RETOUR D'EXPÉRIENCE

La sécurité dès la conception du projet

David Aparicio

SophiaConf
Lundi 27 Juin 2022, 18h

Cap d'Antibes (by Anthony Salerno)
The pictures are from Unsplash

@dadideo

David Aparicio

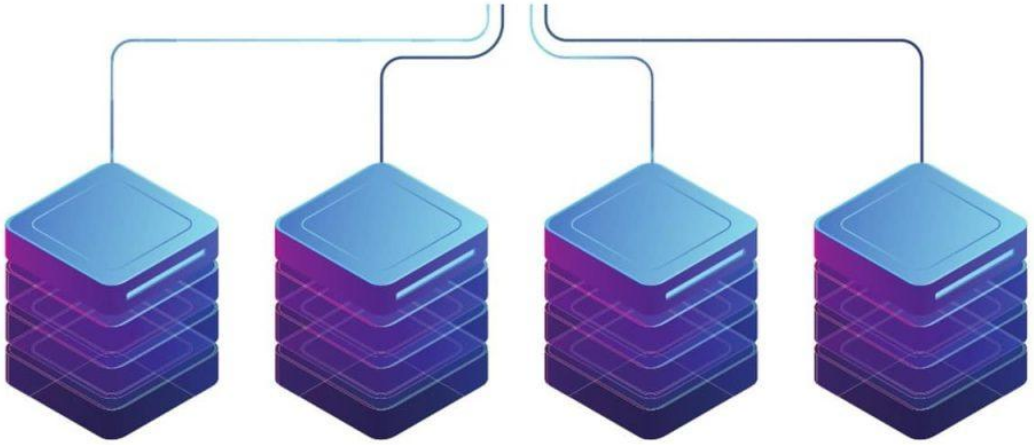
15/ DD INSA de Lyon / UNICAMP (Brésil)

Facebook Open Academy / MIT AppInventor

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

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

OVHcloud



Café de la Bourse

30 Datacenters

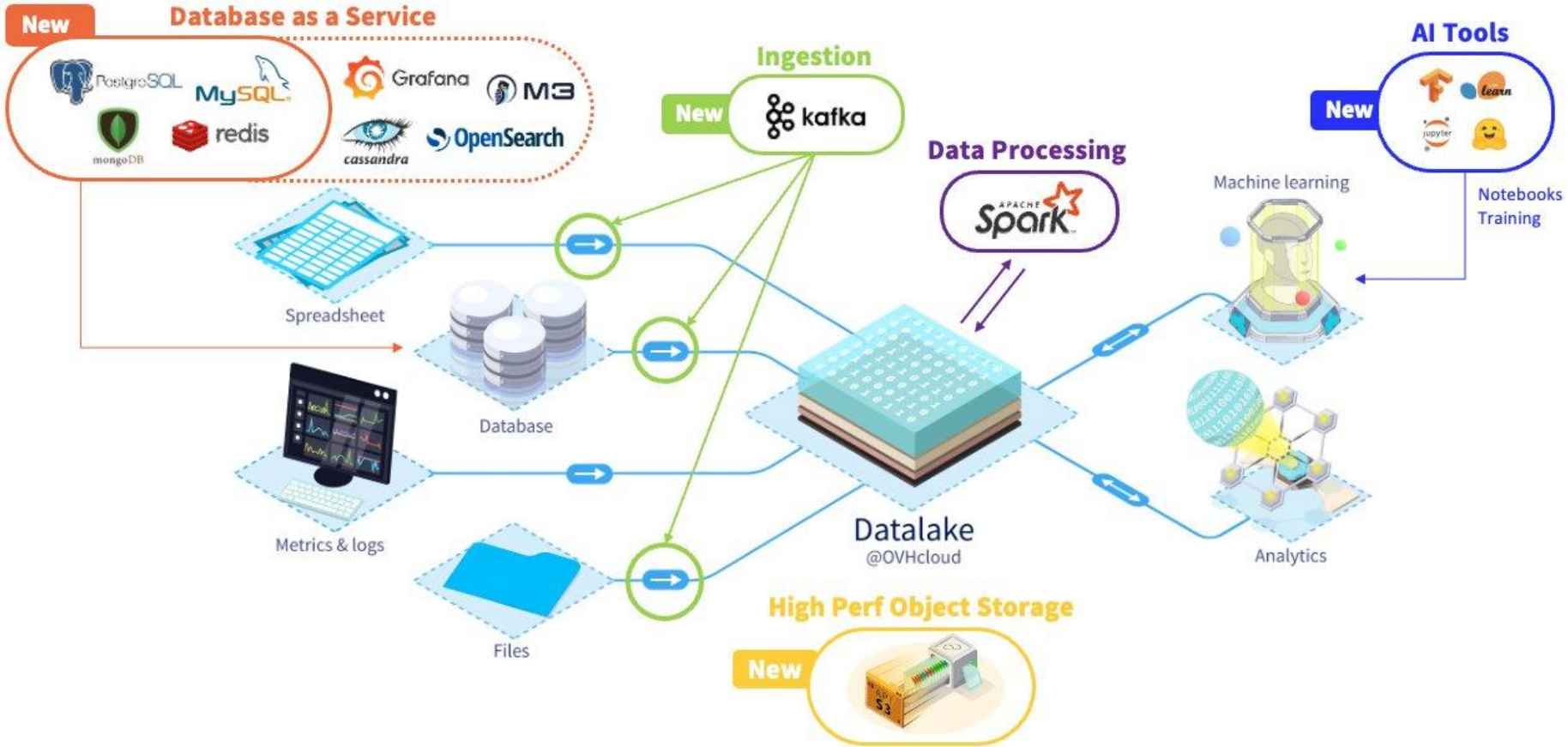
gaia-x

SecNumCloud

Depuis Déc 2020

GIS-DATA

@dadideo



careers.ovhcloud.com

Agenda

Introduction

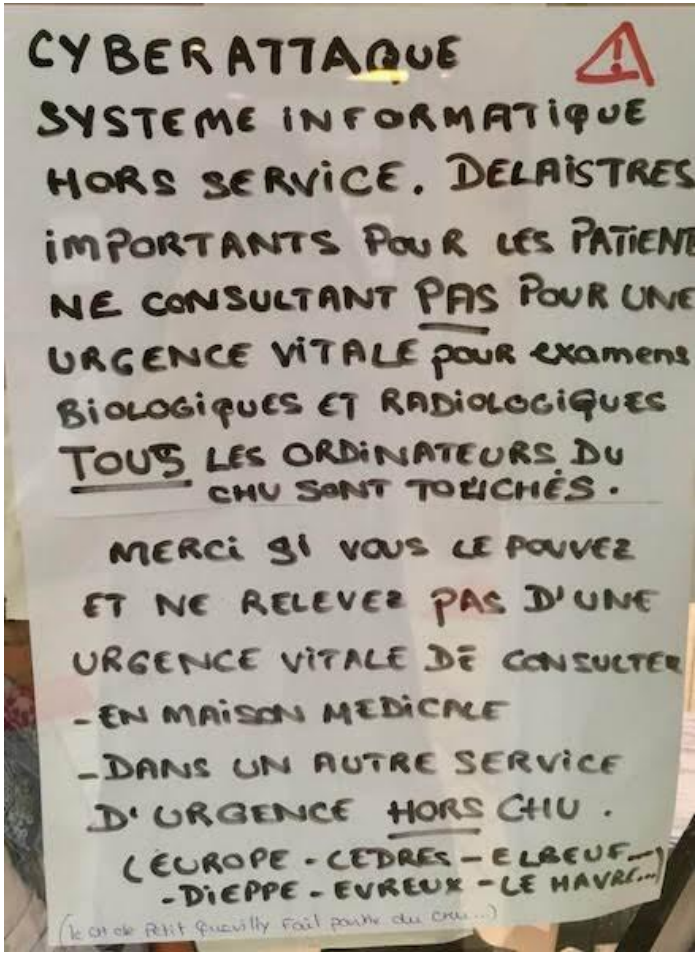
Retour d'expérience

Conseils

Conclusion

Introduction

Pourquoi ce talk ?



Thread @zigazou

Dès la Conception !!

Y a-t-il un pilote à jour dans l'avion ?

En 2015, les autorités états-uniennes de l'aviation alertaient les compagnies aériennes : le Boeing 787 Dreamliner devait être redémarré tous les 248 jours pour contourner un bogue pouvant entraîner une coupure de courant généralisée dont on peut imaginer les conséquences en vol. Cette fois, elles ont annoncé qu'il faut éteindre et rallumer ces mêmes avions tous les 51 jours pour éviter des problèmes informatiques catastrophiques en raison d'une mémoire saturée de données sinon. Mesdames et Messieurs, veuillez regagner vos places et attacher vos ceintures de sécurité, nous allons bientôt rebouter !

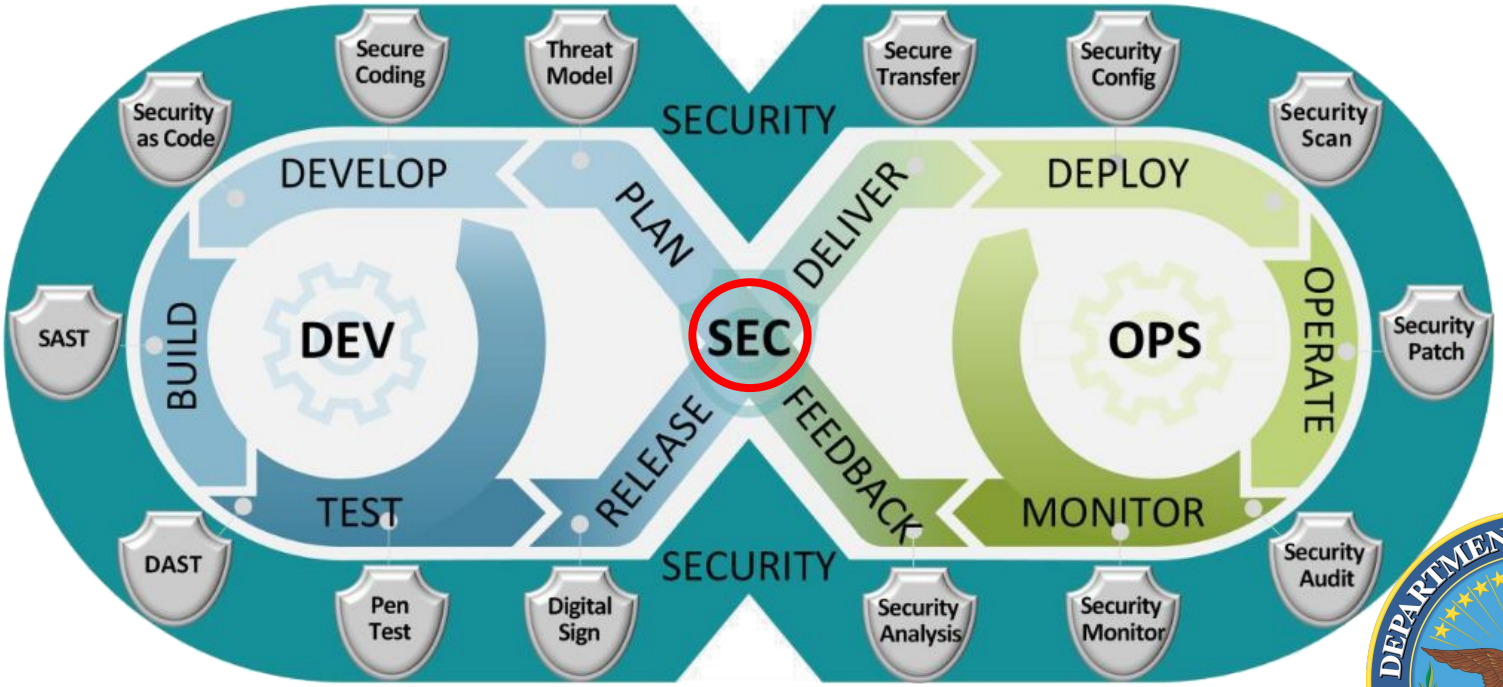
Octobre 2020, Le Virus Informatique n°44 (papier/en ligne)

Sécurité dès la conception

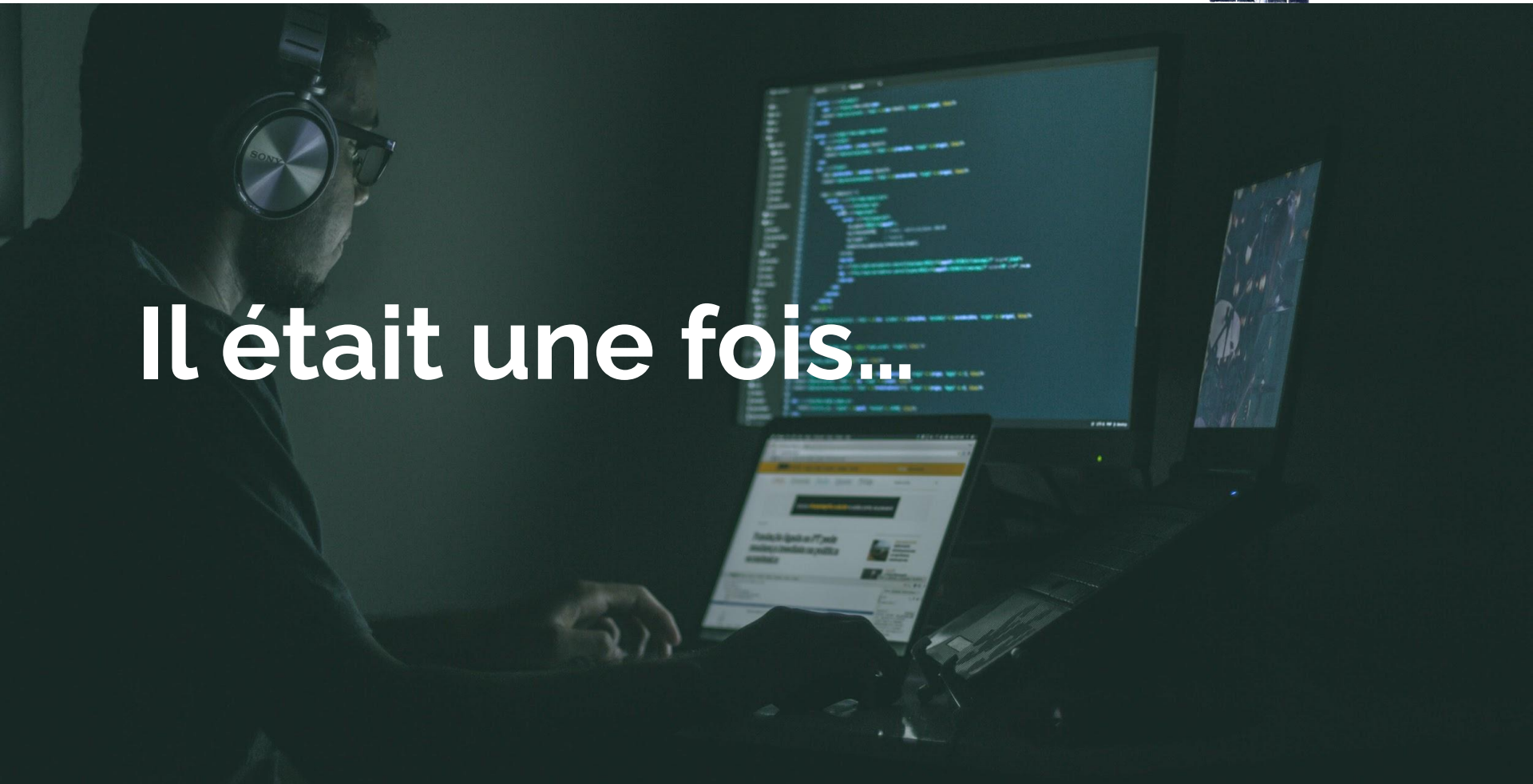
Du domaine du **Génie Logiciel**
Souvent associé à **Privacy By Design**
Considérer la sécurité comme une **partie intégrante**
Conception d'architecture **robuste**
Résistant aux attaques **bien connues**
Utilisant des techniques **réutilisables**
Minimiser l'impact **en prévision** des vulnérabilités

Exigences dans de **multiples domaines** (auth., intégrité, confidentialité, etc..,)
Même lorsque le système est attaqué
Préserver l'architecture pendant l'**évolution du logiciel**
Mise en oeuvre durant tout le **cycle de vie**, jusqu'à la fin du support, et donc une date de **décommissionnement**

Shift-left Security

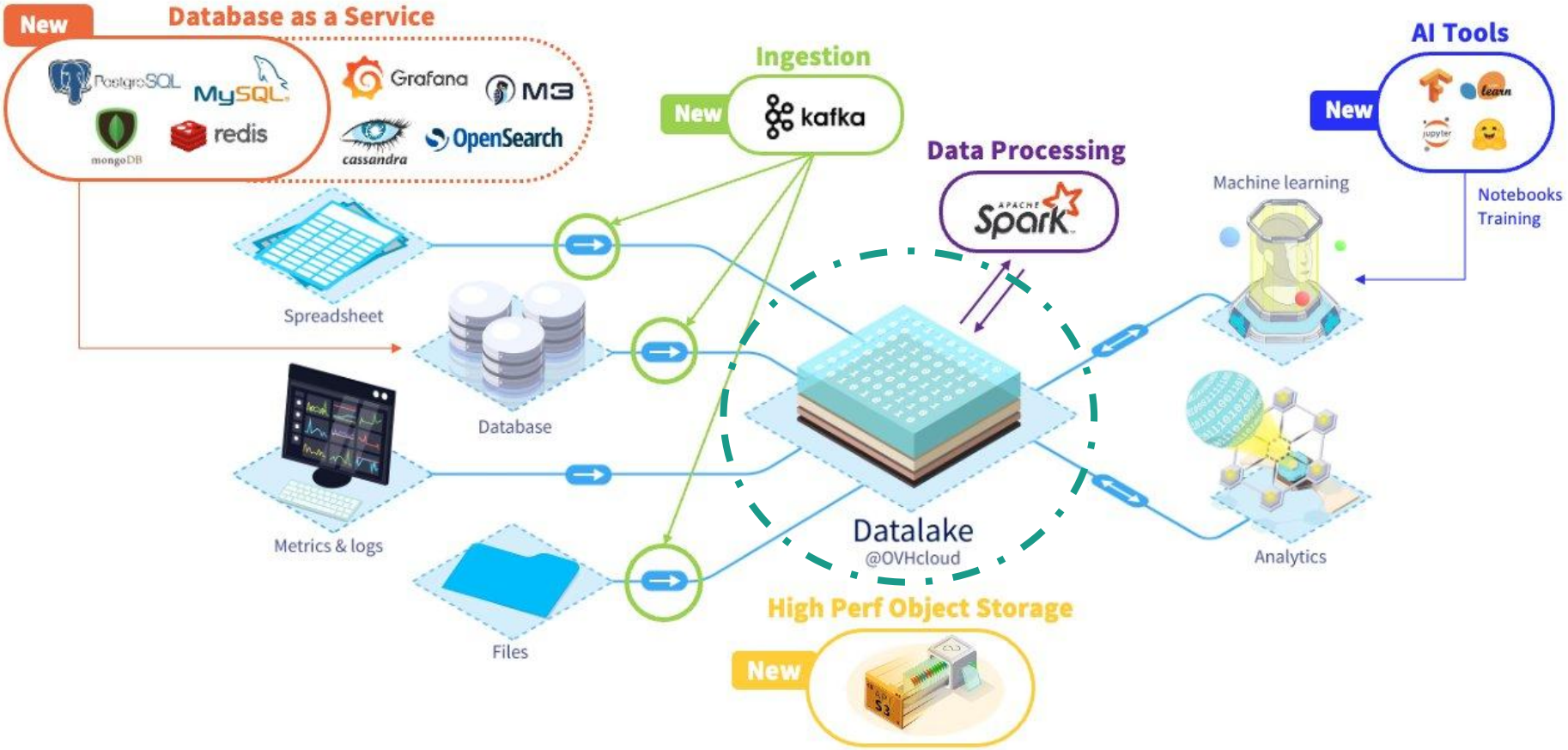


dodcio.defense.gov



Il était une fois...

Un Datalake


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

Un ticket

En tant qu'

utilisateur ou administrateur du Datalake

Je veux

un service toujours disponible, avec de la redondance (SLO/SLA)

Pour cela

Il faut sauvegarder régulièrement la configuration & la base de données de Kerberos
Car c'est un des SPOF (Point de défaillance unique) identifié de l'infrastructure

Un ticket

En tant qu'

utilisateur ou administrateur du Datalake

Je veux

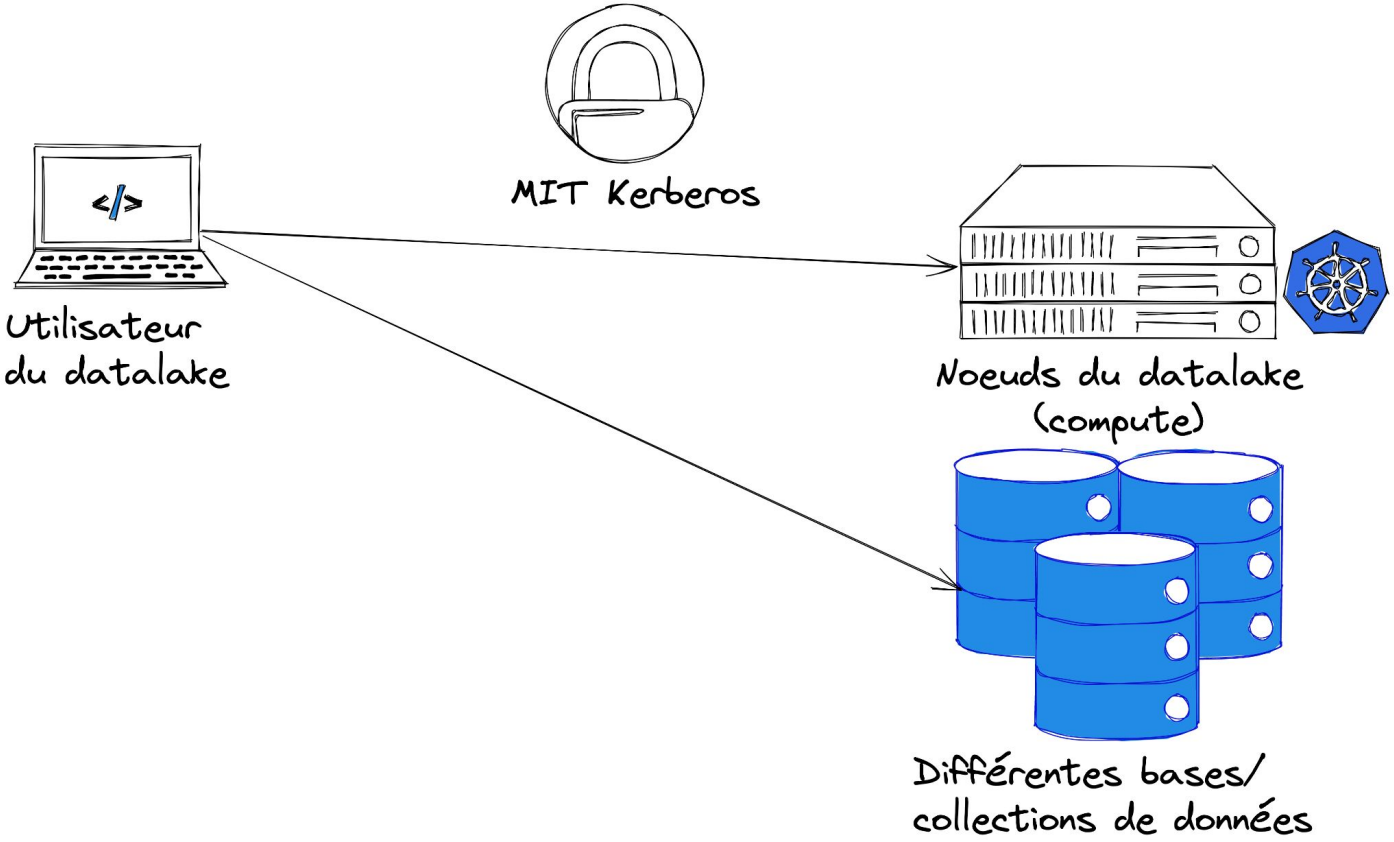
un service toujours disponible, avec de la redondance (SLO/SLA)

Pour cela

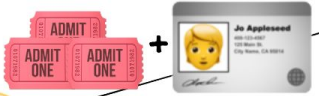
Il faut sauvegarder régulièrement la configuration & la base de données de Kerberos
Car c'est un des SPOF (Point de défaillance unique) identifié de l'infrastructure

En effet, pas de ressources dispo pour rendre Kerberos HA (Haute disponibilité)

Kerberos Kézako?



SSO

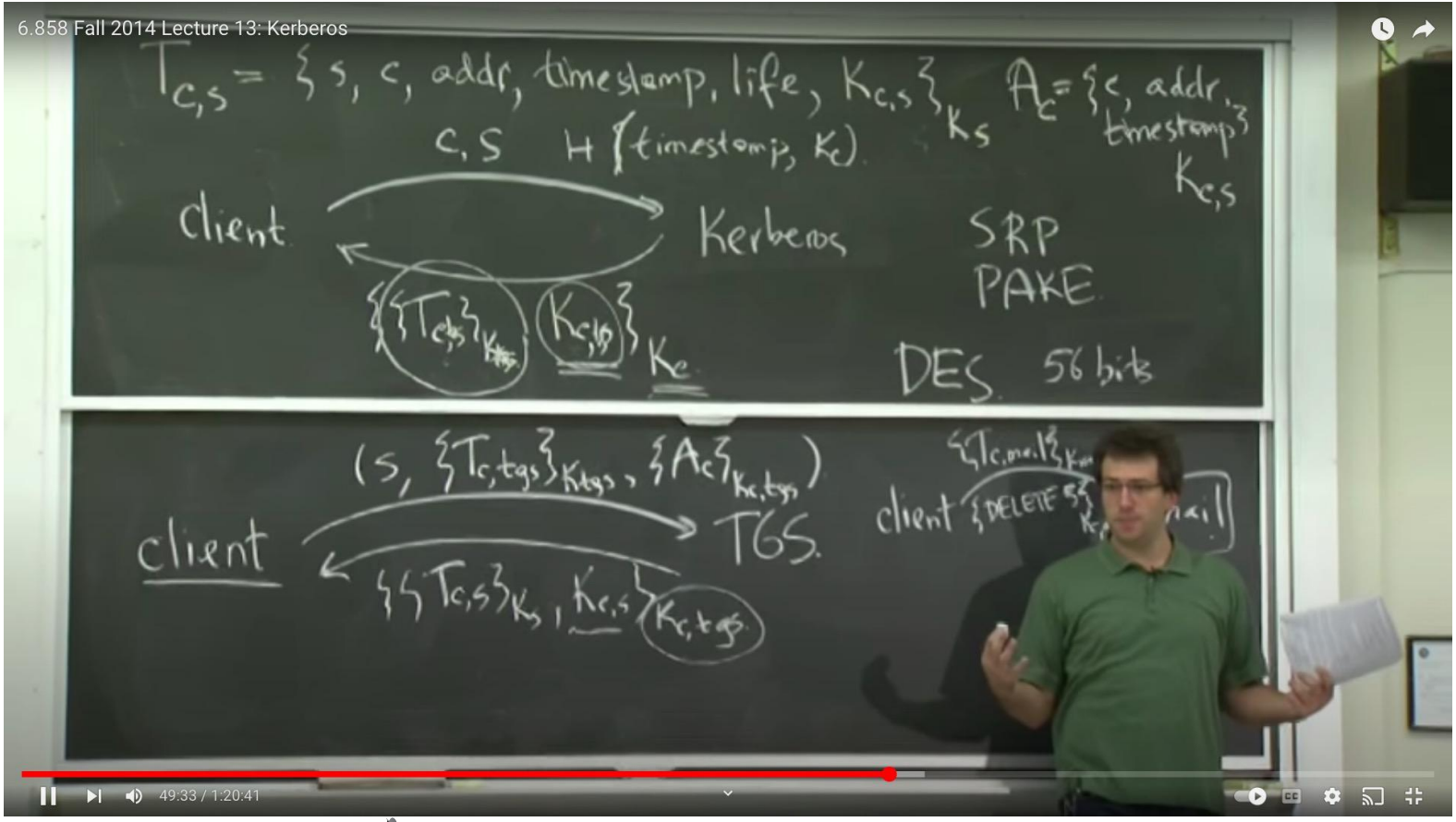


Guichet d'entrée
du parc
MR Kerberos

Utilisateurs
du parc d'attractions

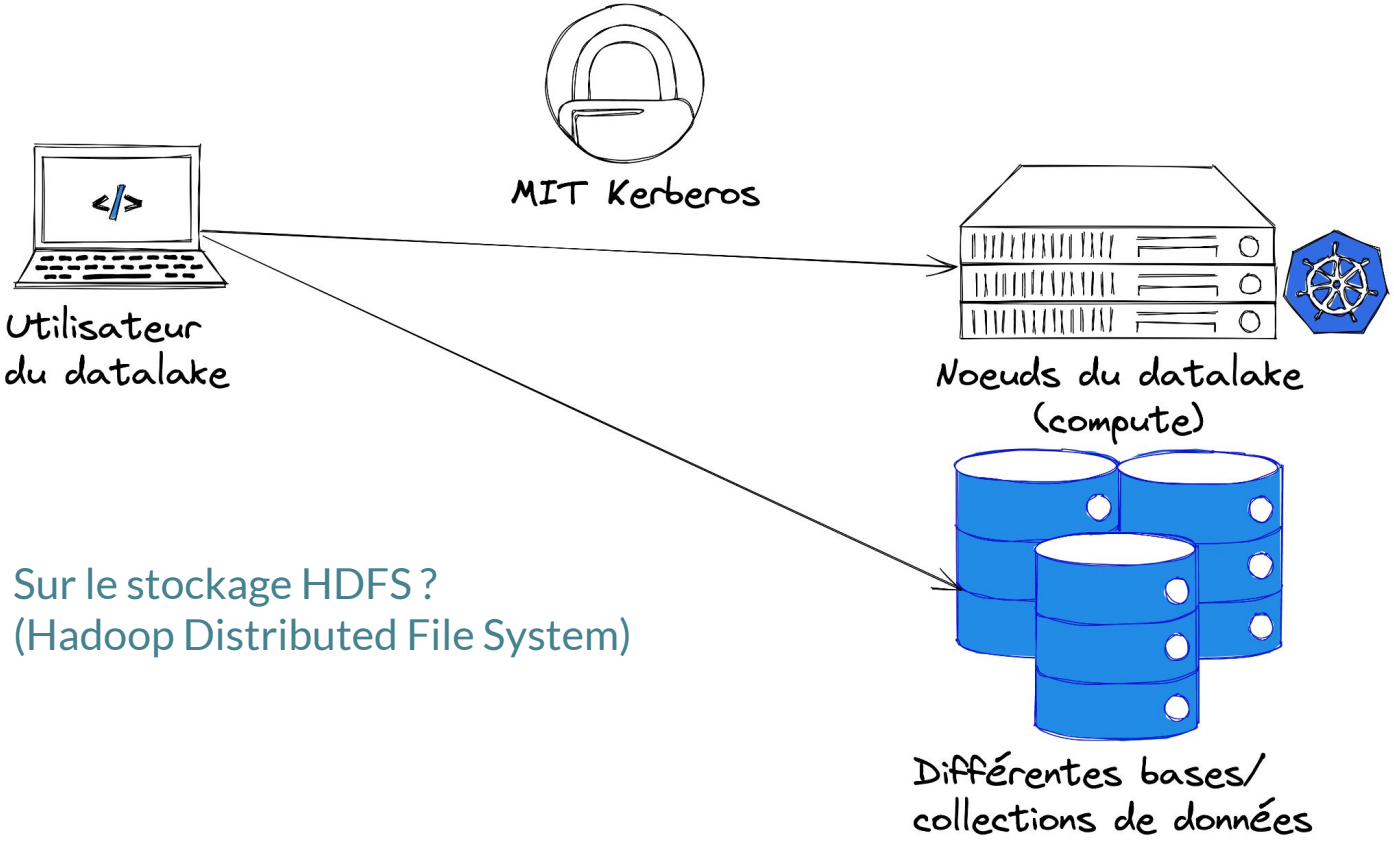
Différents manèges
(autorisés selon
son âge/ses droits)

Pour aller plus loin



6.858 Fall 2014 Lecture 13: Kerberos

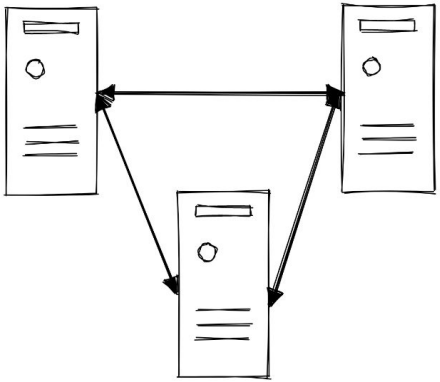
Où stocker le backup ?



Sur le stockage HDFS ?
(Hadoop Distributed File System)

Où stocker le backup ?

Control Plane
(Masters)

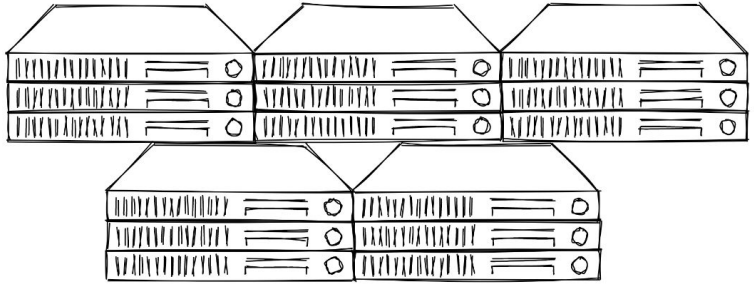


API
Orchestrator

Metadata

Sur les workers
Ou les masters ?

Data Plane
(Workers)



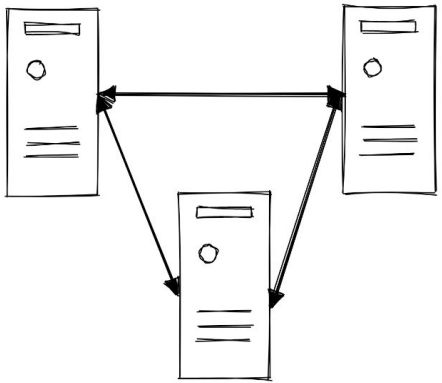
Services

Data

Datalake

SSOT
(source unique de vérité)

Control Plane
(Masters)



API
Orchestrator

Metadata

Sur les masters, avec le déployeur (Puppet Master)

Google

G Search

Searched for ssh accept automatically RSA key finger

3:29 PM • • Details

G Search

Searched for how accept ssh at the first connection

3:29 PM • • Details

askubuntu.com/questions/123072/ssh-automatically-accept-keys

StackExchange   Search on Ask Ubuntu...   Log in

Home

PUBLIC

Questions

Tags

Users

Companies

Unanswered

TEAMS

Stack Overflow for Teams – Start collaborating and sharing organizational knowledge.

Free

Create a free Team

Why Teams?

7 Answers   Sorted by: Highest score (default)

340

Use the StrictHostKeyChecking option, for example:

```
ssh -oStrictHostKeyChecking=no $h uptime
```

This option can also be added to ~/.ssh/config, e.g.:

```
Host somehost
    Hostname 10.0.0.1
    StrictHostKeyChecking no
```

Note that when the host keys have changed, you'll get a warning, even with this option:

```
$ ssh -oStrictHostKeyChecking=no somehost uptime
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
@    WARNING: REMOTE HOST IDENTIFICATION HAS CHANGED!     @
@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@@
IT IS POSSIBLE THAT SOMEONE IS DOING SOMETHING NASTY!
Someone could be eavesdropping on you right now (man-in-the-middle attack)!
It is also possible that a host key has just been changed.
The fingerprint for the RSA key sent by the remote host is
31:6f:2a:d5:76:c3:1e:74:f7:73:2f:96:16:12:e0:d8.
Please contact your system administrator.
Add correct host key in /home/peter/.ssh/known_hosts to get rid of this message.
Offending RSA key in /home/peter/.ssh/known_hosts:24
  remove with: ssh-keygen -f "/home/peter/.ssh/known_hosts" -R 10.0.0.1
Password authentication is disabled to avoid man-in-the-middle attacks.
Keyboard-interactive authentication is disabled to avoid man-in-the-middle attacks.
ash: uptime: not found
```

If your hosts are not often reinstalled, you could make this less secure (but more convenient for often-changing host keys) with the `-oUserKnownHostsFile=/dev/null` option. This discards all received host keys so it'll never generate the warning.

Pas copier-coller depuis StackOverFlow

98% snippets sécu/crypto sont insecures

🎯 Fisher et al., 2017; Nadi et al., 2016; Das et al., 2014, Prevent cryptographic pitfalls by design

Prendre du recul

Feb 11, 2018

Search
Searched for ssh-keyscan multiple hosts
4:01 PM • • Details

Search
Searched for ssh-keyscan examples
3:58 PM • • Details

Search
Searched for ssh test connection
3:57 PM • • Details

Search
Searched for ssh-keyscan
3:43 PM • • Details

Search
Searched for ssh accept automatically RSA key fingerprint
3:29 PM • • Details

Search
Searched for how accept ssh at the first connection
3:29 PM • • Details

147

You can use the following command to add the fingerprint for a server to your known_hosts

```
ssh-keyscan -H <ip-address> >> ~/.ssh/known_hosts
ssh-keyscan -H <hostname> >> ~/.ssh/known_hosts
```

NOTE: Replace < ip-address > and < hostname > with the IP and dns name of the server you want to add.

The only issue with this is that you will end up with some servers in your known_hosts twice. It's not really a big deal, just mentioning. To ensure there are no duplicates, you could remove all the servers first by running the following first:

```
ssh-keygen -R <ip-address>
ssh-keygen -R <hostname>
```

So you could run:

```
for h in $SERVER_LIST; do
    ip=$(dig +search +short $h)
    ssh-keygen -R $h
    ssh-keygen -R $ip
    ssh-keyscan -H $ip >> ~/.ssh/known_hosts
    ssh-keyscan -H $h >> ~/.ssh/known_hosts
done
```

Paramétrisable

@dadideo

Customization

If needed, you can edit the following parameters: ...

```
# This configuration file is managed by Puppet.
# Documentation:                                confluence

#--- DEFAULT PARAMETERS ---
BASE_DIR="/opt/ama
BACKUP_LOCAL_DIR="${BASE_DIR}/backup "
LOG_DIR="${BASE_DIR}/log "
LOG="${LOG_DIR}/ama                    .log"
KERBEROS_DIR="/var/kerberos"
KERBEROS_TMPDB="       ker .db"
KERBEROS_TMBVS="krb-version.tmp"
BACKUP_APPLICATIVEUSER=
BACKUP_APPLICATIVEHOME=
    KEYTAB_DIR=
BACKUP_HOST="$(uname -n)"
CONSUL_BINARY=
SSHKEY_KNOWNHOSTS="${BACKUP_APPLICATIVEHOME}/.ssh/known_hosts"
SSHKEY_PUBKEY="${BACKUP_APPLICATIVEHOME}/.ssh/id_rsa"
#--- CUSTOMIZED PARAMETERS ---
BACKUP_INTERVAL_SECS="86400"
BACKUP_RETENTION_DAYS="31"
BACKUP_REMOTE_DESTINATION="${BACKUP_APPLICATIVEHOME}"
BACKUP_REMOTE_BACKUPS_LOCATION="${BACKUP_REMOTE_DESTINATION}/
```

Avec la mise en place d'une rotation des Sauvegardes pour Éviter la saturation Des masters

How backup/restore Kerberos

Created by David APARICIO (contractor), last modified by on Apr 10, 2019

[redacted] MAPR 5.2.0 MEP 3.0.1 REV4

Main documentation contributor: @David APARICIO (contractor)

Backup

The daemon is automatically deployed by Puppet, you can check its status on GMock with the following command

```
systemctl status -l [redacted]-backup
```

Customization

› If needed, you can edit the following parameters: ...

Done by Puppet, modify the Hieradata (could be found into the module file: templates/gmock/[redacted].conf.erb)

Restore (manual)

1. Optional (if Puppet is disabled):
   a. Move your .tar.gz backup (from one master) with scp to the GMock
      Remark: Only user that can do it with scp is [redacted], otherwise need to pass through the gateway
   b. Install the RPM package, if you stopped Puppet ("sudo yum install backup")
2. If Puppet is enabled, check on /opt/ /backup 😀
3. Launch this script

```
sudo /opt/[redacted]/bin/[redacted]-restore.sh <FULLPATH_ARCHIVE.tar.gz>
```

Chaos Monkey

updated an issue

[kerberos-backup] - Rsync mirroring breaks

Change By:

If a gmock is destroyed and re-created the previous authorized_keys file for krbbackup user is lost and, due to this, the synchronization between masters and gmock is not working properly (i.e. backups created before the destruction of gmock are not copied, whereas the new ones are correctly copied). This is generating a de-synchronization between masters and gmock and user can't understand it since in gmock some backups are present (new ones/useless instead of old ones).

Add Comment

Problèmes

- Cluster sans Kerberos (MapR ticket)
- Pas de 50/50 (épuisement)
- Temps de livraison (junior)
- Sécurité ?
- Accompagnement du Management

Conseils

Quelques bonnes pratiques

- Diminuer surface d'attaque (scratch, distroless)
- Principe de moindre privilège (!root)
- Défense en profondeur (bastion, traceability, siem)
- Détection de connexion, proposer/activer MFA
- Pas de configuration par défaut (K8s, MongoDB)
- Pas de secrets dans les Docker images ou les repositories Git (Vault, .gitignore)
- Pas de données sensibles dans les GUI (cf slide suivante)
- Ne pas afficher de stacktrace (pas debug | Fail securely)
- Ni de version/nom de framework
- Vérifier les entrées/sorties des clients/noeuds (injection/XSS)
- Faire des backups régulièrement et déconnectées du réseau
- Mettre à jour infra/docker images (CI/CD|GitOps)
- PaaS (BUILD/RUN) 🇪🇺 OVHcloud/CleverCloud

Attention au risque humain

ars TECHNICA BIZ & IT TECH SCIENCE POLICY CARS GAMING & CULTURE STO

ELON SPEAKS —

Russian tourist offered employee $1 million to cripple Tesla with malware

"This was a serious attack," Elon Musk says.

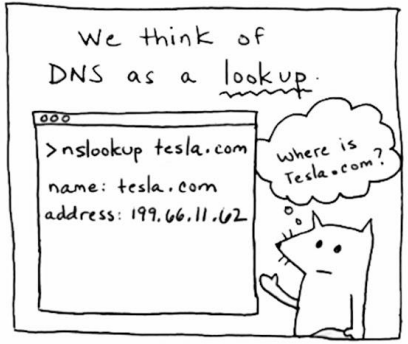
DAN GOODIN - 8/28/2020, 4:12 AM

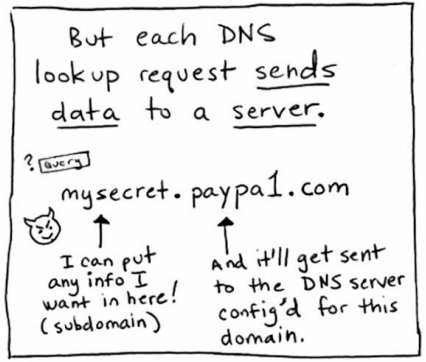
Enlarge

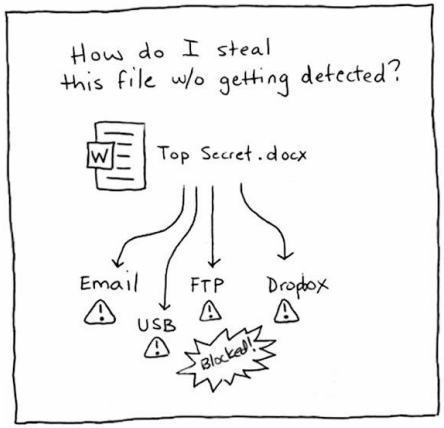
Ars Technica [EN]

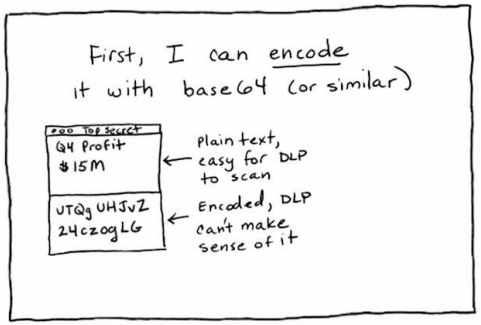
Attention au traffic sortant aussi !

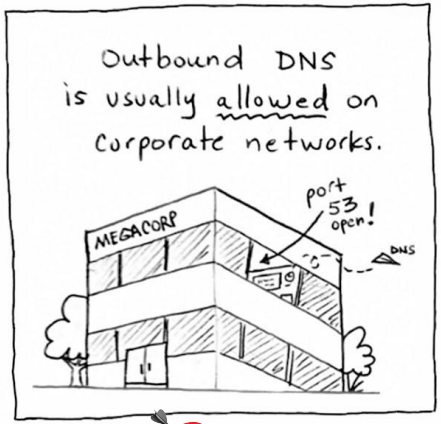
Introduction à DNSSEC

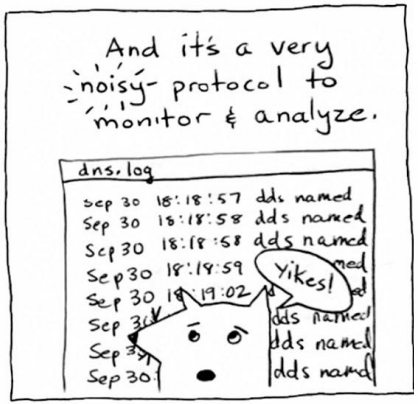


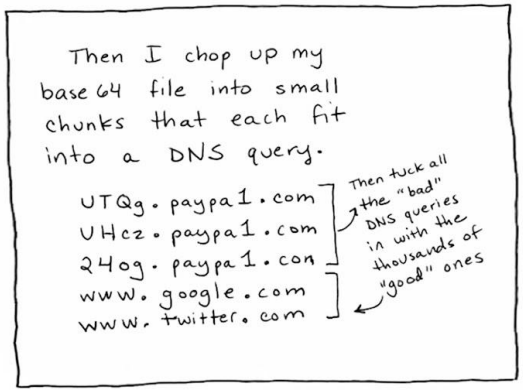


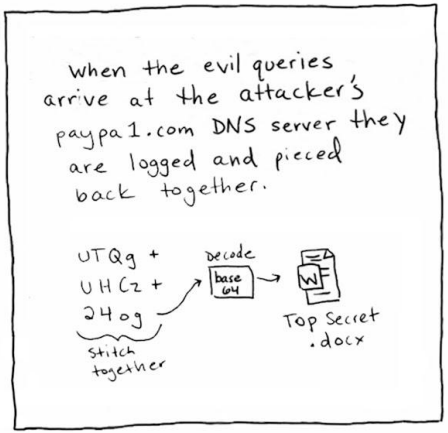












Exfiltration DNS @Rob Sobers

Ne pas afficher des données personnelles (PII)

Site d'Ameli.fr (numéro modifié pour illustrer)

CNIL - Donnée personnelle, Personally identifiable information (PII)

Pourquoi ?

2013	2017 (new, * from the community)	2021 (new, * from the survey)
A1 - Injection	A1 - Injection	A1 - Broken Access Control
A2 - Broken Authentication & Session Management	A2 - Broken Authentication	A2 - Cryptographic Failures
A3 - Cross-Site Scripting (XSS)	A3 - Sensitive Data Exposure	A3 - Injection
A4 - Insecure Direct Object References	A4 - XML External Entities (XXE)	A4 - Insecure Design
A5 - Security Misconfiguration	A5 - Broken Access Control [MERGED A4+A7]	A5 - Security Misconfiguration
A6 - Sensitive Data Exposure	A6 - Security Misconfiguration	A6 - Vulnerable and Outdated Components
A7 - Missing Function Level Access Control	A7 - Cross-Site Scripting (XSS)	A7 - Identification and Authentication Failures
A8 - Cross-Site Request Forgery (CSRF)	A8 - Insecure Deserialization *	A8 - Software and Data Integrity Failures
A9 - Using Components with Known Vulnerabilities	A9 - Using Components with Known Vulnerabilities	A9 - Security Logging and Monitoring Failures *
A10 - Unvalidated Redirects and Forwards	A10 - Insufficient Logging & Monitoring *	A10 - Server-Side Request Forgery (SSRF) *
OWASP TOP 10		

🎯 OWASP Top 10

Conclusion

TL;DR - The state of open source security 2019 report, at a glance

Open source adoption

- Growth in indexed packages, 2017 to 2018
  - Maven Central - 102%
  - PyPI - 40%
  - npm - 37%
  - NuGet - 26%
  - RubyGems - 5.6%
- npm reported 304 billion downloads for 2018
- 78% of vulnerabilities are found in indirect dependencies

Known vulnerabilities

- 88% growth in application vulnerabilities over two years
- In 2018, vulnerabilities for npm grew by 47%. Maven Central and PHP Packagist disclosures grew by 27% and 56% respectively
- In 2018, we tracked over 4 times more vulnerabilities found in RHEL, Debian and Ubuntu as compared to 2017

Known vulnerabilities in docker images

- Each of the top ten most popular default docker images contains at least 30 vulnerable system libraries
- 44% of scanned docker images can fix known vulnerabilities by updating their base image tag

Vulnerability identification

- 37% of open source developers don't implement any sort of security testing during CI and 54% of developers don't do any docker image security testings
- The median time from when a vulnerability was added to an open source package until it was fixed was over 2 years

Who's responsible for open source security?

- 81% of users feel developers are responsible for open source security
- 68% of users feel that developers should own the security responsibility of their docker container images
- Only three in ten open source maintainers consider themselves to have high security knowledge

Snyk stats

- In the second half of 2018 alone, Snyk opened more than 70,000 Pull Requests for its users to remediate vulnerabilities in their projects
- CVE/NVD and public vulnerability databases miss many vulnerabilities, only accounting for 60% of the vulnerabilities Snyk tracks
- In 2018 alone, 500 vulnerabilities were disclosed by Snyk's proprietary dedicated research team

The state of open source security – 2019

Rappelez-vous: Les hackers n'en ont rien à "faire"

- ❑ À propos du scope de votre projet
- ❑ Il est géré par une tierce partie / sous-traitant
- ❑ C'est un système ancien (Legacy)
- ❑ TPCM / " Touche pas ! C'est magique "
- ❑ C'est "trop critique pour être réparé"
- ❑ A propos de vos périodes de maintenance
- ❑ A propos de votre budget
- ❑ Vous l'avez toujours fait de cette façon
- ❑ À propos de votre date de mise en service
- ❑ Il s'agit seulement d'un pilote/PoC
- ❑ À propos des accords de non-divulgation
- ❑ Ce n'était pas une exigence dans le contrat
- ❑ C'est un système interne
- ❑ Il est vraiment difficile de modifier / changer
- ❑ Vous n'êtes pas sûr de savoir comment y remédier
- ❑ Il doit être remplacé
- ❑ C'est géré dans le Cloud
- ❑ À propos de votre inscription au registre des risques
- ❑ L'éditeur ne prend pas en charge cette configuration
- ❑ C'est une solution provisoire
- ❑ Il est conforme à [insérer la norme ici]
- ❑ Il est crypté sur disque
- ❑ Le rapport coût-bénéfice ne scale pas
- ❑ "Personne d'autre ne pouvait le comprendre"
- ❑ Vous ne pouvez pas expliquer le risque au "Business"
- ❑ Vous avez d'autres priorités
- ❑ Sur votre foi dans la compétence de vos utilisateurs internes
- ❑ Vous n'avez pas de justification commerciale
- ❑ Vous ne pouvez pas montrer le retour sur investissement
- ❑ Vous avez sous-traité ce risque
- ❑ C'était à la mode [insérer la technologie hype ici].
- ❑ De vos certifications

 @dadideo + Kiwicon 2009 / Hackers don't give a shit

Analogie

« Nul n’est censé ignorer la loi »

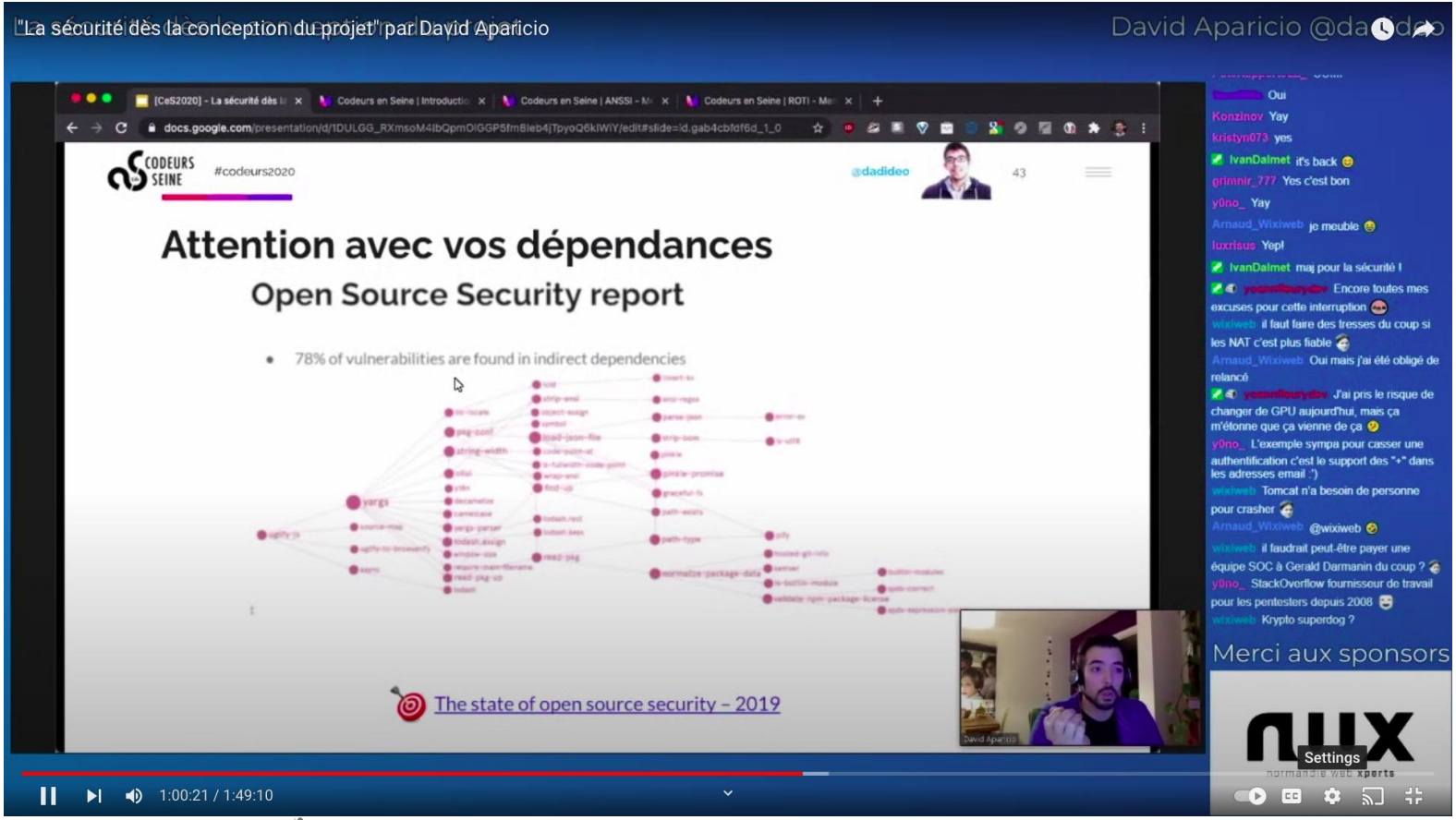
Ma devise

« Nul développeur n'est censé ignorer la sécurité »

🎯 Pour aller plus loin

- Sophia Security Camp 2019
- ANSSI (Atelier Sécurité Agile, Livre Sécurité au déploiement de conteneurs Docker)
- TV5 Monde Analyse d'Incident, ANSSI (SSTIC 2017)
- 10 leçons sur les 10 plus grosses fuites de données, de Adrien Pessu (JSC 2020)
- La Cryptographie en 55' chrono de m4dz (SnowCamp2020)
- Sécurité du Cloud, de Eric Briand (RemoteClazz 2020)
- La nuit tous les hackers sont gris (Fiction écrite par Vincent Hazard, 2019)

Pour aller plus loin



Twitch "Codeurs en Seine 2020" sur la sécurité

Merci pour votre attention !

👩‍🏫📢 N'oubliez pas de me donner votre avis sur cette session:

📃 https://s.42l.fr/sc22sec

👍 Lien des slides dans les commentaires

Bonus: Quelques outils DevSecOps

- Secure Coding
  - Linters, gosec, npm-audit, GitGuardian, 42Crunch
- Security as Code
  - Cilium (Network), gVisor/Kata (Sandbox), Istio/Traefik maesh (SSL)
- SAST / DAST / IAST
  - SonarQube, Gitlab SAST/GitHub, Clair/Anchore/Dagda (CVE)
- Pentest
  - Parrot/Kali, YesWeHack/Yogosha, Burp Suite/SuperTruder/ffuf, OWASP ZAP
- Digital signature / Secure Transfer
  - Notary, JFrog Artifactory
- Security Configuration, Security Scan
  - Argo+Vault, OpenSCAP
- Security Patching, Security Audit
  - Puppet, Chef, Ansible Playbook/AWX ou RedHat Tower
- Security Monitoring
  - Elastic Security, Falco, OVH Bastion
- Security Analysis
  - Saucs, AlienVault OTX