Oracle Linux 7.6 UEK 5 KVM & Virtualization Manager 4.3

Common Criteria Guide

Version 1.6

March 2023

Document prepared by

www.lightshipsec.com

Table of Contents

List of Tables

1 About this Guide

1.1 Overview

1 This guide provides supplemental instructions to achieve the Common Criteria evaluated configuration of Oracle Linux 7.6 UEK 5 KVM & Virtualization Manager 4.3 and related information.

1.2 Audience

2 This guide is intended for system administrators and the various stakeholders involved in the Common Criteria evaluation. It is assumed that readers will use this guide in conjunction with the related documents listed section 1.5.

1.3 About the Common Criteria Evaluation

3 The Common Criteria for Information Technology Security Evaluation (ISO/IEC 15408) is an international standard for security certification of IT products and systems. More information is available at https://www.commoncriteriaportal.org/

1.3.1 Protection Profile Conformance

4 The Common Criteria evaluation was performed against the requirements of the Protection Profile for Virtualization v1.0 (Base PP), the Extended Package for Server Virtualization v1.0 (SV_EP) and Extended Package for Secure Shell (SSH) v1.0 (SSH_EP), available at https://www.niap-ccevs.org/Profile/PP.cfm

1.3.2 Evaluated Software

5 The Target of Evaluation (TOE) is Oracle Linux 7.6 UEK 5 KVM & Virtualization Manager 4.3.

1.3.3 Evaluated Functions

6 The following functions have been evaluated under Common Criteria:

a) **VM Hardware-based Isolation.** The TOE supports isolation mechanisms to constrain a Guest Virtual Machines (VM) direct access to physical devices.

b) **VM Resource Control.** The TOE enables control of Guest VM access to physical platform resources.

c) **VM Residual Information Clearing.** The TOE ensures that any previous information content in memory or physical disk storage is cleared prior to allocation to a Guest VM.

d) **VM Networking & Separation.** The TOE enables control of mechanisms used to transfer data between Guest VMs, including control of virtual networking components.

e) **VM User Interface.** The TOE indicates to users which VM if any has current input focus and supports unique identification of VMs.

f) **VS Integrity.** The TOE maintains integrity of the virtualization system (VS) critical components via measured boot and trusted software updates.

g) **VS Self Protection.** The TOE implements self-protection mechanisms including execution environment mitigations, hardware-assists, hypercall controls, isolation from VMs and controls for removable media.

h) **Protected Communications.** The TOE protects the integrity and confidentiality of communications with remote administrators and remote audit servers.

i) **Secure Administration.** The TOE enables secure management of its security functions, including:

   i) Administrator authentication with passwords

   ii) Configurable password policies

   iii) Role Based Access Control

   iv) Access banners

   v) Management of critical security functions and data

j) **System Monitoring.** The TOE generates audit records and stores them locally and is capable of sending records to a remote audit server. The TOE protects stored audit records and enables their review.

k) **Cryptographic Operations.** The TOE implements cryptographic operations in support if its security functions.

7 **NOTE:** No claims are made regarding any other security functionality.

1.3.4 Evaluation Assumptions

8 The following assumptions were made in performing the Common Criteria evaluation. The guidance shown in the table below should be followed to uphold these assumptions in the operational environment.

Table 1: Evaluation Assumptions

Assumption	Guidance
A.PLATFORM_INTEGRITY - The platform has not been compromised prior to installation of the Virtualization System.	No additional guidance.
A.PHYSICAL - Physical security commensurate with the value of the TOE and the data it contains is assumed to be provided by the environment.	Ensure that the TOE hardware is hosted in a physically secure environment, such as a locked server room.
A.TRUSTED_ADMIN - TOE Administrators are trusted to follow and apply all administrator guidance.	Ensure that administrators are competent, are able to follow the provided guidance.
A.COVERT_CHANNELS - If the TOE has covert storage or timing channels, then for all VMs executing on that TOE, it is assumed that relative to the IT assets to which they have access, those VMs will have assurance sufficient to outweigh the risk that they will violate the security policy of the TOE by using those covert channels.	The evaluation did not address covert channels.
A.NON_MALICIOUS_USER - The user of the VS is not wilfully negligent or hostile and uses the VS in compliance with the applied enterprise security policy and guidance. At the same time, malicious applications could act as the user, so requirements which confine malicious applications are still in scope.	The evaluation considered users to be non-hostile – additional controls should be employed if this is not the case.

1.4 Conventions

9 The following conventions are used in this guide:

a) `CLI Command <replaceable>` - This style indicates to you that you can type the word or phrase on the command line and press [Enter] to invoke a command. Text within <> is replaceable. For example:

Use the `cat <filename>` command to view the contents of a file

b) [key] or [key-combo] – key or key combination on the keyboard is shown in this style. For example:

The [Ctrl]-[Alt]-[Backspace] key combination exits your graphical session and returns you to the graphical login screen or the console.

c) **GUI => Reference** – denotes a sequence of GUI screen interactions. For example:

Select **File => Save** to save the file.

d) [REFERENCE] *Section* – denotes a related document and section reference. For example:

Follow [ADMIN] *Configuring Users* to add a new user.

1.5 Additional Guides

10 This document supplements the following guides:

a) Oracle Linux Virtualization Manager: Getting Started Guide

b) Oracle Linux Virtualization Manager Administration Guide

c) oVirt Administration Guide (upstream OLVM documentation)

d) oVirt Upgrade Guide

e) oVirt Virtual Machine Management Guide

f) oVirt Introduction to the VM Portal

g) Oracle Linux KVM User's Guide

h) Oracle Linux v7.6 Common Criteria Guidance Document, v0.9 [OL7-CC]

11 **NOTE:** The information in this guide supersedes related information in other documentation.

2 Secure Acceptance and Installation

2.1 Obtaining the TOE

12 The TOE is obtained from the Oracle Software Delivery Cloud at https://edelivery.oracle.com.

13 To download the TOE:

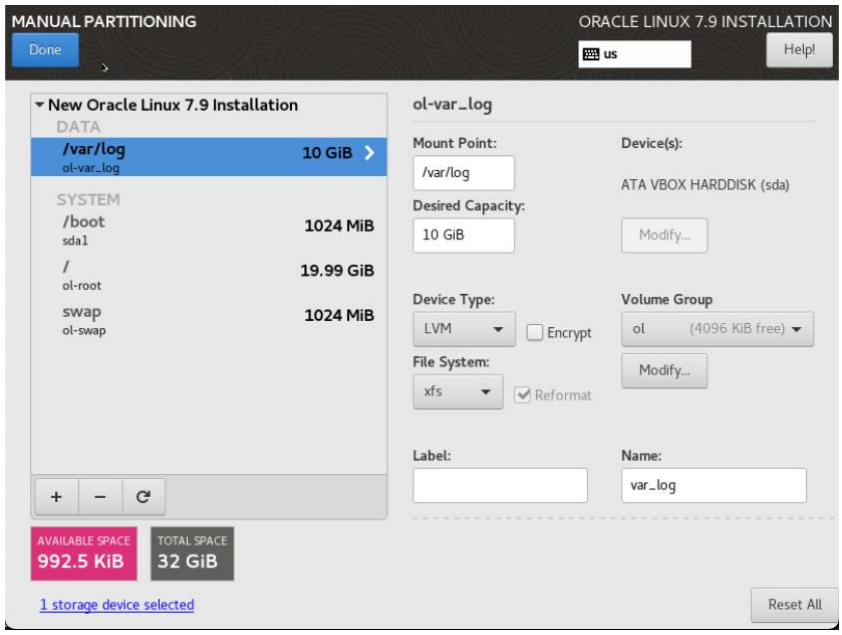
1) Login to the edelivery website.
2) Search for “Oracle Linux 7.6” and select the Oracle Linux 7.6 download package.
3) Press the continue button.
4) Select the x86 64 bit option and press continue.
5) Read and accept all license agreements.
6) Select “V980739-01.iso” and click download.

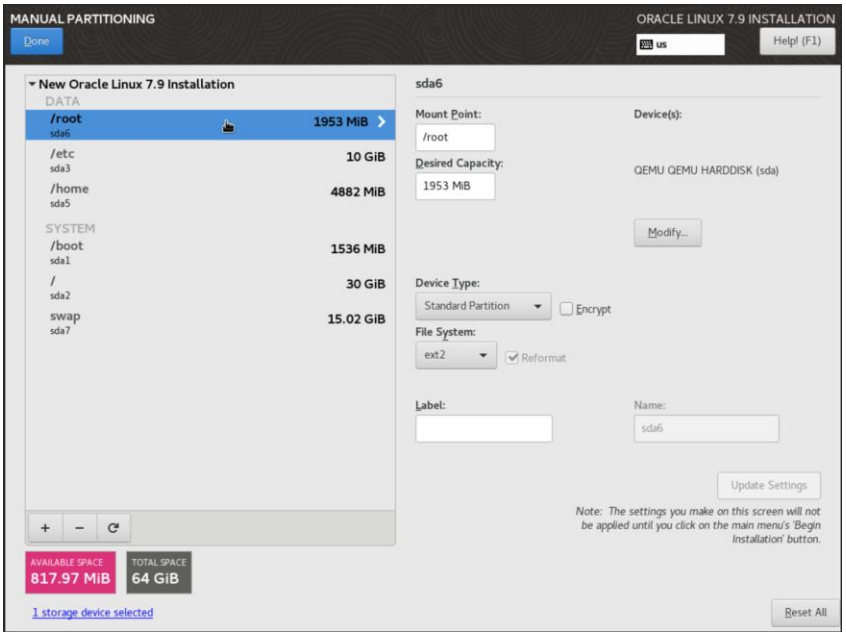
14 Note: KVM is built into the Oracle Linux Unbreakable Enterprise Kernel (UEK) release by default.

2.2 Installing the TOE

15 To install the TOE:

1) Install the V980739-01.iso.
2) At first (red) page, select “Install Oracle 7.6”.
3) At “Welcome to Oracle Linux 7.6” select language and press “continue”.
4) At Installation Summary page, keep “Minimal Install” for Software Selection and "Custom partitioning selected" for Installation Destination; create a dedicated mount point create a dedicated mount point(s) as follow:
   - For OS logs (/var/log) with 10GB of disk space
   - non-journaled filesystem (/etc) with 10GB of disk space (ext2 filesystem type)
   - non-journaled filesystem (/home) with 5GB of disk space (ext2 filesystem type)
   - non-journaled filesystem (/root) with 2GB of disk space (ext2 filesystem type)





5) Reboot, selecting the UEK Kernel (1st option).

6) Create the “yumlog” script in accordance with Annex A: Yumlog Script

   Note: All updates must be performed using the ‘yumlog’ command to ensure required logs are maintained. This is applicable to any updates applied to the TOE.

7) Update the kernel to the evaluated version:

   ```
   # yumlog update kernel-uek-4.14.35-2047.507.7.5.el7uek
   ```

8) Reboot.

9) Install the correct version of OpenSSL and dependencies:

```
# yumlog install openssl-1.0.2k-25.el7_9 openssl-libs-
1.0.2k-25.el7_9 openssl-devel-1.0.2k-25.el7_9
```

10) As per https://docs.oracle.com/en/virtualization/getstart/manager-install.html#manager-install-prepare, install the Oracle Linux Virtualization Manager Release 4.3.10 package and enable the required repositories:

```
# yumlog install oracle-ovirt-release-el7
# yumlog install yum-utils
# yum clean all
# yum repolist
```

Ensure the following repositories are enabled:

- ol7_latest,
- ol7_optional_latest,
- ol7_kvm_utils,
- ol7_gluster6,
- ovirt-4.3,
- ovirt-4.3-extra.

11) Disable ovirt-4.2 and ovirt-4.2-extra:

```
# yum-config-manager --disable ovirt-4.2
# yum-config-manager --disable ovirt-4.2-extra
```

12) If ol7_UEKR6 is enabled, then do the following to re-enable the UEK5 repo:

```
# yum-config-manager --disable ol7_UEKR6
# yum-config-manager --enable ol7_UEKR5
# yum clean all
# yum repolist
```

13) Confirm ol7_UEKR5 is enabled, and ol7_UEKR6 is disabled by verifying the absence of ol7_UEKR6:

```
# yum repolist
```

14) Install the Oracle Linux Virtualization Manager Release 4.3.10 package:

```
# yumlog install ovirt-engine-4.3.10.4-1.0.21.el7
```

15) qemu-kvm, libvirt and all the other KVM user space components are installed when you discover/add the KVM server by OLVM web console. However, to install sooner, and to confirm qemu-kvm and libvirt versions:

```
#yumlog groupinstall "Virtualization Host"
#yumlog install qemu-kvm virt-install virt-viewer
```

16) Verify with `#yum list qemu` that qemu is version 4.2.1-11 and `#yum list libvirt` that libvirt is 5.7.0-20.el7.

2.2.1 Enabling FIPS Mode

16 To enable FIPS mode:

- Enter the command: `touch /etc/system-fips`
- Modify the `/etc/sysconfig/sshd` and `/etc/sysconfig/httpd` files by adding the following parameter: `OPENSSL_FORCE_FIPS_MODE=1`
- Update yumlog with the following:

```
# Enable FIPS mode
Export OPENSSL_FORCE_FIPS_MODE=1
```

2.2.2 Performing Local Updates

17 In environments that require local updates, these may be performed in accordance with the following guidance.

18 Update `/etc/yum.conf` so that the TOE performs signature checking on local packages:

```
local_gpgcheck=1
```

19 Use the yumdownloader to download the required packages:

```
# yumdownloader qemu-kvm-4.2.1-13.el7 qemu-common-4.2.1-13.el7
qemu-system-x86-4.2.1-13.el7 qemu-system-x86-core-4.2.1-13.el7
```

20 Install using yumlog:

```
# yumlog install ./qemu-kvm-4.2.1-13.el7.x86_64.rpm ./qemu-
system-x86-4.2.1-13.el7.x86_64.rpm ./qemu-system-x86-core-
4.2.1-13.el7.x86_64.rpm ./qemu-common-4.2.1-13.el7.x86_64-
modified.rpm
```

2.2.3 mod_proxy_wstunnel Mitigation

21 By default, the TOE is installed with the mod_proxy_wstunnel loaded. To mitigate the vulnerability associated with its use, CVE-2019-17567, follow the instructions provided at: https://access.redhat.com/security/cve/cve-2019-17567.

2.3 Verifying the TOE

22 To verify that Oracle Linux 7.6 UEK 5 is installed:

```
[root@localhost ~]# uname -r
4.14.35-2047.507.7.5.el7uek.x86_64
```

23 **Note:** Numbers starting with 4.14.35 identifies UEK5.

24 To verify that Virtualization Manager 4.3 is installed:

```
[root@ovirt: ~]# yum list ovirt-engine
ovirt-engine-4.3.10.4-1.0.1.el7
```

3 Configuration Guidance

3.1 Services Configuration

3.1.1 Hardware-Based Isolation

25 The TOE supports Intel VT-x and Intel VT-d hardware-based isolation mechanisms which are enabled by default. No configuration is required. Use the following commands to verify that the mechanisms are enabled:

```
# cat /proc/cpuinfo
```

```
# virt-host-validate
```

26 The `cat /proc/cpuinfo` command should contain the “vmx” flag to show Intel VT-x virtualization support is enabled in BIOS.

27 The `virt-host-validate` command should be displayed as follows:

```
QEMU: Checking for hardware virtualization                 : PASS
QEMU: Checking for device /dev/kvm                         : PASS
QEMU: Checking for device /dev/vhost-net                   : PASS
QEMU: Checking for device /dev/net/tun                     : PASS
 LXC: Checking for Linux >= 2.6.26                         : PASS
```

3.1.2 Physical Platform Resource Control

28 Physical platform resources that may be made available to VMs by an administrator are:

a) CPU

b) Memory

c) Network Adapter (Physical NIC)

29 Configuration of physical devices can be done by following Virtual Machine Management Guide Host Devices.

30 Configuration of Virtual-Disks can be performed by following Virtual Disk Tasks.

31 Physical NICs can be configured following Editing Host Network Interfaces and Assigning Logical Networks to Hosts. Passthrough is configured by Enabling passthrough on a vNIC Profile.

3.1.3 VM User Interface

32 Users interact with VMs according as described in oVirt Introduction to the VM Portal

3.1.4 VS Self Protection

33 The TOE functions for self-protection from hardware assists and hypervisor calls are enabled by default and do not require configuration.

3.1.5 Separation of Management and Operational Networks

34 Separate Management and Operational Networks can be configured by Attaching and Configuring a Logical Network to a Host Network Interface.

3.1.6 External Services

35 To restrict libvirt to local virtualization host, execute the following commands:

```
# firewall-cmd --permanent --remove-service=libvirt-tls
# firewall-cmd –reload
```

36 To disable cockpit, execute the following commands:

```
# systemctl disable cockpit
# systemctl disable cockpit.socket
```

3.2 Secure Administration

3.2.1 Syslog Configuration

37 When syslog is configured in accordance with this section, logs will be sent to the remote syslog server as soon as they are generated. If the remote server is not available, the logs will not be sent to the server.

38 To configure the TOE to send audit records to a remote syslog server, follow the instructions provided at: https://blogs.oracle.com/scoter/post/oracle-linux-encrypted-rsyslog-over-ssh augmented as follows:

a) **Correction to SSH instructions.** Replace the “Configuring ssh Reverse Tunnel” command and example with:

```
# ssh -nN -L 10514:<syslog-client-host>:6514 <syslog-server-host>
```

Example:

```
# ssh -nN -L 10514:127.0.0.1:6514 ol7-server
```

Note: Requires SSH Configuration described in section 3.2.3.

b) **Add local logs to be forwarded to syslog.** Insert the following lines into the “ol7client.conf” file created per the “Configuring rsyslog on syslog client” instructions:

```
# add ovirt-engine logs
$ModLoad imfile
$InputFileName /var/log/ovirt-engine/engine.log
$InputFileTag tag_ovirt_engine_log:
$InputFileStateFile ovirt_engine_log
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor


$InputFileName /var/log/ovirt-engine/server.log
$InputFileTag tag_ovirt_server_log:
```

```
$InputFileStateFile ovirt_server_log
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor

$InputFileName /var/log/httpd/ssl_error_log
$InputFileTag httpd_error_log:
$InputFileStateFile httpd_error_log
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor

$InputFileName /var/log/httpd/access_log
$InputFileTag httpd_access_log:
$InputFileStateFile httpd_access_log
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor

$InputFileName /var/log/httpd/ssl_request_log
$InputFileTag httpd_ssl_request_log:
$InputFileStateFile httpd_ssl_request_log
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor

$InputFileName /var/log/httpd/ssl_access_log
$InputFileTag httpd_ssl_access_log:
$InputFileStateFile httpd_ssl_access_log
```

```
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor

$InputFileName /var/log/httpd/ovirt-requests-log
$InputFileTag httpd_ovirt_requests_log:
$InputFileStateFile httpd__ovirt_requests_log
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor

# add ovirt-engine vdsm (kvm-server) logs
$ModLoad imfile
$InputFileName /var/log/vdsm/supervdsm.log
$InputFileTag tag_ovirt_supervdsm_log:
$InputFileStateFile ovirt_supervdsm_log
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor

$InputFileName /var/log/vdsm/vdsm.log
$InputFileTag tag_ovirt_vdsm_log:
$InputFileStateFile ovirt_vdsm_log
$InputFileSeverity info
$InputFileFacility local6
$InputFilePollInterval 1
$InputFilePersistStateInterval 1
$InputRunFileMonitor

$InputFileName /var/log/vdsm/mom.log
$InputFileTag tag_ovirt_mom_log:
```

$InputFileStateFile ovirt_mom_log

$InputFileSeverity info

$InputFileFacility local6

$InputFilePollInterval 1

$InputFilePersistStateInterval 1

$InputRunFileMonitor

3.2.2 TLS Configuration

39 To generate TLS public and private keys, refer to section 3.4 below.

40 To configure the TLS cipher suites, add the following parameter to the `/etc/httpd/conf.d/ssl.conf` file:

```
SSLCipherSuite AES128-SHA: DHE-RSA-AES128-SHA256: DHE-RSA-AES256-SHA256
```

41 For the DHE cipher suites, the FFC keys are determined by the RSA X.509 key sizes (i.e. 2048 and 3072 bit keys). For instructions on replacing the oVIRT engine CA certificate, follow these instructions: https://ovirt.org/documentation/administration_guide/index.html#replacing-manager-apache-ca-certificate.

3.2.3 SSH Configuration

42 To generate SSH public and private keys, refer to section 3.4 below.

3.2.3.1 SSH Installation

43 In the evaluated configuration SSH acts as both a server and client. Ensure SSH is installed or updated, as follows:

```
# yum install openssh openssh-server
# yum install openssh openssh-client
```

Start the sshd service and configure it to start following a system reboot, as follows:

```
# systemctl start sshd
# systemctl enable sshd
```

3.2.3.2 SSH Server and Client Configuration Parameters

44 **SSH Server**

45 To configure the SSH server protocol, add or uncomment the following parameters in the `/etc/ssh/sshd_config` file:

```
# Ciphers aes-ctr-128, aes-ctr-256, aes-cbc-128, aes-cbc-256
# MACs hmac-sha1, hmac-sha2-256, hmac-sha2-512
# KexAlgorithms diffie-hellman-group14-sha1
# HostKeyAlgorithms rsa-sha2-512,rsa-sha2-256,ssh-rsa
# PubkeyAcceptedKeyTypes rsa-sha2-512,rsa-sha2-256,ssh-rsa
# HostKey /etc/ssh/ssh_host_rsa_key
```

```
# AuthorizedKeysFile /etc/ssh/authorized_keys
# PubkeyAuthentication yes
# PasswordAuthentication yes
# AuthenticationMethods publickey, password
```

46 **SSH Client**

47 To configure the SSH client protocol, add the following parameters to the `/etc/ssh/ssh_config` file:

```
# Ciphers aes-ctr-128, aes-ctr-256, aes-cbc-128, aes-cbc-256
# MACs hmac-sha1, hmac-sha2-256, hmac-sha2-512
# KexAlgorithms diffie-hellman-group14-sha1
# HostKeyAlgorithms rsa-sha2-512
# HostKey /etc/ssh/ssh_host_rsa_key
# AuthorizedKeysFile /etc/ssh/authorized_keys
# PubkeyAuthentication yes
# PasswordAuthentication no
# AuthenticationMethods publickey
```

3.2.4 Admin/User Authentication

48 The following interfaces are available:

a) **CLI over SSH.** The Oracle Linux CLI can be accessed over SSH in accordance with [OL7-CC] *Configuring SSH > Using Public Key Authentication*. An SSH client should be used to connect. Once successful authentication is complete, the user will be provided with the command prompt. Password-based authentication is also supported in the evaluated configuration.

b) **VM Portal over HTTPS.** The VM Portal presents a comprehensive view of a virtual machine and allows the user to start, stop, edit, and view details of a virtual machine. The actions available to a user in the VM Portal are set by a system administrator. System administrators can delegate additional administration tasks to a user. Usage and configuration of the VM Portal is described at oVirt Introduction to the VM Portal

Note: VMs are assigned a unique name when they are created. This name is displayed to users of the VM in the title bar of the Remote Viewer window in which the VM is running.

c) **Administration Portal over HTTPS.** The Administration Portal provides system administrators with the ability to manage the TOE as described at oVirt Administration Guide (upstream OLVM documentation)

3.2.5 Password Policies

49 Administrators should use strong passwords in accordance with relevant organizational policies.

3.2.5.1 Oracle Linux Password Configuration

50 Modify `/etc/security/pwquality.conf` to require 1 Uppercase letter, 1 lowercase letter, 1 number and 1 special characters with a minimum password length of 15 characters – set parameters:

```
minlen = 15
dcredit = 0
ucredit = 0
lcredit = 0
ocredit = 0
minclass = 4
```

51 Modify `/etc/pam.d/system-auth` to include "`enforce_for_root`" in the password requisite field with `pam_pwquality.so`:

```
password    requisite     pam_pwquality.so try_first_pass
local_users_only enforce_for_root retry=3 authtok_type=
```

3.2.5.2 OLVM Password Configuration

52 Set password complexity to require 1 Uppercase letter, 1 Lowercase letter, 1 number and 1 special character:

```
ovirt-aaa-jdbc-tool settings set --name=PASSWORD_COMPLEXITY --
value='UPPERCASE:chars=ABCDEFGHIJKLMNOPQRSTUVWXYZ::min=1::LOWE
RCASE:chars=abcdefghijklmnopqrstuvwxyz::min=1::NUMBERS:chars=0
123456789::min=1::SPECIAL:chars=!@#$%^&*()::min=1::'
```

53 Set password minimum length to 15 characters:

```
ovirt-aaa-jdbc-tool settings set --name "MIN_LENGTH" --value
15
```

54 For additional password configuration parameters, refer to: http://machacekondra.blogspot.com/2015/

3.2.6 TOE Access Banner

3.2.6.1 Configuring the OLVM Web GUI Access Banner

55 To configure the OLVM Web GUI access banner:

1) Copy the welcome_page_template from the ovirt branding path to the OLVM branding:

   ```
   # cp /usr/share/ovirt-
   engine/brands/ovirt.brand/welcome_page.template
   /usr/share/olvm-branding/oracle-branding/admin-portal
   ```

2) Edit the `/usr/share/olvm-branding/oracle-branding/admin-portal/branding.properties` file by uncommenting and setting the following parameter:

   ```
   welcome_replace=true
   ```

3) Edit the advisory warning at the beginning of the welcome_page.template at `/usr/share/olvm-branding/oracle-branding/admin-portal/welcome_page.template`, for example:

* Access to this environment available only to authorized users!
*

4) Restart OLVM: `# systemctl restart ovirt-engine`

3.2.6.2 Configuring the SSH Access Banner

56 To configure the SSH Access Banner:

1) Edit the `/etc/ssh/sshd_config` file by adding the following parameter:

   ```
   Banner /etc/ssh/my_banner
   ```

2) Create the my_banner file (`/etc/ssh/my_banner`) and edit to include a warning advisory message.

3) Restart the sshd service:

   ```
   # systemctl sshd restart
   ```

3.2.7 Audit Rules

57 To ensure that the TOE audits administrative actions, the following rules must be appended to `/etc/audit/rules.d/audit.rules`:

```
-w /etc/ssh/ssh_config -p wa
-w /etc/ssh/sshd_config -p wa
-w /etc/ssh/my_banner -p wa
-w /etc/rsyslog.d -p wa
-w /usr/share/olvm-branding/oracle-branding/admin-portal/welcome_page.template -p wa
-w /etc/security/pwquality.conf -p wa
-w /etc/pam.d/system-auth -p wa
-w /etc/chrony.conf -p wa
```

58 The TOE will log when a software update fails. Additional details of failed software updates may be verified under `/var/log/yum.log`.

3.3 Log Types and Format

Logs that are generated by the TOE follow the type and format identified in the following link: https://access.redhat.com/articles/4409591.

3.4 Key Generation

59 To generate SSH public and private keys used in the evaluated configuration, enter the following commands:

```
ssh-keygen -t rsa -b 2048
ssh-keygen -t rsa -b 3072
```

60 To generate TLS public and private keys used in the evaluated configuration, enter the following commands:

```
openssl genrsa -out <server_private.key> 2048
openssl genrsa -out <server_private.key> 3072
```

4 Annex A: Yumlog Script

61 The administrator must create the following script "yumlog" to enable logging of trusted updates.

62 The script must be placed in `/sbin/`

```
#!/bin/env bash


LOG=$(cat /etc/yum.conf | grep logfile | sed -e
's/\([^=]*\)=\s*\(.*\)$/\2/')

LOG=${LOG:-/var/log/yum.log}


echo "$(date): $(id) has initiated an install using yum" >>
$LOG


stdbuf -i0 -o0 -e0 yum $@ 2>&1 | tee -i -a $LOG


ERR=$?

# Set as error unless otherwise told

msg="Error"


case "$ERR" in
      "0")    msg="Success" ;;
      # See man yum.conf for 'check-update'
      "100")  msg="Updates available" ;;
      *)      msg="Error"   ;;
esac
echo "$(date): yum returned exit code $ERR ($msg)" >> $LOG


exit $ERR
```

63 Once create, the script must be made executable:

```
chmod +x yumlog
```