

1. Требования

1.1 Сервер

Параметр	Требование
ОС	Linux x86-64 с systemd. Проверено на Astra Linux SE 1.7.6. Исполняемые файлы статические и не зависят от системных библиотек
СУБД	PostgreSQL 16 (эталонная версия, на ней идут тесты CI). Установка проверена и на PostgreSQL 11 из состава Astra Linux 1.7. Расширения не нужны
ЦП, ОЗУ, диск	Для пилота на 50–100 хостов: 4 vCPU, 8 ГБ ОЗУ, 100 ГБ под БД; сервер и СУБД на одном узле. Ориентир по design/02 §6 для 1 000 хостов: 15–20 млн событий в сутки, БД 200–500 ГБ. Объем зависит от настройки аудита и уточняется по итогам пилота
Резервные копии	отдельный том или хранилище (§ 02 §11)
Размещение	сегмент управления, доступ из пользовательских сетей закрыт (design/02 §4)

Сервер можно запустить и на Windows Server: сборки *_windows_amd64.exe есть. Режимы службы Windows у сервера нет, эталонная установка — Linux (02 §13).

1.2 Контролируемые хосты

ОС	Агент	Примечание
Windows 10 / Server 2016 и новее (x64)	gits-agent_<ver>_windows_amd64.exe	служба gits-agent, LocalSystem; проверено на Windows 10 LTSC 2021
Windows Server 2008 R2 – 2012 R2	gits-agent-legacy_<ver>_windows_amd64.exe	сборка на Go 1.20
Astra Linux SE 1.7+	deb или исполняемый файл	проверено на 1.7.6; дополнительный источник событий — журнал PARSEC
Другие Linux с glibc и systemd	deb, rpm или исполняемый файл	amd64 и arm64

Агент работает от **root** (Linux) или **LocalSystem** (Windows). Без этих прав проверки secedit и auditpol, а также чтение журнала Security завершаются ошибкой.

Целевое потребление ресурсов (design/05 §7): в среднем не больше 1 % ЦП, не больше 150 МБ ОЗУ на APM и 300 МБ на серверах. Агент работает с пониженным приоритетом процесса и ввода-вывода. Дискový буфер событий занимает до 512 МБ: /var/lib/gits-agent/buffer или %ProgramData%\GITS\agent\buffer.

Каталоги агента нужно добавить в исключения антивируса: исполняемый файл и каталог состояния с буфером (пути — в 04 §1). Агент не делает этого сам.

Требования к настройке ОС хоста (аудит, журналы, время) — в 05 и 06.

1.3 Сетевые взаимодействия

Все соединения агента **исходящие**: входящих портов на хостах агент не открывает.

Откуда	Куда	Порт	Протокол	Назначение
Хосты (агенты)	ядро или ретранслятор	TCP 8443	gRPC, TLS 1.2+, mTLS	регистрация, конфигурация, результаты, события, команды
Ретранслятор	ядро	TCP 8443	gRPC, mTLS	трафик агентов сегмента
АРМ администраторов	консоль	TCP 443	HTTPS	веб-консоль и REST API
Ядро, консоль	PostgreSQL	TCP 5432	PostgreSQL (TLS по возможности)	общая БД
Сетевое оборудование, СКУД и др.	ядро	UDP 5514	syslog	необязательно: приём внешних событий
Ядро	SIEM	TCP/UDP 514	CEF / JSON	необязательно: пересылка событий
Ядро	каталог (AD, ALD Pro)	TCP 636	LDAPS	необязательно: сверка учётных записей
Ядро	SMTP	TCP 25/587	SMTP	необязательно: уведомления
Ядро или ретранслятор	хосты	TCP 22 / 5985 / 5986	SSH / WinRM	только на время push-установки агента

Порт шлюза задаётся параметром `gateway.listen`. По умолчанию используется 8443. Можно назначить 443, если политика сети разрешает только его. Адрес, по которому агенты обращаются к ядру или ретранслятору, должен присутствовать в сертификате шлюза как имя DNS или IP-адрес (02 §5).

1.4 Время

Часы сервера, ретрансляторов и хостов должны синхронизироваться с доверенным источником: в домене — с контроллером домена, вне домена — с внутренними серверами NTP.

- Сертификаты выдаются с началом действия «сейчас – 5 минут». Хост, часы которого отстают больше чем на 5 минут, не примет сертификат («certificate not yet valid»).
- Команды с сервера отклоняются, если время выдачи опережает часы агента больше чем на 5 минут («command issued in the future»).
- Проверка CHK-MAS-009a (Windows) требует, чтобы расхождение часов агента и сервера было не больше 5 секунд.

1.5 Учётные записи

Учётная запись	Где	Назначение
<code>gits</code> (системная, без входа)	сервер	служба ядра и консоли, владелец <code>/var/lib/gits</code>
роль <code>gits</code> в PostgreSQL	СУБД	владелец схемы СКР
<code>gits-relay</code> (системная)	ретранслятор	создаётся пакетом
администратор консоли (<code>system_admin</code>)	СКР	первый пользователь, создаётся <code>gitsctl create-user</code>
второй администратор	СКР	утверждение раскатки обновлений и опасных действий («две руки»)
сервисная учётная запись LDAP (только чтение)	каталог	сверка учётных записей, если используется

Учётная запись	Где	Назначение
учётная запись для push-установки	хосты	SSH с sudo или локальный администратор Windows; вводится на одно задание и затем стирается

Пароли пользователей консоли должны быть не короче 16 символов.