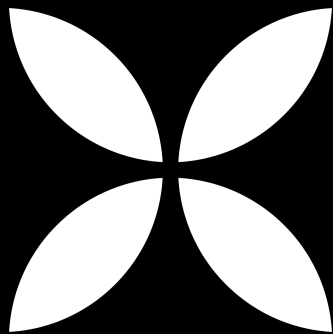




**Rendez vos développeurs autonomes
sur la production**

Mathieu Corbin

Senior Staff SRE @Qonto

<https://www.mcorbin.fr/>

@_mcorbin



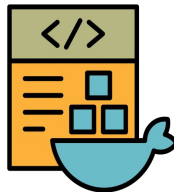
500k clients, 8 pays



1600+ Qontoers



> 150 déploiements en prod
par jour



450 services en prod



Silos

Dev



Développe



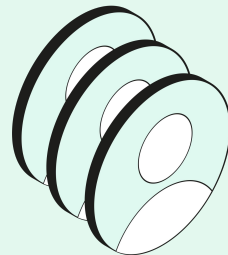
infra (ops)



Gère la production "au sens large"

(la production)

Une culture à changer



Ops : c'est MA prod

Personne ne peut faire une action dessus sans mon autorisation explicite

Ops : Les dev ont ENCORE poussé un bug en prod !

On a encore reçu des alertes !

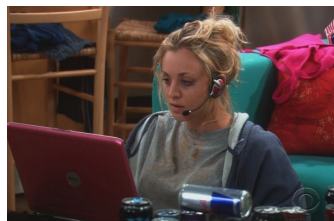
Dev : c'est merge ? Ce n'est plus mon problème

Ce qu'il se passe après ne m'intéresse pas

Dev : les ops ont ENCORE dit non pour l'ajout d'une fonctionnalité dont on a besoin !

Tant pis, on va l'installer en douce et ne pas les prévenir

Ops sur le chemin critique



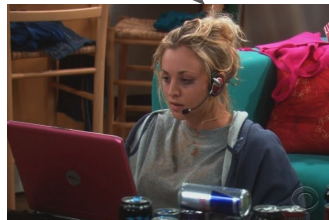
t 0

Tu peux déployer la
release v1.4.1 en prod ?



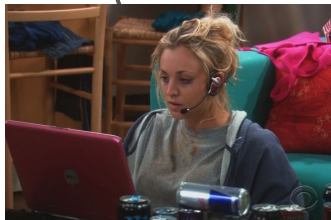
t +1 jour

C'est fait.
On a une erreur au
démarrage, voilà le log



t +3 jours

Problème trouvé, on
sort la v1.4.2



t +2 jours

On a maintenant une
latence élevée sur
certains appels



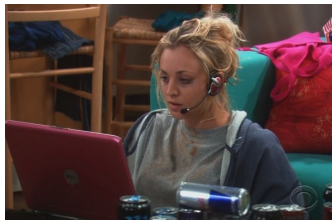
t +1.5 jour

La configuration est incorrecte,
ajoute cette variable
d'environnement

Equipe autonome

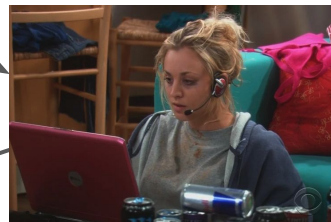
t 0

L'équipe de dev tag la release v1.4.1 qui est envoyée en prod automatiquement



t +5 minutes

Alerte: le “rolling restart” de la nouvelle version s’arrête: les nouvelles instances ne démarrent pas.



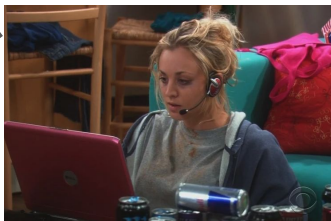
t +15 minutes

La configuration est mise à jour
Problème résolu



t +20 minutes

Alerte: latence élevée sur le service



t +40 minutes

fix déployé en production
(ou rollback)



*ndlr: il serait intéressant de détecter ces problèmes **avant** le déploiement ;)*

Pourquoi ?

Améliorer le lead time

Fréquence et fiabilité des déploiements

Boucle de feedback rapide

Mean time to recovery, rollbacks

Ownership

You built it, you run it

Responsabilité

*Les problèmes causés par mon service
sont mes problèmes*

Mais donc, plus besoin d'ops ?

- Demander aux développeurs de déployer l'infrastructure
- Demander aux développeurs d'être expert Kubernetes
- Demander aux développeurs d'être expert en base de données
- Demander aux développeurs de configurer le réseau entre applications
- ...

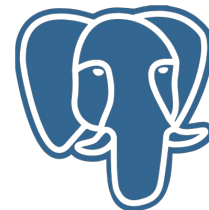
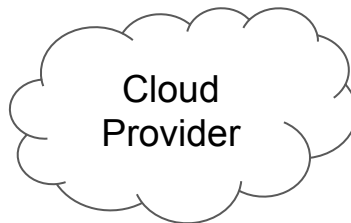
Mais donc, plus besoin d'ops ?

- Demander aux développeurs de déployer l'infrastructure
 - Demander aux développeurs d'être expert Kubernetes
 - Demander aux développeurs d'être expert en base de données
 - Demander aux développeurs de configurer le réseau entre applications
 - ...
- 

Ops



maintient



PostgreSQL

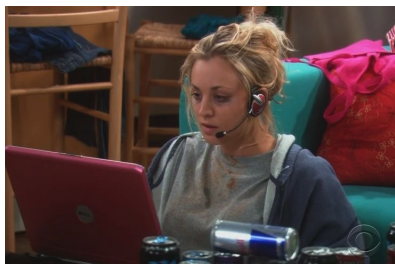
...

Fournit



Consomme

Collaborent



Dev

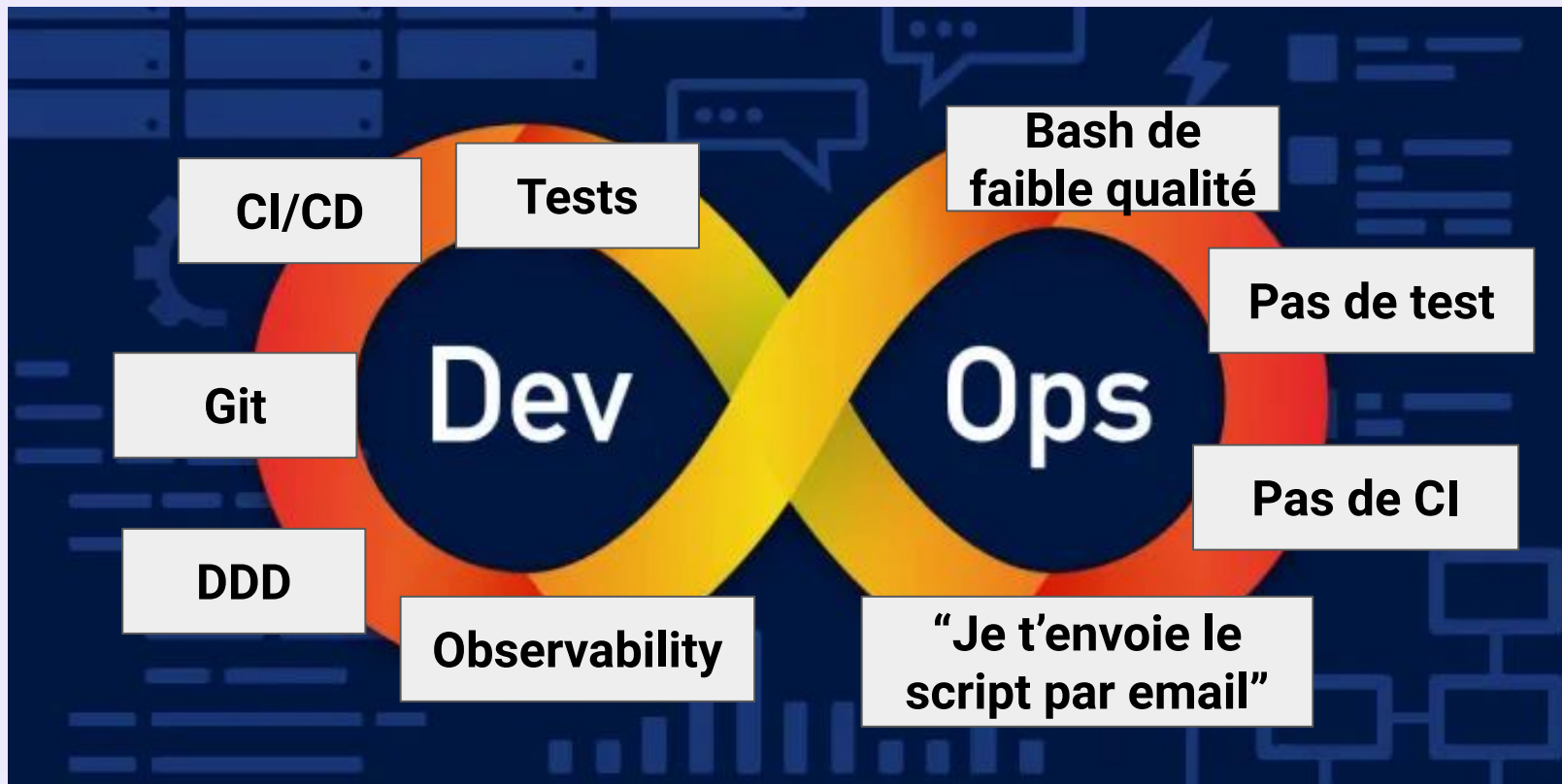
Une équipe infra orientée produit

- Développe un produit interne à destination du département tech
 - Formation interne
- Retours “du terrain” (support, incidents, feedbacks utilisateurs...)
- Contraintes (sécurité, fiabilité, objectif d'équipe et d'entreprise...)
- Lean
 - Obeya
 - Value Analysis
 - A3

Dev et Ops, même vision du développement?



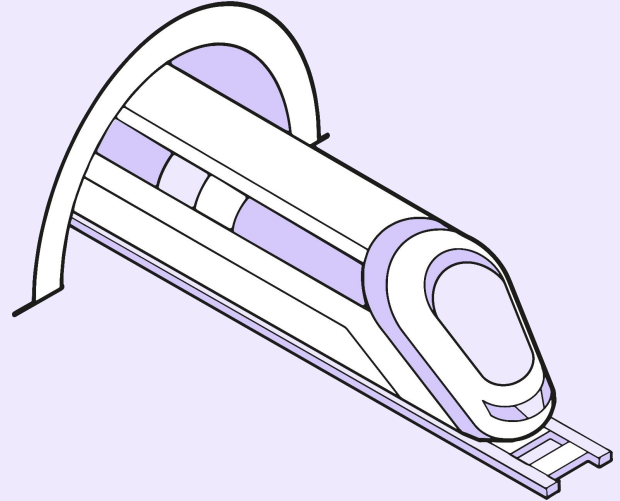
Traditionnellement...



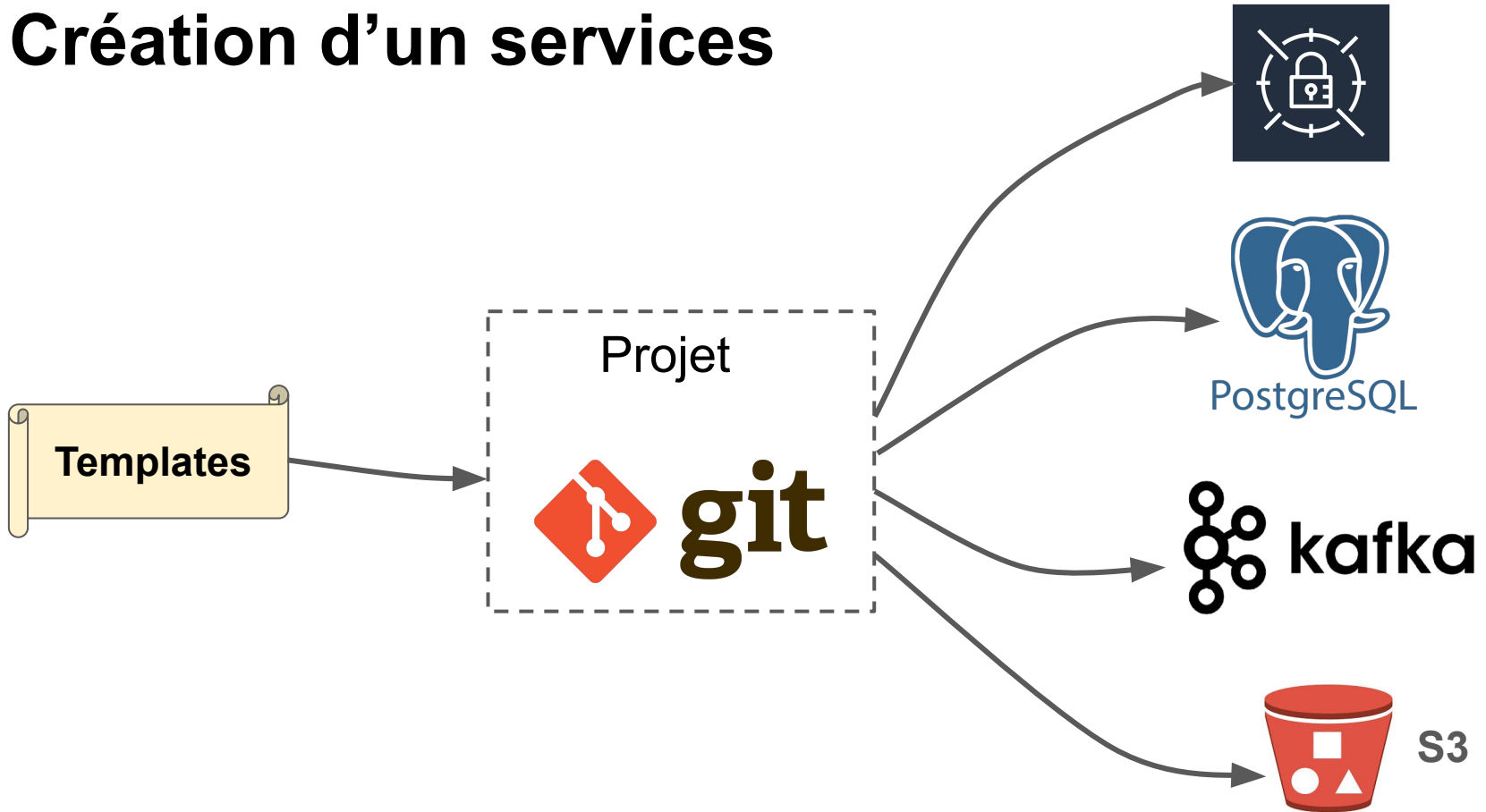
“SRE is what happens when you ask a software engineer to design an operations team”

from <https://sre.google/sre-book/introduction/>

Création d'un service



Création d'un services



→ ~ qontoctl microservice create go --help

Create and deploy a Golang application

Usage:

qontoctl microservice create go <name> [flags]

Examples:

qontoctl microservice create go <name>

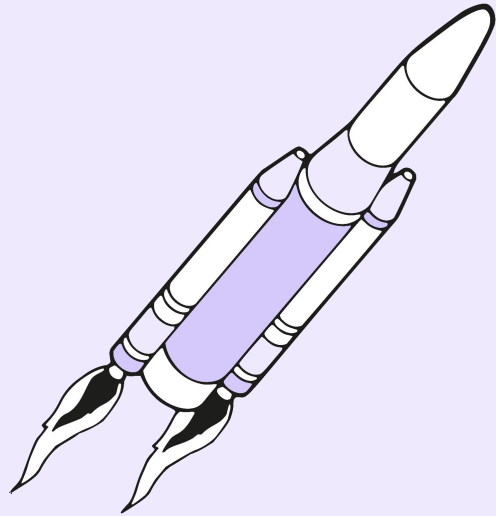
Flags:

--database	Set if the microservice needs a Postgres database
-h, --help	help for go
--internal-http-client	Set to true to add an internal http client. E.g. for calling internal services with Paseto token
--kafka-consumer	Set to true to consume messages from kafka
--kafka-producer	Set to true to produce messages to kafka
--launchdarkly	Set to true to add LaunchDarkly feature flags
--s3	Set to true to create an S3 bucket

Global Flags:

--description string	Description of the service
--gitlab-path string	Gitlab group of the project. E.g. back, cbs, ...
--team string	Name of the team owning the service
--timeout duration	Timeout for the creation of the microservice (default 15m0s)

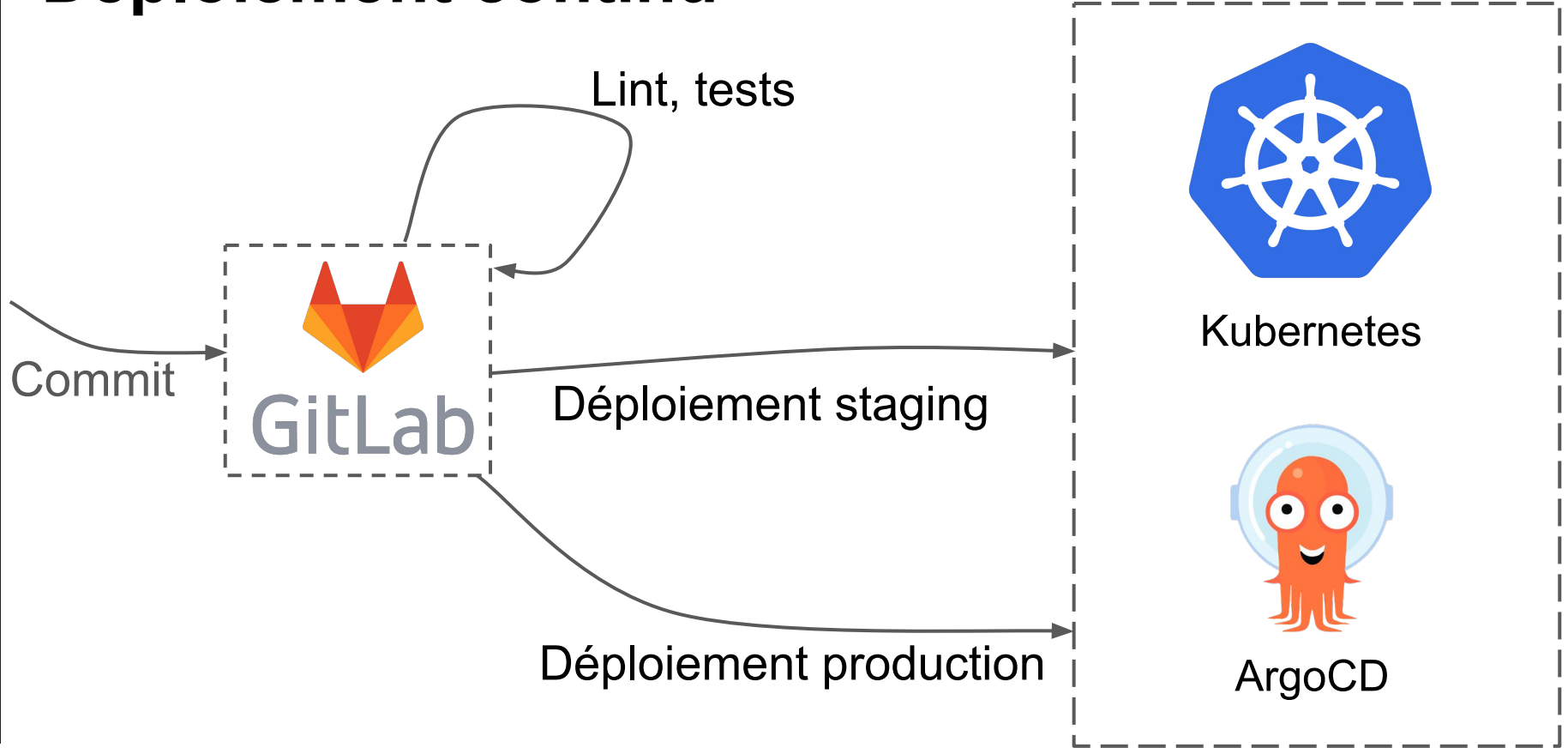
Déploiement en production



```
name: rds-management
replicas: 2
service:
  ports:
    http:
      port: 3000
container:
  args:
    - --config
    - /etc/rds-management/config.yaml
  ports:
    http:
      port: 3000
  resources:
    requests:
      cpu: 100m
      memory: 1Gi
  env:
    secret:
      PG1_PASSWORD: /pg/sre/pg1/qonto-app-rds-management_password:1
autoscaling:
  enabled: true
  min: 3
  max: 10
  memory:
    average: 70
  cpu:
    average: 80
```

- Déclaratif
- Bonnes valeurs par défaut
- Audit (CI, runtime)

Déploiement continu



avatars

 Restart

 Retry

 Abort

 Promote

 PromoteFull

Steps

 Set Weight: 25%

 Pause: 10m

 Set Weight: 50%

 Pause: 15m

 Set Weight: 75%

 Pause: 5m

Summary

Strategy

 Canary

Step

 6/6

Set Weight

 100

Actual Weight

 100

Containers

 Edit

avatars

.dkr.ecr.eu-west-3.amazonaws.com/b:



Init Containers

1-migrate

.ecr.eu-west-3.amazonaws.com/b:



Revisions

Revision 22

.ecr.eu-west-3.amazonaws.com/back/avatars:b0751efc118de76a82c5c46b3ea80d9b6eb888d3

.ecr.eu-west-3.amazonaws.com/back/avatars:b0751efc118de76a82c5c46b3ea80d9b6eb888d3

avatars-686c6687b8

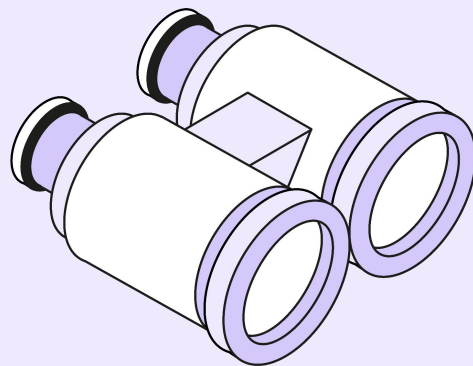


Analysis Runs

 Analysis 686c6687b8-22

Logs, métriques, traces

une “commodité”



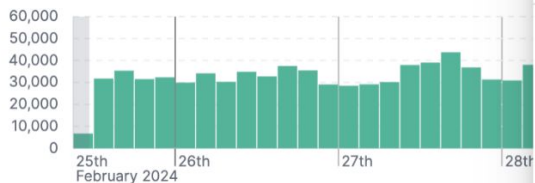
Filter your data using KQL syntax

0

2

266

2,544,586 hits



Feb 25, 2024

Documents Field statistics

1 field sorted

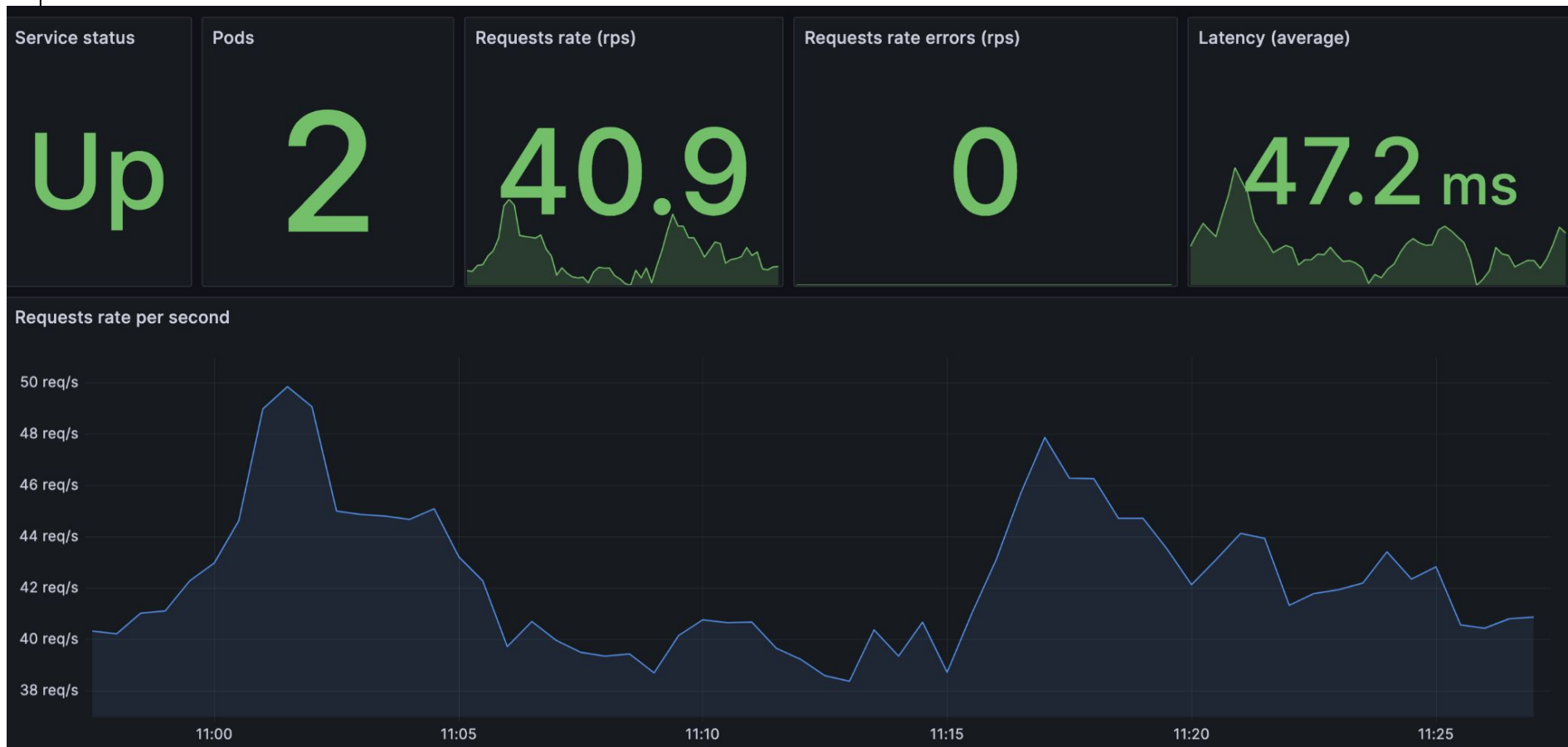
	↓ @timestamp ⌚	Document
⌕	Mar 5, 2024 @ 11:23:12.730	@timestamp Mar agent.hostname t-xvhw9 agent.ty
↶	Mar 5, 2024 @ 11:23:12.126	@timestamp Mar agent.hostname t-xvhw9 agent.ty
↶	Mar 5, 2024 @ 11:23:11.313	@timestamp Mar agent.hostname t-xvhw9 agent.ty
↶	Mar 5, 2024 @ 11:23:10.842	@timestamp Mar agent.hostname t-xvhw9 agent.ty

Expanded document

View: [Single document](#) [Surrounding documents](#) ?

1 of 500

k	kubernetes.pod.name	argocd-notifications-controller-7b9ff565ff-2qzvn
k	kubernetes.pod.uid	60c95891-9154-4ba4-991c-9d8ab00a69aa
k	kubernetes.replicaset.name	argocd-notifications-controller-7b9ff565ff
k	log.file.path	/var/log/containers/argocd-notifications-controller-7b9ff565ff-2qzvn_argocd_notifications-controller-6244a24b3ada1bdc4860567e6425e4737cad199d11dcafc8af9c803b1f8a49dc.log
#	log.offset	4,275,631
⌚	logstash.processed_date_time	2024-03-05T10:23:20.914908Z
⌚	logstash.processed_delay_seconds	8
f	logstash.log.message	time="2024-03-05T10:23:12Z" level=info msg="Start processing" resource=argocd/keda
k	logstash.name	logstash-2
f	message	time="2024-03-05T10:23:12Z" level=info msg="Start processing" resource=argocd/keda



> Node graph

Trace

Internal Gateway (production): http-server 1.41s

Give feedback

Trace ID

Export

2024-03-05 10:39:26.025

GET

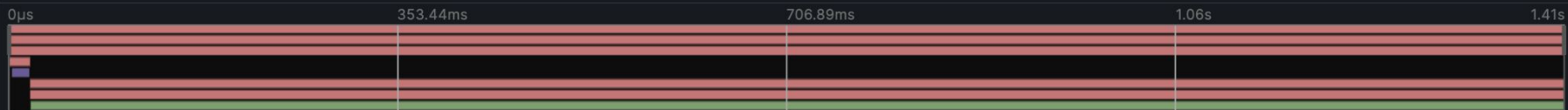
200

> Span Filters ⓘ

8 spans ⓘ

Prev

Next



Service & Operation

▼ > ⌵ >> ||

0µs 353.44ms 706.89ms 1.06s 1.41s

▼ Internal Gateway (production) http-server (1.41s)

▼ middleware:logger (1.41s)

▼ middleware:internal-auth (1.41s)

▼ HTTP POST (20.11ms)

20.11ms

internal-auth /v1/session/aws/presigned-url (15.81ms)

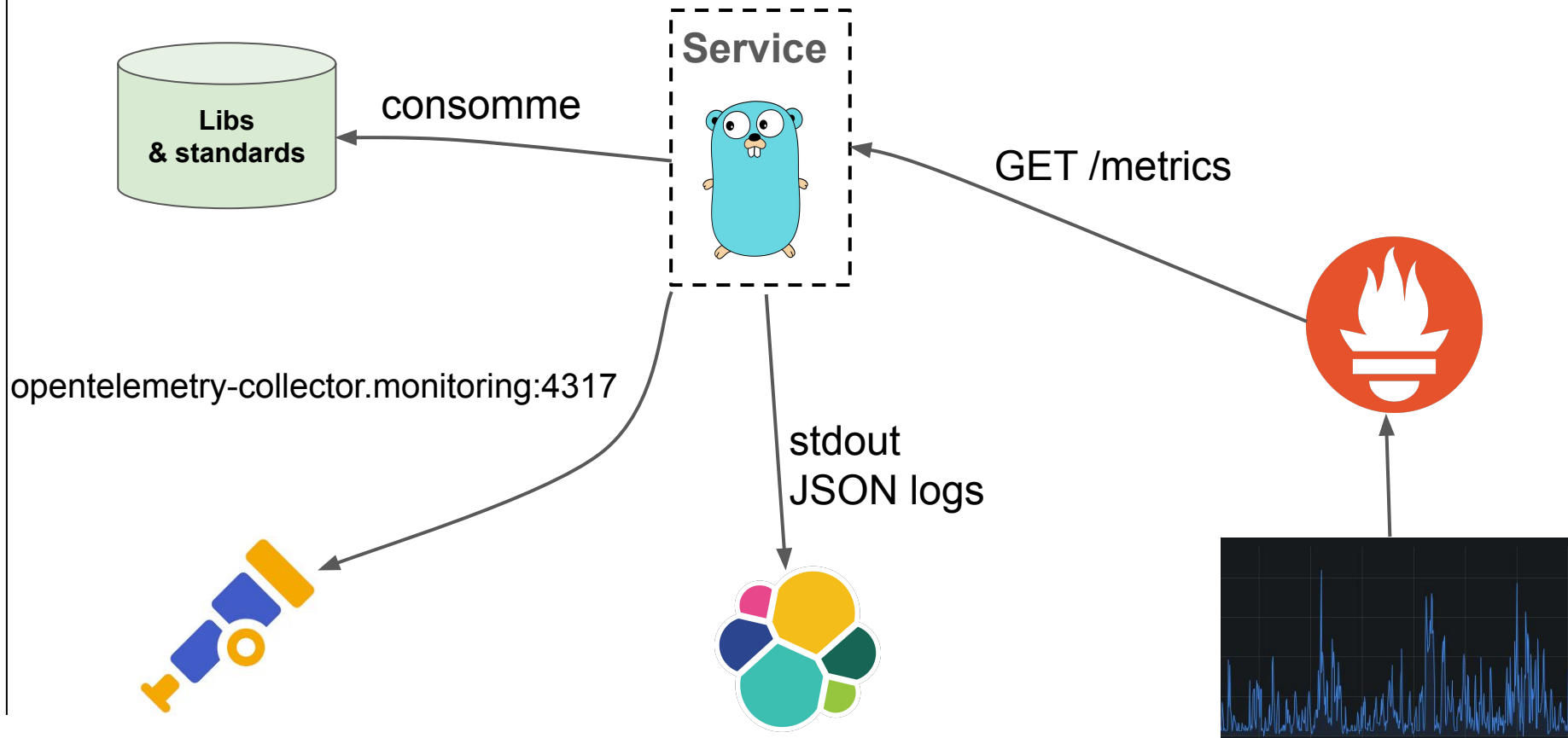
15.81ms

▼ Internal Gateway (production) handler:forward-kafka-manage

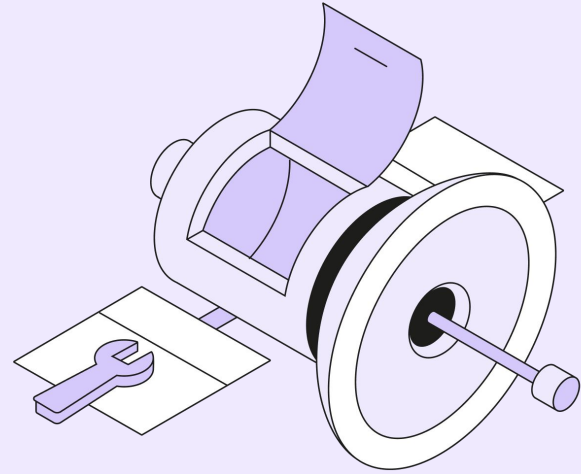
▼ HTTP GET (1.39s)

kafka-management /api/v1/clusters/:clusterName/cons





Tooling interne



Ça marche pas!

```
→ ~ qontoctl aws login --reset
```

```
First configuration or config reset. Files that will be modified:
```

```
- ~/.aws/config
```

```
Onelogin username (ex: firstname.lastname): mathieu.corbin
```

```
Search: █
```

```
? Team:
```

```
↑ it-automation
```

```
compliance
```

```
▶ sre
```

```
frontend
```

```
data-engineering
```



Authorization requested

An application or service has requested access to your AWS account(s) and resources.



Confirm this code matches the one given to you.



If you did not initiate this request or your codes do not match, cancel this request.

Confirm and continue

Cancel

Ça marche pas!

```
➔ ~ qontoctl troubleshoot
```

```
Start analyzing your system to find potential known issues:
```

```
💡 Your team is 'sre'. If you need to reconfigure your team, run: `qontoctl aws login --reset`
```

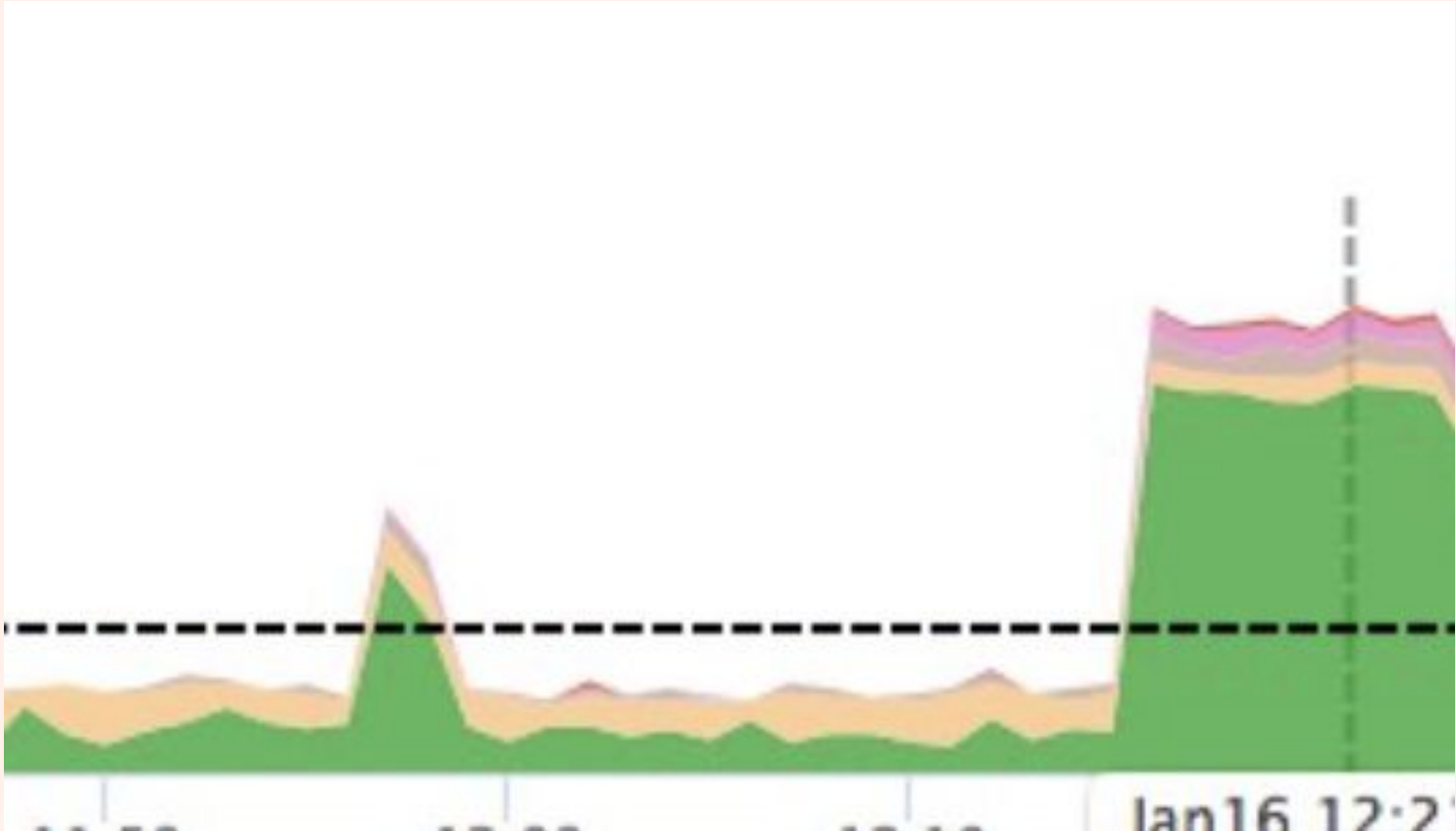
- ✓ Shell environment, no issue found
- ✓ Qonto VPN is enabled
- ✓ Qontoctl latest version.
- ✓ AWS Local Configuration
- ✓ Kubectl Local Configuration, no issue found
- ✓ kubectl version (1.30.1)
- ✓ aws version (2.17.19)
- ✓ Helm + s3 plugin
- ✓ docker-credential-helper-ecr version (0.8.0)
- ✓ Docker Local Configuration, no issue found

Comment je me connecte?

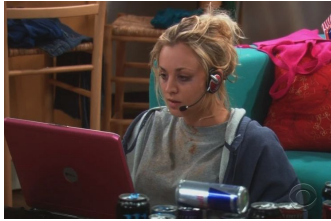
```
→ ~ qontoctl aws ssh pack
Searching for instance pack
Search: █
? EC2 Instances matching pack:
  > package-registry 10.█.
Instance ID: i-█
```

```
→ ~ qontoctl rds connect
Search: █
RDS instances?
  > pg1
    pg1-replica1
```

Une requête bloque la base, help!



“live debugging” SQL: avant



C'est lent



- psql <base>
- select **pg_stat_activity**
- une requête bloque la base



Je peux stop la requête \$PID ?

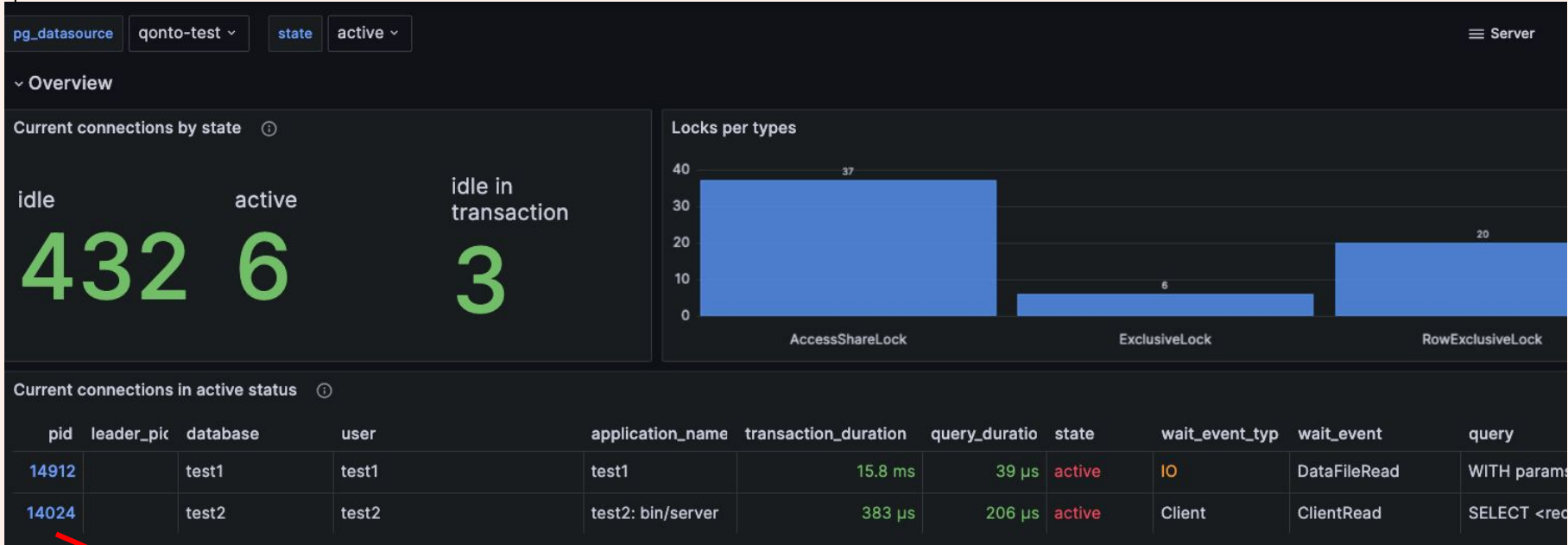


Vas y



stop \$PID

Maintenant



```
→ ~ qontoctl rds cancel-query \  
--context test \  
--identifier qonto-test \  
--pid 14024
```

Gestion de Kafka

Hello @sreduty,

Could you please delete the following Kafka consumer groups: and ?

[Here](#) is a similar request.

Thank you!

Hello 🙌

Could you please delete two consumer groups:

<https://>

<https://>

Thanks 🙏

Hello team,

could you please delete the [card-](#) topic from staging and prod?

The application still doesn't have any traffic in prod, so it's safe to delete it.

Actions de suppression en self service

```
→ ~ qontocctl kafka topics delete \  
--cluster default \  
--topic master.monthly_invoices \  
--approval-description "deleting topic 'monthly_invoices' in staging"
```



Approval System APP 6:30 PM

Description:

deleting topic 'monthly_invoices' in staging

Command for **kafka-management**:

Delete 'master.monthly_invoices' topics on 'default' Kafka cluster

Requested by @mathieu

Approved by @someone

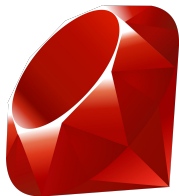
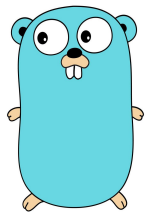
Et beaucoup d'autres fonctionnalités...

- Créer des read replicas RDS ou des instances EC2 à la demande
- Gérer les secrets de ses applications
- Déclarer son astreinte
- Accéder aux endpoints **/debug/pprof** des services Golang
- ...

Alertes et astreintes

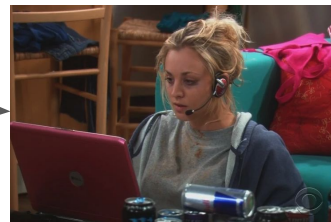


Services



Alertes

Dev



Infrastructure



Alertes

Escalation

Manager

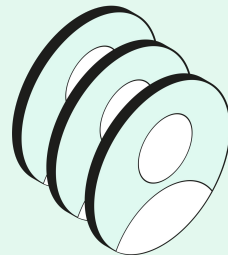


SRE

Recevoir des alertes est souvent intimidant

- *Je ne saurai pas répondre à l'incident*
 - Il est impossible de tout connaître
 - Runbooks, formations, shadowing, escalation
- *Je ne suis pas un ops*
 - Ce n'est pas ce qui est demandé
 - Responsabilisation des équipes
- *Je n'ai pas les bon outils pour gérer les incidents*
 - **Souvent un problème**

Culture de la gestion d'incidents



Blameless

On est une équipe, dev comme ops

Procédures claires

Moyens de communication, escalation, incident commander, documentation

Postmortems (PDCA)

Apprendre de nos problèmes et faire en sorte qu'ils ne reviennent plus

Alert fatigue

Les alertes doivent être actionnables, avec des runbooks et de l'outillage

L'expertise as a service



"Back Office" interne



Sécurité



Data



Votre équipe ?

Merci



Qonto