysconfig/network-scripts/ifcfg-em0

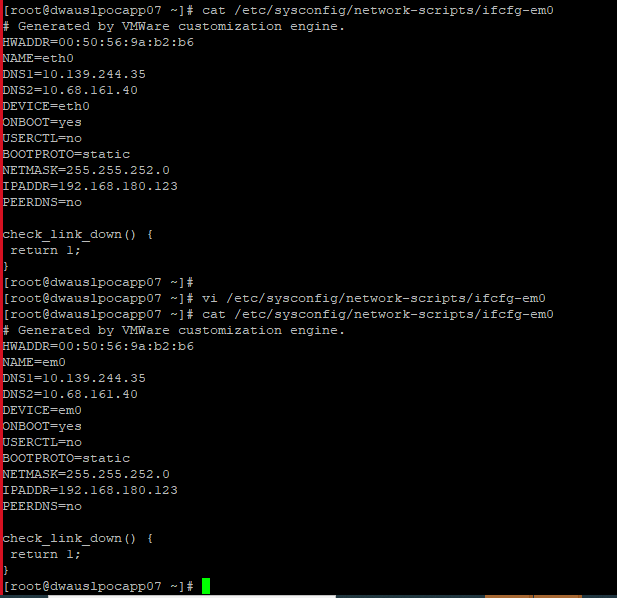
# cat /etc/sysconfig/network-scripts/ifcfg-em0

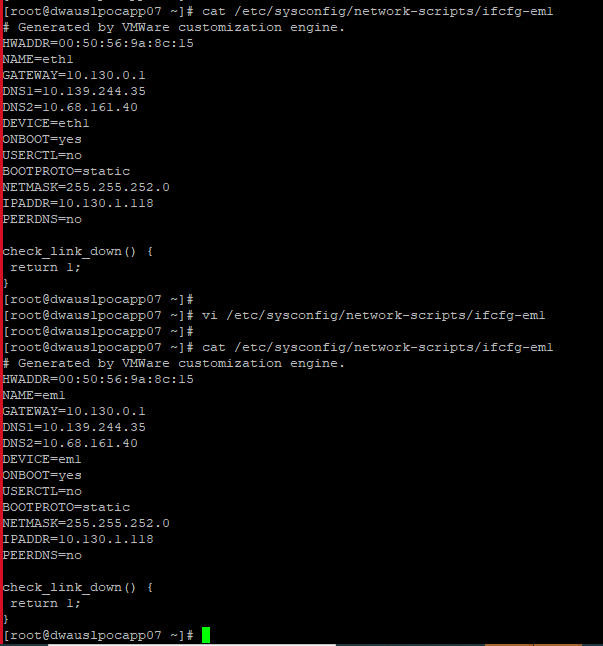
# cat /etc/sysconfig/network-scripts/ifcfg-em1

# vi /etc/sysconfig/network-scripts/ifcfg-em1

# cat /etc/sysconfig/network-scripts/ifcfg-em1



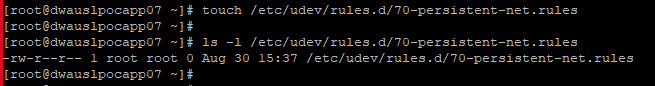




1. Update /etc/udev/rules.d/70-persistent-net.rules (create file if it does not exist).

# touch /etc/udev/rules.d/70-persistent-net.rules

# ls -l /etc/udev/rules.d/70-persistent-net.rules



# ip a

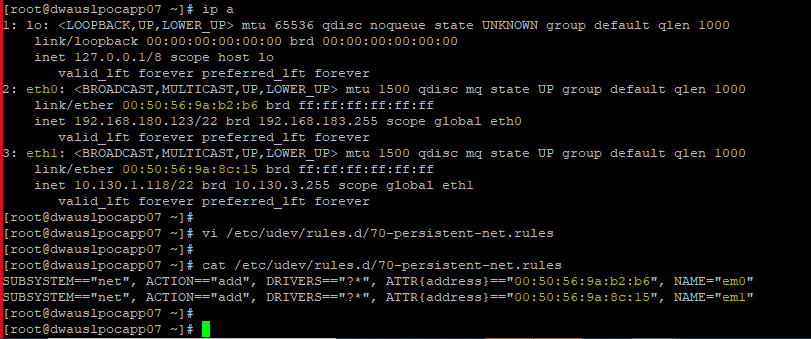
# vi /etc/udev/rules.d/70-persistent-net.rules

NOTE – replace the MAC address with the current interface take from ifconfig -a output

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?\*", ATTR{address}=="00:50:56:bc:3e:e6", NAME="em0"

SUBSYSTEM=="net", ACTION=="add", DRIVERS=="?\*", ATTR{address}=="00:50:56:bc:6c:8c", NAME="em1"

# cat /etc/udev/rules.d/70-persistent-net.rules



**Step – 9**

Vi /boot/efi/EFI/redhat/grub.cfg and Update the grub.cfg

Go to linux 10 and update with ***efi\_no\_storage\_paranoia***

*### BEGIN /etc/grub.d/10\_linux ###*

*menuentry 'Red Hat Enterprise Linux Server (3.10.0-1160.95.1.el7.x86\_64) 7.9 (Maipo)' --class red --class gnu-linux --class gnu --class os --unrestricted $m*

*enuentry\_id\_option 'gnulinux-3.10.0-957.el7.x86\_64-advanced-0701839e-c21a-43bd-a21f-b484e9574a9d' {*

*load\_video*

*set gfxpayload=keep*

*insmod gzio*

*insmod part\_gpt*

*insmod ext2*

*set root='hd0,gpt2'*

*if [ x$feature\_platform\_search\_hint = xy ]; then*

*search --no-floppy --fs-uuid --set=root --hint-bios=hd0,gpt2 --hint-efi=hd0,gpt2 --hint-baremetal=ahci0,gpt2 baa3e5b6-772d-49fa-82e3-1be3c958b8c4*

*else*

*search --no-floppy --fs-uuid --set=root baa3e5b6-772d-49fa-82e3-1be3c958b8c4*

*fi*

*linuxefi /vmlinuz-3.10.0-1160.95.1.el7.x86\_64 root=/dev/mapper/rootvg-rootlv ro rd.lvm.lv=rootvg/rootlv rd.lvm.lv=rootvg/usrlv biosdevname=0 net.ifn*

*ames=0 LANG=en\_US.UTF-8* ***efi\_no\_storage\_paranoia***

*initrdefi /initramfs-3.10.0-1160.95.1.el7.x86\_64.img*

**Step XX**

Check and make sure SELINUX should be disable.

[root@dwauslpamap04 ~]# cat /etc/selinux/config

# This file controls the state of SELinux on the system.

# SELINUX= can take one of these three values:

# enforcing - SELinux security policy is enforced.

# permissive - SELinux prints warnings instead of enforcing.

# disabled - No SELinux policy is loaded.

#SELINUX=enforcing

**SELINUX=disabled**

# SELINUXTYPE= can take one of three values:

# targeted - Targeted processes are protected,

# minimum - Modification of targeted policy. Only selected processes are protected.

# mls - Multi Level Security protection.

SELINUXTYPE=targeted

[root@dwauslpamap04 ~]#

**Step XX**

**Install the Network manager if not installed**

# yum list NetworkManager

# yum install NetworkManager.x86\_64

# Reboot -r now

Update boot manager

#efibootmgr

#efibootmgr -b 0001 -B ( remove the floppy one )

#efibootmgr

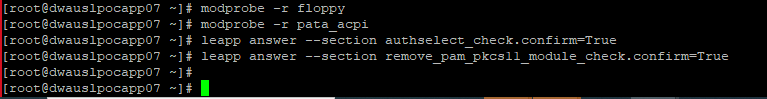
1. Remove unsupported kernel drivers. VMs have two kernel drivers that must be removed before upgrade. And run the leapp answer command for the other 2 high inhibitors as suggested in leapp-report.txt

# modprobe -r floppy

# modprobe -r pata\_acpi

# leapp answer --section authselect\_check.confirm=True

# leapp answer --section remove\_pam\_pkcs11\_module\_check.confirm=True



1. Remove unused kernel-devel packages if any installed on the server. Check the unused kernel-devel on the server by executing the below command and remove them using ‘yum remove’ command.

# rpm -qa | grep kernel-devel

# yum -y remove kernel-devel-3.10.0-957.21.3.el7.x86\_64 kernel-devel-3.10.0-957.46.1.el7.x86\_64

efibootmanager

1. Make sure the system is running open sshd and not centrify-sshd

# systemctl status centrify-sshd.service

# systemctl status sshd.service

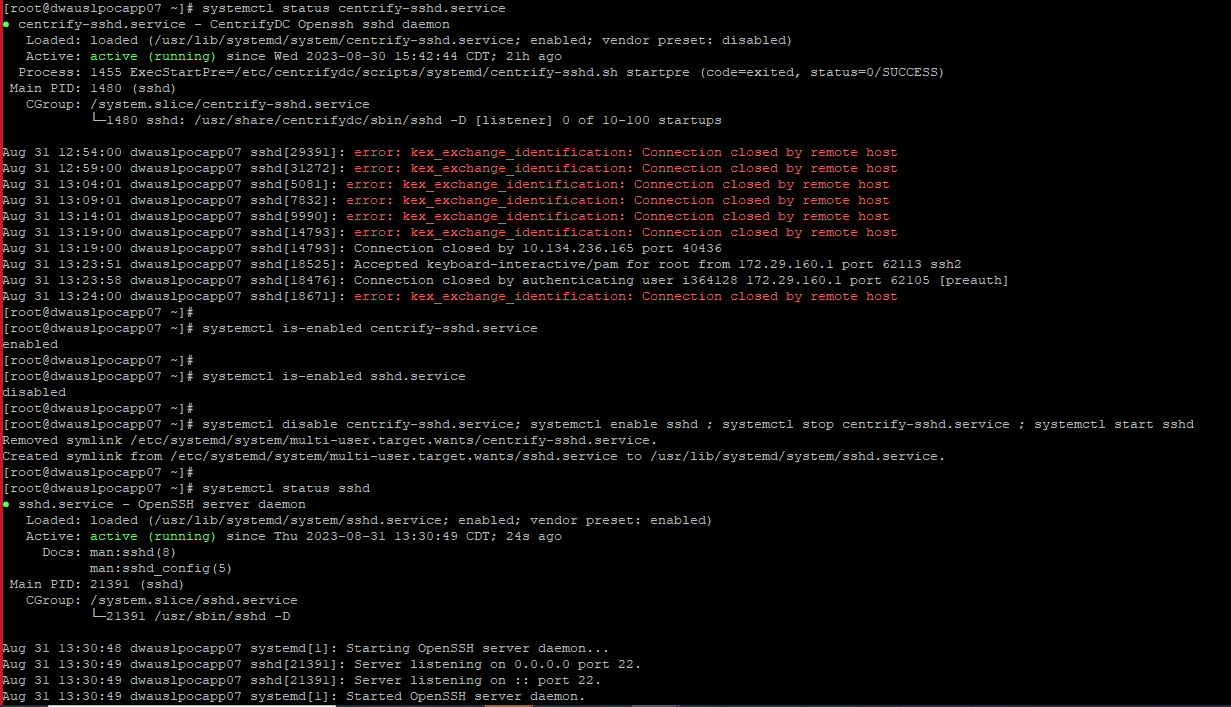
# systemctl is-enable centrify-sshd.service

# systemctl is-enabled sshd.service

# systemctl disable centrify-sshd.service; systemctl enable sshd ; systemctl stop centrify-sshd.service ; systemctl start sshd

# systemctl status sshd

# systemctl status centrify-sshd (should report stopped/disabled or not a known service)



1. Ensure Permit Root Login is set in /etc/ssh/sshd\_config.

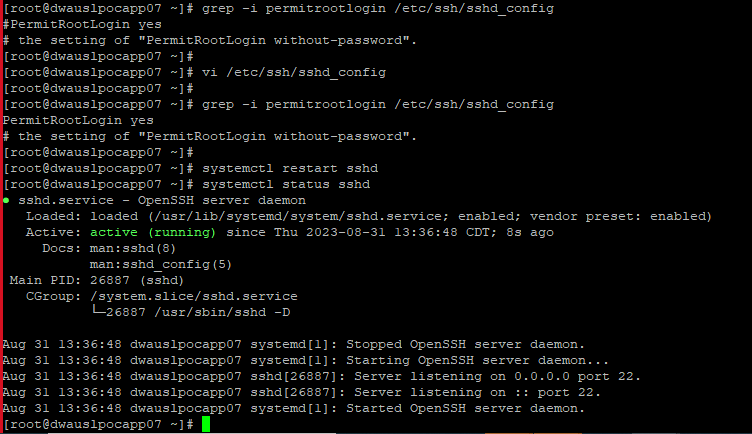
# grep -i permitrootlogin /etc/ssh/sshd\_config

# vi /etc/ssh/sshd\_config

# grep -i permitrootlogin /etc/ssh/sshd\_config

# systemctl restart sshd

# systemctl status sshd



1. Verify mounts. Unmount NFS/SMB mounts. Comment out any NFS/CIFS filesystem in /etc/fstab.

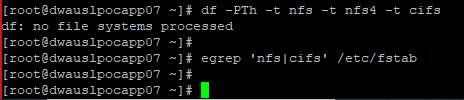
# df -PTh -t nfs -t nfs4 -t cifs

# egrep 'nfs|cifs' /etc/fstab

# systemctl status nfs [ Stop and disable nfs client service if it is running.]

# systemctl stop nfs

# systemctl disable nfs





* STEP 7:

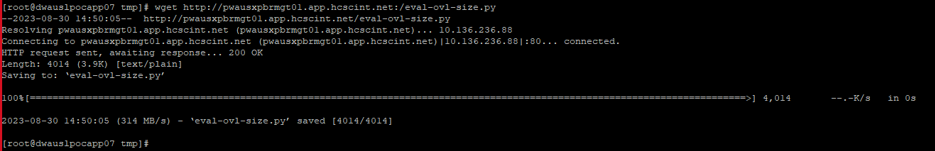
1. Verify space requirements. Download redhat eval-ovl-size.py script from pwausxpbrmgt01 and execute it.

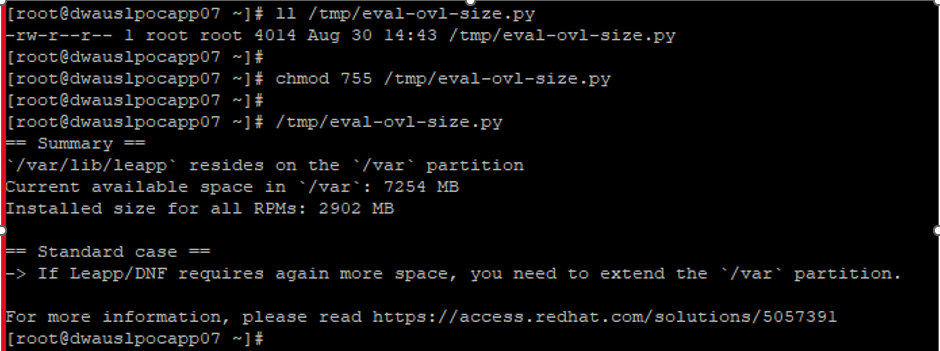
# wget http://pwausxpbrmgt01.app.hcscint.net:/eval-ovl-size.py

# ll /tmp/eval-ovl-size.py

# chmod 755 /tmp/eval-ovl-size.py

# /tmp/eval-ovl-size.py





1. Verify /usr and /opt file system space. /usr should have at least 4GB free space and /opt should have 2GB free space.

# df -PTh /usr /opt

# vgs

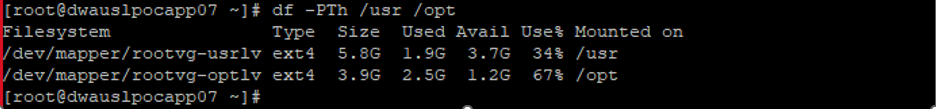
# lvextend -L +1G /dev/rootvg/usrlv

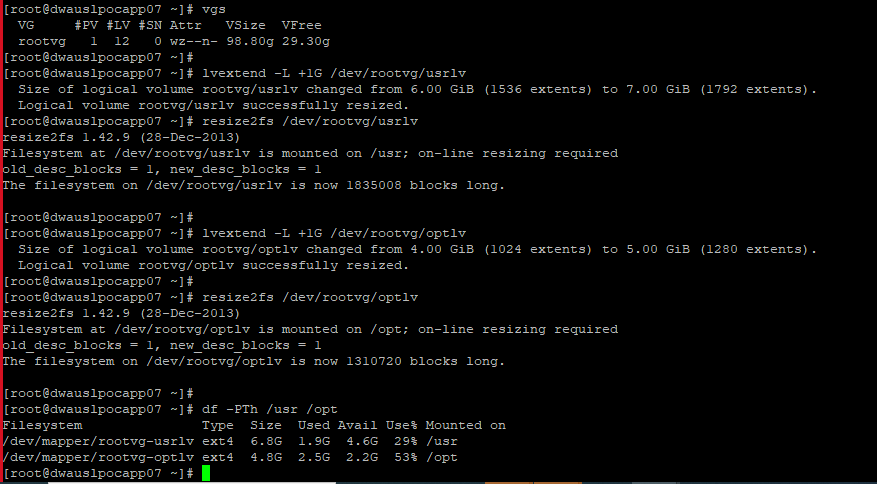
# resize2fs /dev/rootvg/usrlv

# lvextend -L +1G /dev/rootvg/optlv

# resize2fs /dev/rootvg/optlv

# df -PTh /usr /opt





1. Clean-up root (/) and /boot filesystems. Clean-up any unneeded files in / (best to have at least 2GB to 3.5GB). Remove image and support files for unused kernels in /boot.

# cd /

# ll

# rm -rf c

# df -PTh /

# df -PTh /boot/

# ll /boot

# grubby --default-kernel

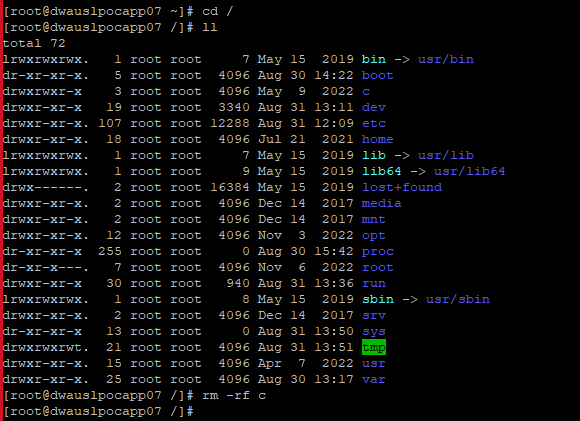
# grubby --remove-kernel=/boot/vmlinuz-3.10.0-957.21.3.el7.x86\_64

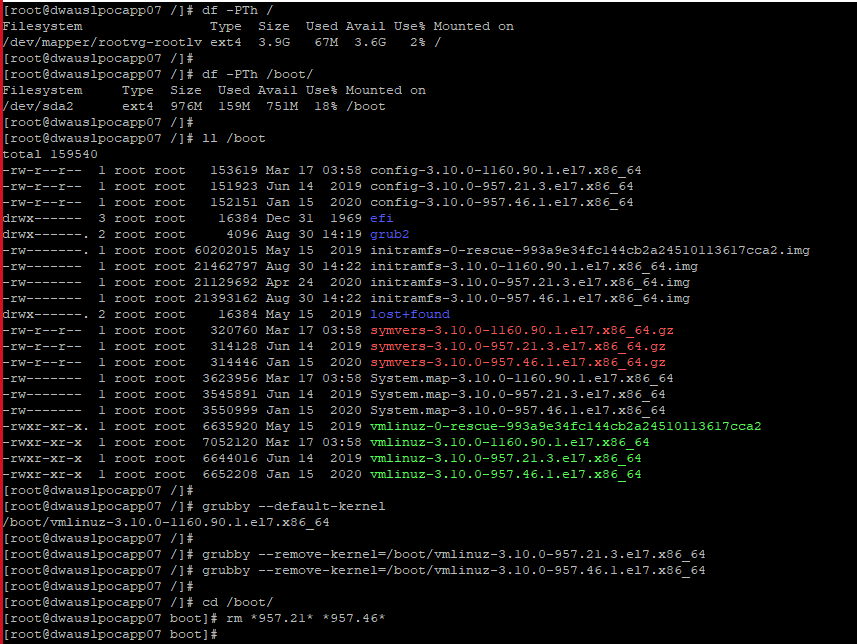
# grubby --remove-kernel=/boot/vmlinuz-3.10.0-957.46.1.el7.x86\_64

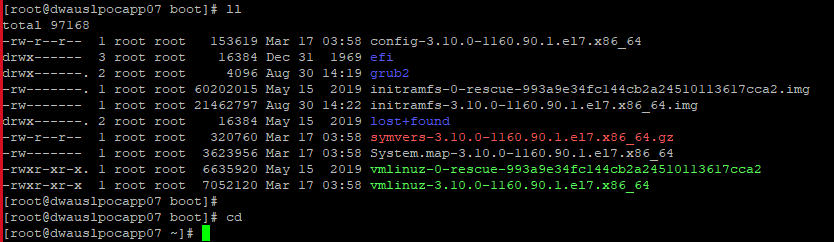
# cd /boot/

# rm \*957.21\* \*957.46\*

# ls -lrt





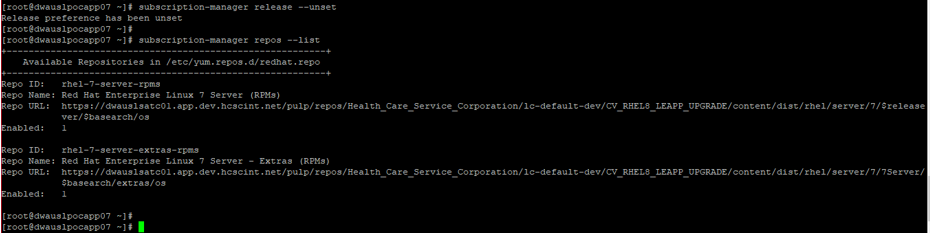


* STEP 8:

1. To execute leapp upgrade, unset release so that 8 repos are available during upgrade and verify the available repos.

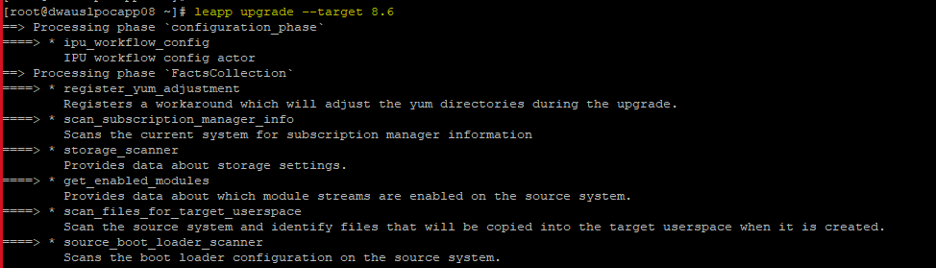
# subscription-manager release --unset

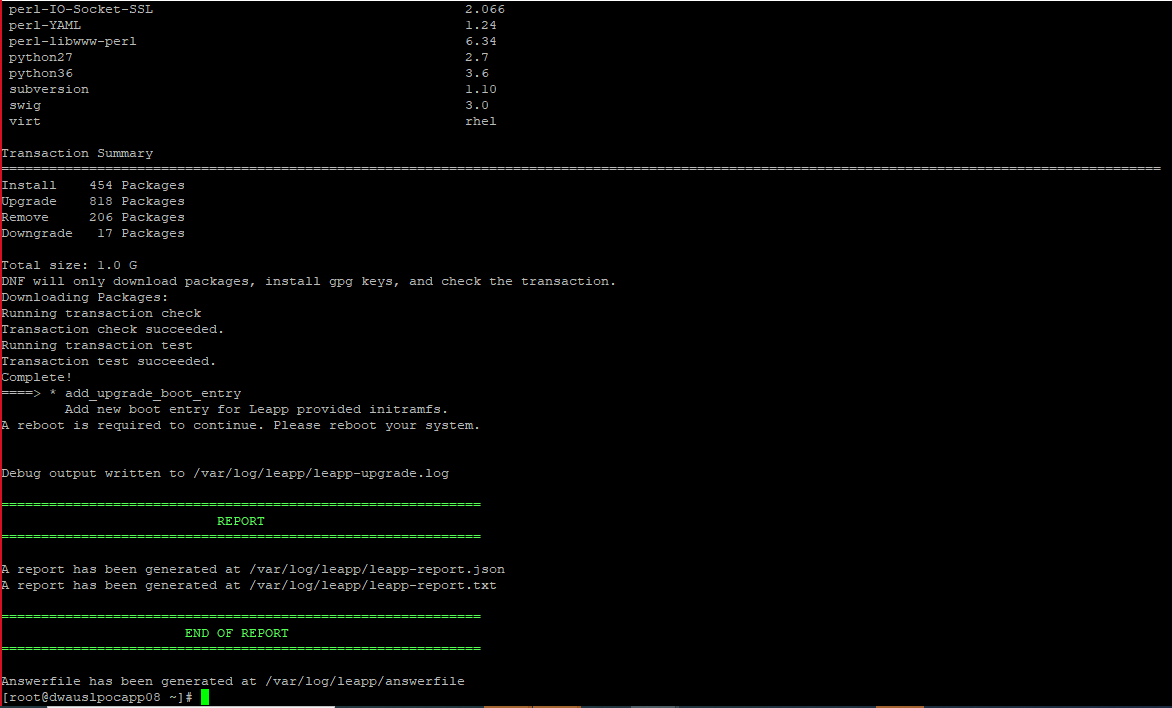
# subscription-manager repos --list



1. Execute the leapp upgrade.

# leapp upgrade --target 8.6



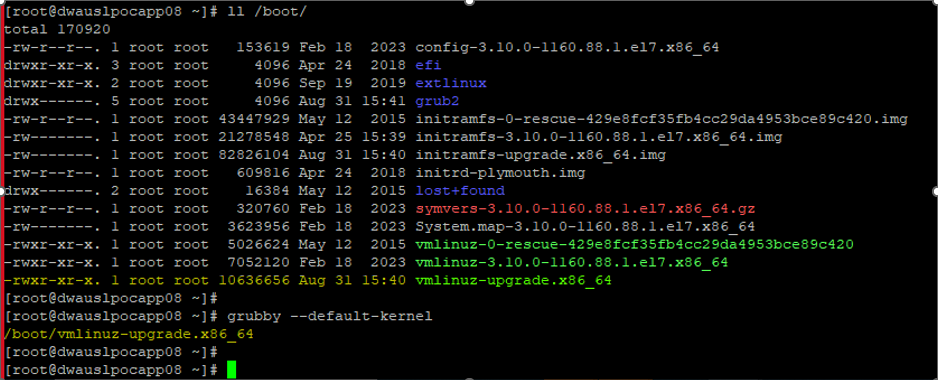


1. Once the leapp upgrade command finishes with Green Report, check the boot file system and the grubby default kernel. /boot filesystem should have vmlinuz-upgrade.x86\_64 compressed Linux kernel image file for booting the Linux operating system. The default kernel should be set to /boot/vmlinuz-upgrade.x86\_64. Reboot the server to start the Upgrade.

# ls -l /boot

# grubby --default-kernel

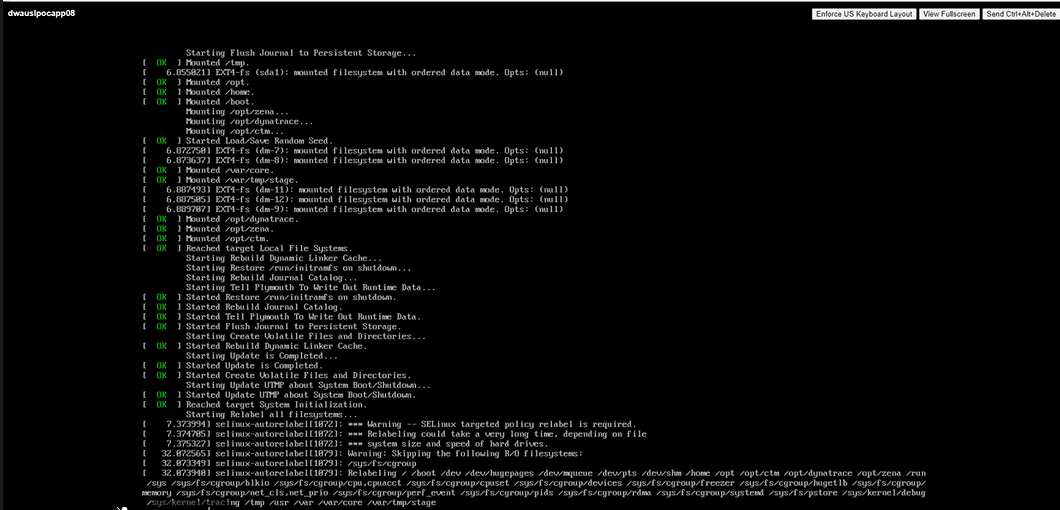
# shutdown -r now





* STEP 9:

1. Monitor upgrade from the VM console of the target host after reboot. If any error occurs during the upgrade process, fix it by login to VM console and then rerun STEP 8 (b) to proceed again.



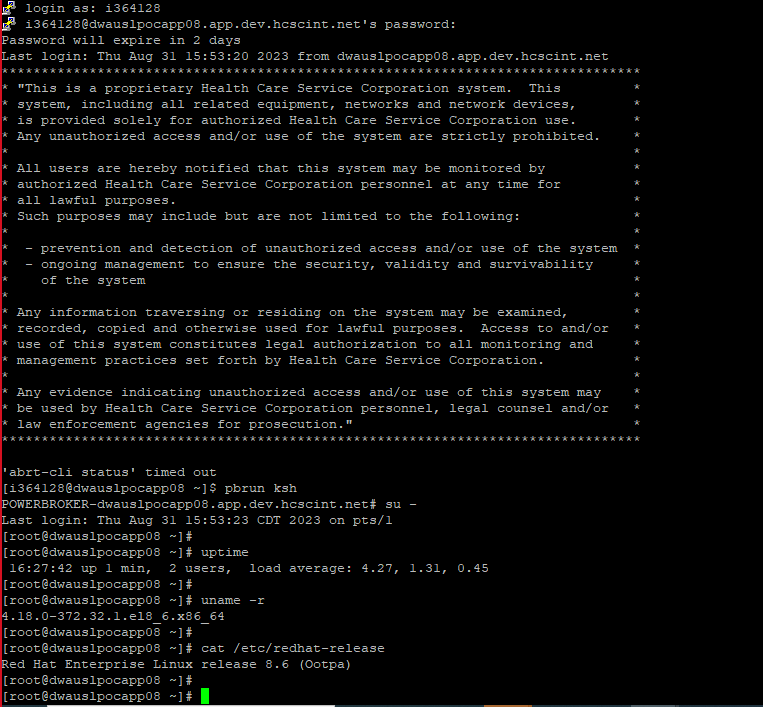
* STEP 10:

1. Once the server comes up after reboot, login to the server to verify the kernel and Redhat version.

# uptime

# uname -r

# cat /etc/Redhat-release



1. Fix python for RHEL 8.

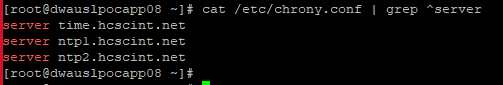
# alternatives --set python /usr/bin/python3



1. Uncomment any NFS/SMB mounts in the /etc/fstab and remount them if any NFS/CIFS were mounted before upgrade.
2. Configure chrony service and restart it. Make sure the below time servers are there in chrony.conf and rest all time servers should be removed.

# cat /etc/chrony.conf | grep ^#

# systemctl restart chronyd



1. Patch server to the latest version of RHEL 8.

# subscription-manager unregister

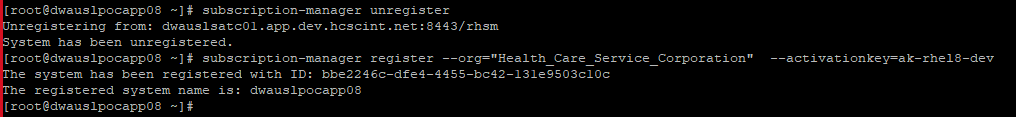
# subscription-manager register --org="Health\_Care\_Service\_Corporation" --activationkey=ak-rhel8-[ENV]

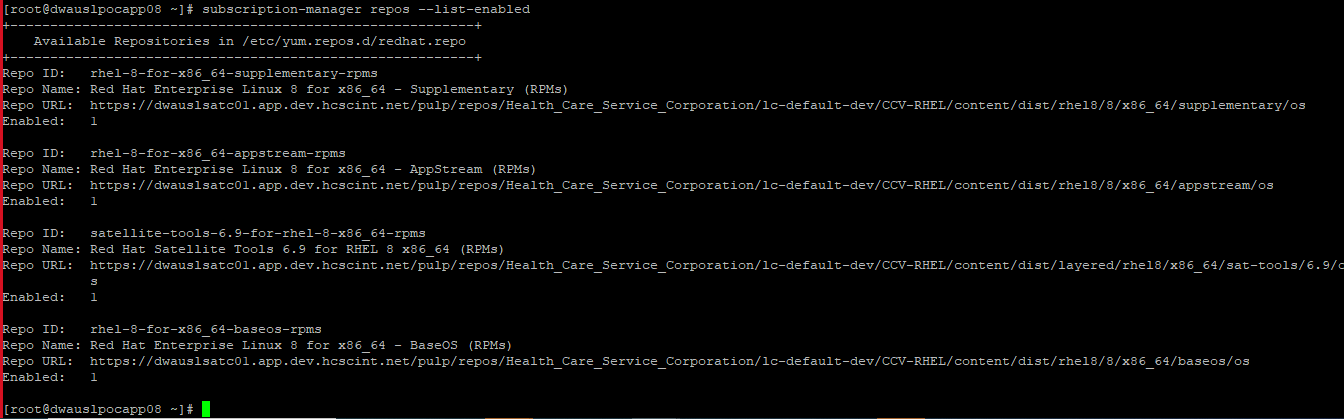
NOTE Activation keys include the target server’s environment: ak-rhel8-dev, ak-rhel8-test, ak-rhel8-prod,

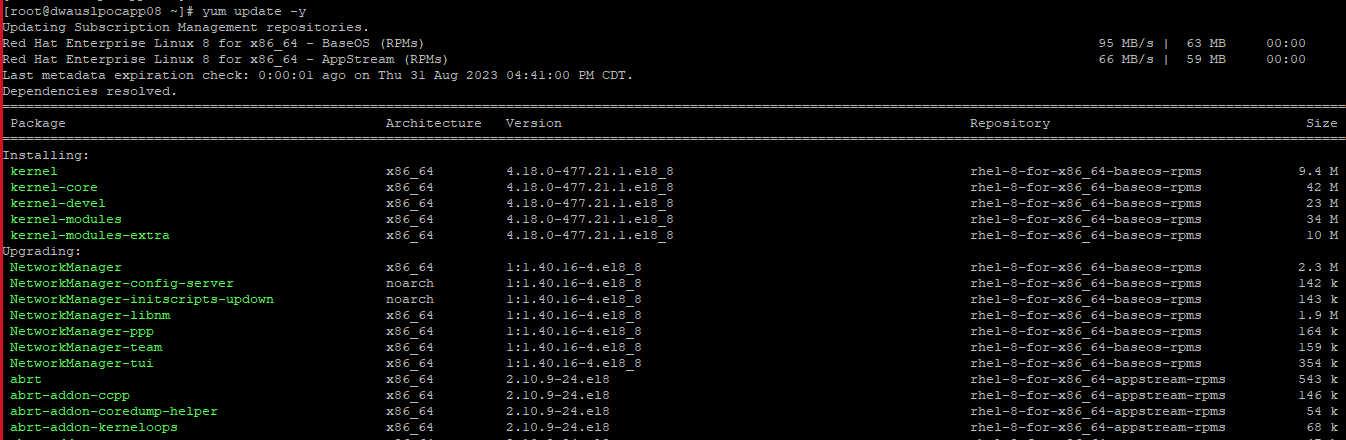
# subscription-manager refresh

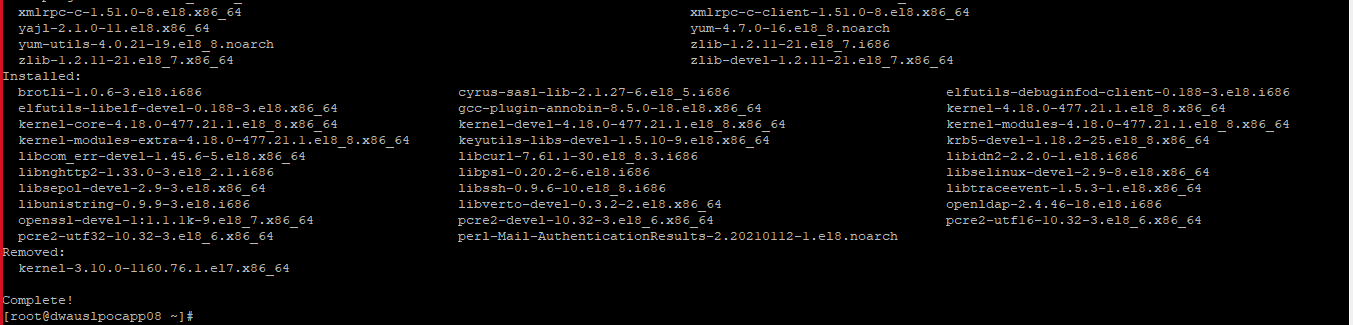
# yum clean all

# yum -y update









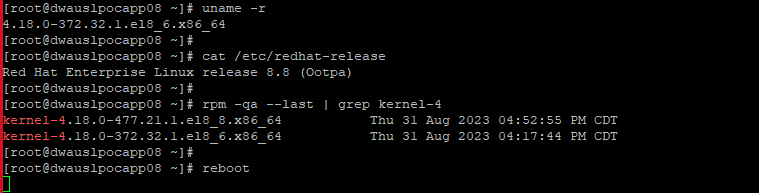
1. Once the patching completes, reboot the server to bring it up with latest kernel.

# uname -r

# cat /etc/Redhat-release

# rpm -qa –last | grep kernel-4

# reboot



1. Perform the post reboot verification before releasing the server back to Application Team. Make sure all filesystems in fstab are mounted correctly.

# uptime

# uname -r

# cat /etc/redhat-release

# rpm -qa –last | grep kernel-4

# df -PTh

# cat /etc/fstab | egrep 'ext4|xfs|nfs|cifs' | wc -l

# df -PTh | awk '$2 == "ext4" || $2 == "xfs" || $2 ~ "nfs" || $2 == "cifs" {print}' | wc -l

