

DevOops 2023

# Security для бедных без ущерба для DevEx

Игорь Кудрин, CIO  
mindbox



# Кто такие mindbox

200 млн

профилей клиентов

40

кластеров kubernetes

260 ТБ

данных в реляционных хранилищах

160

разработчиков

16

SRE/DevOps

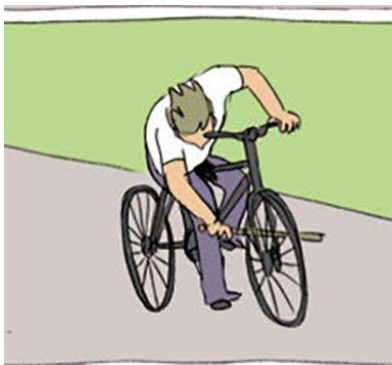
0

безопасников в пиджаках

# Чтобы что?



Выполняем требования сертификаций.  
Не геймим.



Не мешаем людям работать.

# Вижен

Доступы по запросу.

Автоматически.

Доступ временный

```
tsh request create --roles=k8s-admin --reason="скриншот для доклада"
```

```
Creating request...
```

```
Request ID: 2762f757-2b8e-4d57-94b0-3212a2abfc97
```

```
Username: clain23
```

```
Roles: k8s-admin
```

```
Reason: "скриншот для доклада"
```

```
Reviewers: [none] (suggested)
```

```
Access Expires: 2023-08-16 04:37:26
```

```
Status: APPROVED
```

```
hint: use 'tsh login --request-id=<request-id>' to login with an approved request
```


```
Waiting for request approval...
```

```
Approval received, reason="Approve for any reason"
```

```
Getting updated certificates...
```

Все аудирруется

# it-sec-teleport

 Доступ к кластерам k8s +



teleport-auto-approve APP 16:38

Today

 APPROVED

User clain23, request reason: скриншот для доклада, env: yandex-cloud

# Сегодня в программе

- SaaS
- VPN
- SSH и RDP
- Kubernetes
- Privileged access management (PAM)
- Databases
- Pipelines

# SAML – это дорого

SCIM еще дороже 😞



## Plus

A place for small groups to plan & get organized.

### \$8

per user / month  
billed annually  
\$10 billed monthly

[Get started](#)

#### Everything in Free, and

- ✓ Unlimited blocks for teams
- ✓ Unlimited file uploads
- ✓ 30 day page history
- ✓ Invite 100 guests



## Business

For companies using Notion to connect several teams & tools.

### \$15

per user / month  
billed annually  
\$18 billed monthly

[Get started](#)

[or Request a Trial](#)

#### Everything in Plus, and

- ✓ SAML SSO
- ✓ Private teamspaces
- ✓ Bulk PDF export
- ✓ Advanced page analytics
- ✓ 90 day page history
- ✓ Invite 250 guests



## Enterprise

Advanced controls & support to run your entire organization.



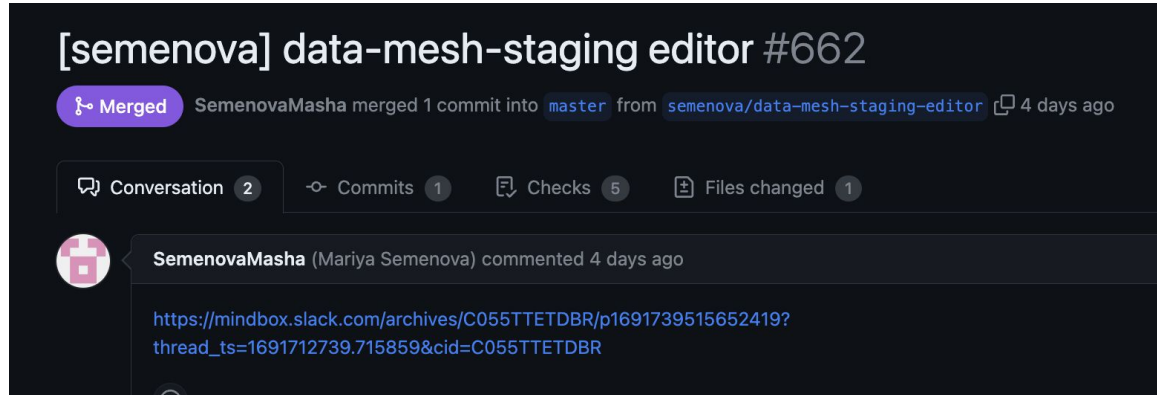
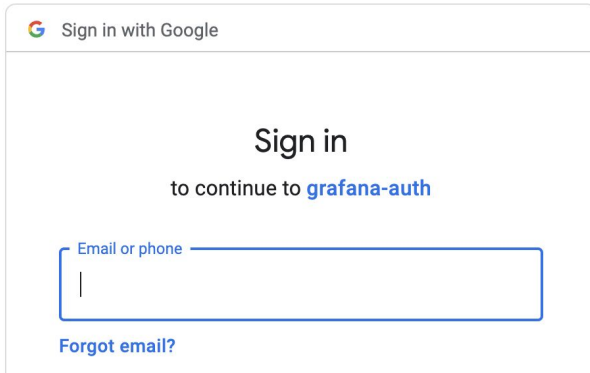
[Request a demo](#)

[or Request a Trial](#)

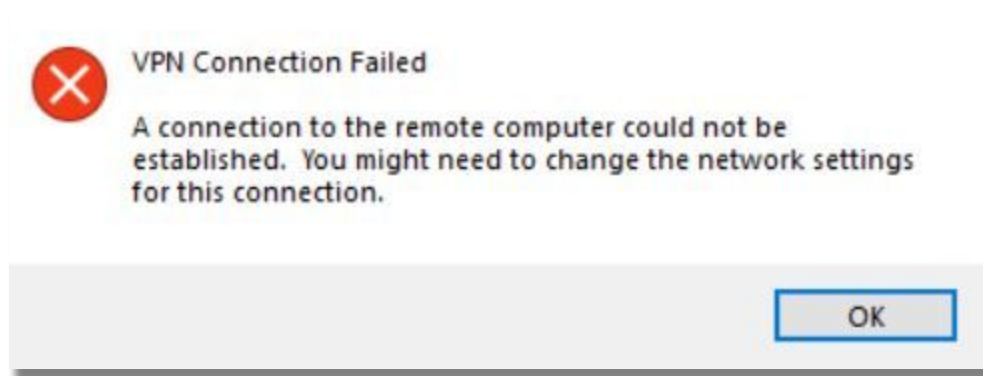
#### Everything in Business, and

- ✓ User provisioning (SCIM)
- ✓ Advanced security & controls
- ✓ Audit log
- ✓ Customer success manager
- ✓ Workspace analytics
- ✓ Unlimited page history
- ✓ Invite 250 guests

# OAuth + Terraform



# VPN дает доступ в периметр





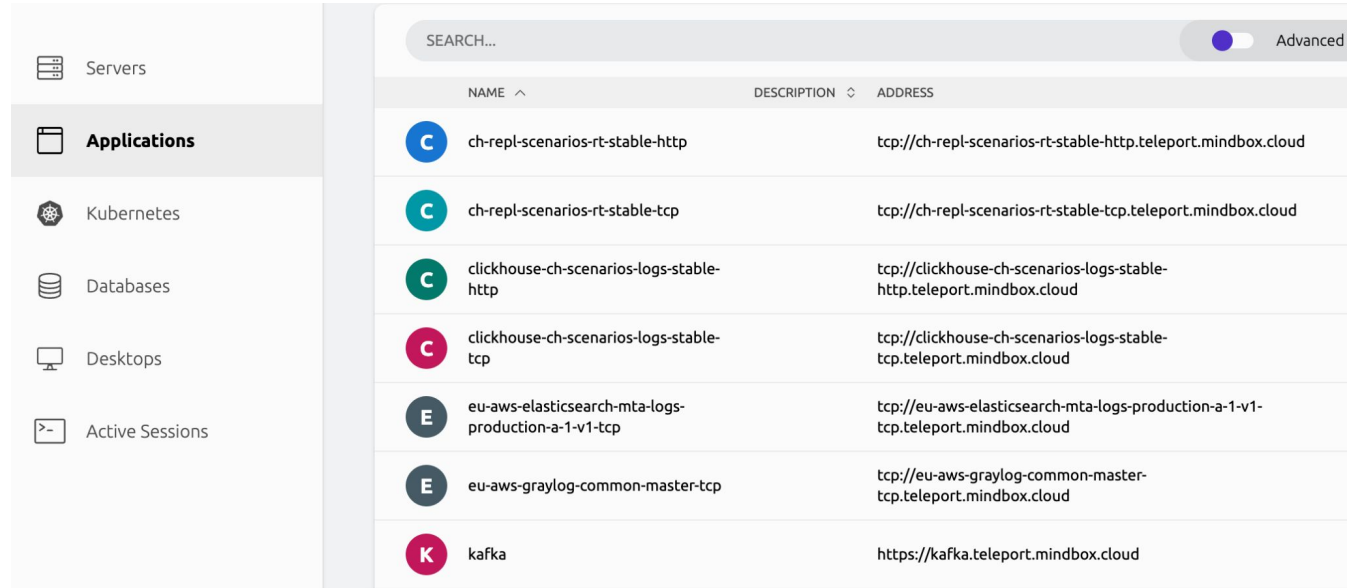
# Zero Trust

2FA

RBAC

Audit

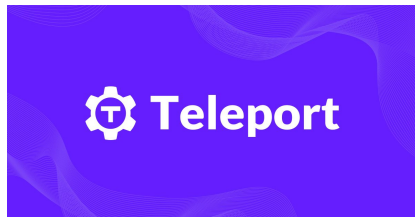
Short-lived



The screenshot shows a management console interface. On the left is a sidebar with navigation items: Servers, Applications (selected), Kubernetes, Databases, Desktops, and Active Sessions. The main area features a search bar and an 'Advanced' toggle. Below is a table listing applications with columns for Name, Description, and Address.

NAME ^	DESCRIPTION ↕	ADDRESS
<b>C</b> ch-repl-scenarios-rt-stable-http		tcp://ch-repl-scenarios-rt-stable-http.teleport.mindbox.cloud
<b>C</b> ch-repl-scenarios-rt-stable-tcp		tcp://ch-repl-scenarios-rt-stable-tcp.teleport.mindbox.cloud
<b>C</b> clickhouse-ch-scenarios-logs-stable-http		tcp://clickhouse-ch-scenarios-logs-stable-http.teleport.mindbox.cloud
<b>C</b> clickhouse-ch-scenarios-logs-stable-tcp		tcp://clickhouse-ch-scenarios-logs-stable-tcp.teleport.mindbox.cloud
<b>E</b> eu-aws-elasticsearch-mta-logs-production-a-1-v1-tcp		tcp://eu-aws-elasticsearch-mta-logs-production-a-1-v1-tcp.teleport.mindbox.cloud
<b>E</b> eu-aws-graylog-common-master-tcp		tcp://eu-aws-graylog-common-master-tcp.teleport.mindbox.cloud
<b>K</b> kafka		https://kafka.teleport.mindbox.cloud

# SSH и RDP



Revoke при увольнении

Passwordless

Session recording

2FA

Mass SSH



# PAM

## RBAC

Членство в группе as code  
опционально CODEOWNERS

Не sudo a specific rights  
например kafka-maintenance

```
- organization: mindbox-cloud
  team: flant
  roles:
    - flant
- organization: mindbox-cloud
  team: product-cdp-admin
  roles:
    - product-cdp-admin
    - apps-all
- organization: mindbox-cloud
  team: it
  roles:
    - k8s-dev
- organization: mindbox-cloud
  team: devwip
  roles:
    - k8s-viewer
```

# Kubernetes

Clusters None ▾

## CLUSTER RESOURCES

Namespaces

Nodes

PersistentVolumes

## META

Resource Types

kube-infra

## kube-infra

API URL: https://not.you.business

### Namespaces

	Name	Labels
<input type="checkbox"/>	<a href="#">alertmanager-global</a>	kind: system   kubernetes.io/metadata.name: alertmanager-global   managed: true   prometheus: old
<input type="checkbox"/>	<a href="#">annotator</a>	kubernetes.io/metadata.name: annotator   name: annotator
<input type="checkbox"/>	<a href="#">cert-manager</a>	kubernetes.io/metadata.name: cert-manager   name: cert-manager


```
- organization: mindbox-cloud
team: platform
roles:
  - k8s-admin-requester
  - k8s-viewer
```

# Kubernetes + Octopus Deploy

Script Console ?

Use the *Script Console* to run one-off scripts remotely on deployment targets. Scripts run this way are not associated with projects or deployments.

**Targets**

The script will run on  Cluster Infrastructure (kube-in...)

**Script**

**Body** Select the script language and enter the body of the

PowerShell  Bash  C#

**TASK SUMMARY** **TASK LOG** **SCRIPT BODY**

Expand Custom Log level Info Log tail Last 20

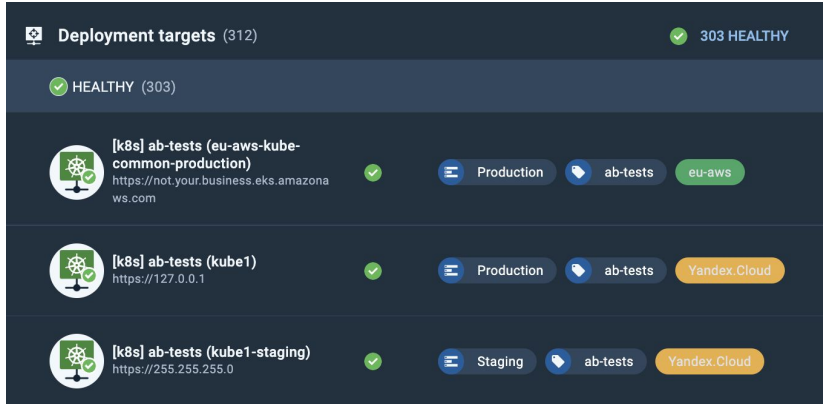
This task started 4 minutes ago and ran for 3 seconds

✓ Script run from management console ?

Run script on: Cluster Infrastructure (kube-infra)

```
Creating kubectl context to https://still.not.your.business/ (namespace default) using a Token
NAME                                READY  STATUS    RESTARTS  AGE  Info
cert-manager-74b8b5fd5f-m6cl2       1/1    Running   0          23d  Info
cert-manager-cainjector-58448cbc99-4d7ww  1/1    Running   0          53d  Info
cert-manager-sync-58f546cb47-ztkxb    1/1    Running   7 (18d ago)  211d  Info
cert-manager-webhook-89f77959f-brmz9   1/1    Running   0          53d  Info
cert-manager-webhook-yandex-6f5987447c-9wbcg  1/1    Running   2 (53d ago)  211d  Info
```

# Kubernetes + Octopus Deploy



The screenshot shows the 'Deployment targets' page in Octopus Deploy. At the top, it indicates '303 HEALTHY' targets. Below this, three specific targets are listed, each with a green checkmark and a 'HEALTHY' status:

- [k8s] ab-tests (eu-aws-kube-common-production)**: URL <https://not.your.business.eks.amazonaws.com>. Environment: Production. Target: ab-tests. Provider: eu-aws.
- [k8s] ab-tests (kube1)**: URL <https://127.0.0.1>. Environment: Production. Target: ab-tests. Provider: Yandex.Cloud.
- [k8s] ab-tests (kube1-staging)**: URL <https://255.255.255.0>. Environment: Staging. Target: ab-tests. Provider: Yandex.Cloud.

```
8 resource "octopusdeploy_token_account" "main" {
9   name = "[k8s] ${var.name} (${var.cluster_name})"
10  token = data.kubernetes_secret.deploy_service_account_token.data.token
11
12  tenanted_deployment_participation = "Tenanted"
13  tenant_tags                       = var.octopus_tenant_tags
14
15  environments = var.octopus_environments
16  lifecycle {
17    ignore_changes = all
18  }
19 }
```

```
"ab-tests" = {
  quotas = {
    limits = {
      cpu    = "2"
      memory = "8Gi"
    }
  }

  deploy_circuits = {
    production = [
      "legacy_stable",
      "legacy_eu",
    ]
    staging = [
      "staging",
    ]
  }

  labels = {
    product = "caprica"
  }

  github = "https://github.com/mindbox-cloud/ab-tests"
}
```

# Databases



Сетевой доступ - VPN / Teleport DB Access / Teleport TCP Application



Где хранить учетки приложений

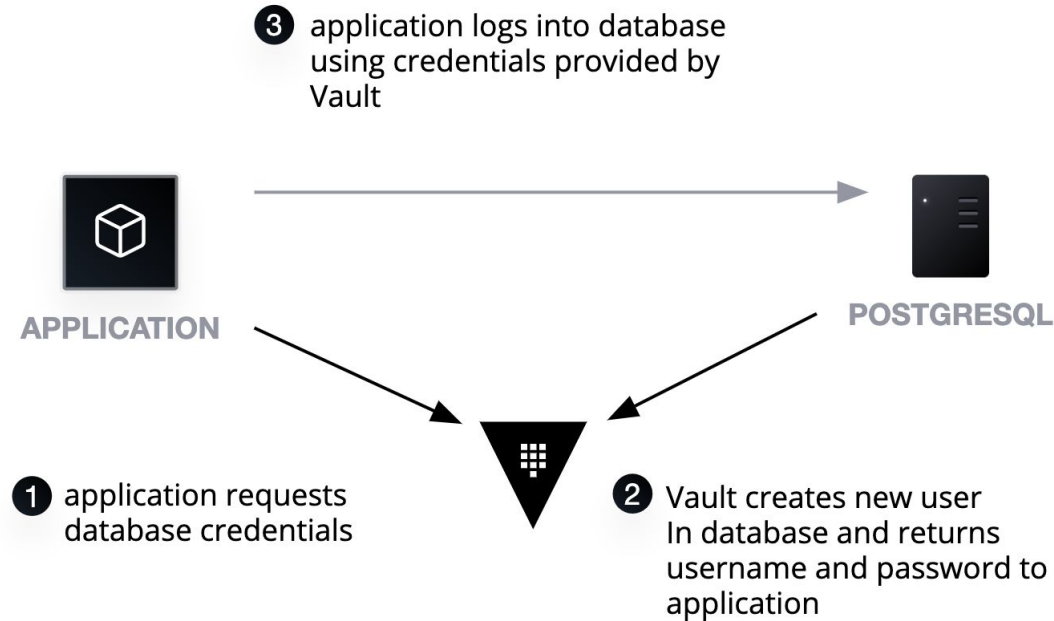


Как ротировать



Как подключаться разработчикам

# Databases



Cassandra

Couchbase

Elasticsearch

HanaDB

IBM Db2

InfluxDB

MongoDB

MongoDB Atlas

MSSQL

MySQL/MariaDB

Oracle

PostgreSQL

Redis

Redis ElastiCache

Redshift

Snowflake



# А если Vault не умеет?

```
apiVersion: v1
kind: Secret
metadata:
  name: "jwt-secret"
type: Opaque
data:
  # retrieve the secret data using lookup function and when not exists, return an empty dictionary / map as result
  {{- $secretObj := (lookup "v1" "Secret" .Release.Namespace "jwt-secret") | default dict }}
  {{- $secretData := (get $secretObj "data") | default dict }}
  # set $jwtSecret to existing secret data or generate a random one when not exists
  {{- $jwtSecret := (get $secretData "jwt-secret") | default (randAlphaNum 32 | b64enc) }}
  jwt-secret: {{ $jwtSecret | quote }}
```

# CI/CD

```
jobs:
  build:
    # ...
    steps:
      # ...
      - name: Import Secrets
        id: import-secrets
        uses: hashicorp/vault-action@v2
        with:
          url: https://vault.mycompany.com:8200
          token: ${ secrets.VAULT_TOKEN }
          caCertificate: ${ secrets.VAULT_CA_CERT }
          secrets: |
            secret/data/ci/aws accessKey | AWS_ACCESS_KEY_ID ;
            secret/data/ci/aws secretKey | AWS_SECRET_ACCESS_KEY ;
            secret/data/ci npm_token
      # ...
```

# Сколько тратить?

- Стоимость сертификации
- ФОТ
- ПО

1%

\*23,5 млн.р. в 23 году

# Итого

- Идем от бизнеса
- Едим слона по кускам, не обязательно вливать миллионы
- Работает только если не ошиблись при найме  
плюс конечно NDA и прочие страшилки для сотрудников

Предпоследний слайд

Вопросы?

# Материалы

- [Доклад от Wildberries на PHDays про Teleport](#)
- [Продолжение на Highload](#)
- Решения
  - <https://github.com/gravitational/teleport>
  - <https://github.com/hashicorp/vault>
  - <https://github.com/hashicorp/boundary>
  - <https://github.com/infracore/infra>
  - <https://github.com/OctopusDeploy>