RHEL Audit System Reference

Updated November 24 2019 at 8:24 PM - English

TABLE OF CONTENTS

Audit Event Fields

The following table lists all currently-supported Audit event fields. An event field is the value preceding the equal sign in the Audit log files.

Event Field	Explanation	RHEL 7	RHEL 8
a0, a1, a2, a3	Records the first four arguments of the system call, encoded in hexadecimal notation.	yes	yes
acct	Record the user account name under which the process was executed.	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
action	Records the action taking place in an integrity policy rule.	yes	yes
appraise_type	Records the appraisal type used in an integrity policy rule.	yes	yes
addr	Records the IPv4 or IPv6 address. This field usually follows a hostname field and contains the address the host name resolves to.	yes	yes
arch	Records information about the CPU architecture of the system, encoded in hexadecimal notation.	yes	yes
auid	Records the Audit user ID. This ID is assigned to a user upon login and is inherited by every process even when the user's identity changes (for example, by switching user accounts with `su -john`).	yes	yes
calipso_doi	Records the DOI of an RFC5570 Calipso entry.	no	yes
calipso_type	Records the type of an RFC5570 Calipso entry.	no	yes
capability	Records the number of bits that were used to set a particular Linux capability. For more information on Linux capabilities, see the `capabilities(7)` man page.	yes	yes
cap_fe	Records data related to the setting of the effective file system-based capability bit.	yes	yes
cap_fi	Records data related to the setting of an inherited file system-based capability.	yes	yes
cap_fp	Records data related to the setting of a permitted file system-based capability.	yes	yes
cap_fver	Records the version of a file system-based capability.	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
cap_pe	Records data related to the setting of an effective process-based capability.	yes	yes
cap_pi	Records data related to the setting of an inherited process-based capability.	yes	yes
cap_pp	Records data related to the setting of a permitted process-based capability.	yes	yes
cause	Records the cause in an integrity policy rule.	yes	yes
cgroup	Records the path to the cgroup that contains the process at the time the Audit event was generated.	yes	yes
cmd	Records the entire command line that is executed. This is useful in case of shell interpreters where the exe field records, for example, `/bin/bash` as the shell interpreter and the cmd field records the rest of the command line that is executed, for example `helloworld.sh --help` .	yes	yes
code	Records the seccomp action.	yes	yes
comm	Records the command that is executed. This is useful in case of shell interpreters where the exe field records, for example, `/bin/bash` as the shell interpreter and the comm field records the name of the script that is executed, for example `helloworld.sh` .	yes	yes
compat	Records the syscall compatibility mode in a seccomp action.	yes	yes
cwd	Records the path to the directory in which a system call was invoked.	yes	yes
data	Records data associated with TTY records.	yes	yes
dev	Records the minor and major ID of the device that contains the file or directory recorded in an event.	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
devmajor	Records the major device ID.	yes	yes
devminor	Records the minor device ID.	yes	yes
egid	Records the effective group ID of the user who started the analyzed process.	yes	yes
euid	Records the effective user ID of the user who started the analyzed process.	yes	yes
exe	Records the path to the executable that was used to invoke the analyzed process.	yes	yes
exit	Records the exit code returned by a system call. This value varies by system call. You can interpret the value to its human-readable equivalent with the following command: `ausearch --interpret --exit exit_code`	yes	yes
family	Records the type of address protocol that was used, either IPv4 or IPv6.	yes	yes
feature	Records the audit feature being set or cleared.	yes	yes
file	Records the file involved in an integrity measurement.	yes	yes
filetype	Records the type of the file.	yes	yes
flags	Records the file system name flags.	yes	yes
fowner	Records the file owner used in an integrity policy rule.	yes	yes
fsgid	Records the file system group ID of the user who started the analyzed process.	yes	yes
fsmagic	Records the filesystem magic used in an integrity policy rule.	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
fsuuid	Records the fsuuid used in an integrity policy rule.	yes	yes
fsuid	Records the file system user ID of the user who started the analyzed process.	yes	yes
func	Records the function involved in an integrity policy rule.	yes	yes
gid	Records the group ID.	yes	yes
hash	Records the hash of a file involved in an integrity measurement.	yes	yes
hostname	Records the host name.	yes	yes
icmptype	Records the type of a Internet Control Message Protocol (ICMP) package that is received. Audit messages containing this field are usually generated by iptables.	yes	yes
id	Records the user ID of an account that was changed.	yes	yes
inode	Records the inode number associated with the file or directory recorded in an Audit event.	yes	yes
inode_gid	Records the group ID of the inode's owner.	yes	yes
inode_uid	Records the user ID of the inode's owner.	yes	yes
ip	Records the instruction pointer in a seccomp action.	yes	yes
items	Records the number of path records that are attached to this record.	yes	yes
key	Records the user defined string associated with a rule that generated a particular event in the Audit log.	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
list	Records the Audit rule list ID. The following is a list of known IDs: 0 – user, 1 – task, 4 – exit, 5 – exclude	yes	yes
mode	Records the file or directory permissions, encoded in numerical notation.	yes	yes
msg	Records a time stamp and a unique ID of a record, or various event-specific = pairs provided by the kernel or user space applications.	yes	yes
msgtype	Records the message type that is returned in case of a user-based AVC denial. The message type is determined by D-Bus.	yes	yes
name	Records the full path of the file or directory that was passed to the system call as an argument.	yes	yes
new-disk	Records the name of a new disk resource that is assigned to a virtual machine.	yes	yes
new-mem	Records the amount of a new memory resource that is assigned to a virtual machine.	yes	yes
new-vcpu	Records the number of a new virtual CPU resource that is assigned to a virtual machine.	yes	yes
new-net	Records the MAC address of a new network interface resource that is assigned to a virtual machine.	yes	yes
new_gid	Records a group ID that is assigned to a user.	yes	yes
new_lock	Records the new value of a lock being set on an audit feature.	yes	yes
nsec	Records the number of nanoseconds by which the system clock was shifted.	no	yes

Event Field	Explanation	RHEL 7	RHEL 8
oauid	Records the user ID of the user that has logged in to access the system (as opposed to, for example, using su) and has started the target process. This field is exclusive to the record of type OBJ_PID.	yes	yes
ocomm	Records the command that was used to start the target process.This field is exclusive to the record of type OBJ_PID.	yes	yes
old_lock	Records the old value of a lock being set on an audit feature.	yes	yes
opid	Records the process ID of the target process. This field is exclusive to the record of type OBJ_PID.	yes	yes
oses	Records the session ID of the target process. This field is exclusive to the record of type OBJ_PID.	yes	yes
ouid	Records the real user ID of the target process	yes	yes
obj	Records the SELinux context of an object. An object can be a file, a directory, a socket, or anything that is receiving the action of a subject.	yes	yes
objtype	Records the intent of the PATH record object in the context of a syscall.	yes	yes
obj_gid	Records the group ID of an object.	yes	yes
obj_lev_high	Records the high SELinux level of an object.	yes	yes
obj_lev_low	Records the low SELinux level of an object.	yes	yes
obj_role	Records the SELinux role of an object.	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
obj_type	Records the type of an object.	yes	yes
obj_uid	Records the UID of an object	yes	yes
obj_user	Records the user that is associated with an object.	yes	yes
ogid	Records the object owner's group ID.	yes	yes
old-disk	Records the name of an old disk resource when a new disk resource is assigned to a virtual machine.	yes	yes
old-mem	Records the amount of an old memory resource when a new amount of memory is assigned to a virtual machine.	yes	yes
old-vcpu	Records the number of an old virtual CPU resource when a new virtual CPU is assigned to a virtual machine.	yes	yes
old-net	Records the MAC address of an old network interface resource when a new network interface is assigned to a virtual machine.	yes	yes
old_prom	Records the previous value of the network promiscuity flag.	yes	yes
ouid	Records the real user ID of the user who started the target process.	yes	yes
path	Records the full path of the file or directory that was passed to the system call as an argument in case of AVC-related Audit events	yes	yes
perm	Records the file permission that was used to generate an event (that is, read, write, execute, or attribute change)	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
pid	The pid field semantics depend on the origin of the value in this field. In fields generated from user-space, this field holds a process ID. In fields generated by the kernel, this field holds a thread ID. The thread ID is equal to process ID for single-threaded processes. Note that the value of this thread ID is different from the values of `pthread_t` IDs used in user-space. For more information, see the `gettid(2)` man page.	yes	yes
ppid	Records the Parent Process ID (PID).	yes	yes
proctitle	Records the full command-line of the command that was used to invoke the analyzed process. The field is encoded in hexadecimal notation to not allow the user to influence the Audit log parser. The text decodes to the command that triggered this Audit event. When searching Audit records with the `ausearch` command, use the `-i` or `--interpret` option to automatically convert hexadecimal values into their human-readable equivalents.	yes	yes
prom	Records the network promiscuity flag.	yes	yes
proto	Records the networking protocol that was used. This field is specific to Audit events generated by iptables.	yes	yes
res	Records the result of the operation that triggered the Audit event.	yes	yes
resp	Records the response from an fanotify access control decision.	yes	yes
result	Records the result of the operation that triggered the Audit event.	yes	yes
saddr	Records the socket address.	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
sauid	Records the sender Audit login user ID. This ID is provided by D-Bus as the kernel is unable to see which user is sending the original auid.	yes	yes
sec	Records the number of seconds by which the system clock was shifted.	no	yes
ses	Records the session ID of the session from which the analyzed process was invoked.	yes	yes
sgid	Records the set group ID of the user who started the analyzed process.	yes	yes
sig	Records the number of a signal that causes a program to end abnormally. Usually, this is a sign of a system intrusion.	yes	yes
subj	Records the SELinux context of a subject. A subject can be a process, a user, or anything that is acting upon an object.	yes	yes
subj_clr	Records the SELinux clearance of a subject.	yes	yes
subj_role	Records the SELinux role of a subject.	yes	yes
subj_sen	Records the SELinux sensitivity of a subject.	yes	yes
subj_type	Records the type of a subject.	yes	yes
subj_user	Records the user that is associated with a subject.	yes	yes
success	Records whether a system call was successful or failed.	yes	yes
suid	Records the set user ID of the user who started the analyzed process.	yes	yes
syscall	Records the type of the system call that was sent to the kernel.	yes	yes

Event Field	Explanation	RHEL 7	RHEL 8
terminal	Records the terminal name (without `/dev/`).	yes	yes
tty	Records the name of the controlling terminal. The value (none) is used if the process has no controlling terminal.	yes	yes
uid	Records the real user ID of the user who started the analyzed process.	yes	yes
vm	Records the name of a virtual machine from which the Audit event originated.	yes	yes
xattr	Records the set of extended attributes modified and protected by EVM.	no	yes

Audit Record Types

The following table lists all currently-supported types of Audit records. The event type is specified in the `type=` field at the beginning of every Audit record.

Event Type	Explanation	RHEL 7	RHEL 8
ACCT_LOCK	Triggered when a user-space user account is locked by the administrator.	yes	yes
ACCT_UNLOCK	Triggered when a user-space user account is unlocked by the administrator.	yes	yes
ADD_GROUP	Triggered when a user-space group is added.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
ADD_USER	Triggered when a user-space user account is added.	yes	yes
ANOM_ABEND[1]	Triggered when a processes ends abnormally (with a signal that could cause a core dump, if enabled).	yes	yes
ANOM_ACCESS_FS[1]	Triggered when a file or a directory access ends abnormally.	yes	yes
ANOM_ADD_ACCT[1]	Triggered when a user-space account addition ends abnormally.	yes	yes
ANOM_AMTU_FAIL[1]	Triggered when a failure of the Abstract Machine Test Utility (AMTU) is detected.	yes	yes
ANOM_CRYPTO_FAIL[1]	Triggered when a failure in the cryptographic system is detected.	yes	yes
ANOM_DEL_ACCT[1]	Triggered when a user-space account deletion ends abnormally.	yes	yes
ANOM_EXEC[1]	Triggered when an execution of a file ends abnormally.	yes	yes
ANOM_LINK[1]	Triggered when suspicious use of file links is detected.	yes	yes
ANOM_LOGIN_ACCT[1]	Triggered when an account login attempt ends abnormally.	yes	yes
ANOM_LOGIN_FAILURES[1]	Triggered when the limit of failed login attempts is reached.	yes	yes
ANOM_LOGIN_LOCATION[1]	Triggered when a login attempt is made from a forbidden location.	yes	yes
ANOM_LOGIN_SESSIONS[1]	Triggered when a login attempt reaches the maximum amount of concurrent sessions.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
ANOM_LOGIN_TIME[1]	Triggered when a login attempt is made at a time when it is prevented by, for example, `pam_time` .	yes	yes
ANOM_MAX_DAC[1]	Triggered when the maximum amount of Discretionary Access Control (DAC) failures is reached.	yes	yes
ANOM_MAX_MAC[1]	Triggered when the maximum amount of Mandatory Access Control (MAC) failures is reached.	yes	yes
ANOM_MK_EXEC[1]	Triggered when a file is made executable.	yes	yes
ANOM_MOD_ACCT[1]	Triggered when a user-space account modification ends abnormally.	yes	yes
ANOM_PROMISCUOUS[1]	Triggered when a device enables or disables promiscuous mode.	yes	yes
ANOM_RBAC_FAIL[1]	Triggered when a Role-Based Access Control (RBAC) self-test failure is detected.	yes	yes
ANOM_RBAC_INTEGRITY_FAIL[1]	Triggered when a Role-Based Access Control (RBAC) file integrity test failure is detected.	yes	yes
ANOM_ROOT_TRANS[1]	Triggered when a user becomes root.	yes	yes
AVC	Triggered to record an SELinux permission check.	yes	yes
AVC_PATH	Triggered to record the dentry and vfsmount pair when an SELinux permission check occurs.	yes	yes
BPRM_FCAPS	Triggered when a user executes a program with a file system capability.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
CAPSET	Triggered to record the capabilities being set for process-based capabilities, for example, running as root to drop capabilities.	yes	yes
CHGRP_ID	Triggered when a user-space group ID is changed.	yes	yes
CHUSER_ID	Triggered when a user-space user ID is changed.	yes	yes
CONFIG_CHANGE	Triggered when the Audit system configuration is modified.	yes	yes
CRED_ACQ	Triggered when a user acquires user-space credentials.	yes	yes
CRED_DISP	Triggered when a user disposes of user-space credentials.	yes	yes
CRED_REFR	Triggered when a user refreshes their user-space credentials.	yes	yes
CRYPTO_FAILURE_USER	Triggered when a decrypt, encrypt, or randomize cryptographic operation fails.	yes	yes
CRYPTO_IKE_SA	Triggered when an Internet Key Exchange Security Association is established.	yes	yes
CRYPTO_IPSEC_SA	Triggered when an Internet Protocol Security Association is established.	yes	yes
CRYPTO_KEY_USER	Triggered to record the cryptographic key identifier used for cryptographic purposes.	yes	yes
CRYPTO_LOGIN	Triggered when a cryptographic officer login attempt is detected.	yes	yes
CRYPTO_LOGOUT	Triggered when a cryptographic officer logout attempt is detected.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
CRYPTO_PARAM_CHANGE_USER	Triggered when a change in a cryptographic parameter is detected.	yes	yes
CRYPTO_REPLAY_USER	Triggered when a replay attack is detected.	yes	yes
CRYPTO_SESSION	Triggered to record parameters set during a TLS session establishment.	yes	yes
CRYPTO_TEST_USER	Triggered to record cryptographic test results as required by the FIPS-140 standard.	yes	yes
CWD	Triggered to record the current working directory.	yes	yes
DAC_CHECK	Triggered to record DAC check results.	yes	yes
DAEMON_ABORT	Triggered when a daemon is stopped due to an error.	yes	yes
DAEMON_ACCEPT	Triggered when the auditd daemon accepts a remote connection.	yes	yes
DAEMON_CLOSE	Triggered when the auditd daemon closes a remote connection.	yes	yes
DAEMON_CONFIG	Triggered when a daemon configuration change is detected.	yes	yes
DAEMON_END	Triggered when a daemon is successfully stopped.	yes	yes
DAEMON_ERR	Triggered when an auditd daemon internal error is detected.	yes	yes
DAEMON_RESUME	Triggered when the auditd daemon resumes logging.	yes	yes
DAEMON_ROTATE	Triggered when the auditd daemon rotates the Audit log files.	yes	yes
DAEMON_START	Triggered when the auditd daemon is started.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
DEL_GROUP	Triggered when a user-space group is deleted	yes	yes
DEL_USER	Triggered when a user-space user is deleted	yes	yes
DEV_ALLOC	Triggered when a device is allocated.	yes	yes
DEV_DEALLOC	Triggered when a device is deallocated.	yes	yes
EOE	Triggered to record the end of a multi-record event.	yes	yes
EXECVE	Triggered to record arguments of the `execve(2)` system call.	yes	yes
FANOTIFY	Triggered when an fanotify access decision is made.	yes	yes
FD_PAIR	Triggered to record the use of the pipe and socketpair system calls.	yes	yes
FEATURE_CHANGE	Triggered when an Audit feature changed value.	yes	yes
FS_RELABEL	Triggered when a file system relabel operation is detected.	yes	yes
GRP_AUTH	Triggered when a group password is used to authenticate against a user-space group.	yes	yes
GRP_CHAUTHTOK	Triggered when a group account password or PIN is modified.	yes	yes
GRP_MGMT	Triggered to record user-space group account attribute modification.	yes	yes
INTEGRITY_DATA[2]	Triggered to record a data integrity verification event run by the kernel.	yes	yes
INTEGRITY_EVM_XATTR[2]	Triggered when an EVM-covered extended attribute is modified.	no	yes

Event Type	Explanation	RHEL 7	RHEL 8
INTEGRITY_HASH[2]	Triggered to record a hash type integrity verification event run by the kernel.	yes	yes
INTEGRITY_METADATA[2]	Triggered to record a metadata integrity verification event run by the kernel.	yes	yes
INTEGRITY_PCR[2]	Triggered to record Platform Configuration Register (PCR) invalidation messages.	yes	yes
INTEGRITY_RULE[2]	Triggered to record a policy rule.	yes	yes
INTEGRITY_STATUS[2]	Triggered to record the status of integrity verification.	yes	yes
IPC	Triggered to record information about a Inter-Process Communication object referenced by a system call.	yes	yes
IPC_SET_PERM	Triggered to record information about new values set by an IPC_SET control operation on an IPC object.	yes	yes
KERN_MODULE	Triggered to record a kernel module name on load or unload.	yes	yes
KERNEL	Triggered to record the initialization of the Audit system.	yes	yes
KERNEL_OTHER	Triggered to record information from third-party kernel modules.	yes	yes
LABEL_LEVEL_CHANGE	Triggered when an object's level label is modified.	yes	yes
LABEL_OVERRIDE	Triggered when an administrator overrides an object's level label.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
LOGIN	Triggered to record relevant login information when a user log in to access the system.	yes	yes
MAC_CALIPSO_ADD	Triggered when a NetLabel CALIPSO DOI entry is added.	no	yes
MAC_CALIPSO_DEL	Triggered when a NetLabel CALIPSO DOI entry is deleted.	no	yes
MAC_CHECK	Triggered when a user space MAC (Mandatory Access Control) decision is made.	yes	yes
MAC_CIPSOV4_ADD	Triggered when a Commercial Internet Protocol Security Option (CIPSO) user adds a new Domain of Interpretation (DOI). Adding DOIs is a part of the packet labeling capabilities of the kernel provided by NetLabel.	yes	yes
MAC_CIPSOV4_DEL	Triggered when a CIPSO user deletes an existing DOI. Adding DOIs is a part of the packet labeling capabilities of the kernel provided by NetLabel.	yes	yes
MAC_CONFIG_CHANGE	Triggered when an SELinux Boolean value is changed.	yes	yes
MAC_IPSEC_EVENT	Triggered to record information about an IPSec event, when one is detected, or when the IPSec configuration changes.	yes	yes
MAC_MAP_ADD	Triggered when a new Linux Security Module (LSM) domain mapping is added. LSM domain mapping is a part of the packet labeling capabilities of the kernel provided by NetLabel.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
MAC_MAP_DEL	Triggered when an existing LSM domain mapping is deleted. LSM domain mapping is a part of the packet labeling capabilities of the kernel provided by NetLabel.	yes	yes
MAC_POLICY_LOAD	Triggered when a SELinux policy file is loaded.	yes	yes
MAC_STATUS	Triggered when the SELinux mode (enforcing, permissive, off) is changed.	yes	yes
MAC_UNLBL_ALLOW	Triggered when unlabeled traffic is allowed when using the packet labeling capabilities of the kernel provided by NetLabel.	yes	yes
MAC_UNLBL_STCADD	Triggered when a static label is added when using the packet labeling capabilities of the kernel provided by NetLabel.	yes	yes
MAC_UNLBL_STCDEL	Triggered when a static label is deleted when using the packet labeling capabilities of the kernel provided by NetLabel.	yes	yes
MMAP	Triggered to record a file descriptor and flags of the mmap(2) system call.	yes	yes
MQ_GETSETATTR	Triggered to record the mq_getattr(3) and mq_setattr(3) message queue attributes.	yes	yes
MQ_NOTIFY	Triggered to record arguments of the mq_notify(3) system call.	yes	yes
MQ_OPEN	Triggered to record arguments of the mq_open(3) system call.	yes	yes
MQ_SENDRECV	Triggered to record arguments of the mq_send(3) and mq_receive(3) system calls.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
NETFILTER_CFG	Triggered when Netfilter chain modifications are detected.	yes	yes
NETFILTER_PKT	Triggered to record packets traversing Netfilter chains.	yes	yes
OBJ_PID	Triggered to record information about a process to which a signal is sent.	yes	yes
PATH	Triggered to record file name path information.	yes	yes
PROCTITLE	Gives the full command-line that triggered this Audit event, triggered by a system call to the kernel.	yes	yes
RESP_ACCT_LOCK[3]	Triggered when a user account is locked.	yes	yes
RESP_ACCT_LOCK_TIMED[3]	Triggered when a user account is locked for a specified period of time.	yes	yes
RESP_ACCT_REMOTE[3]	Triggered when a user account is locked from a remote session.	yes	yes
RESP_ACCT_UNLOCK_TIMED[3]	Triggered when a user account is unlocked after a configured period of time.	yes	yes
RESP_ALERT[3]	Triggered when an alert email is sent.	yes	yes
RESP_ANOMALY[3]	Triggered when an anomaly was not acted upon.	yes	yes
RESP_EXEC[3]	Triggered when an intrusion detection program responds to a threat originating from the execution of a program.	yes	yes
RESP_HALT[3]	Triggered when the system is shut down.	yes	yes
RESP_KILL_PROC[3]	Triggered when a process is terminated.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
RESP_SEBOOL[3]	Triggered when an SELinux Boolean value is set.	yes	yes
RESP_SINGLE[3]	Triggered when the system is put into single-user mode.	yes	yes
RESP_TERM_ACCESS[3]	Triggered when a session is terminated.	yes	yes
RESP_TERM_LOCK[3]	Triggered when a terminal is locked.	yes	yes
ROLE_ASSIGN	Triggered when an administrator assigns a user to an SELinux role.	yes	yes
ROLE_MODIFY	Triggered when an administrator modifies an SELinux role.	yes	yes
ROLE_REMOVE	Triggered when an administrator removes a user from an SELinux role.	yes	yes
SECCOMP	Triggered when a SECure COMPuting event is detected.	yes	yes
SELINUX_ERR	Triggered when an internal SELinux error is detected.	yes	yes
SERVICE_START	Triggered when a service is started.	yes	yes
SERVICE_STOP	Triggered when a service is stopped.	yes	yes
SOCKADDR	Triggered to record a socket address.	yes	yes
SOCKETCALL	Triggered to record arguments of the sys_socketcall system call (used to multiplex many socket-related system calls).	yes	yes
SOFTWARE_UPDATE	Triggered to record software update events.	yes	yes
SYSCALL	Triggered to record a system call to the kernel.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
SYSTEM_BOOT	Triggered when the system is booted up.	yes	yes
SYSTEM_RUNLEVEL	Triggered when the system's run level is changed.	yes	yes
SYSTEM_SHUTDOWN	Triggered when the system is shut down.	yes	yes
TEST	Triggered to record the success value of a test message.	yes	yes
TIME_ADJNTPVAL	Triggered when the system clock is modified.	no	yes
TIME_INJOFFSET	Triggered when a Timekeeping offset is injected to the sytem clock.	no	yes
TRUSTED_APP	The record of this type can be used by third party application that require auditing.	yes	yes
TTY	Triggered when TTY input was sent to an administrative process.	yes	yes
USER_ACCT	Triggered when a user-space user authorization attempt is detected.	yes	yes
USER_AUTH	Triggered when a user-space user authentication attempt is detected.	yes	yes
USER_AVC	Triggered when a user-space AVC message is generated.	yes	yes
USER_CHAUTHTOK	Triggered when a user account password or PIN is modified.	yes	yes
USER_CMD	Triggered when a user-space shell command is executed.	yes	yes
USER_DEVICE	Triggered when a user-space hotplug device is changed.	yes	yes
USER_END	Triggered when a user-space session is terminated.	yes	yes

Event Type	Explanation	RHEL 7	RHEL 8
USER_ERR	Triggered when a user account state error is detected.	yes	yes
USER_LABELED_EXPORT	Triggered when an object is exported with an SELinux label.	yes	yes
USER_LOGIN	Triggered when a user logs in.	yes	yes
USER_LOGOUT	Triggered when a user logs out.	yes	yes
USER_MAC_POLICY_LOAD	Triggered when a user-space daemon loads an SELinux policy.	yes	yes
USER_MGMT	Triggered to record user-space user account attribute modification.	yes	yes
USER_ROLE_CHANGE	Triggered when a user's SELinux role is changed.	yes	yes
USER_SELINUX_ERR	Triggered when a user-space SELinux error is detected.	yes	yes
USER_START	Triggered when a user-space session is started.	yes	yes
USER_TTY	Triggered when an explanatory message about TTY input to an administrative process is sent from user-space.	yes	yes
USER_UNLABELED_EXPORT	Triggered when an object is exported without SELinux label.	yes	yes
USYS_CONFIG	Triggered when a user-space system configuration change is detected.	yes	yes
VIRT_CONTROL	Triggered when a virtual machine is started, paused, or stopped.	yes	yes
VIRT_MACHINE_ID	Triggered to record the binding of a label to a virtual machine.	yes	yes
VIRT_RESOURCE	Triggered to record resource assignment of a virtual machine.	yes	yes

Additional Resources

- `auditd(8)` man page
- `ausearch(8)` man page
- `auditd.conf(5)` man page

---

1. All Audit event types prepended with ANOM are intended to be processed by an intrusion detection program. ↩

2. This event type is related to the Integrity Measurement Architecture (IMA), which functions best with a Trusted Platform Module (TPM) chip. ↩ ↩ ↩ ↩ ↩ ↩ ↩

3. All Audit event types prepended with RESP are intended responses of an intrusion detection system in case it detects malicious activity on the system. ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩ ↩

Product(s) **Red Hat Enterprise Linux** **Category** **Secure** **Component** **audit** **Tags** **audit** **auditing** **rhel** **security**

Article Type **General**

Comments

Login to see comments