Red Hat

Red Hat Enterprise Linux 9.0 EUS

Common Criteria Guide

Version 1.1

January 2024

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 the Red Hat Enterprise Linux 9.0 EUS 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 Red Hat Enterprise Linux 9.0 EUS guidance resources in 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 following requirement specifications available at https://www.niap-ccevs.org/Profile/PP.cfm:

a) Protection Profile for General Purpose Operating Systems, Version 4.3 (PP_OS_V4.3)

b) Functional Package for Transport Layer Security (TLS), Version 1.1 (PKG_TLS_V1.1)

c) Functional Package for Secure Shell (SSH), Version 1.0 (PKG_SSH_V1.0)

1.3.2 Evaluated Version

5 The Target of Evaluation (TOE) is Red Hat Enterprise Linux 9.0 Extended Update Support.

1.3.3 Non-TOE Components

6 The following components must be present in the operational environment to operate the TOE in the evaluated configuration:

a) **Update Server.** The TOE receives updates from an organization's local repository via TLS.

b) **SSH Server.** The TOE is capable of securely communicating with an SSHv2 server.

c) **SSH Client.** The TOE is capable of securely communicating with an SSHv2 client.

d) **Compute Platform.** The TOE requires a compute platform meeting the following specifications:

i) Intel Xeon Silver x86-64 UEFI platforms (of Cascade Lake microarchitecture)

ii) IBM z16 (LPAR) platforms with UEFI 2.3.1 or later.

iii) Power10 PowerVM (LPAR) platforms with UEFI 2.3.1 or later.

7 Platforms that meet the above specifications and were tested with the TOE in this evaluation are listed in Table 1.

Table 1: Tested Platforms

Vendor	Model	CPU
Dell	PowerEdge R440	Xeon Silver 4216 (Cascade Lake)
IBM	z16 3931-A01	IBM z16
IBM	POWER10 9080-HEX	Power10

1.3.4 Functions not included in the TOE Evaluation

8 Only the functions listed in [ST] Section 2.3 are addressed by this evaluation. The use of any other cryptographic engines or the following product functions are not included within the scope of the evaluation:

a) SELinux Mandatory Access Control System

b) OS Virtualization Infrastructure

c) Containerization Infrastructure

d) Gnome desktop environment

1.3.5 Evaluation Assumptions

9 The following assumptions about the operational environment 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 2: Evaluation Assumptions

Assumption	Guidance
The OS relies on being installed on trusted hardware.	Use trustworthy platforms such as those listed in section 1.3.3.
The user of the OS is not wilfully negligent or hostile, and uses the software within compliance of the applied enterprise security policy. Standard user accounts are provisioned in accordance with the least privilege model. Users requiring higher levels of access should have a separate account dedicated for that use.	Users should be trained in enterprise security policies. Don't provide users with more system privileges than they require. Consider using separate accounts for highly privileged users.
The administrator of the OS is not careless, wilfully negligent or hostile, and administers	Administrators should be trained in enterprise security policies.

Assumption	Guidance
the OS within compliance of the applied enterprise security policy.	The OS cannot protect against hostile or negligent administrators – deploying organizations should implement appropriate controls for their environment to mitigate this risk factor (e.g. vetting, training, auditing etc.).

1.4 Conventions

10 The following conventions are used in this guide:

a) `CLI Command, path or text <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.

1.5 Related Guidance

11 [RHEL] Red Hat Enterprise Linux 9, Configuring Basic System Settings, 2023-11-08

This document can be downloaded from:
https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/configuring_basic_system_settings/index

12 **NOTE:** The information in this CC Guide supersedes related information in the general user guidance unless otherwise stated or referenced.

2 Pre-requisites

2.1 Systems Required to Support the Install

13 To install the TOE, you will need 3 supporting systems:

a) A host for accessing https://access.redhat.com/ and downloading the installation image.

b) A system running Red Hat Enterprise Linux 9.0 EUS with the Extended Update Support (EUS) subscription, for extracting additional files from the cc-config RPM package as described here:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/performing_a_standard_rhel_9_installation/installation-methods-advanced_installing-rhel

NOTE: This is not the TOE.

c) A web server for temporarily hosting files required for the TOE installation. See instructions at 2.1.1 for using the above RHEL-9.0 system for this purpose.

d) An FTP server for installation of IBM Z LPAR systems as described in Section 2.1.2.

14 Depending on your company infrastructure, these may be satisfied by the same host.

2.1.1 Web Server (for TOE installation files)

15 Instructions for configuring a web server to host files required for the TOE installation can be found here:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/deploying_web_servers_and_reverse_proxies/setting-apache-http-server_deploying-web-servers-and-reverse-proxies#setting-up-a-single-instance-apache-http-server_setting-apache-http-server

2.1.2 FTP Server (for IBM Z installations)

16 Instructions for configuring an FTP server to host files required for the TOE installation on IBM Z LPAR systems can be found here:

https://access.redhat.com/solutions/1421563

2.2 Hardware Platform

2.2.1 Dell PowerEdge Systems

17 Dell PowerEdge platforms must be configured to use UEFI boot, with Secure Boot signature checking enabled prior to installation of the operating system.

18 Boot the hardware into a system setup (BIOS) configuration software, using iDRAC Virtual Console or by pressing F2 during early boot.

a) Navigate to System BIOS

b) Under Boot Settings, set Boot Mode to UEFI

c) Under System Security, set

i) Secure Boot to Enabled

ii) Secure Boot Policy to Standard

iii) Secure Boot Mode to Deployed

19 Then press the Esc key several times and, when asked, save the modified settings and reboot.

20 To enable the local serial console on Dell PowerEdge systems, the following process must be executed:

a) Modify the /etc/default/grub file to enable console connections.

```
vim /etc/default/grub

GRUB_CMDLINE_LINUX_DEFAULT="console=tty0 console=ttyS0,9600n8"

GRUB_TERMINAL="console serial"
```

```
GRUB_SERIAL_COMMAND="serial --speed=9600 --unit=0 --word=8 --
parity=no --stop=1"
```

Note: Baud rate must be consistent with the terminal and Dell PowerEdge system.

b) Rebuild the grub configuration file.

```
grub2-mkconfig -o /boot/efi/EFI/redhat/grub.cfg
```

c) Reboot the TOE.

2.2.2 IBM Z Systems

21 No specific pre-requisites are required for IBM Z systems.

2.2.3 IBM Power10 Systems

22 IBM PowerVM LPARs need to be configured with Secure Boot signature checking disabled prior to the installation of the operating system, otherwise it won't be possible to boot from the mounted DVD ISO file. Secure Boot needs to be enabled only after the installation. Changing Secure Boot configuration is only possible for LPAR that has been shut down so make sure to do so first. Then in the Hardware Management Console (HMC):

a) Under Partitions click on the LPAR.

b) Navigate to Properties, General Properties and then Advanced Settings.

c) Set Secure Boot to "Disabled" or "Enabled and Log only".

d) Save the configuration.

3 Secure Acceptance and Update

3.1 Obtaining the TOE

23 Red Hat Enterprise Linux 9.0 is downloaded from https://access.redhat.com/

24 You will need to download the following:

a) A Red Hat Enterprise Linux 9.0 installation image (ISO)

b) The cc-config RPM package with additional installation files

c) Select RPM packages (updated versions of the ones bundled on the ISO)

3.1.1 Red Hat Enterprise Linux 9.0 Installation Image (ISO)

25 Perform the following steps to obtain the Red Hat Enterprise Linux 9.0 ISO:

a) Log in to https://access.redhat.com/

b) Click on 'Downloads' in the top left corner

c) Click on the 'Red Hat Enterprise Linux' link under ‘Product’ and then click on the ‘All Red Hat Enterprise Linux Downloads’.

i) For installation on Dell PowerEdge, select 'Red Hat Enterprise Linux for x86_64' as a Product Variant and '9.0' as the version

ii) For installation on IBM Z, search for the 'Red Hat Enterprise Linux for IBM z Systems' as a Product Variant and '9.0' as the version

iii) For installation on IBM Power, search for the ‘Red Hat Enterprise Linux for Power, little endian’ as a Product Variant and '9.0' as the version

d) Below, under 'Product Software' you should see a section called 'Full installation image' and a line with 'Red Hat Enterprise Linux 9.0 Binary DVD'

e) Click 'Download Now' on the right side of that line

NOTE: You may need to follow additional instructions to either burn a DVD or write to a bootable USB drive or otherwise make the ISO available to the hardware.

26 See the related RHEL documentation for instructions for your environment: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/performing_a_standard_rhel_9_installation/assembly_preparing-for-your-installation_installing-rhel#assembly_creating-a-bootable-installation-medium_assembly_preparing-for-your-installation

3.1.2 cc-config RPM Package

27 The cc-config RPM package is Red Hat's way of shipping additional installation files to customers through trusted channels, requiring a RHEL Extended Update Support (EUS) subscription to access.

28 Perform the following steps to obtain the RPM:

a) Log in to https://access.redhat.com/

b) Click on 'Downloads' in the top left corner

c) Click on the 'Red Hat Enterprise Linux' link under Product

d) Select 'Red Hat Enterprise Linux for x86_64 - Extended Update Support' as a Product Variant and '9.0' as the version

e) Click on the 'Packages' tab.

f) In the 'Search' field, enter cc-config without a version or release.

g) In the list of filtered results, click on the cc-config item (not 'Download Latest')

h) Select the 9.0 in the 'Version' tab.

i) In the download RPM section at the bottom, click on the 'Download Now' button beside the package name.

29 After transferring the downloaded file to a RHEL-9.0 system, you can install it:

```
rpm -ivh cc-config-9.0-*.rpm
```

NOTE: Alternatively, you can install the RPM directly on a RHEL-9.0 system with an EUS subscription:

```
dnf install cc-config-9.0
```

30 In either case, you should find the additional installation files in

```
/usr/share/cc-config
```

31 One of these files is an Anaconda Kickstart, an automated script for Anaconda, the RHEL installer, a file named ospp.ks. This "kickstart" is required for the next steps.

32 Note that the cc-config RPM package itself is NOT used by or installed on the TOE. It is just to supply the additional installation files.

3.1.3 Additional RPM Packages

33 Open the kickstart ospp.ks file in a text editor and find a section called sanity_check_nvrs which contains a list of RPM packages described in several columns titled:

a) Source RPM

b) Name

c) Version

d) Release

e) Architectures

34 Download each of the listed RPMs following the same procedure as for downloading cc-config (previous section), using the Name for the initial search, and concatenating Version and Release with a dash (-), selecting it in the Version dropdown on the website.

35 Alternatively, from the RHEL-9.0 EUS subscribed system, use dnf download to download each package individually:

```
dnf download Name-Version-Release.Architecture.rpm
```

36 Note that a package may have noarch as an architecture, in which case it is installable on any hardware architecture.

3.2 Updating the TOE

37 Updates to the TOE must be distributed using a local repository that supports TLS. All updates are signed using a Red Hat controlled RSA 4096 key, so the administrator can be assured of the authenticity of the updates.

3.2.1 Create a Local Repository

38 The TOE must obtain updates from a local repository that supports TLS.

39 During the set up and configuration of this local repo, the admin must make sure that the only rpms being served to the TOE are restricted to those of EUS.

```
rhel-9-for-x86_64-appstream-eus-rpms
rhel-9-for-x86_64-baseos-eus-rpms
```

3.2.2 Configure the TOE to use the Local Repo

3.2.2.1 Add the Repo

40 On the TOE, add the local repos from the server to the TOE's YUM configuration:

sudo vim /etc/yum.repos.d/local-cc.repo

41 Next, paste the following configuration (be sure to change the server IP address according to the TOE environment).

```
[LocalServerRepo]
name=LocalServerRepo
enabled=1
gpgcheck=1
sslverifystatus=1
baseurl=https://<server_ip>/<path_to_repo>
```

42 Finally, test the repo by installing a package.

```
sudo dnf install <package>
```

3.2.2.2 Manual Updates

43 The administrator uses the "dnf" program to check for updates and install updates. The command `dnf check-update` is used for checking whether any updates are available. The command `dnf update` is used to install available updates. dnf automatically verifies signatures when checking for and installing updates. dnf does not install an update if the signature check fails.

44 `dnf check-update` returns an exit value of:

a) 100 if there are packages available for an update and prints a list of the packages to be updated

b) 0 if no packages are available for update.

c) 1 if an error occurred (including invalid signatures)

45 `dnf update` prints messages indicating which packages were updated and any failures in the update process (including invalid signatures).

3.2.2.3 Automatic Updates

46 By default, the kickstart script and SCAP content installs Red Hat Enterprise Linux 9.0 EUS with automatic software updates enabled. The system checks for updates daily.

47 Run the following commands as an administrator to disable automatic software updates:

```
sudo systemctl disable dnf-automatic.timer
```

```
sudo systemctl stop dnf-automatic.timer
```

48 To enable automatic software updates, run the following commands as an administrator:

```
sudo vi /etc/dnf/automatic.conf
change upgrade_type to security
change apply_updates to yes
sudo systemctl enable --now dnf-automatic.timer
```

49 If all updates are to be automatically applied, omit the step to set upgrade_type to ‘security’ above. By default, all updates are applied.

4 Installation Procedures

4.1 Preparing the Installation Files

50 During the TOE installation, the installer needs some way of reaching the kickstart (ospp.ks) and additional RPM packages downloaded in previous steps. This is what the required HTTP/FTP server is for.

51 However, before the files are transferred to it, you need to:

a) Create a YUM (DNF) repository with the downloaded RPM packages

b) Modify ospp.ks to tell the installer where this repository will be hosted

4.1.1 Creating a YUM repository

52 On the RHEL-9.0 system, put all the downloaded RPM packages in a directory, and run the createrepo command on this directory.

```
mkdir  cc-custom
mv  *.rpm   cc-custom/
dnf install createrepo
createrepo cc-custom
```

53 You can now upload the cc-custom directory to the HTTP/FTP server.

4.1.2 Modifying the kickstart

54 Open ospp.ks in a text editor and search for a line beginning with:

```
#repo --name=cc-custom
```

55 Uncomment it (remove the leading hash symbol), and replace http://server.with.repositories/path/to/custom/repository/ with a valid URL to the cc-custom directory uploaded in the previous step.

56 Additionally, find and uncomment a line beginning with

```
#cdrom
```

This will be a few lines above the cc-custom URL.

57 Further, at the bottom of the ospp.ks file, replace

```
content-url = http://server/path/to/scap-security-guide.rpm
```

with a full URL to the scap-security-guide RPM package file, one of the additional RPM packages downloaded in the previous steps, and uploaded to the cc-custom

directory on the HTTP/FTP server. This is required because the OpenSCAP software cannot interact with the YUM/DNF repository directly, and needs its own URL.

58 The following modifications should be made to the kickstart according to your requirements:

a) change the root password

b) change the admin user and its password

c) change the bootloader password

d) alter disk partition sizes and adding optional extra partitions

e) customize the Pre-login banner

59 You can now save and upload this modified ospp.ks to the HTTP/FTP server. It doesn't need to be located inside the cc-custom directory.

4.2 Installing the TOE

60 **WARNING:** Before proceeding, make sure there is no valuable data stored on the TOE hardware. These installation steps may erase any data on any connected drives (including possible USB drives, excluding the USB drive containing the ISO image used for installation).

61 RHEL must be installed with FIPS mode enabled rather than enabling FIPS mode later. Enabling FIPS mode during the installation ensures that the system generates all keys with FIPS-approved algorithms and continuous monitoring tests in place. For more details see the RHEL documentation:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/security_hardening/assembly_installing-the-system-in-fips-mode_security-hardening

4.2.1 Installing on Dell PowerEdge

62 Boot the TOE hardware using the RHEL installation image (ISO). Early in this boot process, you should see the Grub2 boot loader, a black-and-white text interface with three lines, the middle line being selected:

```
Install Red Hat Enterprise Linux 9.0
Test this media & install Red Hat Enterprise Linux 9.0
Troubleshooting -->
```

63 Press the 'e' key to edit the selected middle entry, navigate the cursor (using arrow keys) to the line beginning with linuxefi, and append the following to it:

```
inst.ks=http://server-hostname/path/to/ospp.ks fips=1
```

64 Where http://server-hostname/path/to/ospp.ks is a valid reachable URL of the HTTP/FTP server and the path to ospp.ks on that server. The *fips=1* makes sure that the system will be installed with FIPS mode enabled.

65 The entire line should then look similar to:

```
linuxefi /images/pxeboot/vmlinuz inst.stage2=hd:LABEL=RHEL-9.0.0-BaseOS-x86_64rd.live.check quiet
inst.ks=http://download.yourcompany.tld/ospp.ks fips=1
```

66 If your HTTP/FTP server doesn't have a DNS hostname, you can use an IP address instead. If it further runs on a non-standard port, you can specify that too. For example:

```
inst.ks=http://192.168.1.1:8080/ospp.ks
```

67 You might want to add further options to the kernel command line, i.e. if your system uses static IP addresses instead of DHCP, add an ip= option with the correct arguments, as described by the dracut.cmdline(7) manpage or the RHEL documentation: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/boot_options_for_rhel_installer/kickstart-and-advanced-boot-options_boot-options-for-rhel-installer#network-boot-options_kickstart-and-advanced-boot-options

68 Once done, press [Ctrl]-[x] to begin the installation.

69 The installation should now finish automatically.

4.2.2 Installing on IBM Z LPAR

70 For installations on IBM Z, the standard RHEL documentation applies: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/performing_a_standard_rhel_9_installation/assembly_installing-on-64-bit-ibm-z_installing-rhel#booting-the-installation_assembly_installing-on-64-bit-ibm-z

71 Instead of the images/genericdvd.prm, a customized .prm file with

```
inst.ks=http://server-hostname/path/to/ospp.ks
```

72 This line should be used and referenced from the generic.ins file, where http://server-hostname/path/to/ospp.ks is a valid reachable URL of the HTTP/FTP server and the path to ospp.ks on that server.

73 When enabling FIPS mode, make sure that there is *fips=1* option appended to the very first line of the customized .prm file.

74 Installation then gets started using the Load from Removable Media or Server task in the Hardware Management Console (HMC).

75 After installation finishes, enable Secure Boot with the Enable Secure Boot for Linux checkbox in the Load task screen in the HMC.

4.2.3 Installing on IBM PowerVM LPAR

76 For installation on PowerVM LPAR, the IBM documentation applies: https://www.ibm.com/docs/en/linux-on-systems?topic=systems-installing-linux-powervm-lpar-by-using-hmc and https://www.ibm.com/docs/en/linux-on-systems?topic=aim-installing-linux-powervm-lpar-by-using-virtual-dvd-vdvd

77 Once the TOE hardware is booted using the RHEL installation image (ISO) follow instructions from the “Installing on Dell PowerEdge” section as for PowerVM Grub2 boot loader is also used.

78 After installation finishes, Secure Boot must be enabled.

a) In the Hardware Management Console (HMC), shut down the LPAR.

b) Then navigate to Properties of the LPAR, General Properties > Advanced Settings. Set Secure Boot option to “**Enabled and Enforced**”.

4.3 Post-installation steps

79 Perform shutdown and/or a removal of installation support systems (see section 2.1) as appropriate for your environment.

4.3.1 OpenSCAP Scan Validation

80 Once the RHEL installation is booted, perform verification that the TOE is in the evaluated configuration by running OpenSCAP scan. Follow instructions in section 6.8.2 "*Checking the system configuration",* then inspect a generated HTML report and make sure there are no failing SCAP rules present in the report.

5 Configuration Guidance

81 All steps in this section must be completed to achieve the CC evaluated configuration.

82 By default, the kickstart script and SCAP profile ‘ospp’ will set most necessary configurations to achieve the evaluated configuration. If certain functions have been manually misconfigured, it is possible to rerun the SCAP remediation to reset the configuration options that the rules in the ospp SCAP profile originally set.

83 In summary, the kickstart script and SCAP remediation will configure the following to achieve the evaluated configuration:

a) SSH parameters. See Section 5.1.1 for additional information.

b) Set the warning banner

c) Set timeout between failed authentication attempts

d) Set inactivity timeout

e) Configure audit storage parameters

f) Configure audit rules. See Section 5.3.1 for additional information.

g) Disable user namespaces

84 Additional information on SCAP can be found in Section 6.7

5.1 SSH Configurations

85 The TOE supports the same algorithms and properties in both SSH client and server implementations:

- Authentication Methods:
  - Public Key
  - Password
- Symmetric Algorithms:
  - aes256-ctr
  - aes256-gcm@openssh.com
- Public Key Algorithms:
  - rsa-sha2-256
  - rsa-sha2-512
  - ecdsa-sha2-nistp384
  - ecdsa-sha2-nistp521
- MACs:
  - hmac-sha2-256
  - hmac-sha2-512
  - implicit
- Key Exchange Methods:
  - diffie-hellman-group16-sha512 (RFC 8268)

- diffie-hellman-group18-sha512 (RFC 8268)
- ecdh-sha2-nistp384
- ecdh-sha2-nistp521

86 To ensure that the TOE is restricted to using the algorithms and characteristics listed above, configure the following option in /etc/crypto-policies/back-ends/openssl*.config:

```
SECLEVEL=3
```

5.1.1 Regenerate the ECDSA Host Key

87 RHEL supports the use of P-384 and P-521 curves when using an ECDSA hostkey. By default, RHEL will generate a P-256 ECDSA hostkey, however to achieve the evaluated configuration and comply with PP_OS_V4.3, the ECDSA hostkey must be updated to use the P-384 or P-521 curve by executing the following as the administrator:

```
“sudo ssh-keygen -t ecdsa -b <384|521> -f
/etc/ssh/ssh_host_ecdsa_key -N ''”
```

Note: Do not set a password for this key.

88 ‘*384*’ generates a P-384 key and ‘*521*’ generates a P-521 key.

89 Once the key has been generated, restart sshd by running:

```
sudo systemctl restart sshd.service
```

Note: By default, all files created by *ssh-keygen* are placed in the *.ssh* directory of their home directory. If a filename is given without a path, the key pair will end up in the directory, not in ~/.ssh/.

5.1.1.1 Configure SSH Public Key Authentication

90 To enable the authentication of users to the TOE via public key, first ensure that the following file exists:

```
~/.ssh/authorized_keys
```

91 Once the authorized_keys file exists, ensure that users’ public keys are copied or appended to this file.

5.2 NTP

92 The administrator can configure the name/address of the NTP server(s) by editing /etc/chrony.conf.

93 Within this file each NTP server is specified on a separate line using the syntax:

```
"server <FQDN/IP address> iburst"
```

94 Restart chrony for the changes to take effect:

```
service chronyd restart
```

5.3 Audit

95 The dnf must be reconfigured to store audit logs according to the OSPP:

```
echo -e "\nlogdir=/var/log/audit" >> /etc/dnf/dnf.conf
```

5.3.1 Configure Audit Rules

96 The `auditctl` command allows you to control the basic functionality of the Audit system and to define rules that decide which Audit events are logged. Persistent audit rules are kept in files at /etc/audit/rules.d/.

97 **NOTE:** All commands which interact with the Audit service and the Audit log files require root privileges. Ensure you execute these commands as the root user. Additionally, CAP_AUDIT_CONTROL is required to configure the audit services and CAP_AUDIT_WRITE is required to log user originating messages.

98 The TOE is preconfigured by the SCAP content to enable all auditing suggested by the OSPP Configuration Annex except successful file access. This is because this is normal system behavior rather than an exception to the access policy. And more importantly, it will fill up the logs making it harder to find policy violations.

99 If auditing successful file access is desired, this can be enabled by executing the following as the root user:

```
cp /usr/share/audit/sample-rules/30-ospp-v42-3-access-success.rules /etc/audit/rules.d/
restorecon /etc/audit/rules.d/*
service auditd restart
```

100 Audit listeners must be manually configured for the following events:

a) Changes to the /etc/issue, /etc/issue.net, and /etc/sshd.config files (modifying banner messages)

```
-a always,exit -F path=/etc/issue -F perm=wa
```

b) Changes to /etc/pam.d/system-auth (setting the timeout interval between failed authentication attempts).

```
-a always,exit -F path=/etc/pam.d/system-auth -F perm=wa
```

c) Changes to the /etc/tmux.conf file (modifying the inactivity timeout interval)

```
-a always,exit -F path=/etc/tmux.conf -F perm=wa
```

d) Changes to the /etc/audit/auditd.conf file (modifying audit storage parameters)

```
-a always,exit -F path=/etc/audit/auditd.conf -F perm=wa
```

e) Changes to the /etc/chrony.conf file (modifying NTP parameters)

```
-a always,exit -F path=/etc/chrony.conf -F perm=wa
```

101 After applying the changes, perform a restart of the audit service:

```
service auditd restart
```

102 For additional information, see Section 12.6 *“Using auditctl for defining and executing Audit rules”* of “Red Hat Enterprise Linux 9 Security Hardening”.

103 For specific command syntax, reference the ‘audit.rules’ manpage.

5.4 Software Restriction Policies (fapolicyd)

104 Fapolicyd is a daemon that determines whether or not access to files or execution of programs is allowed based on file path and sha256 hash. By default, all applications that are packaged by rpm are automatically trusted.

105 To enable fapolicyd integrity checks using SHA-256 hashes open the /etc/fapolicyd/fapolicyd.conf file in a text editor of your choice, for example:

sudo vi /etc/fapolicyd/fapolicyd.conf

106 Change the value of the integrity option from '*none*' to '*sha256*', save the file, and exit the editor:

integrity = sha256

Restart the fapolicyd service:

sudo systemctl restart fapolicyd

107 See Section 13.5 '*Enabling fapolicyd integrity checks'* of the Red Hat Enterprise Linux 9 Security Hardening guide for additional information.

108 New rules can be created in the /etc/fapolicyd/rules.d/ directory, for example:

```
touch /etc/fapolicyd/rules.d/80-myapps.rules
vi /etc/fapolicyd/rules.d/80-myapps.rules
```

109 To create a rule that allows the execution of all binaries in a directory (eg. /tmp/), add the following rule to a rule file:

```
allow perm=execute exe=/usr/bin/bash trust=1 : dir=/tmp/
trust=0
```

110 To create a rule that prevents changes to the content of a custom binary, the rule can be defined using a SHA-256 checksum:

```
allow perm=execute exe=/usr/bin/bash trust=1
:sha256hash=<hash_value>
```

111 The rules that ship with the daemon are set up to only audit denied access requests. It is possible to audit successful access by changing any rule in /etc/fapolicyd/rules.d from deny_audit to allow_audit. Restarting the daemon makes the rule take effect. It is not configured to audit successful access by default because it will result in a large quantity of audit events making it hard to find policy violations.

112 See fapolicyd.rules(5) and fapolicyd-cli(1) man pages for detailed information on creating rules.

113 See Section 13.4 '*Adding custom allow and deny rules for fapolicyd'* of the Red Hat Enterprise Linux 9 Security Hardening guide for additional information.

5.5 Updates

114 All updates to Red Hat Enterprise Linux are signed using a Red Hat controlled RSA 4096 key.

115 For additional information, refer to section 3.2.

6 Administration

116 This section details the steps for performing some administrative tasks manually as required for everyday administration of the TOE under normal operation.

6.1 Setting the Warning Banner

117 Edit the /etc/issue file to configure the warning banner that will be displayed prior to authentication attempts. The contents of the file will be displayed to the user.

6.2 Firewall

118 For additional information on administrative tasks pertaining to firewall functionality, see Chapter 1 of "Configuring firewalls and packet filters" found here:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html/configuring_firewalls_and_packet_filters/using-and-configuring-firewalld_firewall-packet-filters

6.3 User/Administrator Accounts

119 The default file permissions need to be restricted to prevent newly created files from being world accessible by running the following command as root:

```
echo -e "\numask 026" >> /etc/profile
```

This example sets the default group permissions to prevent writing (2). The administrator may set the default group permissions according to their organization's security policy.

120 For additional information on the administration of user and administrator accounts, see sections 9.2.1 '*Managing Accounts and Groups Using Command Line Tools'* and 10.2 '*Granting Sudo Access to a User'* in [RHEL].

6.4 Setting the Failed Authentication Parameters

121 The administrator can configure the timeout between failed authentication attempts by editing the /etc/pam.d/system-auth and /etc/pam.d/password-auth files:

```
auth     required    pam_faildelay.so  delay=<microseconds>
```

122 Apply the changes:

```
authselect apply-changes
```

123 The administrator can configure the threshold for locking a user account based on sequential failed authentication attempts by editing the /etc/security/faillock.conf file:

```
deny = <attempts>
```

A value of zero disables the failed authentication lockout.

124 The administrator can unlock a locked account by running:

```
faillock --user <user> --reset
```

6.5 Setting the Inactivity Timeout

125 The lock-command must be configured to terminate inactive sessions by changing the following in /etc/tmux.conf:

```
set -g lock-command vlock
```

to

```
set -g lock-command 'tmux kill-session'
```

126 The administrator can change the local inactivity timeout by changing the lock-after variable setting in /etc/tmux.conf to the desired number of seconds:

```
set -g lock-after-time <seconds>
```

A value of 0 disables the session inactivity timeout.

127 The tmux config must be reloaded for the changes to take effect. To ensure the configuration is reloaded for all users, it is recommended that all tmux servers are terminated or the system is rebooted:

```
pkill tmux
```

or

```
reboot
```

6.6 Password Policies

128 The password policy is enforced by the pam_pwquality PAM module which performs password quality checking. See the *pam_pwquality(8)* man page for additional information. The default policy that is set up by the kickstart guarantees a minimum length of 12 characters.

6.7 Audit Storage Settings

129 The administrator configures the local audit storage by editing /etc/audit/auditd.conf. The amount of local audit storage is determined by a combination of the num_logs and max_log_file settings:

num_logs = <0-999>

130 indicates the number of log files to rotate. When set to 0 or 1, a single log file is saved

max_log_file = <number>

131 This keyword specifies the maximum file size in megabytes. When this limit is reached, it will trigger a configurable action. The value given must be numeric.

max_log_file_action = <value>

132 This parameter tells the system what action to take when the system has detected that the max file size limit has been reached. Valid values are ignore, syslog, suspend, rotate, and keep_logs. If set to ignore, the audit daemon does nothing. syslog means that it will issue a warning to syslog. suspend will cause the audit daemon to stop writing records to the disk. The daemon will still be alive. The rotate option will cause the audit daemon to rotate the logs. It should be noted that logs with higher numbers are older than logs with lower numbers. This is the same convention used by the logrotate utility. The keep_logs option is similar to rotate except it does not use the num_logs setting. This prevents audit logs from being overwritten.

133 The amount of local storage used for audit logs is num_logs multiplied by max_log_file unless keep_logs is specified. All free space on the partition storing logs may be used when keep_logs is specified

6.8 SCAP

134 SCAP (Secure Content Automation Protocol) is a distinguishing feature of RHEL security. It is a standard created by NIST to allow content migration between certified security vendors to check or remediate the security posture of their system.

6.8.1 Viewing the OSPP configuration profile

135 The RHEL installation as previously described includes a package named scap-security-guide. In it, there is a datastream file for RHEL 9, ssg-rhel9-ds.xml. Within it is the OSPP profile which contains the evaluated configuration. A document that describes the evaluated configuration can be viewed by running the following command:

oscap xccdf generate guide --profile ospp /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml \ --output checklist.html

136 The checklist for the evaluated configuration is a full lockdown that not only meets the requirements for OSPP but exceeds them.

6.8.2 Checking the system configuration

137 The details of the evaluated configuration can be viewed with any web browser after generating the checklist. An administrator can verify the configuration of the system at any time.

138 The following command will show the profile name (ospp) in the file:

oscap info /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml

139 To verify the status of the profile being applied to the system, an administrator must use:

oscap xccdf eval --profile ospp /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml

140 This verification can also generate a HTML report via the --report option:

oscap xccdf eval --profile ospp --report report.html \

/usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml

6.8.3 System Remediation

141 If the system is found to be out of the evaluated configuration, it may be put back into configuration by performing an online remediation. Online remediation means that it remediates the system at the time of scanning. To restore the system to the evaluated configuration, run the following command as root:

oscap xccdf eval --remediate --profile ospp --results scan-xccdf-results.xml \

/usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml

142 The results of the command are stored into the scan results XML file. The output consists of two sections. The first section is a TestResult element in an XCCDF file which contains the results of the scan prior to the remediation. The second section contains fixed and error results. The fixed result indicates that the scan passed after the remediation. The error result indicates that even after applying the remediation, the evaluation still does not pass.

6.8.4 Tailoring the OSPP profile

143 Sometimes you need to customize SCAP content to match local policy and needs. For example, suppose you need to enable user namespaces for container applications. First edit the ospp sysctl file /etc/sysctl.d/70-cc-security.conf. Enable user namespace by changing the value of user.max_user_namespaces from 0 to any positive number such as 25. Save the file. Because of this change, the SCAP content will now complain about user namespaces being enabled. To stop this complaint, you would tailor the SCAP content to allow it. The way that you would do this is to use a RHEL workstation with scap-workbench installed. Ensure that the

SCAP content matching the OSPP evaluated configuration is also installed on the workstation. Follow these steps to create a tailoring file:

a) Open scap-workbench

b) Select RHEL 9 content, click on "Load Content"

c) Select "Protection Profile for General Purpose Operating System"

d) Click on the "Customize" button to create a new copy. Use the default name - click "OK"

e) In the search box, type "user_namespaces". Click the "Search" button.

f) If the search was successful, it will highlight the associated SCAP rule. In this case it is checked. Click on the checkmark to deselect this rule. Click "OK".

g) To save this change, click on the "File" menu item and then select "Save Customization Only".

h) In the dialog box give it the name "tailoring-file.xml" and click on "Save". This saves just the changes and not a whole profile.

i) The tailoring file can now be copied to a server in the OSPP configuration and used as follows (adjusting for the actual path to the tailoring file):

*oscap xccdf eval --tailoring-file tailoring-file.xml *

--profile ospp /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml

144 You can find more information about tailoring here:

https://www.open-scap.org/resources/documentation/customizing-scap-security-guide-for-your-use-case/

6.8.5 Changing to a new profile

145 One of the advantages of using SCAP for system configuration is that it makes it easy to move in and out of the evaluated configuration. If one day you were asked to reconfigure the system to meet the DISA STIG, then you would list the available profiles as mentioned here and then choose the STIG ID.

146 To see if your system conforms to the STIG, run the following command as root:

*oscap xccdf eval --profile xccdf_org.ssgproject.content_profile_stig *
/usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml

147 To then switch to the STIG, you would remediate as mentioned in a previous section:

*oscap xccdf eval --remediate --profile xccdf_org.ssgproject.content_profile_stig *
--results scan-xccdf-results.xml /usr/share/xml/scap/ssg/content/ssg-rhel9-ds.xml

148 More information can be found here:

https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/9/html-single/performing_a_standard_rhel_9_installation/index#deploying-systems-that-are-compliant-with-a-security-profile-immediately-after-an-installation_post-installation-tasks

6.9 SWID Tag

149 RHEL 9 ships with a Software Identification (SWID) tag to enable ISO/IEC 19770-2:2015 based software identification. This helps with software inventory management and application of rules based on the platform's identity. It is loosely

associated with SCAP and has been adopted by NIST. The tag's location is /usr/lib/swidtag/redhat.com/com.redhat.RHEL-9-<architecture>.swidtag with the symlink /etc/swid/swidtags.d/redhat.com pointing to the directory containing original file.

150 There will be two tags in the directory. The first is a primary tag that has no version. This tag has all of the mandatory fields populated describing the product. There will be another tag that has a version in its name, in this case 9.0. The second tag is a supplemental which identifies which version of RHEL 9 is installed. Together they describe the product and release.

6.10 TLS Usage

151 Red Hat Enterprise Linux leverages libcurl to provide application initiated TLS client for secure communication with remote systems and supports the following ciphersuites once configured with the ospp SCAP profile:

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384

TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

Note: Ensure that the TLS Server is properly configured to accept TLS 1.2 connections only.

152 RHEL also presents the following curves in the Supported Groups Extension without any additional configuration:

secp384r1

secp521r1

153 All cryptographic algorithms are automatically configured by default as part of the application of the SCAP profile.

154 RHEL 9 verifies that the presented identifier matches the reference identifier according to RFC 6125 as follows. The TOE establishes the reference identifier by parsing the DNS Name or IP address for the configured TLS server. The reference identifier is matched against the SAN, if present. If the SAN is not present, the referenced identifier is matched against the CN for DNS. For IP addresses, the TOE matches the identifier against the SAN only. The TOE supports wildcards in the DNS name of the server certificate. The TOE does not support URI reference identifiers, SRV reference identifiers, or certificate pinning.

155 Libcurl must be configured to use the following options:

CURLOPT_URL (Target URL)

CURLOPT_SSL_VERIFYHOST (Verify the certificate’s name against host)

CURLOPT_SSL_VERIFYSTATUS (Verify the certificate’s status, enables OCSP stapling)

156 These options can be set using the following:

curl_easy_setopt(curl, CURLOPT_URL, “https://example.com”)

curl_easy_setopt(curl, CURLOPT_SSL_VERIFYHOST, 2L)

curl_easy_setopt(curl, CURLOPT_SSL_VERIFYSTATUS, 1L)

157 For additional information see curl_easy_setopt(3), curlopt_url(3), curlopt_ssl_verifyhost(3), and curlopt_ssl_verifystatus(3) man pages.

158 Certificates are validated when the TOE receives the certificate during a TLS handshake and using the certificate path validation algorithm defined in RFC 5280. Revocation status is checked using OCSP stapling per RFC 6066.

6.11 Storage of Sensitive Data

159 RHEL follows standard conventions for storing sensitive data. Applications must store their sensitive data in the /etc directory with restrictive access permissions. Access to sensitive data should be restricted to root and/or the application storing the sensitive data. Sensitive data consists of keys and passwords.

160 RHEL also provides the ability to encrypt/decrypt sensitive files using OpenSSL. The command to use is the following:

*openssl enc [-d] -aes-256-<cbc | ctr> -in <file> -out <file> *

-pass file:<file_with_password> -pbkdf2

161 The -d option is used for decryption instead of encryption

6.12 Secure Erase

162 The TOE has a utility, shred, that can assist in the secure erasure of files and partitions within the limitations expressed in the next section. The utility by default writes 3 patterns to files or disk devices to make retrieval of data more difficult. To securely erase an external drive with default options, as root, use the following (adjusting for the actual drive):

shred /dev/sde1

Note: This function does not work on SSD's.

163 See the man page for additional information.

6.12.1 Non-volatile drives and keys

164 All instances of keys in non-volatile storage might not be deleted if the physical drive has replaced a sector containing a key with a spare sector. To minimize this risk, the physical drive should be end-of-life before a significant amount of damage to the drive's health can occur.

6.13 SSH Usage

165 Remote administrators can connect to the TOEs CLI interface via SSH by launching an SSH client on the administrator device, entering the IP address of the TOE along with specifying port 22 (ssh), and executing the session establishment process. The administrator will be prompted for a username and password or public key credential prior to establishing a successful SSH session.

7 Using The System Safely

166 This section contains additional guidance on mitigating potential issues that are residual in the TOE.

7.1 Disable Kernel Modules Affected by Vulnerabilities

167 The TOE must be configured to disable unused kernel modules that are affected by unmitigated vulnerabilities.

168 The following lines must be added to the */etc/modprobe.d/denylist.conf* file, followed by a reboot of the system to ensure the changes are applied:

install iscsi_tcp /bin/false

blacklist iscsi_tcp

install udf /bin/false

blacklist udf

install hid-asus /bin/false

blacklist hid-asus

install nfnetlink_queue /bin/false

blacklist nfnetlink_queue

install i2c-ismt /bin/false

blacklist i2c-ismt

install gru /bin/false

blacklist gru

install sunrpc /bin/false

blacklist sunrpc

install cls_u32 /bin/false

blacklist cls_u32

install intel-ishtp /bin/false

blacklist intel-ishtp

install slip /bin/false

blacklist slip

install cifs /bin/false

blacklist cifs

install sch_hfsc /bin/false

blacklist sch_hfsc

7.2 Tar Program Usage

169 Administrator must only untar files that are confirmed to be trusted to avoid triggering the following vulnerabilities:

a) CVE-2022-48303

7.3 Unescaped sudo Logs

170 Use of the command *sudoreplay -l* is strictly prohibited when inspecting sudo logs to prevent the following vulnerabilities:

a) CVE-2023-28487

b) CVE-2023-28486

171 Utilities such as "*less*" or "*vim*" should be used for log inspection instead.

7.4 cURL Usage

172 When using cURL, the entire cookie jar should not be passed to each invocation of cURL in order to prevent the following vulnerabilities:

a) CVE-2023-46218

8 Application Developers

8.1 Developer Security Workarounds

8.1.1 OpenSSL

173 Application developers using OpenSSL must not use the function *EVP_CIPHER_meth_new()* to avoid triggering the following vulnerabilities:

CVE-2022-3358

174 Application developers using AES-SIV algorithm implementation from OpenSSL must not use the functions EVP_EncryptUpdate() or EVP_CipherUpdate() with a NULL pointer as the output buffer and 0 as the input buffer length (authentication using empty data) to avoid triggering the following vulnerabilities:

CVE-2023-2975

9 Vulnerability Reporting

175 Red Hat accepts reports of security issues at the secalert@redhat.com email address. Red Hat provides a public GPG key (available at https://access.redhat.com/security/team/contact) so the reporter can protect sensitive aspects of a report. Email sent to secalert@redhat.com is read and acknowledged with a non-automated response within three working days. For issues that are complicated and require significant attention, Red Hat will open an investigation and will provide reporters with a mechanism to check the status at any time.

176 For security issues under embargo, Red Hat does not disclose, discuss, or confirm security issues until an investigation is conducted and the vulnerability is made public. Once an embargoed issue has been made public, Red Hat publishes documentation regarding the flaw including technical details on the issue, a Common Vulnerabilities and Exposures (CVE) identifier, a Common Vulnerabilities Security Score (CVSS), a Red Hat Severity Rating, and the Red Hat products impacted by the vulnerability.

177 Red Hat distributes information about security issues in its products through the Red Hat CVE database and security advisories to active subscription holders. Advisories

are provided through the rhsa-announce mailing list. Security updates are delivered via the standard update mechanism described in FPT_TUD_EXT.1.

178 Red Hat engages with various partners, vendors, researchers, and community coordinators to disclose newly discovered vulnerabilities in a timely manner that takes into account the complexity and severity of each vulnerability and any collaborative efforts with stakeholders to produce coordinated and responsible disclosures and remediation guidance.

10 Annex A: Log Reference

10.1 Using Audit Logs

179 All the audits are found in /var/log/audit/audit.log. The ausearch utility is intended to be the way to see the events. The Audit event format is as follows:

node=<host> type=<type> msg=audit(<timestamp>: <serial_number>): pid=<pid> uid=<uid> auid=<auid> ses=<session> <message> <source> res=<res>

a) <host> Hostname of the system

b) <type> SERVICE_START, SERVICE_STOP, USER_AUTH, SYSCALL, USER_START, USER_CMD, ADD_GROUP, PROCTITLE, CWD, SOFTWARE_UPDATE, SYSTEM_BOOT, SYSTEM_SHUTDOWN, PATH, CWD, or EXECVE

c) <timestamp> Epoch time (seconds since January 1, 1970 12:00:00 AM) to the millisecond

d) <serial_number> unique numerical event identifier appended to the timestamp. Repeats across multiple records that are related to the same event

e) <uid> user ID of the process at the time the audit event was generated

f) <auid> user ID of the user authenticated by the system (regardless if the user has changed his real and / or effective user ID afterwards)

g) <pid> Process ID of the subject that caused the event

h) <session> session ID - used to disambiguating actions when a single user has multiple active sessions

i) <message> Information about the intended operation

j) <source> hostname=<host>, addr=<IP_address>, and/or terminal=<terminal> - identifies how the subject is connected to RHEL

k) <res> success or failure - indicates whether the action succeeded or failed **Note:** Events of type ‘SYSCALL’ do not contain a ‘res’ field and instead use the ‘success=<no/yes>’ syntax to represent the status of the event.

10.2 Audit Events

180 RHEL generates audit logs for the following events (note: some information has been edited, such as IP addresses and DNS names):

10.2.1 Start-up of the audit function

181 node=<hostname> type=SERVICE_START msg=audit(1575382890.659:62388): pid=1 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0

msg='unit=auditd comm="systemd" exe="/usr/lib/systemd/systemd" hostname=? addr=? terminal=? res=success'

10.2.2 Shut-down of the audit function

182 node=<hostname> type=DAEMON_END msg=audit(1695112837.021:1649): op=terminate auid=0 pid=5044 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 res=success'

10.2.3 Software Restriction Policies

183 node=<hostname> type=PROCTITLE msg=audit(1696409831.298:9011): proctitle=6661706F6C696379642D636C69002D2D66696C6500616464002F746D702F6C73

node=<hostname> type=PATH msg=audit(1696409831.298:9011): item=1 name="/etc/fapolicyd/fapolicyd.trust" inode=50406974 dev=fd:03 mode=0100644 ouid=0 ogid=990 rdev=00:00 obj=system_u:object_r:fapolicyd_config_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=PATH msg=audit(1696409831.298:9011): item=0 name="/etc/fapolicyd/" inode=50406972 dev=fd:03 mode=040750 ouid=0 ogid=990 rdev=00:00 obj=system_u:object_r:fapolicyd_config_t:s0 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696409831.298:9011): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696409831.298:9011): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=55b94fb16e48 a2=241 a3=1b6 items=2 ppid=11520 pid=11522 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=22 comm="fapolicyd-cli" exe="/usr/sbin/fapolicyd-cli" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-create"

184 node=<hostname> type=PROCTITLE msg=audit(1696410017.877:9077): proctitle=6661706F6C696379642D636C69002D2D66696C6500616464002F746D702F6C73

node=<hostname> type=PATH msg=audit(1696410017.877:9077): item=0 name="/etc/fapolicyd/fapolicyd.trust" nametype=UNKNOWN cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696410017.877:9077): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696410017.877:9077): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=557d78bb6e48 a2=241 a3=1b6 items=1 ppid=11047 pid=11525 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=22 comm="fapolicyd-cli" exe="/usr/sbin/fapolicyd-cli" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-create"

10.2.4 Authentication Events

185 node=<hostname> type=USER_AUTH msg=audit(1694184936.066:3866): pid=40605 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:authentication

grantors=pam_faillock,pam_usertype,pam_localuser,pam_unix acct="admin" exe="/usr/sbin/sshd" hostname=? addr=? terminal=ssh res=success'

186 node=<hostname> type=USER_AUTH msg=audit(1694185305.066:4066): pid=40685 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=? acct="admin" exe="/usr/sbin/sshd" hostname=? addr=? terminal=ssh res=failed'

10.2.5 Use of privileged/special rights

10.2.5.1 Security

187 node=<hostname> type=PROCTITLE msg=audit(1696327757.022:7222): proctitle=76696D002F6574632F63727970746F2D706F6C69636965732F6261636B2D656E64732F6F70656E737368736572766572652E636F6E666967

node=<hostname> type=PATH msg=audit(1696327757.022:7222): item=1 name="/etc/crypto-policies/back-ends/opensshserver.config" inode=33999233 dev=fd:03 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 nametype=CREATE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=PATH msg=audit(1696327757.022:7222): item=0 name="/etc/crypto-policies/back-ends/" inode=33575061 dev=fd:03 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696327757.022:7222): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696327757.022:7222): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=556b8c883d00 a2=41 a3=1a4 items=2 ppid=10475 pid=10478 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=19 comm="vim" exe="/usr/bin/vim" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-create"

188 node=<hostname> type=PROCTITLE msg=audit(1696327651.922:7222): proctitle=737368643A2061646D696E407074732F31

node=<hostname> type=PATH msg=audit(1696327651.922:7222): item=0 name="/etc/crypto-policies/back-ends/opensshserver.config" inode=33575089 dev=fd:03 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:etc_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696327651.922:7222): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696327651.922:7222): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=55b2110f60e0 a2=401 a3=0 items=1 ppid=10413 pid=10414 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=19 comm="bash" exe="/usr/bin/bash" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-modification"

10.2.5.2 Audit

189 node=<hostname> type=PROCTITLE msg=audit(1696334330.512:8012): proctitle=76696D002F6574632F61756469742F6175646974642E636F6E66

node=<hostname> type=PATH msg=audit(1696334330.512:8012): item=1 name="/etc/audit/auditd.conf" inode=34011757 dev=fd:03 mode=0100640 ouid=0 ogid=0 rdev=00:00 obj=unconfined_u:object_r:auditd_etc_t:s0 nametype=CREATE cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=PATH msg=audit(1696334330.512:8012): item=0 name="/etc/audit/" inode=34000152 dev=fd:03 mode=040750 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:auditd_etc_t:s0 nametype=PARENT cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696334330.512:8122): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696334330.512:8012): arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=558799659d00 a2=41 a3=1a0 items=2 ppid=10519 pid=10522 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=19 comm="vim" exe="/usr/bin/vim" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-create"

190 node=<hostname> type=PROCTITLE msg=audit(1696334222.912:7912): proctitle=737368643A2061646D696E407074732F31

node=<hostname> type=PATH msg=audit(1696334222.912:7912): item=0 name="/etc/audit/auditd.conf" nametype=UNKNOWN cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696334222.912:7912): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696334222.912:7912): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=55b2110f5b50 a2=401 a3=0 items=1 ppid=10413 pid=10414 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=19 comm="bash" exe="/usr/bin/bash" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-modification"

10.2.5.3 Configuration Changes

191 node=<hostname> type=PROCTITLE msg=audit(1696335577.487:8087): proctitle=76696D002F6574632F73656C696E75782F636F6E666967

node=<hostname> type=PATH msg=audit(1696335577.487:8078): item=0 name="/etc/selinux/config" inode=50333212 dev=fd:03 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:selinux_config_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696335577.487:8078): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696335577.487:8078): arch=c000003e syscall=188 success=yes exit=0 a0=55c7bd0f4d00 a1=7f0b64379000 a2=55c7bd366af0 a3=1c items=1 ppid=10542 pid=10545 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1

ses=19 comm="vim" exe="/usr/bin/vim"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="MAC-policy"

192 node=<hostname> type=PROCTITLE msg=audit(1696335469.487:8078):
proctitle=737368643A2061646D696E407074732F31

node=<hostname> type=PATH msg=audit(1696335469.487:8078): item=0
name="/etc/selinux/config" inode=50927558 dev=fd:03 mode=0100644 ouid=0
ogid=0 rdev=00:00 obj=system_u:object_r:selinux_config_t:s0 nametype=NORMAL
cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696335469.487:8078):
cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696335469.487:8078):
arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=55b2110c89e0
a2=401 a3=0 items=1 ppid=10413 pid=10414 auid=1000 uid=1000 gid=1000
euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=19
comm="bash" exe="/usr/bin/bash" subj=unconfined_u:unconfined_r:unconfined_t:s0-
s0:c0.c1023 key="MAC-policy"

10.2.6 Role escalation events

193 node=<hostname> type=USER_START msg=audit(1694430185.787:2788):
pid=21415 uid=1000 auid=1000 ses=4
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='op=PAM:session_open
grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root"
exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/1 res=success'

194 node=<hostname> type=USER_CMD msg=audit(1694430973.787:2978):
pid=21546 uid=1000 auid=1000 ses=4
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
msg='cwd="/home/admin" cmd=7669202F6574632F727379736C6F672E636F6E66
exe="/usr/bin/sudo" terminal=pts/1 res=failed'

10.2.7 File and object events

195 node=<hostname> type=SYSCALL msg=audit(1573571943.644:66555):
arch=c000003e syscall=2 success=no exit=-13 a0=7ffcae0b175f a1=0 a2=0
a3=7ffcae0afb60 items=1 ppid=25815 pid=25889 auid=1000 uid=1000 gid=1000
euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1
ses=348 comm="tail" exe="/usr/bin/tail"

10.2.7.1 Create

196 node=<hostname> type=SYSCALL msg=audit(1694434786.154:2455):
arch=c000003e syscall=257 success=yes exit=3 a0=ffffff9c a1=7ffcfe5e5672
a2=941 a3=1b6 items=2 ppid=21335 pid=21941 auid=1000 uid=1000 gid=1000
euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4
comm="touch" exe="/usr/bin/touch"
subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-
create"

197 node=<hostname> type=SYSCALL msg=audit(1694435024.845:2544):
arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=7ffd5ccdb66a
a2=941 a3=1b6 items=1 ppid=21335 pid=21959 auid=1000 uid=1000 gid=1000
euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4
comm="touch" exe="/usr/bin/touch"

subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-create"

10.2.7.2 Access

198 node=<hostname> type=SYSCALL msg=audit(1694435553.834:2433): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=7fff4afa5663 a2=0 a3=0 items=1 ppid=21335 pid=22012 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4 comm="cat" exe="/usr/bin/cat" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-access"

10.2.7.3 Delete

199 node=<hostname> type=SYSCALL msg=audit(1694435829.067:2676): arch=c000003e syscall=263 success=yes exit=0 a0=ffffff9c a1=55ce3d2bb630 a2=0 a3=200 items=2 ppid=21335 pid=22034 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4 comm="rm" exe="/usr/bin/rm" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-delete"

200 node=<hostname> type=SYSCALL msg=audit(1694435990.634:2656): arch=c000003e syscall=263 success=no exit=-13 a0=ffffff9c a1=55f843cee630 a2=0 a3=20 items=2 ppid=21335 pid=22044 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4 comm="rm" exe="/usr/bin/rm" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-delete"

10.2.7.4 Modify

201 node=<hostname> type=SYSCALL msg=audit(1694436316.183:2634): arch=c000003e syscall=77 success=yes exit=0 a0=3 a1=0 a2=0 a3=1a4 items=0 ppid=21335 pid=22086 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4 comm="vim" exe="/usr/bin/vim" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-modification"

202 node=<hostname> type=SYSCALL msg=audit(1694436489.223:2333): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=5587c1252c50 a2=401 a3=0 items=1 ppid=21334 pid=21335 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4 comm="bash" exe="/usr/bin/bash" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-modification"

10.2.7.5 Modify Permissions

203 node=<hostname> type=SYSCALL msg=audit(1694436604.677:2486): arch=c000003e syscall=268 success=yes exit=0 a0=ffffff9c a1=561a35117660 a2=1ff a3=0 items=1 ppid=21335 pid=22121 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4 comm="chmod" exe="/usr/bin/chmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-perm-change"

204 node=<hostname> type=SYSCALL msg=audit(1694436726.278:2787): arch=c000003e syscall=268 success=no exit=-1 a0=ffffff9c a1=55cc25499660 a2=1ff a3=0 items=1 ppid=21335 pid=22131 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=4 comm="chmod" exe="/usr/bin/chmod"

subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-perm-change"

10.2.8 User and Group management events

10.2.8.1 Add

205 node=<hostname> type=ADD_GROUP msg=audit(1694787254.533:6333): pid=154563 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=add-group id=1002 exe="/usr/sbin/groupadd" hostname=? addr=? terminal=pts/1 res=success'

206 node=<hostname> type=ADD_GROUP msg=audit(1694787326.623:6865): pid=154572 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=add-group acct="group1" exe="/usr/sbin/groupadd" hostname=? addr=? terminal=pts/1 res=failed'

207 node=<hostname> type=ADD_USER msg=audit(1694784340.689:6499): pid=154464 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=add-user acct="tester" exe="/usr/sbin/useradd" hostname=? addr=? terminal=pts/1 res=success'

208 node=<hostname> type=ADD_USER msg=audit(1694787112.832:6235): pid=154559 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=add-user acct="tester" exe="/usr/sbin/useradd" hostname=? addr=? terminal=pts/1 res=failed'

10.2.8.2 Delete

209 node=<hostname> type=GRP_MGMT msg=audit(1695037843.475:8373): pid=156760 uid=0 auid=0 ses=14 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=delete-shadow-group id=1003 exe="/usr/sbin/groupdel" hostname=? addr=? terminal=pts/0 res=success

210 node=<hostname> type=GRP_MGMT msg=audit(1695037703.720:8265): pid=156747 uid=0 auid=0 ses=14 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=delete-group acct="non_existing_group" exe="/usr/sbin/groupdel" hostname=? addr=? terminal=pts/0 res=failed

211 node=<hostname> type=DEL_USER msg=audit(1695037651.612:8321): pid=156738 uid=0 auid=0 ses=14 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=delete-user id=1001 exe="/usr/sbin/userdel" hostname=<hostname> addr=? terminal=pts/0 res=success'

212 node=<hostname> type=DEL_USER msg=audit(1695037523.167:8377): pid=156734 uid=0 auid=0 ses=14 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=deleting-user-not-found acct="non_existing_user" exe="/usr/sbin/userdel" hostname=? addr=? terminal=pts/0 res=failed'

10.2.8.3 Modify

213 node=<hostname> type=USER_MGMT msg=audit(1694791319.953:7056): pid=154687 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=add-user-to-group grp="wheel" acct="tester" exe="/usr/sbin/usermod" hostname=? addr=? terminal=pts/1 res=success'

214 node=<hostname> type=USER_MGMT msg=audit(1694791319.986:7234): pid=154687 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=add-user-to-shadow-group grp="wheel" acct="tester" exe="/usr/sbin/usermod" hostname=? addr=? terminal=pts/1 res=success'

215 node=<hostname> type=PROCTITLE msg=audit(1696589918.127:11111): proctitle=757365726D6F64002D61002D4700776865656C0074657374657231

node=<hostname> type=PATH msg=audit(1696589918.127:11111): item=0 name="/etc/shadow" inode=34011753 dev=fd:03 mode=0100000 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:shadow_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696589918.127:11111): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696589918.127:11111): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=7f00bdf2dcd5 a2=80000 a3=0 items=1 ppid=12885 pid=12927 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=25 comm="usermod" exe="/usr/sbin/usermod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful-access"

216 node=<hostname> type=GRP_MGMT msg=audit(1694790583.913:6643): pid=154619 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=changing-group grp="group1" gid=1002 new_group="group2" acct="group1" exe="/usr/sbin/groupmod" hostname=? addr=? terminal=pts/1 res=success'

217 node=<hostname> type=GRP_MGMT msg=audit(1694790583.247:6236): pid=154619 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=changing-shadow-group grp="group1" new_group="group2" acct="group1" exe="/usr/sbin/groupmod" hostname=? addr=? terminal=pts/1 res=success'

218 node=<hostname> type=GRP_MGMT msg=audit(1694790583.247:6333): pid=154619 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=modify-group acct="group1" exe="/usr/sbin/groupmod" hostname=localhost.localdomain addr=? terminal=pts/1 res=success'

219 node=<hostname> type=GRP_MGMT msg=audit(1694791135.856:7345): pid=154683 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=changing-group grp="group1" gid=1002 acct="group1" exe="/usr/sbin/groupmod" hostname=? addr=? terminal=pts/1 res=failed'

10.2.8.4 Disable

220 node=<hostname> type=ACCT_LOCK msg=audit(1696420135.571:9256): pid=11610 uid=0 auid=1000 ses=22 subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 msg='op=locked-password id=1001 exe="/usr/bin/passwd" hostname=? addr=? terminal=pts/1 res=success'

221 node=<hostname> type=USER_CHAUTHTOK msg=audit(1696420006.047:9056): pid=11602 uid=1000 auid=1000 ses=22 subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 msg='op=attempted-to-change-password-attribute id=1000 exe="/usr/bin/passwd" hostname=? addr=? terminal=pts/1 res=failed'

10.2.8.5 Enable

222 node=<hostname> type=ACCT_UNLOCK msg=audit(1696420413.111:9542): pid=11618 uid=0 auid=1000 ses=22 subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 msg='op=unlocked-password id=1001 exe="/usr/bin/passwd" hostname=? addr=? terminal=pts/1 res=success'

223 node=<hostname> type=USER_CHAUTHTOK msg=audit(1696420331.111:9555): pid=11613 uid=1000 auid=1000 ses=22 subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 msg='op=attempted-to-change-password-attribute id=1000 exe="/usr/bin/passwd" hostname=? addr=? terminal=pts/1 res=failed'

10.2.8.6 Credential Change

224 node=<hostname> type=USER_CHAUTHTOK msg=audit(1694791936.134:7234): pid=154763 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 msg='op=PAM:chauthtok grantors=pam_pwquality,pam_unix acct="admin" exe="/usr/bin/passwd" hostname=? addr=? terminal=pts/1 res=success'

225 node=<hostname> type=USER_CHAUTHTOK msg=audit(1694792231.634:7243): pid=154786 uid=0 auid=1000 ses=12 subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 msg='op=PAM:chauthtok grantors=? acct="admin" exe="/usr/bin/passwd" hostname=? addr=? terminal=pts/1 res=failed'

10.2.9 Audit and Log Data Access Events

10.2.9.1 Success

226 node=<hostname> type=PROCTITLE msg=audit(1695038788.723:8456): proctitle=6C73002D616C002F7661722F6C6F672F61756469742F

227 node=<hostname> type=PATH msg=audit(1695038788.723:8456): item=0 name="/var/log/audit/audit.log" inode=34015100 dev=fd:03 mode=0100600 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:auditd_log_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

228 node=<hostname> type=CWD msg=audit(1695038788.723:8456): cwd="/home/admin"

229 node=<hostname> type=SYSCALL msg=audit(1695038788.723:8456): arch=c000003e syscall=192 success=yes exit=34 a0=7fff83544400 a1=7fdf3dfc7251 a2=55e6a49e5990 a3=ff items=1 ppid=156854 pid=156856 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts1 ses=20 comm="ls" exe="/usr/bin/ls" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="access-audit-trail"

10.2.9.2 Failure

230 node=<hostname> type=PROCTITLE msg=audit(1695038708.711:8104): proctitle=6C73002D2D636F6C6F723D6175746F002D616C002F7661722F6C6F672F61756469742F

231 node=<hostname> type=PATH msg=audit(1695038708.711:8104): item=0 name="/var/log/audit/" inode=34000163 dev=fd:03 mode=040700 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:auditd_log_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

232 node=<hostname> type=CWD msg=audit(1695038708.711:8104): cwd="/home/admin"

233 node=<hostname> type=SYSCALL msg=audit(1695038708.711:8104): arch=c000003e syscall=257 success=no exit=-13 a0=ffffff9c a1=55dc87185200 a2=90800 a3=0 items=1 ppid=156805 pid=156850 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=20 comm="ls" exe="/usr/bin/ls" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="access-audit-trail"

10.2.10 Cryptographic Verification of Software

10.2.10.1 Success

234 2023-10-22T12:14:28-0500 DEBUG Upgraded: sos-4.6.0-5.el9.noarch

10.2.10.2 Failure

235 2023-10-22T12:12:04-0500 DEBUG Using rpmkeys executable at /bin/rpmkeys to verify signatures

2023-10-22T12:12:04-0500 CRITICAL Problem opening package sos-4.6.0-5.el9.noarch.rpm

2023-10-22T12:12:04-0500 DDEBUG Cleaning up.

2023-10-22T12:12:04-0500 INFO The downloaded packages were saved in cache until the next successful transaction.

2023-10-22T12:12:04-0500 INFO You can remove cached packages by executing 'dnf clean packages'.

2023-10-22T12:12:04-0500 SUBDEBUG

Traceback (most recent call last):

File "/usr/lib/python3.9/site-packages/dnf/cli/main.py", line 67, in main

return _main(base, args, cli_class, option_parser_class)

File "/usr/lib/python3.9/site-packages/dnf/cli/main.py", line 106, in _main

return cli_run(cli, base)

File "/usr/lib/python3.9/site-packages/dnf/cli/main.py", line 130, in cli_run

ret = resolving(cli, base)

File "/usr/lib/python3.9/site-packages/dnf/cli/main.py", line 176, in resolving

base.do_transaction(display=displays)

File "/usr/lib/python3.9/site-packages/dnf/cli/cli.py", line 238, in do_transaction

self.gpgsigcheck(install_pkgs)

File "/usr/lib/python3.9/site-packages/dnf/cli/cli.py", line 305, in gpgsigcheck

raise dnf.exceptions.Error(_("GPG check FAILED"))

dnf.exceptions.Error: GPG check FAILED

2023-10-22T12:12:04-0500 CRITICAL Error: GPG check FAILED

10.2.11 Application Invocation with Arguments (Due to Software Restriction Policy)

236 node=<hostname> type=PROCTITLE msg=audit(1696409366.912:8239): proctitle=2F746D702F6C73002D6C61

node=<hostname> type=PATH msg=audit(1696409366.912:8239): item=1 name="/lib64/ld-linux-x86-64.so.2" inode=84051 dev=fd:03 mode=0100755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:ld_so_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=PATH msg=audit(1696409366.912:8239): item=0 name="/tmp/ls" inode=16902054 dev=fd:03 mode=0100755 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696409366.912:8239): cwd="/home/admin"

node=<hostname> type=EXECVE msg=audit(1696409366.912:8239): argc=2 a0="/tmp/ls" a1="-la"

node=<hostname> type=SYSCALL msg=audit(1696409366.912:8239): arch=c000003e syscall=59 success=yes exit=0 a0=55d97a223330 a1=55d97a223170 a2=55d97a1f4bc0 a3=8 items=2 ppid=11047 pid=11442 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=22 comm="ls" exe="/tmp/ls" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)

node=<hostname> type=FANOTIFY msg=audit(1696409366.912:8239): resp=1

237 node=<hostname> type=PROCTITLE msg=audit(1696409366.912:8239): proctitle="-bash"

node=<hostname> type=PATH msg=audit(1696409507.343:8753): item=0 name="/tmp/ls" inode=16902054 dev=fd:03 mode=0100755 ouid=1000 ogid=1000 rdev=00:00 obj=unconfined_u:object_r:user_tmp_t:s0 nametype=NORMAL cap_fp=0 cap_fi=0 cap_fe=0 cap_fver=0 cap_frootid=0

node=<hostname> type=CWD msg=audit(1696409507.343:8753): cwd="/home/admin"

node=<hostname> type=SYSCALL msg=audit(1696409507.343:8753): arch=c000003e syscall=59 success=no exit=-1 a0=55d97a223190 a1=55d97a223440 a2=55d97a1f4bc0 a3=8 items=1 ppid=11047 pid=11509 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=22 comm="bash" exe="/usr/bin/bash" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=(null)

node=<hostname> type=FANOTIFY msg=audit(1696409507.343:8753): resp=2

10.2.12 System Reboot, Restart, and Shutdown Events

10.2.12.1 System Reboot

238 node=<hostname> type=SYSTEM_BOOT msg=audit(1695040032.512:221): pid=811 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=' comm="systemd-update-utmp"

exe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=success'

10.2.12.2 System Shutdown

239 node=<hostname> type=SYSTEM_SHUTDOWN msg=audit(1695040226.812:621): pid=1052 uid=0 auid=4294967295 ses=4294967295 subj=system_u:system_r:init_t:s0 msg=' comm="systemd-update-utmp" exe="/usr/lib/systemd/systemd-update-utmp" hostname=? addr=? terminal=? res=success'

10.2.13 Kernel Module Loading and Unloading Events

10.2.13.1 Success

240 node=<hostname> type=KERN_MODULE msg=audit(1695041270.456:765): name="drm"

241 node=<hostname> type=SYSCALL msg=audit(1695041270.456:765): arch=c000003e syscall=175 success=yes exit=0 a0=7f53b9c9d010 a1=10dce0 a2=5636ae49e962 a3=5 items=50 ppid=1083 pid=1085 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=1 comm="modprobe" exe="/usr/bin/kmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="module-load"

242 node=<hostname> type=PROCTITLE msg=audit(1695041493.823:834): proctitle=726D6D6F640064726D

243 node=<hostname> type=KERN_MODULE msg=audit(1695041493.823:834): name="drm"

244 node=<hostname> type=SYSCALL msg=audit(1695041493.823:834): arch=c000003e syscall=176 success=yes exit=0 a0=5629aaecb7d8 a1=800 a2=a a3=7f0d5761cac0 items=0 ppid=1102 pid=1104 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=1 comm="rmmod" exe="/usr/bin/kmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="module-unload"

10.2.13.2 Failure

245 node=<hostname> type=PROCTITLE msg=audit(1695041556.011:256): proctitle=6D6F6470726F62650064726D

246 node=<hostname> type=SYSCALL msg=audit(1695041556.011:256): arch=c000003e syscall=175 success=no exit=-1 a0=7f8093a9b010 a1=10dce0 a2=5638d9707962 a3=5 items=0 ppid=962 pid=1108 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=1 comm="modprobe" exe="/usr/bin/kmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="module-load"

247 node=<hostname> type=PROCTITLE msg=audit(1695041853.414:847): proctitle=726D6D6F640064726D

248 node=<hostname> type=SYSCALL msg=audit(1695041853.414:847): arch=c000003e syscall=176 success=no exit=-1 a0=55d40e9ef7d8 a1=800 a2=a a3=7fb5d62a1ac0 items=0 ppid=962 pid=1117 auid=1000 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=1 comm="rmmod" exe="/usr/bin/kmod" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="module-unload"

10.2.14 Administrator or root-level Access Events

10.2.14.1 Success

249 node=<hostname> type=USER_START msg=audit(1695381799.535:3535): pid=4041 uid=1000 auid=1000 ses=7 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'

10.2.14.2 Failure

250 node=<hostname> type=USER_CMD msg=audit(1695382392.911:3112): pid=4119 uid=1001 auid=1001 ses=10 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd="/home/tester" cmd="su" exe="/usr/bin/sudo" terminal=pts/1 res=failed'

10.2.15 SSH Connection Events

10.2.15.1 Establishment of SSH Connection

251 node=<hostname> type=USER_LOGIN msg=audit(1695383004.800:3601): pid=4162 uid=0 auid=1000 ses=12 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=1000 exe="/usr/sbin/sshd" hostname=? addr=? terminal=/dev/pts/1 res=success'

252 node=<hostname> type=USER_START msg=audit(1695383004.800:3601): pid=4162 uid=0 auid=1000 ses=12 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=1000 exe="/usr/sbin/sshd" hostname=? addr=? terminal=/dev/pts/1 res=success'

10.2.15.2 Failure to Establish SSH Connection

253 node=<hostname> type=CRYPTO_SESSION msg=audit(1699386141.112:30135): pid=133725 uid=0 auid=4486260812 ses=4486260812 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=unsupported-cipher direction=? cipher=? ksize=? rport=<rport> laddr=<ip_addr> lport=<port> exe="/usr/sbin/sshd" hostname=? addr=<ip_addr> terminal=? res=failed'

10.2.15.3 Termination of SSH Connection Session

254 node=<hostname> type=USER_END msg=audit(1695383352.322:1654): pid=5164 uid=0 auid=1000 ses=16 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=1000 exe="/usr/sbin/sshd" hostname=? addr=? terminal=/dev/pts/1 res=success'

255 node=<hostname> type=USER_LOGOUT msg=audit(1695383352.322:1654): pid=5164 uid=0 auid=1000 ses=16 subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=login id=1000 exe="/usr/sbin/sshd" hostname=? addr=? terminal=/dev/pts/1 res=success'

10.2.15.4 Dropping of Packet(s) Outside Defined Size Limits

256 Nov 10 12:01:11 <hostname> sshd[2447]: Bad packet length 295590.

Nov 10 12:01:11 <hostname> sshd[2447]: ssh_dispatch_run_fatal: Connection from user <user> <ip_address> port <port>: Connection corrupted

Note: This audit message is found in /var/log/secure.