Red Hat Enterprise Linux 8.1 CC Guidance

Version 1.4

December 2020

1 Introduction

This guide provides instructions to configure and operate Red Hat Enterprise Linux (RHEL) 8.1 in the Common Criteria evaluated configuration running on one of the following models:

Vendor	Model	CPU
Dell Inc.	PowerEdge R440	Xeon Silver 42xx
Dell Inc.	PowerEdge R540	Xeon Silver 42xx
Dell Inc.	PowerEdge R640	Xeon Silver 42xx
Dell Inc.	PowerEdge R740	Xeon Silver 42xx
Dell Inc.	PowerEdge R740XD	Xeon Silver 42xx
Dell Inc.	PowerEdge 840	Xeon Silver 42xx
Dell Inc.	PowerEdge 940	Xeon Silver 42xx
Dell Inc.	PowerEdge 940sa	Xeon Silver 42xx

The Target of Evaluation (TOE) consists of the Red Hat Enterprise Linux 8.1 operating systems and the applications installed by the kickstart file.

1.1 Getting Started

Ensure the environment is consistent with the following assumptions:

- The RHEL hardware platform is physically protected and not subject to physical attacks that compromise the security and/or interfere with the device's physical interconnections and correct operation. This protection is assumed to be enough to protect the device and the data it contains.
- The Security Administrator(s) for the device are trusted and act in the best interest of security for the organization. This includes being appropriately trained, following policy, and adhering to guidance documentation. Administrators are trusted to ensure passwords/credentials have enough strength and entropy and to lack malicious intent when administering the device. The device is not expected to be capable of defending against a malicious Administrator that actively works to bypass or compromise the security of the device.
- The device firmware and software are updated by an administrator on a regular basis in response to the release of product updates due to known vulnerabilities.
- The administrator's credentials (private key) used to access the device are protected by the platform on which they reside.
- The administrator must ensure that there is no unauthorized access possible for sensitive residual information (e.g. cryptographic keys, keying material, PINs, passwords etc.) when the equipment is discarded or removed from its operational environment.

RHEL also supports secure connectivity with several other IT environment devices as described below.

Component	Required	Usage/Purpose Description for RHEL performance
HW Platform	Yes	x86_64 platform to run RHEL on. The platform must protect RHEL from hardware vulnerabilities, support UEFI Secure Boot, and provide network connectivity.
Workstation with SSH Client	No	This includes any IT Environment Management workstation with an SSH client installed that is used by RHEL users (including administrators) to remotely connect to RHEL through SSH protected channels. Any SSH client that supports SSHv2 may be used.
Audit Server	No	The audit server is used for remote storage of audit records that have been generated by and transmitted from RHEL.
Update Server	Yes	Provides the ability to check for updates to RHEL as well as providing signed updates.

RHEL also has the ability to connect to remote SSHv2 and TLSv1.2 servers, acting as a client for both of these connections.

1.2 Warnings

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 drive health occurs.

The following security functionality is included in RHEL but was not evaluated:

- gnu-tls provided TLS functions
- SELinux provided access controls

RHEL has two modes of operation:

1. Normal: Once installation has been completed, as described in Section 2 below, RHEL is in a secure mode of operation. The behavior of RHEL can further be configured as specified in Section 3 below.
2. Error: RHEL (with the support of the underlying hardware) verifies the integrity of the bootloader and kernel prior to execution. If a bootloader or kernel integrity error is detected, RHEL enters an error mode and does not boot. This indicates an unknown integrity error has occurred. To safely boot RHEL, a specialist must correct the error and determine if any other modifications (accidental or malicious) have been made to RHEL. Additional recover options can be found at: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html-single/performing_a_standard_rhel_installation/index#using-rescue-mode_troubleshooting-after-installation

2 Installation

2.1 Resources

Ensure you have the following resources available prior to beginning installation:

- Red Hat 8.1 Server installer on bootable media (download from redhat.com).
- Kickstart file hosted on a webserver accessible by the installation system. The Kickstart file can be obtained from the cc-config-8.1 package. This will need to be downloaded with dnf to a local system. Once the package is installed, you will find the kickstart file in /usr/share/cc-config/.
- RPMs available from Red Hat website (openssh-8.0p1-4.el8_1.x86_64.rpm, openssh-clients-8.0p1-4.el8_1.x86_64.rpm, openssh-server-8.0p1-4.el8_1.x86_64.rpm, scap-security-guide-0.1.47-8.el8_1.noarch.rpm, fapolicyd-0.8.10-3.el8_1.3.x86_64.rpm)
- An Internet connection

The Red Hat 8.1 Server installer and cc-config-8.1 package can be downloaded by following these steps:

1. Log in to https://access.redhat.com/
2. Click on 'DOWNLOADS'
3. On Product Downloads page select ‘Red Hat Enterprise Linux 8’.
4. On 'Download Red Hat Enterprise Linux' page, click on the 'Packages' tab.
5. In the 'Search' field, enter cc-config without a version or release.
6. In the list of filtered results, click on the cc-config item.
7. Select the 8.1 in the 'Version' tab.
8. In the download RPM section at the bottom, click on the 'Download Now' button beside the package name.

The installer and cc-config are downloaded over HTTPs. They can be trusted if the download completes successfully and the HTTPs certificate is valid for access.redhat.com.

If you already have a system running Red Hat Enterprise Linux 8, you can download the cc-config-8.1 package by running:

dnf install cc-config

2.2 Installation Steps

Before proceeding to the OS installation, the administrator should ensure that UEFI Secure Boot has been enabled. This is performed in the BIOS configuration, see guide for the Dell PowerEdge R740 here.

Perform the following steps to install Red Hat 8.1:

1. Configure a custom repo to host the SCAP and RPMs on a RHEL-based system (RHEL-6/7/8 or Fedora):
   A. Put the scap-security-guide RPM and all other RPMs into a new directory and call createrepo on it using the following steps:
   If createrepo was not previously installed or available by default, do:
   yum install createrepo
   then do:

mkdir cc-custom ##creates a new directory
cp -f *.rpm cc-custom/. ##moves all required RPMs to the new directory
createrepo cc-custom/ ##creates the DNF repo used by the TOE
This will create a DNF repository in the cc-custom directory, with the repository containing all required RPMs mentioned above.

This repository (the newly created cc-custom directory) will need to be hosted on some HTTP or FTP or NFS server and will be referenced from the kickstart.
Modify the kickstart file:
Set (uncomment) the "repo --name=cc-custom" line and set it to the repository created above, for example:
repo --name=cc-custom --baseurl="http://server/cc-custom/"

2. Boot the system from the Red Hat 8.1 Server installer.
3. At the Installation prompt:
    a. Select “Install Red Hat Enterprise Linux 8.1” (do not press Enter)
    b. Press <Tab>
    c. Append “inst.ks=http://[ipaddressofhost]:[port]/ospp.ks”
    the full string should look like “vmlinuz initrd=initrd.img inst.stage2=hd:LABEL=RHEL-8-1-0-BaseOS-x86_64 quiet inst.ks= http://192.168.1.1:8080/ospp.ks”
    d. Press <Enter>

The functionalities are installed and configured with the kickstart file and SCAP RPM. Please see the HTML report (as explained below in section 3.2.1) to verify the settings applied to the TOE.

Once the installation automated process completes, perform the following steps to complete your installation:

1. Register the appliance with Red Hat to be able to receive updates. To do so, execute the command “subscription-manager register --auto-attach”
2. The administrator will be asked to enter their Red Hat account credentials.

2.2.1 Configuration Verification

The RHEL 8.1 installation as previously described includes a package named the SCAP Security Guide. In it, there is a datastream file for RHEL 8, ssg-rhel8-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-rhel8-ds.xml > checklist.html

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

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

oscap info /usr/share/xml/scap/ssg/content/ssg-rhel8-xccdf.xml

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-rhel8-ds.xml

More information can be found here: https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/pdf/system_design_guide/Red_Hat_Enterprise_Linux-8-System_Design_Guide-en-US.pdf

2.3 Additional Firewall configuration

The administrator should disable ICMP destination unreachable messages to mitigate CVE-2020-25705. To do so, the administrator should enter the following command once the automated installation is complete:

- firewall-cmd --permanent --direct --add-rule ipv4 filter OUTPUT 0 -p icmp --icmp-style destination-unreachable -j DROP

3 Administration

3.1 Audit

3.1.1 Configure Audit Storage

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

max_log_file = <number>
: 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>
: 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.

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.

3.1.2 Configure Audit Rules

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/.

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 set up audit services and CAP_AUDIT_WRITE is required to log user messages.

Please see Section 10.6 of the Red Hat Enterprise Linux 8 Security Hardening for additional details.

3.1.3 Configure Aggregating Syslog Server

The audit logs can be forwarded to rsyslog so that they can be transported in real-time to an aggregating syslog server. To do this, the admin needs to enable the syslog audit dispatcher plugin. This is accomplished by editing the /etc/audisp/plugins.d/syslog.conf file and changing the setting for active to yes. Restart the audit daemon using:

service auditd restart

The administrator can configure the name/address of the syslog server by editing the /etc/rsyslog.conf file. A server is specified as <protocol><host>[:<port>]:

<protocol>
@ - indicates UDP
@@ - indicates TCP
<host>
FQDN or IP address of the Syslog server
<port>
Remote port to connect to. Defaults to 514 if not specified.

For example, @@testserver.com:2514 would send all logs including audit events to testserver.com on TCP port 2514.

3.2 User/Administrator Accounts

3.2.1 Creating User Accounts

The administrator can create user accounts using the "**useradd <username>**" command. A temporary password will need to be specified during the user creation process.

Once a user account has been created, the administrator can make this account an administrator by adding it to the wheel group by running "**usermod -aG wheel <username>**".

The most basic tasks to manage user accounts and groups, and the appropriate command-line tools, include:

- Displaying user and group IDs:

  id

- Creating a new user account:

useradd [options] ***user_name***

- Assigning a new password to a user account belonging to *username*:

  passwd ***user_name***

- Adding a user to a group:

  usermod -a -G ***group_name user_name***

Once an account is created and added to the wheel group, it can be used to administer RHEL from the local console or through a remote SSH connection.

3.2.2 Configure Password Policy

The password policy is enforced by the pam_pwquality PAM module. See the pam_pwquality(8) man page for details. The default policy that is set up by the kickstart guarantees a minimum length of 12 characters.

3.2.3 Change Passwords

A user can change their password using the "passwd" command. The user will be prompted to enter their current password as well as their new password.

3.2.4 Configure Failed Authentication Timeout

The administrator can configure the timeout between failed authentication attempts by editing the /etc/pam.d/system-auth file. Edit the line:

auth required pam_faildelay.so delay=<microseconds>

3.2.5 Configure Inactivity Timeouts

The administrator can change the local inactivity timeout by changing the idle variable setting in /etc/screenrc. The default value setup by the kickstart file is 900 second which is 15 minutes.

The administrator can change the remote (i.e. SSH) inactivity timeout in /etc/ssh/sshd_config by changing the value of **ClientAliveInterval**. This option is specified as "**ClientAliveInterval <time in seconds>**". For example, if the administrator wants to set the timeout to 10 minutes, it would look like "**ClientAliveInterval 600**". A value of "0" disables the remote inactivity timeout. The default value setup by the kickstart is 600.

3.2.6 SSH Public Key-based Authentication

A user can configure SSH public key authentication by adding their public key to the .ssh/authorized_keys file in their home directory.

A user can generate an ssh public/private keypair by running "**ssh-keygen -t [rsa|ecdsa] -b [2048|3072|256|384|521]".** 2048 and 3072 are only valid with rsa. 256, 384, and 521 are only valid with ecdsa.

3.2.7 SSH Password-based Authentication

The administrator can enable or disable SSH password-based authentication to the RHEL by configuration **PasswordAuthentication** in /etc/ssh/sshd_config. "**PasswordAuthentication yes**" enables

password-based authentication while "**PasswordAuthentication no**" disables password-based authentication.

When connecting to a remote SSH server, the RHEL supports password-based authentication by without configuration. If the remote SSH server supports password-based authentication and other authentication methods (e.g. public key) are not supported or fail, the RHEL will prompt the user for a password.

3.3 Configure NTP

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

Within this file each NTP server is specified on a separate line using the syntax "server <FQDN/IP address> iburst".

3.4 TLS Usage

RHEL provides a TLS client for secure communication with remote systems. The TLS client is invoked using "**openssl s_client -connect [host]:[port] -x509_strict -verify_return_error -CAfile [ca certificate] -crl_check_all -tls1_2 -rand /dev/random**". The options are described as follows:

-connect [host]:[port]
: specifies the FQDN or IP address and port of the remote system. [host] is automatically used as the reference identifier used to authenticate the identity presented in the server certificate. The SAN extension is checked first, followed by the CN if the certificate does not contain the SAN extension. When an FQDN is used, the left-most component in the presented certificate may be a wildcard (i.e. "*").

-x509_strict
: checks that all certificates, including issuing CAs, are compliant to x509 standards

-verify_return_error
: terminates the connection if an error is found

-CAfile [ca certificate]
: points to the Root CA used to validate the presented server certificate

-crl_check_all
: checks revocation on the entire chain of certificates

-tls1_2
: force to use TLSv1.2 only

-rand /dev/random
: force the use of entropy from /dev/random

OpenSSL supports the following ciphersuites without any configuration:

- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA256
- TLS_RSA_WITH_AES_256_CBC_SHA256
- TLS_RSA_WITH_AES_128_GCM_SHA256
- TLS_RSA_WITH_AES_256_GCM_SHA384
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA256

- TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
- TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
- TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
- TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
- TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
- TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384

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

- secp256r1
- secp384r1
- secp521r1

3.5 Storage of Sensitive Data

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.

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

openssl enc [-d] -aes-128-cbc|-aes-256-cbc -in <file> -out <file> -pass file:<file_with_password> -pbkdf2

The -d option is used for decryption instead of encryption

3.6 Updates

Updates to RHEL are distributed using the RPM format. All updates are signed using a Red Hat controlled RSA 4096 key, so the administrator can be assured of the authenticity of the updates.

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.

dnf check-update returns an exit value of:

- 100 if there are packages available for an update and prints a list of the packages to be updated
- 0 if no packages are available for update.
- 1 if an error occurred (including invalid signatures)

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

The administrator also has the option to enable automatic updates using the dnf-cron package.

3.7 Configure Automatic Software Updates

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

1. **sudo vi /etc/dnf/automatic.conf**
    a) **change upgrade_type to security**
    b) **change apply_updates to yes**
2. **sudo systemctl enable --now dnf-automatic.timer**

The system will check for updates daily.

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

1. **sudo systemctl disable dnf-automatic.timer**
2. **sudo systemctl stop dnf-automatic.timer**

3.8 Configure the Firewall

Please see Chapter 5 of the Red Hat Enterprise Linux 8 Securing Networks for instructions for configuring the firewall.

3.9 Configure the Warning Banner

Edit the file /etc/issue to configure the warning banner that will be displayed prior to authentication attempts (local as well as remote SSH). The contents of the file will be displayed to the user.

3.10 Changing SSH policies

RHEL 8.1 includes a utility, update-crypto-policies, that is used to set the policies for the various cryptographic back-ends such as OpenSSH. The administrator can make any changes to the files located in /etc/crypto-policies/. Both server and client application inherits the cipher preferences, the key exchange algorithms as well as the GSSAPI key exchange algorithms. To opt-out from the policy for client, override the global ssh_config with a user-specific configuration in ~/.ssh/config. To opt-out from the policy for server, uncomment the line containing CRYPTO_POLICY= in /etc/sysconfig/sshd.

The following command "**update-crypto-policies**" is used to apply the new settings.

3.11 Changing the SSH ECDSA Curve

RHEL supports using P-256 and P-384 curves when using an ECDSA hostkey. By default, RHEL generates a P-256 ECDSA hostkey. To change the curve, the administrator runs "**sudo ssh-keygen -t ecdsa -b 256|384 -f /etc/ssh/ssh_host_ecdsa_key**". Do not set a password for this key.

- 256 generates a P-256 key
- 384 generates a P-384 key

Once the key has been generated, restart sshd by running "**sudo systemctl restart sshd.service**".

3.12 Ensure openssh is strongly seeded

The openssh client and server can be configured to be seeded with 32 bits of entropy. To configure the client perform the following:

echo -e "export SSH_USE_STRONG_RNG=32" > /etc/profile.d/cc-config.sh

Once this is done, all users should log out and then back in. For the server, perform the following:

echo -e "SSH_USE_STRONG_RNG=32" >> /etc/sysconfig/sshd

Once this is done, the server must be restarted by running "**sudo systemctl restart sshd.service**".

3.13 Ext4 Mount Options

The TOE is designed to use the XFS file system. However, it can also mount Ext4 filesystems. The default size of inode in the TOE is 256. This is controlled by a setting in /etc/mke2fs.conf. If this is modified smaller or if the filesystem inodes are smaller that 256, which can be checked with:

tune2fs -l /dev/sdd1

It can have a problem if mounted with the obscure developer only option ext4_expand_extra_isize. When mounting an Ext4 file system, ensure that this option is not used on filesystems who's inodes are less than 256 bytes in size.

4 Application Developers

Application developers can user the included `gcc` compiler and linker to create applications that run on RHEL. When invoking `gcc`, developers should follow best practices for secure development:

- Include the following compiler flags to enable stack smashing protections:
  -fstack-protector-strong --param=ssp-buffer-size=4

- Include the following compiler and linker flags to enable ASLR:

  -fpie -Wl,-pie

5 Audit logs

All the audits are found in /var/log/audit/audit.log. Audits format will be:

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

<type>
SERVICE_STAR, SERVICE_STOP, USER_AUTH, SYSCALL, USER_START, USER_CMD, ADD_GROUP, PROCTITLE, CWD, SOFTWARE_UPDATE, SYSTEM_BOOT, SYSTEM_SHUTDOWN, PATH, CWD, or EXECVE
<timestamp>
Epoch time (seconds since January 1, 1970 12:00:00 AM) to the millisecond
<serial_number>
unique numerical event identifier appended to the timestamp. Repeats across multiple records that are related to the same event
<uid>
user ID of the process at the time the audit event was generated

<auid>
user ID of the user authenticated by the system (regardless if the user has changed his real and / or effective user ID afterwards)
<pid>
Process ID of the subject that caused the event
<session>
session ID – may be useful for disambiguating actions when a single user has multiple active sessions
<message>
Information about the intended operation
<source>
hostname=<host>, addr=<IP_address>, and/or terminal=<terminal> – identifies how the subject is connected to RHEL
<res>
success or failure – indicates whether the action succeeded or failed

RHEL generates audit logs for the following events:

- Start-up of the audit function
  node=ospp type=SERVICE_START msg=audit(1575382890.662:89388): 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'

- Shut-down of the audit function
  node=ospp type=SERVICE_STOP msg=audit(1575382790.412:89043): 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'

- Software Restriction Policies
  node=localhost.localdomain type=PROCTITLE msg=audit(08/05/2020 05:57:33.980:354084) : proctitle=-bash
  node=localhost.localdomain type=PATH msg=audit(08/05/2020 05:57:33.980:354084) : item=0 name=./hex-val.sh inode=160 dev=fd:07 mode=file,750 ouid=admin ogid=admin rdev=00:00 obj=unconfined_u:object_r:user_home_t:s0 nametype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
  node=localhost.localdomain type=CWD msg=audit(08/05/2020 05:57:33.980:354084) : cwd=/home/admin
  node=localhost.localdomain type=SYSCALL msg=audit(08/05/2020 05:57:33.980:354084) : arch=x86_64 syscall=openat success=no exit=EPERM(Operation not permitted) a0=0xffffff9c a1=0x5625fd081300 a2=O_RDONLY a3=0x0 items=1 ppid=53526 pid=53583 auid=admin uid=admin gid=admin euid=admin suid=admin fsuid=admin egid=admin sgid=admin fsgid=admin tty=pts8 ses=126 comm=bash exe=/usr/bin/bash subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=unsuccessful-access

node=localhost.localdomain type=FANOTIFY msg=audit(08/05/2020 05:57:33.980:354084) : resp=deny

- Authentication Events
  node=ospp type=USER_AUTH msg=audit(02/17/2020 07:13:09.773:5805) : pid=42586 uid=root auid=unset ses=unset subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=success acct=admin exe=/usr/sbin/sshd hostname=? addr=10.10.121.166 terminal=ssh res=success'

  node=ospp type=USER_AUTH msg=audit(02/17/2020 07:16:36.927:6494) : pid=42655 uid=root auid=unset ses=unset subj=system_u:system_r:sshd_t:s0-s0:c0.c1023 msg='op=PAM:authentication grantors=? acct=admin exe=/usr/sbin/sshd hostname=ovpn-121-166.rdu2.redhat.com addr=10.10.121.166 terminal=ssh res=failed'

- Use of privileged/special rights
  node=ospp type=SYSCALL msg=audit(1573571951.064:66845): arch=c000003e syscall=2 success=yes exit=3 a0=7f85317c74e4 a1=80000 a2=1 a3=7f85319cd4f8 items=1 ppid=25815 pid=25890 auid=1000 uid=1000 gid=1000 euid=0 suid=0 fsuid=0 egid=1000 sgid=1000 fsgid=1000 tty=pts1 ses=348 comm="sudo" exe="/usr/bin/sudo" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="successful-access"

- Role escalation events
  node=ospp type=USER_START msg=audit(02/21/2020 08:27:59.746:2208) : pid=16861 uid=root auid=admin ses=195 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_keyinit,pam_limits,pam_systemd,pam_unix acct=root exe=/usr/bin/sudo hostname=? addr=? terminal=/dev/pts/1 res=success'

  node=ospp type=USER_CMD msg=audit(02/17/2020 07:32:48.902:9813) : pid=42912 uid=tester auid=tester ses=582 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='cwd=/home/tester cmd=vi /etc/rsyslog.conf terminal=pts/1 res=failed'

- File and object events (Successful and unsuccessful attempts to create, access, delete, modify file, modify permissions)
  node=ospp type=SYSCALL msg=audit(1573571943.611:66844): 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"

- User and Group management events (Successful and unsuccessful add, delete, modify, disable, enable, and credential change)
  node=ospp type=ADD_GROUP msg=audit(1575391931.170:89985): pid=49353 uid=0 auid=1000 ses=884 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=add-group acct="user " exe="/usr/sbin/useradd" hostname=ospp addr=? terminal=pts/0 res=success'4050

- Audit and log data access events (Success/Failure)
  Success:
  node=ospp type=PROCTITLE msg=audit(01/21/2020 07:48:10.775:1235) : proctitle=ls --color=auto -al /var/log/
  node=ospp type=PATH msg=audit(01/21/2020 07:48:10.775:1235) : item=0 name=/var/log/audit inode=64 dev=fd:03 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:auditd_log_t:s0 objtype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
  node=ospp type=CWD msg=audit(01/21/2020 07:48:10.775:1235) : cwd=/root
  node=ospp type=SYSCALL msg=audit(01/21/2020 07:48:10.775:1235) : arch=x86_64 syscall=lgetxattr success=yes exit=34 a0=0x7ffc989bbca0 a1=0x7f94d0e52eaa a2=0x1107480 a3=0xff items=1 ppid=10022 pid=10062 auid=admin uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=1 comm=ls exe=/usr/bin/ls subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=access-audit-trail

  Failure:
  node=ospp type=PROCTITLE msg=audit(01/21/2020 07:48:10.775:1237) : proctitle=ls --color=auto -al /var/log/
  node=ospp type=PATH msg=audit(01/21/2020 07:48:10.775:1237) : item=0 name=/var/log/audit inode=64 dev=fd:03 mode=dir,700 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:auditd_log_t:s0 objtype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
  node=ospp type=CWD msg=audit(01/21/2020 07:48:10.775:1237) : cwd=/root
  node=ospp type=SYSCALL msg=audit(01/21/2020 07:48:10.775:1237) : arch=x86_64 syscall=getxattr success=no exit=ENODATA(No data available) a0=0x7ffc989bbca0 a1=0x7f94d0a2ddb0 a2=0x0 a3=0x0 items=1 ppid=10022 pid=10062 auid=admin uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=1 comm=ls exe=/usr/bin/ls subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key=access-audit-trail

- Cryptographic verification of software (Success/Failure)
  Success:
  node=ospp type=SOFTWARE_UPDATE msg=audit(12/18/2019 07:50:26.337:61554) : pid=25065 uid=root auid=admin ses=347 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='sw=dnf-cron-3.4.3-161.el7.noarch sw_type=rpm key_enforce=0 gpg_res=1 root_dir=/ comm=dnf exe=/usr/bin/python2.7 hostname=ospp addr=? terminal=pts/0 res=success'

  Failure:
  node=ospp type=SOFTWARE_UPDATE msg=audit(08/27/2019 11:21:51.198:3625) : pid=19723 uid=root auid=admin ses=254 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='sw=kernel-3.10.0-1062.el7.x86_64 sw_type=rpm key_enforce=0 gpg_res=1 root_dir=/ comm=dnf exe=/usr/bin/python2.7 hostname=ospp addr=? terminal=pts/0 res=failed'

- System reboot, restart, and shutdown events (Success/Failure)
  Success:
  type=SYSTEM_BOOT msg=audit(09/20/2016 01:10:32.392:7) : pid=657 uid=root auid=unset ses=unset 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'

  Failure: N/A

  System Shutdown:
  node=ospp type=SYSTEM_SHUTDOWN msg=audit(04/23/2020 05:15:54.157:379) : pid=9432 uid=root auid=unset ses=unset 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'

- Kernel module loading and unloading events (Success/Failure)
  Success:
  Jul 30 18:16:19 dell-per430-01.lab.eng.bos.redhat.com dracut[22908]: *** Including module: drm *
  Failure:
  Jul 30 18:16:18 dell-per430-01.lab.eng.bos.redhat.com dracut[22908]: dracut module 'nfs' will not be installed, because command 'mount.nfs4' could not be found!

- Administrator or root-level access events (Success/Failure)

  Success:
  time->Fri Oct 11 10:29:29 2019
  node=ospp type=USER_START msg=audit(1570804169.135:2217): pid=11088 uid=0 auid=1000 ses=93 subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 msg='op=PAM:session_open grantors=pam_keyinit,pam_limits,pam_keyinit,pam_limits,pam_systemd,pam_unix acct="root" exe="/usr/bin/sudo" hostname=? addr=? terminal=/dev/pts/0 res=success'

  Failure:
  node=ospp type=PATH msg=audit(02/17/2020 07:32:15.005:9264) : item=0 name=/bin/passwd inode=805792770 dev=fd:00 mode=file,suid,755 ouid=root ogid=root rdev=00:00 obj=system_u:object_r:passwd_exec_t:s0 objtype=NORMAL cap_fp=none cap_fi=none cap_fe=0 cap_fver=0
  node=ospp type=CWD msg=audit(02/17/2020 07:32:15.005:9264) : cwd=/root
  node=ospp type=EXECVE msg=audit(02/17/2020 07:32:15.005:9264) : argc=2 a0=passwd a1=tester
  node=ospp type=SYSCALL msg=audit(02/17/2020 07:32:15.005:9264) : arch=x86_64 syscall=execve success=yes exit=0 a0=0x17099d0 a1=0x17098b0 a2=0x17007a0 a3=0x7ffcbd833ce0 items=2 ppid=42728 pid=42883 auid=admin uid=root gid=root euid=root suid=root fsuid=root egid=root sgid=root fsgid=root tty=pts0 ses=579 comm=passwd

exe=/usr/bin/passwd subj=unconfined_u:unconfined_r:passwd_t:s0-s0:c0.c1023 key=special-config-changes

6 References

- Red Hat Enterprise Linux 8.1 Security Target, v0.6
- Kickstart file
- scap-security-guide rpm
- Red Hat Enterprise Linux 8 Security Hardening, Updated 2020-07-17