auditd

:

- Astra Linux Special Edition .10015-01 (1.7), .10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

auditd audispd-plugins.
Astra Linux Common Edition , Astra Linux Special Edition . (. synaptic)

```
sudo apt update
sudo apt -y install auditd audispd-plugins
```

kill exit_group

, , /etc/audit/audit.rules
() auditd /etc/audit/audit.d/*.rules

auditctl ( )

auditctl, :

```
auditctl -a exit,always -F arch=b64 -S kill -k kill_process
auditctl -a exit,always -F arch=b64 -S exit_group -k kill_process
```

:
-a exit,always , **exit, always** (always never,)
5 :

- task — , ;
- entry — , ;
- exit — , ;
- user — , ;
- exclude — .

-F arch=b64 , . ;

-S kill , **kill;**

-k kill_process () ;

auditctl , .

/etc/audit/rules.d/audit.rules

/etc/audit/rules.d/audit.rules , **auditctl**, :

```
-a exit,always -F arch=b64 -S kill -k kill_process
-a exit,always -F arch=b64 -S exit_group -k kill_process
```

:

sudo systemctl restart auditd

```
ausearch -k kill_process
```

/var/log/audit/audit.log