🙋‍♂️

OIDC Migration

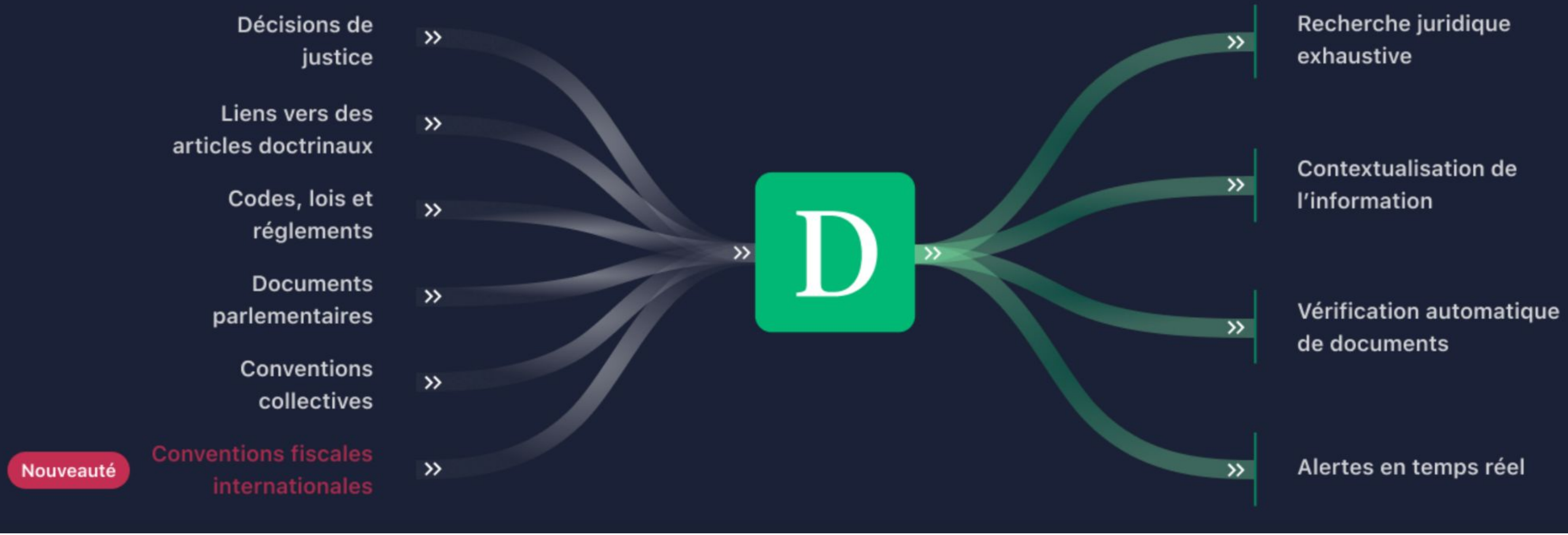
Run your CI without any long-term credentials

Doctrine

***Ben**jamin RIOU*
Devops/SRE

L’information pertinente

Centralisée et surveillée en temps réel, servie sur un plateau



Décisions de justice

Liens vers des articles doctrinaux

Codes, lois et réglements

Documents parlementaires

Conventions collectives

Nouveauté Conventions fiscales internationales

Recherche juridique exhaustive

Contextualisation de l’information

Vérification automatique de documents

Alertes en temps réel

Qui sommes-nous ?

Doctrine en quelques chiffres

110 **employés**
dont 50 ingénieurs

400 **nouveaux utilisateurs**
chaque mois

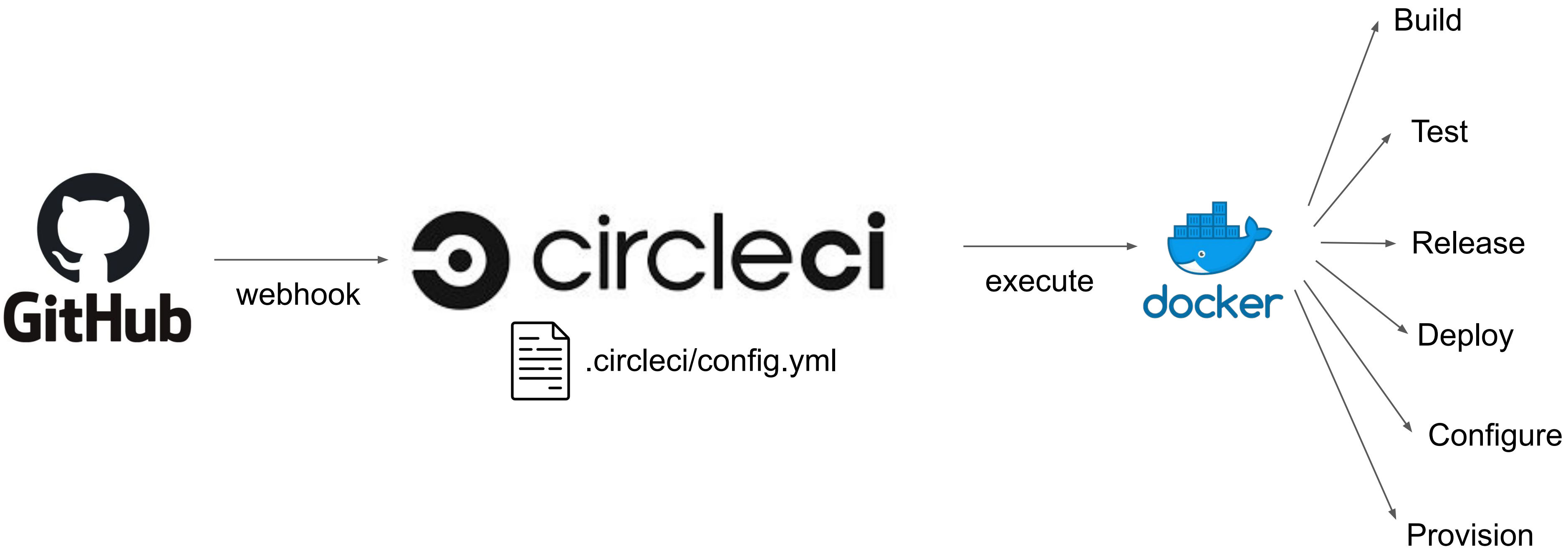
70% **des cabinets du top 100**
& 30% **du CAC 40**
nous ont rejoint en 24 mois

1 million **de visiteurs**
chaque mois

Squad Foundation @ Doctrine

# quizroom
MY MIND IS LIKE MY INTERNET BROWSER. I HAVE 19 TABS OPEN, 3 ARE FROZEN,
CLIMATE CHANGE
AU SOMMET
Jitix
William

Doctrine uses CircleCI



webhook

.circleci/config.yml

execute

Build

Test

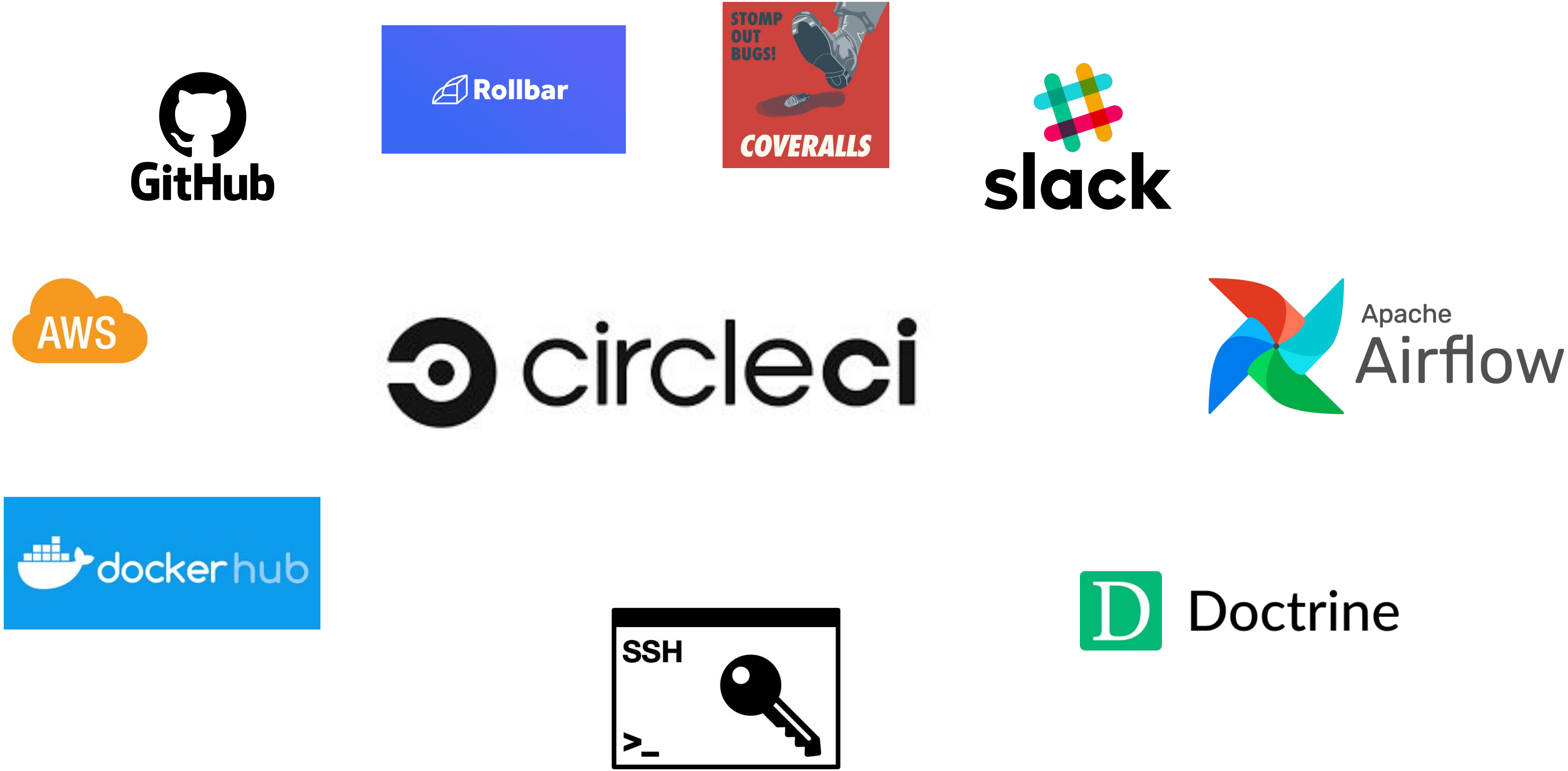
Release

Deploy

Configure

Provision

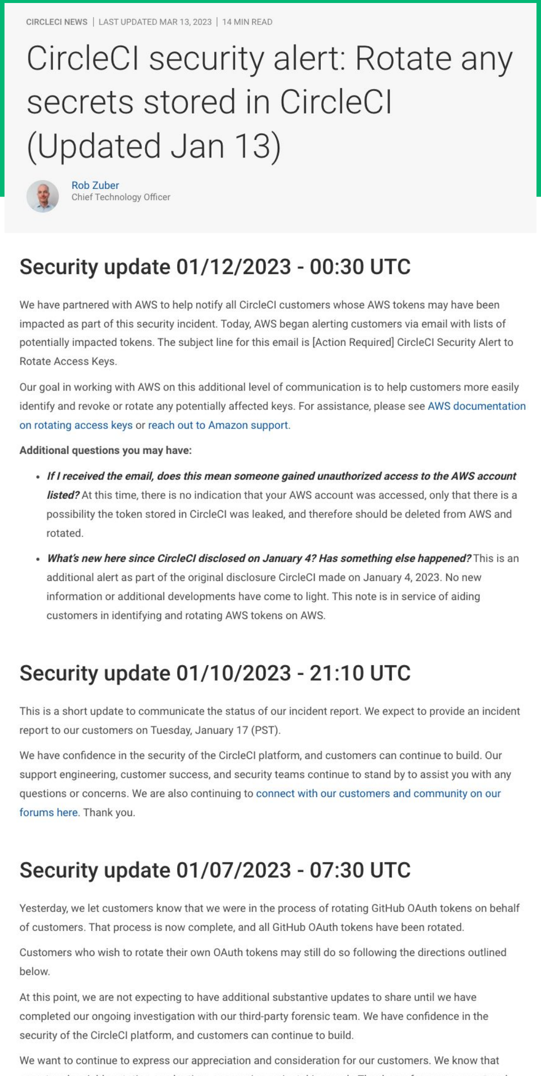
Circle needs a lot of secrets



Happy new year, Foundation !

2023/01/05 - 03h00 (Paris Time) - Security Alert :

+200 secrets on 15 systems potentially leaked.



CIRCLECI NEWS | LAST UPDATED MAR 13, 2023 | 14 MIN READ

CircleCI security alert: Rotate any secrets stored in CircleCI (Updated Jan 13)

Rob Zuber
Chief Technology Officer

Security update 01/12/2023 - 00:30 UTC

We have partnered with AWS to help notify all CircleCI customers whose AWS tokens may have been impacted as part of this security incident. Today, AWS began alerting customers via email with lists of potentially impacted tokens. The subject line for this email is [Action Required] CircleCI Security Alert to Rotate Access Keys.

Our goal in working with AWS on this additional level of communication is to help customers more easily identify and revoke or rotate any potentially affected keys. For assistance, please see AWS documentation on rotating access keys or reach out to Amazon support.

Additional questions you may have:

- ***If I received the email, does this mean someone gained unauthorized access to the AWS account listed?*** At this time, there is no indication that your AWS account was accessed, only that there is a possibility the token stored in CircleCI was leaked, and therefore should be deleted from AWS and rotated.
- ***What's new here since CircleCI disclosed on January 4? Has something else happened?*** This is an additional alert as part of the original disclosure CircleCI made on January 4, 2023. No new information or additional developments have come to light. This note is in service of aiding customers in identifying and rotating AWS tokens on AWS.

Security update 01/10/2023 - 21:10 UTC

This is a short update to communicate the status of our incident report. We expect to provide an incident report to our customers on Tuesday, January 17 (PST).

We have confidence in the security of the CircleCI platform, and customers can continue to build. Our support engineering, customer success, and security teams continue to stand by to assist you with any questions or concerns. We are also continuing to connect with our customers and community on our forums here. Thank you.

Security update 01/07/2023 - 07:30 UTC

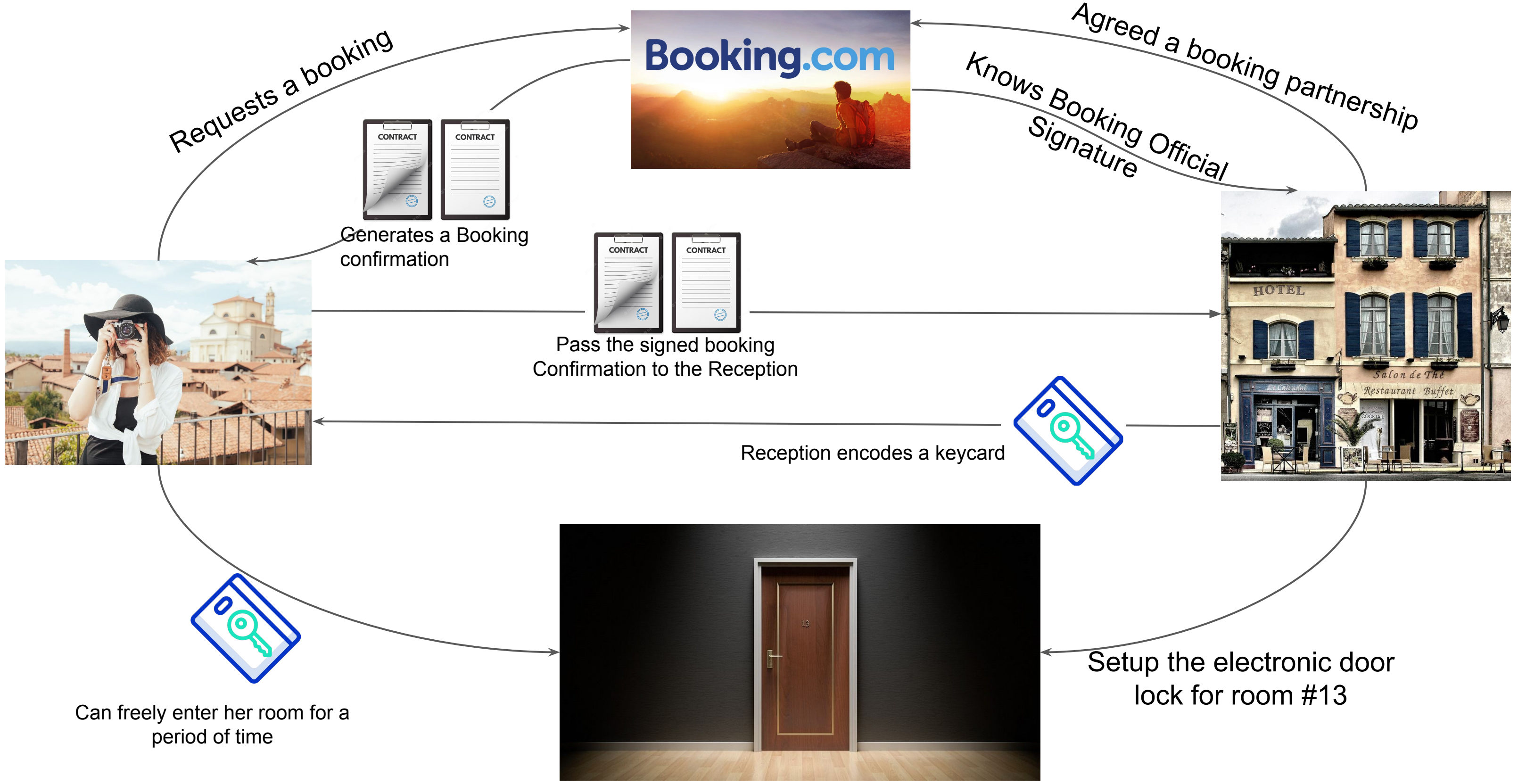
Yesterday, we let customers know that we were in the process of rotating GitHub OAuth tokens on behalf of customers. That process is now complete, and all GitHub OAuth tokens have been rotated.

Customers who wish to rotate their own OAuth tokens may still do so following the directions outlined below.

At this point, we are not expecting to have additional substantive updates to share until we have completed our ongoing investigation with our third-party forensic team. We have confidence in the security of the CircleCI platform, and customers can continue to build.

We want to continue to express our appreciation and consideration for our customers. We know that

Introduction to OIDC Federations



Requests a booking

Generates a Booking confirmation

Agreed a booking partnership

Knows Booking Official Signature

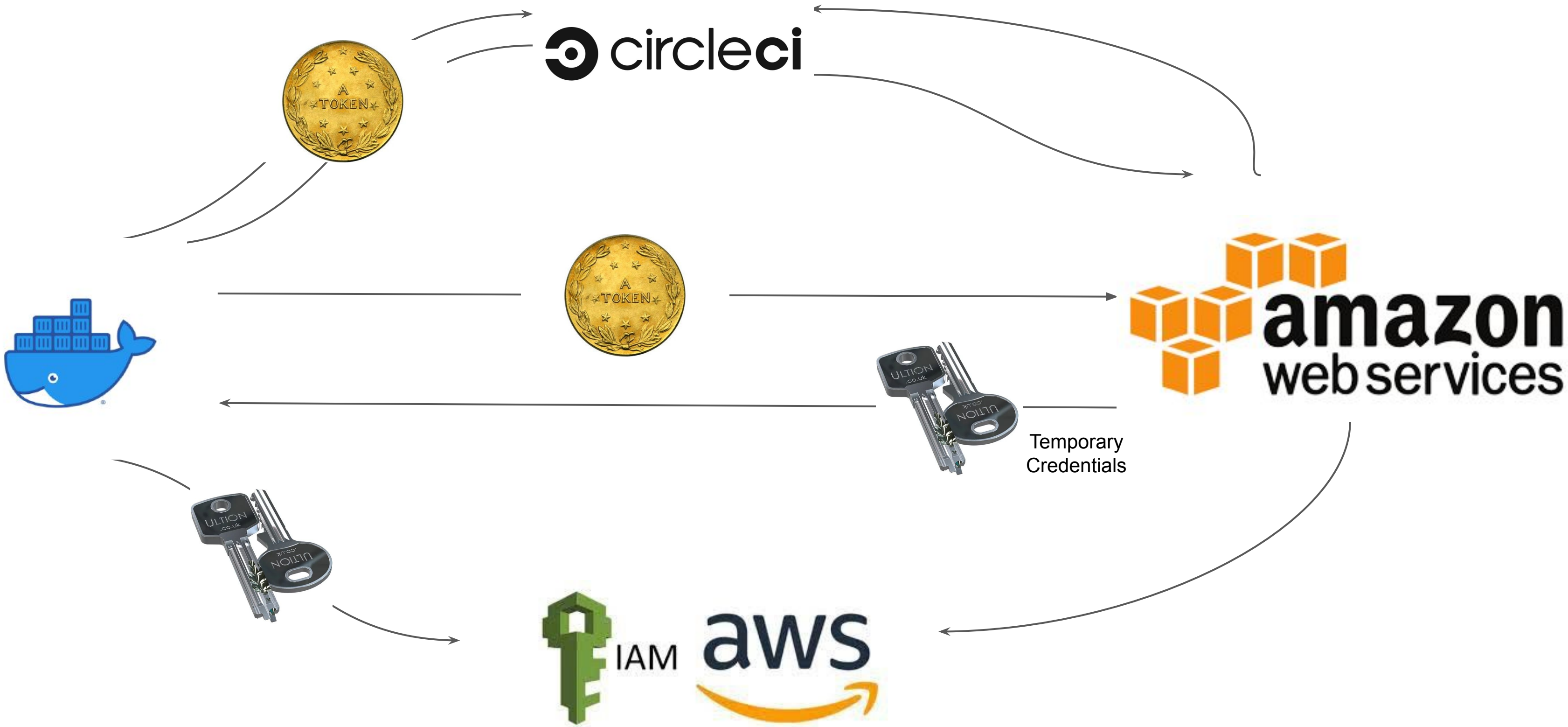
Pass the signed booking Confirmation to the Reception

Reception encodes a keycard

Setup the electronic door lock for room #13

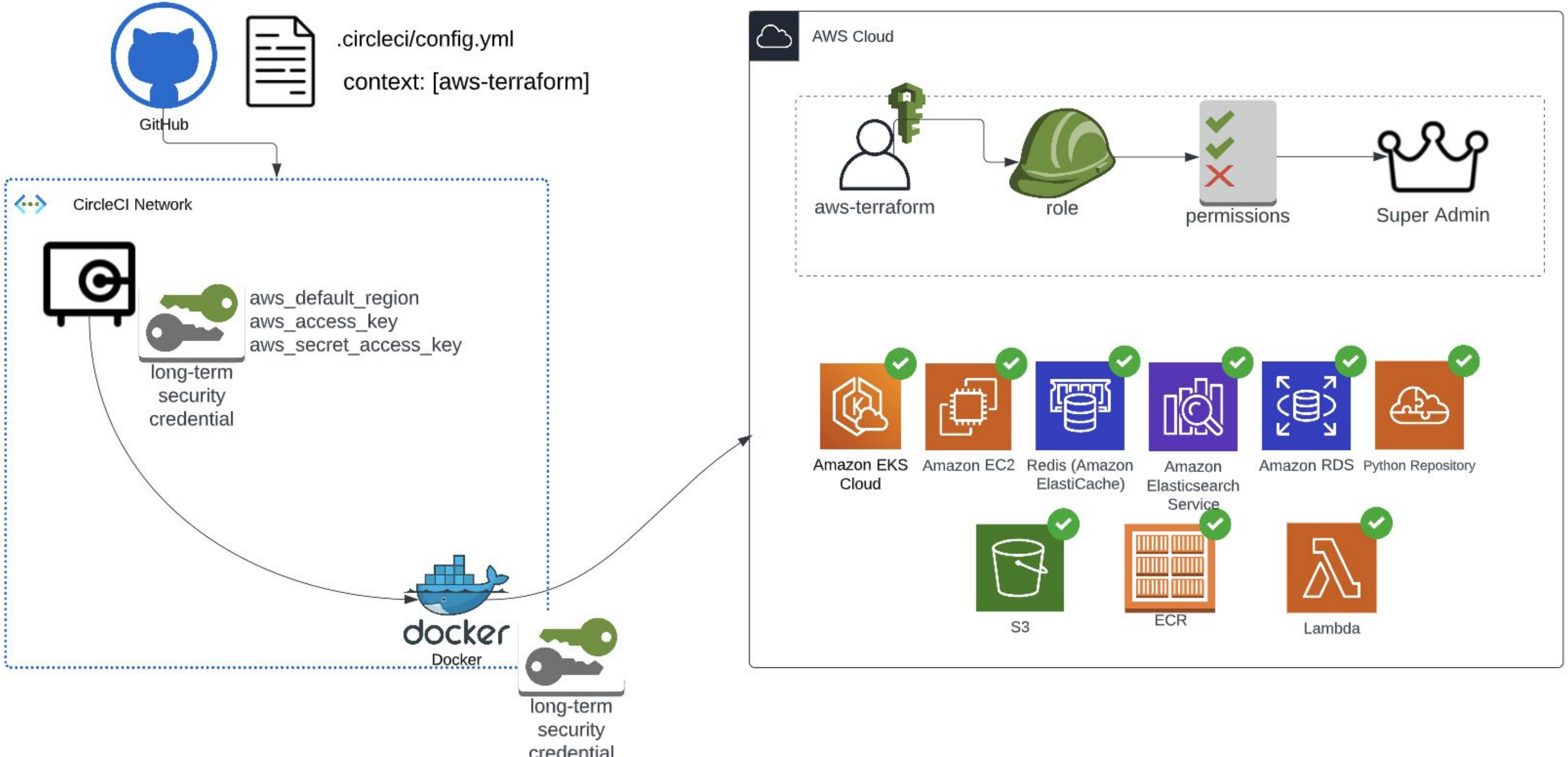
Can freely enter her room for a period of time

Introduction to OIDC Federations

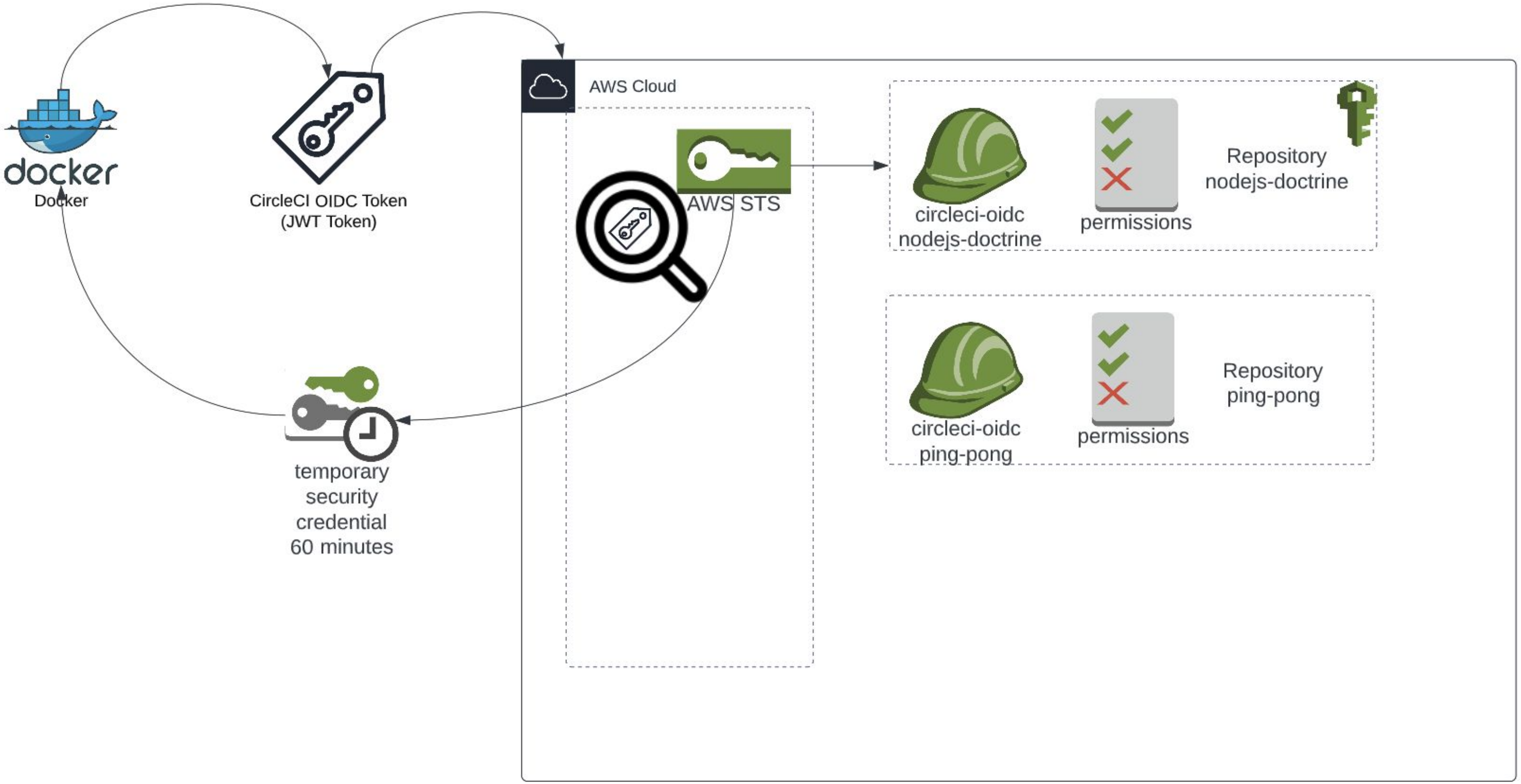


OIDC...
OIDC EVERYWHERE
imgflip.com

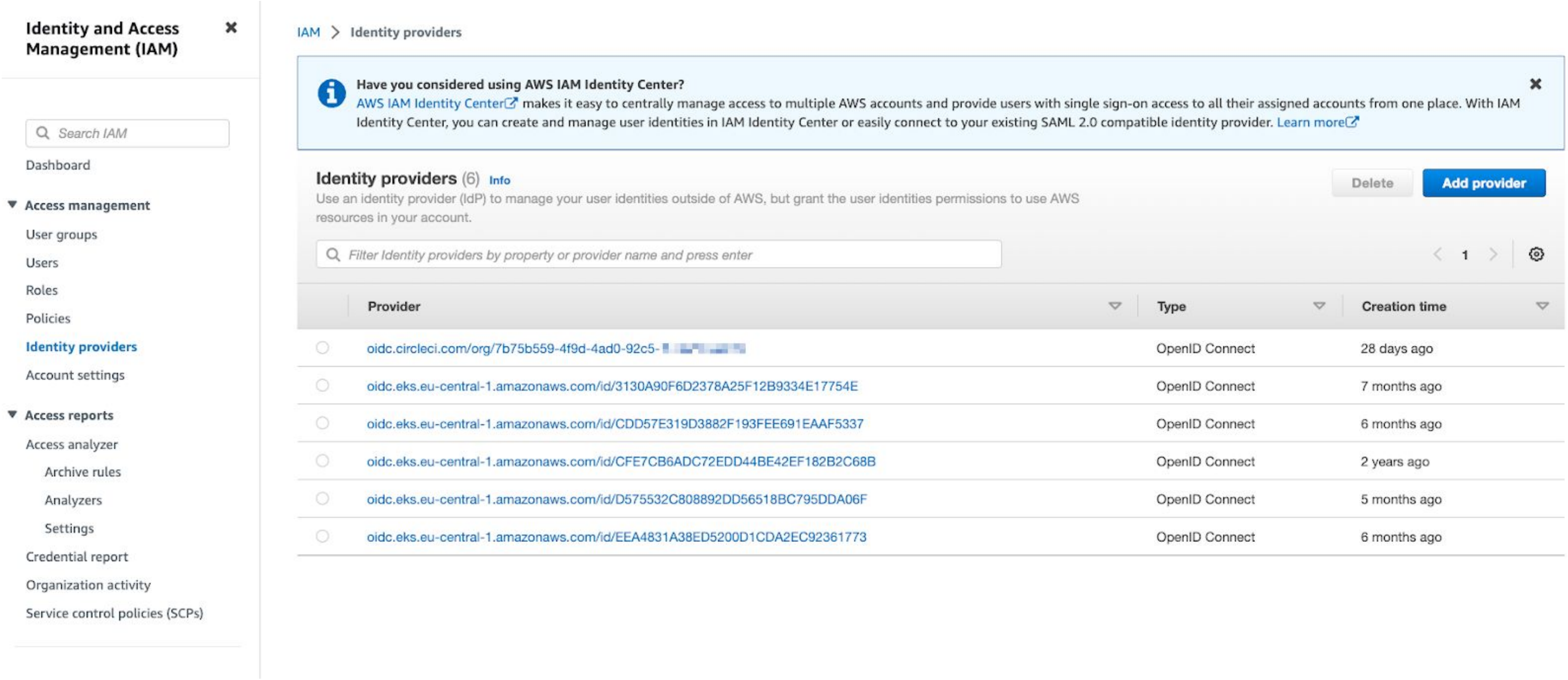
Where do we come from ?



We aim to keep our secrets for ourselves



Setup the OIDC Federation



Have you considered using AWS IAM Identity Center?
AWS IAM Identity Center makes it easy to centrally manage access to multiple AWS accounts and provide users with single sign-on access to all their assigned accounts from one place. With IAM Identity Center, you can create and manage user identities in IAM Identity Center or easily connect to your existing SAML 2.0 compatible identity provider. Learn more

Identity providers (6) Info

Use an identity provider (IdP) to manage your user identities outside of AWS, but grant the user identities permissions to use AWS resources in your account.

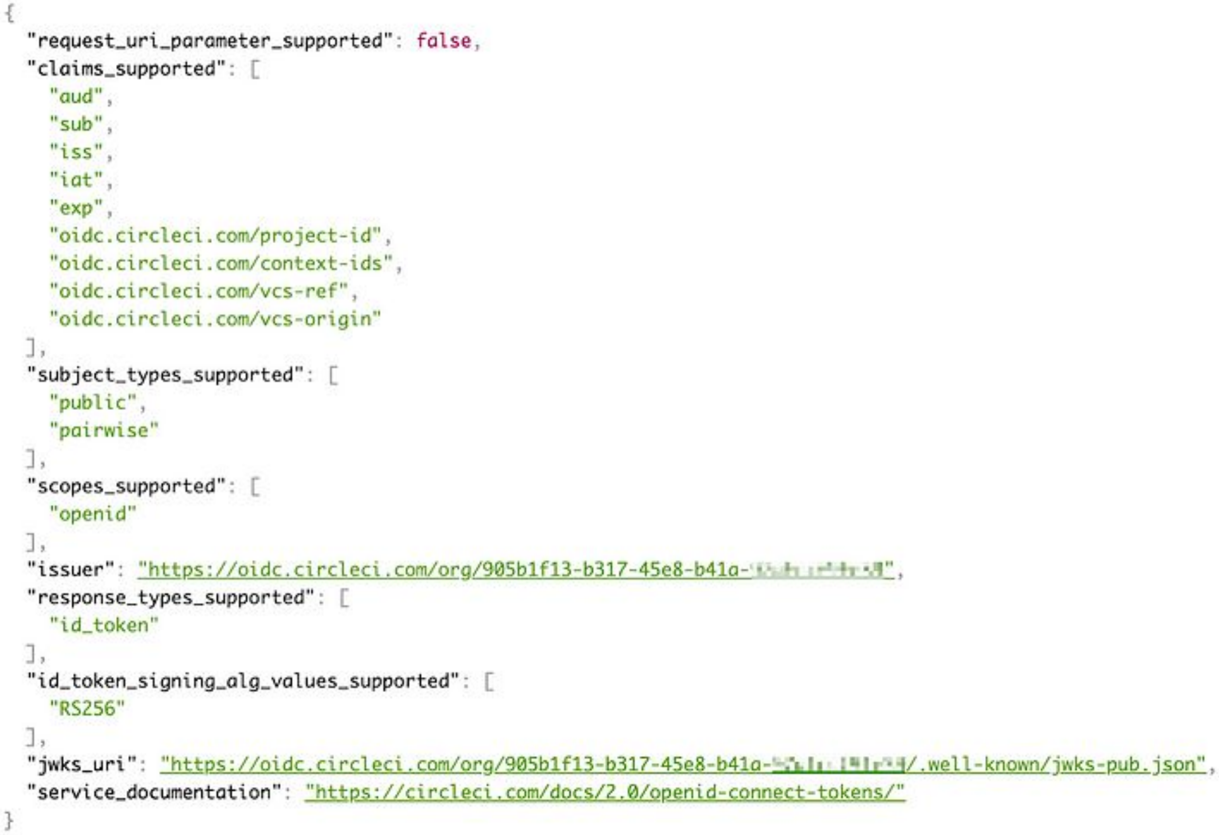
Delete
Add provider
Filter Identity providers by property or provider name and press enter
< 1 >

	Provider	Type	Creation time
○	oidc.circleci.com/org/7b75b559-4f9d-4ad0-92c5-[redacted]	OpenID Connect	28 days ago
○	oidc.eks.eu-central-1.amazonaws.com/id/3130A90F6D2378A25F12B9334E17754E	OpenID Connect	7 months ago
○	oidc.eks.eu-central-1.amazonaws.com/id/CDD57E319D3882F193FEE691EAAF5337	OpenID Connect	6 months ago
○	oidc.eks.eu-central-1.amazonaws.com/id/CFE7CB6ADC72EDD44BE42EF182B2C68B	OpenID Connect	2 years ago
○	oidc.eks.eu-central-1.amazonaws.com/id/D575532C808892DD56518BC795DDA06F	OpenID Connect	5 months ago
○	oidc.eks.eu-central-1.amazonaws.com/id/EEA4831A38ED5200D1CDA2EC92361773	OpenID Connect	6 months ago

Introduction to OIDC Federations

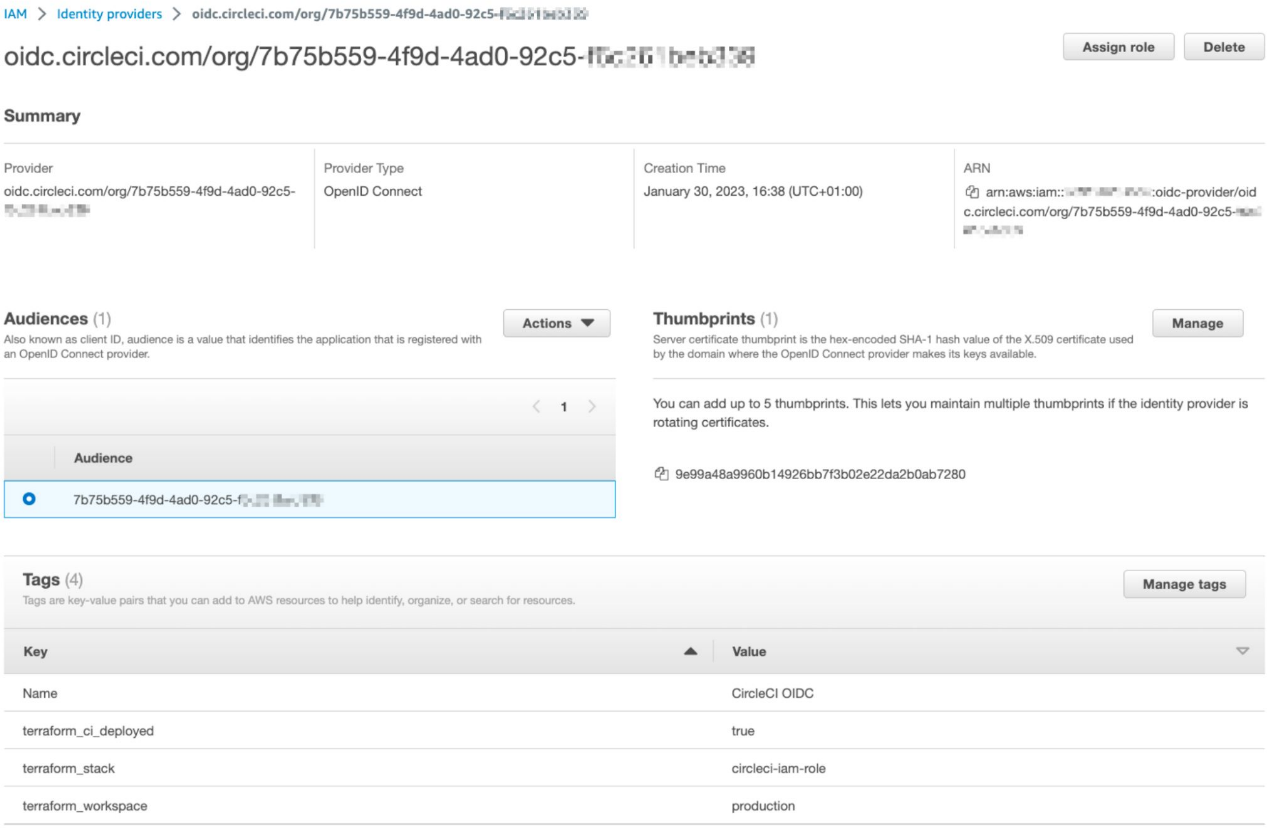
OIDC Configuration portal

https://<oidc>/.well-known/openid-configuration



```
{
  "request_uri_parameter_supported": false,
  "claims_supported": [
    "aud",
    "sub",
    "iss",
    "iat",
    "exp",
    "oidc.circleci.com/project-id",
    "oidc.circleci.com/context-ids",
    "oidc.circleci.com/vcs-ref",
    "oidc.circleci.com/vcs-origin"
  ],
  "subject_types_supported": [
    "public",
    "pairwise"
  ],
  "scopes_supported": [
    "openid"
  ],
  "issuer": "https://oidc.circleci.com/org/905b1f13-b317-45e8-b41a-[redacted]",
  "response_types_supported": [
    "id_token"
  ],
  "id_token_signing_alg_values_supported": [
    "RS256"
  ],
  "jwks_uri": "https://oidc.circleci.com/org/905b1f13-b317-45e8-b41a-[redacted]/.well-known/jwks-pub.json",
  "service_documentation": "https://circleci.com/docs/2.0/openid-connect-tokens/"
}
```

Introduction to OIDC Federations



IAM > Identity providers > oidc.circleci.com/org/7b75b559-4f9d-4ad0-92c5-[redacted]
Assign role
Delete

oidc.circleci.com/org/7b75b559-4f9d-4ad0-92c5-[redacted]

Summary

Provider
oidc.circleci.com/org/7b75b559-4f9d-4ad0-92c5-[redacted]

Provider Type
OpenID Connect

Creation Time
January 30, 2023, 16:38 (UTC+01:00)

ARN
arn:aws:iam::[redacted]:oidc-provider/oidc.circleci.com/org/7b75b559-4f9d-4ad0-92c5-[redacted]

Audiences (1)

Also known as client ID, audience is a value that identifies the application that is registered with an OpenID Connect provider.

	Audience
●	7b75b559-4f9d-4ad0-92c5-f[redacted]

Thumbprints (1)

Server certificate thumbprint is the hex-encoded SHA-1 hash value of the X.509 certificate used by the domain where the OpenID Connect provider makes its keys available.

You can add up to 5 thumbprints. This lets you maintain multiple thumbprints if the identity provider is rotating certificates.

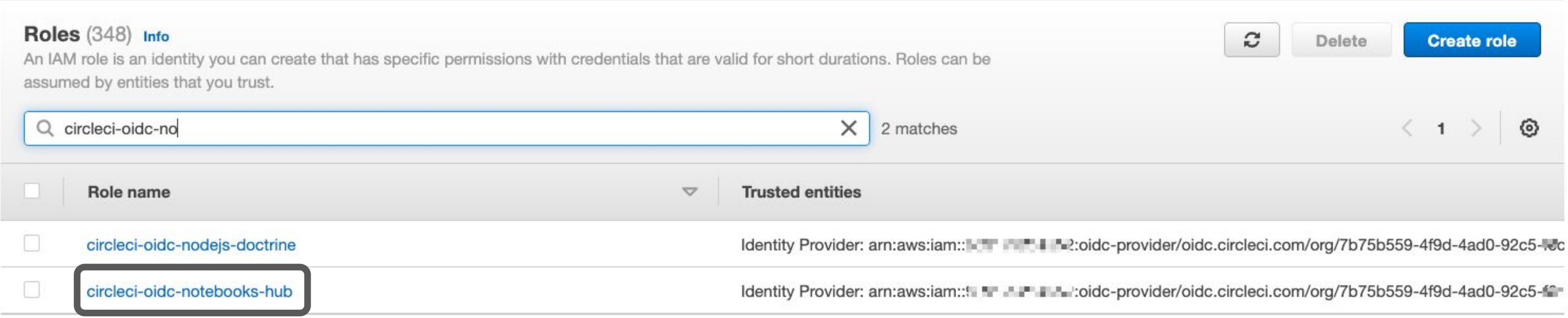
9e99a48a9960b14926bb7f3b02e22da2b0ab7280

Tags (4)

Tags are key-value pairs that you can add to AWS resources to help identify, organize, or search for resources.

Key ▲	Value ▽
Name	CircleCI OIDC
terraform_ci_deployed	true
terraform_stack	circleci-iam-role
terraform_workspace	production

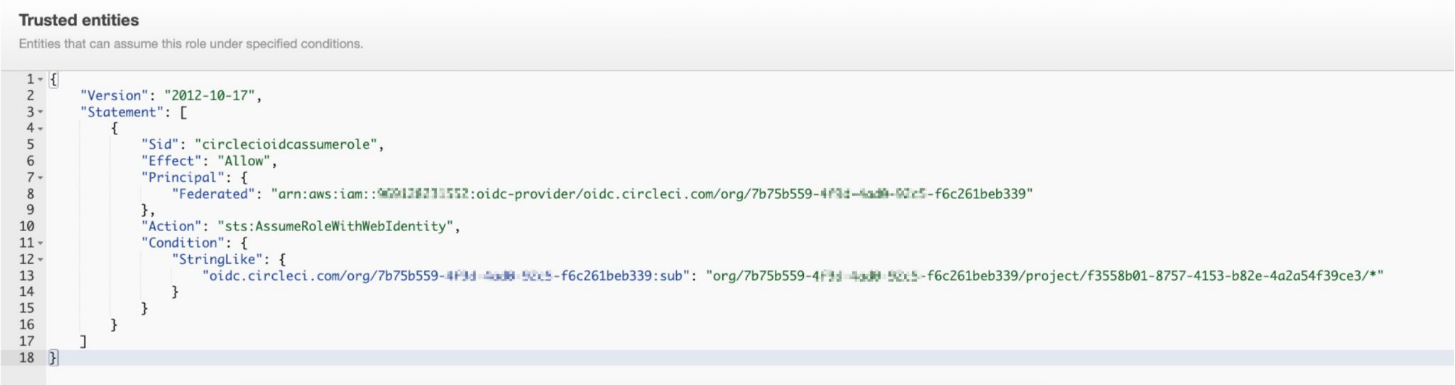
Setup the OIDC Federation



Roles (348) Info

An IAM role is an identity you can create that has specific permissions with credentials that are valid for short durations. Roles can be assumed by entities that you trust.

Role name	Trusted entities
circleci-oidc-nodejs-doctrine	Identity Provider: arn:aws:iam::[redacted]:oidc-provider/oidc.circleci.com/org/7b75b559-4f9d-4ad0-92c5-[redacted]
circleci-oidc-notebooks-hub	Identity Provider: arn:aws:iam::[redacted]:oidc-provider/oidc.circleci.com/org/7b75b559-4f9d-4ad0-92c5-[redacted]

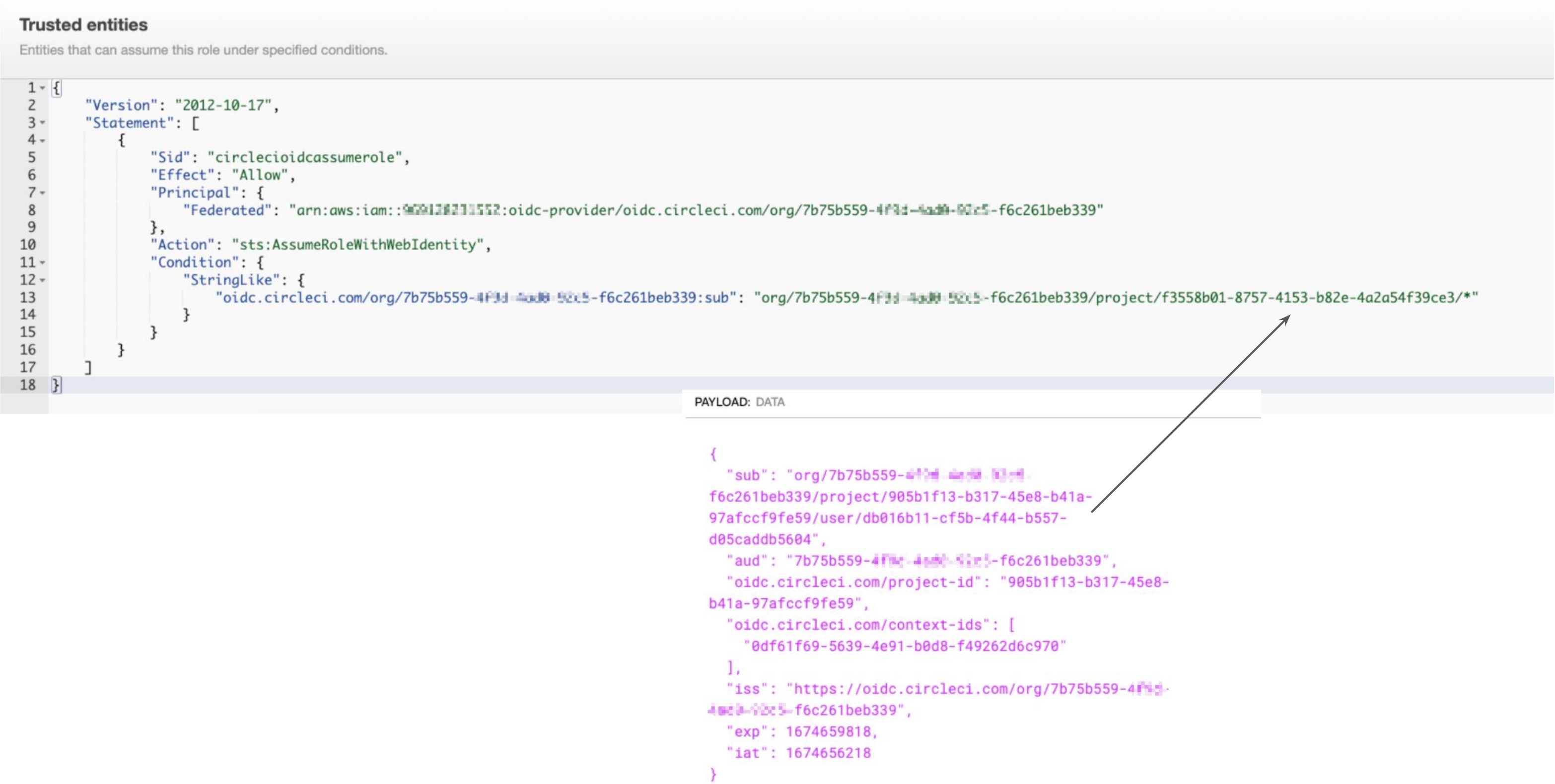


Trusted entities

Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "circlecioidcassumerole",
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::[redacted]:oidc-provider/oidc.circleci.com/org/7b75b559-[redacted]-f6c261beb339"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringLike": {
                    "oidc.circleci.com/org/7b75b559-[redacted]-f6c261beb339:sub": "org/7b75b559-[redacted]-f6c261beb339/project/f3558b01-8757-4153-b82e-4a2a54f39ce3/*"
                }
            }
        }
    ]
}
```

We aim to keep our secrets for ourselves



Trusted entities

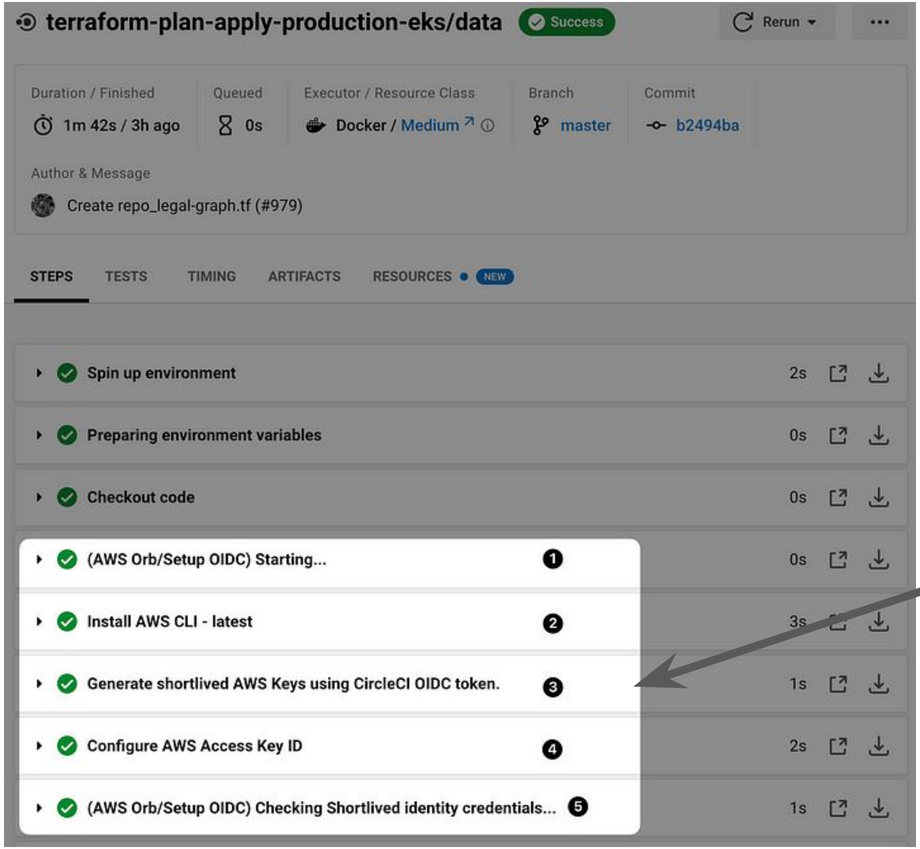
Entities that can assume this role under specified conditions.

```
{
    "Version": "2012-10-17",
    "Statement": [
        {
            "Sid": "circlecioidcassumerole",
            "Effect": "Allow",
            "Principal": {
                "Federated": "arn:aws:iam::[redacted]:oidc-provider/oidc.circleci.com/org/7b75b559-[redacted]-f6c261beb339"
            },
            "Action": "sts:AssumeRoleWithWebIdentity",
            "Condition": {
                "StringLike": {
                    "oidc.circleci.com/org/7b75b559-[redacted]-f6c261beb339:sub": "org/7b75b559-[redacted]-f6c261beb339/project/f3558b01-8757-4153-b82e-4a2a54f39ce3/*"
                }
            }
        }
    ]
}
```

PAYLOAD: DATA

```
{
  "sub": "org/7b75b559-[redacted]
f6c261beb339/project/905b1f13-b317-45e8-b41a-
97afccf9fe59/user/db016b11-cf5b-4f44-b557-
d05caddb5604",
  "aud": "7b75b559-[redacted]-f6c261beb339",
  "oidc.circleci.com/project-id": "905b1f13-b317-45e8-
b41a-97afccf9fe59",
  "oidc.circleci.com/context-ids": [
    "0df61f69-5639-4e91-b0d8-f49262d6c970"
  ],
  "iss": "https://oidc.circleci.com/org/7b75b559-[redacted]
f6c261beb339",
  "exp": 1674659818,
  "iat": 1674656218
}
```

Integration on CircleCI



terraform-plan-apply-production-eks/data — Success

Duration / Finished: 1m 42s / 3h ago

Queued: 0s

Executor / Resource Class: Docker / Medium

Branch: master

Commit: b2494ba

Author & Message: Create repo_legal-graph.tf (#979)

Spin up environment	2s
Preparing environment variables	0s
Checkout code	0s
(AWS Orb/Setup OIDC) Starting... 1	0s
Install AWS CLI - latest 2	3s
Generate shortlived AWS Keys using CircleCI OIDC token. 3	1s
Configure AWS Access Key ID 4	2s
(AWS Orb/Setup OIDC) Checking Shortlived identity credentials... 5	1s

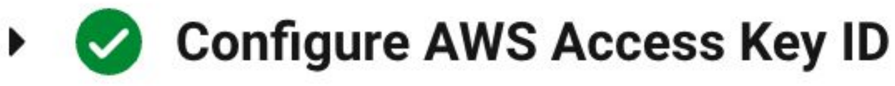
```yaml
jobs:
 terraform-plan-apply:
   executor: python
   parameters:
     stack:
       type: string
   steps:
     - checkout:
         path: ~/project/
     - doctrine-common-aws/setup-oidc
```

Integration on CircleCI

Generate shortlived AWS Keys using CircleCI OIDC token.

```
aws sts assume-role-with-web-identity \\
--role-arn "${PARAM_AWS_CLI_ROLE_ARN}" \\
--role-session-name "${PARAM_ROLE_SESSION_NAME}" \\
--web-identity-token "${CIRCLE_OIDC_TOKEN}" \\
--duration-seconds "${PARAM_SESSION_DURATION}" \\
--query 'Credentials.[AccessKeyId,SecretAccessKey,SessionToken]' \
--output text
```

Integration on CircleCI



▸ ✓ Configure AWS Access Key ID

4

```
aws configure set aws_access_key_id \\
  "$PARAM AWS CLI ACCESS KEY ID" \\
  --profile "$PARAM_AWS_CLI_PROFILE_NAME"
```

```
aws configure set aws_secret_access_key \\
"$PARAM AWS CLI SECRET ACCESS KEY" \\
  --profile "$PARAM_AWS_CLI_PROFILE_NAME"
```

```
aws configure set aws_session_token \\
    "${AWS_SESSION_TOKEN}" \\
   --profile "$PARAM_AWS_CLI_PROFILE_NAME"
```

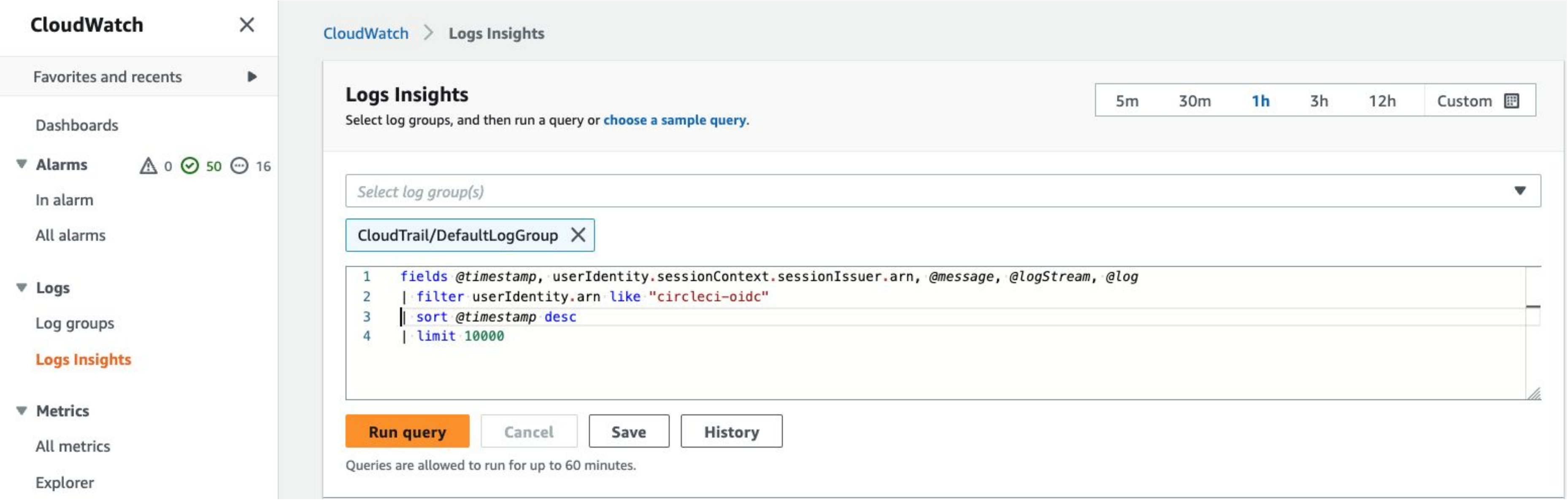
What benefits ?

No more long-term AWS programmatic keys stored

1 CI project = 1 role

Audit at CI project level

What benefits ?



Logs Insights

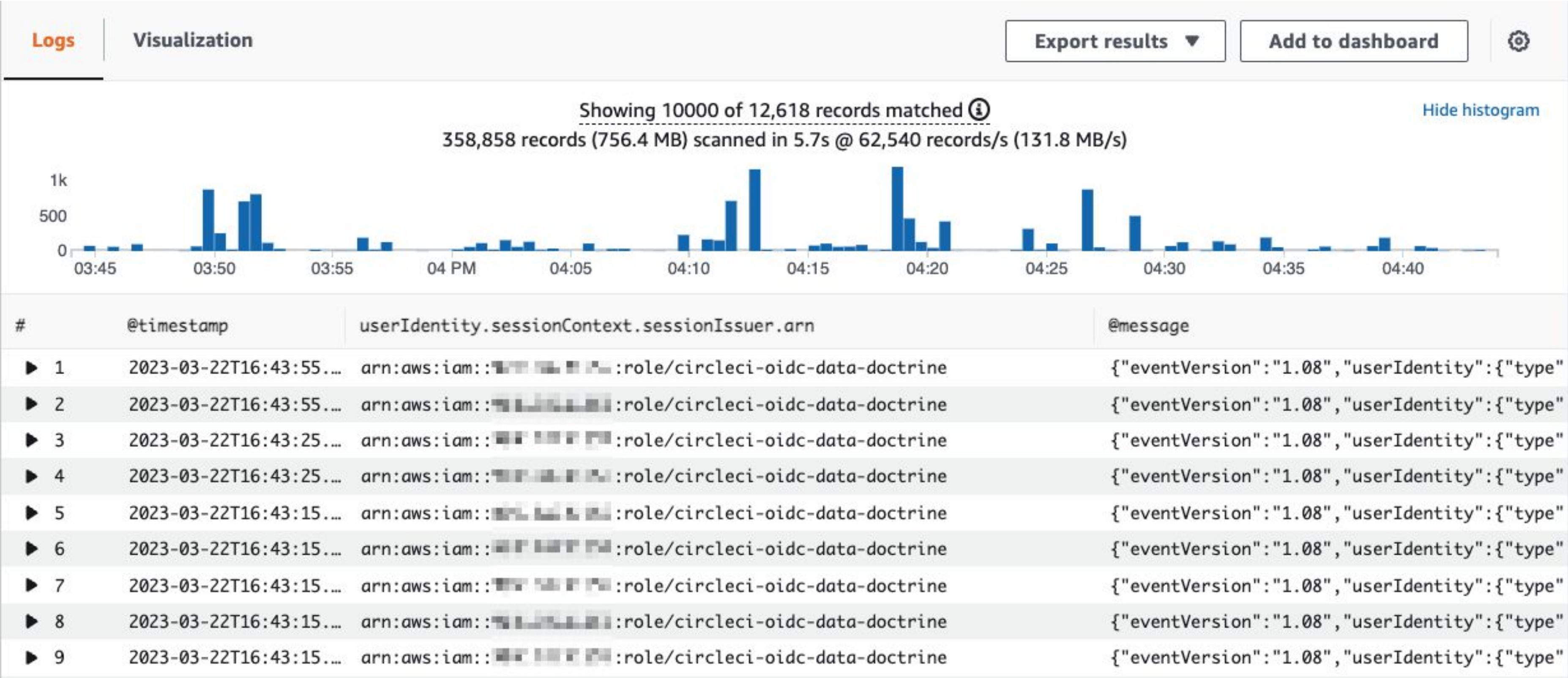
Select log groups, and then run a query or choose a sample query.

CloudTrail/DefaultLogGroup

```
fields @timestamp, userIdentity.sessionContext.sessionIssuer.arn, @message, @logStream, @log
 | filter userIdentity.arn like "circleci-oidc"
 | sort @timestamp desc
 | limit 10000
```

Queries are allowed to run for up to 60 minutes.

What benefits ?

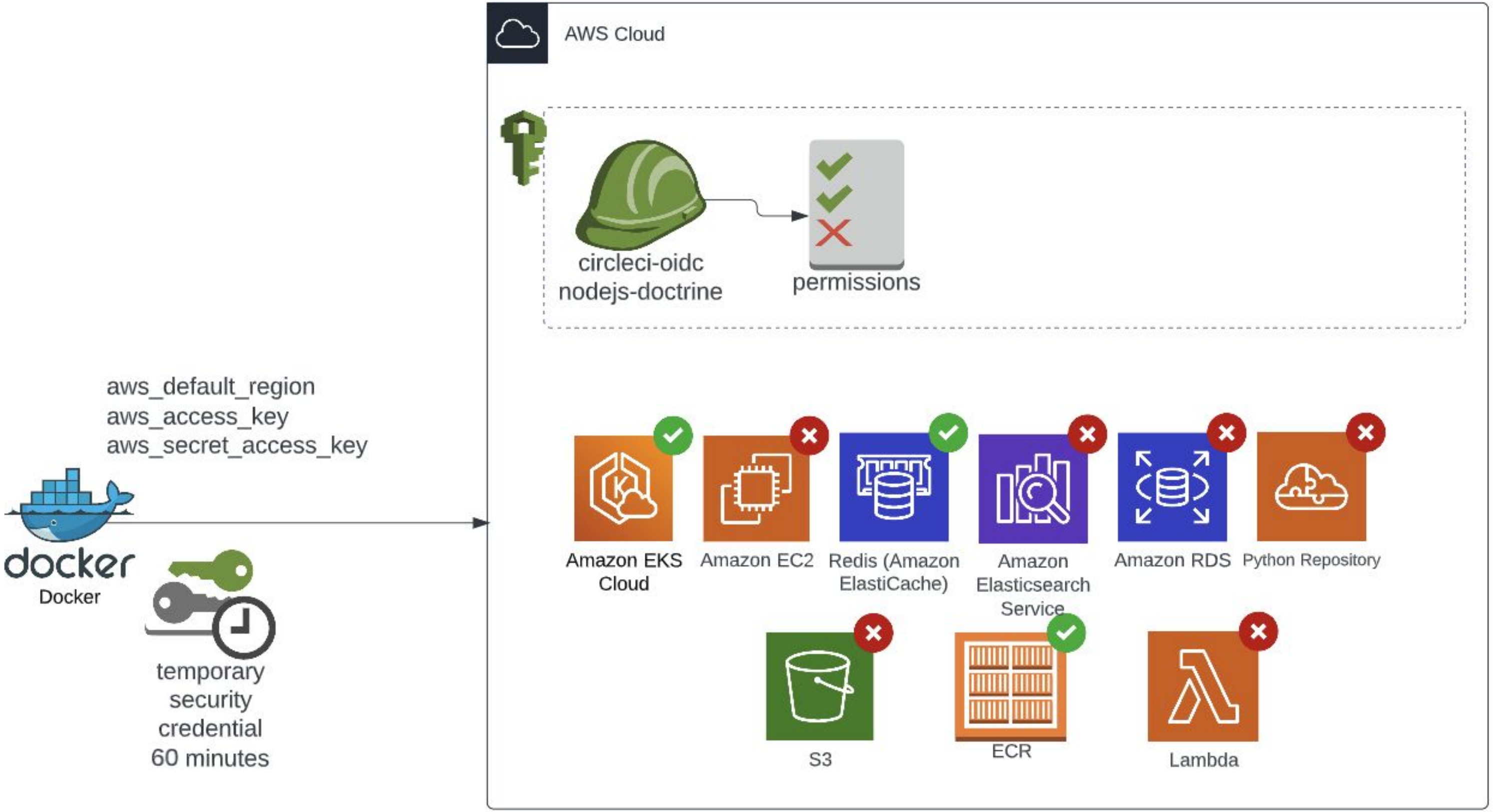


Showing 10000 of 12,618 records matched

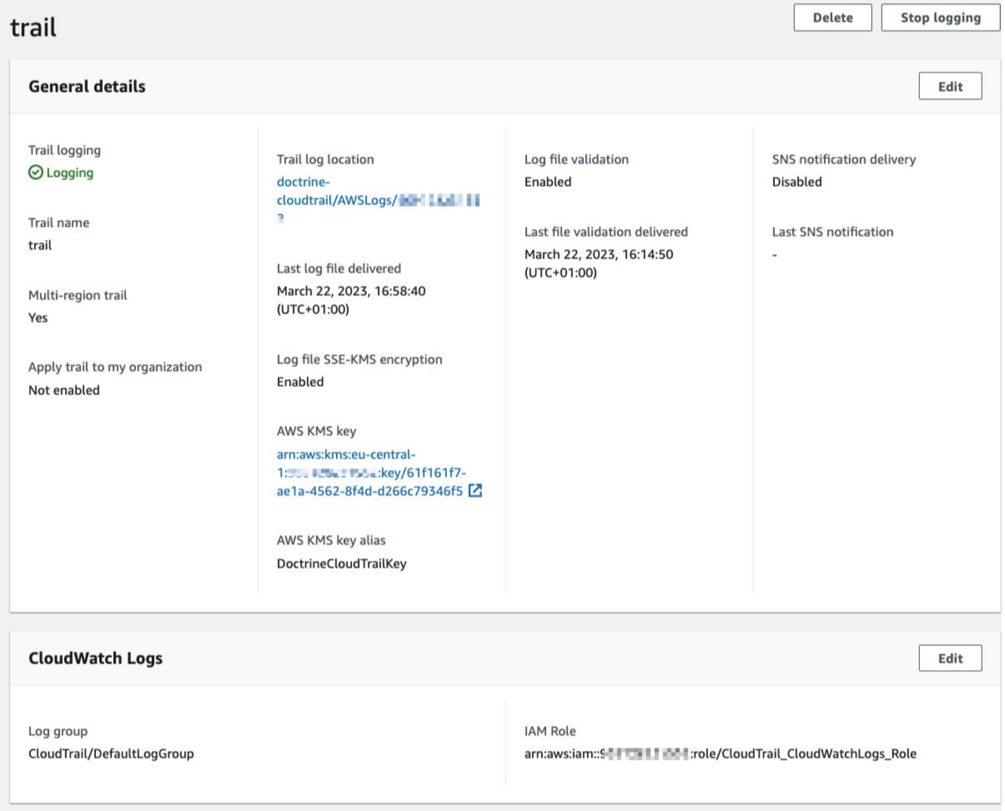
358,858 records (756.4 MB) scanned in 5.7s @ 62,540 records/s (131.8 MB/s)

#	@timestamp	userIdentity.sessionContext.sessionIssuer.arn	@message
▶ 1	2023-03-22T16:43:55.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"
▶ 2	2023-03-22T16:43:55.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"
▶ 3	2023-03-22T16:43:25.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"
▶ 4	2023-03-22T16:43:25.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"
▶ 5	2023-03-22T16:43:15.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"
▶ 6	2023-03-22T16:43:15.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"
▶ 7	2023-03-22T16:43:15.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"
▶ 8	2023-03-22T16:43:15.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"
▶ 9	2023-03-22T16:43:15.…	arn:aws:iam::[redacted]:role/circleci-oidc-data-doctrine	{"eventVersion":"1.08","userIdentity":{"type"

Least-Permissive IAM Statements



Least-Permissive IAM Statements



trail

General details

Trail logging
✓ Logging

Trail name
trail

Multi-region trail
Yes

Apply trail to my organization
Not enabled

Trail log location
doctrine-cloudtrail/AWSLogs/[redacted]

Last log file delivered
March 22, 2023, 16:58:40 (UTC+01:00)

Log file SSE-KMS encryption
Enabled

AWS KMS key
arn:aws:kms:eu-central-1:[redacted]:key/61f161f7-ae1a-4562-8f4d-d266c79346f5

AWS KMS key alias
DoctrineCloudTrailKey

Log file validation
Enabled

Last file validation delivered
March 22, 2023, 16:14:50 (UTC+01:00)

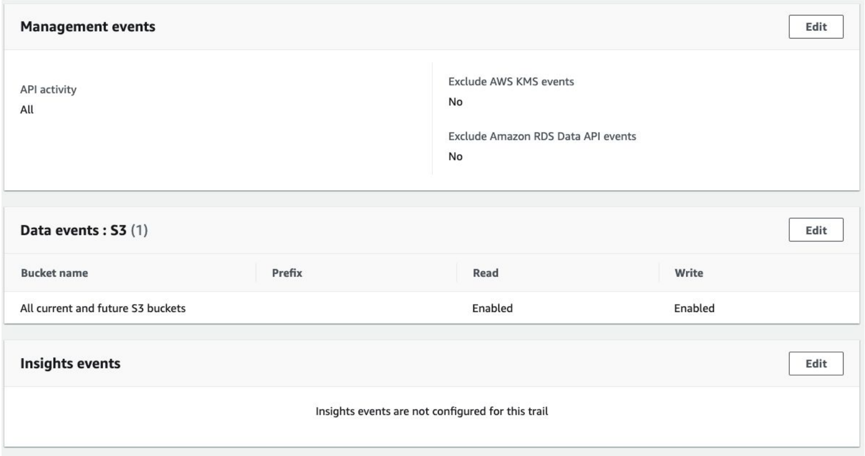
SNS notification delivery
Disabled

Last SNS notification
-

CloudWatch Logs

Log group
CloudTrail/DefaultLogGroup

IAM Role
arn:aws:iam::[redacted]:role/CloudTrail_CloudWatchLogs_Role



Management events

API activity
All

Exclude AWS KMS events
No

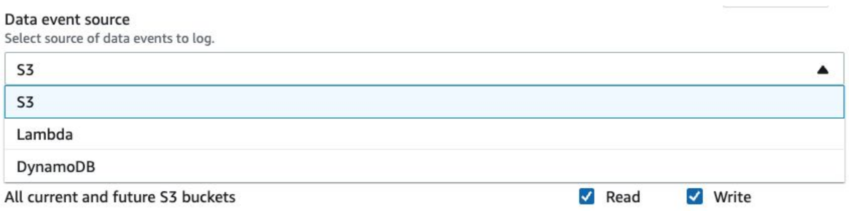
Exclude Amazon RDS Data API events
No

Data events : S3 (1)

Bucket name	Prefix	Read	Write
All current and future S3 buckets		Enabled	Enabled

Insights events

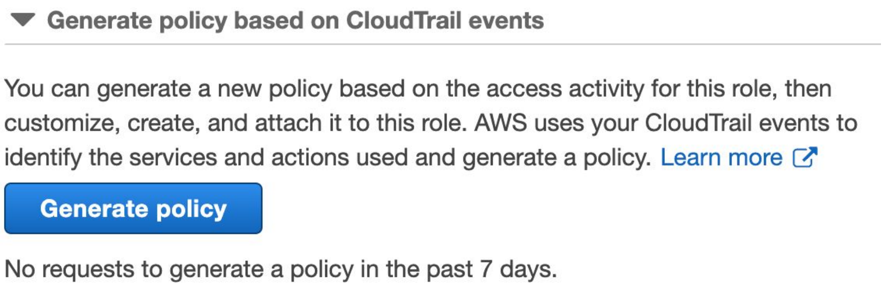
Insights events are not configured for this trail



Data event source
Select source of data events to log.

All current and future S3 buckets ☑ Read ☑ Write

Least-Permissive IAM Statements



▼ Generate policy based on CloudTrail events

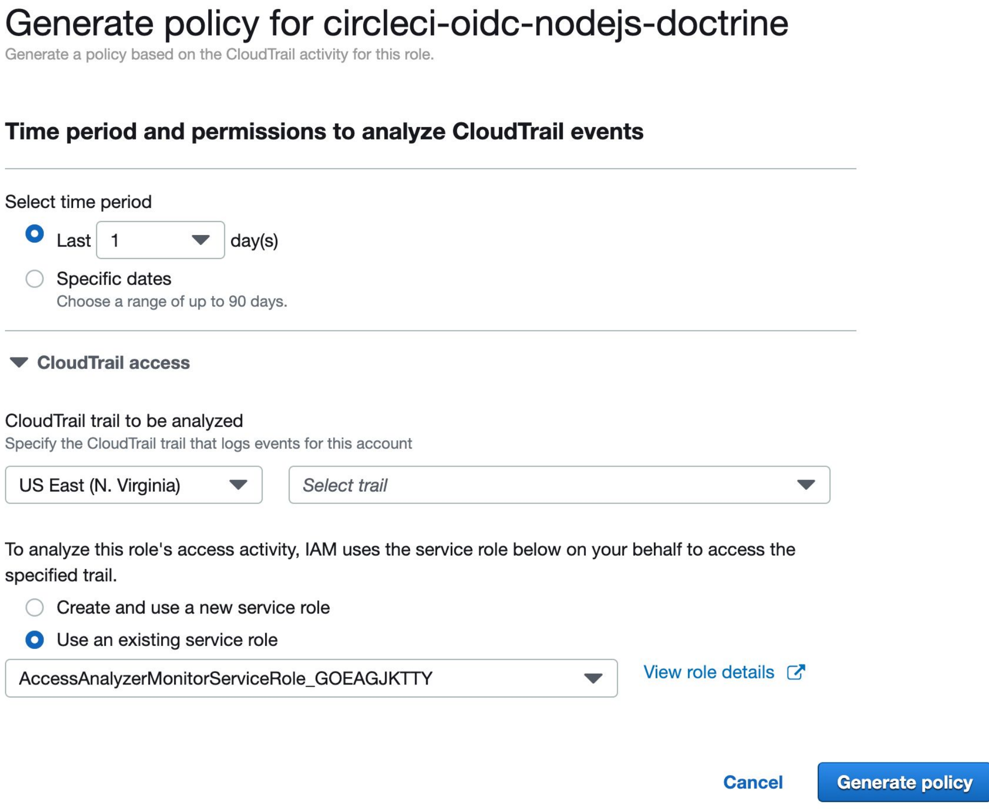
You can generate a new policy based on the access activity for this role, then customize, create, and attach it to this role. AWS uses your CloudTrail events to identify the services and actions used and generate a policy. Learn more

No requests to generate a policy in the past 7 days.

(AWS) IAM Policy Generator

CloudTracker

TrailScaper



Generate policy for circleci-oidc-nodejs-doctrine

Generate a policy based on the CloudTrail activity for this role.

Time period and permissions to analyze CloudTrail events

Select time period

● Last 1 day(s)

○ Specific dates

Choose a range of up to 90 days.

▼ CloudTrail access

CloudTrail trail to be analyzed

Specify the CloudTrail trail that logs events for this account

US East (N. Virginia) | *Select trail*

To analyze this role's access activity, IAM uses the service role below on your behalf to access the specified trail.

○ Create and use a new service role

● Use an existing service role

AccessAnalyzerMonitorServiceRole_GOEAGJKTTY

Wrap-Up

☀️ Multiple benefits to migrate to OIDC Federation

🗝️ No more AWS keys to handle, to rotate, … to leak
🔍 Better Audit

🚀 Quick to implement, easy to operate and reliable

💬 Mind the OIDC token payload

😮‍💨 Least-Permissions automated generation is tricky

1e plateforme d'intelligence juridique

www.doctrine.fr

Thank you !

https://benriou.medium.com

https://medium.com/doctrine