



Census

Доступ на Linux-парке — декларативно, как код

Census приводит устройства к одной подписанной декларации: ролевые учётки, группы, sudoers, systemd-лимиты. Показывает дифф до применения, находит и устраняет расхождения, ничего не ломает.

Декларация

что должно быть на устройстве
— описано файлами и
подписано, а не накоплено
руками

Идемпотентно

повторный прогон не меняет
корректное; чужие учётки и
группы не трогаются

Открытый код

ядро на Rust с открытой
лицензией — проверяемо
вашей службой ИБ

 Разработано в России

Linux и Astra Linux

Вне пути входа — вход не зависит от Census

КАК ЭТО РАБОТАЕТ

Декларация → план → применение → контроль

Тот же цикл, что у инфраструктуры-как-кода, только для доступа: сначала видно, что изменится, потом атомарное применение.

01

Декларация

Роли, учётки, группы, sudoers и лимиты — **подписанные TOML-файлы на диске**. Источник истины, а не история ручных правок.

```
/etc/census/*.toml
```



02

План

Полный дифф с текущим состоянием устройства — **до любых изменений**. Ничего не применяет.



03

Применение

Идемпотентно и атомарно. Census помечает своё и **не удалит последний путь доступа** — от блокировки самого себя есть защита.

```
census apply
```



04

Контроль

Расхождение с декларацией (drift) видно по каждому устройству и **приводится обратно к декларации**, а не накапливается годами.

```
census status
```

 **Доставка декларации — любым каналом:** Tessera Control, Ansible, золотой образ или курьер. Census просто читает файлы с диска — сеть устройству не нужна, интернет тем более.

Кто на самом деле имеет доступ — видно до проверки регулятора

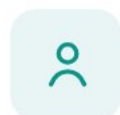
Встроенный аудит фактических прав файловой системы. Только чтение: ничего не меняет, работает офлайн.



Снимок прав файловой системы

CENSUS AUDIT FS

- Фактические права по каждому пути: владельцы, группы, ACL, SUID-биты
- Не «как настроено в документации», а **как есть на устройстве сейчас**



Кто дотягивается до объекта

CENSUS AUDIT EXPOSE

- Для критичного файла или каталога — **полный список субъектов**, которые реально могут читать или писать
- Учитывает цепочки: членство в группах, ACL, права на родительские каталоги



Мандатные метки учитываются

ASTRA (PARSEC) И SELINUX

- Достижимость считается с **учётом мандатных ограничений**, а не только классических прав
- На Astra Linux — обе координаты: целостность (МКЦ) и конфиденциальность (МРД)



Отчёт для службы ИБ

ТОЛЬКО ЧТЕНИЕ · ОФЛАЙН

- Скрытые пути до критичных файлов видны **раньше, чем их найдёт аудитор** или злоумышленник
- Аудит ничего не меняет на устройстве — безопасно запускать в проде

Разделение ответственности с Tessera Access

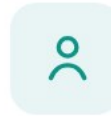
Census готовит доступ заранее, Tessera проверяет личность при входе.
Продукты работают в паре — и каждый сам по себе.



Вне пути входа

ВХОД НЕ ЗАВИСИТ ОТ CENSUS

- Учётки, группы и лимиты материализуются **заранее**, а не в момент входа
- Отказ или отсутствие Census не блокирует вход инженера — на пути аутентификации его просто нет



Ролевые учётки вместо личных

ЕДИНИЦЫ НА УСТРОЙСТВО, НЕ N×M

- На устройстве несколько ролевых учёток (оператор, обслуживание, администратор) — **не по учётке на человека**
- Личность инженера — в сертификате Tessera, а не в учётке: подотчётность без разрастания



Защита от самоблокировки

FAIL-SAFE ПРИ ПРИМЕНЕНИИ

- Census **не удалит последний путь доступа** к устройству — аварийный вход защищён
- Применение атомарно: не бывает «наполовину применённой» декларации



Одна платформа с Tessera

ОБЩИЙ СЛОВАРЬ РОЛЕЙ

- Роли в декларации Census и в сертификатах Tessera — **один словарь**, без двойного ведения
- Доставка деклараций через Tessera Control — или любым вашим каналом

Census за 30 секунд

01

Доступ как код

Учётки, группы, sudoers, лимиты — из одной подписанной декларации.

02

План до применения

Полный дифф с текущим состоянием; применение идемпотентно и атомарно.

03

Аудит фактических прав

Кто реально дотягивается до критичных файлов — с учётом ACL и мандатных меток.

04

Безопасно по построению

Вне пути входа, защита от самоблокировки, чужие объекты не трогаются.

05

Открытый код

Ядро на Rust с открытой лицензией; разработано в России, работает на Astra.

06

Пара к Tessera Access

Census готовит ролевые учётки, Tessera персонализирует вход по сертификату.

🔗 Персонализированный офлайн-вход на эти же устройства — **Tessera Access**: сертификаты, делегирование подрядчикам, аудит. [смотреть презентацию →](#)

Следующий шаг — пилот на срезе вашего парка

Опишем роли декларацией, покажем дифф с текущим состоянием и отчёт аудита фактических прав.

docs.tessera-access.ru tessera@tessera-access.ru TesseraLabs · Россия

