Проект модернизации инфраструктуры предприятия <COMP_NAME>

Исполнитель: Зайцев Г. Э.

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.

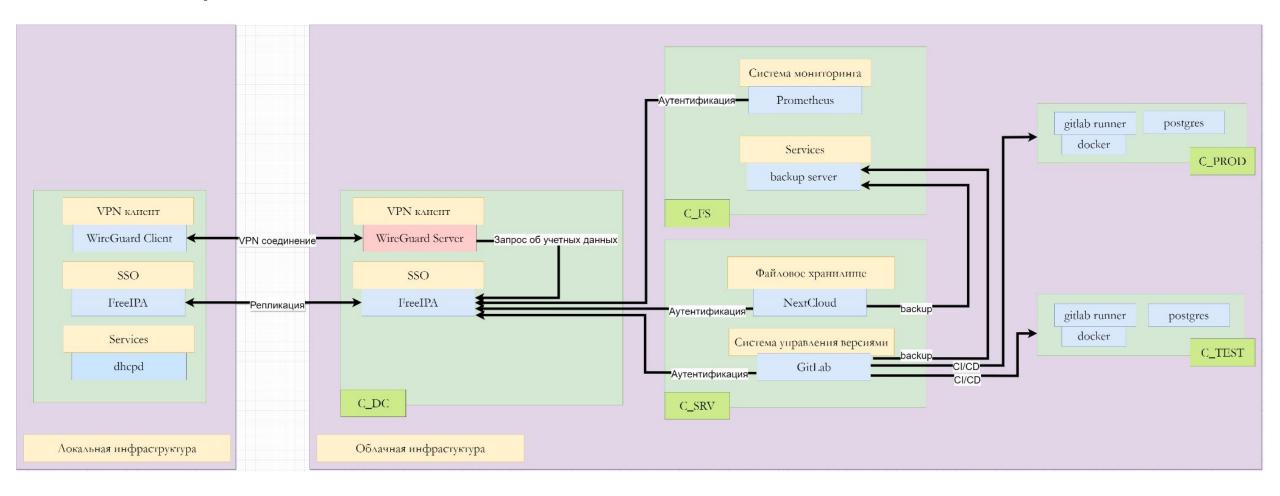
Проект инфраструктуры предприятия

L3 диаграмма Условные обозначения ртуальный линк VPN висотуальные динки виутри облака 192.168.0.0/24 COMP_NAME Заказчики единая система аутентификации COTOVARIIK-N разработка (имеется набор ПО для разработки) локальное тестирование (docker) не имеют доступа к чужим ПК обмен данными через NextCloud (подключается как Маршрутизатор в качестве системы контроля версиями используется **UHTEPHET** (провайдерский) GitLab (используется единая система аутентификации) DNS K - тестовая система (отрабатывает CI/CD в gitlab) DHCP - для связи с облаком используется клиент WireGuard ПК-1 ПК-3 ПК-4 L-DC ПК-резерв-3 Ubuntu 20.04 Ubuntu 20.04 CentOS 7 Программисты vCPU - 8 vCPU - 8 vCPU - 8 vCPU - 8 CentOS 7 O3Y - 16 Gb vCPU - 4 (привлекаемые сотрудники) O3Y 16 Gb O3Y 16 Gb O3V 16 Gb O3Y 16 Gb SSD - 500 Gb O3V - 4 Gb vCPU-2 SSD - 500 Gb SSD - 500 Gb SSD - 500 Gb O3Y - 1 Gb SSD - 250 Gb ПК-резерв 2 SSD - 50 Gb - единая система vCPU - 8 единая система аутентификации аутентификации FreeIPA O3V - 16 Gb разработка (имеется набор ПО для разработки) 192.168.1.0/24 192.168.1.0/24 офисная работа - dhcp (раздает -SSD - 500 Gb - локальное тестирование (docker) обмен данными через адрес, адрес - не имеют доступа к чужим ПК NextCloud в облакс ПК-резерв-1 - обмен данными через NextCloud (подключается как Knacrep docker swarm ДНС, маршрут vCPU - 8 (iptables) VCPU - 8 по умодчанию) O3V - 16 Gb - в качестве системы контроля версиями используется - gitlab O3V - 5 Gb SSD - 500 Gb C-DC Директор GitLab (используется единая система аутентификации) - WireGuard Server - nextcloud SSD - 100 Gb - тестовая система (отрабатывает CI/CD в gitlab) SSD - 500 Gb vCPU - 4 - для доступа извне можно настроить WireGuard из дома Резерв SSD - 500 Gb O3Y - 4 Gb SSD - 50 Gb C-FS **iServers** oServers Ubuntu 22.04 172.16.0.0/24 Программисты Серверная 172.16.1.0/24 vCPU - 8 (постоянный сотрудник) инфраструктуры O3V - 2 Gb - backup-сервер SSD - 50 Gb SSD - 500 Gb vCPU - 8 динамическое развертывание COMP_NAME C-TEST O3Y - 5 Gb Ubuntu 22.04 - динамическое SSD - 50 Gb vCPU - 8 развертывание тестовых O3V - 5 Gb SSD - 50 Gb

Cloud

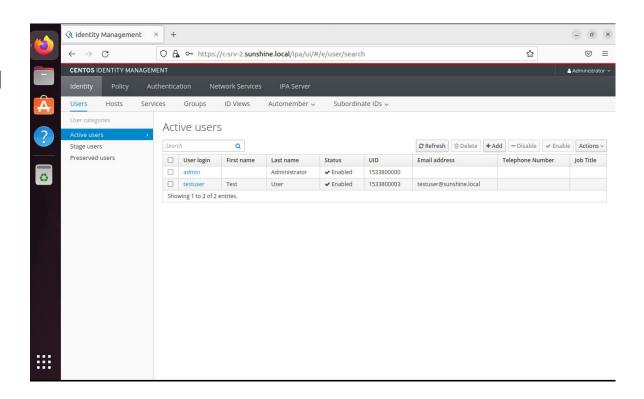
Проект инфраструктуры предприятия

• Диаграмма взаимодействия компонентов



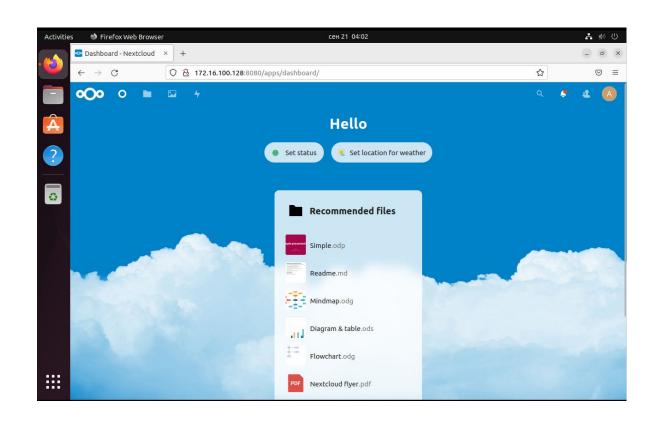
Модуль "Единая система аутентификации"

- 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 FreelPA серверов;



Модуль "Файловое хранилище"

- 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)

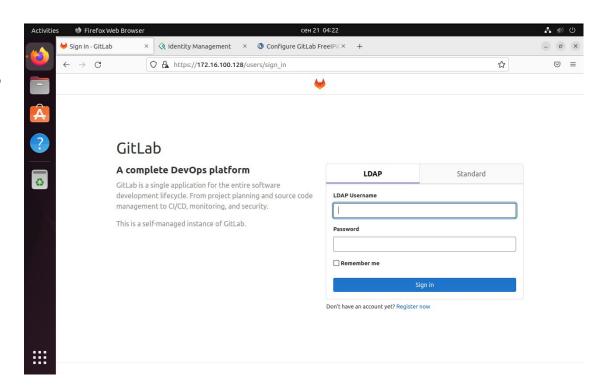
бэкап производится на backup сервер

данная система поддерживает CI/CD

 предполагается наличие двух хостов PROD и TEST для запуска Docker контейнеров

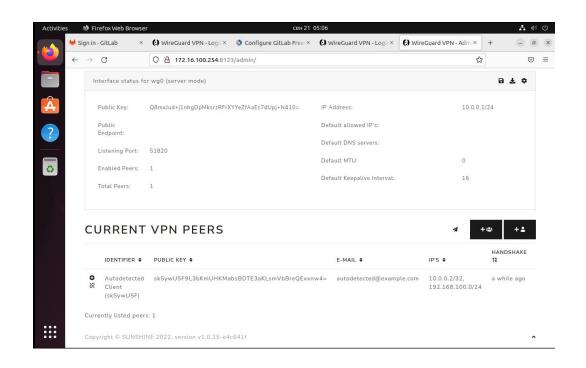
 при добавлении контейнера в PROD (ветка master) также пробрасывает порт для доступа Заказчиков по белому адресу и порту;

 при добавлении контейнера в TEST (ветка branch) доступ к приложению возможно только устройствам в локальной сети



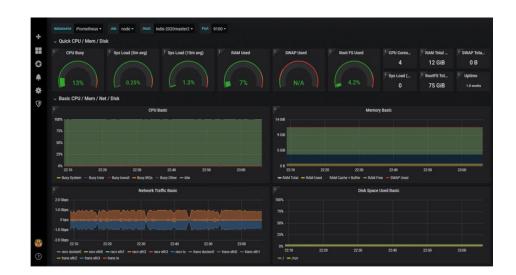
Модуль "VPN"

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



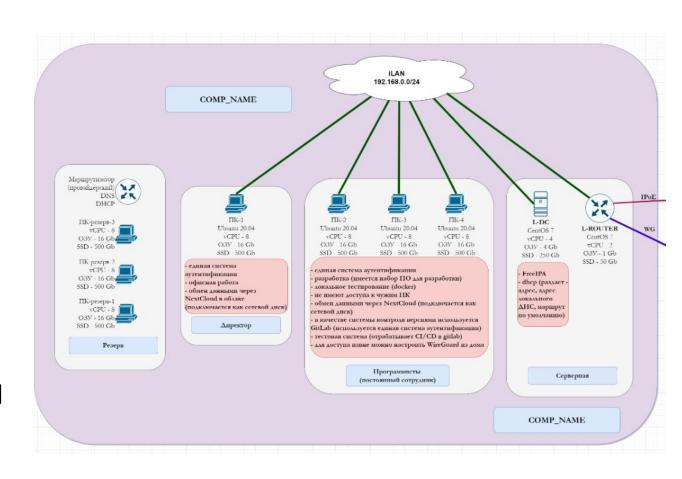
Модуль "Мониторинг"

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



Модуль "Локальная сеть предприятия"

- 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!