3 июня 2025 Москва, LOFT HALL#2

БЕКОН '25

Конференция по БЕзопасности
КОНтейнеров и контейнерных сред

Без секретов! Workload Identity Federation: безопасная аутентификация в облаке

Дмитрий Лютов
Менеджер продуктов безопасности Yandex Cloud

TLDR

Secrets Management - #5 in Top 10 Kubernetes Security Issues by SentinelOne

Управление секретами - это сложно

Не расскажу как правильно управлять секретами в k8s

Вы итак это знаете

OpenID Connect – всех спасет!

Но это неточно

Управление секретами — боль

- Ротация
- Аудит
- Мониторинг утечек

  Репозитории

  Логи

  …

allthingswildlyconsidered.blogspot.com/2019/07/turtles-all-way-down-respect-them-all.html

OWASP® Non-Human Identity (NHI) Top 10 (2025)

NHI1: 2025 Improper Offboarding

NHI2: 2025 Secret Leakage

NHI6: 2025 Insecure Cloud Deployment Configurations

NHI7: 2025 Long-Lived Secrets

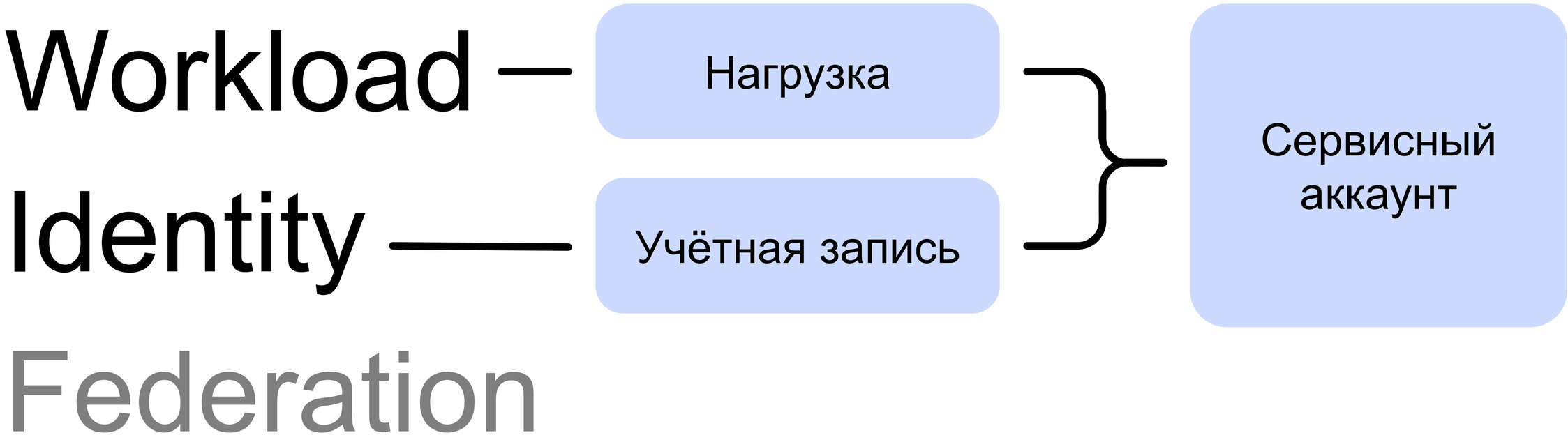
Привязка сервисного аккаунта к…

- виртуальной машине
- функции

```
vm-instance$ curl  -H Metadata-Flavor:Google 169.254.169.254/computeMetadata/v1/ins
tance/service-accounts/default/token
{"access_token":"t1.9euelZrMzM_Ky4-axo3NjY6NjpTPl-3rnpWaioyVlMqPjpPGz8eNxpqLjonl8_c
dX29e-e9MUGgQ_t3z910NbV7570xQaBD-.XnCGcW-yuM5S5CHwkWnMyiRGylk-WPf5p_PZm_vaCca9lllhD
Ii413-[redacted],"expires_in":42731,"token_type":"Bearer"}
vm-instance$
```

Workload Identity Federation одним предложением

Возможность Workload Identity из одной экосистемы получать доступ к API целевой экосистемы без необходимости хранить аутентификационные секреты целевой экосистемы


Workload
Identity
Federation
Нагрузка
Учётная запись
Сервисный аккаунт

Система	Workload Identity
Yandex Cloud	Сервисный аккаунт
Google Cloud Platform (GCP)	Service Account
Microsoft Azure	Managed Identity
Amazon Web Services (AWS)	≈ Role
Kubernetes®	Service Account

Workload Identity Federation

Федерация удостоверений

Workload Identity Federation

Yandex Cloud

Федерации сервисных аккаунтов

Google Cloud

Workload Identity Federation

aws

IAM Roles Anywhere

Azure

Workload Identity Federation

Workload Identity Federation

Гибкость

Работает с любыми провайдерами OpenID Connect

Контролируемость

Требует предварительной установки доверия

Безопасность

Не используются долгоживущие секреты

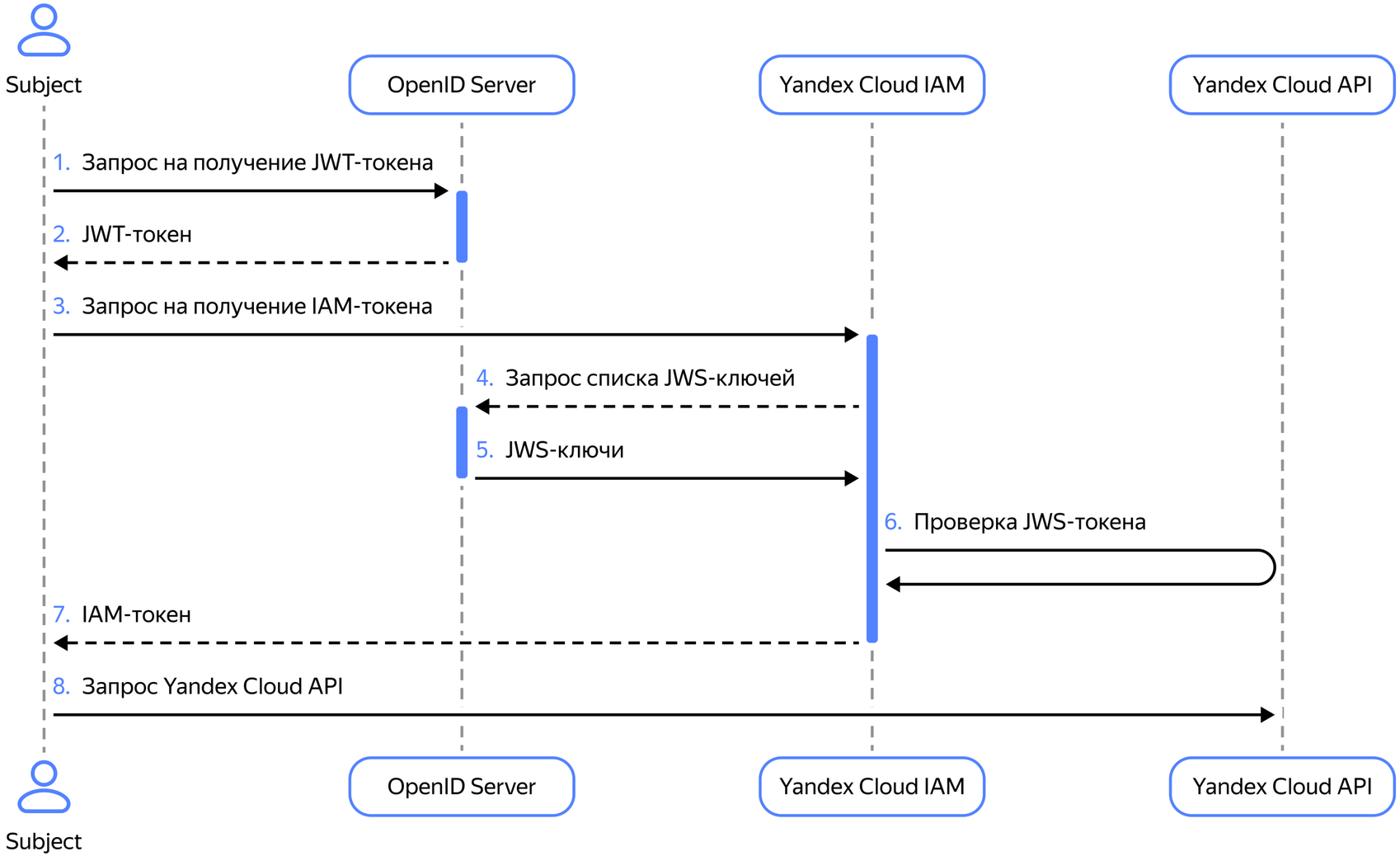
Доверие к id_token

```
{
  "alg": ”RS256",
  "typ": "JWT",
  "kid": "aGVsbG8gc2VudCBsdWlzCgo"
}.
{
  "iss": "https://idp.example.com",
  "aud": "https://relying-party.example.com",
  "sub": "identity-123",
  "iat": 1516239022,
  "exp": 1516339022,
   ...
}
```

```
{
  "keys": [
    {
      "alg": "RS256",
      "kty": "RSA",
      "kid": "aGVsbG8gc2VudCBsdWlzCgo",
      ...
    }
  ]
}
```

https://idp.example.com/.well-known/openid/jwks

Workload Identity Federation



Workload Identity Federation

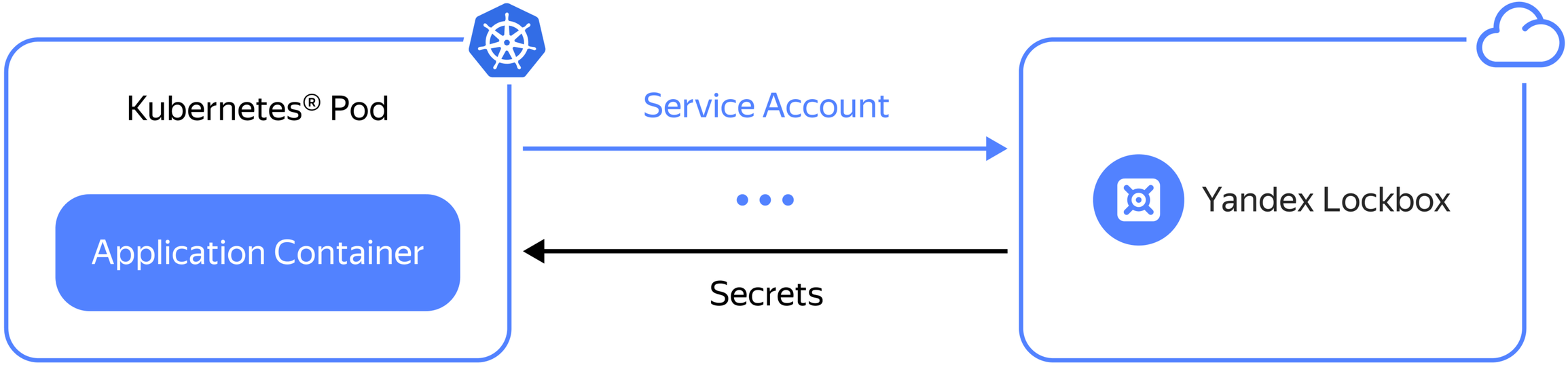
Примеры использования

CI/CD → Cloud (например, для деплоя инфраструктуры через Terraform использую GitHub Actions)

Workload Identity Federation

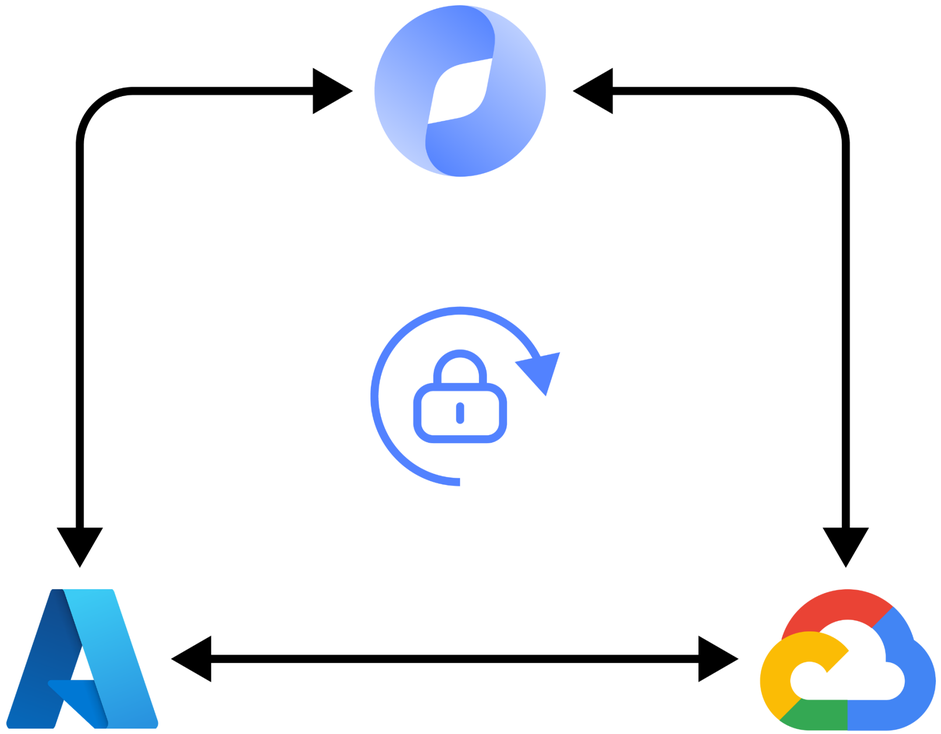
Примеры использования

K8s® → Cloud
(например, получение секретов из Yandex Lockbox)



Workload Identity Federation

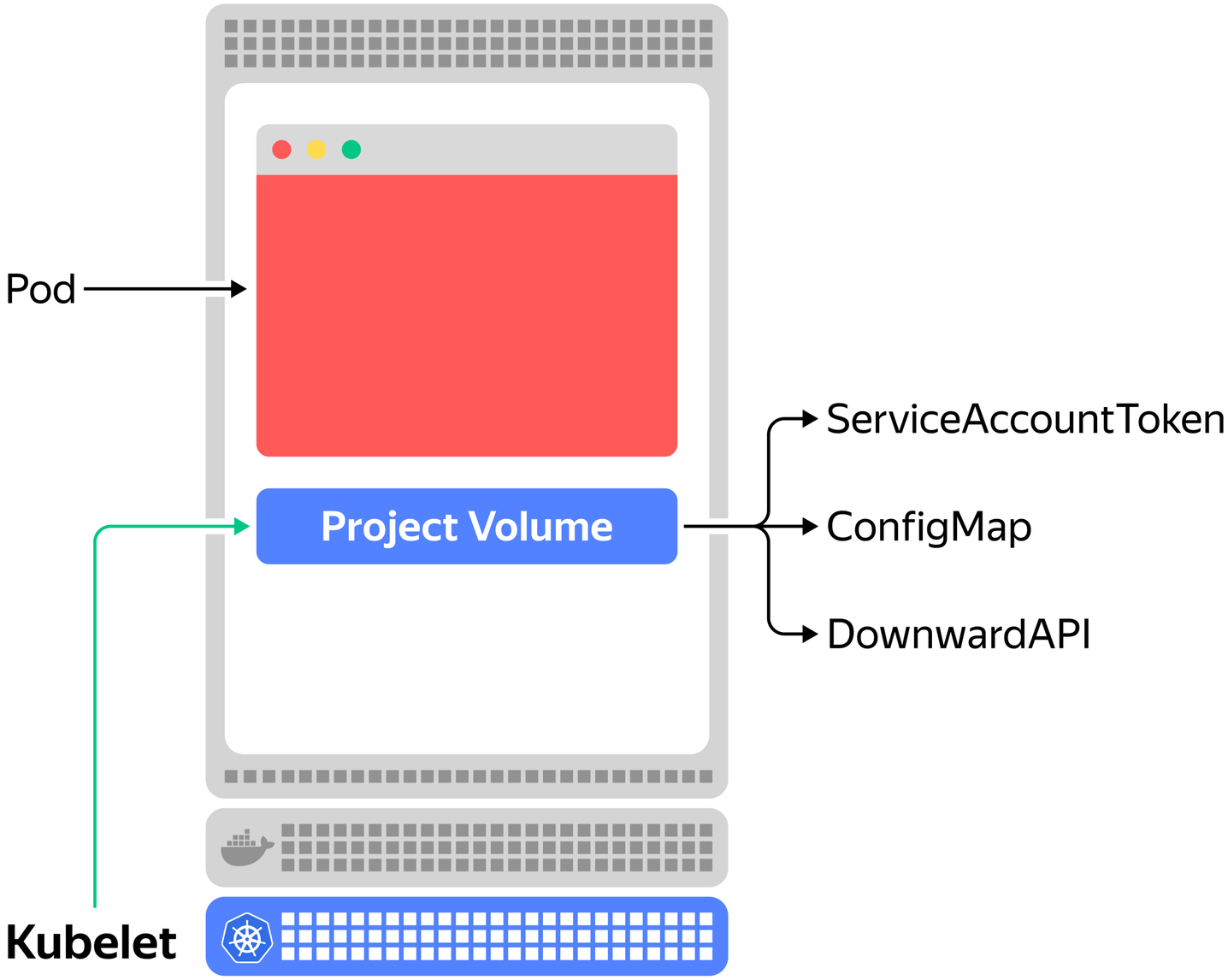
Примеры использования



Cloud → Cloud
Работа в мультиоблачных инфраструктурах (например, Google Cloud Platform → Yandex Cloud)

K8s® Demo: получение секрета Yandex Lockbox из пода

ServiceAccountToken Volume Projection (K8s® 1.24+)



K8s® Demo: получение секрета Yandex Lockbox из пода

Шаг 1. Создание пода

```
apiVersion: v1
kind: Pod
metadata:
  name: jump
  namespace: default
spec:
  containers:
  - image: smallstep/step-cli
    name: step-cli
    volumeMounts:
    - mountPath: /var/run/secrets/tokens
      name: test-token
  serviceAccountName: wli-test
  volmes:
  - name: test-token
    projected:
      sources:
      - serviceAccountToken:
          path: test-token
          expirationSeconds: 3600
          audience: test
```

HEADER: ALGORITHM & TOKEN TYPE

```
{
  "alg": "RS256",
  "kid": "UsvxJzzWFkwPsj9TB1PH0Ixf7TZ7qMg0WMQnt7fVYYw"
}
```

PAYLOAD: DATA

```
{
  "aud": [
    "test"
  ],
  "exp": 1675513281,
  "iat": 1675509681,
  "iss": "kubernetes.default.svc",
  "kubernetes.io": {
    "namespace": "default",
    "pod": {
      "name": "jump2",
      "uid": "3f086092-94fa-4aa4-9e33-86216e717a27"
    },
    "serviceaccount": {
      "name": "wli-test",
      "uid": "5a07ba73-e58d-498f-b1a6-9f9935085058"
    }
  },
  "nbf": 1675509681,
  "sub": "system:serviceaccount:default:wli-test"
}
```

K8s® Demo: получение секрета
Yandex Lockbox из пода

Шаг 2. Сбор данных кластера

Получаем значение Issuer для кластера:

```
kubectl get --raw /.well-known/openid-configuration | jq -r .issuer
(default - https://kubernetes.default.svc.cluster.local)
```

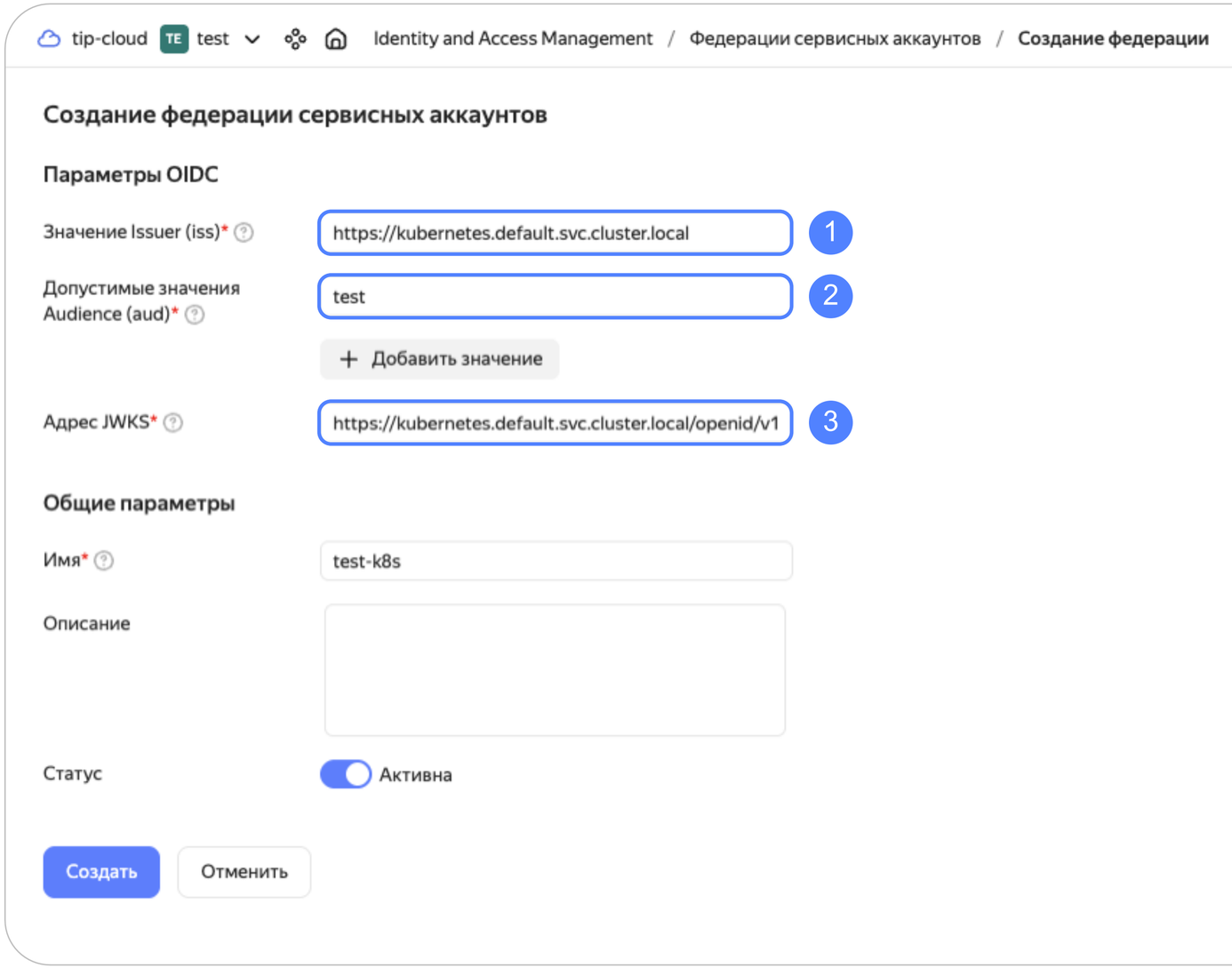
Получаем JWKS-файл (опционально для непубличных кластеров):

```
kubectl get --raw /openid/v1/jwks > cluster-jwks.json
```

K8s® Demo: получение секрета Yandex Lockbox из пода

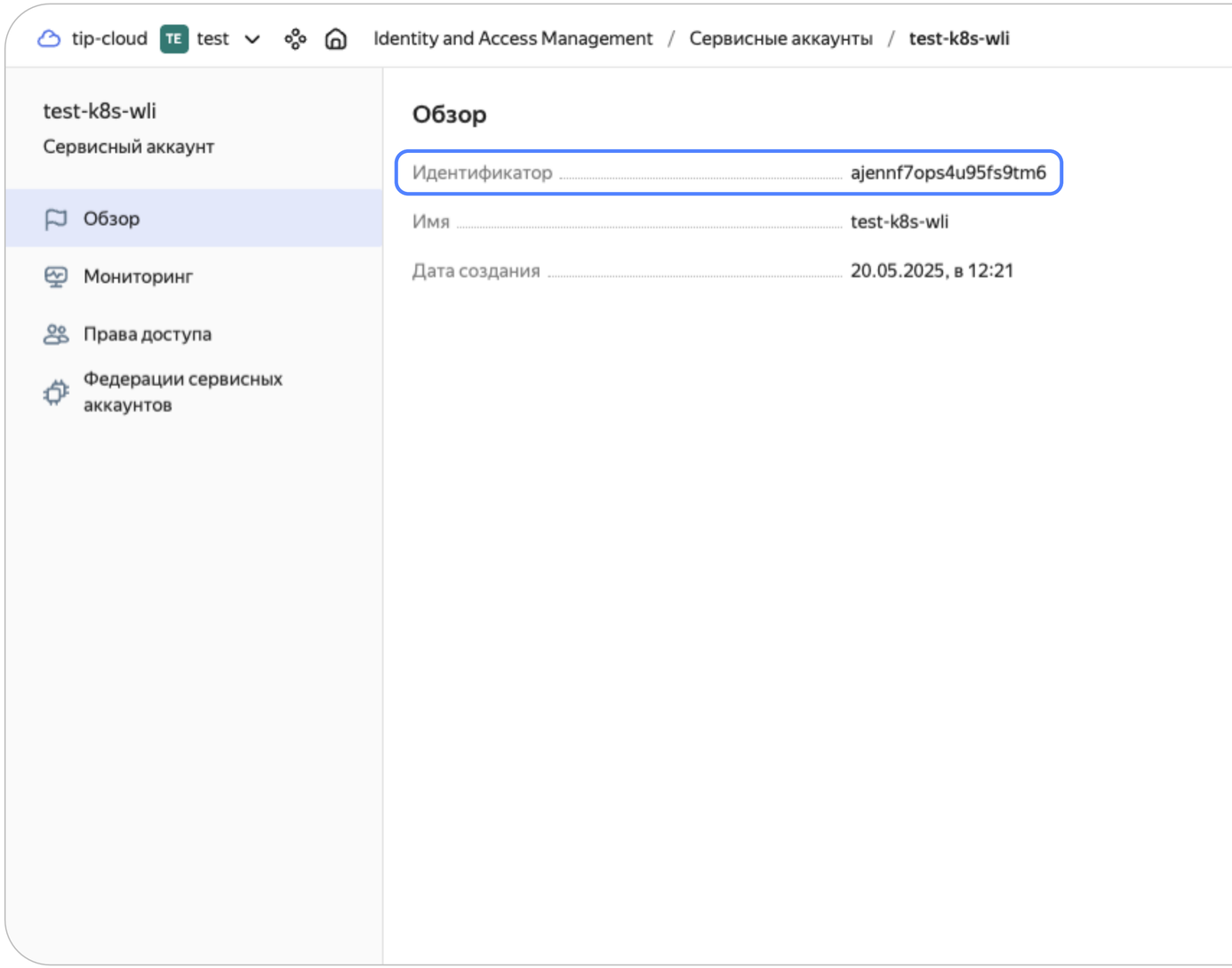
Шаг 3. Настройка федерации в Yandex Cloud

1. Получен на шаге 2
2. Задан на шаге 1
3. Получен на шаге 2



K8s® Demo: получение секрета Yandex Lockbox из пода

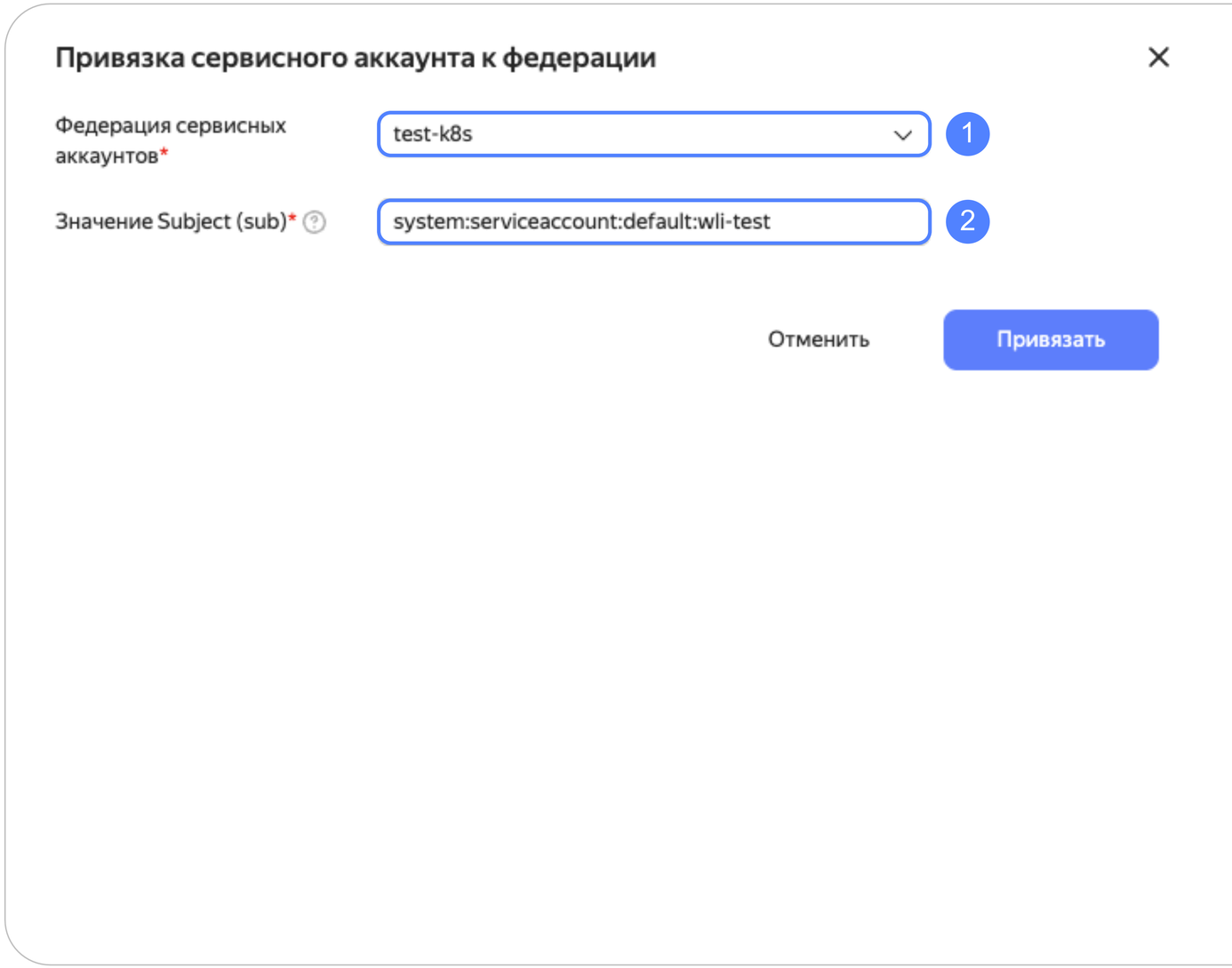
Шаг 4. Создание сервисного аккаунта в Yandex Cloud



K8s® Demo: получение секрета Yandex Lockbox из пода

Шаг 5. Привязка федерации к сервисному аккаунту

1. Создана на шаге 3
2. Определено на шаге 1



K8s® Demo: получение секрета
Yandex Lockbox из пода

Шаг 6. Получение секрета Yandex Lockbox

Заполняем необходимые переменные:

```
SA_ID=<идентификатор_сервисного_аккаунта>
SECRET_ID=<идентификатор_секрета>
```

Получаем токен K8s® ServiceAccount внутри пода:

```
SA_TOKEN=`cat /var/run/secrets/tokens/test-token`
```

K8s® Demo: получение секрета
Yandex Lockbox из пода

Шаг 6. Получение секрета Yandex Lockbox

Обмениваем ID-токен на облачный IAM-токен:

```
IAMTOKEN=$(curl -sH "Content-Type: application/x-www-form-urlencoded”
           -d "grant_type=urn:ietf:params:oauth:grant-type:token-exchange
               &requested_token_type=urn:ietf:params:oauth:token-type:access_token
               &audience=$SA_ID
               &subject_token=$SA_TOKEN
               &subject_token_type=urn:ietf:params:oauth:token-type:id_token”
           -X POST https://auth.yandex.cloud/oauth/token | jq -r '.access_token’)
```

K8s® Demo: получение секрета
Yandex Lockbox из пода

Шаг 6. Получение секрета Yandex Lockbox

Получаем значение секрета:

```
SECRET_DATA=$(curl -sH "Authorization: Bearer ${IAMTOKEN}"
https://payload.lockbox.api.cloud.yandex.net/lockbox/v1/secrets/$SECRET_ID/payload)
echo ${SECRET_DATA}
```

```
{
  "entries": [
    {
      "key": "secret",
      "textValue": "67cH2£?pO********"
    }
  ],
  "versionId": "e6q8isknpcp7********"

}
```

Workload Identity Federation + k8s

Поддержка k8s (1.24+)

Работает с любыми k8s кластерами в том числе с приватными

Managed Service for k8s

В разработке

External Secrets Operator (Yandex Cloud provider)

В разработке

Call to Action

Минимизируйте использование долгоживущих кредов

Контролируйте использование ключей

Используйте Workload Identity Federation


3 июня 2025 Москва, LOFT HALL#2
Конференция по БЕзопасности
КОНтейнеров и контейнерных сред
БЕКОН
LUNTRY
@tip_ikt
dlyutov@yandex-yeam.ru
https://yandex.cloud