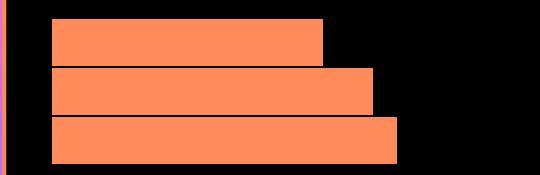




ORY / summit-22

Mal Curtis



✉ mal@mal.co.nz

ORY in the  
inMusic Cloud

20 - 10 - 2022  
@ Ory Summit 2022



ORY in the inMusic Cloud

#ory-summit

2

# inMusic

HOME OF THE WORLD'S PREMIER MUSIC AND AUDIO TECHNOLOGY BRANDS

air

AKAI  
PROFESSIONAL

ALESIS

ALTO  
PROFESSIONAL

DENON DJ

DENON  
PROFESSIONAL

HEADRUSH

ION

M-AUDIO

marantz  
PROFESSIONAL

MARQ

MixMeister

Numark

RANE

SONIVOX

arkaos

Switch  
Sounds

stanton



# DENON DJ



# Numark®



# HEADRUSH



# AKAI PROFESSIONAL





The screenshot shows the BFD3 software interface. At the top, there's a menu bar with File, Tools, Help, Presets, Kits, Drums, Grooves, Auto, Kit, Effects, Groove Editor, Key Map, and Tech. The title is "Presets Dashboard - Emre HipHop 1". On the right, there are track controls for Volume (95.00), Pan (4 / 4), and Gain. Below the title, there are tabs for Audience, Drummer, Select, and Link. The main area features a 3D drum set visualization with various drums and cymbals labeled with OH (Overhead) microphones. Below the visualization is a grid of controls for the "Drummer" kit. The grid includes sections for Export, View, Faders, Effects, Sends, Tweaks, and a Mini Mixer. Each section contains multiple knobs and buttons for adjusting sound parameters. To the right of the main controls, there are sections for General (with a preview image of a snare drum), Tuning (st 3.36 Hz, Tune st), Bleed (Kick, Snare, Dir, On, Trim, Send, Return), and Loudness (Range 0-1000, Curve 0-100, Vel Dyn 0-100). The bottom right corner shows a section for Ambient Mics with various衰减器 (Attenuators) and trim controls.

ORY in the inMusic Cloud

#ory-summit

# Overview

The inMusic Cloud

What ORY services inMusic uses

How we use Hydra

How we use Oathkeeper

How we use Keto

Questions



# The inMusic Cloud

Product Purchases and Registrations

Software Authorization / Unlock

Software / Firmware updates

Brand Specific Profiles and “Clouds”

Headrush Cloud

Engine Cloud

# The inMusic Cloud

Homogenous REST and GraphQL API

Authenticated via inMusic Profile (Hydra + Magento)

Heterogenous service based architecture

Go, Python, Javascript, PHP

Provided to internal teams as a service.

# The inMusic Cloud

Monorepo. Docker. Gitlab. AWS ECS. Terraform.

55 services at last count

Contract driven: RPC services defined with Protocol  
Buffers

# The inMusic Cloud

Protocol Buffer RPC definitions are the source of truth

REST via grpc HTTP Gateway protoc-gen-grpc-gateway

GraphQL via 99designs gqlgen protoc-gen-gogql

Validation via Envoy protoc-gen-validate

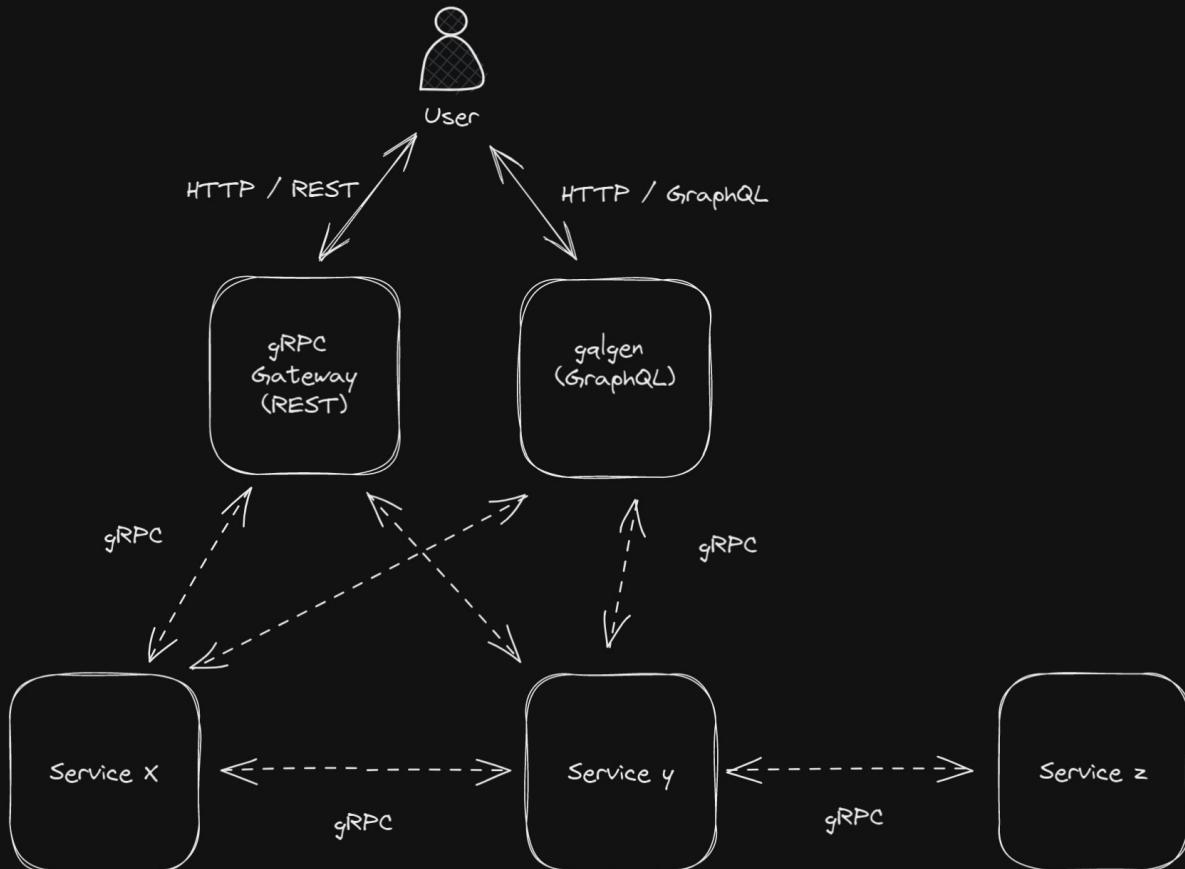
Documentation Site

docusaurus

GraphQL Explorer - GraphiQL

REST Explorer Stoplight Elements

protoc-gen-openapiv2



# List Connectable Accounts

**GET** [https://api.inmusicbrands.com/v1/connectable\\_accounts/{namespace}](https://api.inmusicbrands.com/v1/connectable_accounts/{namespace})

List a set of account providers for a specific namespace.

## Request

Security: OAuth 2.0  
Authorization Code OAuth Flow  
Authzrize URL: <https://auth.profile.inmusicbrands.com/oauth2/auth>  
Token URL: <https://auth.profile.inmusicbrands.com/oauth2/token>

## Path Parameters

**namespace** string required  
Allowed values: NAMESPACE\_INMUSIC\_PROFILE, NAMESPACE\_INMUSIC\_SOFTWARE\_INSTALLER, NAMESPACE\_ENGINE, NAMESPACE\_HEADRUSH

## Responses

200 default

A successful response.

## Body

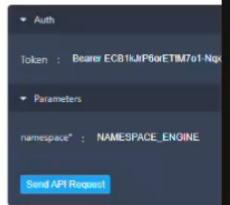
**accounts** array[object] required

**provider** string  
Allowed values: ACCOUNT\_PROVIDER\_DROPBOX, ACCOUNT\_PROVIDER\_BEATPORT, ACCOUNT\_PROVIDER\_BEATSOURCE, ACCOUNT\_PROVIDER\_SOUNDCLLOUD, ACCOUNT\_PROVIDER\_TIDAL, ACCOUNT\_PROVIDER\_AMAZON\_MUSIC

**name** string required  
Example: Dropbox

**is\_connected** boolean required

**initiate\_connection\_url** string<curl> required  
Example: [https://api.inmusicbrands.com/connectable\\_accounts/dropbox/initiate](https://api.inmusicbrands.com/connectable_accounts/dropbox/initiate)



Request Sample: Shell / cURL ▾  
curl --request GET \  
--url https://api.inmusicbrands.com/v1/connectable\_accounts/{namespace} \  
--header 'Authorization: Bearer {token}' \  
--header 'Content-Type: application/json'

Response Example  
1 {  
2 "accounts": [  
3 {  
4 "provider": "ACCOUNT\_PROVIDER\_DROPBOX",  
5 "name": "Dropbox",  
6 "is\_connected": true,  
7 "initiate\_connection\_url": "[https://api.inmusicbrands.com/connectable\\_accounts/dropbox/initiate](https://api.inmusicbrands.com/connectable_accounts/dropbox/initiate)"  
8 }  
9 ]  
10 }

```

19 // devices that need to be authenticated against a service
20 // Accounts are namespaced so that each namespace can have
21 // linked account for each Account Provider. This allows
22 // account for say, Akai Pro, than you have for Engine.
23 service ConnectedAccountsService {
24   option (graphql.v1.svc) = {
25     type : QUERY
26     name : ""
27     upstream : UPSTREAM_CLIENT
28   };
29
30 // List Connectable Accounts
31
32 // List a set of account providers for a specific namespace
33 rpc ListConnectableAccounts(ListConnectableAccountsRequest)
34   returns (ListConnectableAccountsResponse) {
35   option (google.api.http) = {
36     get : "/v1/connectable_accounts/{namespace}"
37   };
38   option (grpc.gateway.protoc_gen_openapiv2.options.openapi) = {
39     tags : "Connected Accounts 🔍"
40   };
41 }
42
43 // Get Account Credentials
44 //
45 // Returns current credentials for the supplied namespace
46 // When requesting credentials that are expired, they are
47 // renewed via the request.
48 rpc GetAccountCredentials(GetAccountCredentialsRequest)
49   returns (GetAccountCredentialsResponse) {
50   option (google.api.http) = {
51     get : "/v1/connectable_accounts/{namespace}/{provider}"
52   };
53   option (grpc.gateway.protoc_gen_openapiv2.options.openapi) = {
54     tags : "Connected Accounts 🔍"
55   };
56 }
57
58 // Disconnected Account
59 //
60 // Deletes account credentials and marks the account type
61 rpc DisconnectAccount(DisconnectAccountRequest)
62   returns (DisconnectAccountResponse) {
63   option (google.api.http) = {
64     delete : "/v1/connectable_accounts/{namespace}/{provider}"
65   };
66   option (graphql.v1.rpc) = {
67     type : MUTATION
68   };
69   option (grpc.gateway.protoc_gen_openapiv2.options.openapi) = {
70     tags : "Connected Accounts 🔍"
71   };
72 }
```

GraphiQL ▶ Prettify Merge Copy History

```

1 # Welcome to GraphiQL
2 #
3 # GraphiQL is an in-browser tool for
4 # testing GraphQL queries.
5 #
6 # Type queries into this side of the
7 # typeahead's aware of the current Gr
8 # validation errors highlighted with
9 #
10 # GraphQL queries typically start wi
11 # with a # are ignored.
12 #
13 # An example GraphQL query might loc
14 #
15 # {
16 #   field(arg: "value") {
17 #     subField
18 #   }
19 # }
```

QUERY VARIABLES REQUEST HEADERS

# What ORY services?

Hydra

Backed by Magento  
Custom Device Auth implementation

Oathkeeper

Public API only  
Authed by Hydra OAuth2 Introspection  
JWT for Internal Services

Keto

User Groups  
Service based authorization



# How We Use Hydra

# How Why we use Hydra

inMusic Profile due to be released - Magento

Needed "Desktop Login" via inMusic Profile for BFD Player

No Session API existed

Existing user profiles merged from many brands

Hydra was best fit

Portable: not tied to Magento

Cloud Native, OSS, Standards Based (OAuth2)

Not trying to do too much

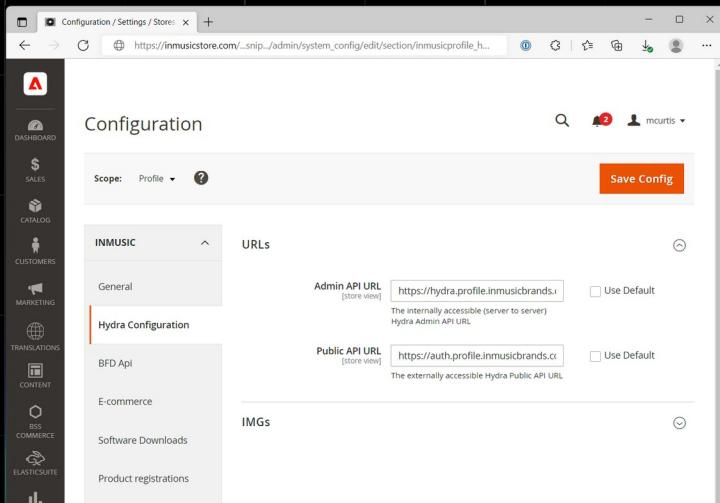
# How We Use Hydra

Custom Magento Module

Copied Login Controller and Views

Created Consent Controller

Managed via Admin Settings



# How We Use Hydra

Clients Managed via  
Terraform

```
resource "hydra_oauth2_client" "dev_inmusic_aws_canary" {
  client_id      = "dev.inmusic.aws.canary"
  client_name    = "AWS Canary Client"

  grant_types     = ["authorization_code", "refresh_token"]
  redirect_uris   = [
    "https://oauth-tokens.admin.local.inmusic.dev",
    "http://127.0.0.1:5555/callback",
  ]
  response_types   = ["code"]
  scopes          = ["email", "openid", "offline"]
  token_endpoint_auth_method = "none"
  lifecycle {
    ignore_changes = [
      "client_secret"
    ]
  }
}
```

The screenshot shows the Terraform Cloud interface. On the left, a sidebar lists 'Workspaces' (cloud-prod), 'Overview', 'Runs' (selected), 'States', 'Variables', and 'Settings'. The main area displays a run titled 'oauth: Allow canary client tokens locally' with status 'Applied'. It shows a log entry from 'Mal Curtis' triggered by a GitLab run 3 days ago. Below it, a 'Plan finished' message indicates 3 days ago with resources: 1 to add, 2 to change, 1 to destroy. A detailed view of the resource 'module.oauth\_clients.hydra\_oauth2\_client.dev\_inmusic\_aws\_canary[0]' is shown, listing its ID ('dev.inmusic.aws.canary') and redirect URIs ('https://oauth-tokens.admin.local.inmusic.dev'). At the bottom, there are buttons for 'Download Sentinel mocks' and 'Apply finished'.

# How We Use Hydra

Custom RFC 8628 Device Auth Implementation

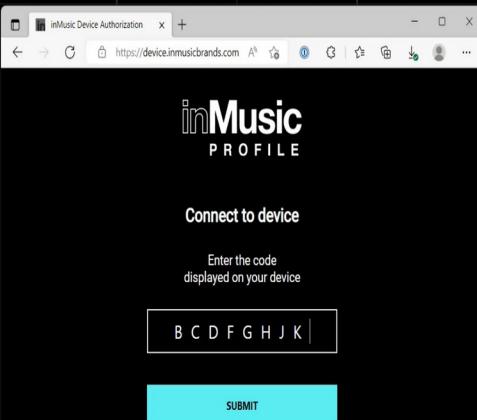
Adds Device Authorization API Endpoint

Handles "device code" Grant Type

Proxies other token requests

"Sidequests" force UI flows

"Brand Aware" UI



# How We Use Hydra

## Authorized Devices

Associates user agent data to consents in Hydra

A bit of a hack!

Provides remote logout

The screenshot shows the Engine DJ software interface. On the left, there's a sidebar with 'inMusic Account' and a 'Sign out' button. The main area is titled 'Authorized Devices' and lists various devices categorized by platform:

- Engine DJ OS**: Denon DJ SC6000 (XJKLASD), Last active 5 days ago, Sign Out; Denon DJ SC6000 (XJKLASD), Last active 5 days ago, Sign Out.
- Engine DJ Desktop**: Numark Mixstream Pro (XJKLASD), Last active 5 days ago, Sign Out; Denon DJ Prime 4 (XJKLASD), Last active 5 days ago, Sign Out.
- Engine DJ Website**: Mal's Windows Computer (Windows), Last active 5 days ago, Sign Out; Phil's Macbook Pro (MacOS), Last active 5 days ago, Sign Out.
- inMusic Account**: Chrome (MacOS), Last active 5 days ago, Sign Out.

# How We Use Oathkeeper

# How We Use Oathkeeper

Traefik "forward auth" middleware

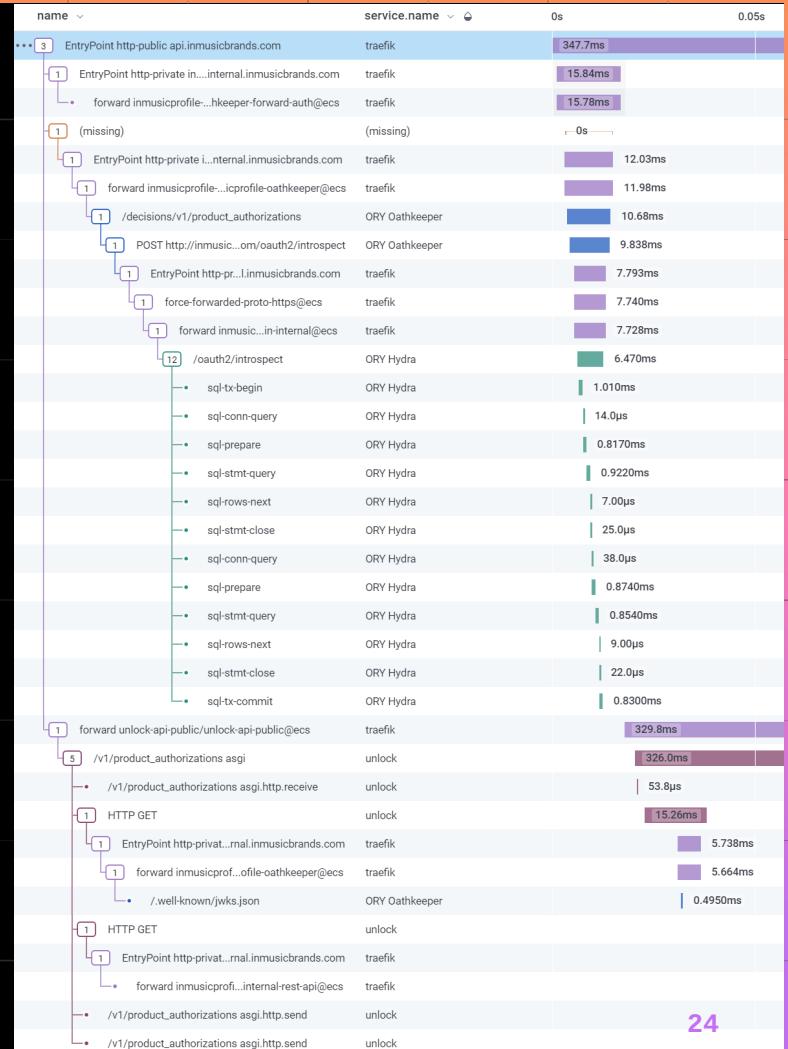
Forwards Request to Oathkeeper

Hydra Introspects OAuth2 token

Oathkeeper Writes JWT on success

Traefik forwards request w/ JWT

Service Validates JWT



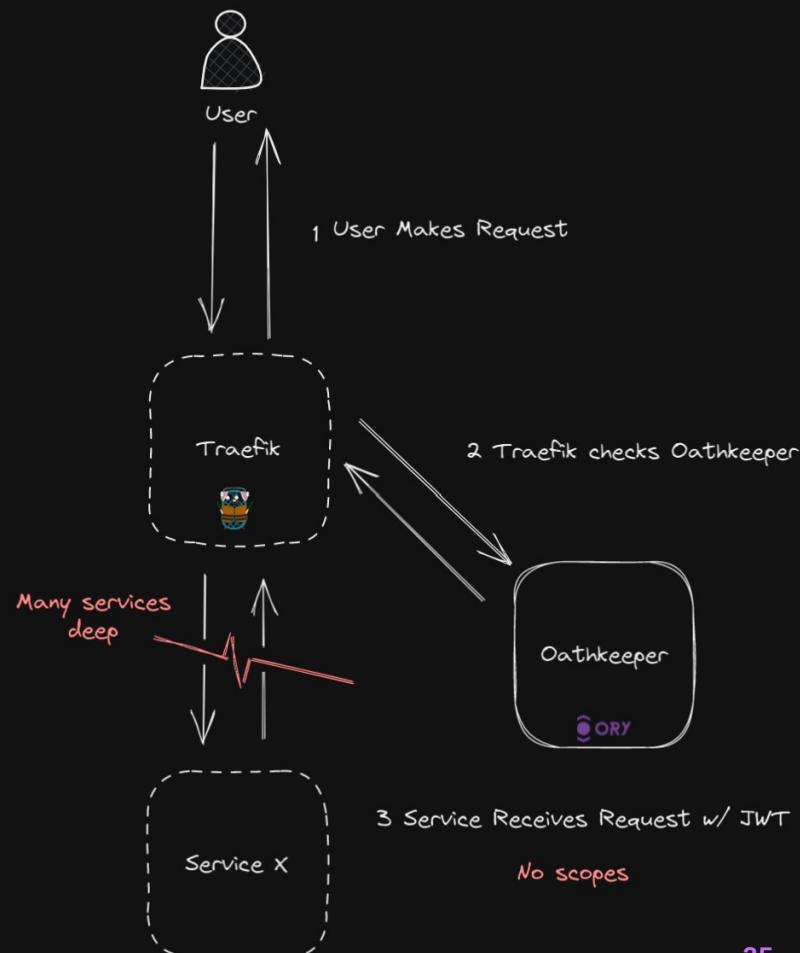
# Oathkeeper Problem

How to check scopes for  
GraphQL requests?

Single request may aggregate  
many different services

Services want to define their  
own scope requirements

Oathkeeper didn't assign  
scopes to JWTs



# Oathkeeper Problem

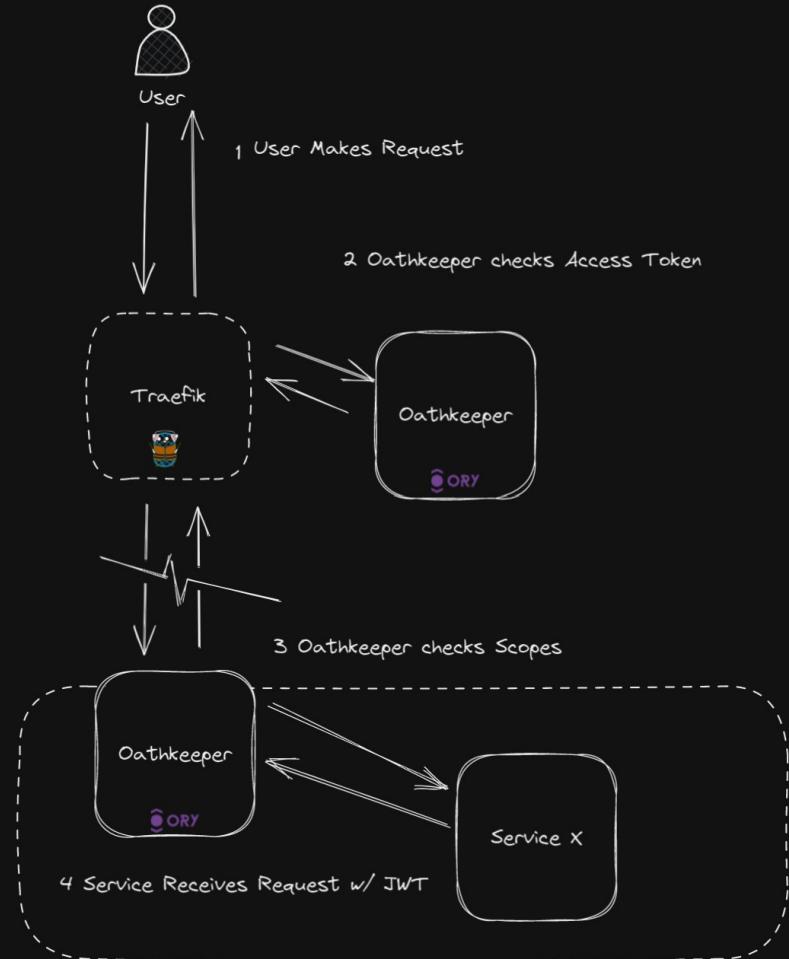
HTTP & GraphQL gateways  
"swallow" scopes

GraphQL especially hard to  
enforce at edge

Recently added Scopes to  
Oathkeeper JWT Claims

Plan to add Oathkeeper sidecar  
to enforce scopes

Remove service JWT check



# How We Use Keto

# How We Use Keto

Only recently spun up

## User Groups

```
usergroup:engine/beta-testers#member@<user_id>

message UserGroupMembership {
    inmusicapi.v1.Namespace namespace = 1;
    string user_group = 2;
    string user_id = 3;
}
```

## Service Permissions

```
software-installer/version:<sku>/<platform>/<version>#access@<user_id>
arkaos/lighting-stream:<owner_id>/<stream_id>#access@<user_id>

message DomainObjectAccess {
    inmusicapi.v1.Domain domain = 1;
    string object = 2;
    string user_id = 3;
}
```

### inMusic Cloud Admin API

#### Overview

#### ENDPOINTS

App Entitlements

Devices

Files

Serials

Software Installer

Software Unlock

Users

Get Profile Set

Update Profile Set

Batch Get User Group Memberships

List User Group Memberships

Create User Group Membership

Get User Group Membership

Delete User Group Membership

List Customer Product Registrations

Create Customer Product Registrations

List Customer Product Registrations

Create Customer Product Registrations

#### SCHEMAS

Authorization

AuthsList

ClearDeauthorisationsRequest

CreateDemo

Deauthorization

DeauthsList

Demo

## List User Group Memberships

GET

[https://.inmusic.dev/admin/v1/user\\_groups/{user\\_group\\_key.id}/members](https://.inmusic.dev/admin/v1/user_groups/{user_group_key.id}/members)

## Request

> Security: OAuth 2.0

## Path Parameters

`user_group_key.id` string

The group identifier. This is a simple, hyphenated, string that represents the group.

`user_group_key.namespace` string

The namespace within inMusic that this user group belongs to.

Allowed values: `NAMESPACE_INMUSIC_PROFILE` `NAMESPACE_INMUSIC_SOFTWARE_INSTALLER`

## Query Parameters

`page_size` integer<int64>

How many results to return per page.

Default: 100

`page_token` string

The `page_metadata.next_page_token` from a previous page of results.

## Responses

200

default

A successful response.

## Body

# How We Use Keto

"Permissions" service

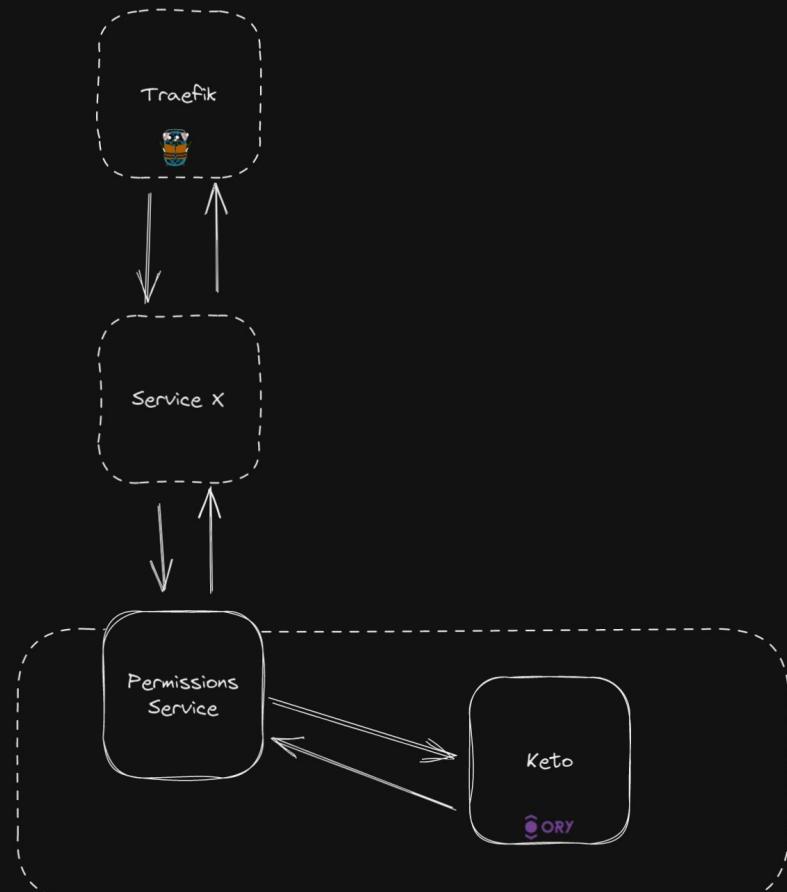
abstracts Keto away

enforces "inMusic" concepts

Keto runs as a sidecar

Not exposed directly to services

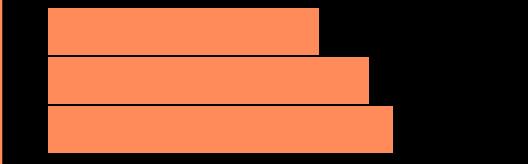
Managing Migrations TBD





ORY / summit-22

Mal Curtis



✉️ [mal@mal.co.nz](mailto:mal@mal.co.nz)

# Questions?

Hit me up on  
the ORY Slack

20 - 10 - 2022  
@ Ory Summit 2022