

ДНК им. В.А. Котельникова

Проект модернизации инфраструктуры предприятия <COMP_NAME>

Исполнитель: Зайцев Г. Э.

2022 г.

Техническое задание

В ходе технического задания перед нами стояла задача проанализировать существующую инфраструктуру и, исходя из современных стандартов, составить план по её модернизации. Модернизация состоит из следующих этапов:

- перевод основных сервисов на облако;
- введение единой точки входа;
- реализация отказоустойчивости;
- внедрение технологического стека CI/CD.

Также стоит отметить, что перед нами стояла задача использовать только **лицензионно “чистое”** ПО.

Анализ существующей инфраструктуры

Анализ данной инфраструктуры выявил её многочисленные недостатки. В их числе:

- уязвимость инфраструктуры к внештатным ситуациям;
- отсутствие единой точки входа для всех сервисов;
- проблемы с лицензией, в частности, это касается продуктов Microsoft;

Наш подход к решению задачи

Мы подошли к данному проекту, исходя из следующих принципов:

- **Независимость**

Opensource - наше все! Никаких больше проблем с лицензией

- **Бесплатность**

Избежать затруднений финансовой логистики так просто, когда она отсутствует

- **Надежность**

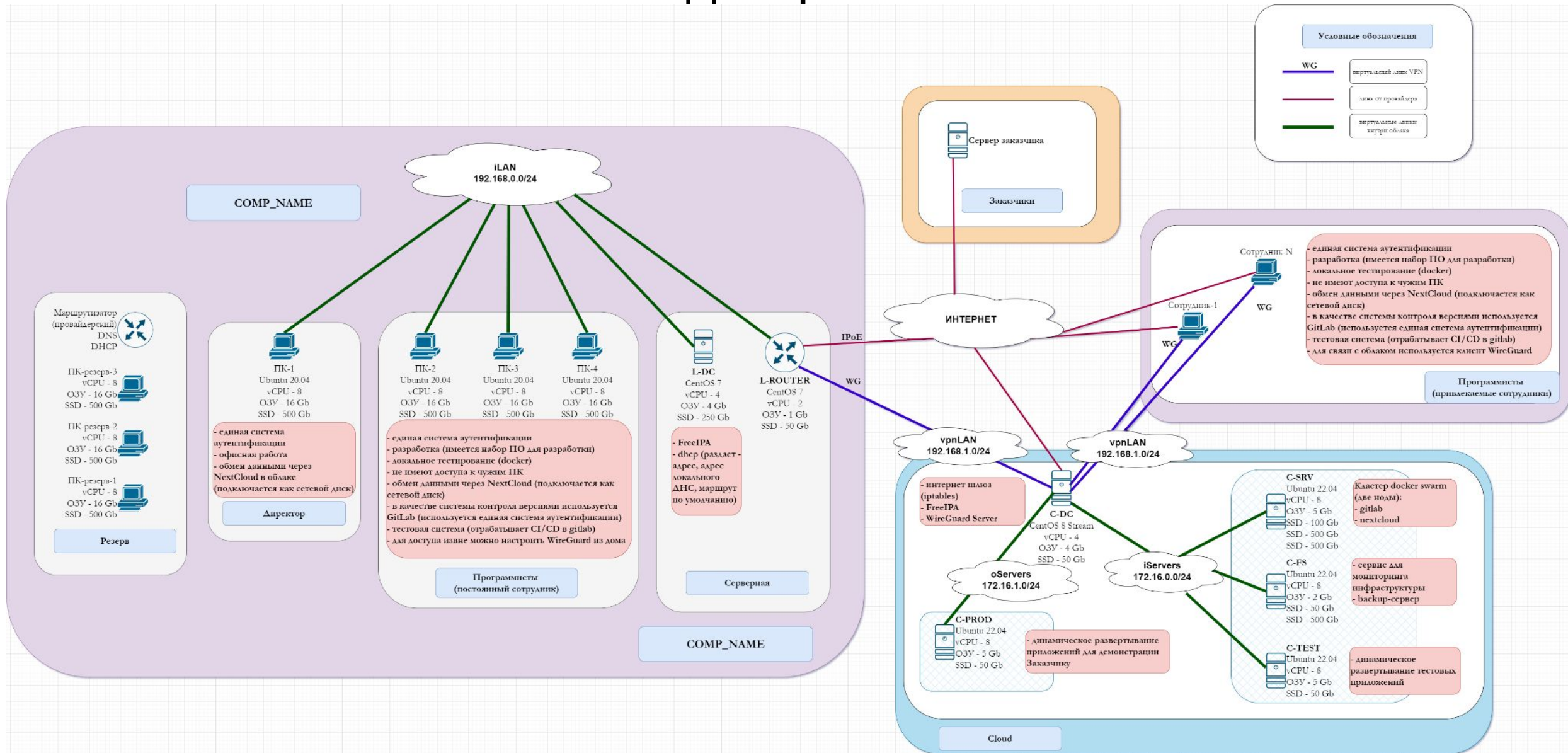
Отказоустойчивость всем и каждому. Теперь работа не встрянет из-за одного упавшего сервера

- **Строгость**

Зачем десятилетке XXXXXL-футболка? Иногда самое продвинутое ПО бывает излишним и ему стоит уступить место более лаконичным аналогам.

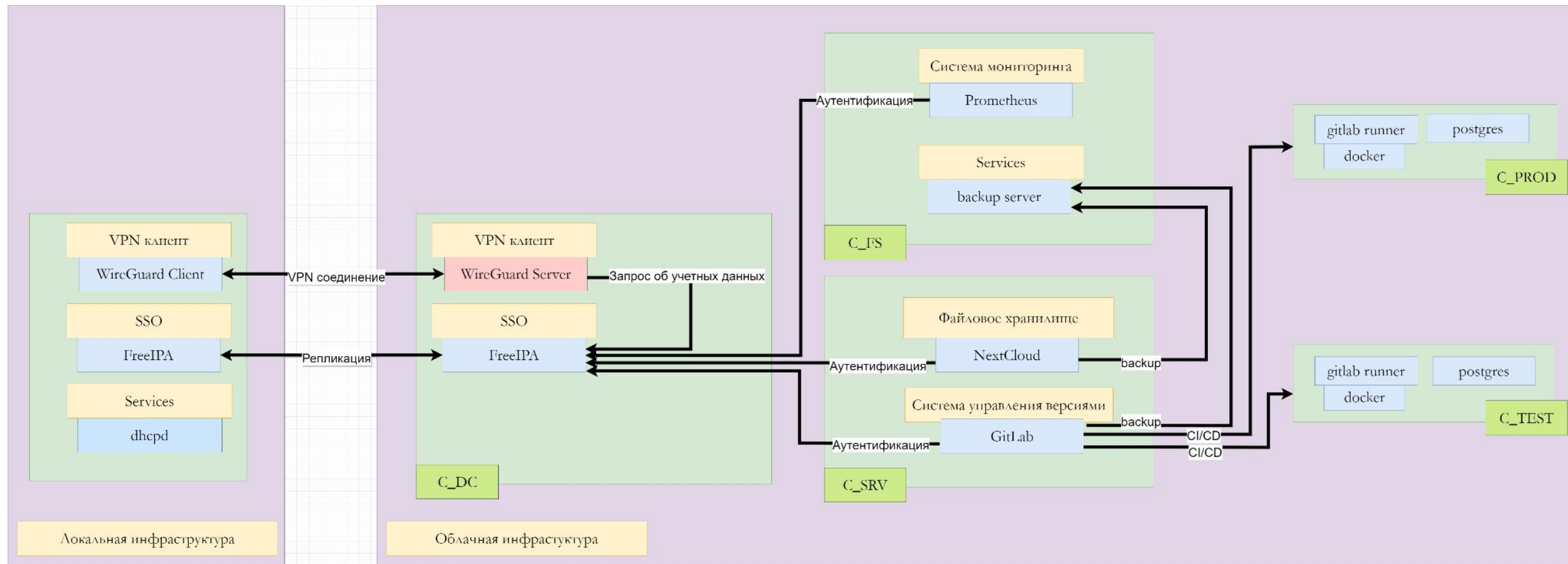
Проект инфраструктуры предприятия

L3 диаграмма



Проект инфраструктуры предприятия

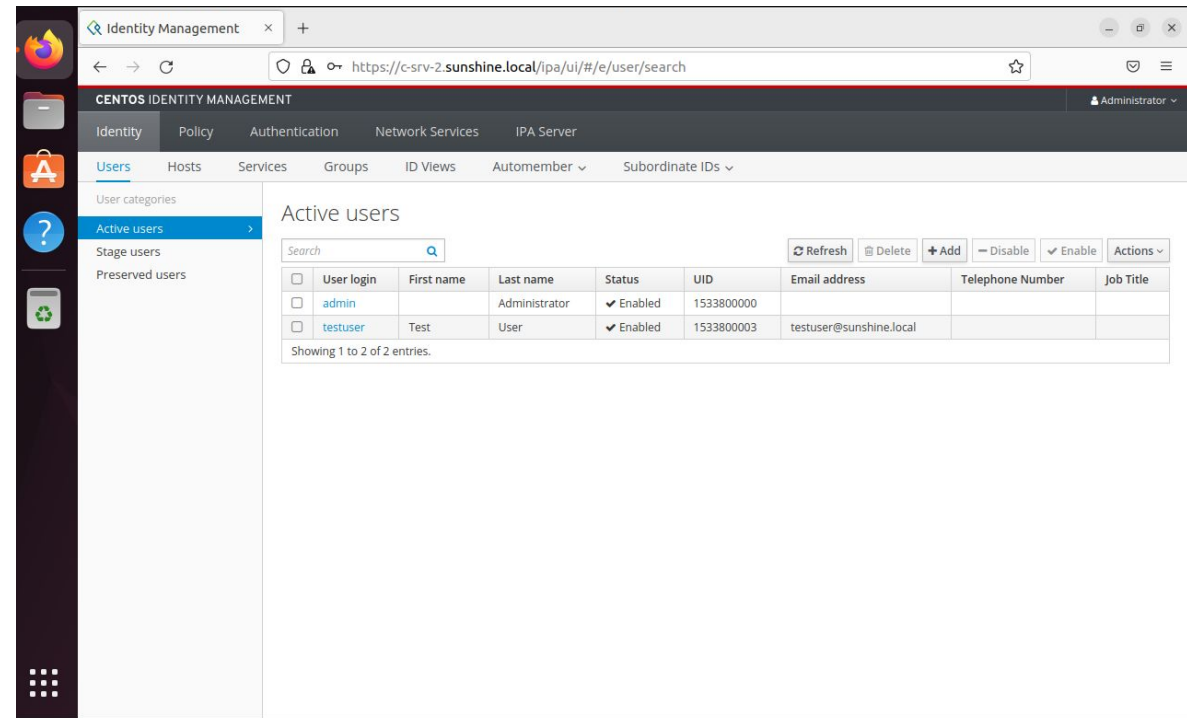
- Диаграмма взаимодействия компонентов



Модуль “Единая система аутентификации”

Предполагается:

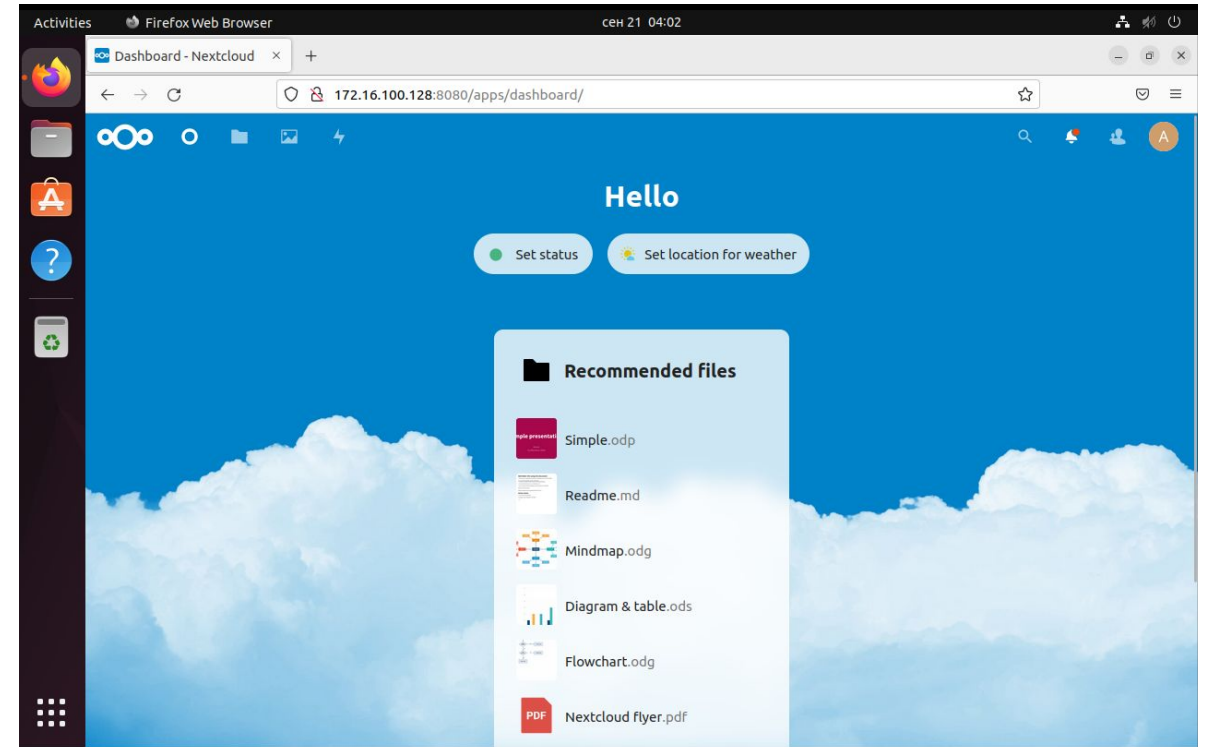
- единое управление учетными данными пользователей и их доступы в различные системы;
- добавлена возможность ограниченного доступа в системы, доступа в системы по времени, отключение учетной записи по истечению времени;
- резервирование за счет репликаций FreeIPA серверов;



Модуль “Файловое хранилище”

Предполагается:

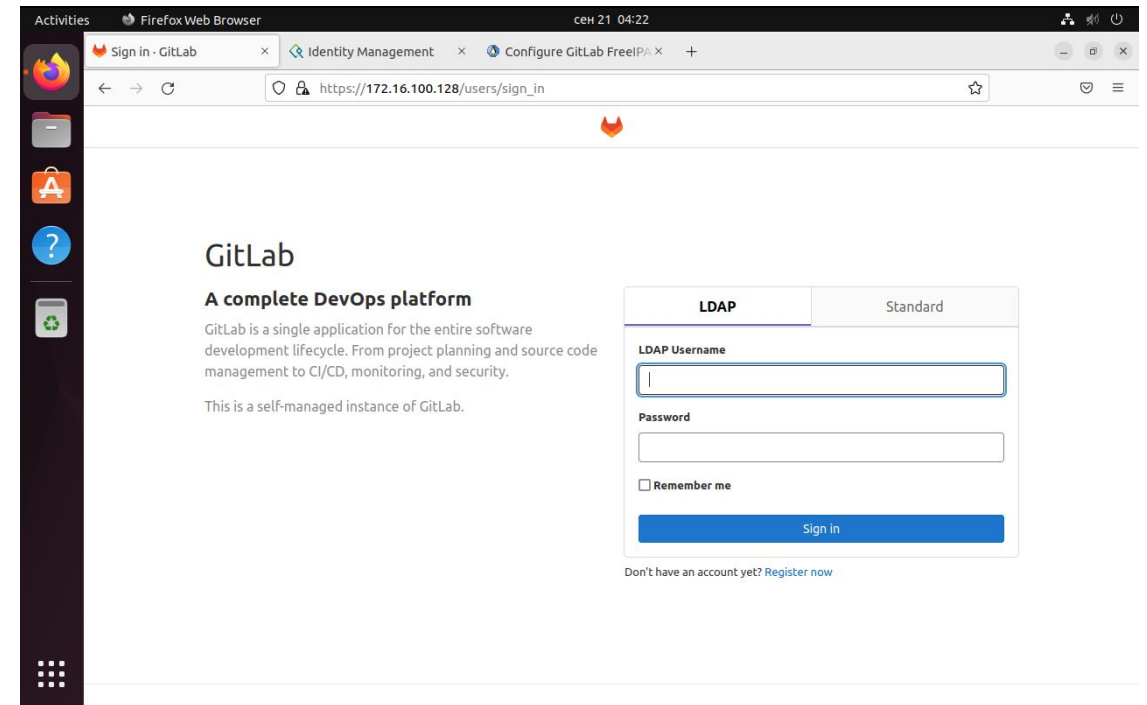
- в качестве файлового хранилища выступает NextCloud
- данные бэкапятся на backup-сервере
- используется LDAP
- подключение клиентов с помощью WebDAV



Модуль “Система контроля версий”

Предполагается:

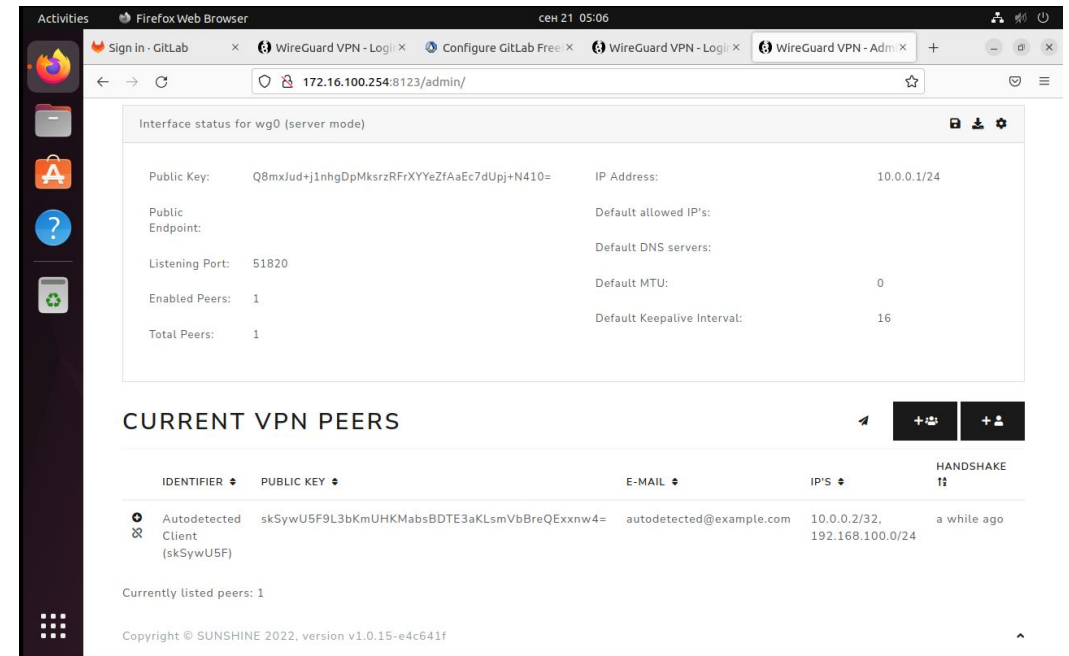
- в качестве системы контроля версий выступает gitlab;
- аутентификация и авторизация через LDAP (FreeIPA)
- бэкап производится на backup сервер
- данная система поддерживает CI/CD
- предполагается наличие двух хостов PROD и TEST для запуска Docker контейнеров
- при добавлении контейнера в PROD (ветка master) также пробрасывает порт для доступа Заказчиков по белому адресу и порту;
- при добавлении контейнера в TEST (ветка branch) доступ к приложению возможно только устройствам в локальной сети



Модуль “VPN”

Предполагается:

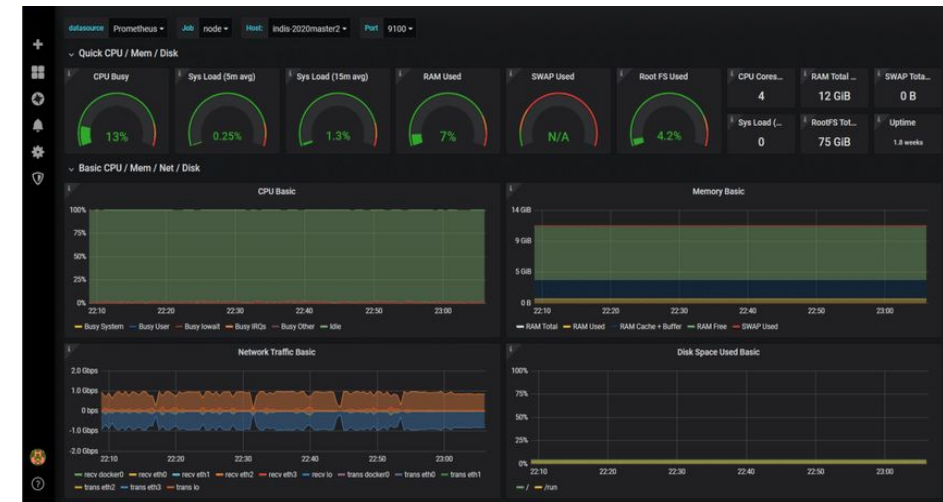
- в качестве VPN сервера выбран WireGuard;
- Wireguard-сервер расположен на C-DC
- прикручен OpenSource WebGUI к данному сервису;
- используется LDAP



Модуль “Мониторинг”

Предполагается:

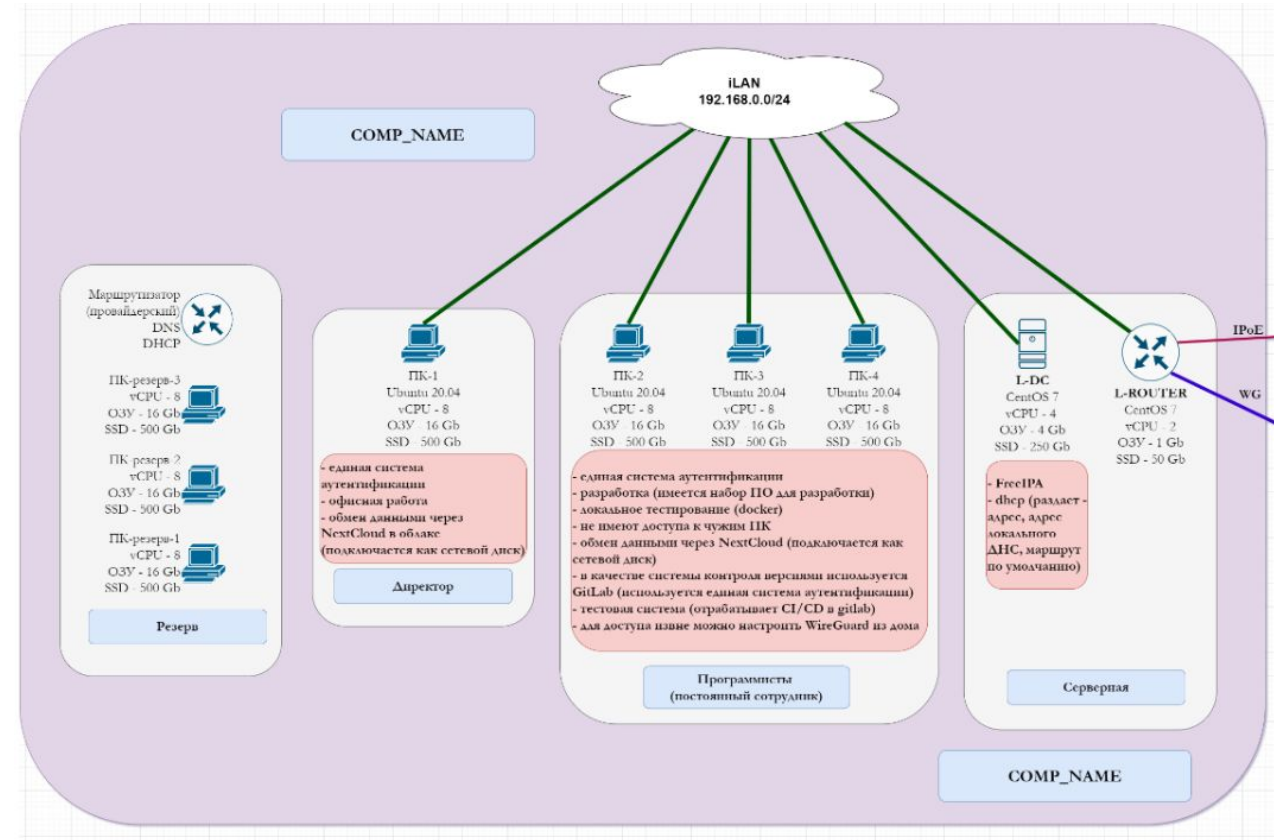
- в качестве системы мониторинга выступает Prometheus + Grafana;
- данная система мониторит все устройства компании;
- используется LDAP;
- также добавлена возможность оповещений:
 - оповещение в бот Telegram



Модуль “Локальная сеть предприятия”

Предполагается:

- в качестве ОС для постоянных сотрудников выбран Ubuntu 22.04 с графикой;
- аутентификация клиентских машин через FreeIPA
- в случае отказа L_DC аутентификация проводится через C_DC
- удаленный рабочий стол - VNC



Контакты

- **Участник:** Зайцев Георгий Эдуардович
- **Эксперт-компатриот:** Жигжитов Максим Владимирович

Вопросы для обсуждения

Спасибо за внимание!