Teleport

Saying Goodbye to Manual Kubernetes User Access Onboarding

With OSS Teleport

Teleport

secrets.txt

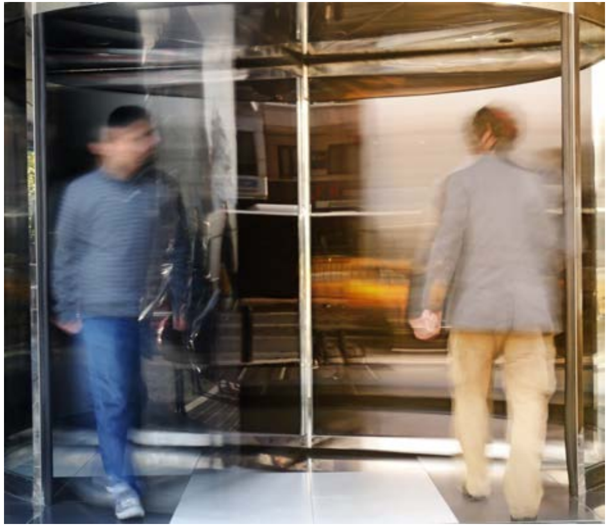
```
$ cat secrets.txt
  AWS_Public Key:        AKIAIOSFODNN7B7E0P3T
  AWS_Secret_Key:        wJalrXUtnFEMI/K7MDENG/bPxRfiCYUT3RpG8K7Y
  ADMIN_SHARED_DEV:      C00DO9GBQS7/DLI9TTU6LTNt3WHxNAEDH98995V8
  ADMIN_BOT:             3M8pXC/732dCm3BD7JMH!MQJT6VI3W1YT$WA3B4R
```

```
-----BEGIN PRIVATE KEY-----
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBKcwggSjAgEAAoIBAQCjFzNHGt+JUbjv
6wRktEKcsfjBVPDhsp17Y3+qACZrhE1X9x5sMfjx51MxtPwWadz3kWa8c5GU1edm
u2BbBxOx0mczSl/+cyOjB2PgOEW67X6+JBjkgrk2OhIpArQp64MGT8RMtrAHvjIn
a80wA5Da2j92Zh+Gtho6sEWYLyWtIn7+o5JHCMiZl/gGjzO0NNDhrsFPrwKNzjRN
XEsu1Gg/fBMDKh4cKJwx7chmgv0IUrl9sVgwhmG0oThBglVVDm14CmEOpbZpzKG/
yz6T5jqMxWajvlDPXQC6G8CWDH6NBe+tR9lAmcpKr94SuBSU7s1bkAzdtYy0Dv4X
LtZPzV4zAgMBAAECggEBAITf+xw8jdFgbs+x59NwdjEaYzSI0vTfxKTqDPJhyuug
UC+SHAxErrHQKZz++r/8Ilbl9REnC356xFyT305qtqYTaZeFSi6Sen9yHvJoho9k
vfWGjW1oACRpLbCSDl11DzxOMv3ZfhPg5xXtI7Cxxww38qqxS5BCv53/TcRO7WBf
xHo518/Lv6UJFYI533QfD+WVBMJz2+5gXtpzC8wsMfNSSD9RFyszw7n2UivR+h3j
+jcKJ1ocpxW6AsvizgAH2pfYxW95J/IWPV7IRCiT4Ug3rKGP1+ntkODz04BfC5lA
cnEqv07fRqT7Z/gx20oWGEukVxD/0gJJvTageePoJ5ECgYEA00MAQefioIw1fHoL
Deljqmds5TqoId2E03k17HetvEnv2KcWqZhXCPf7J1WxgJdoL0GeF2ZmGSPojDPb
EAOTz+EoVkyYpiT4Oc53R70oEYN3dldXlHbzdaKXAljhfvA8vukl15fJXvDY/Ab4
46HZgLKUrWg3w1VgFES6nR1oycsCgYEAxaC62/4mU7J/W2VR10c8Rw2E90/4xAkr
a98Ha6tEAOyOmnFHvvY6pV13Ah1JuMZwcZ/ojUFMDk+UIYq/WpeR4BNXLI2O+N2v
iNKtw8ExCUDgkD7De3GjbrmyfVmNpjzQpvJRIjrhFlHsakXO/JM+tk6kSHGlkPBH
GLqy7rQbUDkCgYAMXMBYGvSlBm9e0FlzP/QIFbNGmq8aBDdwlIg2RS6SdRUm7Wgj
FnoJWVGGFLqlVrbPBRz2K5TP5c0G30XzYvI0WO2eVy8bkdBAubc7KHN+yt2jvCqw
0mEewhvqFD9lyTMUzNndCtHKz3czEEliMKdko46VsyKIOKe9p+Pvq7flDwKBgC2Q
f0SVdjS55M8nrxTZYbZoEY4LrClWi+JVC5rxY75qy/4jvAz1LFRQFk4wfnzRk78+
xRk8QtLR2i9ZlADJDWMCUoj9IkeSpRQArvuBIVMm2B+puNxPOQUgX1yzNwtq3hh/
qeEgfiDtRnrCGZT2RfE2dH4XZbrjCyFSekq6z8lRAoGAao0cSl0ZEqPB3F0/cMnt
wUlLW3eofbE3q1zHQ68lra/DdCh/u7LiWOqWNw4bGYsTwAs40ooPxWDTeKEVQff6
RztKIGDxC+hduCxcV6LRDZhY+NviUcP5ObDFijzgn6TitRzXo4l0EOtnpMaoCgQD
PFJbhngGMzeIVrNg9e88//E=
-----END PRIVATE KEY-----
```

```
-----BEGIN CERTIFICATE-----
MIIDgjCCAmoCCQCuKkPUJhhITjANBgkqhkiG9w0BAQsFADCBgjELMAkGA1UEBhMC
QVUxETAPBgNVBAgMCEJyaXNiYW5lMQ8wDQYDVQQHDAZTeW5kZXkxDTALBgNVBAoM
BFN3YWcxCjAIBgNVBAsMATIxFzAVBgNVBAMMDnd3dy5nb29nbGUuY29tMRswGQYJ
KoZIhvcNAQkBFgxrQGdvb2dsZS5jb20wHhcNMjIwOTMwMTkzODEyWhcNMzIwOTI3
MTkzODEyWjCBgjELMAkGA1UEBhMCQVUxETAPBgNVBAgMCEJyaXNiYW5lMQ8wDQYD
VQQHDAZTeW5kZXkxDTALBgNVBAoMBFN3YWcxCjAIBgNVBAsMATIxFzAVBgNVBAMM
Dnd3dy5nb29nbGUuY29tMRswGQYJKoZIhvcNAQkBFgxrQGdvb2dsZS5jb20wggEi
MA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCjFzNHGt+JUbjv6wRktEKcsfjB
VPDhsp17Y3+qACZrhE1X9x5sMfjx51MxtPwWadz3kWa8c5GU1edmu2BbBxOx0mcz
Sl/+cyOjB2PgOEW67X6+JBjkgrk2OhIpArQp64MGT8RMtrAHvjIna80wA5Da2j92
Zh+Gtho6sEWYLyWtIn7+o5JHCMiZl/gGjzO0NNDhrsFPrwKNzjRNXEsu1Gg/fBMD
Kh4cKJwx7chmgv0IUrl9sVgwhmG0oThBglVVDm14CmEOpbZpzKG/yz6T5jqMxWaj
vlDPXQC6G8CWDH6NBe+tR9lAmcpKr94SuBSU7s1bkAzdtYy0Dv4XLtZPzV4zAgMB
AAEwDQYJKoZIhvcNAQELBQADggEBABZsmWX31ENy9PT0VGs3o7eGh97MnM3A9JzU
UK9k+AXF7HDr/OWWrnKUn2HnZx0iMuetdCwqZYNpx43ec+3RoPvRcKPzSGjDMJXa
I5efzCN9BTGizIKFixZwYb4u3pcWrfNH8p+x9lxgCAQXT8g5ElyTW3MEn17l103/
mDWqLjhD20Un7roJZ1Jpr4P3489dvECV0+2t/QD4z7vHs5Seu+W1VvxGLx3oYiqC
5Yx/IM56i8blvwFU/z1ONV1orrA9CRCp9TebcftEQTq2+pVTQvKNerwjxq8aLi2c
n8alxudo3DC8nWdb5CyBzmnVF8kQAip5LusnIulHXvEsdr+2BO4=
-----END CERTIFICATE-----
```

Offboarding Access

- 1 in 4 employees still have access to old passwords
- 41.7% of employees admitted to having shared workplace passwords



source: Beyond Identity 2021

Every Security Breach Has Two Things In Common:

- A human error for initial infiltration
- An attempt to pivot to maximize the blast radius

Teleport

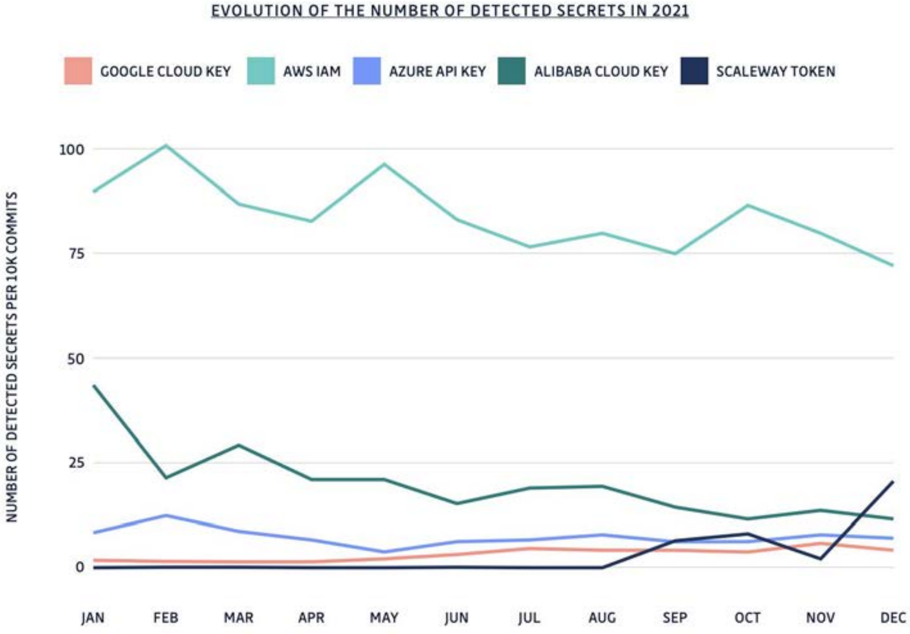
Human Error

6,000,000+

The number of leaked secrets GitGuardian detected in 2021

2x Increase since 2020

Types of Secrets Leaked



But We’re Not Open Source!

- 85% of corporate leaks came from developers personal repos
- 15% from public corporate repos

Maximize Blast Radius

- You get into a Slack workspace
- Get access to a server
- You get into a server
- Elevate privileges
- ??????
- Profit
- 50/50 Bahamas or Jail

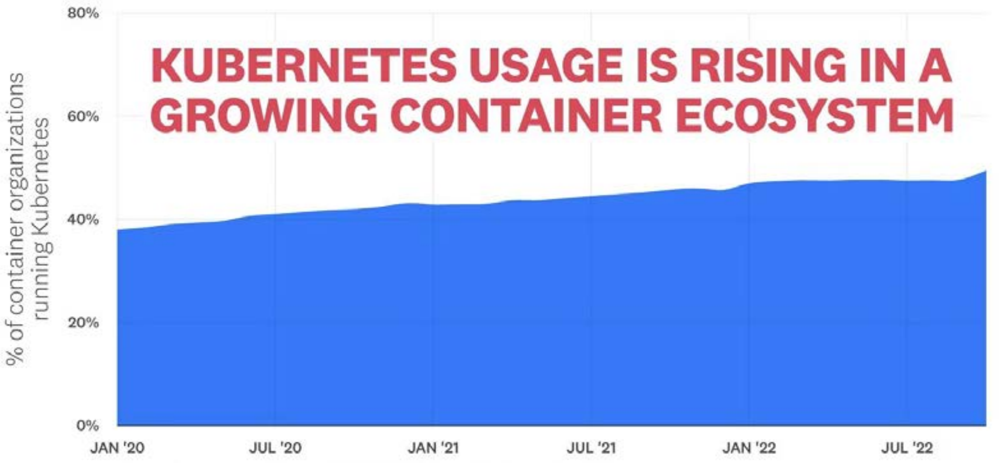
Teleport

Kubernetes Today

Container Research Report 2022:

- 1.5 billion containers
- tens of thousands of companies

Kubernetes Share Among Container Organizations



The definition of a container organization includes organizations running Kubernetes, Amazon Elastic Container Service, serverless container technologies, and more.

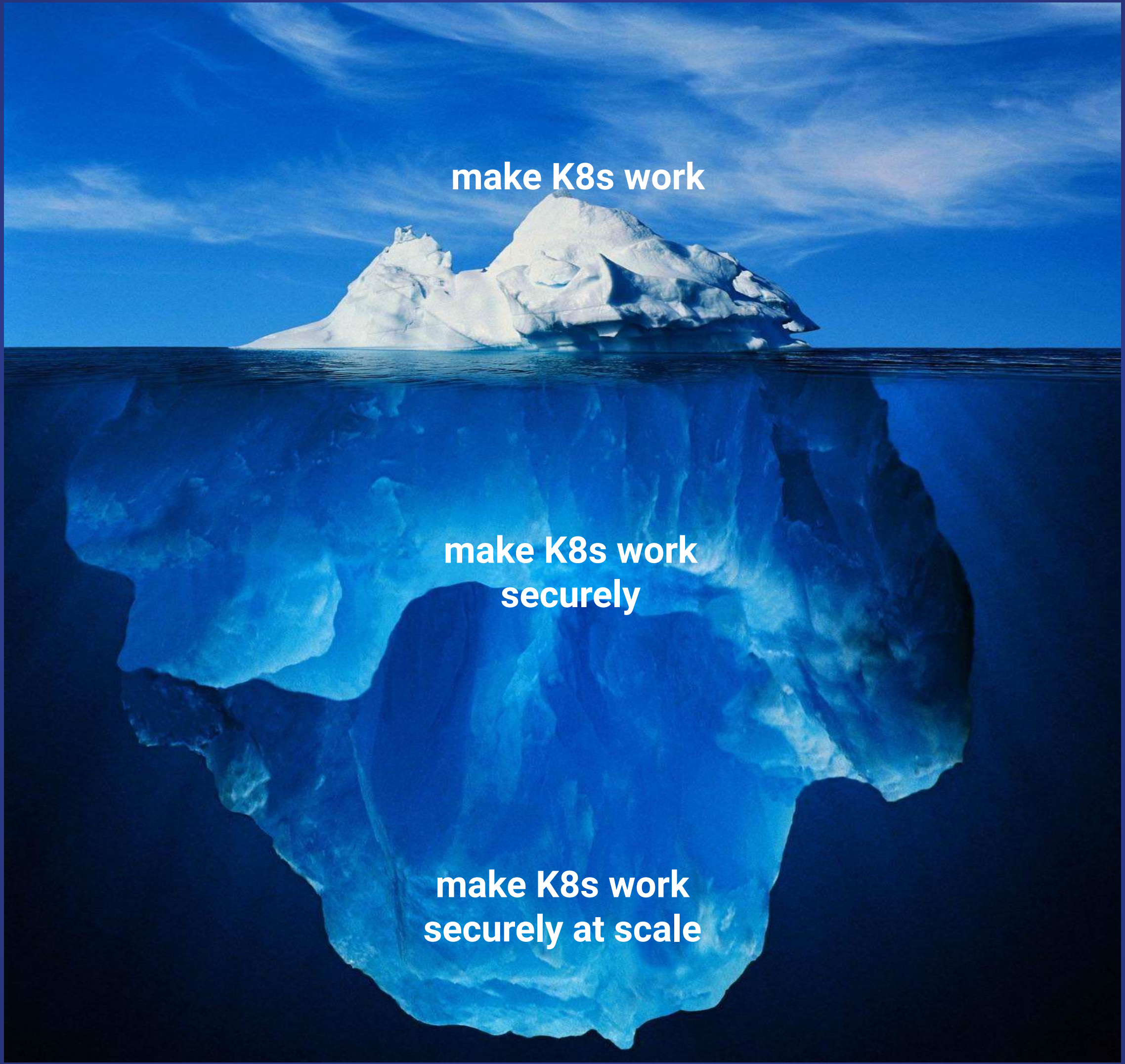
Source: Datadog

All running K8s clusters configured by humans...

who make mistakes.

Misconfiguration

- ~40 percent of clusters still use lax privileges
  - list all secrets
  - create workloads/certificates
  - privilege escalation token requests



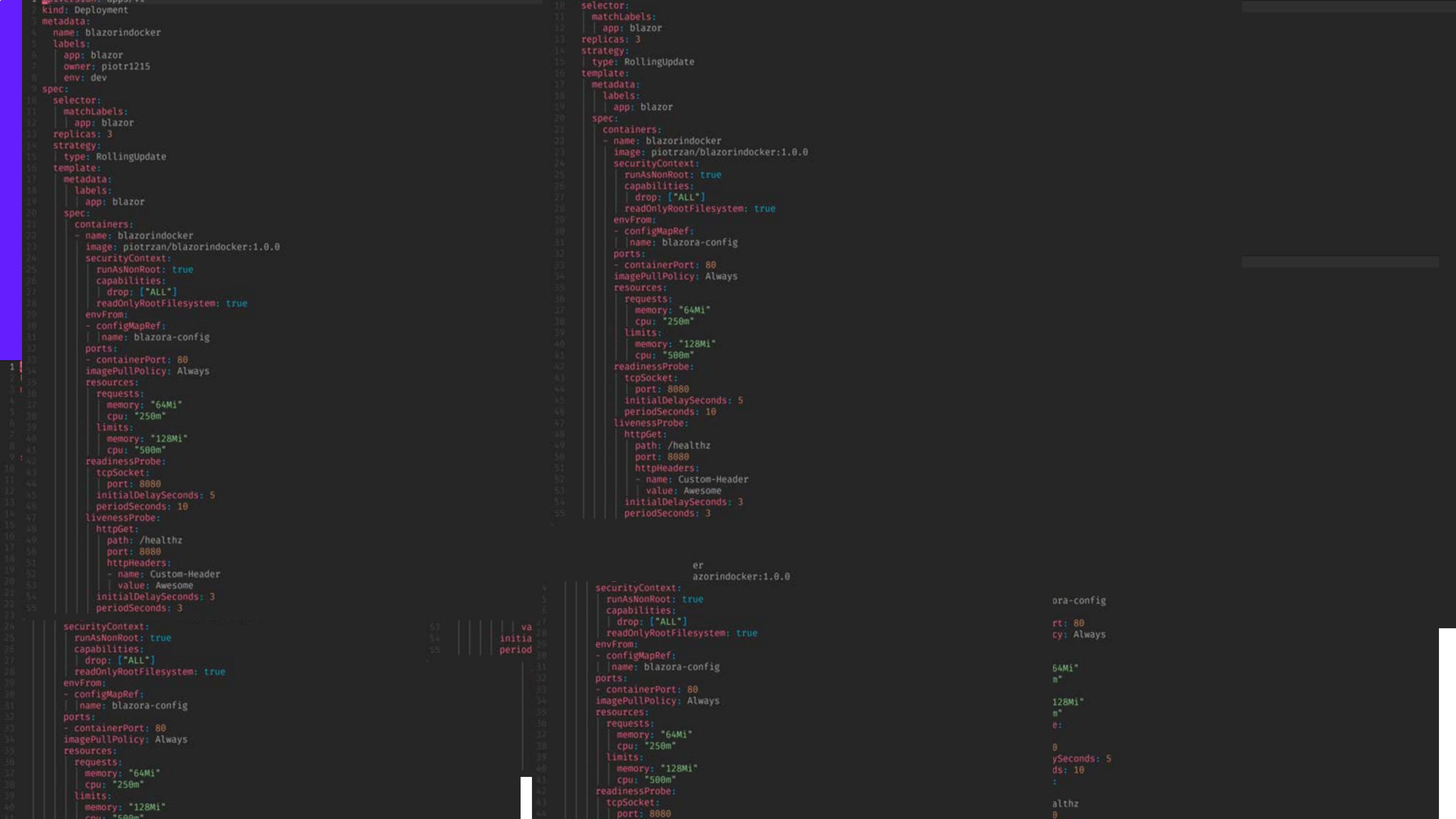
make K8s work

make K8s work
securely

make K8s work
securely at scale

Teleport

Kubernetes is NOT safe by default



```yaml
apiVersion: apps/v1
kind: Deployment
metadata:
  name: blazorindocker
  labels:
    app: blazor
    owner: piotr1215
    env: dev
spec:
  selector:
    matchLabels:
      app: blazor
  replicas: 3
  strategy:
    type: RollingUpdate
  template:
    metadata:
      labels:
        app: blazor
    spec:
      containers:
      - name: blazorindocker
        image: piotrzan/blazorindocker:1.0.0
        securityContext:
          runAsNonRoot: true
          capabilities:
            drop: ["ALL"]
          readOnlyRootFilesystem: true
        envFrom:
        - configMapRef:
            name: blazora-config
        ports:
        - containerPort: 80
        imagePullPolicy: Always
        resources:
          requests:
            memory: "64Mi"
            cpu: "250m"
          limits:
            memory: "128Mi"
            cpu: "500m"
        readinessProbe:
          tcpSocket:
            port: 8080
          initialDelaySeconds: 5
          periodSeconds: 10
        livenessProbe:
          httpGet:
            path: /healthz
            port: 8080
            httpHeaders:
            - name: Custom-Header
              value: Awesome
          initialDelaySeconds: 3
          periodSeconds: 3
```

```yaml
  selector:
    matchLabels:
      app: blazor
  replicas: 3
  strategy:
    type: RollingUpdate
  template:
    metadata:
      labels:
        app: blazor
    spec:
      containers:
      - name: blazorindocker
        image: piotrzan/blazorindocker:1.0.0
        securityContext:
          runAsNonRoot: true
          capabilities:
            drop: ["ALL"]
          readOnlyRootFilesystem: true
        envFrom:
        - configMapRef:
            name: blazora-config
        ports:
        - containerPort: 80
        imagePullPolicy: Always
        resources:
          requests:
            memory: "64Mi"
            cpu: "250m"
          limits:
            memory: "128Mi"
            cpu: "500m"
        readinessProbe:
          tcpSocket:
            port: 8080
          initialDelaySeconds: 5
          periodSeconds: 10
        livenessProbe:
          httpGet:
            path: /healthz
            port: 8080
            httpHeaders:
            - name: Custom-Header
              value: Awesome
          initialDelaySeconds: 3
          periodSeconds: 3
```

```yaml
        securityContext:
          runAsNonRoot: true
          capabilities:
            drop: ["ALL"]
          readOnlyRootFilesystem: true
        envFrom:
        - configMapRef:
            name: blazora-config
        ports:
        - containerPort: 80
        imagePullPolicy: Always
        resources:
          requests:
            memory: "64Mi"
            cpu: "250m"
          limits:
            memory: "128Mi"
```

```yaml
              va
          initia
          period
```

```yaml
er
azorindocker:1.0.0
        securityContext:
          runAsNonRoot: true
          capabilities:
            drop: ["ALL"]
          readOnlyRootFilesystem: true
        envFrom:
        - configMapRef:
            name: blazora-config
        ports:
        - containerPort: 80
        imagePullPolicy: Always
        resources:
          requests:
            memory: "64Mi"
            cpu: "250m"
          limits:
            memory: "128Mi"
            cpu: "500m"
        readinessProbe:
          tcpSocket:
            port: 8080
```

```yaml
ora-config

rt: 80
cy: Always

64Mi"
m"

128Mi"
m"
e:

0
ySeconds: 5
ds: 10
:

althz
0
```

What can we do?

Teleport

OSS Teleport Kubernetes Access

Kubernetes Access

- Authentication
- Authorization
- Connectivity
- Audit

Teleport

Authentication

Generate an identity (in the form of a short-lived X.509 certificate) for the user and tie that identity to a role managed by Teleport

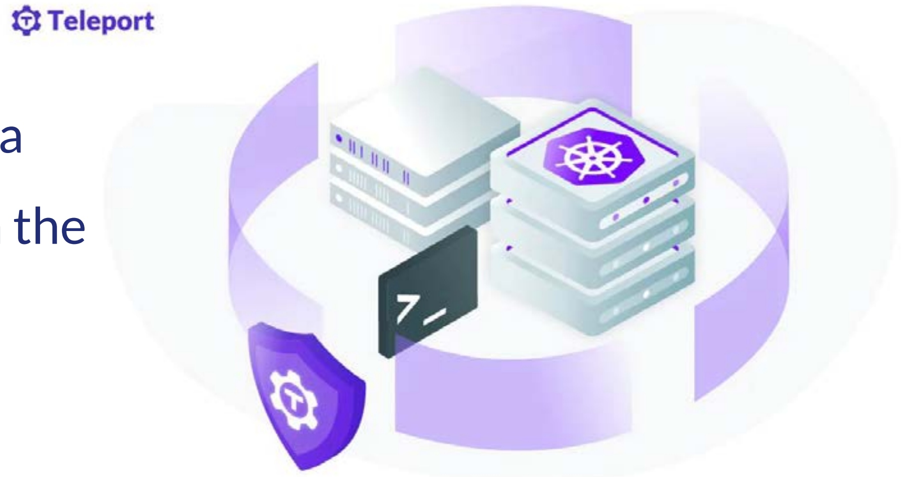
Teleport

Authorization

Automatically approve or deny access requests to a range of resources (e.g. servers, databases, Kubernetes clusters, and microservices, CI/CD systems)

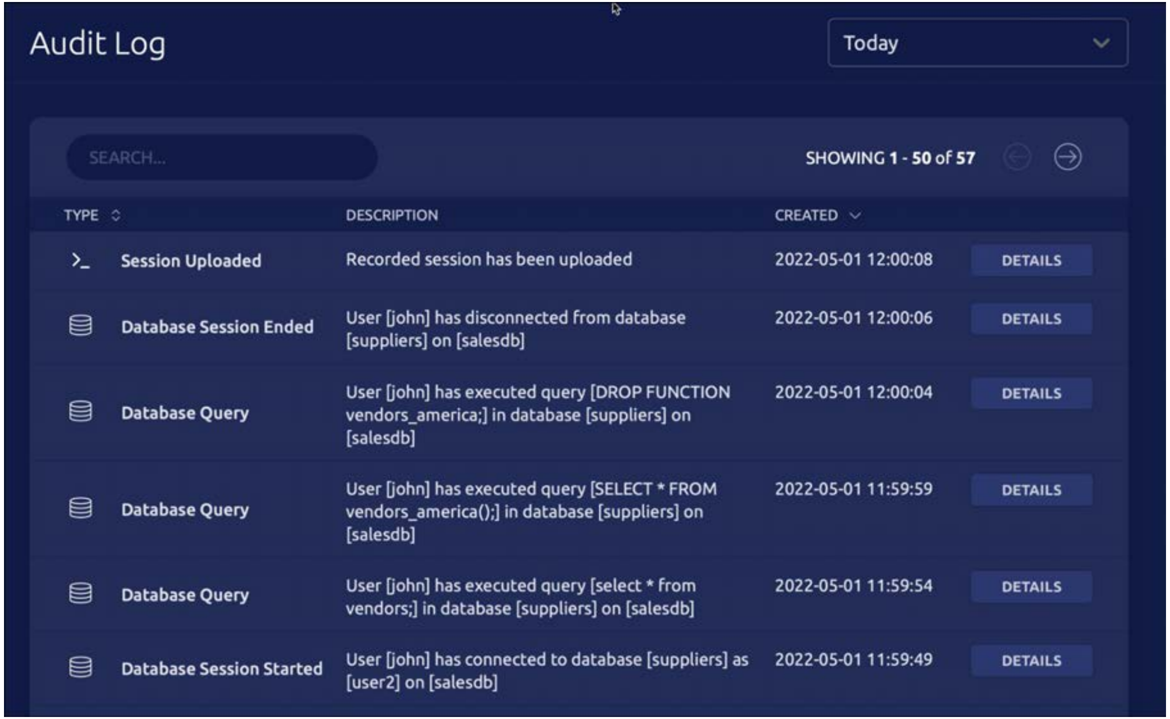
Connectivity

Establish a connection between the user and the requested resource using a reverse proxy tunnel from the Teleport server to the resource.



Audit

Logs actions for diagnostic and compliance purposes



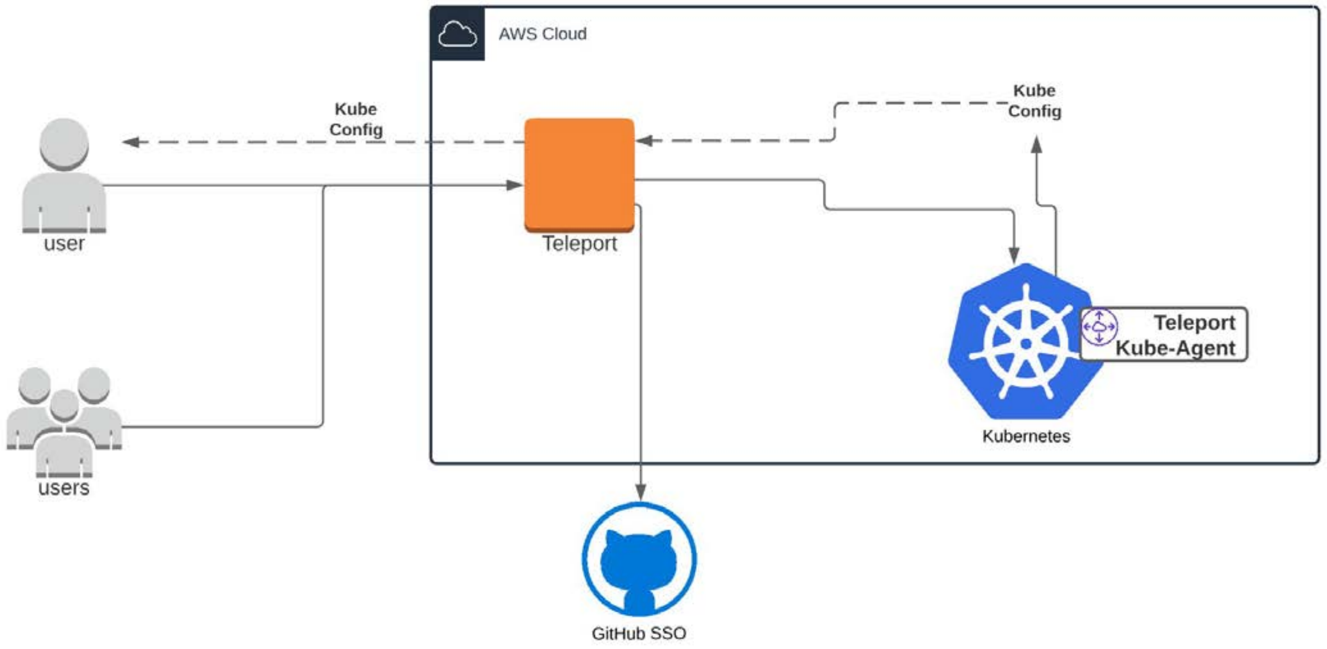
Audit Log

SHOWING 1 - 50 of 57

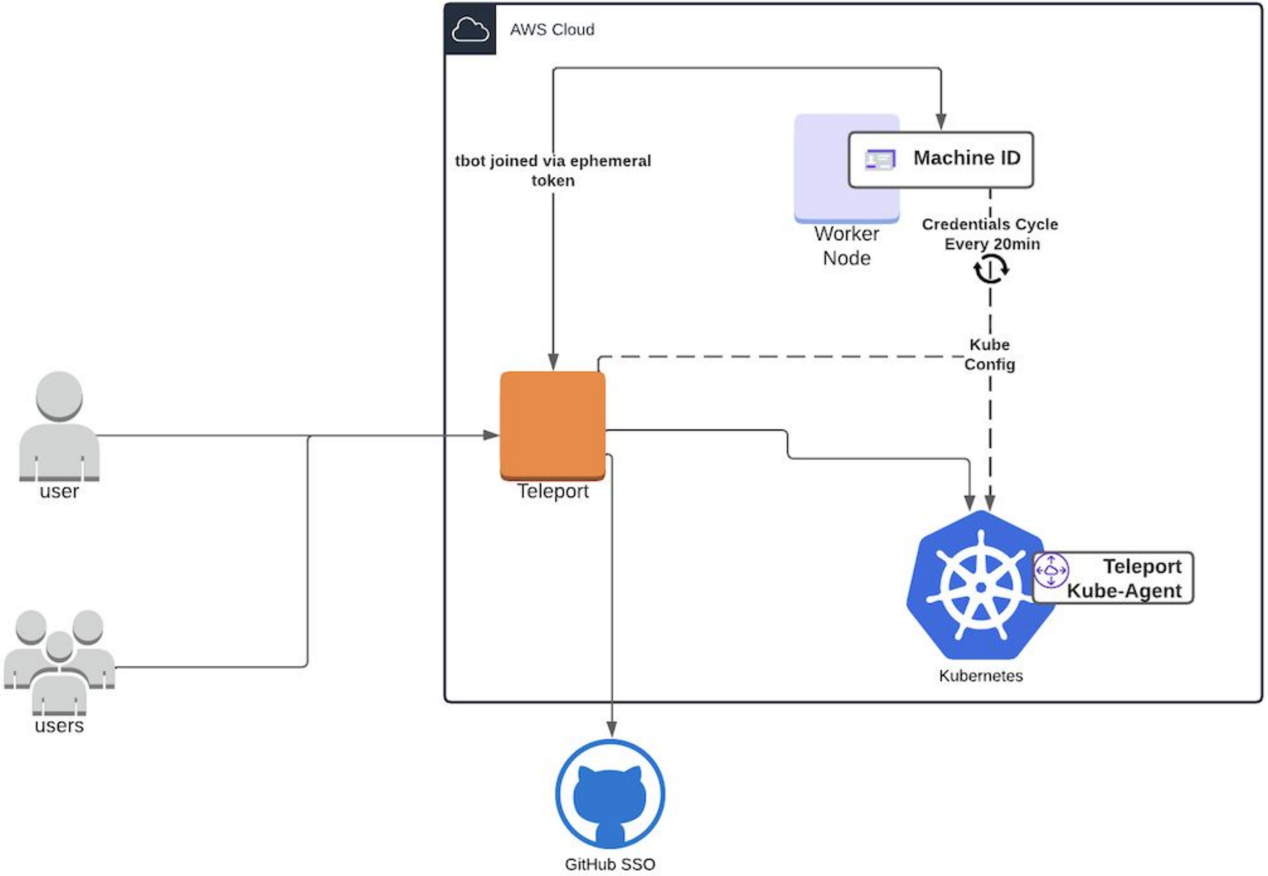
TYPE	DESCRIPTION	CREATED	
>_ Session Uploaded	Recorded session has been uploaded	2022-05-01 12:00:08	DETAILS
Database Session Ended	User [john] has disconnected from database [suppliers] on [salesdb]	2022-05-01 12:00:06	DETAILS
Database Query	User [john] has executed query [DROP FUNCTION vendors_america;] in database [suppliers] on [salesdb]	2022-05-01 12:00:04	DETAILS
Database Query	User [john] has executed query [SELECT * FROM vendors_america();] in database [suppliers] on [salesdb]	2022-05-01 11:59:59	DETAILS
Database Query	User [john] has executed query [select * from vendors;] in database [suppliers] on [salesdb]	2022-05-01 11:59:54	DETAILS
Database Session Started	User [john] has connected to database [suppliers] as [user2] on [salesdb]	2022-05-01 11:59:49	DETAILS

Teleport

High Level Architecture



High Level Architecture(Machine-ID)



Demo!

What’s Next

- Teleport 11
- Github Actions support
- Interact with Teleport protected resources (SSH, Kubernetes, Database) from GitHub Actions workflows
- No need for a long lived credential - or the need to share any sensitive values.
- K8s support for automatic service discovery

Teleport

Thank you so much!

Teleport

goteleport.slack.com

https://goteleport.com