

5. Подготовка Linux-хоста

Агент **ничего не меняет в настройках аудита хоста**. Он читает то, что пишет система, и проверяет настройки. Чтобы события собирались полностью, а проверки отражали реальное состояние, хост готовят заранее: вручную по этому разделу, скриптом `prepare-host.sh` или ролью Ansible с `gits_agent_prepare_host=true`.

1. Что читает агент

Источник	Откуда	Что нужно на хосте
auditd	<code>/var/log/audit/audit.log</code>	auditd включён, <code>log_format = RAW</code> . Записи PAM и shadow-utils (входы, операции с учётными записями) пишутся без дополнительных правил. SYSCALL-записи агент передаёт только с ключами <code>exec</code> , <code>identity</code> , <code>sudoers</code> , <code>sshd</code> , <code>pam</code> , <code>audit_rules_logs</code> , <code>szi</code>
journald	<code>journalctl -o json -f</code>	фильтр по <code>sshd</code> , <code>sudo</code> , <code>su</code> , <code>login</code> , <code>systemd</code> , ядру. Постоянное хранение журнала, иначе после перезагрузки теряется позиция чтения
astra	<code>/parsec/log/astra/events</code> (только Astra Linux)	syslog-ng с модулем <code>syslog-ng-mod-astra</code> , включённые события PARSEC (<code>astra-admin-events</code>)

2. Быстрая подготовка: prepare-host.sh

Скрипт находится в `deploy/host-prep/linux/` внутри `gits-deploy_<ver>.zip`. Копируйте каталог целиком: рядом со скриптом лежат правила аудита.

```
sudo ./prepare-host.sh --check      # только отчёт; код возврата 1 – есть несоответствия
sudo ./prepare-host.sh              # применить
```

Параметр	Действие
<code>--check</code>	ничего не менять
<code>--no-packages</code>	не устанавливать auditd, если его нет
<code>--no-noise</code>	не ставить правила подавления шума
<code>--astra-quiet</code>	Astra: выключить шумные события PARSEC (запуск процессов, сеть, открытие файлов)
<code>--szi <каталог></code>	контролировать изменения конфигурации СЗИ (ключ <code>szi</code>); можно указать несколько раз

Что делает скрипт (подробности — §3–§7):

- Устанавливает auditd, если его нет.
- В `auditd.conf` задаёт `log_format = RAW`, `max_log_file ≥ 32`, `num_logs ≥ 10`, `max_log_file_action = ROTATE`. Исходный файл сохраняется как `auditd.conf.gits.bak`.
- Кладёт правила `30-gits.rules` и `31-gits-noise.rules` в `/etc/audit/rules.d/` и загружает их (`augenrules --load`).
- Включает и запускает auditd, выставляет права 0750 root на `/var/log/audit`.
- Включает постоянное хранение журнала journald.
- На Astra включает обязательные события PARSEC.

7. Проверяет, что работает служба времени.

Скрипт идемпотентен: повторный запуск ничего не меняет. Отчёт:

```
== Правила аудита (/etc/audit/rules.d)
[ FIX] 30-gits.rules установлен
[ FIX] правила загружены (augenrules --load)
[ OK ] загружено: -w /etc/passwd -p wa
...
== Синхронизация времени
[ FAIL] нет активной службы времени (chrony/ntp/systemd-timesyncd)

Изменений: 9. Несовпадений: 1.
```

Синхронизацию времени скрипт только проверяет: источники времени зависят от сети организации (§7).

3. auditd

Установка: `apt install auditd` (Debian, Astra) или `dnf install audit` (RHEL-совместимые).

`/etc/audit/auditd.conf`, значимые параметры:

```
log_format = RAW                # агент разбирает RAW; ENRICHED не использовать
max_log_file = 32                # МБ; проверка CHK-MAS-013b требует не меньше 8
num_logs = 10                   # CHK-MAS-013b: не меньше 5
max_log_file_action = ROTATE
space_left = 500
space_left_action = SYSLOG
admin_space_left = 100
admin_space_left_action = SUSPEND
disk_full_action = SUSPEND
disk_error_action = SUSPEND
```

auditd запрещает `systemctl restart`. Чтобы применить `auditd.conf`, выполните `service auditd reload`.

Каталог журналов: `chown root /var/log/audit && chmod 0750 /var/log/audit` (CHK-MAS-014b).

4. Правила аудита

`/etc/audit/rules.d/30-gits.rules` — обязательные правила (CHK-MAS-010b):

```

-w /etc/audit/          -p wa -k audit_rules
-w /var/log/audit/      -p wa -k logs
-w /etc/passwd          -p wa -k identity
-w /etc/shadow          -p wa -k identity
-w /etc/group           -p wa -k identity
-w /etc/gshadow         -p wa -k identity
-w /etc/sudoers         -p wa -k sudoers
-w /etc/sudoers.d/      -p wa -k sudoers
-w /etc/ssh/sshd_config -p wa -k sshd
-w /etc/pam.d/          -p wa -k pam
-a always,exit -F arch=b64 -S execve -F euid=0 -F auid!=unset -k exec
-a always,exit -F arch=b32 -S execve -F euid=0 -F auid!=unset -k exec

```

Ключ	Событие СКР
identity	integrity/file_modified — изменение базы учётных записей
sudoers, sshd, pam	policy/security_setting_changed
audit_rules	policy/audit_policy_changed
logs	integrity/log_tampered
exec	process/created — команды, запущенные людьми от root
szl	изменение конфигурации СЗИ: -w /etc/<сзи> -p wa -k szl

Имена ключей менять нельзя: записи с другими ключами агент отбрасывает. Правило `exec` ограничено действиями людей (`auid>=1000`) под root. Без этого ограничения основной поток событий дадут демоны и cron.

`/etc/audit/rules.d/31-gits-noise.rules` — подавление шума. Правила необязательные: на полноту контроля они не влияют, старт и остановку служб агент берёт из journald.

```

-a always,exclude -F msgtype=SERVICE_START
-a always,exclude -F msgtype=SERVICE_STOP
-a always,exclude -F msgtype=1334
#-a always,exclude -F exe=/usr/sbin/cron      # только auditd ≥ 3.0

```

Загрузка и проверка:

```

augenrules --check && augenrules --load
auditctl -l | grep -E 'key=|-k '
auditctl -s | head -3          # enabled 1

```

- **auditd 2.8** (Astra 1.7, Debian 10) не принимает поле `exe` в правилах `exclude`. Строка с `exe` прерывает `augenrules --load`, и следующие за ней правила не загружаются. Поэтому правило для cron закомментировано.
- Не добавляйте `-e 2` (запрет изменения правил до перезагрузки) на Astra: он ломает `astra-admin-events` и проверку CHK-MAS-010с. На других системах с `-e 2` новые правила применяются только после перезагрузки.
- Файлы правил не содержат `-D`, `-b` и `-f`: эти параметры задаёт базовый `audit.rules` дистрибутива.

5. journald

/etc/systemd/journald.conf.d/50-gits.conf:

```
[Journal]
Storage=persistent      # на Astra по умолчанию журнал в памяти
SystemMaxUse=512M
RateLimitIntervalSec=30s
RateLimitBurst=10000    # не терять строки sshd при переборе паролей
```

```
mkdir -p /var/log/journal && systemd-tmpfiles --create --prefix /var/log/journal
systemctl restart systemd-journald && journalctl --flush
```

Проверка CHK-MAS-013b читает Storage из основного /etc/systemd/journald.conf: там не должно быть Storage=volatile или Storage=none.

6. Astra Linux: события PARSEC

Нужны пакеты parsec-base (утилита astra-admin-events), syslog-ng-core и syslog-ng-mod-astra. syslog-ng не отключайте: он пишет журнал /parsec/log/astra/events, который читает агент. Файлы mod-astra*.conf, 10-parsec.rules и astra-syslog.rules принадлежат пакетам, руками их не правьте: состав событий меняется только через astra-admin-events.

Проверка CHK-MAS-010с требует включить 25 событий:

```
astra-admin-events -E succeeded-authorization failed-authorization user-session add-rule remove-rule \
  creating-account deleting-account changing-account-password changing-primary-group changing-uid \
  adding-user-to-group removing-user-from-group creating-group removing-group modifying-group-members \
  audit-log-removed events-log-removed daemon-start daemon-end syslog-ng-stop package-installed \
  new-usb-device usb-mass-storage-detected unsigned-binary-file modifying-file -e
astra-admin-events | grep -E ' 1 '
```

Рекомендуемый для СКР состав шире: всё, что классифицирует агент, плюс значимые события вне его таксономии. prepare-host.sh включает этот состав, а с параметром --astra-quiet выключает шумные события:

```
# Включить
astra-admin-events -G authorization user-accounting user-groups audit security-logs \
  safepolicy general-software system-time system-operation -e
astra-admin-events -E previous-login user-blocked-by-tally modifying-directory package-not-installed \
  package-removing-started usb-disconnect device-mount device-unmount \
  device-mount-attempt-blocked process-ends-abnormally \
  self-diagnostics-critical self-diagnostics-error -e

# Шум (--astra-quiet): запуск процессов, сеть, открытие и удаление файлов
astra-admin-events -G network network-addressing resources access-rights -d
astra-admin-events -E execute-process execute-sudo-process process-ends kernel-module file-opened file-re
moval \
  package-installation-started package-upgrade-started process-out-of-ram \
  self-diagnostics-started self-diagnostics-completed self-diagnostics-warning -d
```

События печати (группа `printing`) оставьте включёнными, если нужен контроль печати (ПУИ.30).

Правила `parsec` на Astra не содержат наблюдения за `/etc/passwd`, `/etc/sudoers` и т. п., поэтому правила `30-gits.rules` на Astra нужны так же, как на других системах. Они дополняют правила `parsec` и не мешают им.

PostgreSQL на Astra пишет мандатный аудит (`USER_AVC`) в `audit.log`. Это даёт большой объём записей, до 40 МБ за 8 часов. Если аудит СУБД ведётся её собственными средствами, раскомментируйте последнее правило в `31-gits-noise.rules`, указав путь к `postgres` своей версии.

7. Время

Нужна служба синхронизации времени с внутренними источниками или с контроллером домена (01 §1.4).

```
# chrony (Debian, RHEL): в /etc/chrony/chrony.conf или /etc/chrony.conf – server ntp1.bank.local iburst
systemctl enable --now chrony          # RHEL: chronyd
# ntp (Astra 1.7):          в /etc/ntp.conf – server ntp1.bank.local iburst
systemctl enable --now ntp
timedatectl                            # System clock synchronized: yes
```

8. Прочее

- **sshd**. Проверки SSH (CHK-RD-030b, 036, 037b) читают эффективную конфигурацию `sshd -T`. На хостах без `openssh-server` они вернут `error`.
- **mokutil**. Проверка Secure Boot (CHK-CZI-025b) использует `mokutil --sb-state`.
- **Антивирус**. Добавьте в исключения `/usr/local/bin/gits-agent` (или `/usr/bin/gits-agent`) и `/var/lib/gits-agent`.

9. Проверки агента и настройки хоста

Проверка	Что должно быть на хосте	Где настроить
CHK-MAS-010b	<code>auditd</code> активен и в автозапуске; наблюдение <code>-p wa</code> за <code>/etc/passwd</code> , <code>/etc/shadow</code> , <code>/etc/group</code> , <code>/etc/sudoers</code> , <code>/var/log/audit</code> , <code>/etc/audit</code> , <code>/etc/ssh/ssh_config</code> , <code>/etc/pam.d</code> ; правило <code>execve</code>	§3, §4
CHK-MAS-010c (Astra)	25 событий PARSEC включены	§6
CHK-MAS-013b	<code>max_log_file ≥ 8</code> , <code>num_logs ≥ 5</code> , <code>max_log_file_action = rotate</code> ; <code>journald</code> не <code>volatile</code>	§3, §5
CHK-MAS-014b	<code>/var/log/audit</code> — владелец <code>root</code> , права 0700, 0740 или 0750	§3
CHK-RD-017b	<code>/etc/shadow</code> , <code>/etc/gshadow</code> — 0000/0600/0640; в <code>/etc/passwd</code> только <code>x</code> ; <code>ENCRYPY METHOD SHA512</code> или <code>YESCRYPT</code> в <code>login.defs</code>	политика ОС
CHK-RD-019	<code>PASS_MAX_DAYS ≤ 365</code> в <code>/etc/login.defs</code>	политика ОС
CHK-RD-021	<code>minlen ≥ 8</code> в <code>pwquality.conf</code> или в параметрах <code>pam_pwquality</code> . На Astra сложность пароля настраивается другим механизмом, и проверка может показать <code>fail</code> при корректной настройке	политика ОС
CHK-RD-023	<code>minclass ≥ 3</code> или <code>ucredit/lcredit/dcredit ≤ -1</code>	политика ОС
CHK-RD-030b, 036, 037b	<code>PermitEmptyPasswords no</code> , <code>PrintLastLog yes</code> , задан <code>Banner</code> , <code>PermitRootLog in no</code> или <code>prohibit-password</code>	<code>sshd_config</code>

Проверка	Что должно быть на хосте	Где настроить
CHK-UZP-010c	нет <code>NOPASSWD: ALL</code> в <code>/etc/sudoers*</code>	<code>sudoers</code>
CHK-RD-033	нет файлов с записью для всех в <code>/etc</code> , <code>/usr</code> , <code>/opt</code>	права файлов
CHK-PUI-018b	<code>install usb-storage /bin/false</code> или <code>blacklist usb-storage</code> в <code>/etc/modprobe.d/</code>	политика ОС
CHK-CZI-025b	Secure Boot включён	UEFI
CHK-ZVK-001L, CHK-ZVK-009	активна и в автозапуске служба антивируса: <code>kes1</code> , <code>drweb-configd</code> или <code>clamav-daemon</code>	AB
CHK-CZI-018, CHK-CZI-024	утверждённый эталон пакетов и целостности конфигурации	консоль, карточка хоста
CHK-MAS-021	буфер агента заполнен меньше чем на 80 %, доставка работает	связь с сервером

10. Самопроверка

```

sudo ./prepare-host.sh --check
systemctl is-active auditd systemd-journald gits-agent
auditctl -l | grep -c -- '-k \key='
# Сгенерировать события и найти их в консоли («События», роль auditor)
sudo id; sudo touch /etc/passwd
ssh nosuchuser@localhost                # неуспешный вход

```

На стенде после подготовки хоста Astra Linux 1.7.6 в консоль пришли события `process/created` (ключ `exec`), `integrity/file_modified` (`identity`), `policy/audit_policy_changed` (`audit_rules`), а также события входа из `journald`, `auditd` и `PARSEC`. Проверка CHK-MAS-010b сменила результат с `fail` на `pass`.