AD и MSA: дружим системы для защиты контейнеров

Вильмов Андрей

- Работаю с базами данных (в основном MsSQL) 10 лет (из них 2 — на фрилансе и 8 — в компании ПГС).
  Стек: TSQL/PSQL/Python/C++
- Последние 5 лет также разрабатываю микросервисную архитектуру и занимаюсь аналитикой данных.
- Успешно помогал бизнесу решать проблемы, связанные с медленной работой баз и с аналитикой больших данных

AD и MSA. Как мы дружили системы

Проблема с которой столкнулись

- Увеличение сотрудников в IT отделе

Проблема с которой столкнулись

- Увеличение сотрудников в IT отделе
- Неконтролируемый доступ сотрудников в системам

Проблема с которой столкнулись

- Увеличение сотрудников в IT отделе
- Неконтролируемый доступ сотрудников в системам
- Беспорядок в доступах (забывали у кого какие доступы есть)

Все это приводило к угрозам

- Утечки данных

Все это приводило к угрозам

- Утечки данных
- Неконтролируемого доступа

Все это приводило к угрозам

- Утечки данных
- Неконтролируемого доступа
- Большим дырам в безопасности

Появились идеи

- Автоматическое развертывание SSH-ключей

Появились идеи

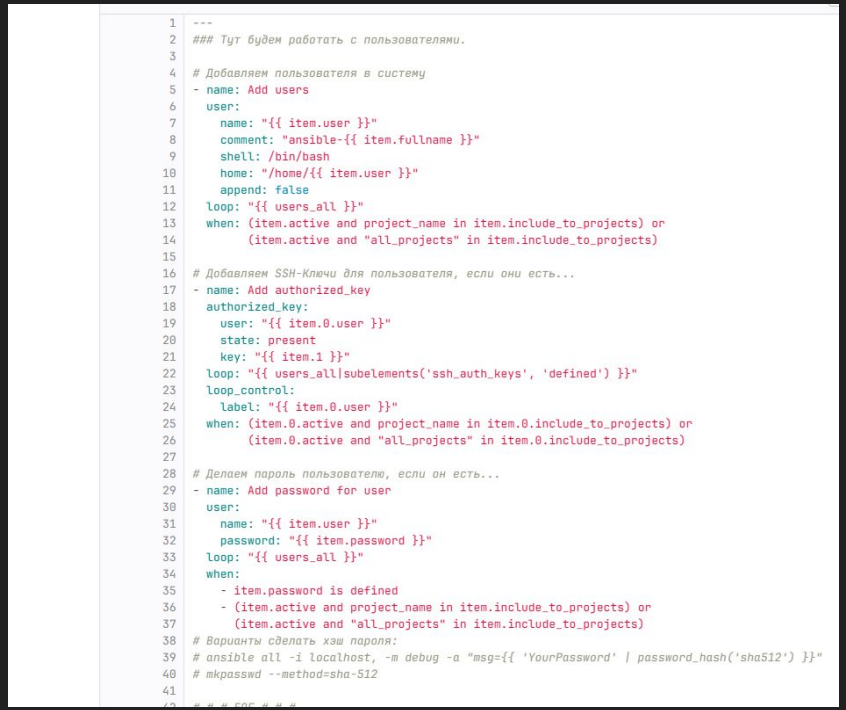
- Автоматическое развертывание SSH-ключей
- Интеграция с Active Directory (AD)

Автоматическое развертывание SSH-ключей

1. Развернули Ansible и подключили все сервера

Автоматическое развертывание SSH-ключей

1. Развернули Ansible и подключили все сервера
2. Реализовали роли для добавления SSH ключей



```yaml
---
### Тут будем работать с пользователями.

# Добавляем пользователя в систему
- name: Add users
  user:
    name: "{{ item.user }}"
    comment: "ansible-{{ item.fullname }}"
    shell: /bin/bash
    home: "/home/{{ item.user }}"
    append: false
  loop: "{{ users_all }}"
  when: (item.active and project_name in item.include_to_projects) or
        (item.active and "all_projects" in item.include_to_projects)

# Добавляем SSH-Ключи для пользователя, если они есть...
- name: Add authorized_key
  authorized_key:
    user: "{{ item.0.user }}"
    state: present
    key: "{{ item.1 }}"
  loop: "{{ users_all|subelements('ssh_auth_keys', 'defined') }}"
  loop_control:
    label: "{{ item.0.user }}"
  when: (item.0.active and project_name in item.0.include_to_projects) or
        (item.0.active and "all_projects" in item.0.include_to_projects)

# Делаем пароль пользователю, если он есть...
- name: Add password for user
  user:
    name: "{{ item.user }}"
    password: "{{ item.password }}"
  loop: "{{ users_all }}"
  when:
    - item.password is defined
    - (item.active and project_name in item.include_to_projects) or
      (item.active and "all_projects" in item.include_to_projects)
# Варианты сделать хэш пароля:
# ansible all -i localhost, -m debug -a "msg={{ 'YourPassword' | password_hash('sha512') }}"
# mkpasswd --method=sha-512
```

Автоматическое развертывание SSH-ключей

1. Развернули Ansible и подключили все сервера
2. Реализовали роли для добавления SSH ключей
3. Создали репозиторий в гите с CI/CD

Но этого было мало

- При создании пользователя он автоматически не добавлялся на сервера
- При увольнении права у пользователя автоматически не забирались

И тут на помощь приходит AD

Интеграция с Active Directory (AD)

Реализован скрипт который проверяет новых пользователей в AD и запускает Annsible PlayBook для того чтобы добавить нового пользователя.

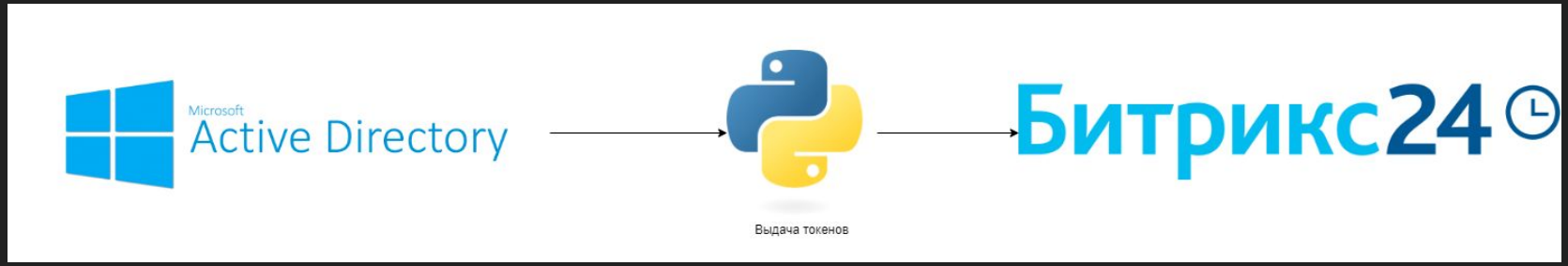
проблема с правами была решена. Но осталось…

- Решить проблему в контейнерами
- Решить проблему с внутренним доступом по API

И мы решили сохранять все образы в nexus, чтобы не забирать их из внешних репозиториев.

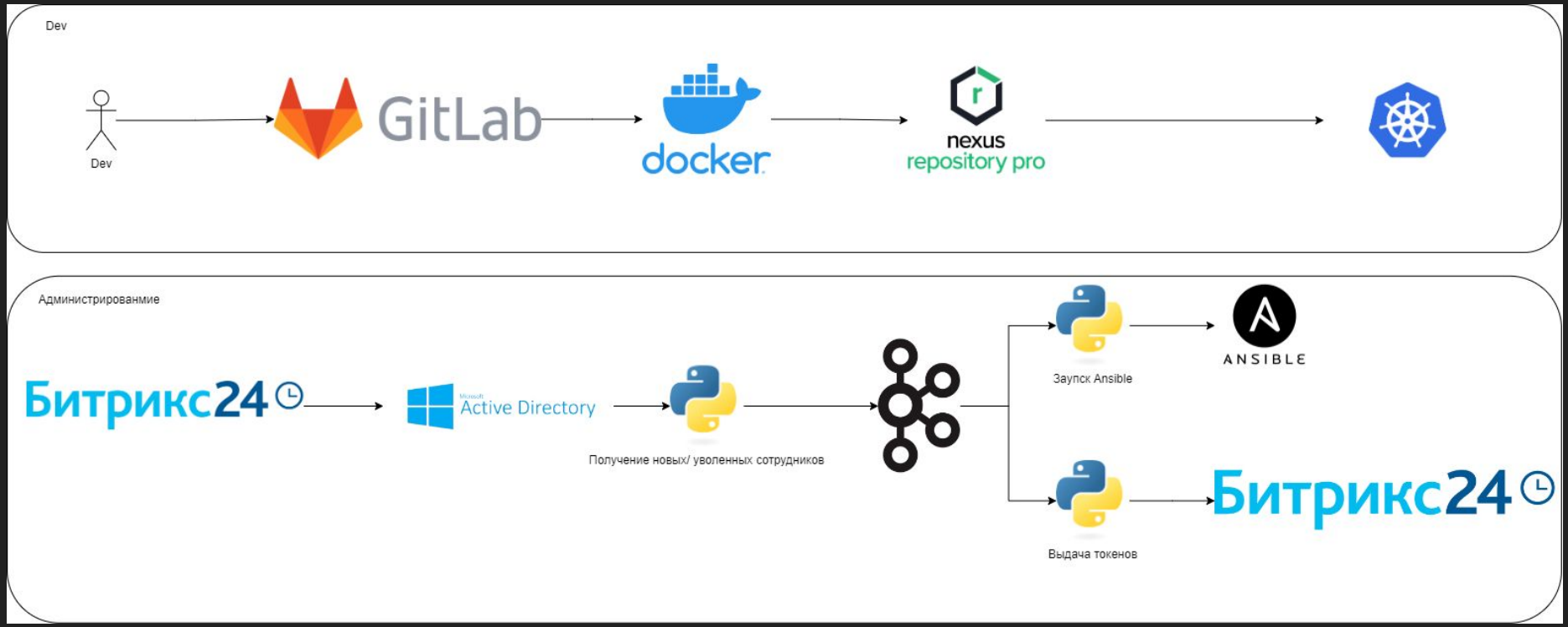
И мы решили сохранять все образы в nexus, чтобы не забирать их из внешних репозиториев.

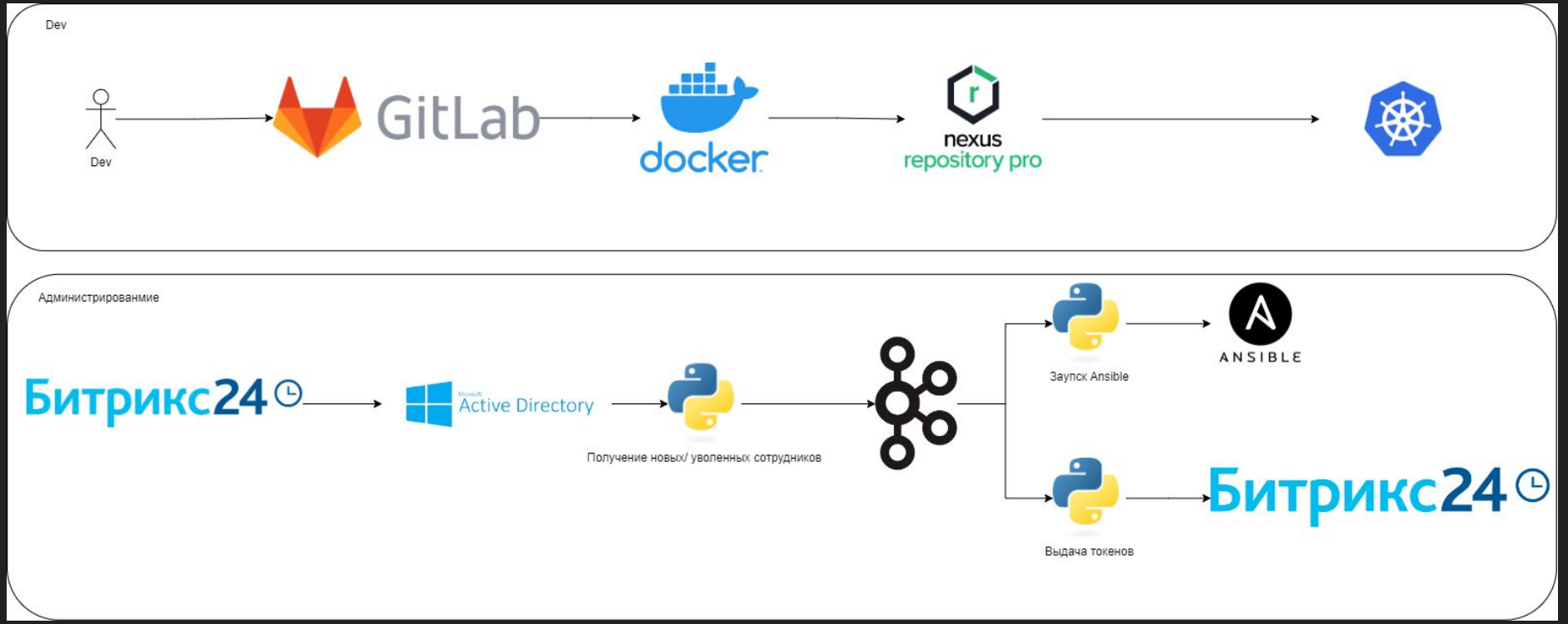
А с доступами к внутренним системам было сложнее



И мы решили забирать новых пользователей из AD, генерировать токены доступа и сохранять их в Б24. И на стороне Б24 их обновлять.

По итогу получили следующее


Dev
Dev
GitLab
docker
nexus
repository pro
Администрированмие
Битрикс24
Active Directory
Получение новых/ уволенных сотрудников
Запуск Ansible
ANSIBLE
Выдача токенов
Битрикс24



- Автоматизировали раздачу прав
- Убрали пунаницу в правах
- Реализовали Политику zero trust

Спасибо за Внимание

telegram: https://t.me/AsinusAsinorum
Телефон: 8 925 405 09 07