

4. Установка агента

Перед установкой подготовьте хост (05 — Linux, 06 — Windows). Агент заработает и без подготовки, но часть проверок покажет несоответствие, а часть событий не будет собираться.

Способы установки:

Способ	Когда использовать
Установочный комплект из консоли	основной: вручную, через GPO/SCCM, Ansible, ALD Pro
<code>gits-agent install</code> вручную	единичные хосты, свои сценарии развёртывания
Пакет deb/rpm	Linux-хосты, управляемые через репозитории пакетов
Роль Ansible	массовая установка на Linux
Push-установка из консоли	нет своих средств развёртывания; SSH или WinRM до хостов

Все способы идемпотентны: повторный запуск не перерегистрирует уже зарегистрированный агент.

1. Раскладка файлов

	Linux (<code>gits-agent install</code> , комплект, Ansible)	Linux (пакет deb/rpm)	Windows
Исполняемый файл	<code>/usr/local/bin/gits-agent</code>	<code>/usr/bin/gits-agent</code>	<code>%ProgramFiles%\GITS Agent\gits-agent.exe</code>
Конфигурация	<code>/etc/gits-agent/agent.yaml</code> (0600)	<code>/etc/gits-agent/agent.yaml</code>	<code>%ProgramFiles%\GITS Agent\agent.yaml</code>
Состояние, буфер	<code>/var/lib/gits-agent</code> (0700)	<code>/var/lib/gits-agent</code>	<code>%ProgramData%\GITS\agent</code>
Служба	<code>gits-agent.service</code> в <code>/etc/systemd/system</code>	<code>gits-agent.service</code> в <code>/lib/systemd/system</code>	служба <code>gits-agent</code> , LocalSystem, автозапуск

На Windows доступ к каталогам агента есть только у SYSTEM и группы «Администраторы» (наследование отключено). В каталоге состояния хранятся сертификат и ключ агента, кэш подписанной конфигурации, буфер событий и журнал выполненных команд.

2. Перед установкой

1. **Пакет агента опубликован** на сервере (02 §10). Иначе установочный комплект не соберётся.
2. **Адреса подключения** заданы в карточке ИС или в `gateway.agent_endpoints`. Адреса должны быть в сертификате шлюза или ретранслятора.
3. **Токен регистрации.** Токен ограничен по сроку действия (от 1 до 72 часов) и по числу установок. Выдаётся в консоли («Агенты и токены» → «Выдать токен регистрации») или командой `gctl create-token -uses 50 -ttl 72h`. Токен — секрет: с ним любой хост может зарегистрироваться в СКР.
4. **Доступ к серверу:** хост → ядро или ретранслятор по TCP 8443, часы синхронизированы.

3. Установочный комплект из консоли

Консоль: «Агенты и токены» → «Установочный пакет агента». Укажите ОС, архитектуру, ИС (хост сразу попадёт в неё), адреса подключения (если не заданы в ИС), число установок и срок токена. Консоль выпустит токен и соберёт архив:

ОС	Архив	Состав
Linux	<code>gits-agent-<ver>-linux-<arch>.tar.gz</code>	<code>gits-agent</code> , <code>agent.yaml</code> , <code>install.sh</code> , <code>README.txt</code>
Windows	<code>gits-agent-<ver>-windows-<arch>.zip</code>	<code>gits-agent.exe</code> , <code>agent.yaml</code> , <code>install.cmd</code> , <code>README.txt</code>

В `agent.yaml` уже записаны адреса подключения, корневой сертификат СКР и токен. **Храните архив как секрет** и удалите его после истечения срока токена.

Linux:

```
tar xzf gits-agent-<ver>-linux-amd64.tar.gz
sudo ./gits-agent-install/install.sh
```

Windows (от имени администратора):

```
install.cmd
```

GPO. Распакуйте архив в сетевую папку, доступную на чтение учётным записям компьютеров, и назначьте `install.cmd` сценарием автозагрузки компьютера: «Конфигурация компьютера» → «Политики» → «Конфигурация Windows» → «Сценарии» → «Автозагрузка». Число установок в токене должно быть не меньше числа компьютеров, а срок токена — достаточным для перезагрузки всех машин. После регистрации последующие запуски ничего не меняют, а при замене исполняемого файла служба перезапускается.

Результат установки выводится в JSON:

```
{ "enrolled": true, "binary_new": true, "service_new": true, "host_id": "01a0...", "service": "gits-agent.s
ervice" }
```

4. Вручную: gits-agent install

Нужны исполняемый файл агента из релиза, корневой сертификат СКР (`/var/lib/gits/ca/ca.crt` с узла ядра) и токен.

`agent.yaml`:

```
servers:                # ядро и/или ретрансляторы; выбирается случайный, при сбое — следующий
  - gits.bank.local:8443
ca_file: /root/gits-install/ca.pem  # или ca.pem: | ... (PEM прямо в файле)
log_level: info
# server_name: gits.bank.local # если имя в сертификате отличается от адреса
```

```
sudo ./gits-agent install -config agent.yaml -token '<токен>'
```

Команда копирует агента в штатный каталог (`$1`) и пишет итоговый `agent.yaml` с корневым сертификатом внутри. Токен в файл не записывается. Затем команда регистрирует агента, создаёт и запускает службу. На Windows команда выполняется так же, из командной строки администратора: `gits-agent.exe install -config agent.yaml -token <токен>`.

5. Пакет deb/rpm

```
apt install ./gits-agent_<ver>-1_amd64.deb          # или dnf install ./gits-agent-<ver>-1.x86_64.rpm
cp ca.crt /etc/gits-agent/ca.pem
cat > /etc/gits-agent/agent.yaml <<'EOF'
servers: ["gits.bank.local:8443"]
ca_file: /etc/gits-agent/ca.pem
state_dir: /var/lib/gits-agent
log_level: info
EOF
chmod 0600 /etc/gits-agent/agent.yaml
gits-agent enroll -config /etc/gits-agent/agent.yaml -token '<токен>'
systemctl enable --now gits-agent
```

Пакет включает службу автоматически, только когда агент уже зарегистрирован. Иначе после установки он печатает эти шаги. Подключить репозитории пакетов Gitea: README, раздел «CI и релизы».

6. Ansible

Роль `deploy/ansible/roles/gits-agent` (в `gits-deploy_<ver>.zip`) устанавливает агента на Linux-хосты.

```
# из установочного комплекта консоли
ansible-playbook -i inventory -b deploy/ansible/install-agent.yml \
  -e gits_agent_bundle=files/gits-agent-<ver>-linux-amd64.tar.gz \
  -e gits_agent_prepare_host=true
```

Переменная	Назначение
<code>gits_agent_bundle</code>	архив из консоли (вариант 1)
<code>gits_agent_binary</code> , <code>gits_agent_endpoints</code> , <code>gits_agent_ca_pem</code> , <code>gits_agent_enroll_token</code>	отдельные параметры (вариант 2); токен — через <code>ansible-vault</code>
<code>gits_agent_prepare_host</code>	<code>true</code> — перед установкой выполнить <code>prepare-host.sh (05)</code>
<code>gits_agent_prepare_host_args</code>	параметры <code>prepare-host.sh</code> , например <code>--astra-quiet --szi /etc/kesl</code>
<code>gits_agent_prepare_host_strict</code>	<code>true</code> — остановить установку, если после настройки остались несоответствия

Рабочий каталог с токеном удаляется в конце роли.

7. Push-установка из консоли

Консоль: «Агенты и токены» → «Push-установка агента». Укажите ОС, исполнителя (ядро или ретранслятор сегмента), ИС, адреса хостов, учётную запись, пароль и порт. Исполнитель подключается к хостам, копирует установочный комплект и запускает установку. Одновременно обрабатываются 4 хоста. Задание, которое выполняется дольше 30 минут, завершается с ошибкой. Учётные данные шифруются ключом исполнителя и стираются после завершения задания.

Требования к целевым хостам:

	Linux (SSH)	Windows (WinRM)
Порт	TCP 22 от исполнителя	TCP 5985 (HTTP, NTLM с шифрованием сообщений) или 5986 (HTTPS, Basic)
Учётная запись	root или пользователь с sudo на любые команды; вход по паролю или ключу	локальный или доменный администратор
Настройка	для sudo не должен требоваться tty (Defaults requiretty выключен); SFTP не нужен	WinRM включён: <code>prepare-host.ps1 -EnableWinRM</code> или <code>Enable-PSRemoting</code> (06 §6)

Ключ SSH-хоста не проверяется, а только записывается в журнал задания. Сертификат WinRM на порту 5986 тоже не проверяется. Поэтому запускайте push-установку только в доверенном сегменте. Push-установка по WinRM на стенде разработчика вживую не подтверждена: стендовые Windows-хосты отклоняли NTLM. Сначала проверьте её на пилотной группе.

8. Проверка после установки

На хосте:

```
systemctl status gits-agent
journalctl -u gits-agent -n 30 -o cat      # нет ошибок TLS и подключения
```

```
sc query gits-agent
```

В консоли:

1. «Хосты»: хост появился со статусом online, ОС и инвентарь заполнены.
2. Карточка хоста → «Проверки»: результаты появляются в течение минуты. Результат `error` обычно означает, что агенту не хватает прав или на хосте нет нужной утилиты.
3. «События» (пользователь с ролью `auditor` или `analyst`): от хоста приходят события, например вход по SSH или RDP.
4. Проверка CHK-MAS-021 («Исправность конвейера сбора событий») — pass.

9. Обновление

Агенты обновляются централизованно: пакеты публикуются (`gctl publish-agent` или «Обновления агентов»), затем раскатка идёт волнами. Раскатку утверждает второй администратор. Если новая версия не вышла на связь за 2 минуты, агент сам откатывается. Агент, установленный из deb/rpm, обновляется пакетом того же формата, остальные — исполняемым файлом (`bin / exe`).

Повторный запуск установочного комплекта с новым исполняемым файлом тоже обновляет агента: файл заменяется, служба перезапускается.

10. Удаление

Сначала отзовите агента в консоли («Агенты и токены» → «Агенты и сертификаты»), затем удалите его с хоста.

Linux (установка `gits-agent install`):

```
systemctl disable --now gits-agent  
rm -f /etc/systemd/system/gits-agent.service /usr/local/bin/gits-agent && systemctl daemon-reload  
rm -rf /etc/gits-agent /var/lib/gits-agent
```

Linux (пакет): `apt remove gits-agent / dnf remove gits-agent`, затем `rm -rf /var/lib/gits-agent`.

Windows (от имени администратора):

```
"%ProgramFiles%\GITS Agent\gits-agent.exe" service stop  
"%ProgramFiles%\GITS Agent\gits-agent.exe" service uninstall  
rmdir /s /q "%ProgramFiles%\GITS Agent" "%ProgramData%\GITS\agent"
```

11. Windows Server 2008 R2 – 2012 R2

Используйте `gits-agent-legacy_<ver>_windows_amd64.exe`: переименуйте его в `gits-agent.exe` и установите способом из §4 или установочным комплектом (в комплекте замените `gits-agent.exe`). Каталог проверок рассчитан на Windows 10 / Server 2016. Проверки компонентов, которых нет в старых ОС (например, Microsoft Defender), на таких хостах завершатся с результатом `error` или `fail`: оценивайте их вручную.