Безагентский сканер Unix-систем в AxelNAC

Виталий Резинкин

Ведущий системный аналитик Axel PRO

Кто я

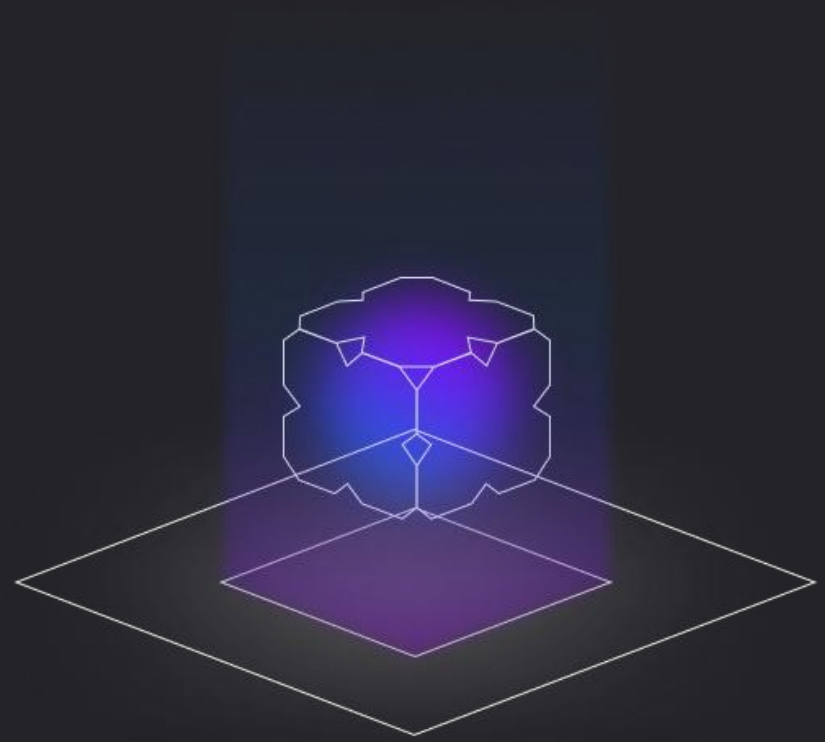
Виталий Резинкин

Ведущий системный аналитик Axel PRO

- 15 лет в IT
- Разработка ПО для IoT устройств
(более 50 протоколов промышленной автоматизации)
- 5 лет опыта в разработке электроники для промышленных и коммерческих зданий
- 5 лет проектирования сетевых решений

Сегодня поговорим о...

- Сканер Unix-систем. Для чего нужен?
- Как работает сканер?
- SSH, как надежный транспорт
- Проверки
- Система репортов
- Перфоманс и настройка
- О подходе проектирования. Гибкость и максимальная ясность



Сканер Unix-систем

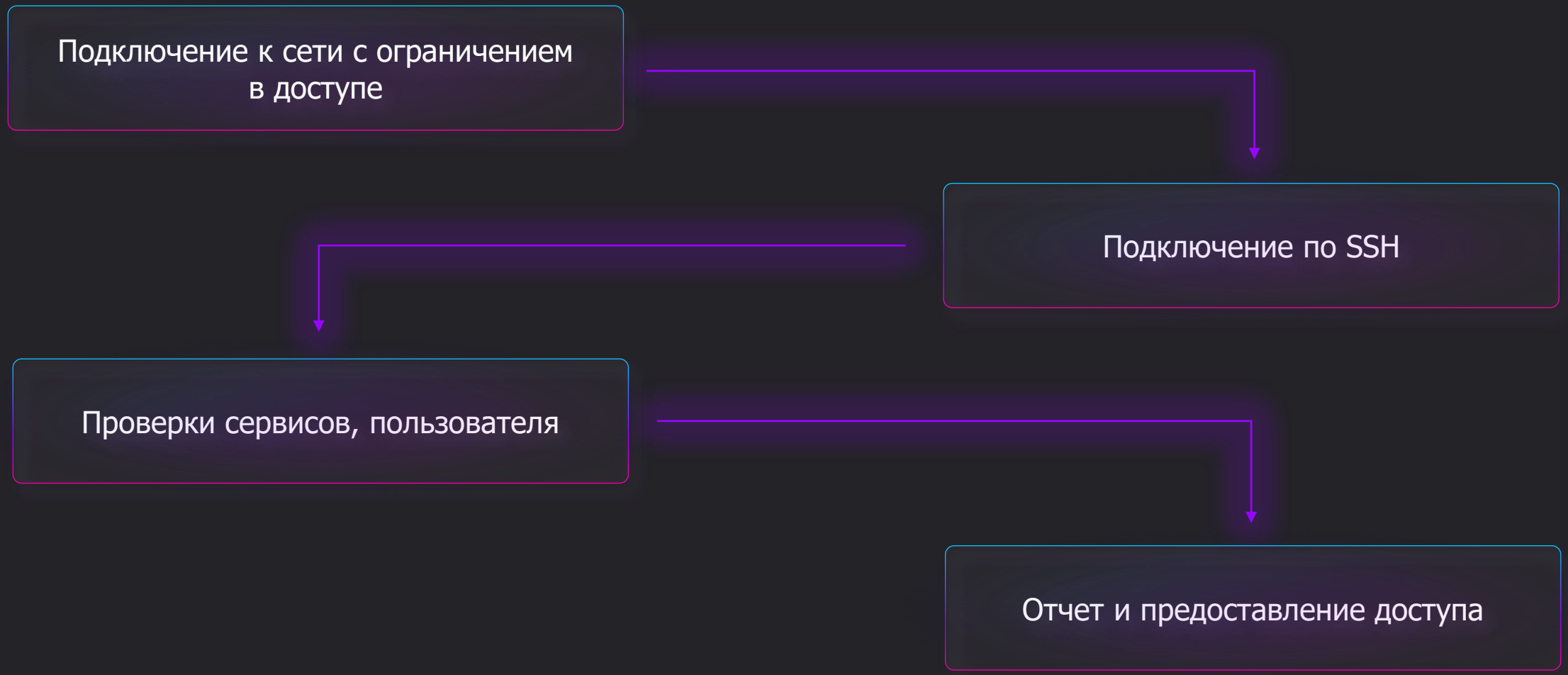
Дополнительная точка проверки АРМ

- Проверка соответствия требованиям политик для АРМ
- Контроль за состоянием АРМ в ходе работы
- Реагирование в случае инцидента
- Информирование пользователя

Безагентский сканер

- Не накладывает дополнительную нагрузку в виде сервиса
- Не требует постоянного обновления приложения
- Достаточно SSH и bash

Как работает сканер



Как работает сканер

SSH как надежный транспорт

- Подключения по сертификату
- Безопасные алгоритмов и шифров
- Надежность установки соединения при пиковых нагрузках
- Гибкость в настройках

Состояние сервисов и автозагрузки

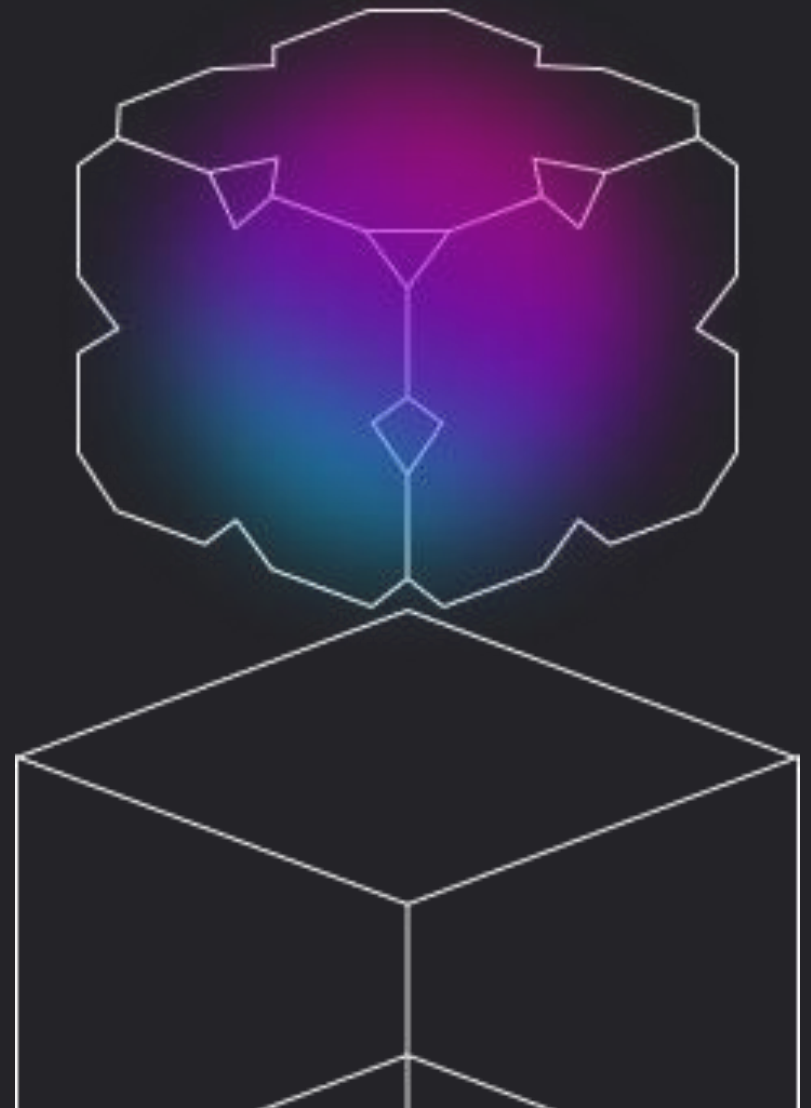
Статус сервиса

Запущен | Остановлен

Наличие сервиса в автозагрузке

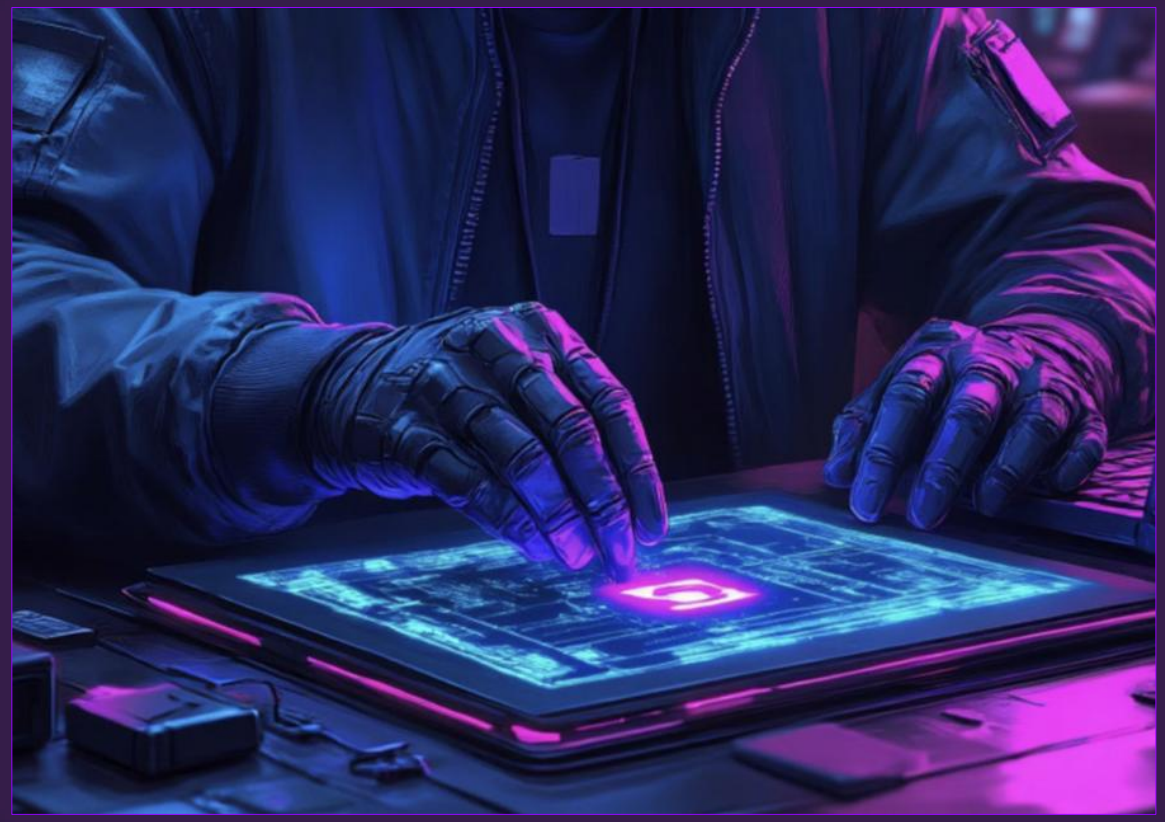
Принадлежность пользователя к группам

- Определение активного пользователя
- Проверка на соответствия списку групп



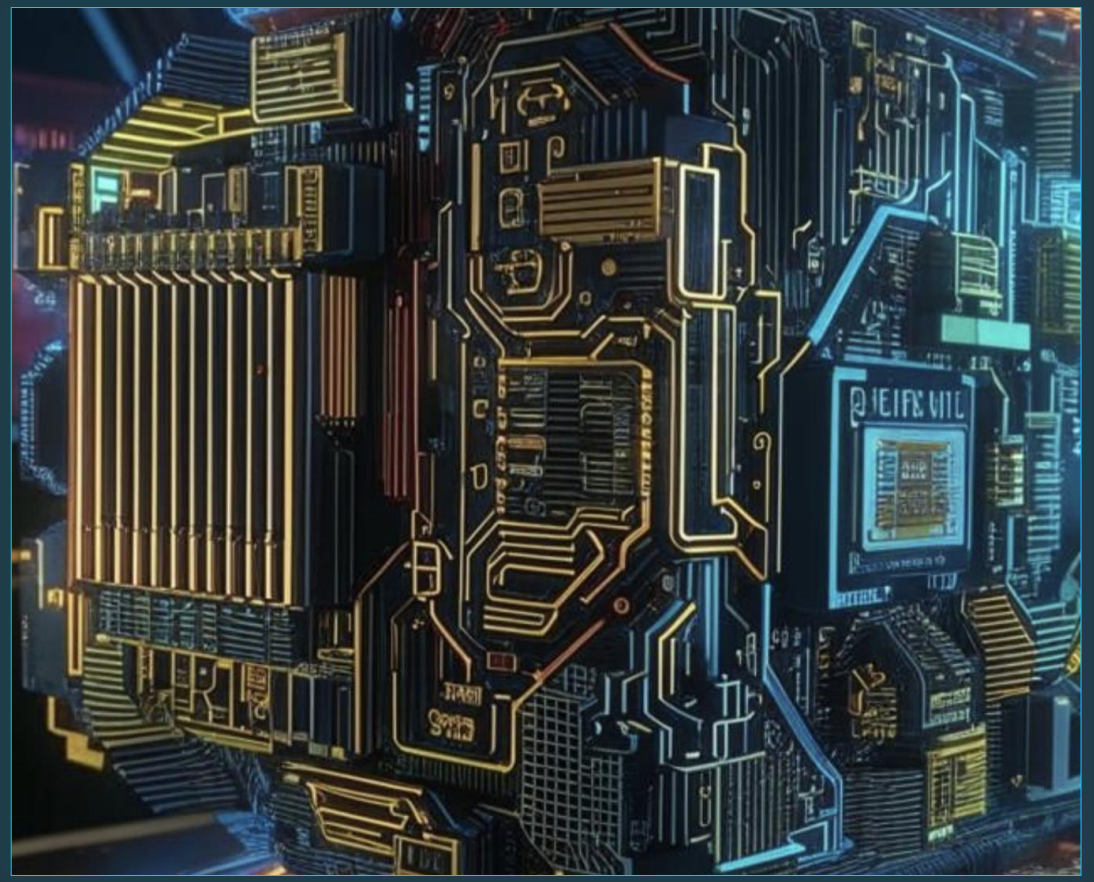
Целостность и наличие файлов

- Проверка наличия файла по указанному пути
- Проверка 128-битной hash-суммы



Обновления системы

- Наименование ядра системы
- Проверка версии ядра: основная версия, релизная версия, версия патча



Антивирус

- Версия
- Дата обновления
- Статус службы
- Статусы внутренних компонентов

Система репортов

- Логи на всех уровнях (подключение, система, консоль)
- Проблемы: общие ошибки в парадигме NAC и используемых инструмкнтов
- Уведомления администратора (mail, sms), логи системы
- **API и передача на внешние ИС**

Производительность

- 300-500ms на 1 проверку
- 1000 подключений за 1,5 секунды при выполнении 3-х проверок
- **4000** подключений с временем ожидания в 2 секунды, **100%** успешных соединений
- При 1,5-секундном таймауте - **99,6%**

Настройка

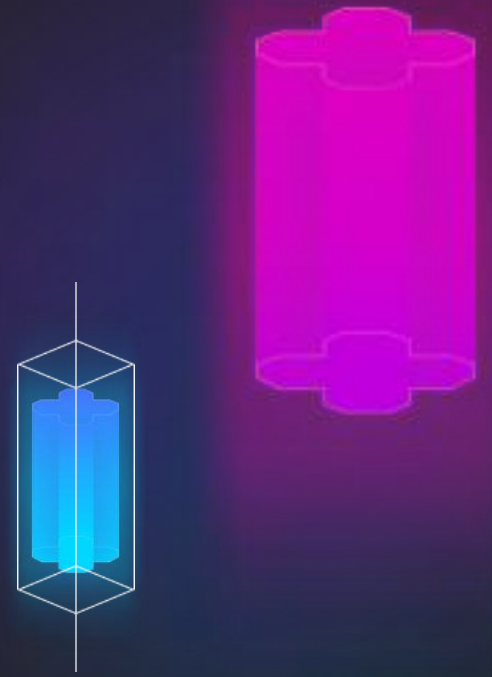
- Гибкая настройка с учетом требований безопасности SSH за счет скрипта
- Широкий спектр предварительных проверок супликанта на наличие пакетов
- Логирование шагов настройки и системных ошибок
- Скрипт генерируется автоматически под настройки сканера

Как мы проектируем и создаем

Решение для всех участников процесса:
Администратор, пользователь, инсталлятор

Высокий SLA:
Каждый шаг тестируется на производительность

Подробная документация:
Описываем работу не только нашего продукта,
но и работу взаимодействующих систем



Спасибо

Если у вас остались вопросы, задайте их нам

info@axel.pro

+7 (495) 909-00-60

https://axel.pro/axelnac

https://axel.pro/