

Administration Linux avancée

PREVIOUSLY ON

GAME OF THRONES

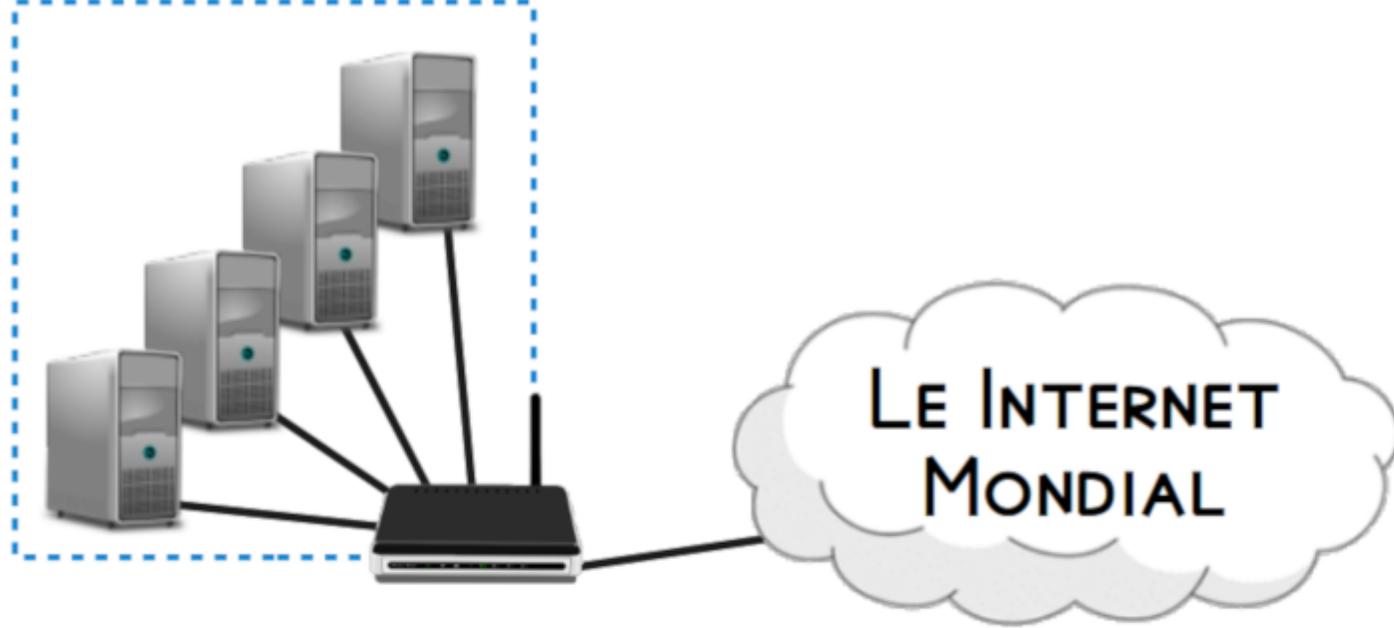
Recap'

- Installer une distribution
- Le gestionnaire de paquet
- Notions de réseau
- Notion de chiffrement
- Administrer à distance avec SSH
- Gérer des services
- Notions de sécurité
- Installer un serveur web

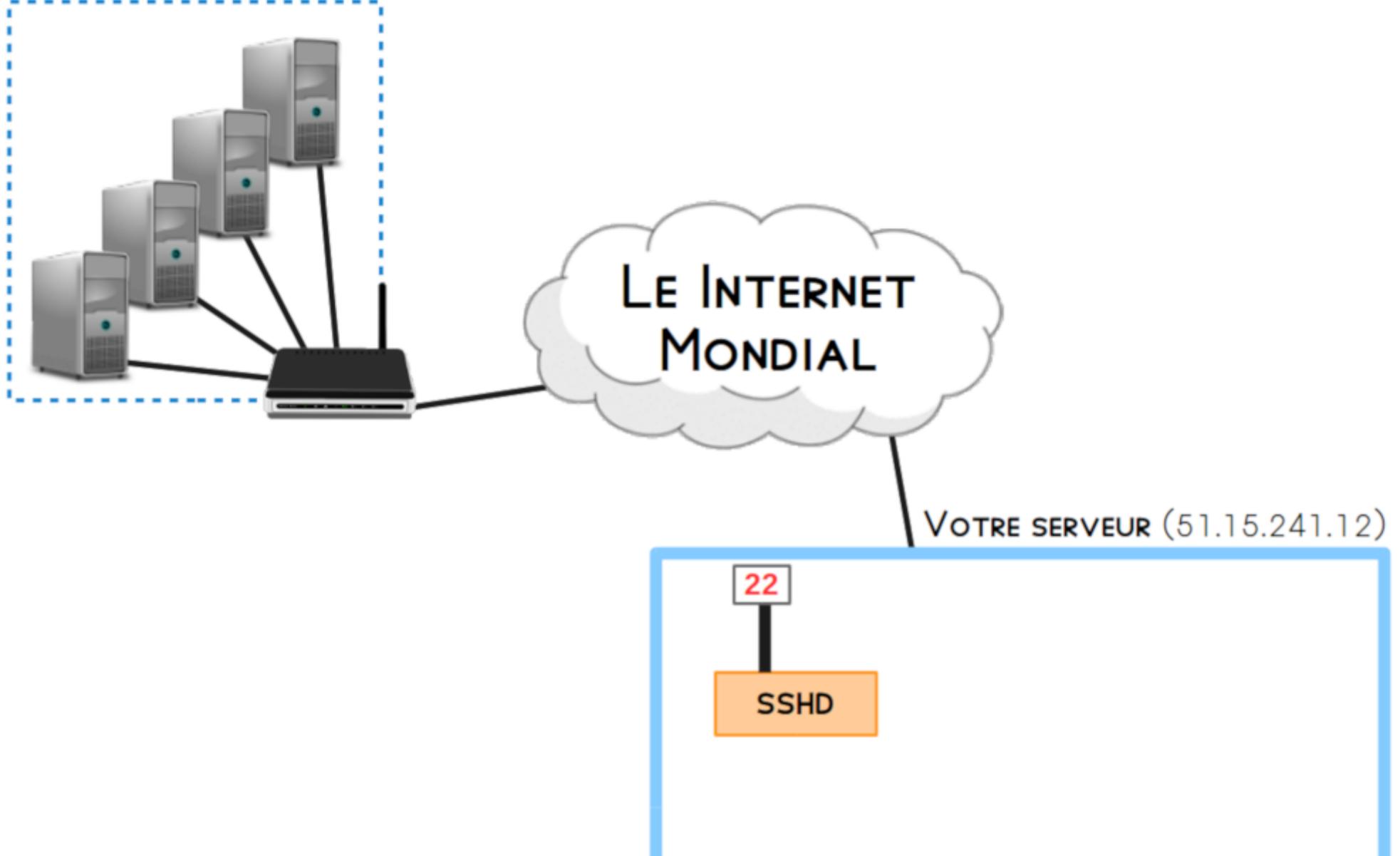
Recap'

(tentative de représentation)

CENTRE DE FORMATION



CENTRE DE FORMATION



CENTRE DE FORMATION



SERVEUR DNS (NETLIB.RE)

VOUS.NETLIB.RE → 51.15.241.12

LE INTERNET
MONDIAL

VISITEUR / CLIENTS



VOTRE SERVEUR (51.15.241.12)

22

SSHD

1. Déployer une app PHP/Mysql

1. Déployer une app PHP/Mysql

- Jusqu'ici : des pages statiques !

1. Déployer une app PHP/Mysql

Comment créer des pages "dynamiques", par exemple :

- espaces utilisateurs (mur facebook, compte amazon)
- compte généré via des données variables (cours de bourse, ...)
- ... ou stockées dans des bases de donnée (liste d'élèves d'une université...)
- ...

"Bricolage" : cron job qui rafraîchit la page toutes les minutes

1. Déployer une app PHP/Mysql

Methode générale / versatile / "moderne"

- Reverse-proxy (c.f. `proxy_pass`)

1. Déployer une app PHP/Mysql

Historiquement / classiquement : PHP

- Le serveur web transmet la requête à un programme / daemon PHP
- (Basé sur FastCGI, pas exactement un reverse-proxy)
- PHP interprête le code et genere la réponse
- .. et renvoie la réponse à nginx qui la renvoie au client
- PHP est la "Gateway" dans le contexte de Nginx
 - c.f. 502 Bad Gateway, et 504 Gateway Timeout

1. Déployer une app PHP/Mysql

et aussi : MySQL

- MySQL est classiquement utilisé pour gérer des bases de données
 - Les données sont structurées de façon cohérente pour être accédées de manière efficace
 - Interface avec PHP qui peut venir piocher dynamiquement des données
 - PHP / L'app met ensuite en forme ces données pour générer la page
-
- N.B. : MariaDB est un fork du MySQL originel
 - Alternatives à MySQL/MariaDB : PostgreSQL

1. Déployer une app PHP/Mysql

Nextcloud



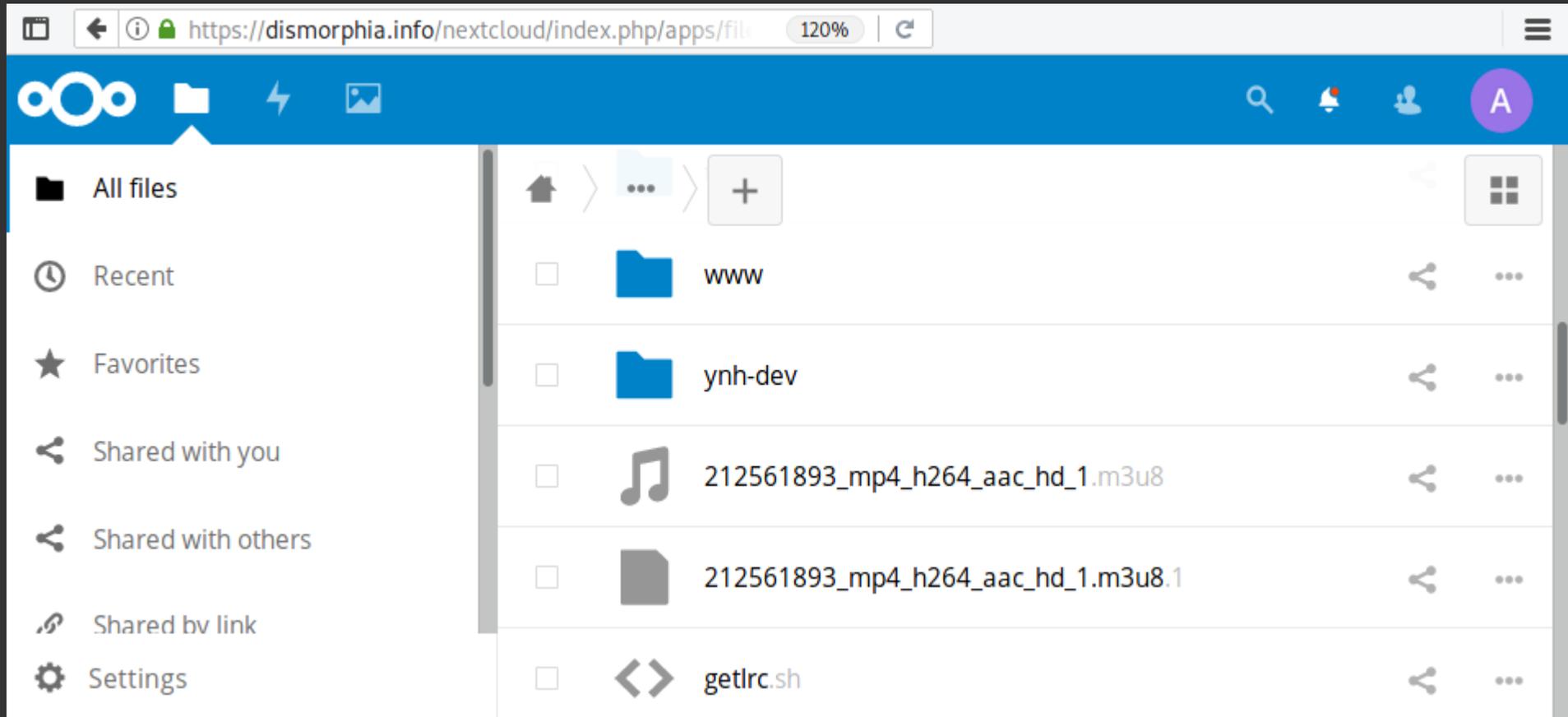
1. Déployer une app PHP/Mysql

Nextcloud

- Un logiciel libre, auto-hébergeable
 - Stockage et synchronisation de fichiers sur un serveur
 - (similaire à Google Drive, Dropbox,)
 - Basé sur PHP / MySQL
-
- Et aussi : calendrier, contacts, et pleins de modules variés

1. Déployer une app PHP/Mysql

Nextcloud



1. Déployer une app PHP/Mysql

Nextcloud : procédure d'installation

- Télécharger (et décompresser) les sources
- (Configurer PHP)
- Créer une base de donnée MySQL
- Configurer Nginx
- Configurer l'application
- Tester et valider

1.5. Investiguer et réparer des problèmes

1.5. Investiguer et réparer des problèmes

Méthode générale

- Comprendre que le débogage fait partie du job !
- Être attentif, méthodique
- Chercher et consulter les logs...
 - ... et lire les messages attentivement !
- Comparer les messages à ce que l'on vient de faire, identifier à quel niveau se situe le problème ...
- Chercher des infos sur Internet ...
 - avec des mots clefs approprié

1.5. Investiguer et réparer des problèmes

Méthode générale

Malheureusement ...

- Logs pas forcément trouvable (ou alors messages abscons)
- Demande un peu d'expérience pour savoir quoi / où chercher ...

1.5. Investiguer et réparer des problèmes

Sources d'information

Savoir lire des posts sur Stack Overflow et ses dérivés :

- Stack Overflow (développement / programmation)
- Super User (administration système généraliste / amateur)
- Server Fault (contexte pro., e.g. maintenance de serveur)

2 - Introduction aux LXC

2 - Introduction aux LXC

Jusqu'ici : machines virtuelle

- Une machine entière simulée dans une autre machine
- Bonne isolation
- Ressources "garanties", allouées explicitement à la VM
- "Lourd" en terme de taille (plusieurs Go) et performances

THE COST OF RUNNING VIRTUAL MACHINES



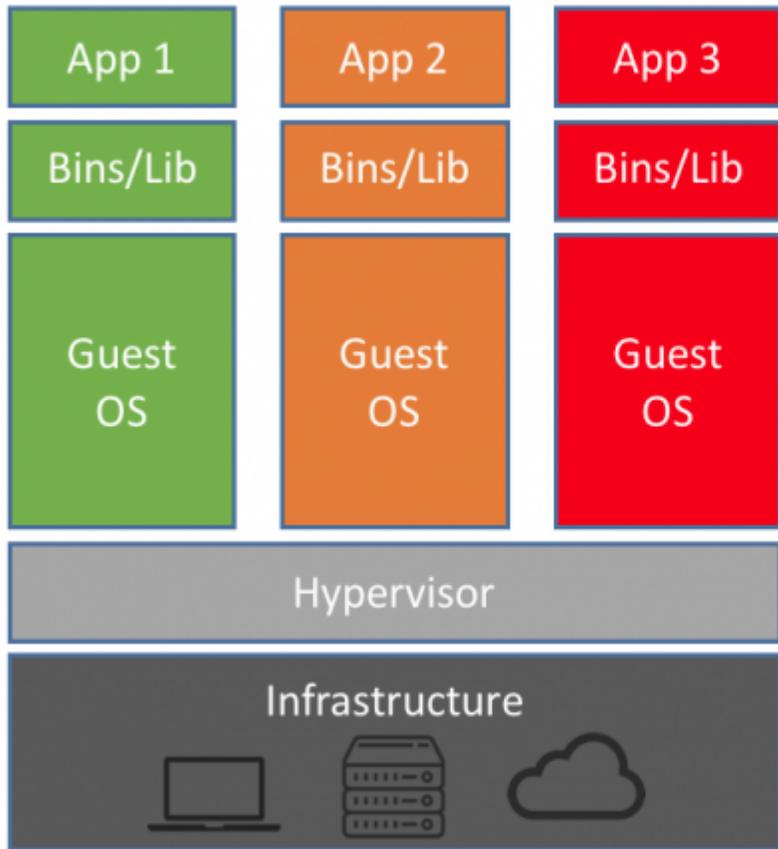
IS TOO DAMN HIGH

2 - Introduction aux LXC

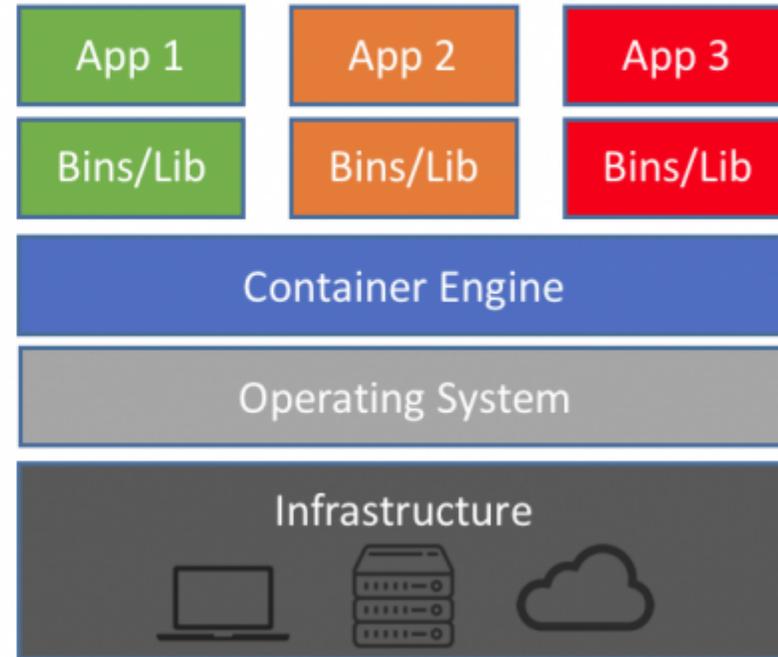
Généralités sur la conteneurisation

La conteneurisation permet :

- de créer des systèmes isolés, similaire à des VM
- mais qui partagent un kernel commun ... !
- (et potentiellement des fichiers commun)
- ⇒ système léger (taille et perf), déployable rapidement, "jetable"
- (mais : ressources partagées, non garanties)



Machine Virtualization



Containers

2 - Introduction aux LXC

Généralités sur les LXC

- Technologie de conteneurisation de Linux
 - (c.f. fonctionnalité du kernel, les cgroups)
- Relativement récent !
 - V1.0 date de début 2014 !
 - V3.0 cette année
- À l'intérieur : un mini-système complet

2 - Introduction aux LXC

"Vanilla" LXC

`apt install lxc` puis utilisation des commandes `lxc-<stuff>`

LXD !

- "Hyperviseur" pour gérer des LXC
- UX bien meilleure (commande `lxc <stuff>` (et non `lxd` !))
- Développé par Canonical (c.f. Ubuntu)

Usage:

```
lxc [command]
```

Available Commands:

config	Manage container and server configuration options
delete	Delete containers and snapshots
exec	Execute commands in containers
file	Manage files in containers
image	Manage images
info	Show container or server information
launch	Create and start containers from images
list	List containers
snapshot	Create container snapshots
start	Start containers
stop	Stop containers

2 - Introduction aux LXC

Creer un LXC (1/2)

- De nombreuses images de systeme disponible

```
$ lxc image list images:
+-----+-----+
|          ALIAS          |      SIZE      |
+-----+-----+
| alpine/3.8              | 2.34MB         |
| archlinux               | 137.20MB       |
| centos/7                | 83.47MB        |
| debian/10               | 122.36MB       |
| fedora/28               | 60.40MB        |
| gentoo                  | 242.96MB       |
| ubuntu/18.10           | 124.88MB       |
+-----+-----+
```

2 - Introduction aux LXC

Creer un LXC (2/2)

```
$ lxc launch images:debian/stretch test1  
Creating test1  
Starting test1
```

2 - Introduction aux LXC

Interagir avec un LXC (1/2)

```
$ lxc exec text1 -- ps -ef --forest
UID          PID    CMD
root         103    ps -ef --forest
root          1     /sbin/init
root         32     /lib/systemd/systemd-journald
systemd+    39     /lib/systemd/systemd-networkd
root        53     /lib/systemd/systemd-logind
message+    55     /usr/bin/dbus-daemon --system
root        80     /sbin/dhclient -4 -v -pf /run/
systemd+    94     /lib/systemd/systemd-resolved
root        95     /sbin/agetty --noclear --keep-
```

2 - Introduction aux LXC

Interagir avec un LXC (2/2)

```
root@scw-32c380:~$ lxc exec stretch1 -- /bin/bash
root@stretch1:~$          # <<< Dans le LXC !
```

```
root@scw-32c380:~$ lxc console stretch1
To detach from the console, press: <ctrl>+a q

Debian GNU/Linux 9 stretch1 console

stretch1 login:
```

2 - Introduction aux LXC

I can haz internet ?

- Les LXC sont sur un réseau local, via `lxcbr0`

```
$ lxc list
+-----+-----+-----+
|      NAME      | STATE |      IPV4      |
+-----+-----+-----+
| saperlipopette | RUNNING | 10.0.0.51 (eth0) |
| veganaise       | RUNNING | 10.0.0.32 (eth0) |
| vinaigrette     | STOPPED |                  |
+-----+-----+-----+
```

2 - Introduction aux LXC

Push / pull files

```
# Envoyer un fichier sur un LXC
$ lxc file push -- <fichier> <machine>/<destination>
# Recuperer un fichier dans un LXC
$ lxc file pull -- <machine>/<fichier> <destination>
```

Exemples :

```
$ lxc file push -- template.html test1/var/www
$ lxc file pull -- test1/var/log/auth.log test1.auth.log
```

2 - Introduction aux LXC

Snapshots

- Il est possible de sauvegarder l'état d'un LXC pour le restaurer plus tard
- (ACHTUNG : Le LXC doit être à l'arrêt !)

```
$ lxc snapshot <container> <nom_du_snapshot>
```


3 - Introduction à YunoHost

3 - Introduction à YunoHost

Un outil pour démocratiser l'auto-hébergement

- héberger ses propres services
- réduire la barrière technique (et le coût en temps)

Contextes : domestique, associatif, PME

Supports : Carte ARM, vieux laptop, VPS, ...

Déploiement d'outils "classiques" :

- synchronisation de fichier, de contacts, de calendrier
- blog, lecteur RSS, mail, messagerie instantannée
- tableau de tâche, ERP, ...
- ...?

3 - Introduction à YunoHost

D'un point de vue pratique

- gain de temps et d'énergie (déploiement et maintenance)
- principes de base de sécurité déjà implémenté
- garder le contrôle de ses données

D'un point de vue pédagogique

- écosystème "complet" : apps, mail, LDAP, IM, ..
- perspectives d'automatisation

3 - Introduction à YunoHost

Aspect historique

- *kload* découvre l'adminsyst et se rends compte que c'est galère
- Volonté de simplifier / automatiser
- Script qui font ce qu'un adminsyst aurait fait "à la main"

3 - Introduction à YunoHost

YUNOHOST

-  Basé sur Debian
-  Administration en CLI ou via une gentille interface web
-  Installation d'applications en quelques clics
-  Multi-domaines et intégration HTTPS (Let's Encrypt)
-  Multi-utilisateurs avec portail "Single Sign On"
-  Stack mail complète + messagerie instantannée XMPP
-  Sécurité (fail2ban, firewall)
-  Système de sauvegardes

3 - Introduction à YunoHost

Multi-domaines

- Votre serveur peut héberger plusieurs domaines
 - par ex. `jean-dupont.com`
 - ... et `curling.alsace`
- Il est ensuite possible d'avoir des mails et des apps sur ces domaines
- En HTTPS ! (Certificats Let's Encrypt en quelques clics)

3 - Introduction à YunoHost

Applications

<p>Kanboard</p> <p>7 validated AGPL-3.0</p> <p>Kanboard is a simple visual task board web application</p> <p>22 August 2018 - jibec</p> <p>Code Doc + Install</p>	<p>Nextcloud</p> <p>7 validated AGPL-3.0</p> <p>Access & share your files, calendars, contacts, mail & more from any device, on your terms</p> <p>28 September 2018 -</p> <p>Code Doc + Install</p>	<p>OpenSondage</p> <p>7 validated CECILL-B</p> <p>OpenSondage is an online service for planning an appointment or making a decision quickly and easily. No</p> <p>1 September 2018 - ljf</p> <p>Code Doc + Install</p>
<p>phpMyAdmin</p> <p>7 validated GPL-2.0-only</p> <p>Manage MySQL databases over the web</p> <p>8 October 2018 - julien</p> <p>Code Doc + Install</p>	<p>Piwigo</p> <p>7 validated GPL-2.0</p> <p>photo gallery</p> <p>15 September 2018 - JimboJoe</p> <p>Code Doc + Install</p>	<p>Rainloop</p> <p>7 validated AGPL-3.0</p> <p>Lightweight multi-account webmail</p> <p>17 January 2018 - scith, Djip007, polytan02</p> <p>Code Doc + Install</p>

3 - Introduction à YunoHost

Info

ID zerobin

Description A minimalist, opensource online pastebin where the server has zero knowledge of pasted data

Multi instance Yes

Install

Label for Zerobin

Choose a domain for Zerobin

Example: domain.org [Manage domains](#)

Choose a path for Zerobin

Example: /zerobin

ou bien : `yunohost app install zerobin`

3 - Introduction à YunoHost

Applications

- L'installation fait "ce que vous auriez fait à la main"
- Une application peut être privée (réservée à certains utilisateurs)
- Intègre aussi la mise à jour et les backups
- ~20 apps officielles, ~100+ communautaires

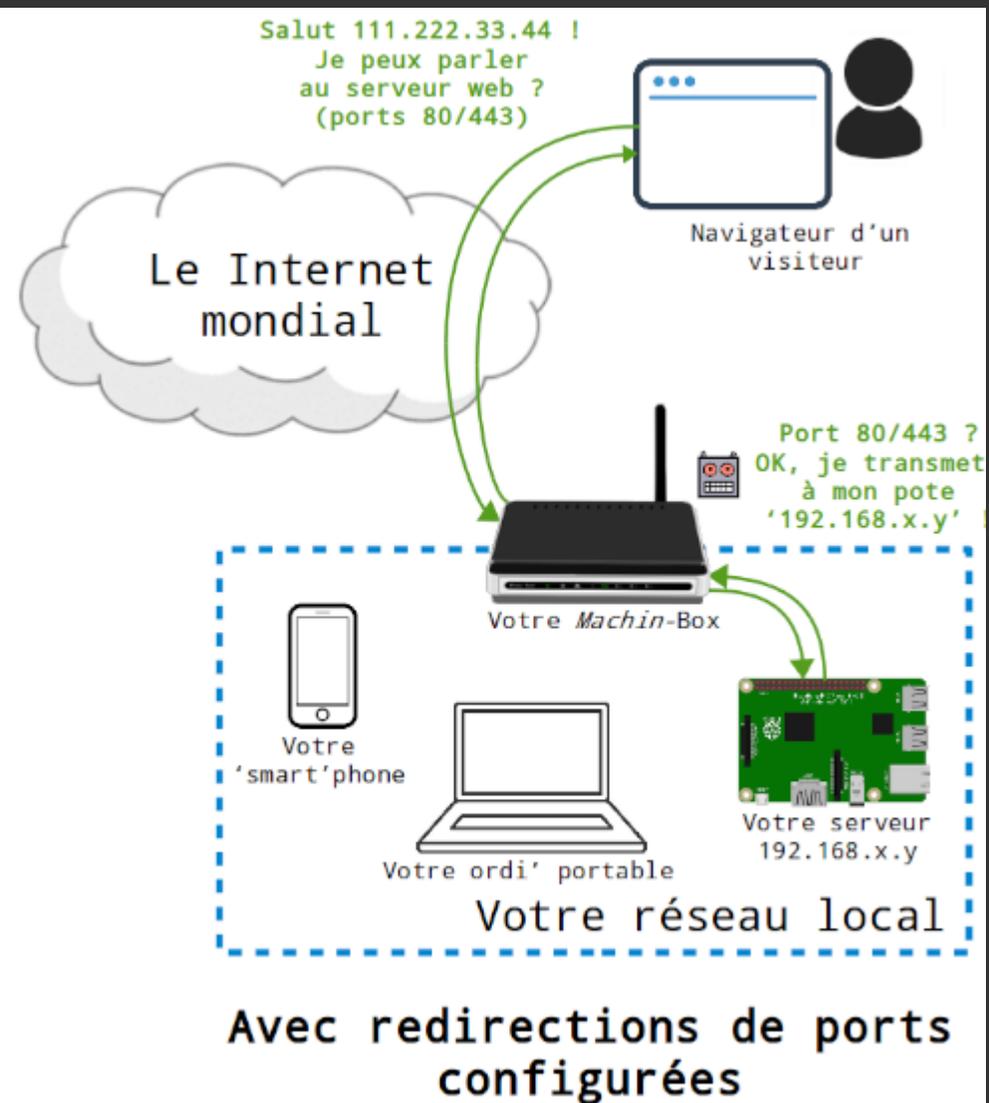
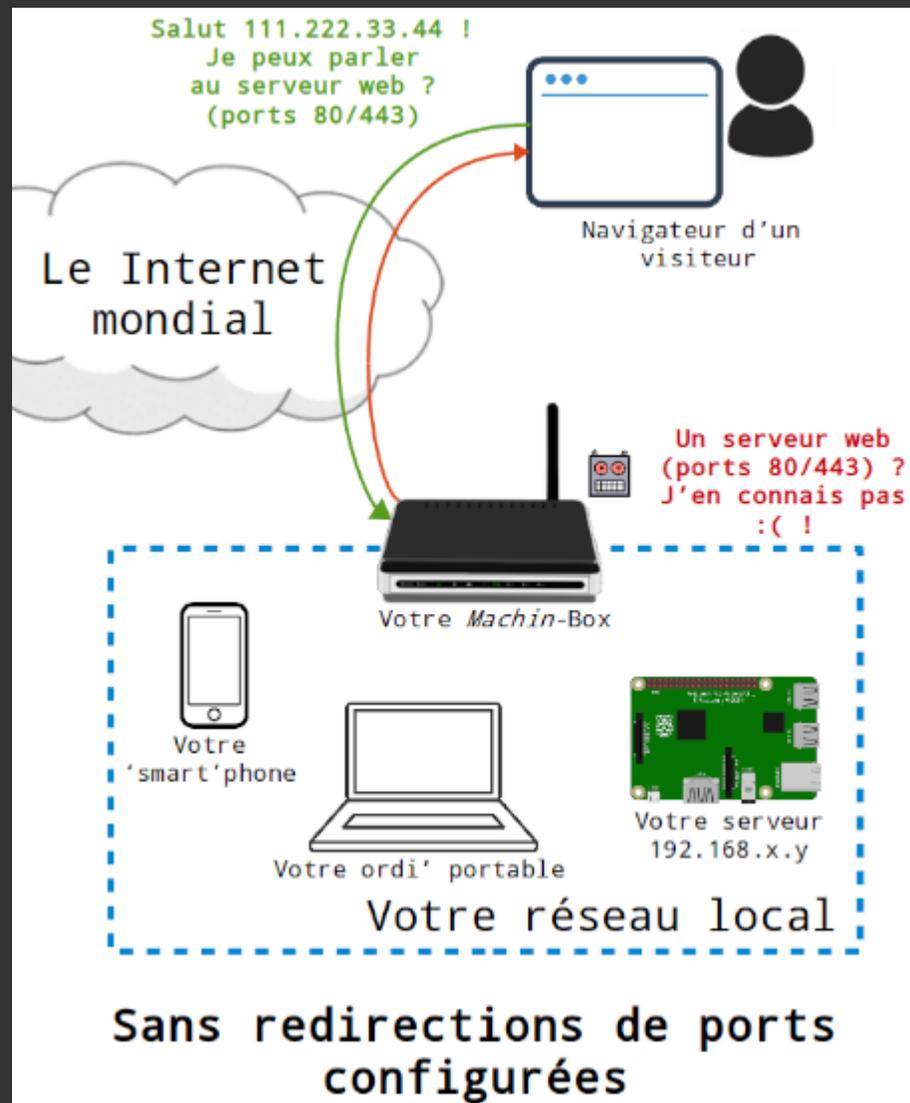
3 - Introduction à Yunohost

Utilisateurs

- Multi-utilisateurs, "les vrais gens de la vraie vie"
- Portail utilisateur avec "Single Sign On" (`votre.domaine.tld/yunohost/sso`)
- Ils ont automatiquement une adresse mail (et un compte XMPP)

3 - Introduction à YunoHost

Administration (`votre.domaine.tld/yunohost/admin`)



Ingénierie d'infrastructure

Ingénierie d'infrastructure

Problématiques qui émergent lorsque l'infrastructure ou le nombre d'user grandi

- Haute disponibilité
- Redondance, sauvegarde
- Quel bottleneck (goulot d'étranglement)
 - Storage I/O ? (interactions avec le stockage)
 - Requests I/O ? (gestion des demandes)
 - Computing power ? (gestion des calculs)

Ingénierie d'infrastructure

Storage engineering

- Lorsque le besoin grandit : nécessité de séparer la partie OS/application de la partie stockage
- Exemples de technique:
 - NAS
 - SAN
 - RAID
 - Tiering
 - ...

Ingénierie d'infrastructure

Storage engineering : NAS

- NAS (network attached storage)
- Un (unique?) périphérique branché au réseau dont la fonction est de s'occuper de la partie stockage des données
- Le NAS s'occupe de la partie système de fichier
- Plusieurs OSs peuvent se connecter sur ce stockage et interagir avec
- Ex. : un espace de partage de documents dans une entreprise

Ingénierie d'infrastructure

Storage engineering : NAS



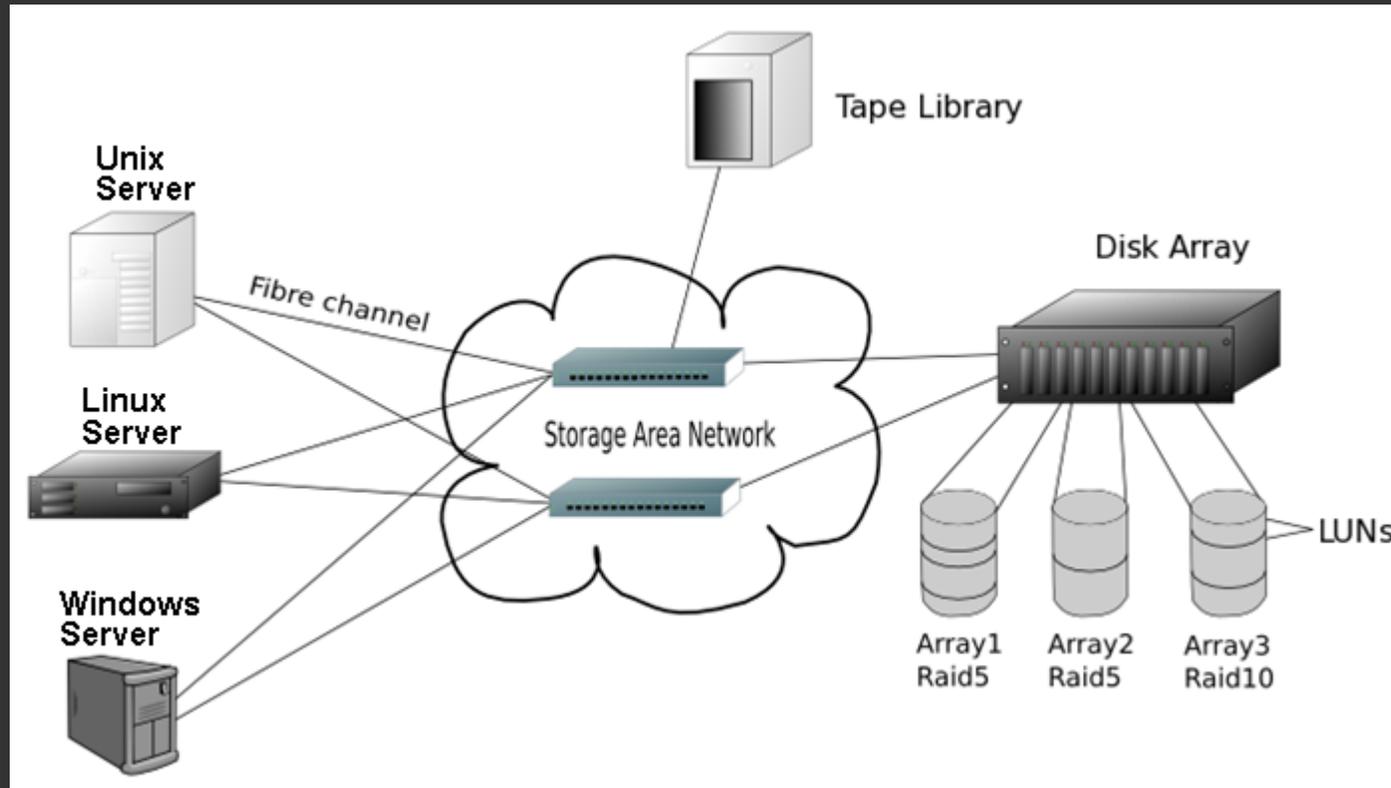
Ingénierie d'infrastructure

Storage engineering : SAN

- SAN (storage area network)
- Un réseau de périphériques de stockage
- ... connectés sur les machines pour faire "comme si" les disques étaient branchés directement sur la machine
- Accès au niveau "block" : c'est à la machine de gérer l'aspect système de fichier
- Performance + redondance

Ingénierie d'infrastructure

Storage engineering : SAN



Ingénierie d'infrastructure

Storage engineering : SAN

Ingénierie d'infrastructure

Storage engineering : RAID

- RAID (Redundant Array of Inexpensive Disks)
- Un ensemble d'architecture de stockage pour gérer la redondance, disponibilité, performance, ou capacité
- Géré au niveau software ou hardware
- On parle de "grappe" de disque



Ingénierie d'infrastructure

Storage engineering : RAID

- RAID 0 (striping) :
 - les morceaux d'un fichier sont répartis entre les disques
 - pas d'augmentation de redondance, mais augmentation de la performance
 - (lecture/écriture sur plusieurs disques en parallèle)

Ingénierie d'infrastructure

Storage engineering : RAID

- RAID 1 (mirror) :
 - copie des données sur chaque disques (bottleneck = slowest drive)
 - lecture sur n'importe lequel des disques
 - ajouter un disque augmente la redondance mais pas la capacité

Ingénierie d'infrastructure

Storage engineering : RAID

- RAID 10 (1+0) : stripping + mirroring
 - nécessite au moins 4 disques
 - performance + redondance
 - jusqu'à 50% de perte de disque (tant qu'un disque + son miroir n'est pas perdu)

Ingénierie d'infrastructure

Storage engineering : RAID

- RAID 5 :
 - nécessite au moins 3 disques
 - information répartie entre les disques
 - tradeoff capacité/redondance : une seule perte de disque tolérée

Ingénierie d'infrastructure

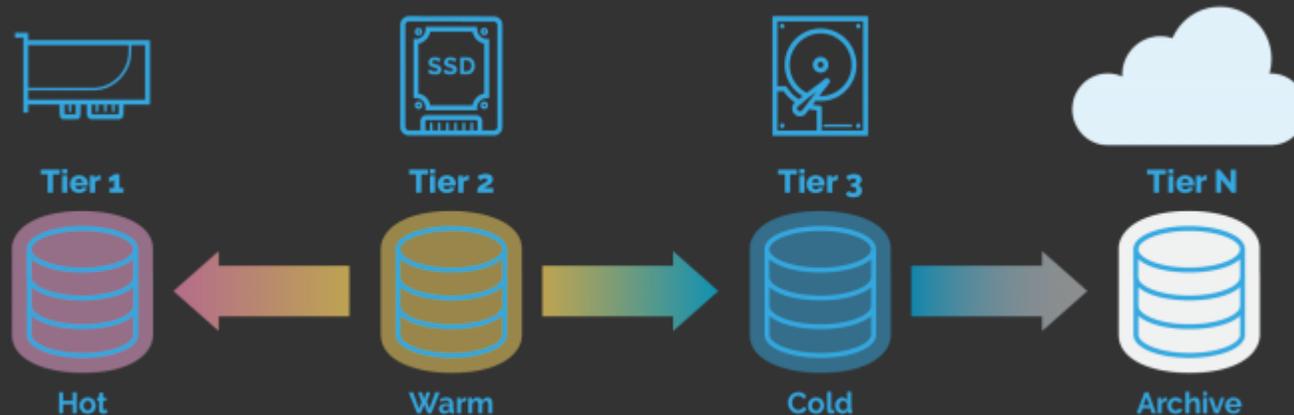
Storage engineering : RAID

- RAID 6 :
 - nécessite au moins 4 disques
 - information répartie entre les disques
 - tradeoff capacité/redondance : jusqu'à deux pertes de disque tolérée

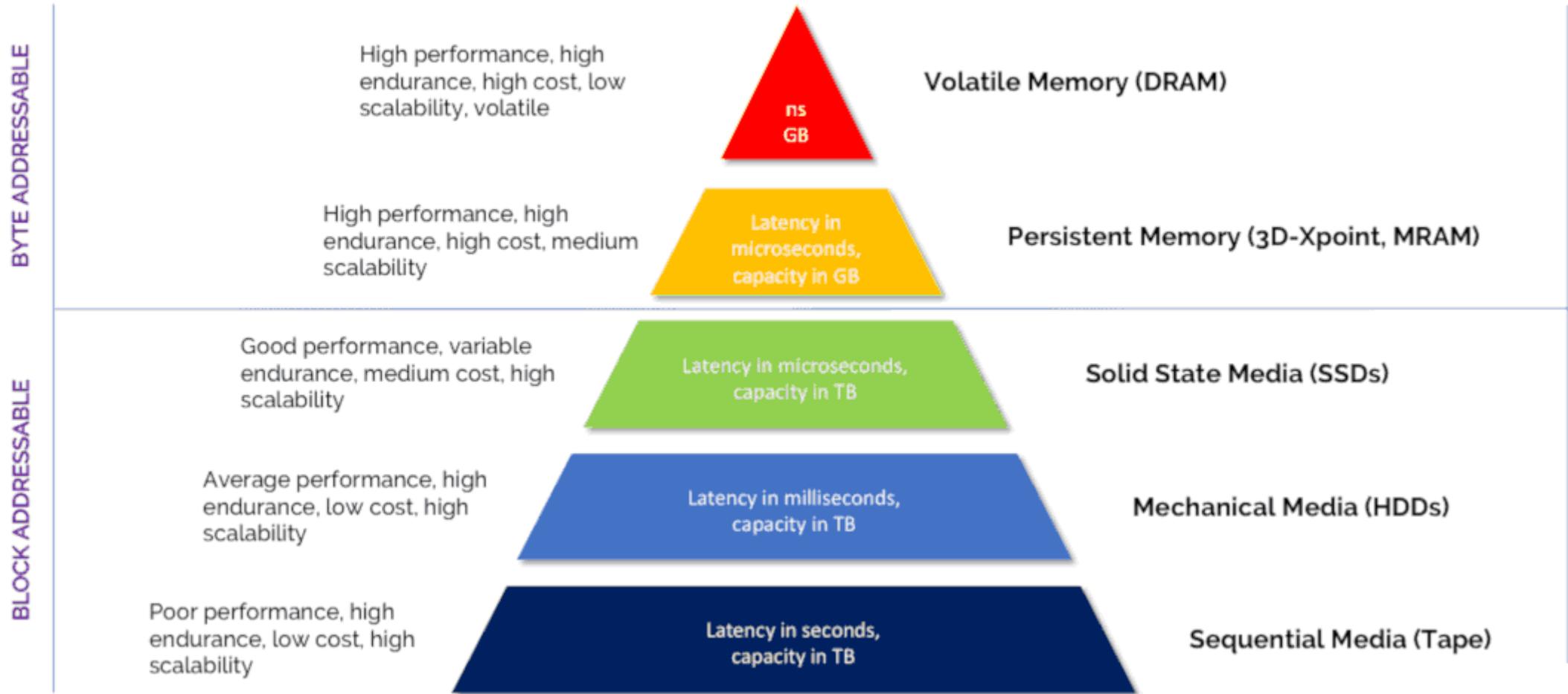
Ingénierie d'infrastructure

Storage engineering : tiering

- Optimiser la disponibilité des données et leur coût de stockage, en fonction de la demande



THE STORAGE MEDIA HIERARCHY



Ingénierie d'infrastructure

Traffic engineering

- Lorsque le nombre d'utilisateur grandit : besoin d'optimiser le traitement des requêtes
- Exemple de quelques techniques:
 - caching, zipping
 - load balancing
 - DNS round robin
 - CDN

Ingénierie d'infrastructure

Traffic engineering : caching, compression

- Caching
 - par ex. côté client: le navigateur garde en mémoire certaine image pour ne pas les re-demander à chaque requête
- Compression (e.g. avec gzip)
 - compression des données statiques textuels (.html, .js, .css, ...)
 - gain en débit
 - (attention, implications de sécu non triviale, c.f. BREACH)

Ingénierie d'infrastructure

Traffic engineering : load balancing

- Peut avoir lieu au niveau software, ou bien niveau hardware (équipement dédié)
- Le daemon principal réparti le traitement des requêtes entre des workers
- Beaucoup de serveurs logiciels intègrent cette fonctionnalité (`nginx`, `apache`, ..)

Ingénierie d'infrastructure

Traffic engineering : DNS round robin

- Il s'agit d'une autre technique de load balancing
- Associer plusieurs IP (A record) à un nom de domaine
- Lors de la résolution du nom de domaine, un enregistrement est choisi aléatoirement (round robin)

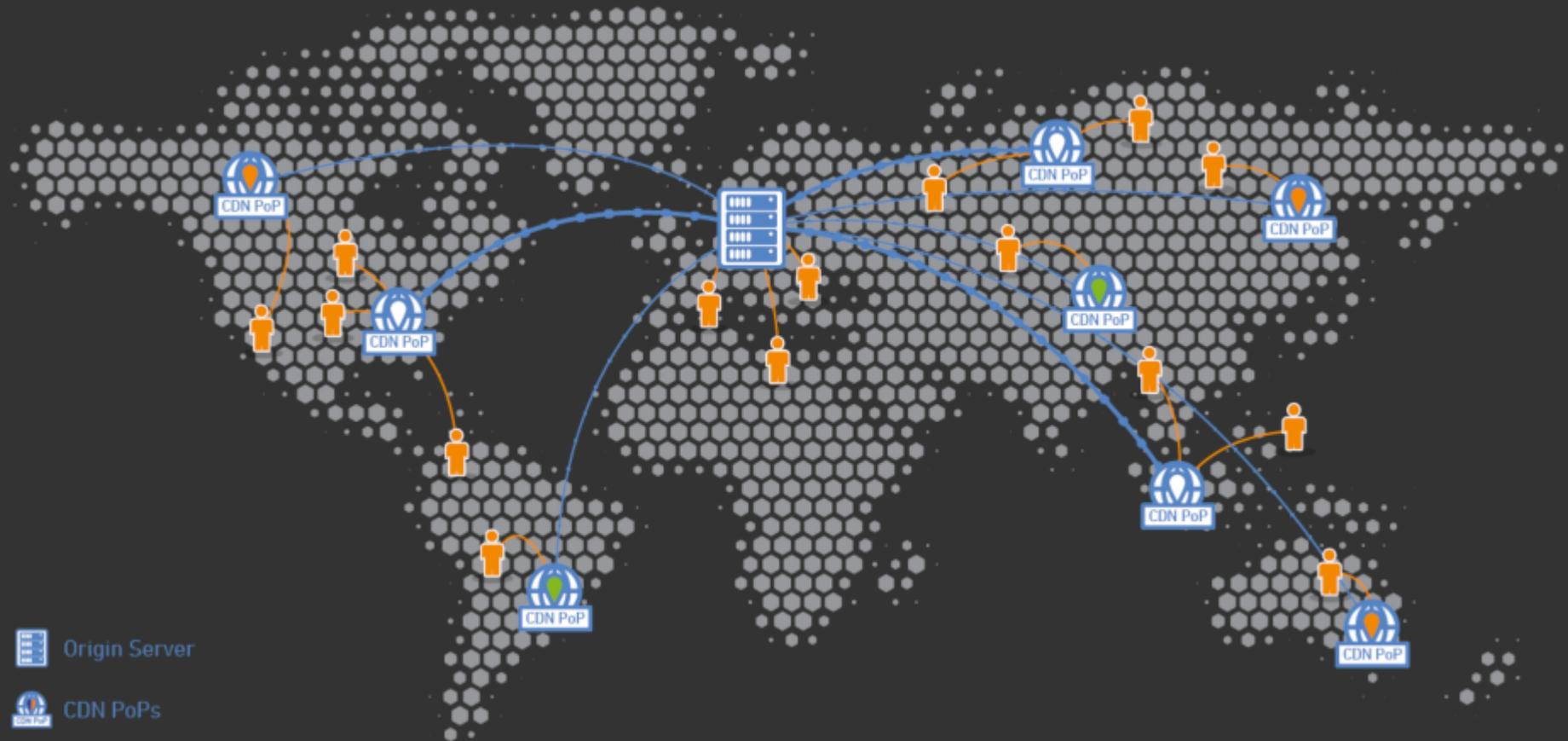
Ingénierie d'infrastructure

Traffic engineering : CDN

- CDN (Content Delivery Network)
- Sorte d'opérateur "haut-niveau" (couche 5+) qui proposent comme service une haute dispo pour certains fichiers web (e.g. `.js`) ou contenus multimédias (e.g. video)
- Répartition de serveurs géographiquement dans des "points de présence" (PoP)
- Réponse du DNS en fonction de la proximité géographique
- Interfaçage privilégié avec les opérateurs réseaux directement dans les datacenter / IXP
- Typiquement appliqué au web mais pas seulement (par ex. miroir des dépôts debian)

Ingénierie d'infrastructure

Traffic engineering : CDN

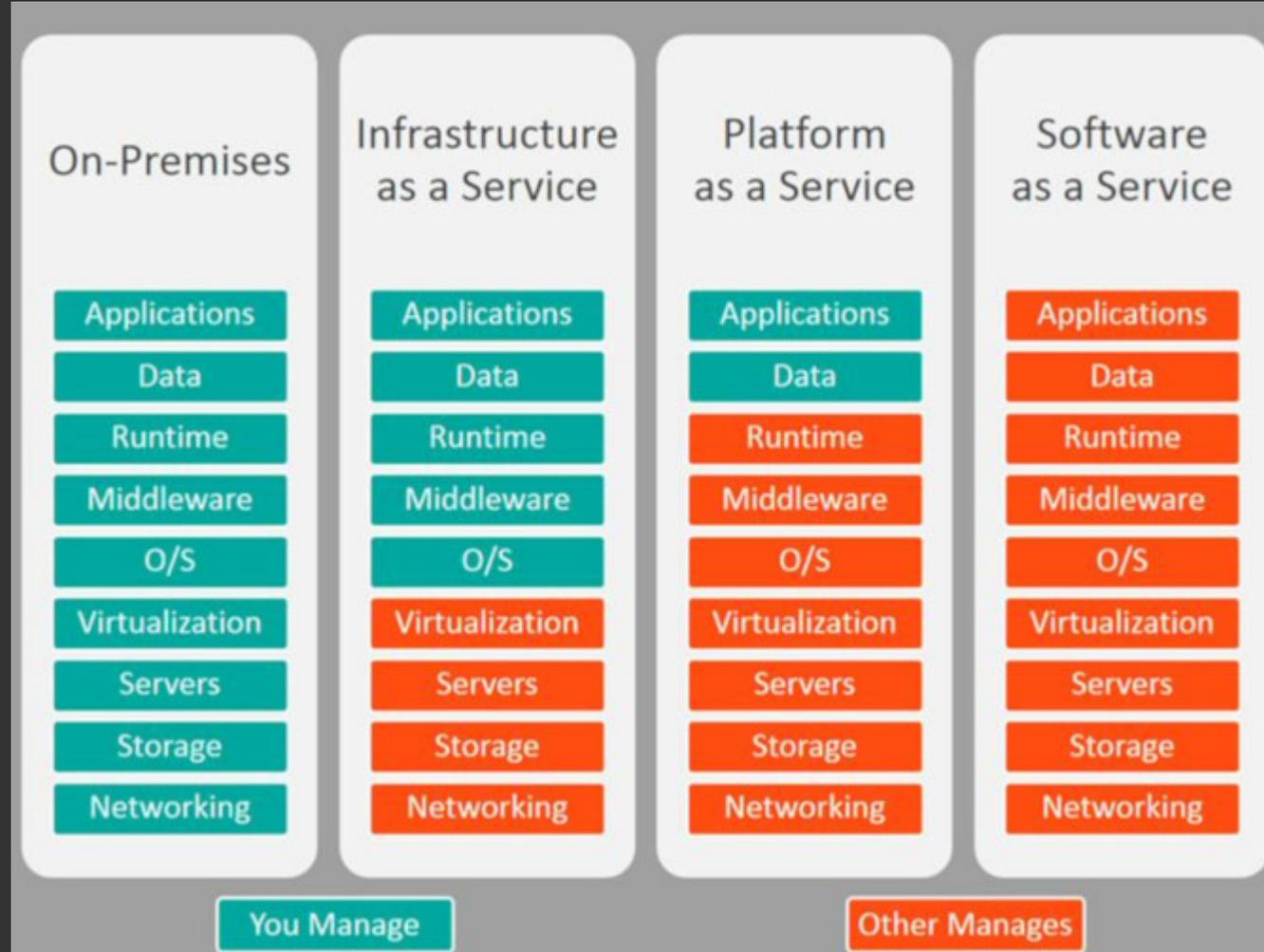


Ingénierie d'infrastructure

Anything As A Service

- Un des fondement du cloud : l'abstraction de l'infrastructure, de la plateforme et des applications

Ingénierie d'infrastructure



Ingénierie d'infrastructure

Anything As A Service

- N.B. : Sur les plateformes d'IaaS, on peut non seulement louer des machines, mais aussi des services comme : stockage additionnels, load balancer, firewall, ...



Pizza as a Service 2.0

<http://www.paulkerrison.co.uk>

Tradition
On-Premises
(legacy)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Infrastructure as a
Service
(IaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Containers as a
Service
(CaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Platform as a
Service
(PaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Function as a
Service
(FaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas

Software
Service
(SaaS)

Conversation

Friends

Beer

Pizza

Fire

Oven

Electric / Gas