нетология

Безопасность в облачных провайдерах

Елисей Ильин

План занятия

1. Identity Access Management
2. Key Management Service
3. Certificate Manager
4. Итоги
5. Домашнее задание

Identity Access Management (IAM)

Identity Access Management (IAM)

IAM — централизованный сервис управления доступом к облачным ресурсам

- **Users** — управление пользователями, политикой паролей. В Yandex Cloud — аккаунты Яндекс, сервисные аккаунты и федеративные
- **Groups** — объединение пользователей в группы с одинаковыми ролями и политиками. В Yandex Cloud — allAuthenticatedUsers и allUsers
- **Polices** — правила определения разрешений на использование ресурсов
- **Roles** определяет набор разрешений для выполнения запросов к сервисам. В Yandex Cloud — примитивные роли (admin, editor и viewer) и сервисные роли + роли на ресурсы

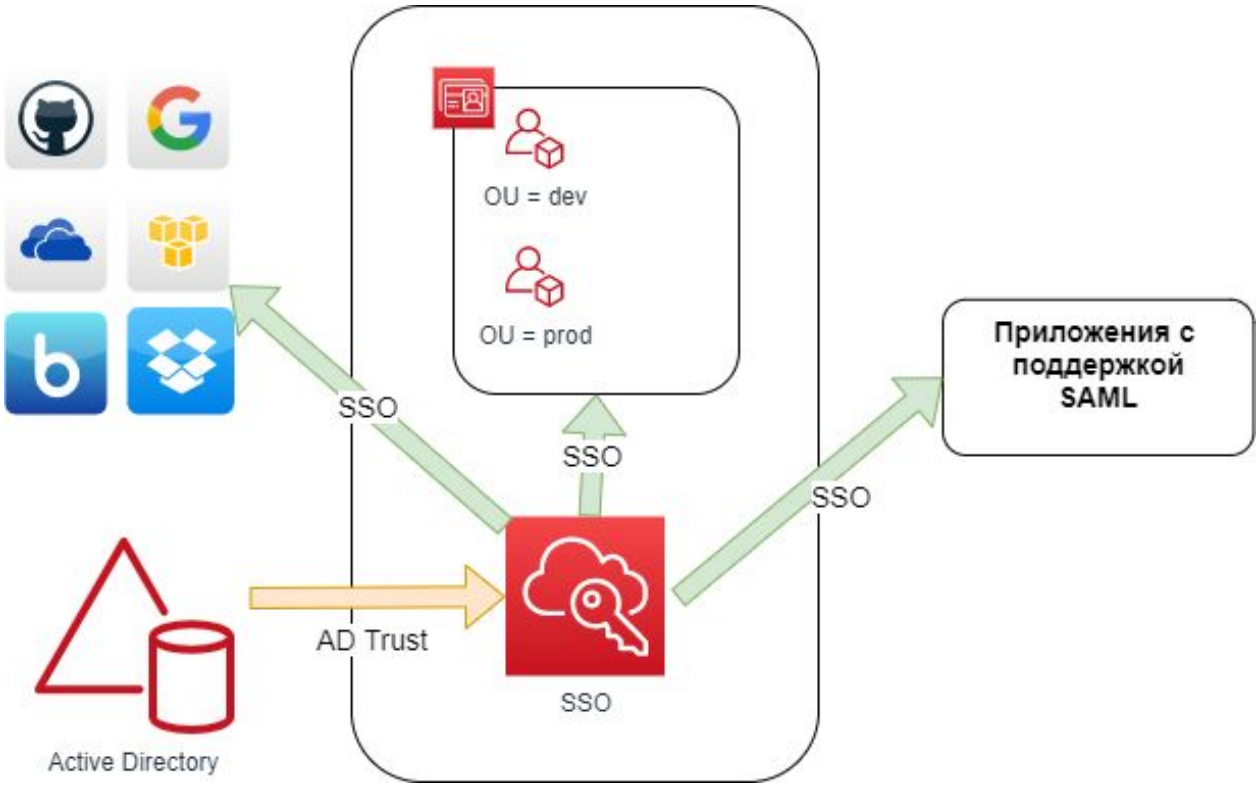
Single Sign-On (SSO)

SSO — пользователь переходит из одной системы в другую, не связанную с первой системой, без повторной аутентификации

Сервис SSO — это единый административный интерфейс для точного определения, настройки и выдачи доступов

SSO — можно использовать, чтобы просто и быстро обеспечить доступ сотрудников к нескольким аккаунтам, облачным приложениям, поддерживающим **SAML**

Пример использования



SAML — Security Assertion Markup Language

Key Management Service (KMS)

Key Management Service (KMS)

KMS — сервис для создания ключей шифрования и управления ими

KMS позволяет создавать и управлять Customer Master Keys (CMK)

- Ключ CMK генерируется внутри аппаратных модулей безопасности (HSM), которые находятся под управлением облачного провайдера. CMK не могут быть экспортированы
- Можно импортировать ключ из собственной инфраструктуры управления ключами и связать его с CMK
- Можно генерировать и использовать в кластере AWS CloudHSM в рамках возможности собственного хранилища ключей в AWS KMS (в Yandex Cloud — в стадии preview)

HSM — https://en.wikipedia.org/wiki/Hardware_security_module

Key Management Service (KMS)

- Позволяет шифровать данные до 4 Кбайт (в Yandex Cloud — до 32 КБ)
- Интегрирован со многими сервисами AWS (Yandex Cloud — Managed Service for Kubernetes, Certificate Manager, шифрование бакетов, Terraform)
- Оплата по вызову API (в Yandex Cloud — количество ключей и число операций)
- AWS KMS интегрирован с CloudTrail — логи в S3
- FIPS 140 — 2Level2 (Крипто-ПРО)

KMS — идеально для шифрования S3-объектов, паролей БД, API и пр.

Возможности | AWS Key Management Service (KMS)

Симметричные и асимметричные CMK

Симметричный (по умолчанию)	Асимметричный
Единый ключ для шифрования и дешифрования	Public и private-ключи
AES-256	RSA и Elliptic Curve Cryptography
Данные не покидают AWS незашифрованными	Приватный ключ не покидает AWS незашифрованным
AWS-сервисы, интегрированные с KMS, используют симметричные ключи	AWS-сервисы, созданные в KMS, не могут использовать асимметричные ключи
Должен использовать вызов API	Должен использовать вызов API, чтобы использовать **private**-ключ
Используется по умолчанию	Используется чаще всего для подписи

Шифрование бакета S3

Объекты S3 могут шифроваться:

- **на стороне клиента (Client side)—** зашифровать на стороне клиента и перенести объекты
- **на лету** — используя SSL/TLS
- **на стороне Облака (Server side)**— данные шифруются в S3:
  a. **S3 Managed Keys** — SSE-S3
  b. **AWS KMS** (в Yandex Cloud только KMS) — SSE-KMS
  c. **Customer provider keys** - SSE-C

Certificate Manager

AWS Certification Manager

ACM — это сервис, позволяющий предоставлять и развёртывать публичные и частные сертификаты Secure Sockets Layer/Transport Layer Security (SSL/TLS) для использования вместе с сервисами AWS или внутренними подключенными ресурсами, а также помогающий управлять этими сертификатами

- Централизованное управление сертификатами
- Аудит использования в CloudTrail
- Интеграция с сервисами AWS
- Публичные сертификаты SSL/TLS, выпускаемые с помощью сервиса AWS Certificate Manager, являются **бесплатными** Оплате подлежат только ресурсы AWS, используемые для запуска приложений

YC Certificate Manager

Сервис получения и обновления сертификатов от Let's Encrypt® и частные сертификаты

Сертификаты из Certificate Manager можно использовать в сервисах Yandex Cloud:

- Yandex Object Storage (HTTPS-хостинг)
- Application Load Balancer (HTTPS)
- Yandex API Gateway

Итоги

Итоги

Сегодня мы изучили:

- что такое IAM и как организовано управление пользователями
- что такое KMS, как организовано хранение и использование ключей
- что такое SSO и как используется с другими приложениями
- что такое Certificate manager, как создавать и управлять сертификатами

Домашнее задание

Домашнее задание

Ваше домашнее задание можно посмотреть по ссылке

- Вопросы по домашней работе задавайте **в чате** учебой группы
- Задачи можно сдавать **по частям**
- Задачи со звёздочкой (*) выполняются по желанию
- Зачёт по домашней работе проставляется после того, как **приняты все задачи**

нетология

Задавайте вопросы и пишите отзыв о лекции!

Елисей Ильин