NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kovas 2026

Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
Regioninio kibernetinės gynybos centro

INFORMACINIS BIULETENIS

AUDITAVIMO ĮRAŠAI „LINUX“ APLINKOJE

Rekomendacijų tikslas

Nacionalinis kibernetinio saugumo centras (toliau – NKSC), vykdydamas kibernetinių incidentų tyrimus, fiksuoja nemažai incidentų susijusių su „Linux“ šeimos operacinėmis sistemomis (toliau – **„Linux“**). Nemažai organizacijų ar įmonių yra klaidingai įsitikinusios, kad **„Linux“** operacinė sistema yra saugi ir be papildomų apsaugos ar auditavimo priemonių. Tačiau kaip ir „Windows“ operacinėse sistemose, taip ir „Linux“ būtina įdiegti papildomas apsaugos priemones ir tinkamai sukonfigūruoti auditavimo, įvykių žurnalų registravimo ir saugojimo funkcionalumus, kad įvykus kibernetiniam incidentui būtų galima identifikuoti kenkėjiškus veiksmus ir įrankius.

Pagal nutylėjimą **„Linux“** įvykių žurnaluose audituojami (kaupiami) įvairūs įrašai: naudotojų prisijungimai, programinės įrangos diegimas, operacinių sistemų veikimo sutrikimai ir pan. Tačiau dažnu atveju šios informacijos neužtenka, todėl NKSC rekomenduotina įdiegti ir tinkamai sukonfigūruoti papildomą auditavimo funkcionalumą.

„Audit“ – tai populiariausia ir dažnai sutinkama **„Linux“** programinė įranga leidžianti audituoti failų prieigą (angl. file access), stebėti sisteminius kreipinius (angl. system calls), jų argumentus, naudotojo veiksmų informaciją ir pan. Priklausomai nuo „Linux“ distribucijos, ši programinė įranga jau gali būti įdiegta, todėl reikia ją tik

I. „Audit“ konfigūravimas

„Ubuntu“, **„RedHat“** ar **„CentOS“** operacinėse sistemose **„Audit“** konfigūracijos failas ***„audit.conf“*** saugomas direktorijoje ***„/etc/audit“***. Pirmoje lentelėje nurodyti pagrindiniai **„Audit“** konfigūracijos parametrai, kurie saugomi ***„audit.conf“*** faile (gali skirtis priklausomai nuo **„Linux“** distribucijos ar **„Audit“** versijos).

1 lentelė. Parametrai

Parametrai	Reikšmė
log_file, log_format ir **log_group**	„***log_file“*** – nurodo direktoriją (kelią), kurioje turėtų būti saugomi audito įrašai (failai).
	„log_format“ – nustato, kaip (kokiu formatu) audito informacija įrašoma. Galimos reikšmės ***„raw“*** ir ***„nolog“***.
	„log_group“ – apibrėžia naudotojų grupę, kuriai priklauso įvykių žurnalų failai;
flush ir **freq**	nurodo „ar“, „kaip“ ir „kaip dažnai“ audito įrašai turi būti įrašomi į diską. Galimos „***flush“*** reikšmės: ***„none“, „incremental“, „data“*** ir ***„sync“***. **„freq“** parametras naudojamas, kai ***„flush“*** parametro

	reikšmė yra ***„incremental“***;
disp_qos, dispatcher ir **dispatcher_num_workers**	„***dispatcher“*** startuoja ***„Audit“*** paleidimo metu. ***„Audit“*** procesas perduoda audito pranešimus „***dispatcher“*** nurodytai programai. ***„disp_qos“*** nustato ar leidžiama ***„Audit“*** procesui ir „***dispatcher“*** bendrauti su nuostoliais (***„lossy“***) ar be nuostolių (***„lossless“***). Jei pasirenkama reikšmė ***„lossy“***, ***„Audit“*** procesas gali atmesti kai kuriuos audito pranešimus / įvykius;
	„dispatcher_num_workers“ – nurodomi lygiagretumo parametrai;
name_format ir **name**	„***name_format“*** – kontroliuoja kaip kompiuterių vardai yra įrašomi į audito įrašus. Galimos reikšmės ***„none“*** (vardai nėra naudojami), ***„hostname“*** (pateikiama ***„gethostname“*** reikšmė), ***„fqd“*** (vardas gaunamas iš DNS), ***„numeric“*** (įrašomas IP adresas) ir ***„user“*** (apibrėžiama ***„name“*** parametre);
max_log_file, max_log_file_action ir **num_logs**	***„max_log_file“*** – nurodomas įvykių žurnalo (failo dydis) megabaitais.
	„max_log_file_action“ – nurodomas veiksmas, kuris bus atliekamas pasiekus maksimalų failo dydį. Galimos ***„max_log_file_action“*** reikšmės***: „ignore“***, ***„syslog“***, ***„suspend“***, ***„rotate“*** ir ***„keep_logs“***;
	„num_logs“ – nurodo žurnalinių įrašų (failų) skaičių. Galimos reikšmės nuo 0 iki 99. Reikšmė mažesnė nei 2 reiškia, kad žurnaliniai įrašai (failai) nėra rotuojami;
space_left ir ***space_left_action***	***„space_left“*** nurodoma reikšmė megabaitais. Disko vietai sumažėjus iki nurodytos reikšmės, ***„Audit“*** procesas inicijuoja veiksmą, kuris nurodytas parametre ***„space_left_action“***. Galimos reikšmės ***„ignore“, „syslog“***, ***„email“***, ***„exec“***, ***„suspend“***, ***„single“*** ir ***„halt“***;
action_mail_acct	nurodomas el. pašto adresas kuriuo turi būti siunčiami pranešimai;
admin_space_left, **admin_space_left_action** ir ***disk_full_action***	***„admin_space_left“*** – nurodoma disko talpa (vieta) megabaitais. Disko vietai sumažėjus iki nurodytos reikšmės, ***„Audit“*** procesas inicijuoja veiksmą, kuris nurodytas parametre **„admin_space_left_action“**. Galimos reikšmės ***„ignore“***, ***„syslog“***, ***„email“***, ***„exec“***, ***„suspend“***,

	„single“ ir ***„halt“***. Parametro ***„admin_space_left“*** reikšmė turi būti mažesnė už parametre ***„space_left“*** nurodytą reikšmę;
	disk_full_action – nurodo veiksmą, kuris turi būti atliktas, kai baigiasi disko talpa (vieta). Galimos reikšmės: ***„ignore“***, ***„syslog“***, ***„rotate“***, ***„exec“***, ***„suspend“***, ***„single“*** ir ***„halt“***;
disk_error_action	nurodo veiksmą, kuris turi būti atliktas, kai įvykių įrašymo metu įvyksta bet kokio tipo disko klaida. Galimos reikšmės: ***„ignore“***, ***„syslog“***, ***„exec“***, ***„suspend“***, ***„single“*** ir ***„halt“***;
tcp_listen_port, ***tcp_listen_queue***, ***tcp_client_ports***, ***tcp_client_max_idle*** ir ***tcp_max_per_addr***	***„Audit“*** procesas gali priimti įvykius ir iš kitų ***„Audit“*** procesų. ***„TCP“*** parametrai leidžia reguliuoti įeinančius sujungimus. ***„tcp_listen_port“*** – parametre nurodomas tinklo prievadas (galimos reikšmės nuo 0 iki 65535), kurį kontroliuos ***„Audit“*** procesas.
	„tcp_listen_queue“ – parametras leidžia nustatyti maksimalų laukiančių tinklo sujungimų skaičių.
	„tcp_client_ports“ – parametras nustato kokie kliento tinklo prievadai yra leidžiami.
	„tcp_client_max_idle“ – parametre nurodoma reikšmė sekundėmis, po kurios ***„Audit“*** procesas sugeneruos pranešimą dėl prarasto tinklo sujungimo su klientu (kitu ***„Audit“*** procesu).
	„tcp_max_per_addr“ – parametre nurodoma reikšmė, kiek savarankiškų sujungimų leidžiama iš vieno IP adreso;
enable_krb5	Jeigu parametro reikšmė yra nurodyta ***„yes“***, tai reiškia, kad autentifikavimui ir šifravimui bus naudojamas ***„Kerberos 5“***
krb5_principal ir ***krb5_key_file***	***„Kerberos“*** parametrų nustatymas

Daugiau informacijos apie **„Audit“** konfigūraciją ir parametrus galima rasti:

- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-configuring_the_audit_service
- https://doc.opensuse.org/documentation/leap/security/html/book-security/cha-audit-setup.html
- http://manpages.ubuntu.com/manpages/trusty/man5/Audit.conf.5.html
- https://documentation.suse.com/sles/15-SP1/html/SLES-all/cha-audit-comp.html#sec-audit-Audit
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/8/html/security_hardening/auditing-the-system_security-hardening

II. „Audit“ taisyklės

„Ubuntu“, **„RedHat“** ar **„CentOS“** operacinėse sistemose **„Audit“** taisyklės saugomos ***„/etc/audit/rules.d“*** direktorijoje ***„audit.rules“*** faile. **„Audit“** proceso startavimo metu taisyklės yra nukopijuojamos į ***„/etc/audit/“*** direktorijoje esantį ***„audit.rules“*** failą.

„Audit“ taisyklės sudaromos naudojantis pagrindiniais raktais:
-a <s,v> – prideda taisyklę į taisyklių sąrašo **<s>** pabaigą, kurioje nurodomas veiksmas **<v>**;
-A <s,v> – prideda taisyklę į taisyklių sąrašo **<s>** pradžią, kurioje nurodomas veiksmas **<v>**;
-F l=<r> – sudaroma taisyklė, kurioje nurodomas lauko pavadinimas **<l>**, operatorius **(=,!=,<,>,<=, >=,&,&=)** ir reikšmė **<r>**;
-k <raktas> – filtro raktas;
-p <r|w|x|a> – stebėsenos teisių filtras. **<r>** – skaityti, **<w>** – rašyti, **<x>** – vykdyti, **<a>** – požymis;
-S <s> – sudaroma taisyklė, kurioje nurodomas sisteminis krepinys **<s>** (angl. ***„system call“***) arba jo numeris;
-w <kelias> – įtraukia failą / direktoriją į stebėseną (angl. ***„monitoring“***);
-W <kelias> – neįtraukia failo / direktorijos į stebėseną (angl. ***„monitoring“***);

III. Taisyklių sudarymo pavyzdžiai

Taisyklė ***„-a always,exit -F perm=r /etc/passwd-k users“*** nustato, kad bus stebimas failas ***„/etc/passwd“***. Įvykis įvykių žurnale bus registruojamas tik tada, kai failą bus bandoma perskaityti **(-F perm=r)**. Įvykdžius komandą ***„cat /etc/passwd“*** į įvykių žurnalą įrašomi įrašai:

- type=SYSCALL msg=audit(1634023306.463:**803**): arch=c000003e syscall=2 success=yes exit=3 a0=7ffc807ec8a1 a1=0 a2=20000 a3=69d items=1 ppid=1431 pid=1701 auid=1000 uid=0 gid=0 euid=0 suid=0 fsuid=0 egid=0 sgid=0 fsgid=0 tty=pts0 ses=1 comm="cat" exe="/bin/cat" key="users"
- type=PATH msg=audit(1634023306.463:**803**): item=0 name="/etc/passwd" inode=1306167 dev=fc:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 nametype=NORMAL
- type=PROCTITLE msg=audit(1634023306.463:**803**): proctitle=636174002F6574632F706173737764

Įvykių žurnale, įrašytus įvykius, galima interpretuoti taip:

type=SYSCALL – ***„type“*** laukelyje nurodomas įvykio tipas. Reikšmė ***„SYSCALL“*** nurodo, kad įvykis užregistruotas užfiksavus sisteminį kreipinį (angl. ***„system call“***) į branduolį (angl. ***„kernel“***).
msg=audit(1634023306.463:803) – ***„msg“*** laukelyje nurodomas įvykio data, laikas ir unikalus identifikacinis numeris (toliau – ID) (data_laikas:ID). Data ir laikas pateikiami ***„Unix“*** formatu.
arch=c000003e – ***„arch“*** laukelyje nurodoma sistemos procesoriaus architektūra. Reikšmė įrašoma ***„Hex“*** formatu.
syscall=2 – ***„syscall“*** laukelyje nurodoma sisteminio kreipinio (angl. ***„system call“***) tipas. Šiuo atveju reikšmė **„2“** atitinka reikšmę ***„open“***.
success=yes – ***„success“*** laukelyje nurodoma sisteminio kreipinio (angl. ***„system call“***) būsena (pavykęs (***„yes“***) ar nepavykęs (***„no“***)).
exit=3 – ***„exit“*** laukelyje nurodoma sisteminio kreipinio (angl. ***„system call“***) grąžinama reikšmė (angl. ***„exit code“***).
a0=7ffc807ec8a1, **a1=0**, **a2=20000**, **a3=69d** – ***„a0“*** – ***„a3“*** laukeliuose nurodomi pirmieji sisteminio kreipinio (angl. ***„system call“***) argumentai ***„Hex“*** formatu.
items=1 – ***„items“*** laukelyje nurodomas kelių (angl. ***„paths“***) skaičius įvykyje.
ppid=1431 – ***„ppid“*** laukelyje nurodomas šakninio proceso ID (angl. ***„Parent Process ID (PPID)“***).
pid=1701 – ***„pid“*** laukelyje nurodomas proceso ID (angl. ***„Process ID (PID)“***).
auid=1000 – ***„auid“*** laukelyje nurodomas naudotojo ID.
uid=0 – ***„uid“*** laukelyje nurodomas naudotojo ID, kuris startavo analizuojamą procesą.
gid=0 – ***„gid“*** laukelyje nurodomas grupės ID, kuriai priklauso naudotojas, kuris startavo analizuojamą procesą.
euid=0 – ***„euid“*** laukelyje nurodomas „efektyvaus“ naudotojo ID, kuris startavo analizuojamą procesą.
suid=0 – ***„suid“*** laukelyje nurodomas „nustatytas“ naudotojo ID, kuris startavo analizuojamą procesą.

fsuid=0 – ***„fsuid“*** laukelyje nurodomas „failų sistemos“ naudotojo ID, kuris startavo analizuojamą procesą.
egid=0 – ***„egid“*** laukelyje nurodomas „efektyvios“ grupės ID, kuriai priklauso naudotojas, kuris startavo analizuojamą procesą.
sgid=0 – ***„sgid“*** laukelyje nurodomas „nustatytos“ grupės ID, kuriai priklauso naudotojas, kuris startavo analizuojamą procesą.
fsgid=0 – ***„fsgid“*** laukelyje nurodomas „failų sistemos“ grupės ID, kuriai priklauso naudotojas, kuris startavo analizuojamą procesą.
tty=pts0 – ***„tty“*** laukelyje nurodomas terminalas iš kuriuo buvo paleistas analizuojamas procesas.
ses=1 – ***„ses“*** laukelyje nurodomas sesijos ID. Tos sesijos, kurios metu buvo paleistas analizuojamas procesas.
comm="cat" – ***„comm“*** laukelyje nurodoma komanda, kurios pagalba buvo paleistas analizuojamas procesas.
exe="/bin/cat" – ***„exe“*** laukelyje nurodomas kelias (direktorija) kurioje yra vykdomasis failas, kuriuo pagalba buvo paleistas analizuojamas procesas.
key="users" – ***„key“*** laukelyje nurodoma Jūsų apibrėžta filtro rakto reikšmė.
type=PATH – ***„type“*** laukelyje nurodomas kelias (angl. ***„path“***), kuris sisteminiame kreipinyje pateikiamas kaip argumentas (***„/etc/passwd“***).
msg=audit(1634023306.463:803) – ***„msg“*** laukelyje nurodomas įvykio data, laikas ir unikalus ID. Data ir laikas pateikiami ***„Unix“*** formatu.
item=0 – ***„item“*** laukelyje nurodomas kuris elementas iš visų nurodytų ***„type=SYSCALL“*** įraše elementų yra dabartinis įrašas. Reikšmė ***„0“*** reiškia, kad tai pirmasis elementas.
name="/etc/passwd" – ***„name“*** laukelyje nurodomas kelias (angl. ***„path“***) į failą ar direktoriją, kuris sisteminiame kreipinyje pateikiamas kaip argumentas.
inode=1306167 – ***„inode“*** laukelyje *nurodomas „inode“* numeris, kuris susietas su failu ar direktorija, kuri pateikta įraše.
dev=fc:00 – ***„dev“*** laukelyje nurodomas šalutinis ir pagrindinis įrenginio ID („dev/fc/0“), kuriame yra failas ar direktorija, kuri pateikta įraše.
mode=0100644 – ***„mode“*** laukelyje nurodomo failo teisės (***„-rw-r--r--“***).
ouid=0 – ***„ouid“*** laukelyje nurodomas objekto „savininko“ (naudotojo) ID.
ogid=0 – ***„ogid“*** laukelyje nurodomas objekto „savininko“ (naudotojo) grupės ID.
rdev=00:00 – ***„rdev“*** laukelyje nurodomas įrašytas įrenginio identifikatorius. Naudojamas tik specialiems failams.
nametype=NORMAL – ***„nametype“*** laukelyje nurodomas kiekvieno kelio (angl. ***„path“***) įraše operacijos paskirtis.
type=PROCTITLE – ***„type“*** laukelyje nurodomas įvykio tipas.
msg=audit(1634023306.463:803) – ***„msg“*** laukelyje nurodomas įvykio data, laikas ir unikalus ID. Data ir laikas pateikiami ***„Unix“*** formatu.
proctitle=636174002F6574632F706173737764 – ***„proctitle“*** laukelyje nurodoma komanda, kuri iššaukė taisyklės suveikimą t. y. audito įrašo įrašymą. Konvertavus iš ***„Hex“*** – ***„cat./etc/passwd“***.

Taisyklė ***„-a always,exit -F dir=/etc -F perm=w -F uid>=1000 -F success=0 -k unsuccessful_write“*** nustato, kad bus stebima direktorija ***„etc“***. Įvykis įvykių žurnale bus registruojamas tik tada, kai naudotojai ***(uid>=1000)*** įvykdys nesėkmingus bandymus ***(success=0)*** įrašyti ***(perm=w)*** į direktoriją ***(dir=/etc)***. Naudotojo teisėmis atlikus bandymą įrašyti į ***„etc“*** direktorijoje esantį failą ***„yum.conf“*** į įvykių žurnalą įrašomi įrašai:

- type=SYSCALL msg=audit(1636005088.985:191): arch=c000003e syscall=2 success=no exit=-13 a0=11a6f00 a1=241 a2=1b6 a3=7ffc6d873fa0 items=2 ppid=1765 pid=1780 auid=0 uid=1000 gid=1000 euid=1000 suid=1000 fsuid=1000 egid=1000 sgid=1000 fsgid=1000 tty=pts0 ses=2 comm="nano" exe="/usr/bin/nano" subj=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023 key="unsuccessful_write"
- type=PATH msg=audit(1636005088.985:191): item=0 name="/etc" inode=16777281 dev=fd:00 mode=040755 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=PARENT cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
- type=PATH msg=audit(1636005088.985:191): item=1 name="yum.conf" inode=16892512 dev=fd:00 mode=0100644 ouid=0 ogid=0 rdev=00:00 obj=system_u:object_r:etc_t:s0 objtype=NORMAL cap_fp=0000000000000000 cap_fi=0000000000000000 cap_fe=0 cap_fver=0
- type=PROCTITLE msg=audit(1636005088.985:191): proctitle=6E616E6F0079756D2E636F6E66

Tokiu pat principu į auditavimo procesą įmanoma įtraukti ir sėkmingus bandymus įrašyti ar skaityti. Nurodyti Jūsų informacinėje infrastruktūroje naudojamus naudotojų vardus, audituoti jų veiksmus. Rekomenduojame auditavimo įrašus peržiūrinėti pasinaudojus ***„ausearch“*** funkcionalumu.

Antroje lentelėje yra pateikiami taisyklių pavyzdžiai. Kuriant taisykles rekomenduojame remtis oficialiomis *„auditd“* rekomendacijomis ir kiekvienoje taisyklėje nurodyti savo sistemos architektūrą („***arch=b32***“ ar ***„arch=b64“***). Taip yra paspartinamas stebėjimo procesas, kadangi reikalingų taisyklių kiekis sumažinamas perpus (pagal nutylėjimą, nenurodant ***„arch“*** argumento, stebimi abiejų architektūrų sisteminiai kreipiniai – taip sukuriant dvi atskiras taisykles kiekvienai aprašytai taisyklei). Atkreipiame dėmesį, kad priklausomai nuo tarnybinės stoties paskirties (failų, el. pašto ar *„Web“*) **„Audit“** gali generuoti pasikartojančius įvykius, kurių kaupimas ar stebėjimas neturės jokios prasmės. Diegiant **„Audit“** taisykles, pirmiausiai rekomenduojame tai atlikti testavimo aplinkoje, išfiltruoti t. y. neauditуoti nereikalingų audito įrašų ar sukurti Jūsų informacinei infrastruktūrai pritaikytas taisykles. **„Linux“** palaikomų sisteminių kreipinių sąrašą galima sužinoti įvykdžius ***„ausyscall --dump“*** komandą.

Žemiau pateikiamų taisyklių veikimas išbandytas šiuose 64 bitų ***„server“*** operacinėse sistemose:

- ***„CentOS Stream 10“***, ***„Audit“*** versija 4.0.3;
- ***„Ubuntu 24.04 LTS““***, ***„Audit“*** versija 3.1.2.

2 lentelė. Taisyklės

Įvykių kategorija	**Taisyklės**	**Pastabos**
Darbinės direktorijos įvykiai	-a always,exclude -F msgtype=CWD	Rekomenduojame įtraukti šią taisyklę, kadangi šio tipo įrašų kaupimas neturi prasmės
Laiko sinchronizavimas	-a never,exit -F arch=b64 -S adjtimex -F auid=unset -F uid=chrony -F subj_type=chronyd_t	Rekomenduojame įtraukti šias taisykles, kadangi operacinė sistema ***„CentOS“*** sugeneruoja didelį šių įvykių skaičių, kurių kaupimas neturi prasmės
Prisijungimas prie operacinės sistemos	-a always,exclude -F msgtype=CRYPTO_KEY_USER	Rekomenduojame įtraukti šią taisyklę, kadangi šių įvykių kaupimas neturi prasmės. Susigeneruoja ***„CentOS“*** operacinėje sistemoje
Vykdomieji failai, scenarijai (angl. *„scripts“*) ar procesai	-a exit,always -F arch=b64 -S execve -k all_exec	Generuoja didelį įvykių skaičių. Rekomenduojama įgalinti tik vykdant taisyklių kūrimą, testavimą, įvykus kibernetiniam incidentui ar pan.

Auditavimo įrašai / funkcionalumas	-a always,exit -F arch=b64 -F dir=/var/log/audit -k audit_logs -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/audit -k audit_tools -a always,exit -F arch=b64 -F perm=x -F path=/sbin/auditctl -k audit_tools -a always,exit -F arch=b64 -F perm=x -F path=/sbin/audit -k audit_tools	Centralizuotai kaupiant auditavimo įrašus rekomenduojame išjungti procesą kuris surenka audito įrašus
Operacinės sistemos veikimo sutrikimai (angl. *„crash“*)	-a always,exit -F arch=b64 -F perm=wa -F dir=/var/crash -k system_crash	
Branduolio (angl. *„kernel“*) parametrai	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/sysctl.conf -k kernel_param -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/sysctl.d -k kernel_param	
Branduolio (angl. *„kernel“*) moduliai	-a always,exit -F arch=b64 -F perm=wa -F dir=/etc/modprobe.d -k kernel_mod	
	-a always,exit -F arch=b64 -F perm=wa -F dir=/etc/sysconfig/modules -k kernel_mod	***„CentOS“***
Bendrinamų bibliotekų nuorodos (angl. *„shared libraries paths“*)	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/ld.so.conf -k lib_path_settings -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/ld.so.conf.d -k lib_path_settings	
Branduolio (angl. *„kernel“*) parametrai	-a always,exit -F arch=b64 -S init_module -k kernel_module -a always,exit -F arch=b64 -S finit_module -k kernel_module -a always,exit -F arch=b64 -S delete_module -k kernel_module	
„Systemd“	-a always,exit -F arch=b64 -F perm=x -F path=/bin/systemctl -k systemd_monitoring -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/systemd -k systemd_monitoring	
Pirminis procesas ***„init.d“***, paleidimo parametrai / procesai	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/inittab -k startup_scripts -a always,exit -F arch=b64 -F perm=wa -F	

	dir=/etc/init.d -k startup_scripts	
„SSL“ / ***„TLS“*** tunelis	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/stunnel4 -k stunnel	Priklausomai ar įdiegtas ir naudojamas
	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/stunnel -k stunnel	***„CentOS“***
„cron“ įvykiai	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/cron.allow -k cron_events -a always,exit -F arch=b64 -F perm=wa -F path=/etc/cron.deny -k cron_events -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/cron.d -k cron_events -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/cron.daily -k cron_events -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/cron.hourly -k cron_events -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/cron.monthly -k cron_events -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/cron.weekly -k cron_events -a always,exit -F arch=b64 -F perm=wa -F path=/etc/crontab -k cron_events -a always,exit -F arch=b64 -F dir=/var/spool/cron -k cron_events	
Ugniasienės įvykiai	-a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/ufw -k firewall -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/firewalld -k firewall -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/firewalld -k firewall -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/ufw -k firewall	
„PAM“ (Pluggable Authentication Modules) nustatymai	-a always,exit -F arch=b64 -F perm=wa -F dir=/etc/pam.d -k pam_config -a always,exit -F arch=b64 -F perm=wa -F path=/etc/security/limits.conf -k pam_config	

	-a always,exit -F arch=b64 -F perm=wa -F dir=/etc/security/limits.d -k pam_config -a always,exit -F arch=b64 -F perm=wa -F path=/etc/security/pam_env.conf -k pam_config -a always,exit -F arch=b64 -F perm=wa -F path=/etc/security/namespace.conf -k pam_config -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/security/namespace.d -k pam_config -a always,exit -F arch=b64 -F perm=wa -F path=/etc/security/namespace.init -k pam_config	
IP lentelių (angl. *„IP tables“*) įvykiai	-a always,exit -F arch=b64 -F perm=x -F path=/sbin/xtables-nft-multi -k IP_tables	
Tinklo parametrai / konfigūracija	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/hosts -k net_environment -a always,exit -F arch=b64 -F perm=wa -F path=/etc/networks -k net_environment -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/netplan -k net_environment -a always,exit -F arch=b64 -F perm=wa -F path=/run/systemd/resolve/stub-resolv.conf -k net_environment -a always,exit -F arch=b64 -F perm=wa -F path=/etc/nsswitch.conf -k net_environment	***„Ubuntu“***
	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/hosts -k net_environment -a always,exit -F arch=b64 -F perm=wa -F path=/etc/networks -k net_environment -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/netplan -k net_environment -a always,exit -F arch=b64 -F perm=wa -F path=/etc/resolv.conf -k net_environment -a always,exit -F arch=b64 -F perm=wa -F path=/etc/authselect/nsswitch.conf -k	***„CentOS“***

	net_environment -a always,exit -F arch=b64 -F perm=wa -F path=/etc/sysconfig/network -k net_environment -a always,exit -F arch=b64 -F perm=wa -F dir=/etc/sysconfig/network-scripts -k net_environment	
Tinklo parametrai / konfigūracija	-a always,exit -F dir=/etc/NetworkManager/ -F perm=wa -k net_environment_exe	
	-a always,exit -F arch=b64 -S sethostname -S setdomainname –k net_environment_exe	
Tinklo sujungimai	-a always,exit -F arch=b64 -S connect -F auid!=unset -k net_conn	Sugeneruoja nemažai įvykių. Priklausomai nuo tarnybinės stoties paskirties galimai bus reikalingas papildomas įvykių išfiltravimas
Laiko juosta	-a always,exit -F arch=b64 -F perm=wa -F path=/usr/share/zoneinfo/Etc/UTC -k time_zone	
Data ir laikas	-a exit,always -F arch=b64 -S adjtimex -S settimeofday -S clock_settime -k time_change	
Programinės įrangos diegimas / atnaujinimas	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/apt -k software_mgmt -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/add-apt-repository -k software_mgmt -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/apt-get -k software_mgmt	Pasirinkti priklausomai nuo ***„Linux“*** distribucijos
	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/rpm -k software_mgmt -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/dnf-3 -k software_mgmt	
„Python“ programinė įranga	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/pip -k python_soft	Pašalinti ar pridėti naudojamas

	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/pip3 -k python_soft -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/python3.12 -k python_soft	programinės įrangos versijas.
„KExec“ naudojimas	-a always,exit -F arch=b64 -S kexec_load -k kexec_monitoring	Priklausomai ar įdiegtas, ar naudojamas
„Mount“ veiksmai	-a always,exit -F arch=b64 -S mount -S umount2 -F auid!=unset -k mount_operations	
Procesų ir sesijų informacija	-a always,exit -F arch=b64 -F perm=wa -F path=/var/run/utmp -k session_info -a always,exit -F arch=b64 -F perm=wa -F path=/var/log/btmp -k session_info -a always,exit -F arch=b64 -F perm=wa -F path=/var/log/wtmp -k session_info	
Naudotojo prisijungimo metu vykdomi scenarijai (angl. *„scripts“*)	-a always,exit -F arch=b64 -F perm=wa -F dir=/etc/profile.d -k user_profiles -a always,exit -F arch=b64 -F perm=wa -F path=/etc/profile -k user_profiles	
Prisijungimo apvalkalai (angl. *„shells“*)	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/shells -k login_shells	
Išorinės laikmenos	-a always,exit -F arch=b64 -F perm=rwxa -F dir=/media -k external_media	
„MAC“ prieigos teisės	-a always,exit -F arch=b64 -F perm=wa -F dir=/etc/selinux -k MAC_policy	
„DAC“ prieigos teisės	-a always,exit -F arch=b64 -S chmod -S fchmod -S fchmodat -k perm_mod -a always,exit -F arch=b64 -S chown -S fchown -S fchownat -S lchown -k perm_mod -a always,exit -F arch=b64 -S setxattr -S lsetxattr -S fsetxattr -S removexattr -S lremovexattr -S fremovexattr -k perm_mod	Operacinės sistemos įjungimo, išjungimo ar atnaujinimo metu gali generuoti didelį įvykių skaičių

	-a always,exit -F arch=b64 -F perm=x -F path=/bin/chmod -k perm_mod -a always,exit -F arch=b64 -F perm=x -F path=/bin/chown -k perm_mod -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/xattr -k perm_mod	
Naudotojų paskyrų nustatymai	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/login.defs -k login	
Paskyrų perjungimas	-a always,exit -F arch=b64 -F perm=x -F path=/bin/su -k privilege_esc -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/sudo -k privilege_esc	
Komandų paleidimas ***„root“*** teisėmis	-a always,exit -F arch=b64 -F euid=0 -S execve -k root_commands	Analogiškai pakeitus ***„euid“*** reikšmę galima audituoti kitų naudotojų veiksmus. Priklausomai nuo tarnybinės stoties paskirties ir joje vykstančių procesų gali generuoti didelį įvykių skaičių. Prireikus, nereikalingus įrašus galima išfiltruoti
Naudotojai, grupės ir slaptažodžiai	-a always,exit -F arch=b64 -F perm=wa -F path=/etc/group -k user_group -a always,exit -F arch=b64 -F perm=wa -F path=/etc/passwd -k user_list -a always,exit -F arch=b64 -F path=/etc/gshadow -k group_accounts -a always,exit -F arch=b64 -F path=/etc/shadow -k user_pass -a always,exit -F arch=b64 -F path=/etc/security/opasswd -k passwd_history -a always,exit -F arch=b64 -F perm=x -F	

	path=/usr/bin/passwd -k passwd_change	
Naudotojai ir grupės	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/gpasswd -k user_add -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/groupadd -k group_add -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/adduser -k user_add -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/groupmod -k group_modification -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/useradd -k user_add -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/userdel -k user_del -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/deluser -k user_del -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/usermod -k user_modification -a always,exit -F arch=b64 -F perm=rw -F path=/etc/sudoers -k sudoers_change -a always,exit -F arch=b64 -F perm=rw -F dir=/etc/sudoers.d -k sudoers_change	
Programinė įranga siejama su informacijos rinkimu (žvalgyba)	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/whoami -k reconnaissance -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/ifconfig -k reconnaissance -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/id -k reconnaissance -a always,exit -F arch=b64 -F perm=x -F path=/bin/hostname -k reconnaisance -a always,exit -F arch=b64 -F perm=x -F path=/bin/uname -k reconnaisance -a always,exit -F arch=b64 -F perm=r -F path=/etc/issue -k reconnaisance -a always,exit -F arch=b64 -F perm=r -F	

	path=/etc/hostname -k reconnaisance -a always,exit -F arch=b64 -F perm=r -F path=/proc/version -k reconnaisance -a always,exit -F arch=b64 -F perm=r -F path=/proc/sys/kernel/domainname -k reconnaisance -a always,exit -F arch=b64 -F perm=r -F path=/proc/swaps -k reconnaisance -a always,exit -F arch=b64 -F perm=r -F path=/proc/partitions -k reconnaisance -a always,exit -F arch=b64 -F perm=r -F path=/proc/cpuinfo -k reconnaisance	
Programinė įranga siejama su kenkimo veikla	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/wget -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/curl -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/base64 -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/bin/nc.openbsd -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/ssh -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/scp -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/sftp -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/tnftp -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/dmesg -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/ps -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/pstree -k suspicious -a always,exit -F arch=b64 -F perm=x -F	Pasirinkti atsižvelgiant į tarnybinės stoties specifiką.

	path=/usr/bin/top -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/htop -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/kill -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/killall -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/last -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/lsof -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/kmod -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/arp -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/bin/bash -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/xtables-nft-multi -k suspicious	
	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/wget -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/curl -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/base64 -k suspicious-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/nc -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/ssh -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/scp -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/sftp -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/tnftp -k suspicious	**„CentOS“**

	-a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/dmesg -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/ps -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/pstree -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/top -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/htop -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/kill -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/killall -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/last -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/lsof -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/bin/kmod -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/arp -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/bin/bash -k suspicious -a always,exit -F arch=b64 -F perm=x -F path=/usr/sbin/xtables-nft-multi -k suspicious	
32 bitų sisteminių kreipinių vartojimas 64 bitų sistemoje	-a always,exit -F arch=b32 -S all -k 32bit_abi	32 bitų kreipinių vartojimas 64 bitų sistemose yra įtartinas ir turėtų būti stebimas.
Nesėkmingas bandymas rašyti į direktorijas	-a always,exit -F dir=/etc -F perm=w -F uid>=1000 -F success=0 -k unsuccessful_write -a always,exit -F dir=/var -F perm=w -F uid>=1000 -F success=0 -k unsuccessful_write	Pagal poreikį pasirinkti reikiamas direktorijas, nurodyti naudotojus ar pan.

	-a always,exit -F dir=/bin -F perm=w -F uid>=1000 -F success=0 -k unsuccessful_write -a always,exit -F dir=/sbin -F perm=w -F uid>=1000 -F success=0 -k unsuccessful_write -a always,exit -F dir=/usr/bin -F perm=w -F uid>=1000 -F success=0 -k unsuccessful_write -a always,exit -F dir=/usr/sbin -F perm=w -F uid>=1000 -F success=0 -k unsuccessful_write	
Failų trynimas (naudotojai)	-a always,exit -F arch=b32 -S rename -F auid!=unset -F uid>=1000 -k user_delete_files -a always,exit -F arch=b32 -S renameat -F auid!=unset -F uid>=1000 -k user_delete_files -a always,exit -F arch=b32 -S rmdir -F auid!=unset -F uid>=1000 -k user_delete_files -a always,exit -F arch=b32 -S unlink -F auid!=unset -F uid>=1000 -k user_delete_files -a always,exit -F arch=b32 -S unlinkat -F auid!=unset -F uid>=1000 -k user_delete_files	
	-a always,exit -F arch=b64 -S rename -F auid!=unset -F uid>=1000 -k user_delete_files -a always,exit -F arch=b64 -S renameat -F auid!=unset -F uid>=1000 -k user_delete_files -a always,exit -F arch=b64 -S rmdir -F auid!=unset -F uid>=1000 -k user_delete_files	

	-a always,exit -F arch=b64 -S unlink -F auid!=unset -F uid>=1000 -k user_delete_files -a always,exit -F arch=b64 -S unlinkat -F auid!=unset -F uid>=1000 -k user_delete_files	
Kita programinė įranga	Priklausomai nuo tarnybinės stoties paskirties galima įtraukti į stebėseną **(-w)** šią programinę įrangą: ***„NPM“***, ***„PHP“***, ***„PERL“***, ***„Ruby“***, ***„Java“***, ***„Xterm“***, ***„Lua“***, ***„Golang“***, ***„Node.js“*** ar ***„Dart“***.	

Daugiau informacijos apie taisyklių sudarymą ir taisyklių pavydžius galima rasti:

- https://access.redhat.com/articles/4409591#audit-record-types-2
- https://access.redhat.com/documentation/en-us/red_hat_enterprise_linux/7/html/security_guide/sec-defining_audit_rules_and_controls
- https://static.open-scap.org/ssg-guides/ssg-rhel7-guide-C2S.html#xccdf_org.ssgproject.content_group_auditing
- https://static.open-scap.org/ssg-guides/ssg-centos8-guide-index.html
- https://static.open-scap.org/ssg-guides/ssg-rhel9-guide-index.html
- https://static.open-scap.org/ssg-guides/ssg-sle15-guide-index.html
- https://github.com/linux-audit/audit-userspace/blob/master/rules/30-pci-dss-v31.rules
- https://github.com/alphagov/puppet-Audit/pull/1
- https://github.com/Neo23x0/auditd
- https://unix.stackexchange.com/questions/102926/how-to-interpret-the-saddr-field-of-an-audit-log