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

David Aparicio @dadideo

@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)

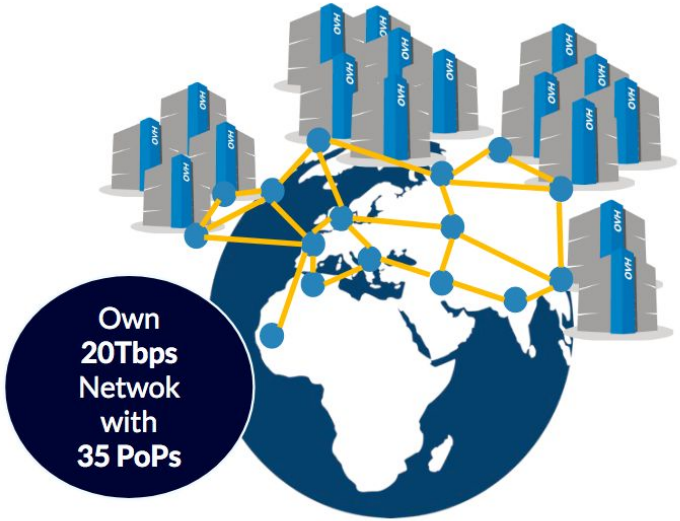
OVHcloud: un leader européen

200k Private cloud VMs running

1 **Dedicated IaaS Europe**

Hosting capacity : 1.3M Physical Servers

360k Servers already deployed



30 Datacenters

GAIA-X

SecNumCloud

Depuis Déc. 2020

> **1.3M** Customers in **138** Countries

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 — T2 >20e
- SuperPlan — T3 >80e
- Game — T4 >300e
- Virtualization — T5 >600e
- Storage — 12KVA /32KVA
- Database
- Bigdata
- 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
- Baremetal
- K8S, IA IaaS
- 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)
- Stortage, Network, Databases

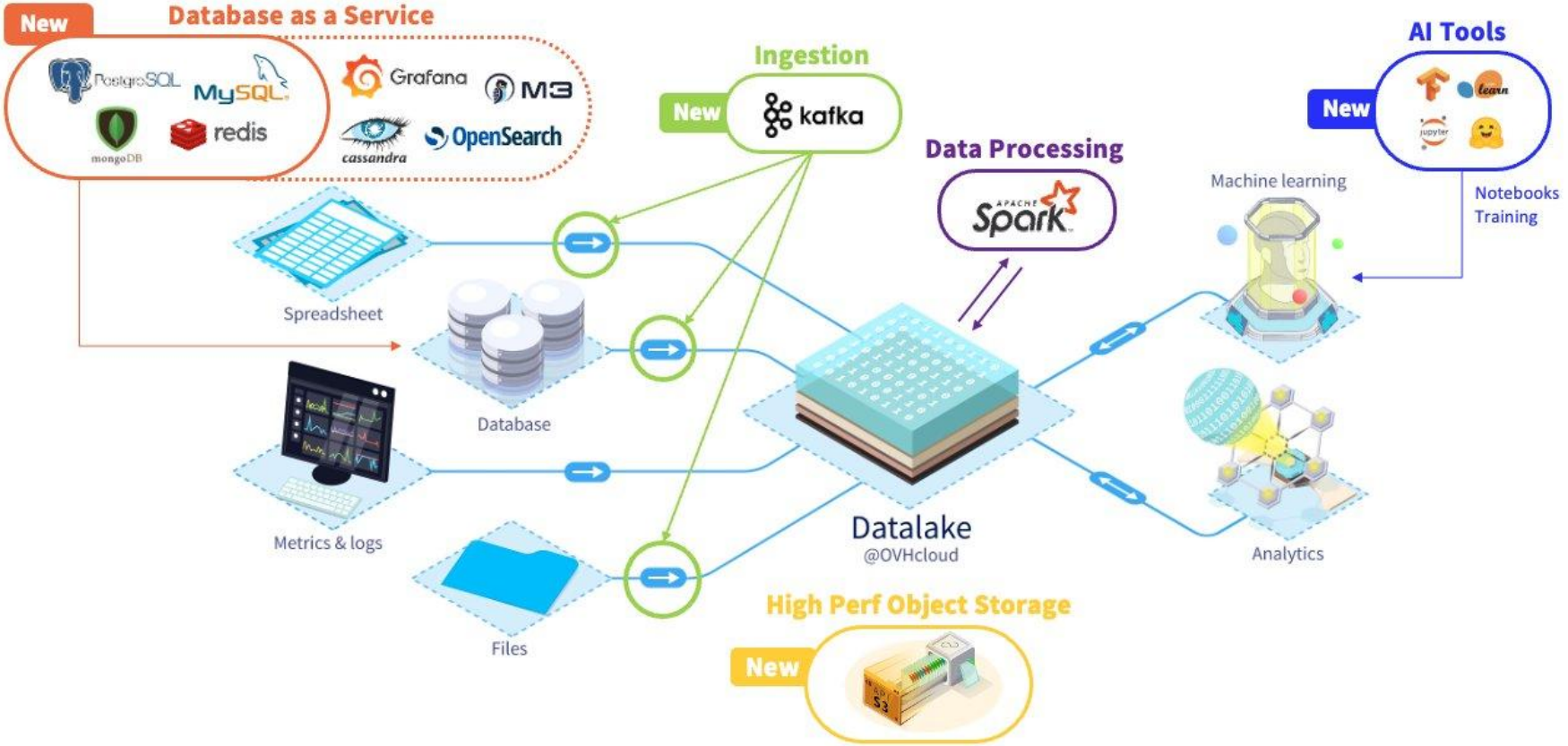
Storage
- Ontap Select, Nutanix File
- OpenIO, MinIO, CEPH
- Zerto, Veeam, Atempo

AI
- ElementAI, HuggingFace,
- Deepopmatic, Systran,
- EarthCube

Bigdata / Analitics / ML
- Cloudera over S3, Dataiku,
- Saagie, Tableau,

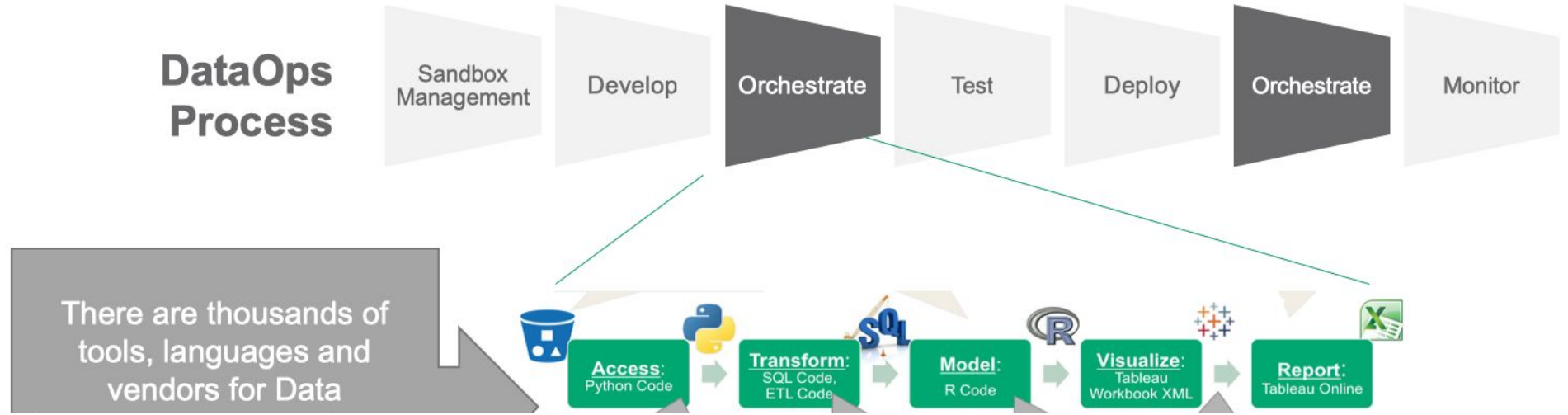
Hybrid Cloud
- vRack Connect, Edge-DC, Private DC
- Dell, HP, Cisco, OCP, MultiCloud

Secured Cloud
- GOV, FinTech, Retail, HealtCare


New
Database as a Service
PostgreSQL
MySQL
mongoDB
redis
Grafana
M3
cassandra
OpenSearch
Ingestion
New
kafka
Data Processing
APACHE Spark
AI Tools
New
learn
jupyter
Notebooks
Training
Machine learning
Spreadsheet
Database
Metrics & logs
Files
Datalake
@OVHcloud
Analytics
High Perf Object Storage
New

DataOps @ GIS-DATA

- Installation / Configuration du datalake
- Industrialisation / Automatisation des procédures
- Day1 & Day2 Operations



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

Conclusion

Introduction

Photo by Chris Karidis on Unsplash

🎯 Alex Hidalgo

https://forum.compagnons-devops.fr/t/partage-de-minutes-fail/1659

Discourse

Partage de minutes fail

Général

Uggla Compagnon avr. '21

Bonjour un petit sujet pour partager un peu nos mésaventures quotidiennes…
Et se défouler quand les choses vont mal.

La vm du jour, tout va bien… (note la vm host le node d'un cluster flink qui bizarrement est hs.)

```
top - 12:24:11 up 66 days, 17:34, 1 user, load average: 1688,85, 1011,22, 712,98
Tasks: 1191 total,  1 running, 1188 sleeping,  0 stopped,  2 zombie
%Cpu(s): 0,2 us  0,4 sy, 0,0 ni, 99,4 id, 0,0 wa, 0,0 hi, 0,0 si, 0,0 st
KiB Mem : 16259496 total, 8284772 free, 4928824 used, 3045900 buff/cache
KiB Swap: 4194300 total, 4194212 free,      88 used. 10080532 avail Mem
```

Note 1: En bon 🐱 noir, ça arrive forcement juste le Vendredi avant les vacances.
Note 2: J'ai pas la main sur cette infra, mais je crois que qq chose va pas bien.

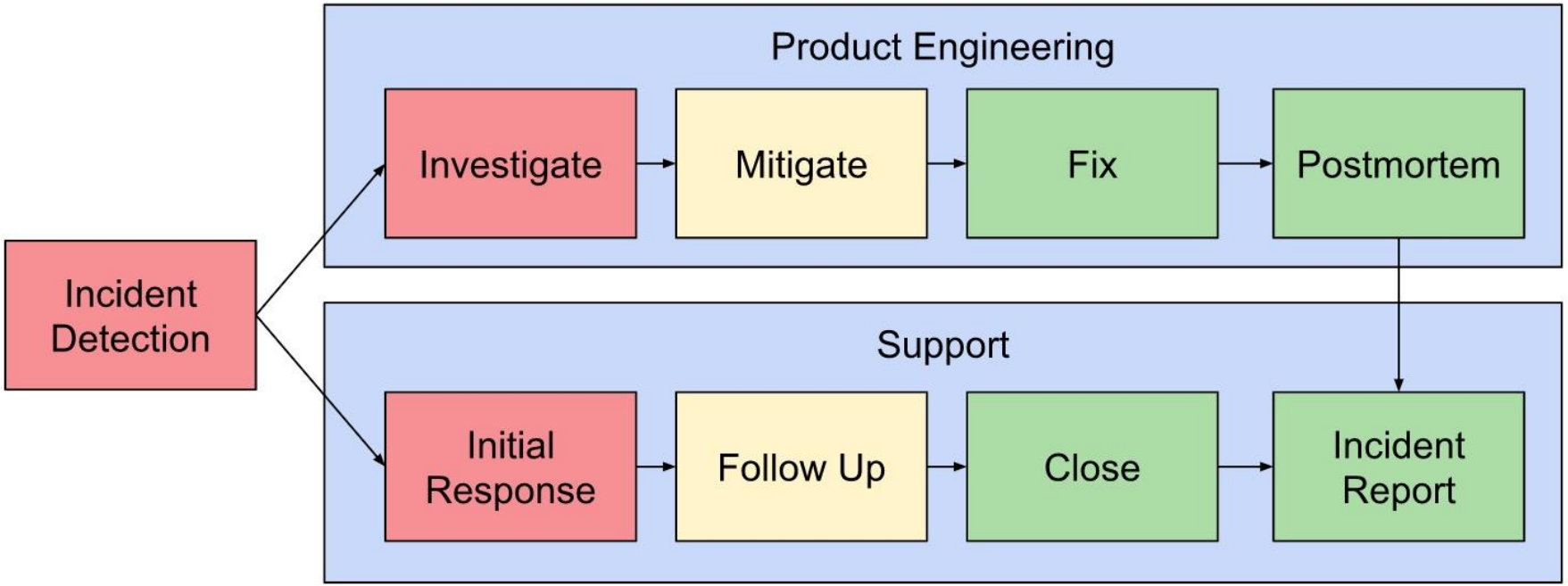
3

Un live tous les premiers vendredis de chaque mois à 17h !

créé	dernière réponse	73 réponses	1,1 k vues	17 utilisateurs	108 J'aime	9 liens
avr. '21	2 j					

🎯 Forum des Compagnons DevOps / 🎤 Raconte-nous tes gros échecs ! | Libre Antenne

Post-mortem


Product Engineering
Investigate
Mitigate
Fix
Postmortem
Incident Detection
Support
Initial Response
Follow Up
Close
Incident Report

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

Exemples récents

https://www.gitpodstatus.com

Gitpod

SUBSCRIBE TO UPDATES

Degraded workspace performance Subscribe

Update - All workspace starts for XL clusters are entirely running on *41xl. 50% of workspace starts for other clusters land on *41, which also contains the fix for performance degradation.
Apr 21, 19:45 UTC

Update - We've received positive feedback from customers who were previously experiencing issues. Additionally, metrics looks promising, too. We've increased the traffic shift for XL clusters to 50%.
Apr 21, 12:30 UTC

Monitoring - We've deployed a fix for workspaces that run in XL clusters.

25% of new XL workspaces will start on *41xl, which include a fix for this issue: https://github.com/gitpod-io/gitpod/issues/9406
Apr 21, 00:23 UTC

Identified - We've identified a likely suspect and are testing multiple fixes internally.
Apr 20, 19:15 UTC

Investigating - Customers have reported that workspaces which were previously running well now have performance issues. We are inspecting recent changes to the system, and are running internal tests.
Apr 20, 13:45 UTC

https://status.heroku.com/incidents/2413

Heroku Status Subscribe

Heroku Security Notification

US EU

Apps 115 HOURS, 50 MINUTES

ACTIVITY

Update

We continue to make progress on our investigation into this issue. During the course of our investigation, information we have received from Heroku customers has been useful. If you have obtained logs from GitHub and identified suspicious activity that you believe may assist us in our investigation, please contact security@salesforce.com. We appreciate your collaboration and trust as we continue to make your success our top priority.

We will continue to post updates to status.heroku.com as additional information becomes available.

POSTED 2 DAYS AGO, APR 20, 2022 01:09 UTC

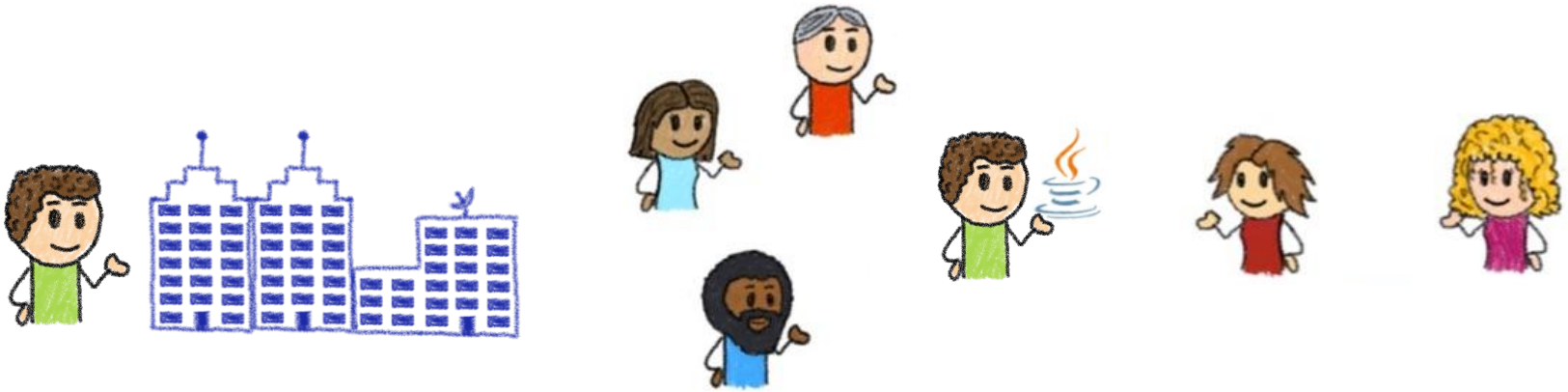
🎯 Incidents du jeudi 21 Avril 2022 : Status de Gitpod / Status d'Heroku

Elliot

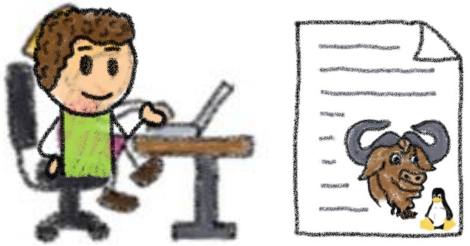
Photo by Chris Karidis on Unsplash

Elliot Alderson

Allsafe, great place to work 2022

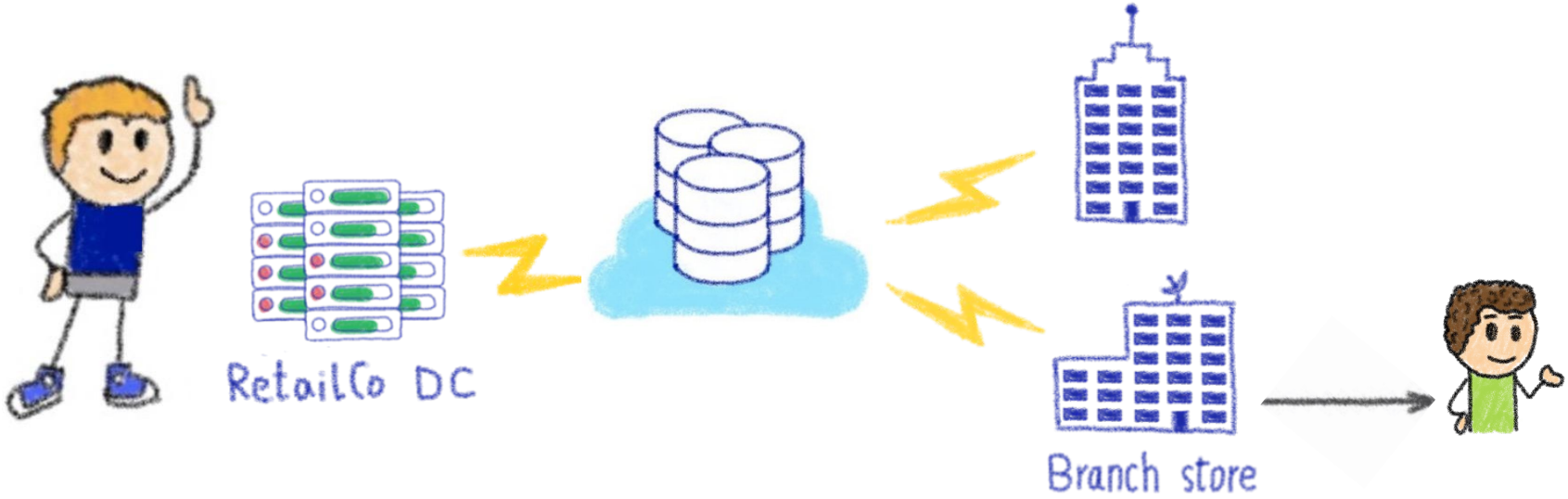


Time to code



P1 detected, tout le monde sur le pont

Root cause



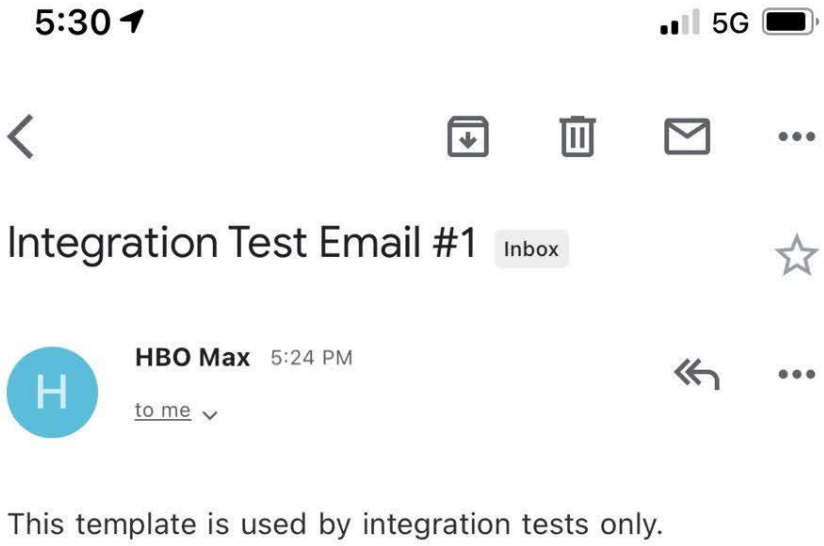
AWS, GitLab, DigitalOcean

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

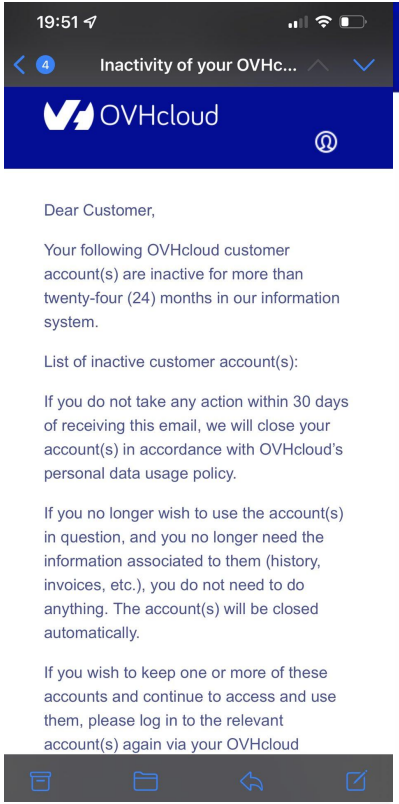
Insérer une approbation manuelle / revue
Auditer et protéger l'environnement (SIEM,RBAC)
Informations d'identification/connexion protégé en lieu sûr (Vault, KeePass)
Tester vos procédures de restauration (backup)

Cas non isolé: le stagiaire



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

Mailing / Publipostage



🎯 OVHcloud - Answer (11 October 2021)

Les tests en PROD

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 :)

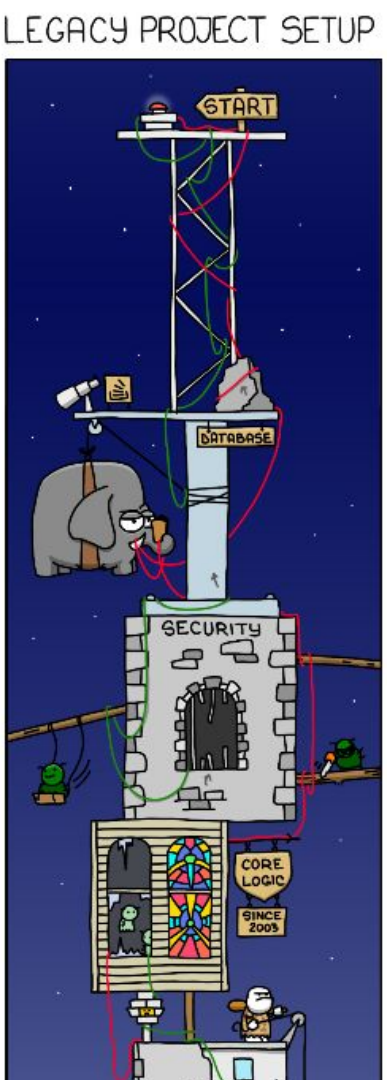
🎯 AirFrance (24 Janvier 2022)

Legacy

Photo by Chris Karidis on Unsplash

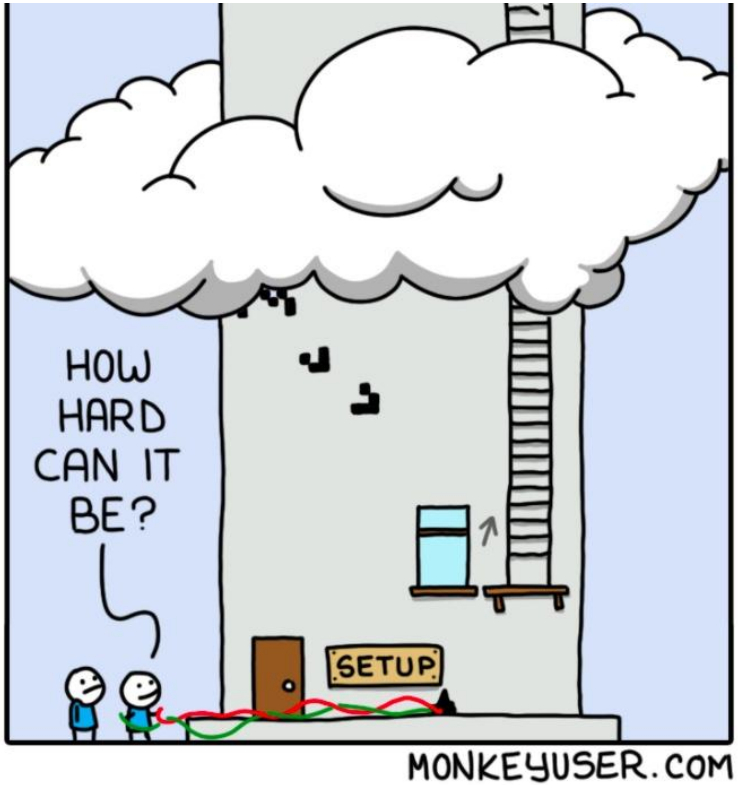
Il était une fois.. (en 2020)

Quand soudain l'astreinte sonne


LEGACY PROJECT SETUP
START
DATABASE
SECURITY
CORE LOGIC
SINCE 2003

Legacy

Legacy..

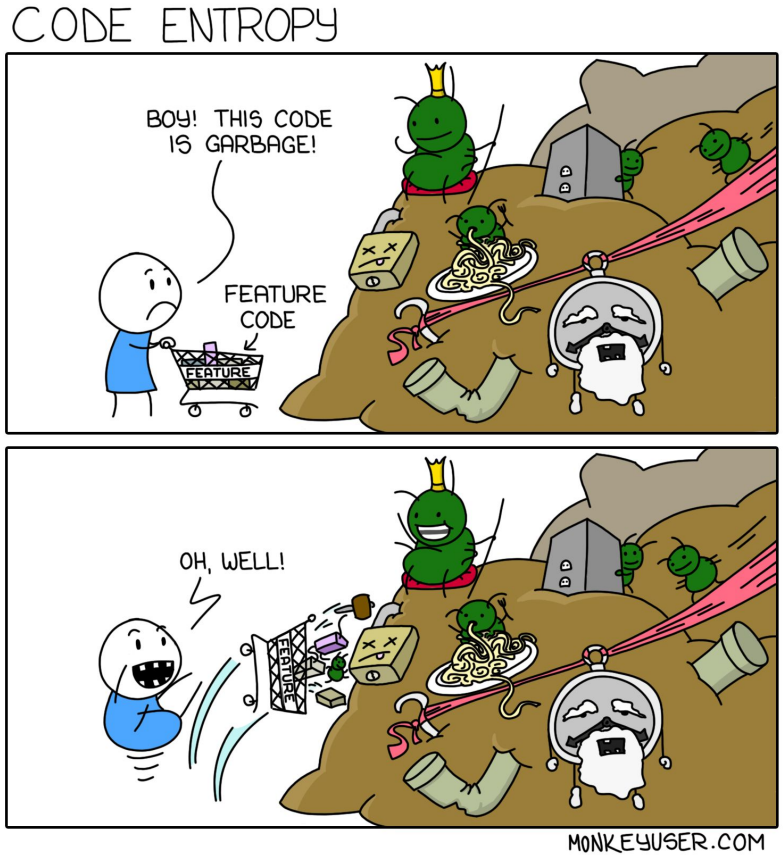


L'astreinte sonne à nouveau

TECH DEBT


THIS WAY!
WE ARE PROGRESSING SO FAST TOGETHER
THIS DOESN'T LOOK GOOD
TECH DEBT
MONKEYUSER.COM

Codons! Le bon et le mauvais patch (dev)



Méthode KISS

KEEP
CALM
AND
KISS

Original:	*Variante :*
Keep	*Keep*
It	*It*
Simple	*Super*
Stupid	*Simple*


```
#!/bin/bash
# Script to test server connectivity
set -euo pipefail
IFS=$'\n\t'

HOST="host"
PORT="8080"
TIMEOUT="10"
EXIT_FAIL_AND_RESTART="1"
EXIT_FAILURE_ON_RESTART="255"

## Did we get a timeout? ##
if echo "Hello Server, please kick me" | timeout ${TIMEOUT} nc -w20 ${HOST} ${PORT}
then
  echo "Success: Server alive."
  exit 0
else
  "$(date)"
  echo "Failure: Server timeout." >&2
  echo "Restarting the service..."
  if service server status && date && service server restart
  then
    echo "Restart done"
    exit ${EXIT_FAIL_AND_RESTART}
  else
    echo "Restart failure"
    exit ${EXIT_FAILURE_ON_RESTART}
  fi
fi
```

Legacy

Attention: Serveur

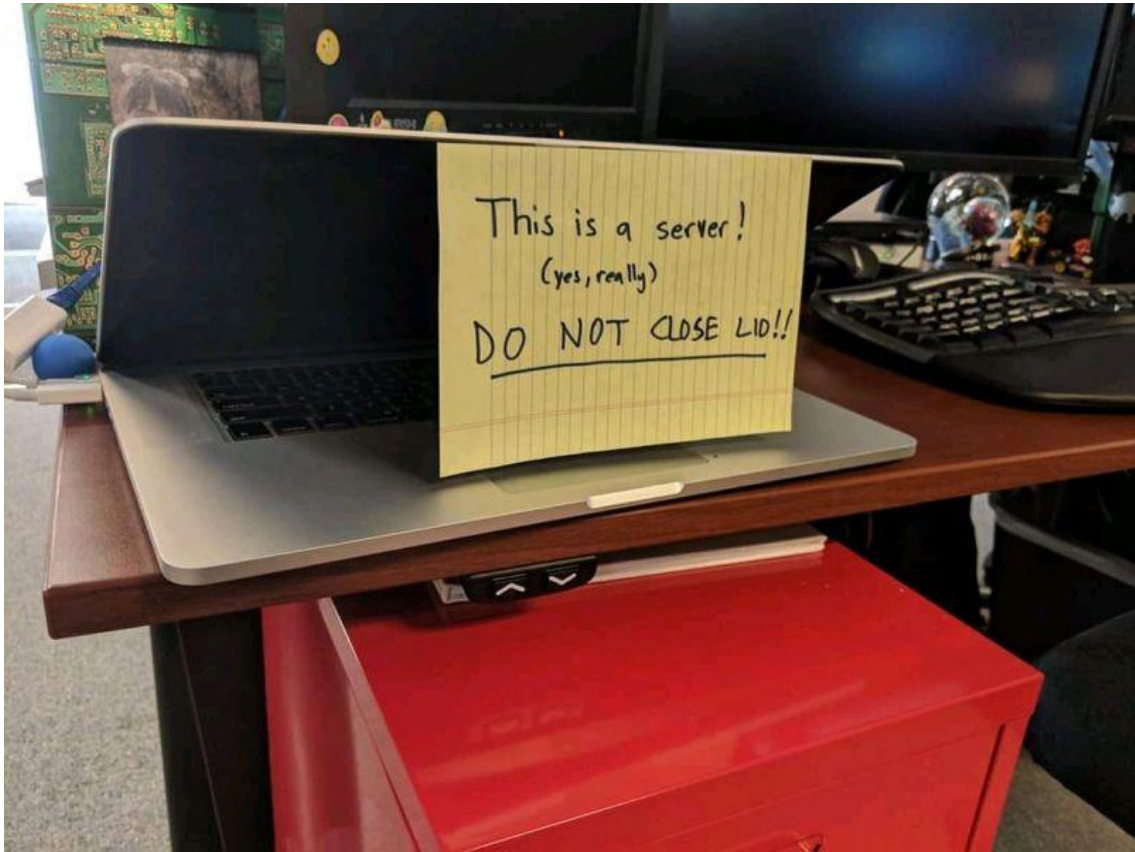
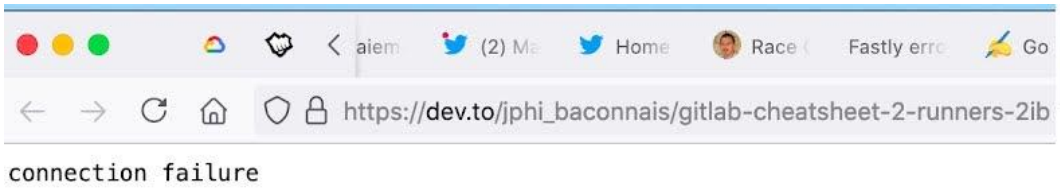


Image trouvée sur la twittosphère

CDN

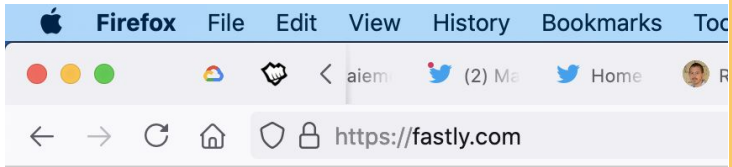
Photo by Chris Karidis on Unsplash

Marmiton


https://dev.to/jphi_baconnais/gitlab-cheatsheet-2-runners-2ib
connection failure


https://dev.to/rinkiyakedad/race-conditions-in-golang-57n2
Fastly error: unknown domain: dev.to.
Details: cache-ams21071-AMS

Fastly



Error 503 Service Unavailable

Service Unavailable

Guru Mediation:

Details: cache-ams21041-AMS 1623148153 16274930

Varnish cache server

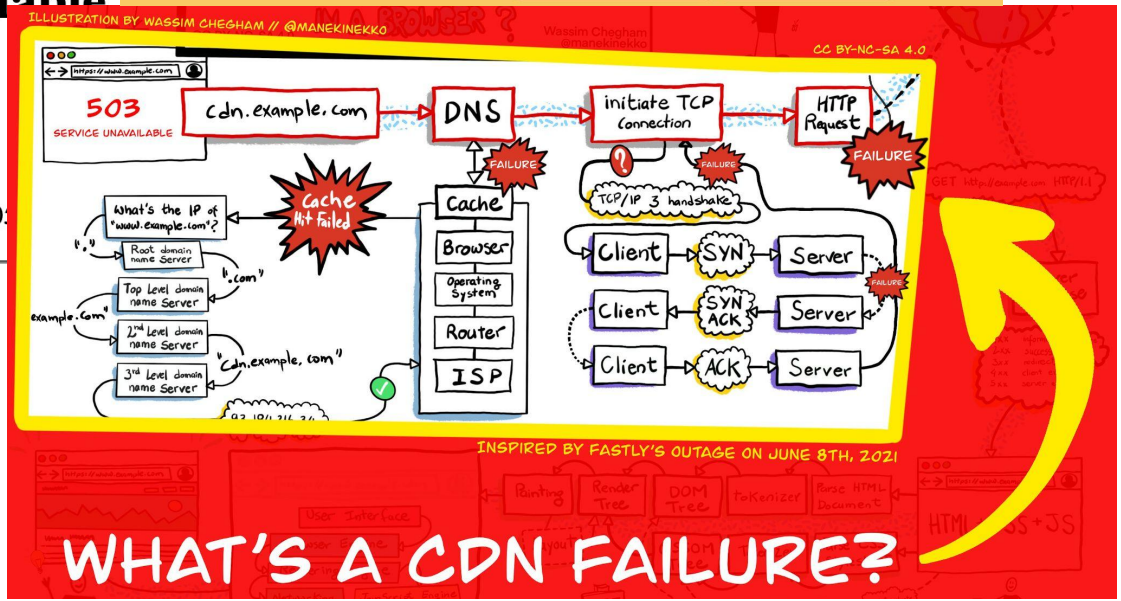
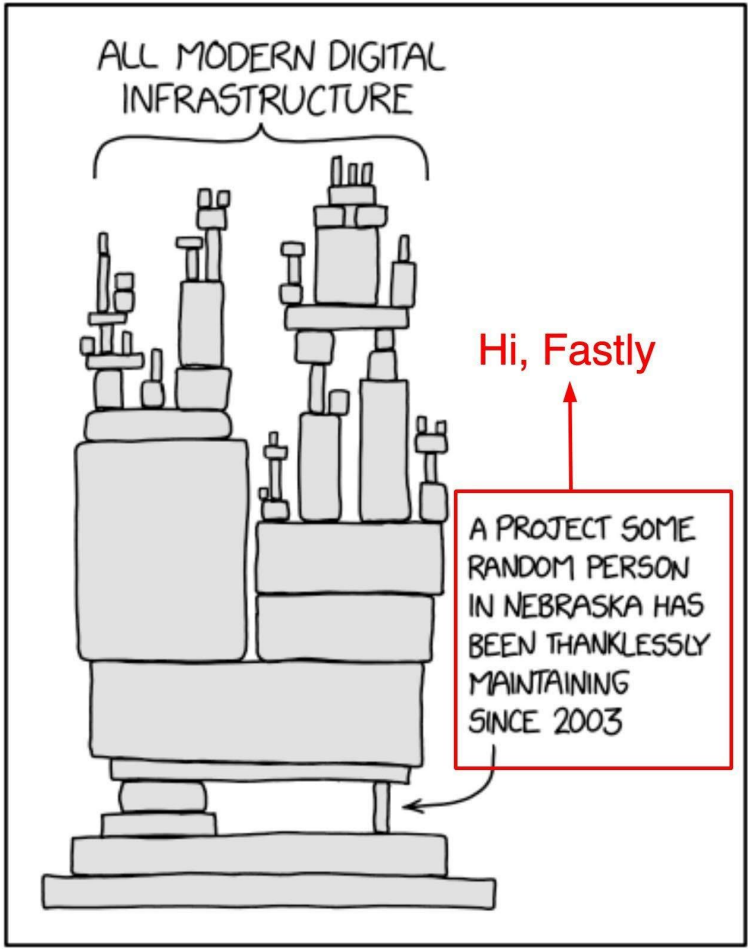


Schéma de Wassim Chegham

Resilience



XKCD 2347 Dependency

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)
Réponse inconnue => S'arrêter proprement

Free food

Posted by u/luciferous22 3 years ago

52

A glitch in uber eats payment method with a partner company allowed users to order food without paying. Students in our city completely exploited this glitch and ordered around 14000 USD of free food.

🎯 https://twitter.com/GergelyOrosz/status/1502947315279187979

Le retour du Legacy

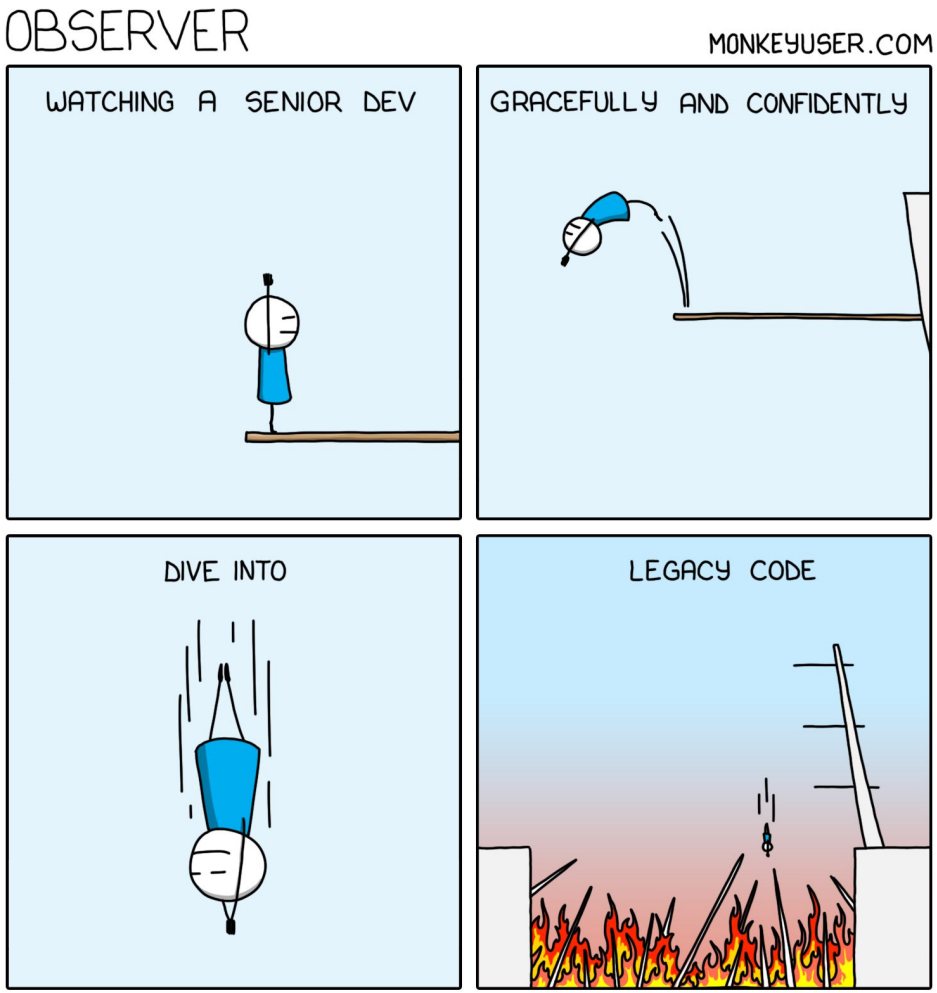
Photo by Chris Karidis on Unsplash

L'astreinte sonne.. ...

Il était une autre fois.. (en 2021)

Message de Santé Publique France

Senior vs Junior



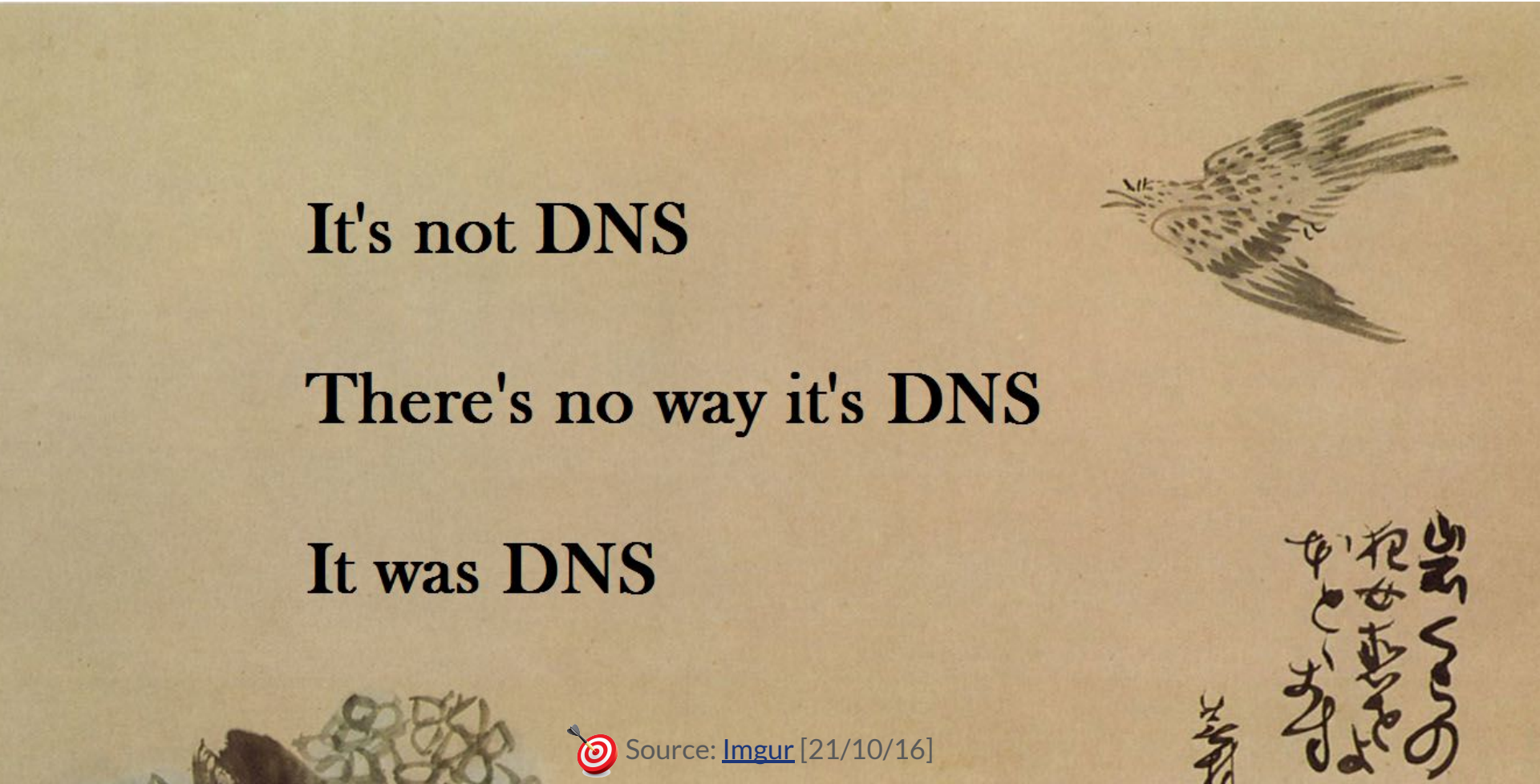
Code

```
#!/bin/bash
FLAG=/home/myuser/_MAINTENANCE_ONGOING.flag

echo "STEP 1 - STOP SERVICE"
systemctl status dremio && systemctl stop dremio

echo "STEP 2 - CREATE THE FLAG TO AVOID OTHER actions"
touch $FLAG

echo "STEP 3 - RUN DREMIO CLEANING SCRIPT"
dremio-admin clean --max-job-days 15
dremio-admin clean --delete-orphans
dremio-admin clean --compact
dremio-admin clean --reindex-data

echo "STEP 4 - START SERVICE"
systemctl status dremio && systemctl start dremio

echo "STEP 5 - REMOVE THE FLAG"
rm $FLAG
```

DNS

Photo by Chris Karidis on Unsplash


Disaster
Nominal
Source



Source: Imgur [21/10/16]

Slack

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:

🎯 Capture d'écran du PM 30/09/2021: Slack Status

DNS workaround

THERE ARE 40 COMMENTS.

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**

Pixelated

Just change it to 8.8.8.8

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

🎯 Capture d'écran TheVerge [4/10/21 20h52], Post-Mortem

Slack & FB


I make sure that one bad config on one component doesn't bankrupt the entire company.. that's what the F#@ I do


facebook
FACEBOOK OUTAGE
Hello. Fancy a coffee?
Bridging Gap Protocol
sky news .com
ing young people's mental health
BREAKING NEWS
Facebook's Director of Poli

FB: 04-Oct-21

Cloudflare détecte des changements BGP

Cloudflare rapporte un pic suite à des changements de routage de BGP effectués par Facebook.
Immédiatement les utilisateurs ont été incapables de résoudre les URL de Facebook.

15:40 UTC

16:00

Incident débuté chez FB

D'après le Post-Mortem de Facebook
Les serveurs DNS ne propagent plus les BGP si le réseau n'est pas sain (protection)

LDAP

Tous les utilisateurs n'arrivent plus à accéder aux services (Facebook, Instagram, WhatsApp)
Même les employés ne peuvent pas rentrer dans les bureaux avec leurs badges. Documentation/Messagerie interne indisponibles

17:00

Pénétration du DC, modifications manuelles

L'accès était hautement difficile, de plus des mécanismes de protection, empêchent des modifications directes/manuelles

Fin de l'incident

Les dernières erreurs disparaissent
Les utilisateurs arrivent pleinement à utiliser les outils de Meta

5 Oct - 03:00 UTC

Julia Evans

FAV

Lectures

Tools to explore BGP

Julia Evans @b0rk · Oct 5

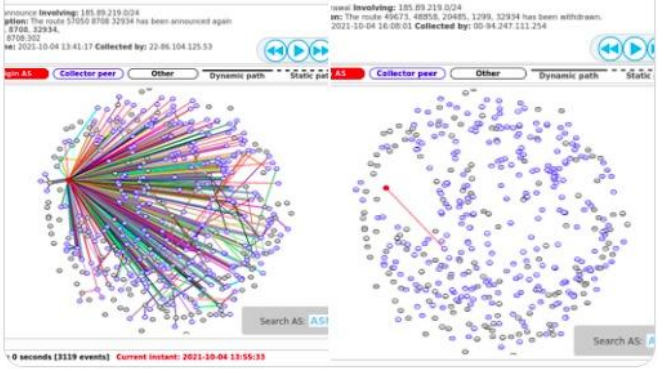
ok I think I understand it better thanks to this tweet! it's much easier to look at the route announcements right before / right after all the routes were deleted because it's a lot less messy

NAYF IELD @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

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

Le message d'erreur de beaucoup d'utilisateurs :

JE SUIS CHARLIE

Autres trucs

Accueil
Seulement les RFC
Seulement les fiches de lecture

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

CLOUDFLARE The Cloudflare Blog

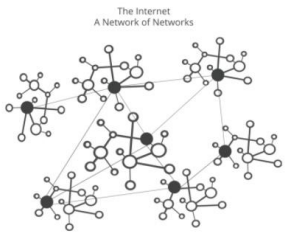
Email Address

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

Understanding How Facebook Disappeared from the Internet

04/10/2021

Celso Martinho Tom Strickx



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 inparfaite)

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 entraine l'inaccessibilité partout dans le monde des services Facebook (Facebook, Instagram, What'sApp)" 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

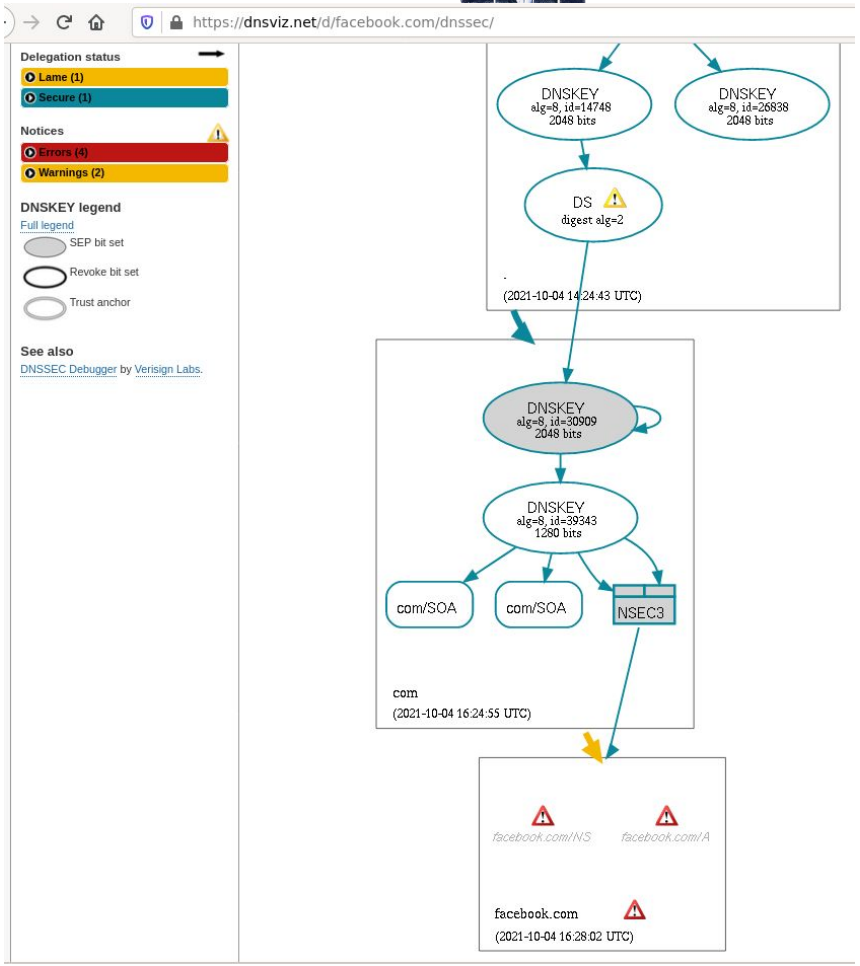
Comment Facebook, Insta et WhatsApp ont pu tomber ?
Cloudflare (qui fournit un CDN très utilisé), a écrit un article complet qui détaille ce qui s'est passé hier soir.
blog.cloudflare.com/october-2021-f...

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."

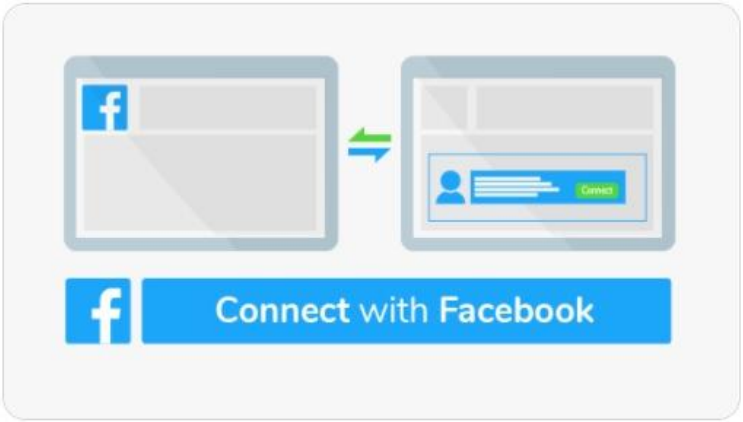
Instagram.com is flashing a 5xx Server Error message, while the Facebook site merely tells us that something went wrong. The problem also appears to be affecting its virtual reality arm, Oculus. Users can load games they already have installed and the browser works, but social features or installing 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.

Capture d'écran TheVerge [4/10/21 20h52]

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.

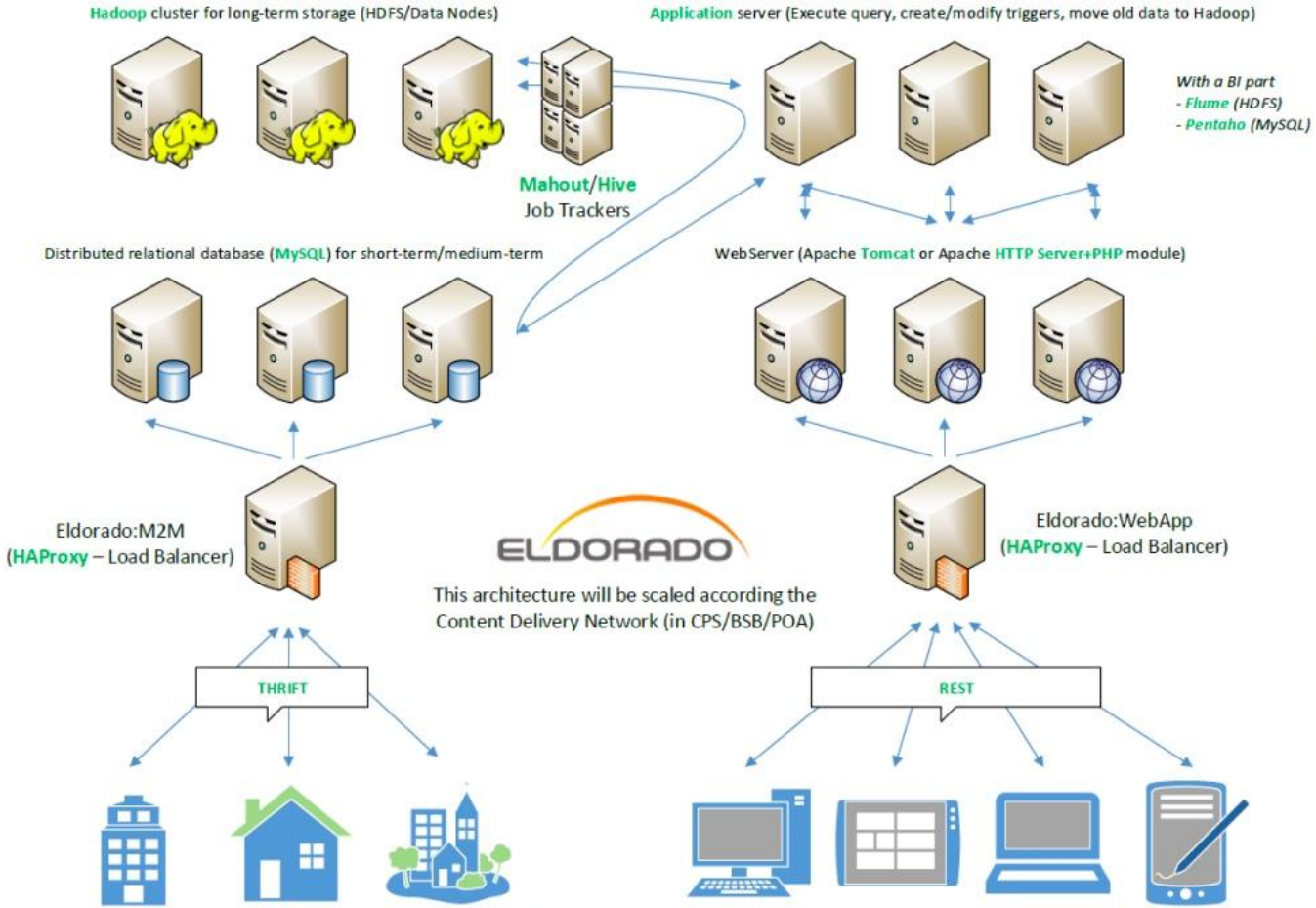
1:51 PM · 10/4/21 · Twitter for iPhone

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!

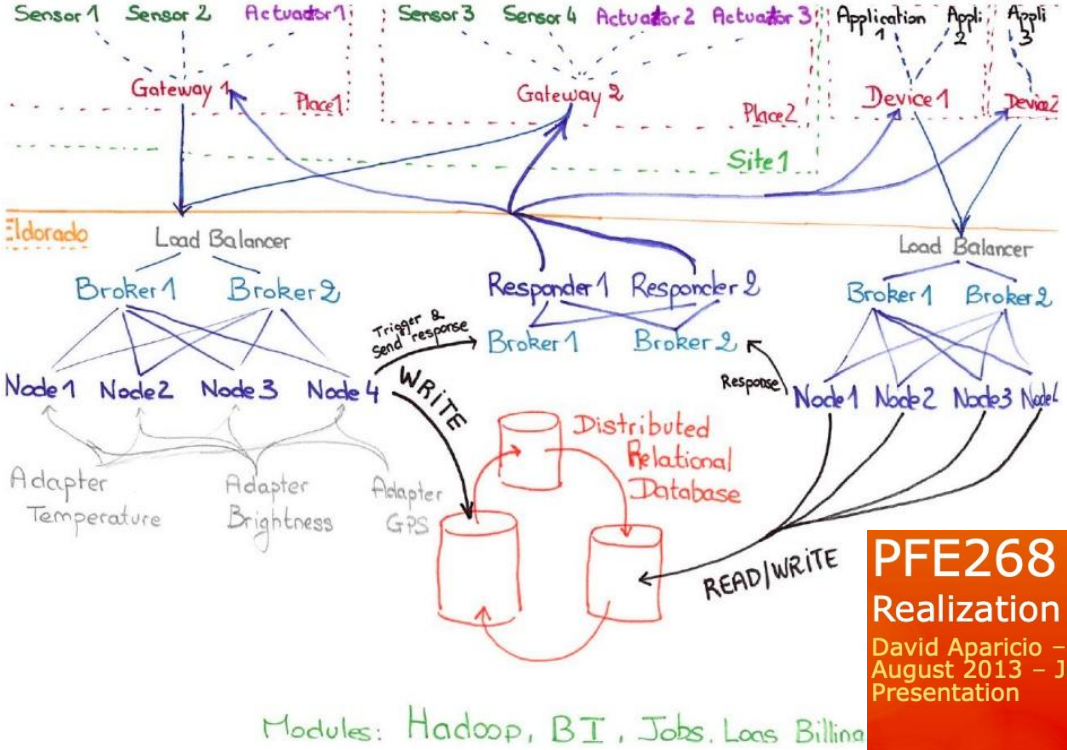
1:07 PM · 10/4/21 · Twitter Web App

Channels

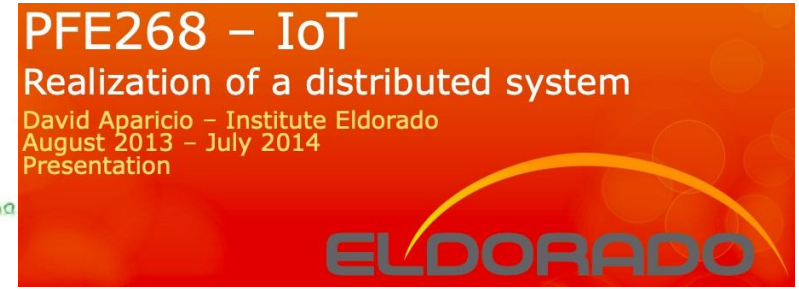


Capture d'écran
PFE268 (2014)

Entrypoint / Exitpoint (Separation of concerns)



Capture d'écran PFE268 (2014)



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 (Iot/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)

NewsBlur

Photo by Chris Karidis on Unsplash

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
XXXXXXFTHISGUYXXXXXXX 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
twitch-leaks-part-one	125.89 GiB	Normal
twitch-payouts	4.88 GiB	Normal
3rdparty.zip	15.1 KiB	Normal
abuse.zip	3.9 MiB	Normal
admin-services.zip	37.2 MiB	Normal
ads.zip	1.14 GiB	Normal
ags-sonic.zip	544.8 MiB	Normal
amzn.zip	44.6 MiB	Normal
andaries.zip	22.1 KiB	Normal
archive.zip	73.2 MiB	Normal
astith.zip	810.3 KiB	Normal
availability.zip	239.0 MiB	Normal
awsi.zip	164.4 MiB	Normal
beefcake.zip	5.8 MiB	Normal
benherr.zip	3.9 MiB	Normal
blade-legacy.zip	2.67 GiB	Normal
bobbcarp.zip	382.4 KiB	Normal
bootcamp.zip	33.9 MiB	Normal

Capture d'écran : [Twitch confirms hack after source code and creator payout data leaks online]

Avoid HDD

Hype Driven Development
ou
face au code du monde réel

Quentin ADAM

CEO @ Clever Cloud
@waxzce on twitter

🎯 2018 - Hype Driven Development - Quentin Adam

Conseils

Hype-driven development
CI/CD
DevSecOps: Tests automatique de penétration (pentest) sur des admin:admin, no password etc..
Isolation de la configuration DEV // PROD (Différent Jenkins ou Vault, Approbation manuelle)

Blast Effect

Photo by Chris Karidis on Unsplash

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

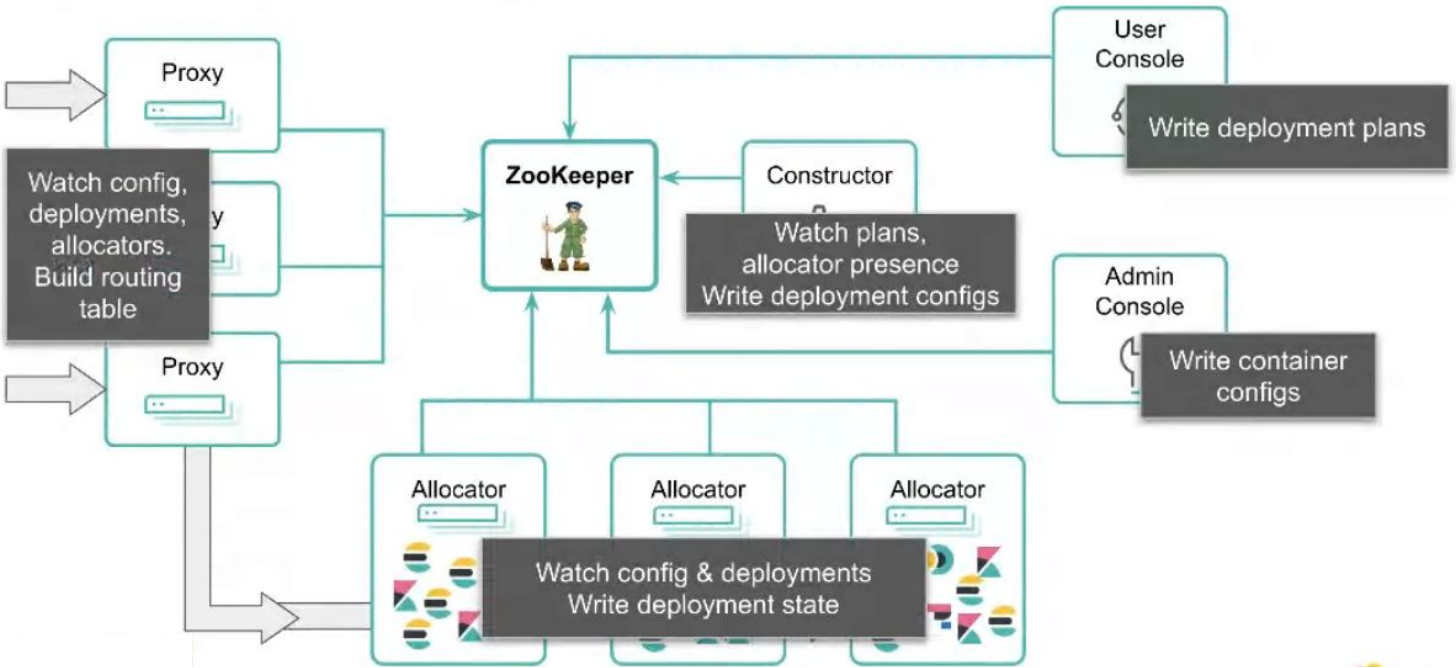


Schéma issu du meetup Toulouse JUG: War Story, comment les pauses du GC ont pété la prod (Sylvain Wallez)

Conseils

Identifier les SPOF (Point de défaillance unique)
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 (Cloudfare Waiting Room)
Chaos Monkey / Analyse des effets de bord

Same JVM, Shoot again

Photo by Chris Karidis on Unsplash

Les limites de la technologie

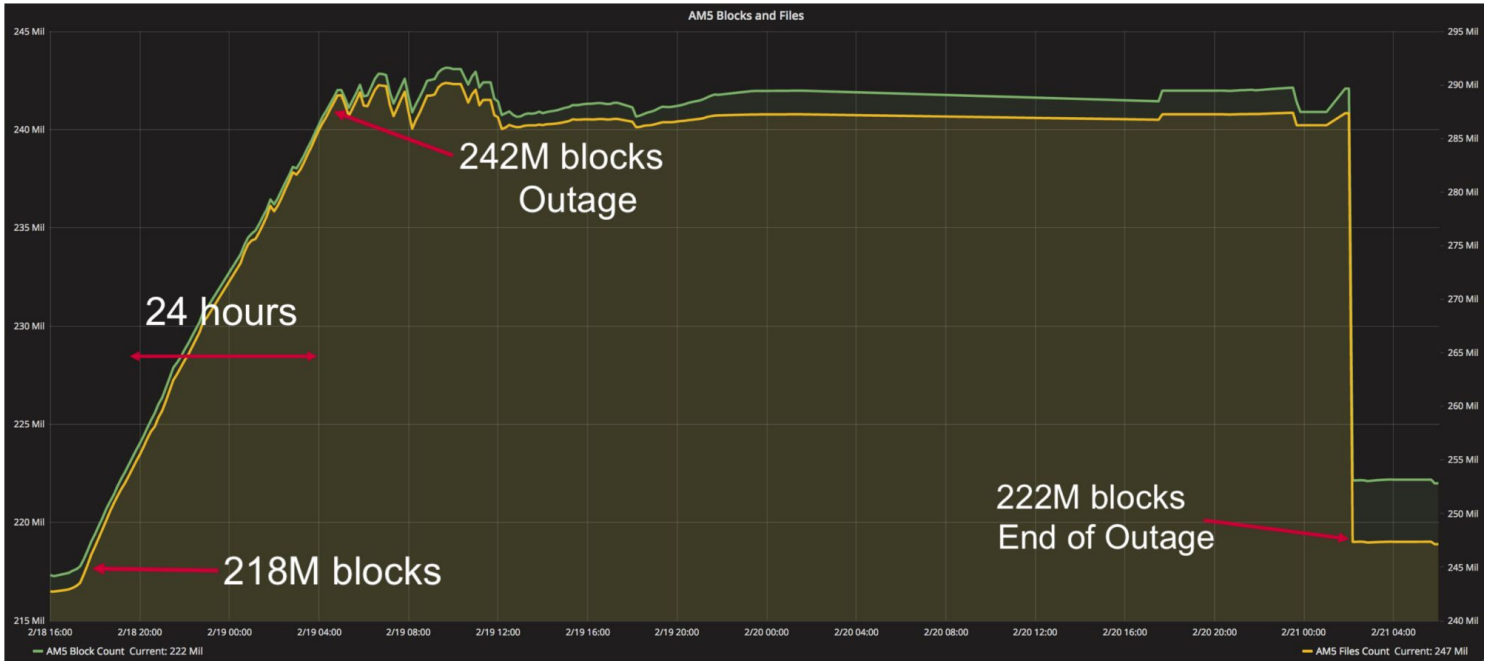


Schéma extrait de Medium : [+40PB per year — The challenge of data growth at Criteo]
Hadoop sous pression Retour sur une année d'exploitation à Criteo (Rémy Saissy)

Conseils

Tests de performance
Monitoring des KPI OS
Observabilité / Sondes applicatives
Serveurs de délestage (backup) pour les applications critiques

Foxstuck

Photo by Chris Karidis on Unsplash

🔥 Fox

🎯 Foxstuck: Firefox browser bug boots legions of users offline (The Register)

network.http.http3.enabled: false

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

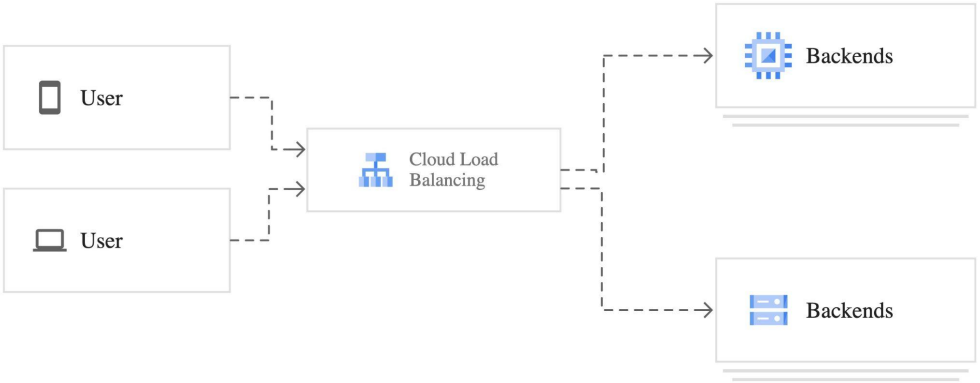
Product: Core ▾ 2022-01-13 00:18 PST = CET 8h18
Component: Networking ▾
Platform: Desktop All
Type: defect
Priority: Not set Severity: --

▾ Tracking

Status: VERIFIED DUPLICATE of ~~bug 1749910~~

▸ People (Reporter: heftig, Unassigned)

▸ Details



Mozilla Bugzilla #1749908

[Update] - Mercredi 2 Février 2022

mozilla HACKS

Download Firefox

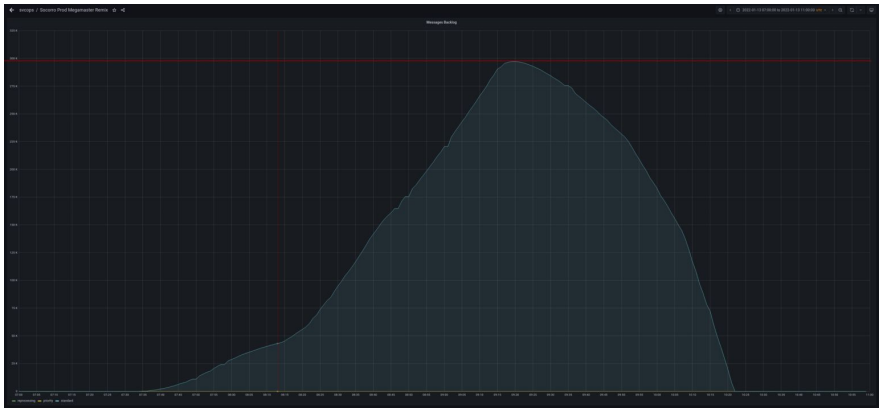
Search Mozilla Hacks

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)

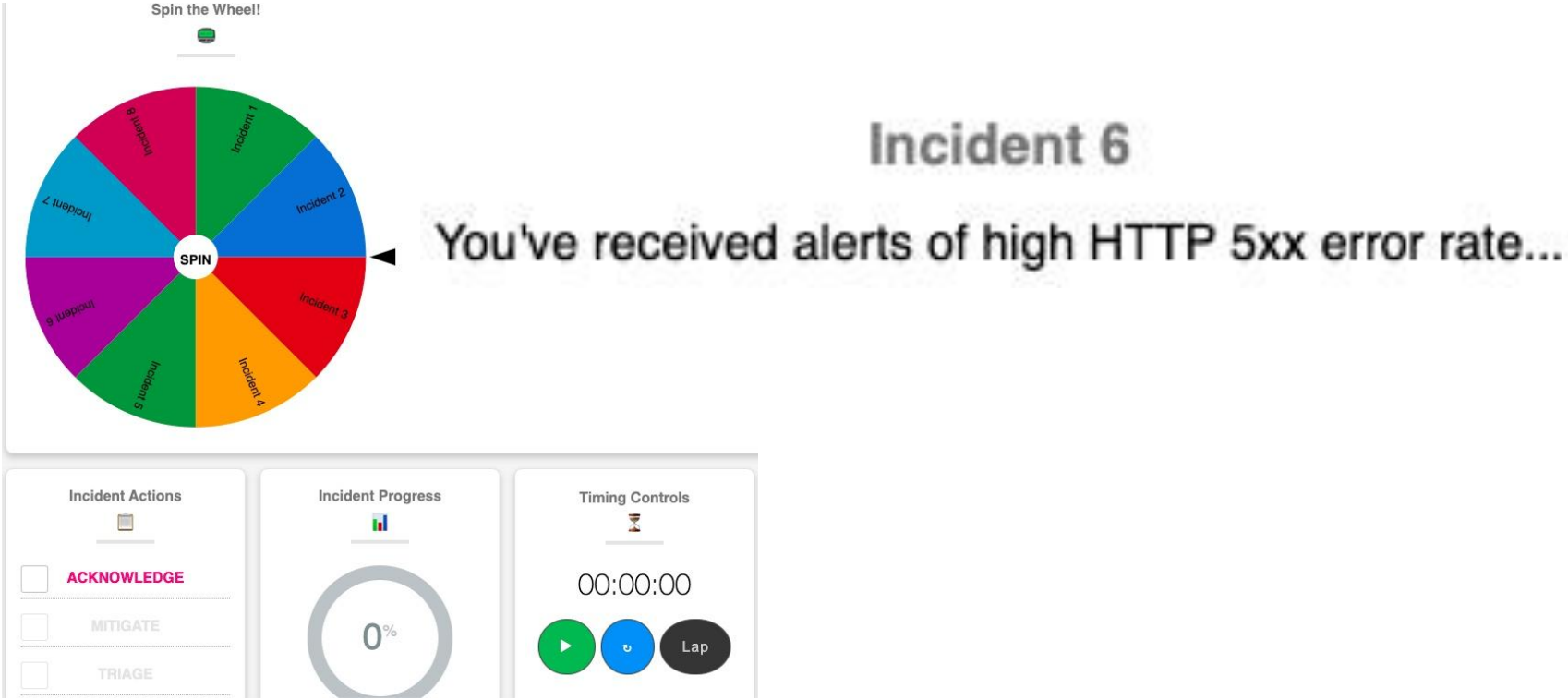
Conclusion

Photo by Anthony Tan on Unsplash

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



🎯 Capture d'écran de la "Roue de la malchance": https://dastergon.gr/wheel-of-misfortune/

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-mor | hacktoberfest

Readme

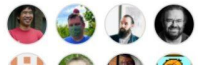
Releases

No releases published

Packages

No packages published

Contributors 86



Not Secure | danluu.com/postmortem-lessons/

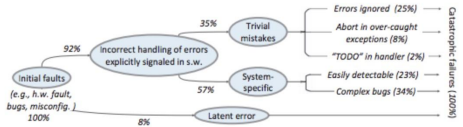
Reading postmortems

I love reading postmortems. They're educational, but unlike most educational docs, they tell an entertaining story. I've spent a decent chunk of time reading postmortems at both Google and Microsoft. I haven't done any kind of formal analysis on the most common causes of bad failures (yet), but there are a handful of postmortem patterns that I keep seeing over and over again.

Error Handling

Proper error handling code is hard. Bugs in error handling code are a major cause of *bad* problems. This means that the probability of having sequential bugs, where an error causes buggy error handling code to run, isn't just the independent probabilities of the individual errors multiplied. It's common to have cascading failures cause a serious outage. There's a sense in which this is obvious -- error handling is generally regarded as being hard. If I mention this to people they'll tell me how obvious it is that a disproportionate number of serious postmortems come out of bad error handling and cascading failures where errors are repeatedly not handled correctly. But despite this being "obvious", it's not so obvious that sufficient test and static analysis effort are devoted to making sure that error handling works.

For more on this, Ding Yuan et al. have a great paper and talk: Simple Testing Can Prevent Most Critical Failures: An Analysis of Production Failures in Distributed Data-Intensive Systems. The paper is basically what it says on the tin. The authors define a critical failure as something that can take down a whole cluster or cause data corruption, and then look at a couple hundred bugs in Cassandra, HBase, HDFS, MapReduce, and Redis, to find 48 critical failures. They then look at the causes of those failures and find that most bugs were due to bad error handling. 92% of those failures are actually from errors that are handled incorrectly.



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

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
Mozilla Firefox / Google Cloud, HTTP3 impact https://hacks.mozilla.org/2022/02/	13/01/2022

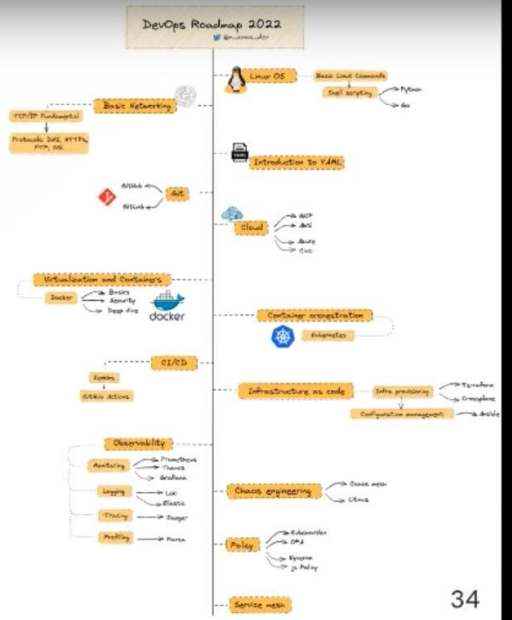
Pour aller plus loin

[GDG Cloud Nantes] SRE ! SRE partout ! par Denis Germain - CI/CD Week with Google Cloud

Quelles compétences ?

- Linux & les bases en réseau
- 1 langage & git
- 1 cloud provider

Padok - De dev à SRE / Reddit - "go into DevOps" / Roadmap to DevOps / Tweet Anas Khan



34

48:01 / 59:37

SRE ! SRE partout ! par Denis Germain

Voulez-vous travailler avec David  ?

Voici 3 offres dans l'équipe GIS :

IT Technical Leader

Développeur Python

Manager
Database Opensource

Dans les autres équipes :

Software Engineer Python
Object Storage

Senior C/C++
Software Engineer
Public Cloud

Développeur Python
Storage

careers.ovhcloud.com

Merci 🥳

J'ai besoin de vos retours
https://s.42l.fr/devoxxcastor

Lien des slides dans les commentaires