7 июня 2023 Москва, МЦК ЗИЛ

БЕКОН'23

Первая в России конференция
по БЕзопасности КОНтейнеров и контейнерных сред

Kubernetes, ответь мне: кто я для тебя?

Аксёнов Константин

Руководитель разработки Deckhouse
Kubernetes Platform, Флант

Обо мне

БЕКОН

Константин Аксёнов

Руководитель разработки
Deckhouse Kubernetes Platform

konstantin.aksenov@flant.com

github.com/**konstantin-axenov**

Чем занимаюсь

Больше 5 лет засыпаю и просыпаюсь с мыслями о Kubernetes.

Опыт

С 2011 занимаюсь разработкой.

С 2017 работаю в компании **«Флант»**.

С 2020 руководитель разработки **Deckhouse Kubernetes Platform**.

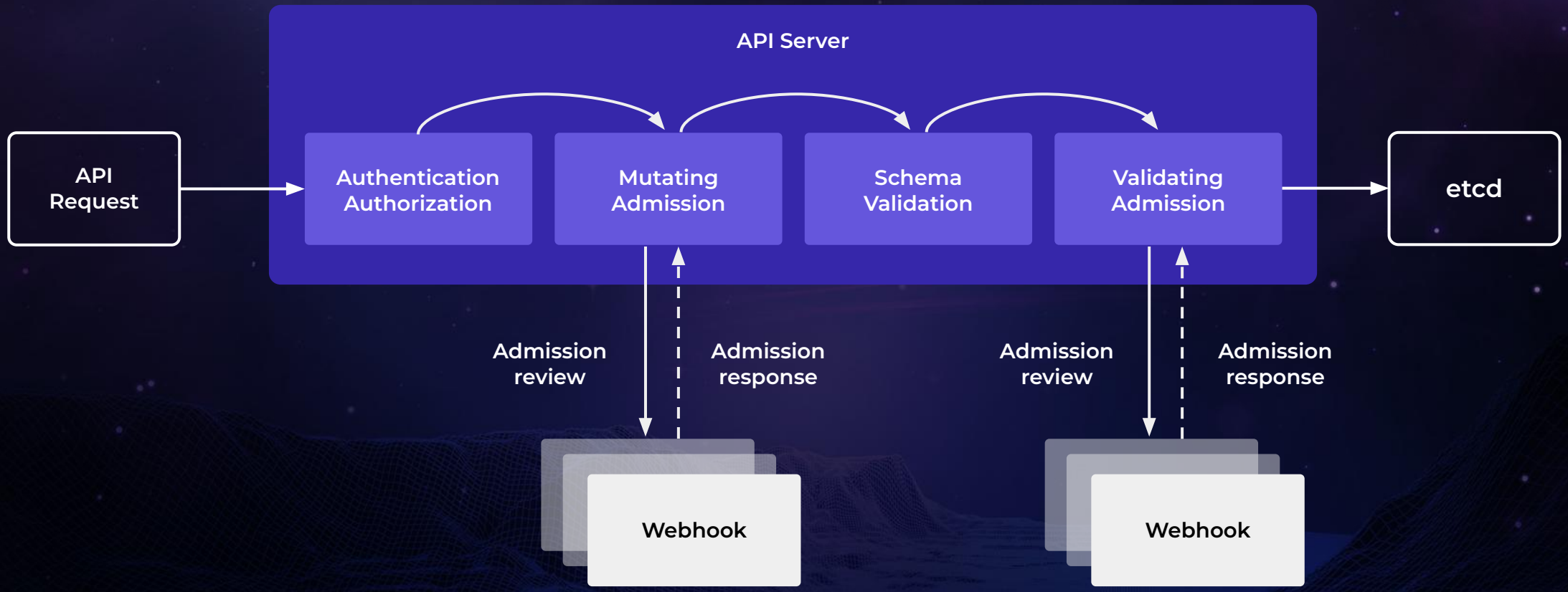
С чем работаю больше всего

kubernetes

FLANT Deckhouse Kubernetes Platform

Всё начинается с аутентификации

БЕКОН



План

- Определение аутентификации
- Принцип работы аутентификации в Kubernetes
- Проблемы и способы диагностики
- Новые “фичи” в Kubernetes для аутентификации

Что такое аутентификация?

БЕКОН

С древних времён перед людьми стояла довольно сложная задача — убедиться в **достоверности** важных сообщений.

Аутентификация — процесс, в ходе которого мы можем убедиться в подлинности чего-либо.

Примеры:

- Проверка паспорта в аэропорту
- Дверной замок

Что такое аутентификация (IT version)?

БЕКОН

Процесс получения **доступа к сервису** путем отправки ранее выданных “доказательств”.

Примеры:

- Ввод **логина** и **пароля** в форму.
- **Приложения** для аутентификации на мобильном телефоне.
- Кнопка “Войти **через Google**”.

Рассмотрим, что это такое, на примере известного сервиса — **Kubernetes API.**

Kubernetes

БЕКОН

Внутри Kubernetes **нет сущности “пользователь”**.

Вместо этого Kubernetes полагается на различные источники аутентификации, или **аутентификаторы**.

Аутентификатор возвращает нам **пользовательские атрибуты**:

- Имя
- Группы
- Уникальный идентификатор
- Экстра (карта дополнительных атрибутов)

Рассмотрим **существующие аутентификаторы**.

Варианты аутентификации

БЕКОН

- **Для сервисов**
  - Service Account Tokens
  - Bootstrap Tokens
- **Для обычных пользователей**
  - Static Token File
  - X509 Client Certs
  - OpenID Connect Tokens
  - Authenticating Proxy
  - Webhook Token Authentication

X509 Client Certs

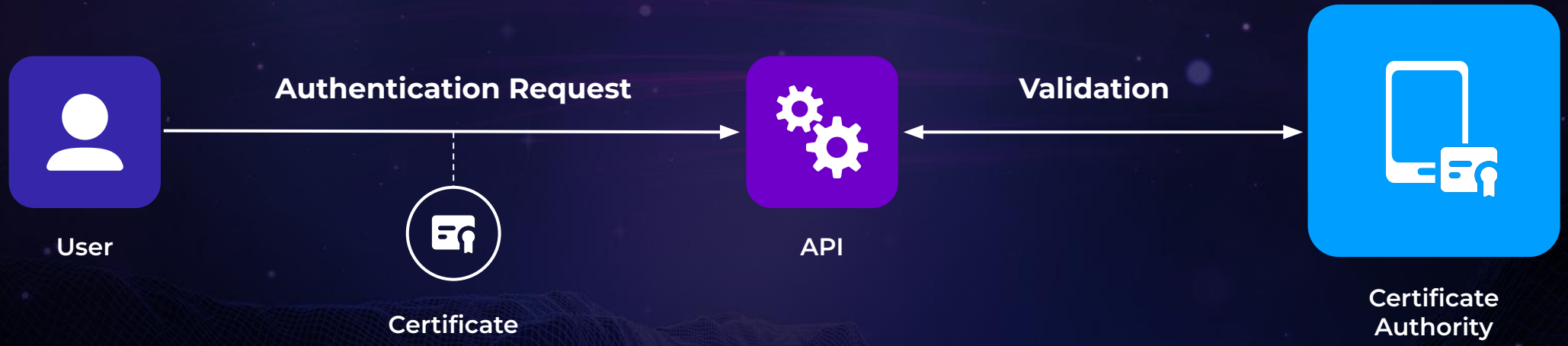
БЕКОН

В сертификате определены **пользователь** (Common Name) и **группа** (Organization)

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            9f:a8:78:7e:b3:70:6e:5e:ec:96:d7:df:44:90:15:45
        Signature Algorithm: sha256WithRSAEncryption
        Issuer: CN = kubernetes
        Validity
            Not Before: Jun  2 09:38:39 2023 GMT
            Not After : Jun  1 09:38:39 2024 GMT
        Subject: O = team-developers, CN = batman
```

X509 Client Certs

БЕКОН



После аутентификации

БЕКОН

В кластере существуют ClusterRole или Role

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: node-reader
rules:
- apiGroups: [""]
  resources: ["nodes"]
  verbs: ["get", "watch", "list"]
```

После аутентификации

БЕКОН

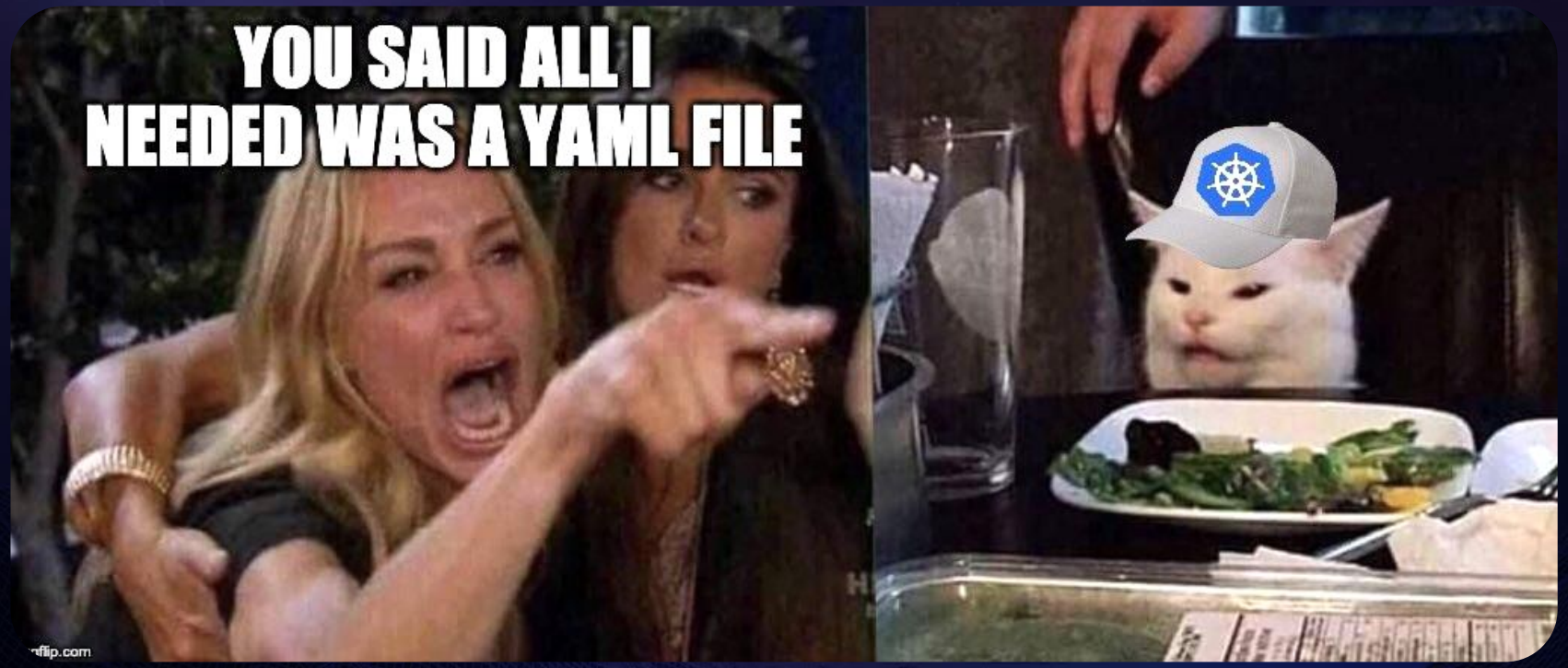
- RoleBinding или ClusterRoleBinding связаны с Role и ClusterRole
- В поле subjects указан список, который может содержать kind User, Group или ServiceAccount

```yaml
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRole
metadata:
  name: node-reader
...
---
apiVersion: rbac.authorization.k8s.io/v1
kind: ClusterRoleBinding
metadata:
  name: team-developers-node-reader
subjects:
- kind: Group
  name: team-developers
  apiGroup: rbac.authorization.k8s.io
roleRef:
  kind: ClusterRole
  name: node-reader
  apiGroup: rbac.authorization.k8s.io
```

После аутентификации

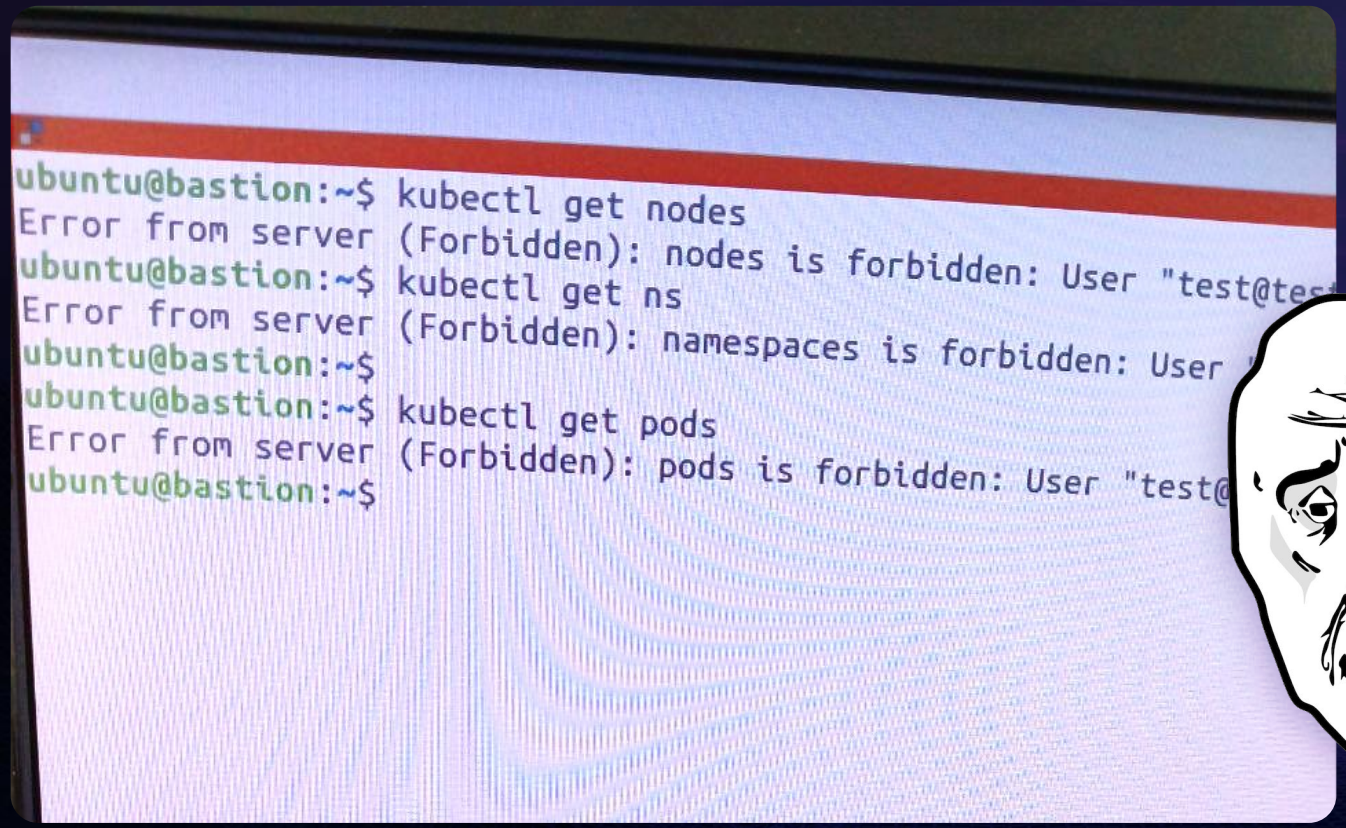
Проверяем, что всё получилось

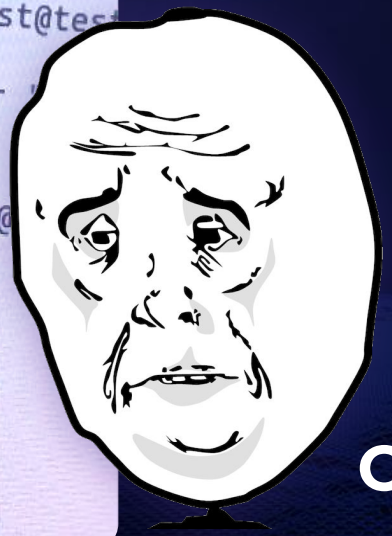
```
kubectl auth can-i get nodes -A
yes

kubectl auth can-i --list=true
Warning: the list may be incomplete: webhook authorizer does not support user rule resolution
Resources                                       Non-Resource URLs   Resource Names   Verbs
selfsubjectreviews.authentication.k8s.io        []                  []               [create]
selfsubjectaccessreviews.authorization.k8s.io   []                  []               [create]
selfsubjectrulesreviews.authorization.k8s.io    []                  []               [create]
nodes                                           []                  []               [get watch list]
                                                [/api/*]            []               [get]
                                                [/api]              []               [get]
...
```


YOU SAID ALL I
NEEDED WAS A YAML FILE

Личная боль

- Deckhouse Kubernetes Platform **очень часто** используют в закрытых окружениях
- **Диагностировать** проблему приходится **по фотографии**





Okay

Личная боль

БЕКОН

Надо найти **группы пользователя**, которые мы получили от провайдера:

- Но у пользователя **не работает** kubectl 🥲
- Логи могли отротироваться, **надо объяснить**, что нужно сделать *logout/login*

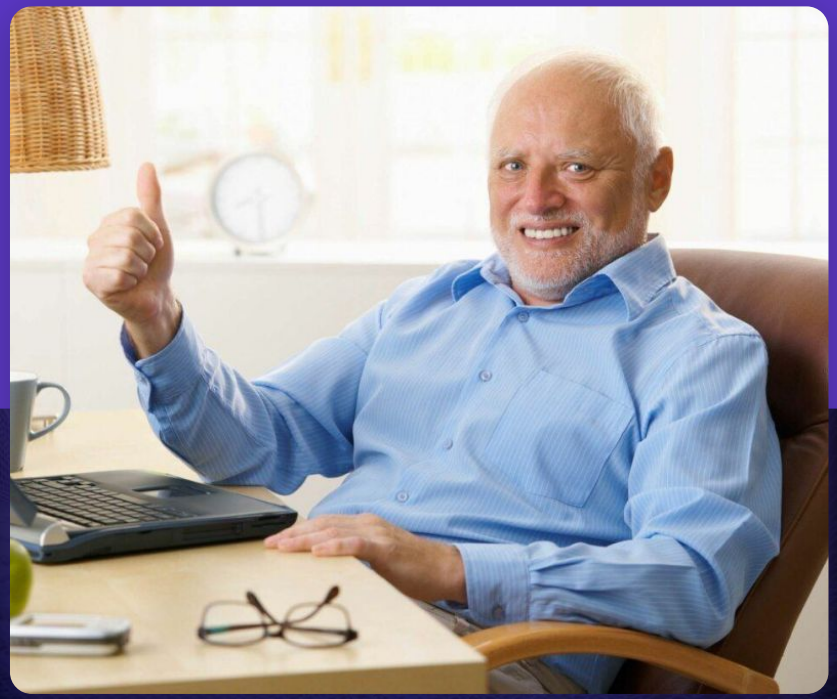
```
kubectl -n d8-user-authn logs -l app=dex --tail 10000 -c dex | grep login | grep "test@test.test"
{"level":"info","msg":"login successful: connector \"gitlab-local\", username=\"test@test.test\",
preferred_username=\"\", email=\"test@test.test\", groups=[\"team/bravo\" \"team/echo\"
\"team/charlie\" \"team/foxtrot\"]","time":"2023-05-27T08:34:57Z"}
```

Личная боль

БЕКОН

- **Неопределённость** в kubeconfig
- Какой будет **приоритет** у методов аутентификации?
- Как такое **диагностировать**?

```
users:
- name: aks
  user:
    token: MY_TOKEN
    client-certificate-data: MY_CRT
    client-key-data: MY_KEY
```



Новые возможности

БЕКОН

- KEP 3325 решает проблему
- В 1.26 в Alpha, в 1.27 в Beta, в 1.28 планируется в Stable

```
kubectl auth whoami
ATTRIBUTE   VALUE
Username    batman
Groups      [team-developers system:authenticated]
```

Новые возможности

БЕКОН

SelfSubjectReview API

```
kubectl create --raw '/apis/authentication.k8s.io/v1beta1/selfsubjectreviews' -f - <<EOF
{
  "apiVersion": "authentication.k8s.io/v1beta1",
  "kind": "SelfSubjectReview"
}
```

Новые возможности

БЕКОН

SelfSubjectReview API

```
{
    "kind": "SelfSubjectReview",
    "apiVersion": "authentication.k8s.io/v1beta1",
    "metadata": {
        "creationTimestamp": "2023-06-02T09:40:04Z"
    },
    "status": {
        "userInfo": {
            "username": "batman",
            "groups": [
                "team-developers",
                "system:authenticated"
            ]
        }
    }
}
```

Как включить whoami

БЕКОН

Kubernetes 1.26

- --feature-gates=APISelfSubjectReview=true
- --runtime-config=authentication.k8s.io/v1alpha1
- kubectl alpha auth whoami

Kubernetes 1.27

- --runtime-config=authentication.k8s.io/v1beta1

Вопрос, который мучает всех

БЕКОН

Какой **вид аутентификации** для пользователей выбрать?

Что лучше: **сертификаты** или **сервисные аккаунты**?

Варианты аутентификации

БЕКОН

- **Для сервисов**
  - Service Account Tokens
  - Bootstrap Tokens
- **Для обычных пользователей**
  - Static Token File
  - X509 Client Certs
  - OpenID Connect Tokens
  - Authenticating Proxy
  - Webhook Token Authentication

Варианты аутентификации

БЕКОН

- **Для сервисов**
  - ~~Service Account Tokens~~
  - ~~Bootstrap Tokens~~
- **Для обычных пользователей**
  - Static Token File
  - X509 Client Certs
  - OpenID Connect Tokens
  - Authenticating Proxy
  - Webhook Token Authentication

Варианты аутентификации

БЕКОН

- **Для сервисов**
  - ~~Service Account Tokens~~
  - ~~Bootstrap Tokens~~
- **Для обычных пользователей**
  - ~~Static Token File~~ нельзя использовать для **production** (CIS Benchmark)
  - X509 Client Certs
  - OpenID Connect Tokens
  - Authenticating Proxy
  - Webhook Token Authentication

Варианты аутентификации

БЕКОН

- **Для сервисов**
  - ~~Service Account Tokens~~
  - ~~Bootstrap Tokens~~
- **Для обычных пользователей**
  - ~~Static Token File~~ нельзя использовать для **production** (CIS Benchmark)
  - ~~X509 Client Certs~~ сложно выпускать, **невозможно отозвать** сертификат
  - OpenID Connect Tokens
  - Authenticating Proxy
  - Webhook Token Authentication

Варианты аутентификации

БЕКОН

- **Для сервисов**
  - ~~Service Account Tokens~~
  - ~~Bootstrap Tokens~~
- **Для обычных пользователей**
  - ~~Static Token File~~ нельзя использовать для **production** (CIS Benchmark)
  - ~~X509 Client Certs~~ сложно выпускать, **невозможно отозвать** сертификат
  - ~~OpenID Connect Tokens~~
  - ~~Authenticating Proxy~~
  - ~~Webhook Token Authentication~~

Structured Authentication Config

БЕКОН

В работе [KEP 3331]

- Можно использовать **не только** OIDC ID JWT
- Динамическое изменение конфигурации
- Одновременное подключение нескольких провайдеров
- Использование CEL (Common Expression Language)
  - Правила валидации при аутентификации
  - Правила извлечения информации о пользователе из claim’ов токена

Structured Authentication Config

БЕКОН

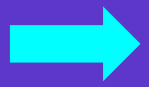
```yaml
apiVersion: apiserver.config.k8s.io/v1alpha1
kind: AuthenticationConfiguration
jwt:
- issuer:
    url: https://example.com
    clientIDs:
    - my-app
  claimMappings: {...}
  claimValidationRules: [...]
  userInfoValidationRules: [...]
```

Правила извлечения информации о пользователе

БЕКОН

```yaml
claimMappings:
  username:
    expression: 'claims.username + ":external-user"'
  groups:
    expression: 'claims.roles.split(",")'
  uid:
    claim: 'sub'
  extra:
  - key: '"client_name"'
    value: 'claims.aud'
```

```
{
  "sub": "119abc",
  "aud": "kubernetes",
  "username": "jane_doe",
  "roles": "admin,user",
  ...
}
```

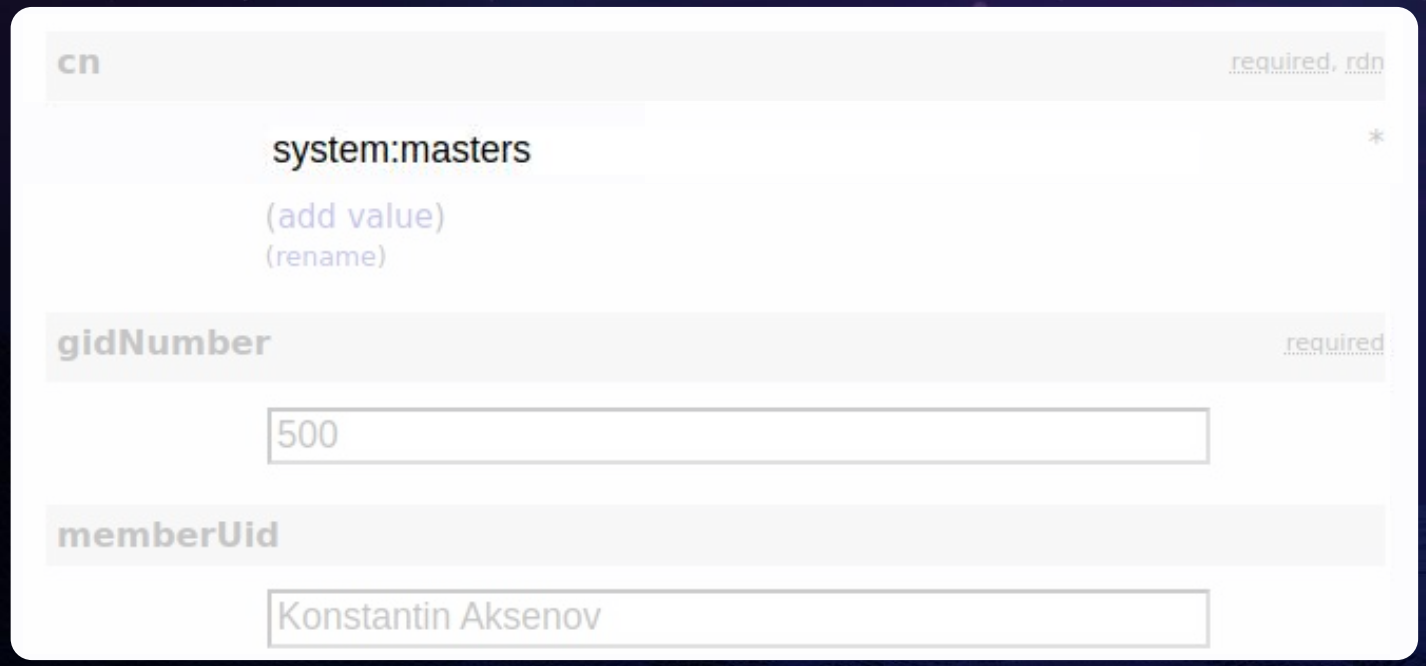


```yaml
username: jane_doe:external-user
uid: "119abc"
groups: ["admin", "user"]
extra:
  client_name: kubernetes
```

Правила валидации при аутентификации

БЕКОН

Префикс **system:** зарезервирован для внутреннего использования в Kubernetes, вы должны убедиться, что у вас **случайно** не используются пользователи или группы, имена которых начинаются с **system:**



Правила валидации при аутентификации

БЕКОН

Префикс **system:** зарезервирован для внутреннего использования в Kubernetes, вы должны убедиться, что у вас **случайно** не используются пользователи или группы, имена которых начинаются с **system:**

```
{"level":"info","msg":"login successful: connector \"ldap-local\", username=\"kaksenov\",
preferred_username=\"\", email=\"konstantin.aksenov@flant.com\", groups=[\"system:masters\"
\"developers:maintainers\"]","time":"2023-06-01T19:12:09Z"}

ATTRIBUTE   VALUE
Username    konstantin.aksenov@flant.com
Groups      [system:masters developers:maintainers system:authenticated]
```

Правила валидации при аутентификации

БЕКОН

Префикс **system:** зарезервирован для внутреннего использования в Kubernetes, вы должны убедиться, что у вас **случайно** не используются пользователи или группы, имена которых начинаются с **system:**

```
{"level":"info","msg":"login successful: connector \"ldap-local\", username=\"kaksenov\",
preferred_username=\"\", email=\"konstantin.aksenov@flant.com\", groups=[\"system:masters\"
\"developers:maintainers\"]","time":"2023-06-01T19:12:09Z"}

ATTRIBUTE   VALUE
Username    konstantin.aksenov@flant.com
Groups      [system:masters developers:maintainers system:authenticated]

kubectl auth can-i '*' '*'
yes
```

Правила валидации при аутентификации

БЕКОН

Для решения есть следующие варианты

- Задать префикс через параметр --oidc-groups-prefix
- Например, в Dex у коннекторов есть фильтр для групп

```
connectors:
  - type: gitlab
    id: gitlab
    name: GitLab
    config:
      # If `groups` is provided, this acts as a whitelist - only the user's GitLab groups that
are in the configured `groups` below will go into the groups claim.  Conversely, if the user is
not in any of the configured `groups`, the user will not be authenticated.
      groups:
      - my-group
```

Правила валидации при аутентификации

БЕКОН

```yaml
claimValidationRules:
- claim: hd
  requiredValue: example.com
- expression: 'claims.hd == "example.com"'
  message: the hd claim must be set to example.com
- expression: 'claims.exp - claims.nbf <= 86400'
  message: total token lifetime must not exceed 24 hours
```

```yaml
userInfoValidationRules:
- rule: "!userInfo.username.startsWith('system:')"
  message: username cannot used reserved system: prefix
- rule: "userInfo.groups.all(group, !group.startsWith('system:'))"
  message: groups cannot used reserved system: prefix
```

Правила валидации при аутентификации

БЕКОН

```yaml
claimValidationRules:
- claim: hd
  requiredValue: example.com
- expression: 'claims.hd == "example.com"'
  message: the hd claim must be set to example.com
- expression: 'claims.exp - claims.nbf <= 86400'
  message: total token lifetime must not exceed 24 hours
```

```yaml
userInfoValidationRules:
- rule: "!userInfo.username.startsWith('system:')"
  message: username cannot used reserved system: prefix
- rule: "userInfo.groups.all(group, !group.startsWith('system:'))"
  message: groups cannot used reserved system: prefix
```

Kubernetes SIG Auth Deep Dive KubeCon EU 2023

БЕКОН

Enhancements

KubeCon CloudNativeCon Europe 2023

Stable

- 2799 Reduce legacy service account token attack surface area
  - Stop auto-generating legacy tokens (beta v1.24, stable v1.26)

Implementable

- 2799 Reduce legacy service account token attack surface area
  - Track use of legacy tokens (beta v1.27, targeting stable v1.28)
  - Clean up unused legacy tokens (targeting alpha v1.28)
- 3325 API to get current user attributes, `kubectl whoami` (beta v1.27, targeting stable v1.28)
- 3299 KMS v2 encryption at rest (beta v1.27, targeting stable v1.29)
- 3257 Cluster Trust Bundles (API alpha in v1.27, targeting volume mount alpha in v1.28)

Provisional

- 3221 Structured Authorization Configuration (in design, targeting alpha v1.28)
- 3331 Structured OIDC Configuration (in design, targeting alpha v1.28)
- 3766 ReferenceGrant (in design)
- 2718 Client Exec Proxy (in design)

Источник: Презентация Kubernetes SIG Auth Deep Dive

Кому поставить лайк

БЕКОН

Максим Набоких

github.com/**nabokihms**

- Участник рабочей группы Kubernetes sig-auth
- Maintainer провайдера аутентификации Dex

dex

github.com/dexidp/dex

Материалы

БЕКОН

- **Документация Kubernetes**
  https://kubernetes.io/docs/reference/access-authn-authz/authentication/
- **Документация по модулю аутентификации в Deckhouse**
  https://deckhouse.ru/documentation/v1/modules/150-user-authn/
- **Видео доклада Kubernetes SIG Auth Deep Dive**
  https://kccnceu2023.sched.com/event/1HyTv
- **Презентация Kubernetes SIG Auth Deep Dive**
  https://static.sched.com/hosted_files/kccnceu2023/35/SIG-Auth%20Deep%20Dive%20CloudNativeCon%20EU%202023.pdf

7 июня 2023 Москва, МЦК ЗИЛ

Первая в России конференция
по БЕзопасности КОНтейнеров и контейнерных сред

БЕКОН

Спасибо за внимание

Контакты:

konstantin.aksenov@flant.com

konstantin_aksenov

deckhouse.ru