



Père Castor 🐻, raconte nous une histoire (d'OPS)

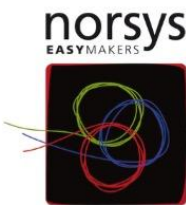
David Aparicio | 4 Février 2022 | 16h00 | Auditorium

David Aparicio | +33 (0)6 50 55 70 00 | www.dadideo.com



Merci à nos sponsors

« Etoile »



« Flocon »





@dadideo

David Aparicio

15/ DD INSA de Lyon / UNICAMP (Brésil)

Facebook Open Academy / MIT AppInventor

17/ Dev(Sec)Ops @ AMADEUS (Nice, 2 ans)

19/ Data(Sec)Ops @ OVHcloud (Lyon, 3 ans)





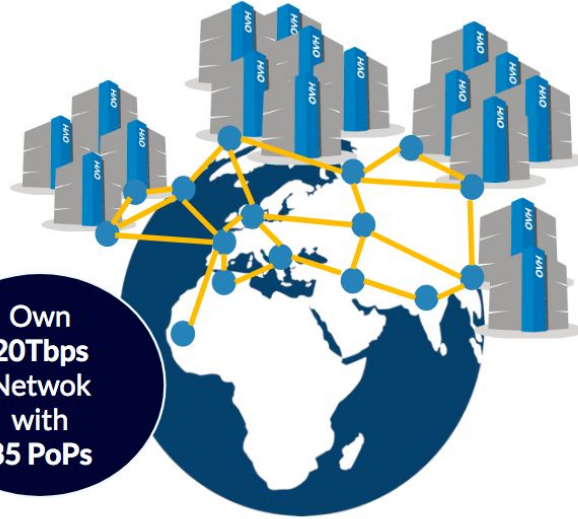
OVHcloud: un leader européen

200k Private cloud
VMs running



Dedicated
IaaS
Europe

...
...
...
...
...
...
...
...
...
...



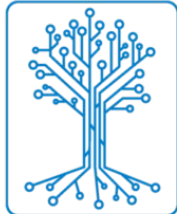
Own
20Tbps
Network
with
35 PoPs

30 Datacenters

Hosting capacity :
1.3M Physical
Servers

360k
Servers already
deployed

> 1.3M Customers in 138 Countries



GAIA-X



Depuis Déc. 2020



OVHcloud: 4 univers de produits

Domain / Email ▾

Domain names, DNS, SSL, Redirect

Email, Open-Xchange, Exchange

Collaborative Tools, NextCloud

PaaS for Web ▾

Mutu, CloudWeb

Plesk, CPANEL

PaaS with Platform.sh

Virtual servers ▾

VPS, Dedicated Server

SaaS ▾

Wordpress, Magento, Prestashop

CRM, Billing, Payment, Stats

MarketPlace

Support, Managed ▾

Support Basic

Support thought Partners

Managed services

Standalone, Cluster ▾

General Purpose SuperPlan

Game T2 >20e

Virtualization T3 >80e

Storage T4 >300e

Database T5 >600e

Bigdata 12KVA /32KVA

HCI

AI

VDI Cloud Game

Network

VPS aaS ▾

pCC DC

Virtuozzo Cloud

Wholesales ▾

IT Integrators, Cloud Storage,

CDN, Database, ISV, WebHosting

High Intensive CPU/GPU,

Encrypt ▾

KMS, HSM

Encrypt (SGX, Network, Storage)

Compute ▾

VM K8S, IA IaaS

Baremetal PaaS for DevOps

Storage ▾

File, Block, Object, Archive

Databases ▾

SQL, noSQL, Messaging,

Dashboard

Network ▾

IP FO, NAT, LB, VPN, Router,

DNS, DHCP, TCP/SSL Offload

Security ▾

IAM, MFA, Encrypt, KMS

IA, DL ▾

Standard Tools for AI, AI Studio,

IA IaaS, Hosting API AI

Bigdata, ML, Analytics

DataLake, ML, Dashboard

Hosted Private Cloud ▾

VMware

SDDC, vSAN 1AZ / 2AZ

vCD, Tanzu, Horizon, DBaaS, DRaaS

Nutanix

HCI 1AZ / 2AZ, Databases, DRaaS, VDI

OpenStack

IAM, Compute (VM, K8S)

Storage, Network, Databases

Storage

Ontap Select, Nutanix File

OpenIO, MinIO, CEPH

Zerto, Veeam, Atempo

AI

ElementAI, HuggingFace,

Deepomatic, Systran,

EarthCube

Bigdata / Analytics / ML

Cloudera over S3, Dataiku,

Saagie, Tableau,

Hybrid Cloud ▾

vRack Connect, Edge-DC, Private DC

Dell, HP, Cisco, OCP, MultiCloud

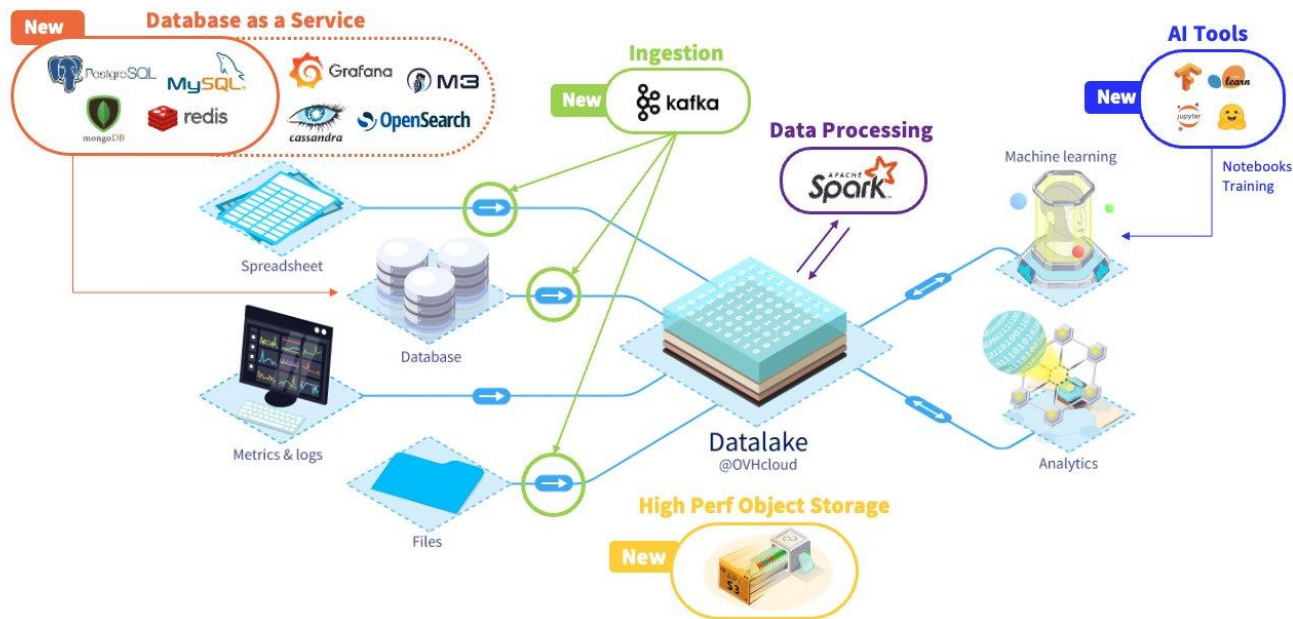
Secured Cloud ▾

GOV, FinTech, Retail, HealthCare



Data @ OVHcloud

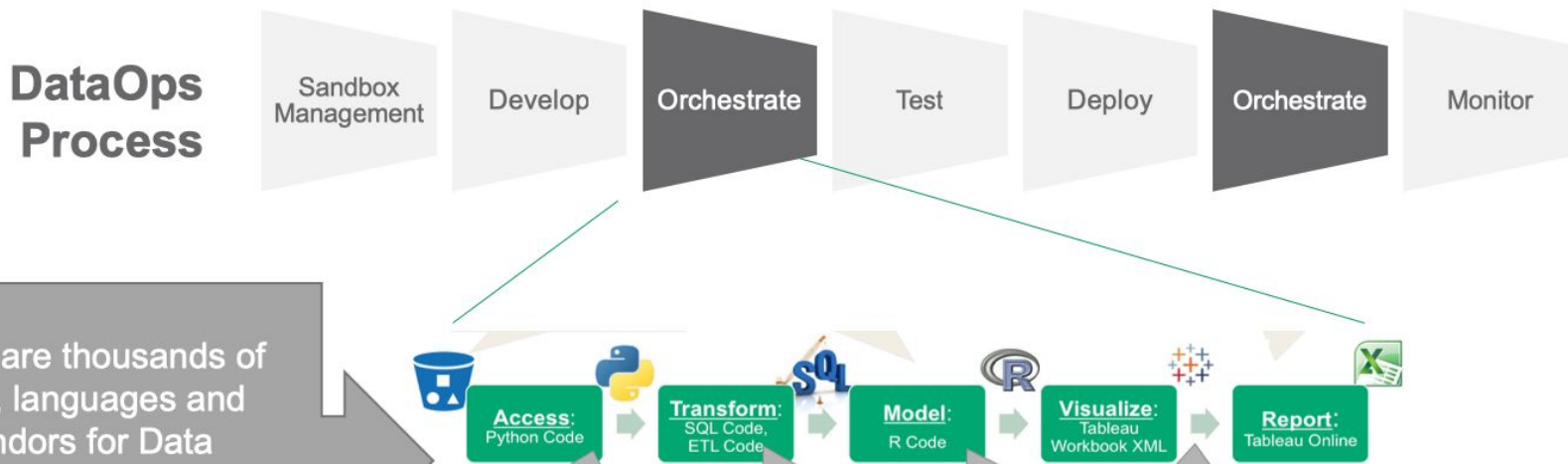
2021 : Improving our Public Cloud ecosystem for data projects





DataOps @ GIS-DATA

- Réplication des données
- Opérations Scaling (up/down), Maintenance (compactions, cleaning DB)
- PoC / Benchmarks / Performance tuning
- Industrialisation / Automatisation des procédures
- Mise en place de plate-forme de machine learning
- Urbanisation du Datalake
- Réalisation des Audits / Security assessment
- Migration des solutions
- Onboarding des projets
- RUN/BAU





Qui êtes-vous ?

Plutôt Dev, Ops, Étudiant, Autre (Designer, PM, Coach Agile) ?



Qui a déjà possédé un téléphone d'astreinte ?



Agenda

Introduction

Elliot

Legacy

CDN

Retour du Legacy

Blast effect

Same JVM, shoot again

NewsBlur

Foxstuck

DNS

(Split-Brain)

Conclusion

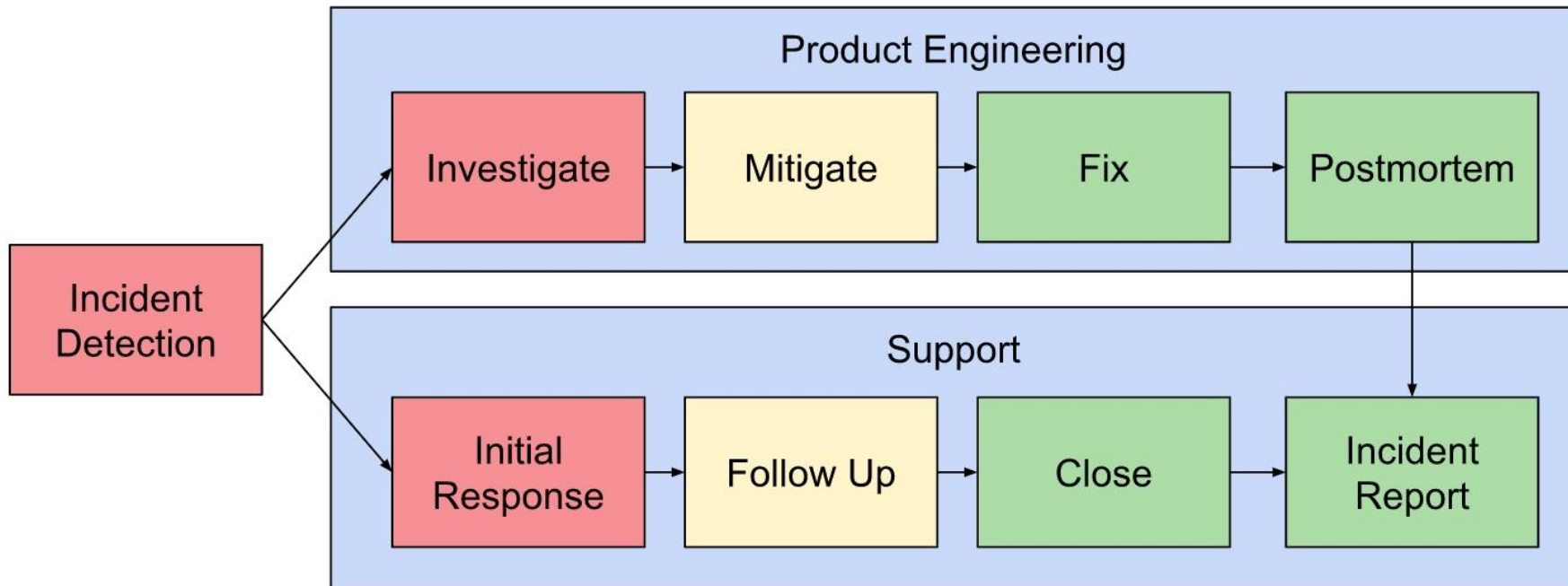


Introduction



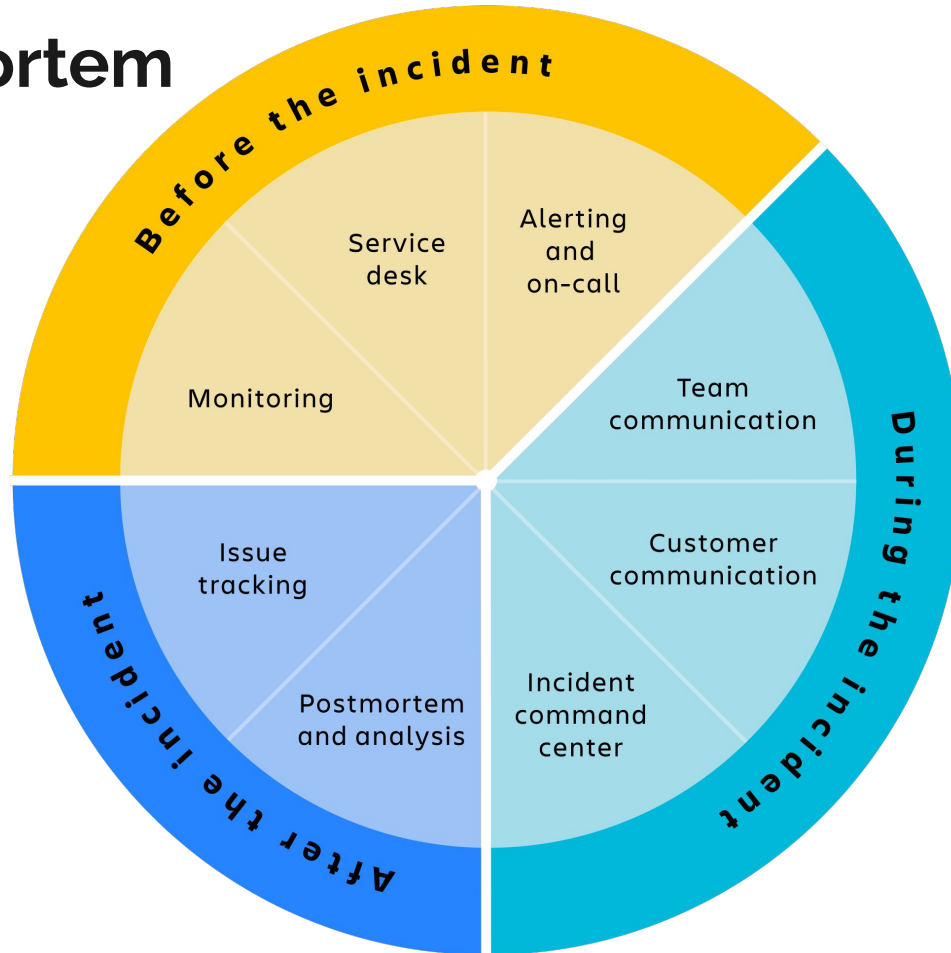


Post-mortem





Post-mortem





Examen post-incident

Identification de l'incident (détection, sonde)
Flux d'informations et communication (canaux)
Structure (organisation)

Utilisation des ressources (vitesse, optimum)
Processus (SLA)
Création de rapports (interne et externe)

 [Le guide complet de gestion des incidents ITIL](#)





Regroupés en chapitres

Background

Incident timeline / What Happened

Root cause

Workaround / Mitigation

Impact / Customers

Next steps / Action item

(Engineering & Architecture,

Process & Communications)



Exemples: [GitHub](#) / [Elastic](#)





Exemples récents

status.docker.com

 docker system status

Docker system status real-time view

SUBSCRIBE

Active Incident

Updated a few seconds ago

Intermittent problems accessing Repositories API

Partial Service Disruption

Incident Status	Partial Service Disruption
Components	Docker Package Repositories
Locations	AWS

January 31, 2022 6:22AM PST
January 31, 2022 2:22PM UTC

[Investigating] The repositories API is experiencing intermittent failures. Our team is investigating. Serving of images (pulls) is functioning normally.

status.gitlab.com



SUBSCRIBE

Active Incident

Updated a few seconds ago

We continuously monitor GitLab.com and all its services. If there are any performance or service interruptions, an update will be posted here.

System Wide Outage

Service Disruption

Incident Status	Service Disruption
Components	Website, API, Git Operations, Container Registry, GitLab Pages, CI/CD - GitLab SaaS Shared Runners, CI/CD - GitLab SaaS Private Runners, CI/CD - Windows Shared Runners (Beta), SAML SSO - GitLab SaaS, Background Processing, GitLab Customers Portal, Support Services, packages.gitlab.com, version.gitlab.com, forum.gitlab.com, Canary, dashboards.gitlab.com
Locations	Google Compute Engine, Azure, Digital Ocean, Zendesk, AWS

January 31, 2022 16:22 CET
January 31, 2022 15:22 UTC

[Investigating] GitLab.com is unavailable and users are getting 500 errors.



Incidents du Lundi 31 Janvier 2022 : [Status de Docker](#) / [Status de GitLab](#)



#SnowCamp #SC2022

@dadideo



17



First blood





Quand date le premier bug de Grace Hooper ?



Un vrai bug (insecte)

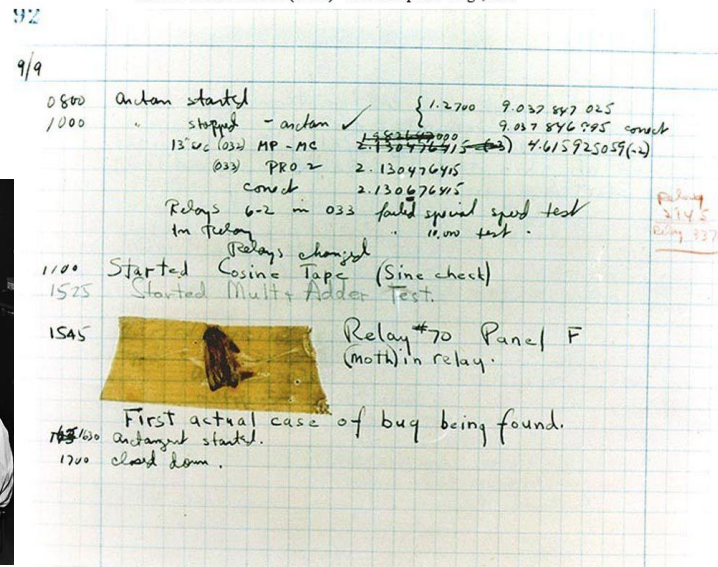
Bureaux de EMCC

1947

Inventeur du COBOL



Photo # NH 96566-KN (Color) First Computer "Bug", 1947



9/2

9/9

0800 Antan started
 1000 " stopped - antan ✓
 13:00 (032) MP - MC ~~1.3047645~~ 4.615925059(-2)
 (033) PRO 2 2.13047645
 correct 2.13067645
 Relays 6-2 in 033 failed special speed test
 in Relay " 11.00 test.

1100 Started Cosine Tape (Sine check)
 1525 Started Multi Adder Test.

1545 Relay #70 Panel F
 (moth) in relay.

1700 First actual case of bug being found.
 Antan started.
 closed down.

Relay #70
 2145
 2145
 2145



Cette anecdote n'est pas "isolée"

22 Juin

2021

Inondation de la fibre optique
d'un datacenter

Past Incidents

Tuesday 22nd June 2021



Infrastructure PAR: connectivity issue / high latency

[3 months ago](#)

2021-06-22

We are currently having connectivity issue or high latency to some part of our Paris infrastructure. Our network provider is aware of the issue and is currently investigating.

10:03 UTC: It seems like the issue is only affecting one of the datacenter. Applications that use services deployed on another datacenter might suffer from connectivity issue or increased latency

10:15 UTC: We are removing the IPs of the affected datacenter from all DNS records of load balancers (public, internal and Clever Cloud Premium customers) and are awaiting more info from our network provider.



#SnowCamp #SC2022

@dadideo



21



Elliot





Elliot Alderson





Allsafe, great place to work 2021



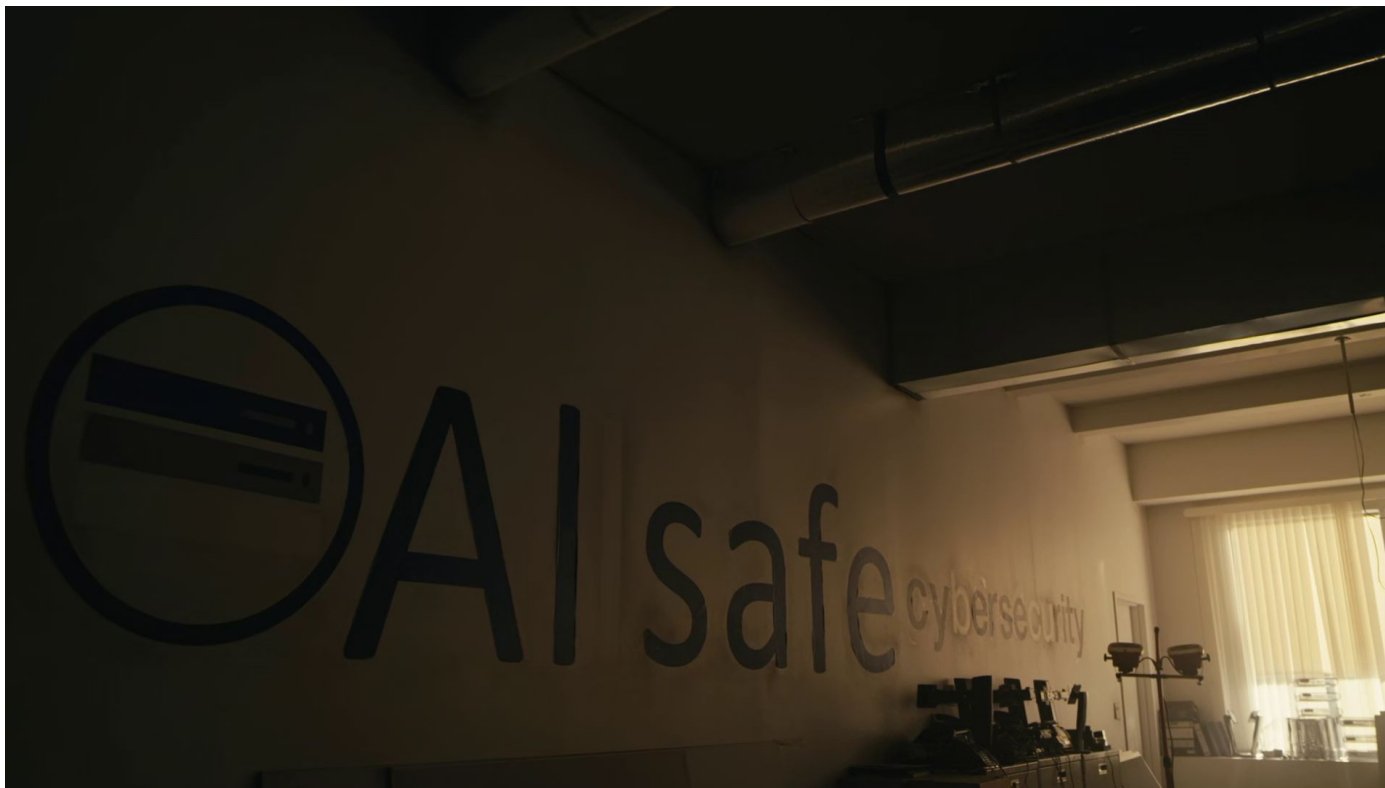


P1 detected, tout le monde sur le pont





Time is money





Beware Prod behind

"With great power comes great responsibility"





AWS, GitLab, DigitalOcean

AWS / Drop database https://aws.amazon.com/message/680587/	24/12/2012
Gitlab / Drop database https://about.gitlab.com/blog/2017/02/10/postmortem-of-database-outage-of-january-31/	31/01/2017
DigitalOcean / Drop database https://www.digitalocean.com/blog/update-on-the-april-5th-2017-outage/	05/04/2017



Conseils

Insérer une approbation manuelle / revue

Auditer et protéger l'environnement (SIEM, RBAC)

Informations d'identification/connexion protégé en lieu sûr (Vault, KeePass)

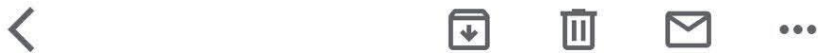
Tester vos procédures de restauration (backup)



Cas non isolé: le stagiaire

5:30 ↗

📶 5G 🔋



Integration Test Email #1 Inbox



HBO Max 5:24 PM

to me ▾



This template is used by integration tests only.



[Today](#) - HBO Max explains cryptic email that accidentally went to subscribers (18 June 2021)



Mailing / Publipostage



Dear Customer,

Your following OVHcloud customer account(s) are inactive for more than twenty-four (24) months in our information system.

List of inactive customer account(s):

If you do not take any action within 30 days of receiving this email, we will close your account(s) in accordance with OVHcloud's personal data usage policy.

If you no longer wish to use the account(s) in question, and you no longer need the information associated to them (history, invoices, etc.), you do not need to do anything. The account(s) will be closed automatically.

If you wish to keep one or more of these accounts and continue to access and use them, please log in to the relevant account(s) again via your OVHcloud



Dear Customer,

Earlier today, we have sent you an email by mistake.

Indeed, as part of our ongoing activities to maintain our compliance with GDPR, we are constantly conducting campaigns towards our inactive customers.

Due to a settings issue, you have received this communication. Please disregard it.

We sincerely apologize for the inconvenience.

Kind regards,

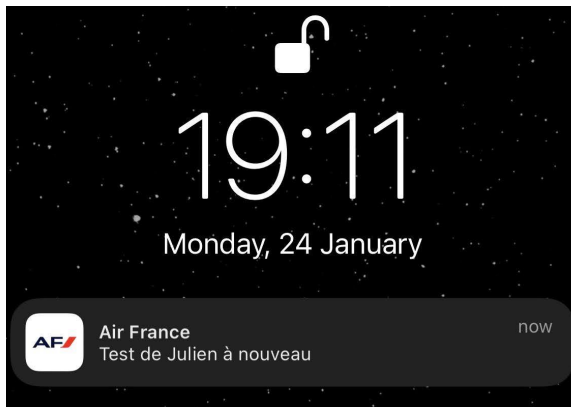
OVHcloud team



OVHcloud - Answer (11 October 2021)



Les tests en PROD



← Notifications

lundi 24 janvier, 20:27

"C'est bon Julien, ça fonctionne ! 👍"
Il s'agissait bien sûr d'un test de nos équipes techniques :)

"OK Julien, it works! 👍"
It was of course a technical test :)



#SnowCamp #SC2022

@dadideo



32



Legacy





Il était une fois.. (en 2020)





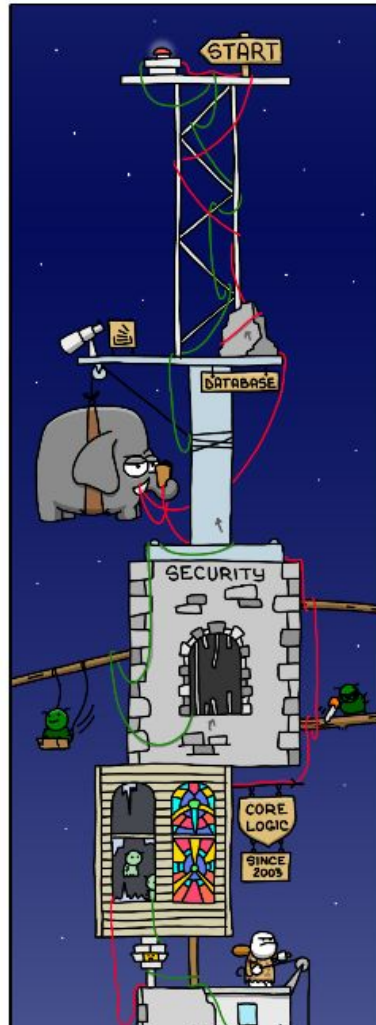
Quand soudain l'astreinte sonne





Legacy

LEGACY PROJECT SETUP



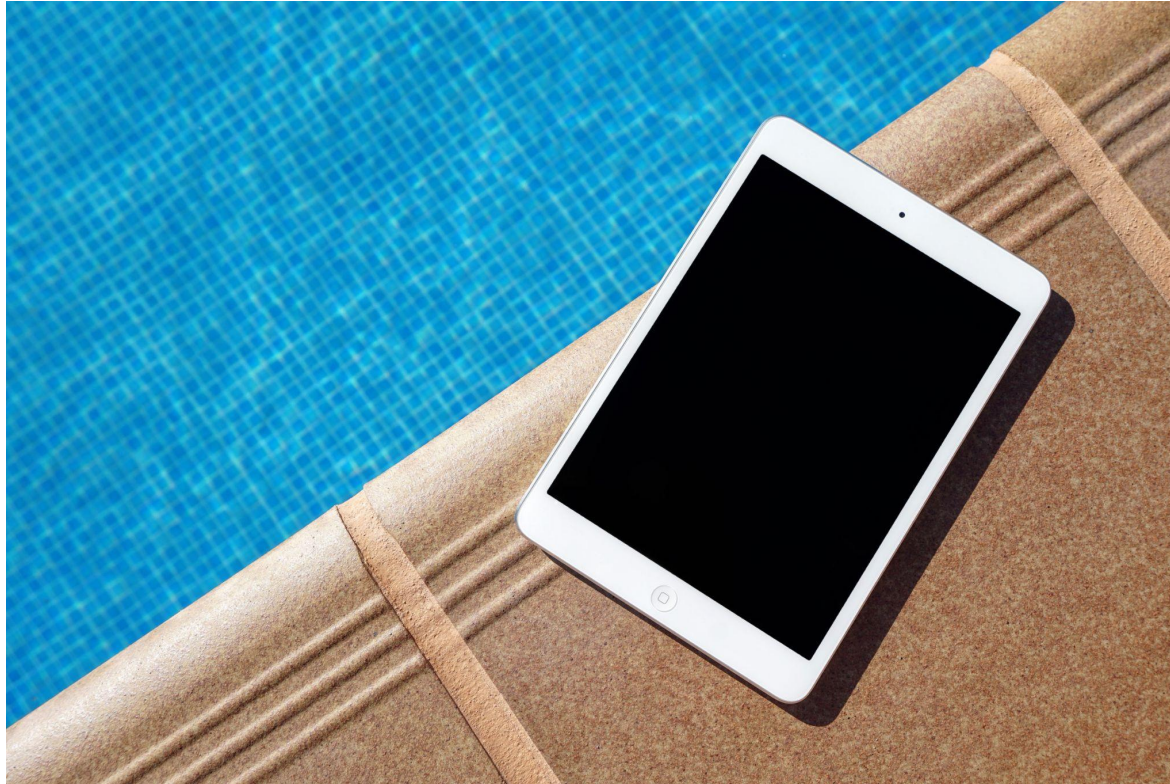


Legacy..



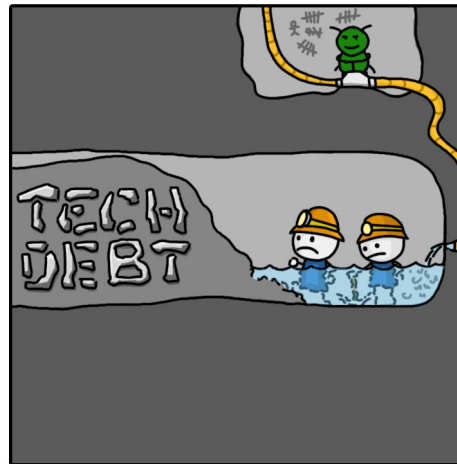
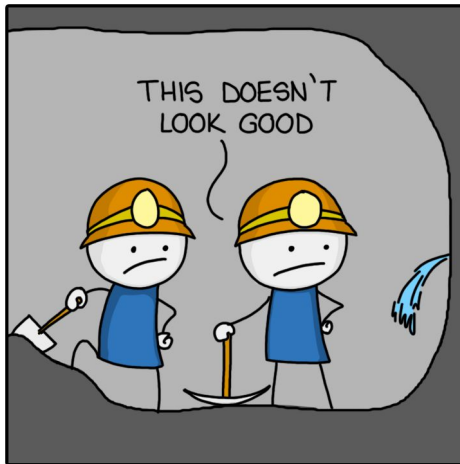
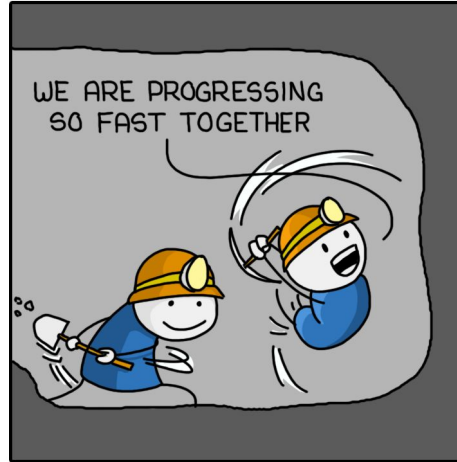
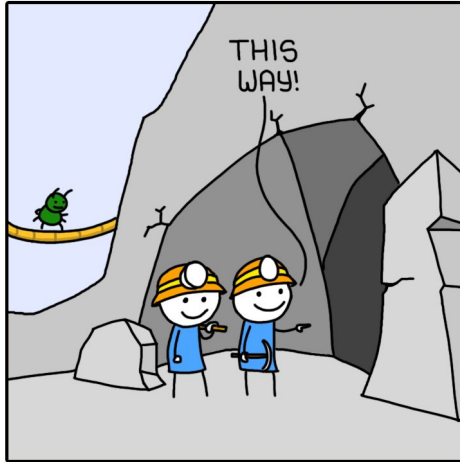


L'astreinte sonne à nouveau





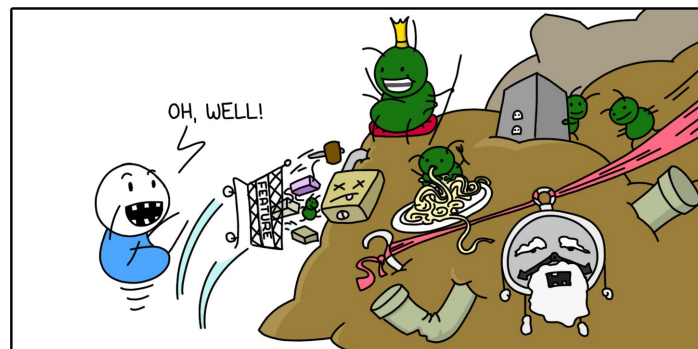
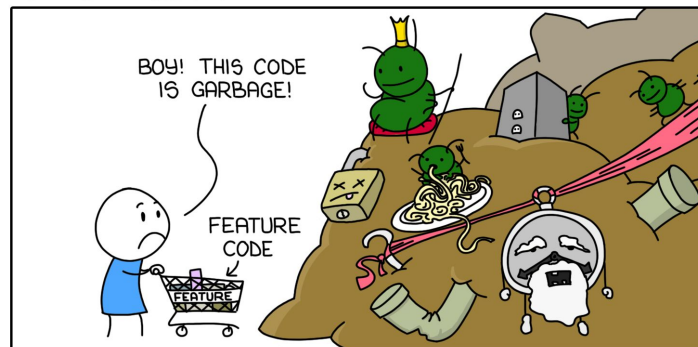
TECH DEBT





Codons! Le bon et le mauvais patch (dev)

CODE ENTROPY





Méthode KISS



**KEEP
CALM
AND
KISS**

Original:

*Keep
It
Simple
Stupid*

Variante :

*Keep
It
Super
Simple*

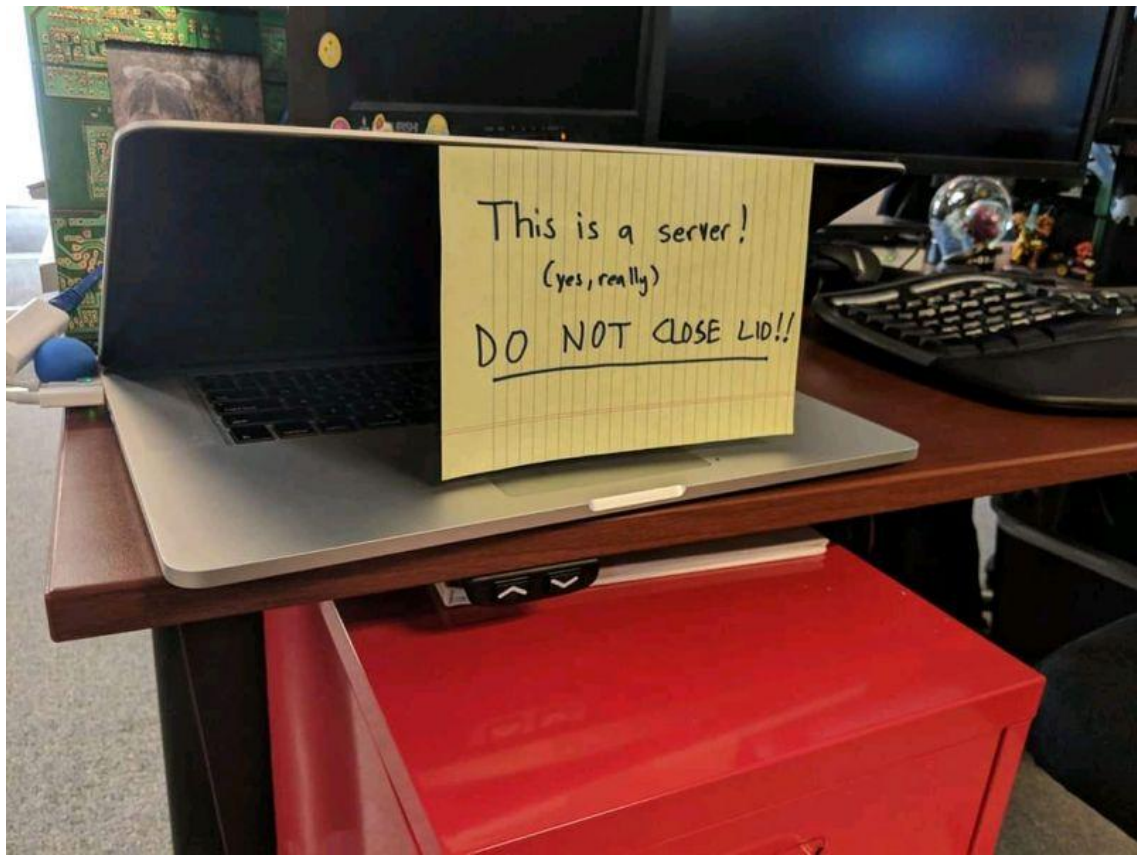


Legacy





Attention: Serveur





#SnowCamp #SC2022

@dadideo



43



CDN





#SnowCamp #SC2022

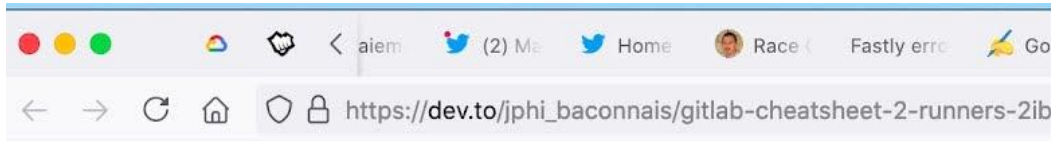
@dadideo



44



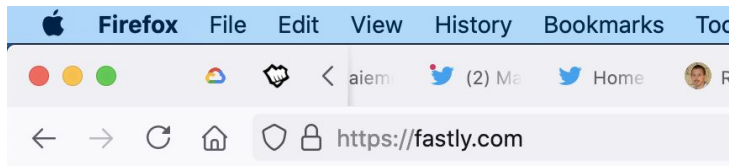
Marmiton



Details: cache-ams21071-AMS



Fastly



Error 503 Service Unavailable

Service Unavailable

Guru Mediation:

Details: cache-ams21041-AMS 1623148153 16274930

Varnish cache server

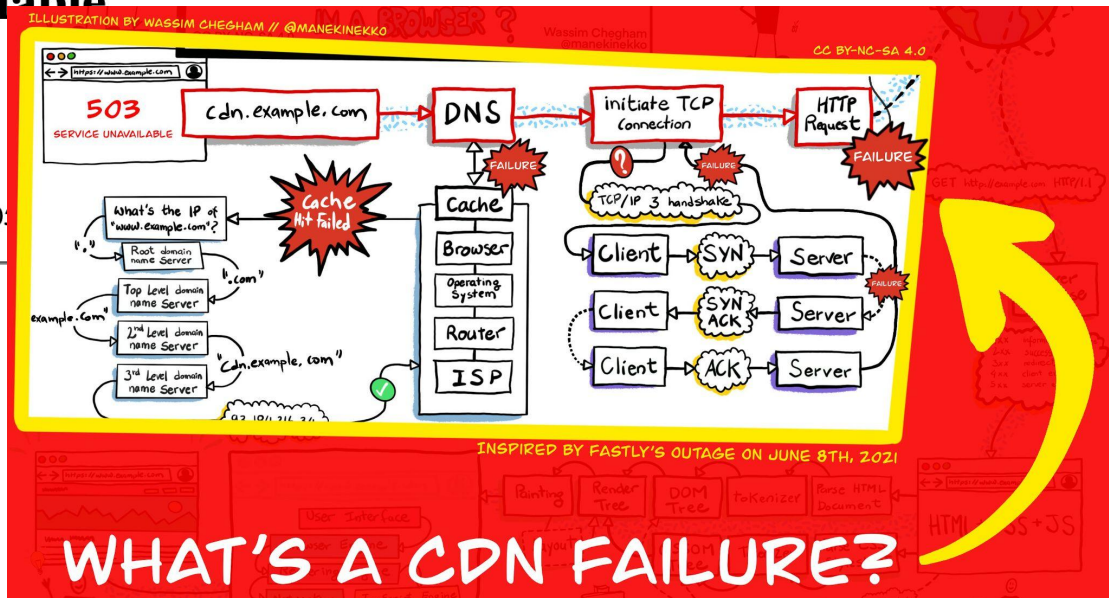
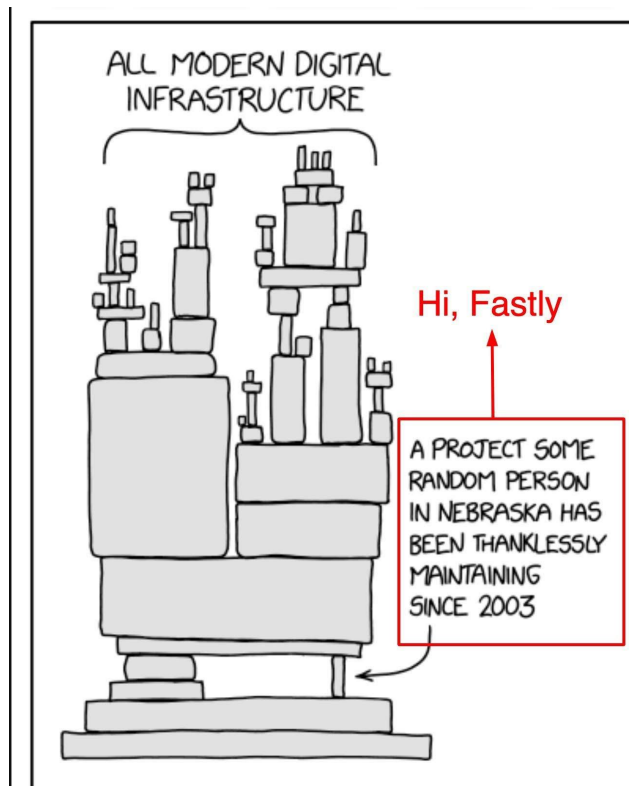


Schéma de [@manekinekk0](#)



Resilience





Details

Summary of June 8 outage

We experienced a global outage due to an undiscovered software bug that surfaced on June 8 when it was triggered by a valid customer configuration change. We detected the disruption within one minute, then identified and isolated the cause, and disabled the configuration. Within 49 minutes, 95% of our network was operating as normal.

This outage was broad and severe, and we're truly sorry for the impact to our customers and everyone who relies on them.

What happened?

On May 12, we began a software deployment that introduced a bug that could be triggered by a specific customer configuration under specific circumstances.

Early June 8, a customer pushed a valid configuration change that included the specific circumstances that triggered the bug, which caused 85% of our network to return errors.



Conseils

Personnaliser les messages d'erreur

Tester les demandes clients (E2E/Staging/Red-Black plate-forme)

Tester les procédures du IT Runbook (Role-play afternoon)

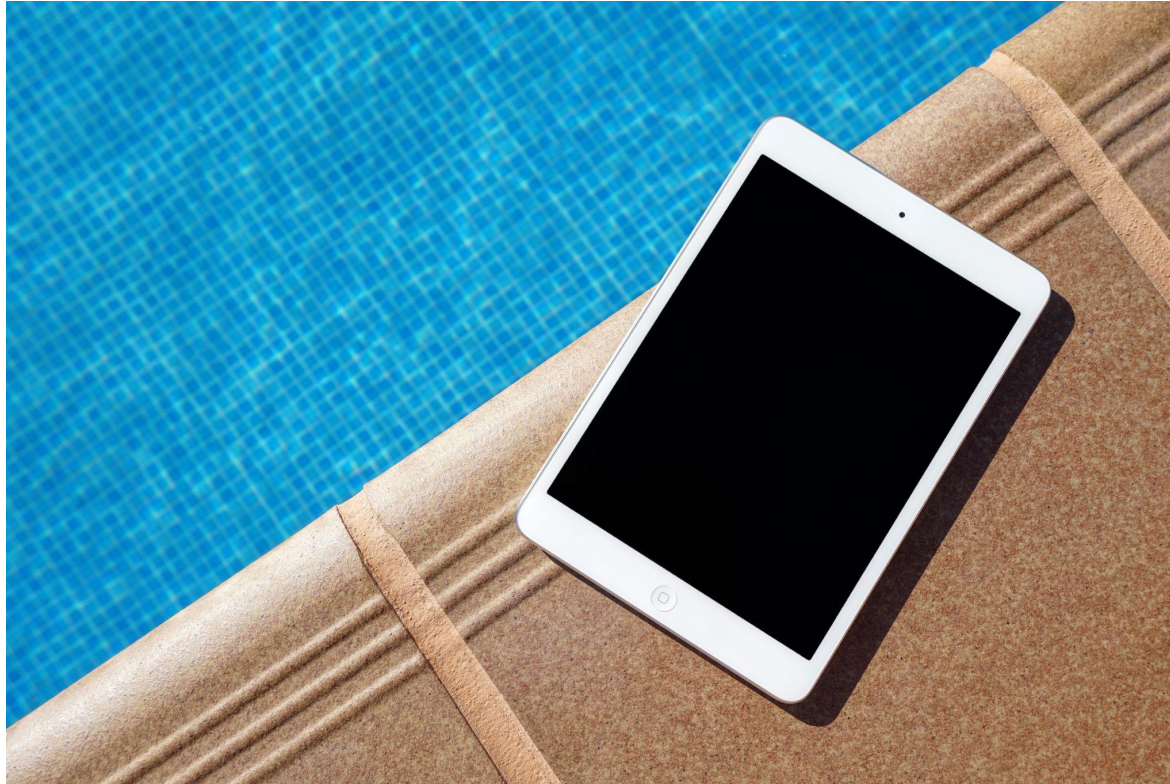


Le retour du Legacy





L'astreinte sonne.. ...





Il était une autre fois.. (en 2021)





Message de Santé Publique France

LEGACY

LE CODE LEGACY, POUR SE PROTÉGER ET PROTÉGER LES AUTRES

- 

Se laver les mains avant,
pendant et après avoir touché
cette merde inmaintenable
- 

Protéger ses yeux de ce code
imbuvable en profitant
notamment des compilations
- 

Utiliser des mouchoirs propres
quand l'envie de pleurer vous
vient et que vous questionnez
votre choix de vie pour ce poste
- 

Ne saluez plus et
n'adressez plus la parole à
la personne responsable
de ce code de merde

Vous avez des questions sur le code legacy ?

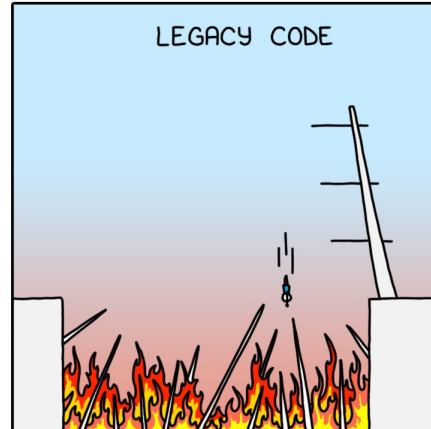
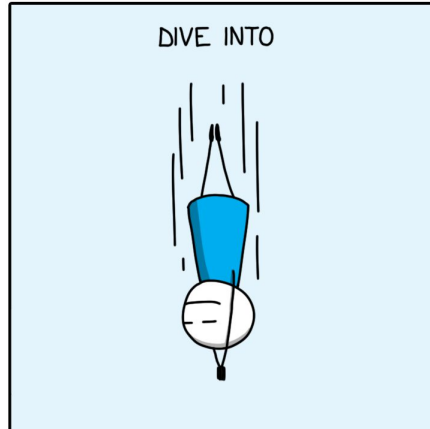
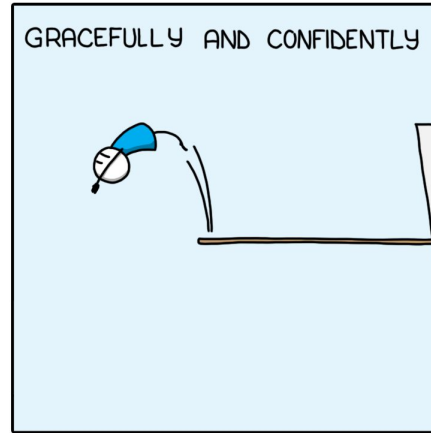
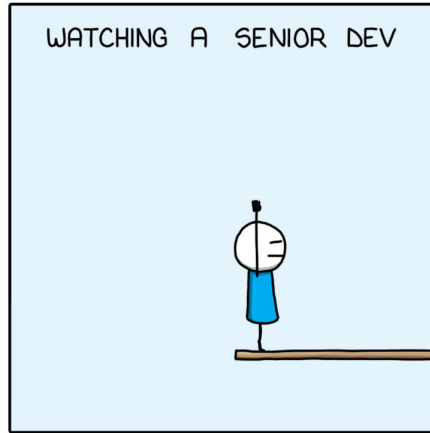
 [LESJOIESDUCODE.FR](https://lesjoiesducodes.fr)



Senior vs Junior

OBSERVER

MONKEYUSER.COM





#SnowCamp #SC2022

@dadideo



54



Blast Effect





Apache Zookeeper

- Créé en même temps qu'à Hadoop
- Base de beaucoup de systèmes distribuées (Kafka v<2.8 / KIP-500)
- Ancêtre de consul/etcd
- Key-Value Store hiérarchique

- Très bons résultats aux tests Jepsen

- Avantages
 - Suivre des changements sur un path (watcher)
 - Noeuds éphémères
 - Notion de sessions



Architecture

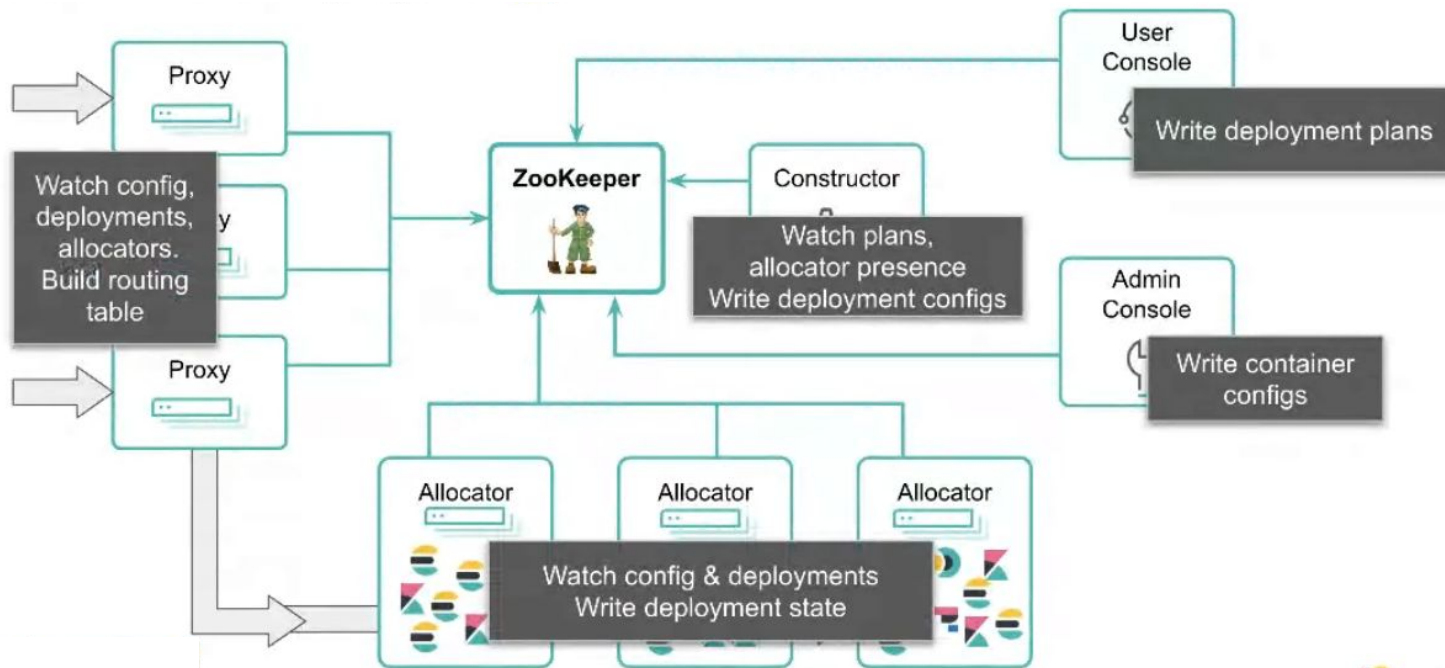


Schéma issu du meetup Toulouse JUG: [War Story, comment les pauses du GC ont pété la prod](#)



Conseils

Avoir un système d'automatisation des incidents (ouverture d'une war room, d'un document collaboratif, etc.)

Maintenir les versions à jour pour gagner les patch/bug fixes

Mise en place d'un circuit breaker

Règles de Warm-up / Slow startup (mode Diesel)

Ajout d'une liste d'attente (Cloudflare Waiting Room)

Chaos Monkey / Analyse des effets de bord



Same JVM, Shoot again





Les limites de la technologie

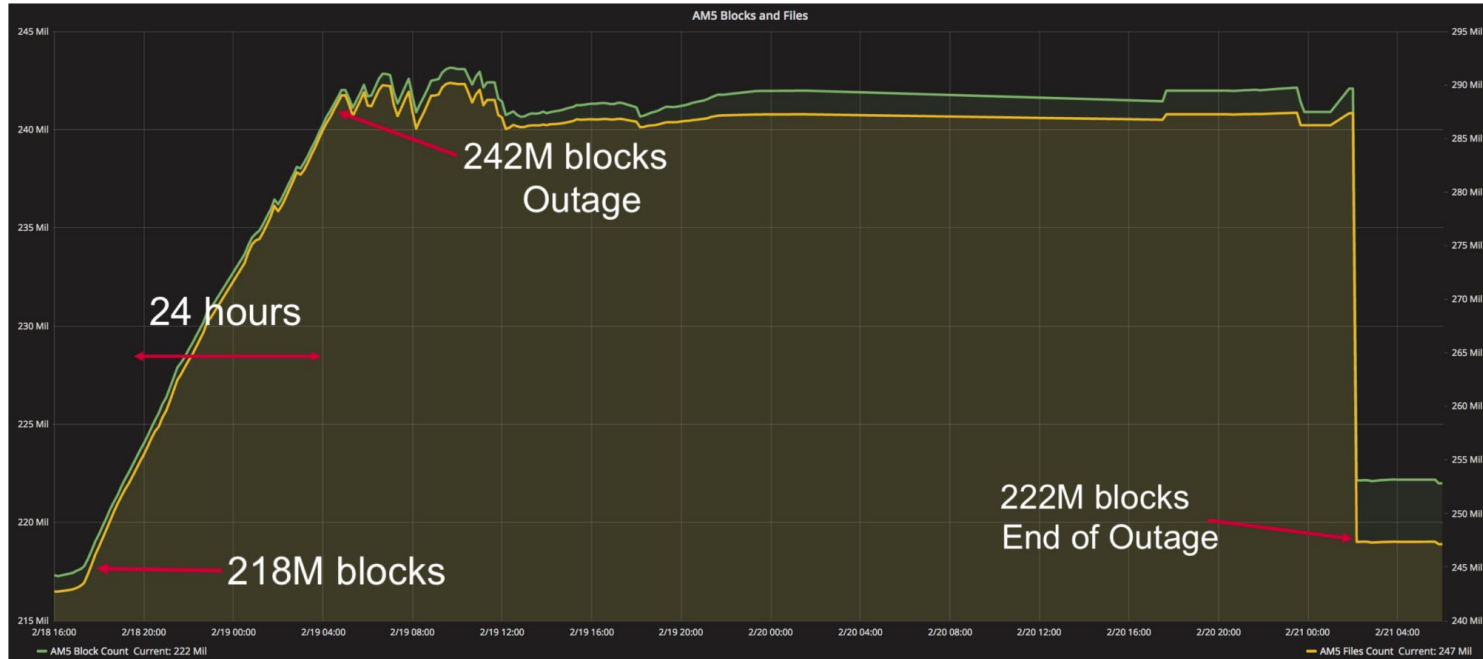


Schéma extrait de Medium : [+40PB per year – The challenge of data growth at Criteo](#)

Hadoop sous pression Retour sur une année d'exploitation à Criteo ([Rémy Saissy](#))



Conseils

Tests de performance

Monitoring des KPI OS

Observabilité / Sondes applicatives

Serveurs de délestage (backup) pour les applications critiques



NewsBlur





Attaque ? Pas de sécurisation sur la DEV->PRD



The NewsBlur Blog

Visit NewsBlur >

```
"query killed during yield: renamed collection 'newsblur.feed_icons' to 'newsblur.system.drop.1624498448i220t-1.feed_icons'"
```

There is honestly no set of words in that error message that I ever want to see again. What is `drop` doing in that error message? Better go find out.

Logging into the MongoDB machine to check out what state the DB is in and I come across the following...

```
nbset:PRIMARY> show dbs
READ_ME_TO_RECOVER_YOUR_DATA  0.000GB
newsblur                       0.718GB

nbset:PRIMARY> use READ_ME_TO_RECOVER_YOUR_DATA
switched to db READ_ME_TO_RECOVER_YOUR_DATA

nbset:PRIMARY> db.README.find()
{
  "_id" : ObjectId("60d3e112ac48d82047aab95d"),
  "content" : "All your data is a backed up. You must pay 0.03 BTC to
XXXXXXXXFTHISGUYXXXXXXX 48 hours for recover it. After 48 hours expiration we
will leaked and exposed all your data. In case of refusal to pay, we will
contact the General Data Protection Regulation, GDPR and notify them that you
store user data in an open form and is not safe. Under the rules of the law,
you face a heavy fine or arrest and your base dump will be dropped from our
server! You can buy bitcoin here, does not take much time to buy
https://localbitcoins.com or https://buy.moonpay.io/ After paying write to me
in the mail with your DB IP: FTHISGUY@recoverme.one and you will receive a link
to download your database dump."
}
```



Capture d'écran du post: [How a Docker footgun led to a vandal deleting NewsBlur's MongoDB database](#)



Twitch

twitch-leaks-part-one

Torrent Management Mode: Manual

Save at

E:\Torrent Downloads

Remember last used save path

Torrent settings

Category:

Set as default category

Start torrent Download in sequential order

Keep top-level folder Download first and last pieces first

Skip hash check

Torrent information

Size: 125.89 GiB (Free space on disk: 819.50 GiB)

Date: Not available

Hash:

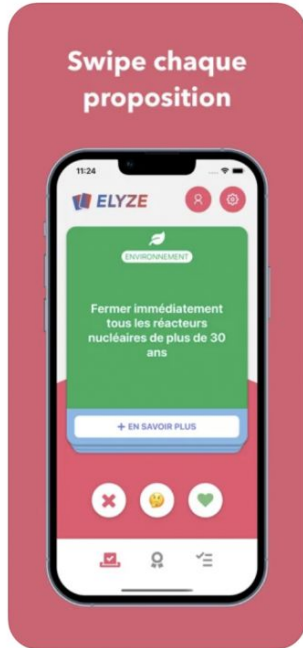
Comment:

Name	Size	Download Priority
▼ <input checked="" type="checkbox"/> twitch-leaks-part-one	125.89 GiB	Normal
> <input checked="" type="checkbox"/> twitch-payouts	4.88 GiB	Normal
<input checked="" type="checkbox"/> 3rdparty.zip	15.1 KiB	Normal
<input checked="" type="checkbox"/> abuse.zip	3.9 MiB	Normal
<input checked="" type="checkbox"/> admin-services.zip	37.2 MiB	Normal
<input checked="" type="checkbox"/> ads.zip	1.14 GiB	Normal
<input checked="" type="checkbox"/> ags-sonic.zip	544.8 MiB	Normal
<input checked="" type="checkbox"/> amzn.zip	44.6 MiB	Normal
<input checked="" type="checkbox"/> andaries.zip	22.1 KiB	Normal
<input checked="" type="checkbox"/> archive.zip	73.2 MiB	Normal
<input checked="" type="checkbox"/> astith.zip	810.3 KiB	Normal
<input checked="" type="checkbox"/> availability.zip	239.0 MiB	Normal
<input checked="" type="checkbox"/> awsi.zip	164.4 MiB	Normal
<input checked="" type="checkbox"/> beefcake.zip	5.8 MiB	Normal
<input checked="" type="checkbox"/> benherr.zip	3.9 MiB	Normal
<input checked="" type="checkbox"/> blade-legacy.zip	2.67 GiB	Normal
<input checked="" type="checkbox"/> bobbcarp.zip	382.4 KiB	Normal
<input checked="" type="checkbox"/> bootcamp.zip	33.9 MiB	Normal





ELYZE - Présidentielle 2022





Avoid HDD

Hype Driven Development
ou
face au code du monde réel



[Quentin ADAM](#)

CEO @ Clever Cloud

@[waxzce](#) on twitter





Conseils

Hype-driven development

CI/CD

[DevSecOps](#): Tests automatique de pénétration (pentest) sur des admin:admin, no password etc..

Isolation de la configuration DEV // PROD (Différent Jenkins ou Vault, Approbation manuelle)



#SnowCamp #SC2022

@dadideo



67



Foxstuck





Foxstuck: Firefox browser bug boots legions of users offline ([The Register](#))



network.http.http3.enabled: false

m Bugzilla Search Bugs

Copy Summary View

Closed Bug 1749908 Opened 7 days ago Closed 7 days ago

Infinite loop in HTTP3 hangs socket thread

▼ Categories

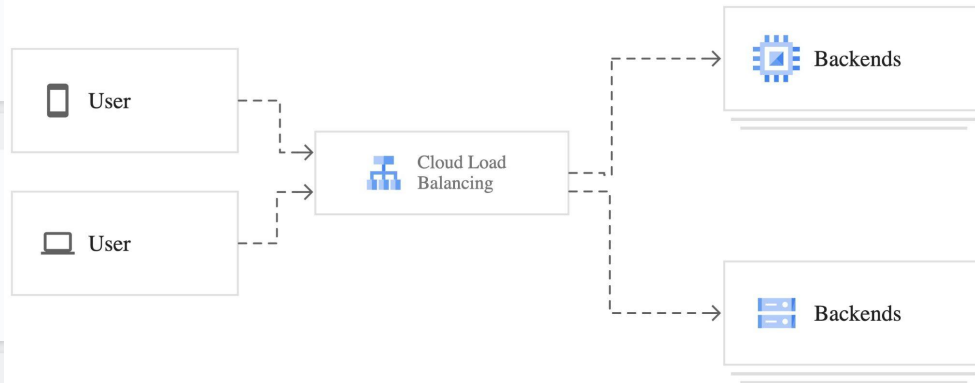
Product: Core 2022-01-13 00:18 PST = CET 8h18
 Component: Networking
 Platform: Desktop All
 Type: defect
 Priority: Not set Severity: --

▼ Tracking

Status: VERIFIED DUPLICATE of [bug 1749910](#)

► People (Reporter: heftig, Unassigned)

► Details





[Update] - Mercredi 2 Février 2022



Retrospective and Technical Details on the recent Firefox Outage



By [Christian Holler](#)

Posted on [February 2, 2022](#) in [Firefox](#)

On January 13th 2022, Firefox became unusable for close to two hours for users worldwide. This incident interrupted many people's workflow. This post highlights the complex series of events and circumstances that, together, triggered a bug deep in the networking code of Firefox.



Retrospective and Technical Details on the recent Firefox Outage (hacks.mozilla.org)



#SnowCamp #SC2022

@dadideo



71



DNS





Disaster Nominal Source

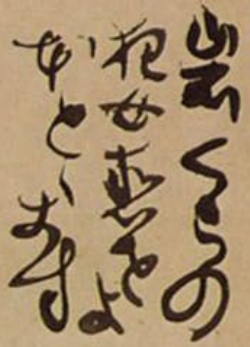




It's not DNS

There's no way it's DNS

It was DNS





Slack

 | Status

Thursday September 30, 2021

Incident

Less than 1% of users may be experiencing trouble connecting to Slack



We've confirmed this issue is now resolved. If you're still encountering any issues connecting, please reload Slack using Ctrl + Shift + R (Windows/Linux) / Command + Shift + R (Mac) on desktop, or fully quit and reopen Slack on mobile. If that doesn't help, let us know at feedback@slack.com.

If you tried switching to Google DNS during the course of this issue, you can choose to keep this enabled, or switch back using these steps:
https://developers.google.com/speed/public-dns/docs/using#switch_back_to_your_old_dns_settings

Our sincere apologies for the interruption to your work, and we appreciate you bearing with us in the meantime. We'll be back with a full summary of the issue.

Note: We've adjusted the timestamp of this update to accurately reflect the issue's time of resolution.

Oct 1, 5:49 PM GMT+2

Apologies for the continued trouble. It will take some time for the DNS changes to resolve this issue for everyone. If organization policy permits, and if you are comfortable making this change, switching to Google DNS may improve things in the meantime. Please find guides below:





DNS workaround



THERE ARE 40 COMMENTS.

Pixelated

Just change it to 8.8.8.8

Posted on **Oct 4, 2021 | 12:08 PM**

shacky003

Pointing your DNS queries to Google (8.8.8.8) or Cloudflare (1.1.1.1) isn't a solution as the article clearly states that BGP route lists were removed globally for the affected domains. It may have worked temporarily due to stale records, but it isn't a fix, as the BGP routes were removed from all public DNS providers.

If a phone number is erased from all phonebooks, getting another phonebook isn't going to help. The routes have to be refreshed/reloaded from the top down..

Posted on **Oct 4, 2021 | 1:46 PM**

Tommy_P

Or 1.1.1.1

Posted on **Oct 4, 2021 | 12:26 PM**

descendency

Tried both. Neither are showing records for facebook.

Posted on **Oct 4, 2021 | 12:49 PM**

mobile_phoney

Or 1-800-PP5-1-DOODOO

Posted on **Oct 4, 2021 | 2:19 PM**

NukedKaltak

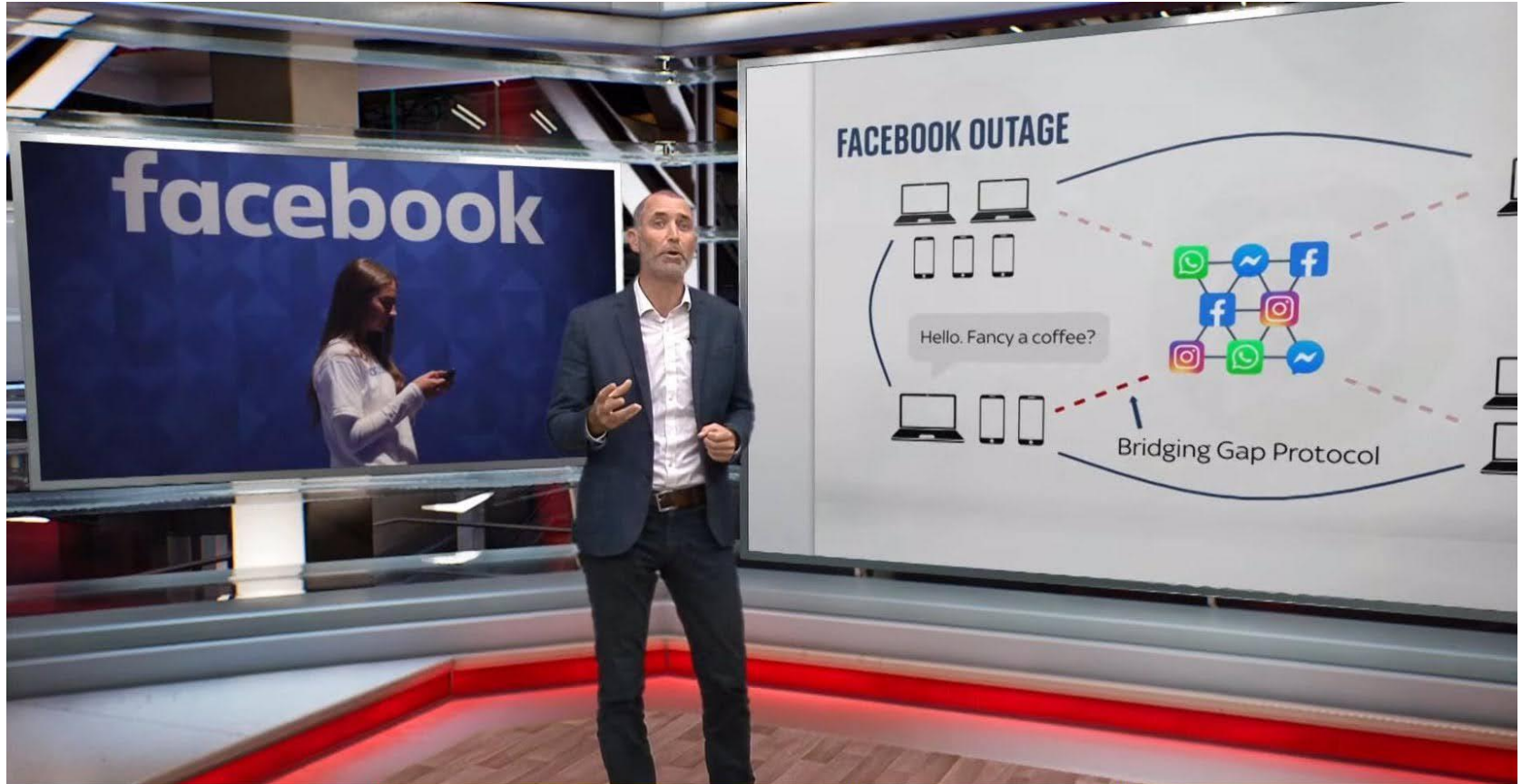
That's not how it works.





Slack & FB







#SnowCamp #SC2022

Julia Evans

FAV

Tools to explore BGP Lectures

Julia Evans @bOrk · Oct 5

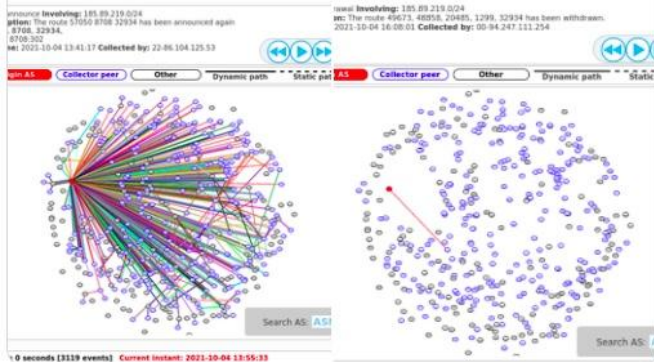
ok I think I understand it better thanks to this tweet! it's much easier to look at the route announcements right before / right after all the routes were deleted because it's a lot less messy

NAYFIELD @Nayfield · Oct 4

Replying to @Nayfield and @JaneLytv

This is connectivity of that network block before and after the configuration change.

Factual summary: The network used to be well connected to the Internet. After a config change, it's not connected. This network contains half of the DNS servers for Facebook and properties.



Mon blog



La panne Facebook du 4 octobre 2021

Première rédaction de cet article le 4 octobre 2021
Dernière mise à jour le 5 octobre 2021

Autres trucs

Accueil
Seulement les RFC

Seulement les fiches de lecture

Aujourd'hui, Facebook a connu une panne importante. Que s'est-il passé ? On sait désormais que la cause racine était un configuration des routeurs BGP. A-t-on des détails ?

Le message d'erreur de beaucoup d'utilisateurs :

Hum, nous ne parvenons pas à trouver ce site.



Mathis Hammel @MathisHammel · Oct 5

THREAD : Hier, une panne massive a affecté Facebook et plein de ses services (Instagram, WhatsApp, Messenger, ...)

Mais il s'est passé quoi au juste ? Je vous explique tout ça. [👉](#)

[#FacebookDown](#) [#InstagramDown](#)



Thanks for being here, come back so



The Cloudflare Blog

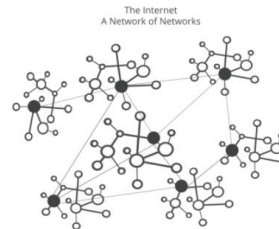
Email Address

Product News Speed & Reliability Security Serverless Zero Trust Developers Deep Dive

Understanding How Facebook Disappeared from the Internet

04/10/2021

Celso Martinho Tom Strick



@dadideo



78



Cécile @AtaxyaNetwork · Oct 4

Bon, on va faire un petit thread plus technique ou je vais tenter d'expliquer au fur et à mesure que je récupère des infos de vous expliquer ce qui se passe chez Facebook !
(Spoiler alert: je suis pas la plus grande experte du réseau, alors il peut y avoir des choses imparfaite)

Cécile @AtaxyaNetwork · Oct 4

On peut dire que j'ai franchi un nouveau palier ? 🤔
bfmtv.com/tech/facebook-...

demandé, qui prend en réalité la forme d'une suite de chiffres baptisée adresse IP.

"Vers 15h50, Facebook a arrêté d'envoyer ses IPs au reste du monde. En conséquence, les serveurs DNS ne sont plus accessibles par les opérateurs, et donc la traduction du nom de domaine vers l'adresse IP ne peut plus se faire. Ce qui entraîne l'inaccessibilité partout dans le monde des services Facebook (Facebook, Instagram, WhatsApp)" résumé Cécile Morange, technicienne réseau, auprès de BFMTV.

Par analogie, le système de DNS d'Internet peut être assimilé à un GPS

👍 29 🔄 515 ❤️ 907 📌 🗨️ Tip



GRZ @GuillaumeRozier

Comment Facebook, Insta et WhatsApp ont pu tomber ?

Cloudflare (qui fournit un CDN très utilisé), a écrit un article complet qui détaille ce qui s'est passé hier soir.
blog.cloudflare.com/october-2021-f-...

J'essaye de vous le résumer en Français #Thread [👉](#)

[Translate Tweet](#)

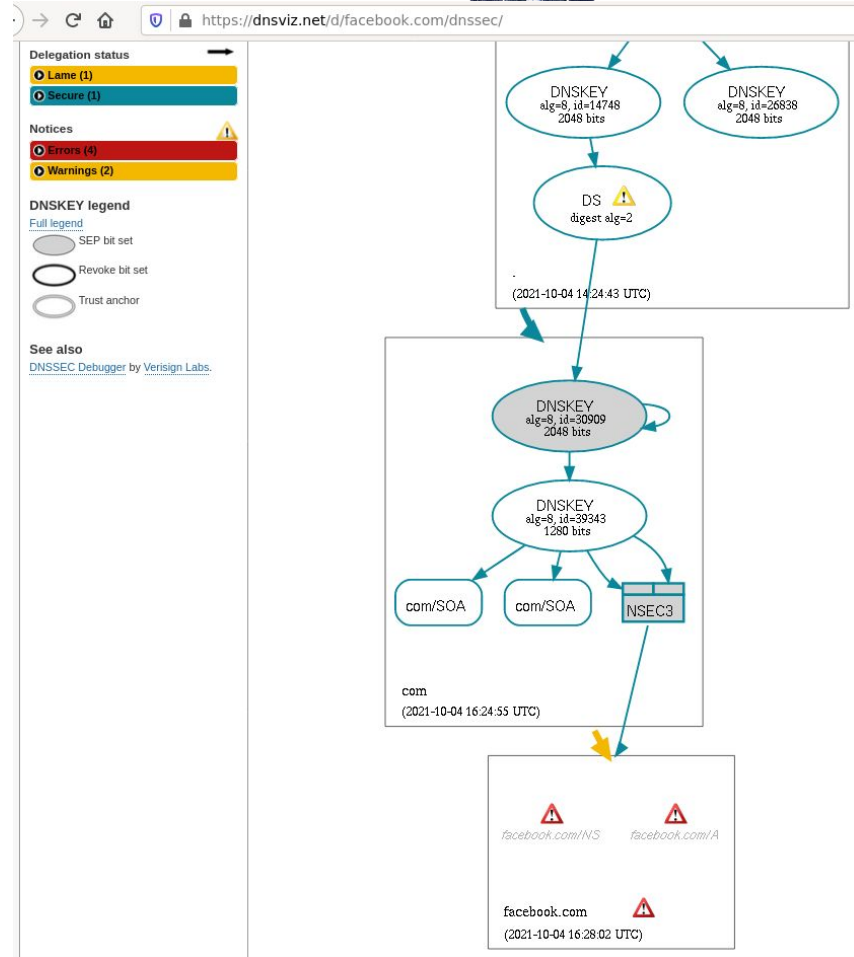


Visualisation de la requête

DNS (TTL=300s) -> trop court!



Blog Stéphane Bortzmeyer:
[La panne Facebook du 4 octobre 2021](#)





Conséquences

-5% du cours de la bourse
6 Milliards \$ (121.6B)

30x DNS queries @ Cloudflare (1.1.1.1)

A peek at [Down Detector](#) (or your Twitter feed) reveals the problems are widespread. While it's unclear exactly why the platforms are unreachable for so many people, their DNS records show that, [like last week's Slack outage](#), the problem is apparently DNS ([it's always DNS](#)). Cloudflare senior vice president Dane Knecht [notes](#) that Facebook's border gateway protocol routes — [BGP](#) helps networks pick the best path to deliver internet traffic — have been “withdrawn from the internet.”



[Instagram.com](#) is flashing a 5xx Server Error message, while the Facebook site merely tells us that something went wrong. The problem also appears to be affecting its virtual reality arm, Oculus. Users can load games they already have installed and the browser works, but social features or installing new games does not. The outage is thorough enough that it's affecting Workplace from Facebook customers and, [according to Jane Manchun Wong](#), Facebook's internal sites.

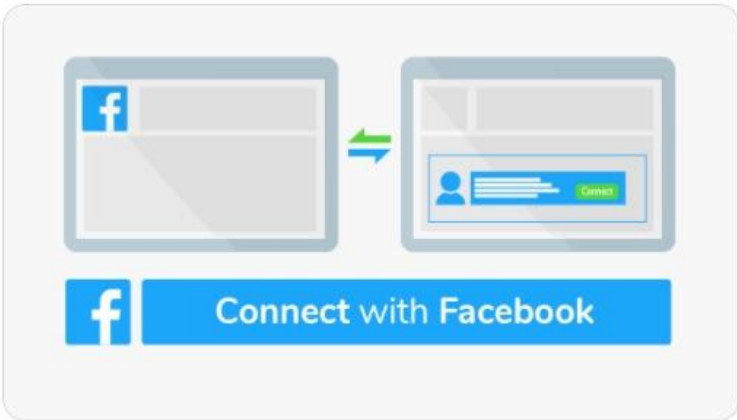




Conséquences latérales

Alexis Kauffmann @framaka · Oct 4

Je ne veux pas en rajouter une couche mais y'a aussi ça.
Tu es seul ce soir au milieu de nulle part car tu n'as pas réussi à ouvrir ton compte **Airbnb** inscrit avec Facebook Connect...
[#facebookdown](#)



Sheera Frenkel ✓
@sheeraf

Was just on phone with someone who works for FB who described employees unable to enter buildings this morning to begin to evaluate extent of outage because their badges weren't working to access doors.

1:51 PM · 10/4/21 · [Twitter for iPhone](#)



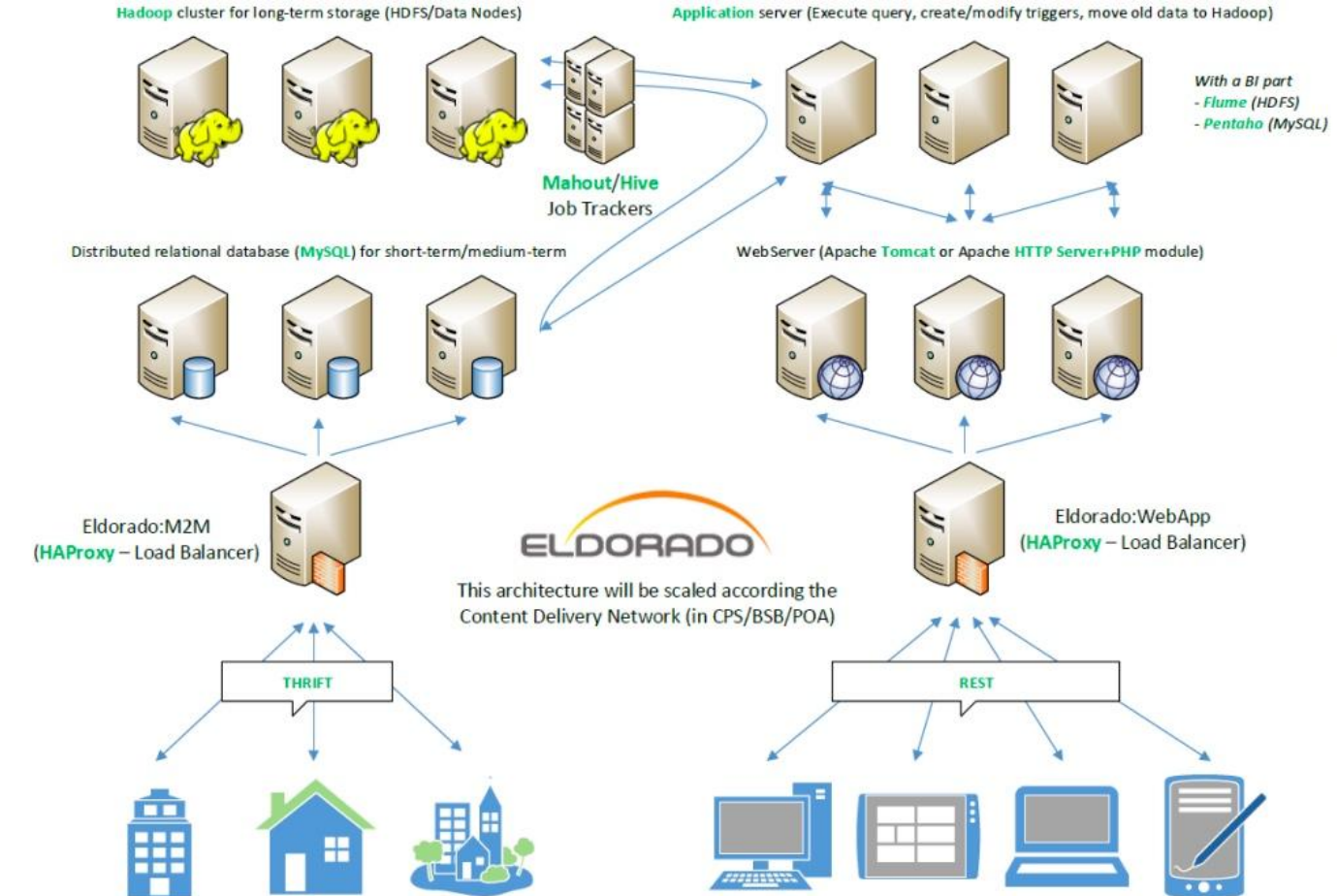
Kevin Collier ✓
@kevincollier

“Don't yet know exactly what's behind the DNS issue that's knocked Facebook/Instagram/WhatsApp offline, but it's really bad. Pretty much everything that runs through those three companies are inaccessible. Employees can't even enter conference rooms because they're IoT!

1:07 PM · 10/4/21 · [Twitter Web App](#)



Channels



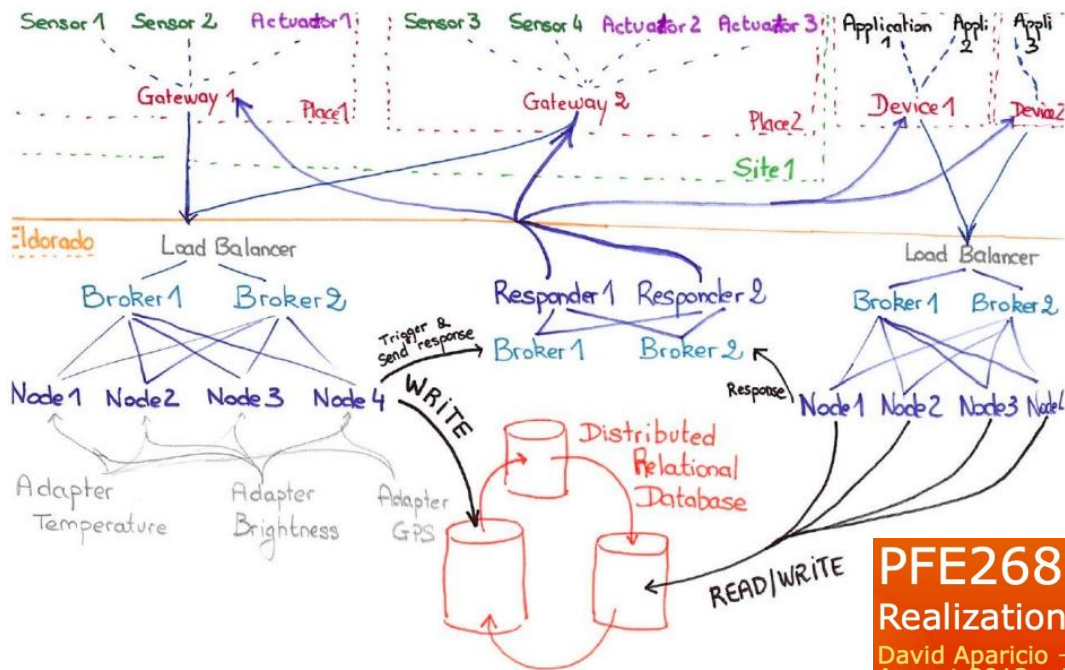
Capture d'écran
PFE268 (2014)

Sensors (information only) and Actuators (actions only) in the client building. They are communicated with Eldorado thanks to a Gateway (Raspberry Pi/Arduino/Other stuff).

Responsive and ergonomic web pages to see sensors values, execute actions and programming some "triggers" (like Lego™ LabVIEW) [Web Browser: HTML5/CSS3/JS]



Entrypoint / Exitpoint (Separation of concerns)



Modules: Hadoop, BI, Jobs, Loas Billing

Capture d'écran PFE268 (2014)

PFE268 – IoT

Realization of a distributed system

David Aparicio – Institute Eldorado
August 2013 – July 2014
Presentation





Conseils

Ne pas avoir un même DNS centralisé à tous les produits (SPOF)
Avoir un TTL plus grand (cache)

Avoir des routes de secours (Inbound/out of bound, bastions, PoP chez d'autres cloud providers)
Avoir la documentation (accessible papier/pdf au cas-où, pour réparer le réseau/liste d'IPs)

Ne pas mettre Statuspage au même endroit que l'INFRA, idem pour la messagerie (Messenger ou Slack)
Sinon impossible de communiquer aux clients

Séparation des préoccupations
Ne pas se reposer uniquement sur les logiciels d'audit (code/ops)

Multi-IPs et nom de domaines (au lieu de sous-domaine)
QoS / Prioriser les flux importants de l'entreprise (lot/Web/etc..)

Ne pas changer ses DNS (1.1.1.1) ou (8.8.8.8) de manière permanente
(car ainsi ils ont l'historique de votre navigation web)



#SnowCamp #SC2022

@dadideo



85

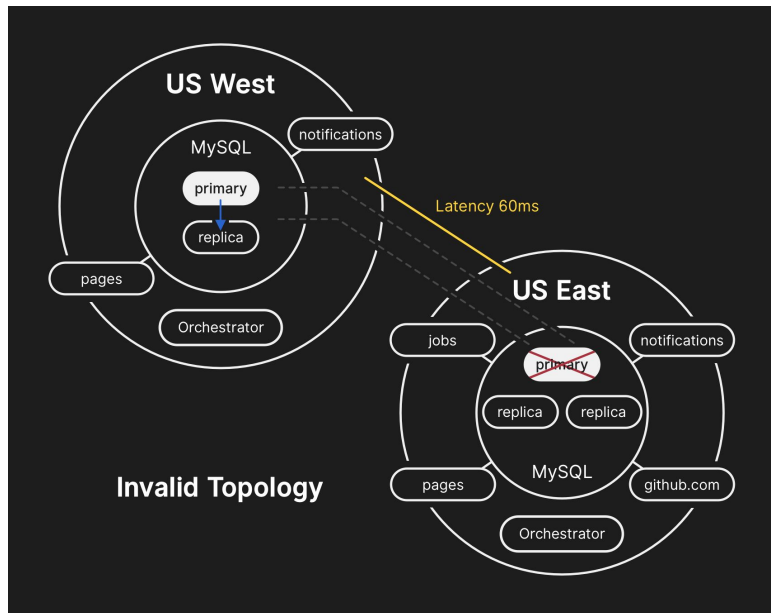


Split-Brain





GitHub



Schémas issus du blog post : [October 21 post-incident analysis](#)

- STATUS RED**
- 1 The site is in an unsupported topology: apps don't support crosssite latencies to MySQL master
 - 2 Database restore from backups
 - 3 Synchronize data across all nodes
 - 4 Manual failover
 - 5 Churn through backlogs
A race against incoming traffic, serving capacity, and not DoSing partners
 - 6 Manual follow up and restoration of missing data
This work is still in progress
- STATUS YELLOW**
Service restored but monitored during playback
- STATUS GREEN**



Conclusion



En bref

- [SRE Blameless culture](#) / With great power comes great responsibility
- QA / Chaos tests
- Former vos équipes : Game day / Wheel of Misfortune
- Tester fréquemment vos backups & hors d'un Drive pour les données médicaux ;-)
- CI/CD & DevSecOps pipelines
- Implémenter & monitorer les metrics importantes issues des incidents (GC Pause, etc)





Wheel of Misfortune

Spin the Wheel!

Incident 6

You've received alerts of high HTTP 5xx error rate...

SPIN

Incident Actions

- ACKNOWLEDGE
- MITIGATE
- TRIAGE

Incident Progress

0%

Timing Controls

00:00:00

▶ ⏪ Lap





Pour aller plus loin

Entreprise / Incident	Date
AWS / Drop database https://aws.amazon.com/message/680587/	24/12/2012
Gitlab / Drop database https://about.gitlab.com/blog/2017/02/10/postmortem-of-database-outage-of-january-31/	31/01/2017
DigitalOcean / Drop database https://www.digitalocean.com/blog/update-on-the-april-5th-2017-outage/	05/04/2017
OVHCloud / Watercooling https://blog.ovh.com/fr/blog/hebergements-web-post-mortem-incident-29-juin-2017/	29/06/2017
Criteo / Datalake HDFS limits + Friday night & New-comer on-call https://medium.com/criteo-engineering/40pb-per-year-the-challenge-of-data-growth-at-criteo-5d5b73ec5294	18/02/2018
GitHub / DataBase Split Brain https://github.blog/2018-10-30-oct21-post-incident-analysis/	30/10/2018
ElasticCloud / Proxy Layer+Zookeeper https://www.elastic.co/blog/elastic-cloud-january-18-2019-incident-report	18/01/2019
CleverCloud / Orages à Paris (Redondance/Dépendance au network provider) https://www.clevercloudstatus.com/incident/376	22/06/2021
NewsBlur / Docker PROD DB exposé sur le net, sans mot de passe https://blog.newsblur.com/2021/06/28/story-of-a-hacking/	23/06/2021
Slack / DNS, pas de post-mortem pour le moment https://status.slack.com/2021-09-30	30/09/2021
Facebook / BGP operations https://engineering.fb.com/2021/10/04/networking-traffic/outage/	04/10/2021

Pour aller plus loin



danluu / post-mortems Public Watch 516 Unstar 8.5k Fork 333

<> Code Pull requests 2 Actions Projects Wiki Security Insights

master 1 branch 0 tags Go to file Add file Code

- andygrunwald Adding new post mortem: Removing all use... 3b2b386 9 hours ago 290 commits
- .github/workflows pass in github token to notfound workflow 3 months ago
- README.md Adding new post mortem: Removing all users from githu... 9 hours ago

README.md

A List of Post-mortems!

Table of Contents

- [Config Errors](#)
- [Hardware/Power Failures](#)
- [Conflicts](#)
- [Time](#)
- [Uncategorized](#)
- [Other lists of postmortems](#)
- [Analysis](#)
- [Contributors](#)

About

A collection of postmortems. Sorry for the delay in merging PRs!

danluu.com/postmortem-les...

debugging post-mortem hacktoberfest

Readme

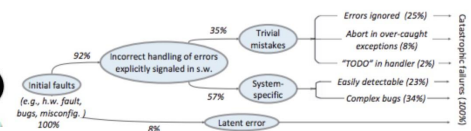
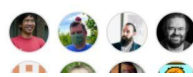
Releases

No releases published

Packages

No packages published

Contributors 86



<http://github.com/danluu/post-mortems>



Voulez-vous travailler avec David  ?

Voici 3 offres dans l'équipe GIS :



IT Technical Leader



Développeur Python



Manager
Database Opensource





#SnowCamp #SC2022



@dadideo



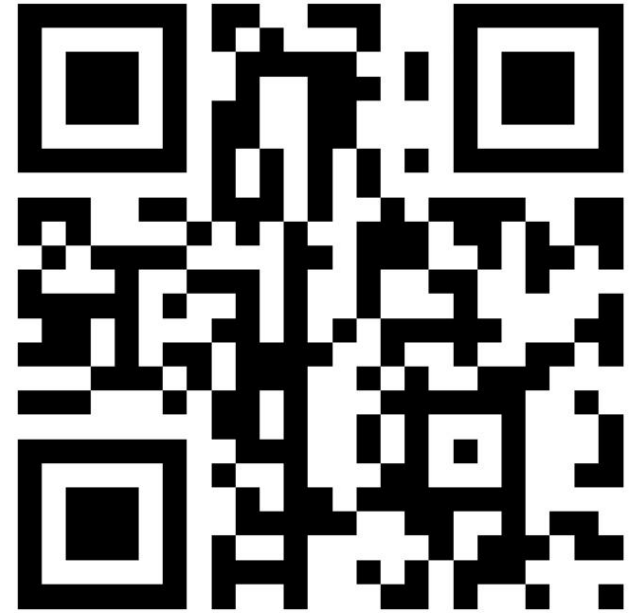
93



Avez-vous des questions ?

  N'oubliez pas de me donner votre ROTI / avis sur : <https://s.42l.fr/sc22>

 Rejoignez-nous sur <https://careers.ovhcloud.com>



<https://roti.express/r/sc22-043>





Vouchers



ESSAI GRATUIT PUBLIC CLOUD

Profitez maintenant de 30 € de crédit offert* avec le code : CLOUD

Commencer



ESSAI GRATUIT AI NOTEBOOKS

Profitez d'un crédit offert* de 70€ pour démarrer votre notebook Jupyter ou VS Code en quelques minutes ! **Code : AI-NTBK21**

En profiter





Slides



**Merci pour
votre attention !**