

7. Диагностика

Журналы компонентов:

Компонент	Журнал
Сервер, ядро, консоль	<code>journalctl -u gits-server (gits-core, gits-console)</code>
Ретранслятор	<code>journalctl -u gits-relay</code>
Агент Linux	<code>journalctl -u gits-agent</code>
Агент Windows	журнал «Приложение», источник <code>gits-agent</code> ; <code>sc query gits-agent</code>

Сервер

Симптом	Причина и решение
<code>run gitsctl init-ca? / run gitsctl gen-signing-keys?</code> при запуске	нет УЦ или ключей в <code>data_dir</code> : выполните 02 §5 или восстановите <code>/var/lib/gits</code> из копии
<code>... is accessible by group/others (mode ...); expected 0600</code>	у файла ключа слишком широкие права: <code>chmod 0600</code> и владелец <code>gits</code> . Обычно так бывает после копирования или запуска <code>gitsctl</code> не от <code>gits</code>
<code>error obtaining MAC configuration for user "gits" (Astra)</code>	нет мандатной метки у пользователя БД: <code>pdpl-user -l 0:0 gits</code>
<code>failed to connect to user=gits database=gits</code>	неверный <code>db_dsn / GITS_DB_DSN</code> , СУБД не запущена или подключение запрещено в <code>pg_hba.conf</code>
консоль не стартует, в журнале ожидание схемы	консоль не применяет миграции: сначала запустите ядро или выполните <code>gits-server migrate</code>
<code>bind: permission denied</code> на порту 443	служба запущена не из штатного юнита (нет <code>CAP_NET_BIND_SERVICE</code>) или порт занят
консоль открывается, но в журнале действий у всех один адрес	консоль работает за обратным прокси (02 §6)
<code>permission denied</code> в <code>gitsctl load-measures</code>	CSV-файл недоступен пользователю <code>gits</code> : скопируйте его в <code>/tmp</code> с правами 0644

Регистрация и подключение агента

Симптом	Причина и решение
<code>x509: certificate is valid for ..., not ...</code>	агент обращается по адресу, которого нет в сертификате шлюза или ретранслятора. Выпустите сертификат с этим адресом (<code>issue-server-cert -dns ... -ip ..., dns_names / ip_addresses</code> ретранслятора) или задайте <code>server_name</code> в <code>agent.yaml</code>
<code>certificate signed by unknown authority</code>	в <code>ca_file / ca_cert</code> не тот корень: возьмите <code>/var/lib/gits/ca/ca.crt</code> с узла ядра
<code>certificate has expired or is not yet valid</code>	часы хоста расходятся с сервером больше чем на 5 минут. Синхронизируйте время (01 §1.4). На виртуальных машинах после паузы или восстановления из снимка часы гостя могут отставать на дни, пока не включена синхронизация с гипервизором

Симптом	Причина и решение
токен отклонён	срок токена истёк или исчерпан лимит установок: выпустите новый. Лимит регистраций с одного адреса — <code>gateway.enroll_per_minute</code>
<code>connection refused</code> / тайм-аут	шлюз слушает <code>127.0.0.1</code> (задайте <code>gateway.listen: 0.0.0.0:8443</code>) или порт закрыт межсетевым экраном
агент долго не переподключается после перезапуска сервера	повтор подключения растягивается до 5 минут, это штатное поведение. Для ускорения перезапустите службу агента
хост зарегистрировался как новый, в консоли предупреждение о клоне	ВМ клонирована вместе с каталогом состояния агента. Решение принимает оператор: карточка хоста → «Экземпляры агента»
пакет <code>deb/rpm</code> установлен, служба не запускается	агент не зарегистрирован: <code>gits-agent enroll ...</code> , затем <code>systemctl enable --now gits-agent</code>

Команды и действия реагирования

Симптом	Причина и решение
<code>command issued in the future</code> / команда просрочена	расхождение часов агента и сервера больше 5 минут
блокировка локальной учётной записи Linux завершается ошибкой записи в <code>/etc/shadow</code>	агент установлен с юнитом старой версии, где был <code>ProtectSystem=full</code> . Выполните <code>gits-agent install</code> новой версии (юнит перезапишется) или удалите строки <code>ProtectSystem/ReadWritePaths</code> из юнита и выполните <code>systemctl daemon-reload && systemctl restart gits-agent</code>

Проверки и события

Симптом	Причина и решение
проверки дают <code>error</code> на Windows	агент запущен не от <code>LocalSystem</code> или не работает WMI/EventLog
CHK-MAS-010a fail при настроенной политике	проверьте <code>auditpol /get /category:*</code> и значение <code>SCENoApplyLegacyAuditPolicy</code> . Доменная GPO могла перезаписать локальные настройки. Старые версии агента на русской Windows неверно разбирали подкатегорию «Использование прав, затрагивающее конфиденциальные данные». Обновите агента
CHK-MAS-009a fail на русской Windows при исправном времени	старые версии каталога читали подпись <code>Source:</code> из <code>w32tm /query /status</code> . Обновите сервер: каталог доставляется агентам автоматически
CHK-MAS-010b fail на Astra	правил <code>parsecs</code> недостаточно: установите <code>30-gits.rules</code> (05 §4)
<code>augenrules --load</code> завершился ошибкой, часть правил не загружена	в правилах есть конструкция, которую не поддерживает <code>auditd</code> , например <code>exclude -F exe=</code> на <code>auditd 2.8</code> . Проверьте построчно: <code>auditctl <строка правила></code>
нет событий <code>auditd</code>	<code>log_format</code> не RAW, либо ключи правил не из списка (05 §1)
после перезагрузки Linux-хоста пропали события	<code>journald</code> хранит журнал в памяти: включите постоянное хранение (05 §5)
нет событий 4688, 4728 и др.	подкатегория аудита не включена (06 §2)
проверка CHK-MAS-021 fail	буфер агента заполняется: нет связи с сервером или мал диск. Проверьте подключение и место в каталоге состояния агента

Push-установка

Симптом	Причина и решение
WinRM: 401	NTLM отклонён: проверьте учётную запись, LocalAccountTokenFilterPolicy для локальных администраторов и политику NTLM домена. Альтернативы — порт 5986 (HTTPS, Basic) или установочный комплект через GPO
SSH: sudo: sorry, you must have a tty	в sudoers включён requiretty: отключите его для учётной записи установки
задание «зависло»	задание, которое выполняется дольше 30 минут, завершается с ошибкой. Проверьте связь исполнителя с хостом