

# M.E.P. et déploiement - MS2D / ERIS

Christophe Brun

Campus Saint-Michel IT

17 avril 2024



# Table des matières

- 1 Table des matières
- 2 Programme du module
- 3 Introduction
- 4 Le matériel
- 5 Le logiciel
- 6 Le ressources partagées
- 7 Les services
- 8 Ansible
- 9 Docker
- 10 Kubernetes
- 11 OpenStack
- 12 Serveur Web Apache et Nginx
  - Généralités
  - Reverse Proxy
  - Certificat SSL
- 13 Indicateurs et mesure de performances - Systèmes / Réseau et web
  - Syslogd

# Mise en production et déploiement

Compétence acquise au cours des 5 jours du module

## Compétences :

- “Préparer l'environnement et déployer le progiciel ou la solution.”



# Mise en Production et déploiement

Le programme officiel des 5 jours du module

## ① Mise en exploitation des ressources matérielles et logicielles

- Vérification des configurations
- Déploiement des applications
- Automatisation des procédures de déploiement
- Élaborer les bilans de l'exploitation
- Prévoir les évolutions de l'infrastructure

## ② Indicateurs et mesure de performance – Systèmes / Réseau et web

- Centralisation des journaux et exploitation des logs avec syslogd
- Analyse du trafic réseau avec MRTG
- Analyse des journaux de type d'Apache Web Server avec Analog
- Consolidation d'indicateur de qualité avec rrdtool
- Création de page HTML de type tableau de bord avec rrdtool – Tableau de bord
- Gestion d'incidents et actions correctives

# Evaluation

- Bons et mauvais points tout au long du module.
- 80 % x évaluation continue avec les résultats des exercices.
- 20 % sur une évaluation écrite finale

# Intervenant sur le module Architecture d'Application

Christophe Brun, conseil en développement informatique

- 1<sup>ère</sup> année d'intervenant à Saint-Michel 😊.
- 7 ans de conseil en développement au sein d'SSII .
- 7 ans de conseil en développement à mon compte [PapIT](#).
- Passionné !



# Les ressources matérielles

## Les machines du web

On peut résumer un serveur web à :

- Un CPU (Architectures x86, ARM, RISC-V, etc.)
- De la mémoire RAM
- De l'IO
  - Disque dur (NVMe)
  - Réseau (Ethernet, optique)
  - Disque DVD

A l'imagine de n'importe quel ordinateur, mais souvent avec plus de capacités et de redondances.

# Les ressources logicielles

## Les stacks du web

Une stack web est faite en général de :

- Un OS, qui est une couche d'abstraction du hardware présenté précédemment (Ubuntu, Red Hat, Windows, BSD).
- Un reverse Proxy (Apache, Nginx, etc.)
- Un serveur web (Apache, Nginx, Gunicorn, NextJS, etc.)
- L'application web un ensemble de “Business rules” implémentées grâce à des bases de données, des IHM, des connections aux API (en PHP, Python, NodeJS, etc.)
- Une base de données (MySQL, PostgreSQL, MongoDB, etc.)

# Les ressources partagées

## Les machines du web

Dans un environnement de production, on retrouve une forte variabilité des ressources CPU mais surtout des ressources logicielles.

A cette variabilité des environnements de production, il faut ajouter la variabilité des environnements de développement.

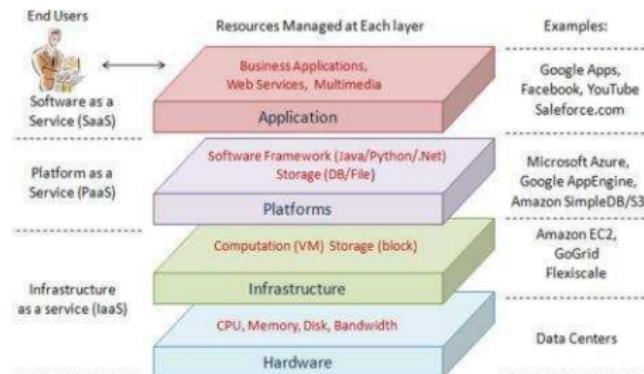
Beaucoup de développeurs travaillent sous Windows ou Mac OS qui sont rarement des environnements de production. Les capacités hardware sont souvent très différentes, la production a plus de capacité que le développement en général.

C'est cette variabilité des environnements qui est la difficulté majeur du déploiement et de la mise en production.

# Les ressources partagées

## Les environnements cloud

Pour palier à cette variabilité, diverses architectures en nuage ont vu le jour. Certaines ont abstraient le hardware voir même une partie du software pour ne laisser que l'application.



## IAAS, PAAS et SAAS

On voit que SAAS et Paas ont fait abstraction du hardware<sup>1</sup>.

<sup>1</sup>Patel et al., [https://www.researchgate.net/publication/324692035\\_Arcus\\_Cloud\\_A\\_Private\\_Cloud\\_Establishment](https://www.researchgate.net/publication/324692035_Arcus_Cloud_A_Private_Cloud_Establishment)

# Les ressources partagées

## Les environnements cloud

Abstraction du hardware ne veut plus dire qu'on a plus du tout besoin de s'en soucier. Même dans le cloud public il faut adapter les capacités des ressources aux besoins et aux coûts.

Essential	
Nombr e de nœuds	1
RAM par nœud	De 4 à 30 Go
Stockage total utile	De 80 à 640 Go
Engagement de niveau de service (SLA)	Non
Passage à une offre supérieure en un clic	Oui
Chiffrement des données au repos et en transit (SSL)	Oui
Graphique de performance	Oui
Sauvegarde en temps réel vers une localisation distante	Oui
Période de rétention des sauvegardes	2 jours
Point de restauration antérieur (Point in Time Recovery)	Oui
Database fork ing	Oui
Connection pooling	Non
Support de Terraform ( <a href="#">en savoir plus</a> )	Oui
Connexivité au réseau privé (vRack)	Oui
Haute-disponibilité	Non
Accès en lecture seule aux nœuds de replication	

Resource Allocation  
Select an initial resource allocation preset, or customize your deployments resources

**Templates**

Small	Medium	
RAM	Disk	IOPS
12GB	120GB	1200
Cores	Members	
3	3	

MySQL sur le cloud public IBM

MySQL sur le cloud public OVH

Qu'est-ce qui vous étonne dans ces deux captures d'écran ?

# Les ressources partagées

## Les environnements cloud

Le cloud public donne souvent l'impression que les ressources sont infinies, mais c'est faux.

Ils ne communiquent même pas les métriques requises pour comprendre les capacités de leur cloud.

Le cloud privé à l'avantage de présenter de manière plus claire les ressources hardware.

# Les ressources partagées

## Les environnements cloud

Même dans le cloud privé, les vCPU ne sont pas des CPU physiques, mais des CPU partagés.

Ce n'est indiqué nul part, mais c'est probablement le cas chez OVH . Cela implique que OS qui héberge l'hyperviseur équilibre en permanence les ressources CPU entre les VM . Cela a un coût en performance qui est inconnu.

Techniquement ce n'est pas obligatoire de partager les CPU, mais c'est souvent le cas pour des raisons de scalabilité. Au besoin un coeur physique peut être dédié à une seule VM .

Linode, un cloud provider, apporte des informations claires sur ce sujet  
<https://www.linode.com/docs/products/compute/compute-instances/plans/comparing-shared-and-dedicated-cpus/>.

# Les ressources partagées

## La virtualisation

Développée par IBM dès les années 60, la virtualisation permet de créer plusieurs machines virtuelles sur un seul hardware. Elle fut d'abord commercialement disponible sur les mainframes avant les plus petites plateformes AS400, iSeries et Power. La technologie TIMI d'IBM permet depuis les années 80 de faire tourner des programmes qui restent compatibles avec des hardwares de plus en plus puissants (changement d'ISA, d'*endianness* A.K.A boutisme en français).

Cela permet de mutualiser les ressources hardware, de les partager en fonction des besoins et même de changer de hardware.

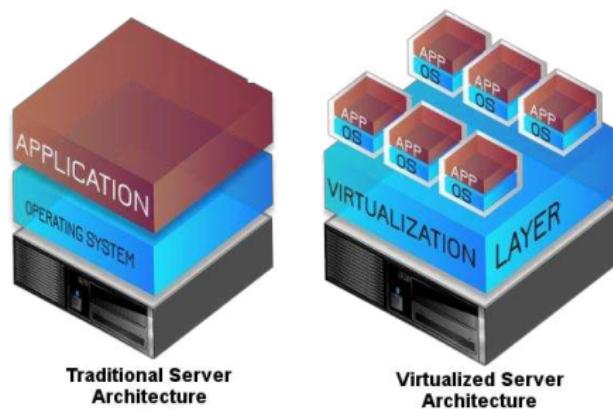
Elle apporte un gain de sécurité en isolant les VM les unes des autres.

Quid des gros bugs /failles de sécurité comme Meltdown et Spectre ?

# Les ressources partagées

## La virtualisation<sup>1</sup>

Aujourd’hui la virtualisation est principalement utilisée pour le partage des ressources et isoler les applications dans une VM pour raison de sécurité. Un OS hôte fait tourner un hyperviseur qui lui fait tourner des VM et plus juste un soft compilé.



# Les ressources partagées

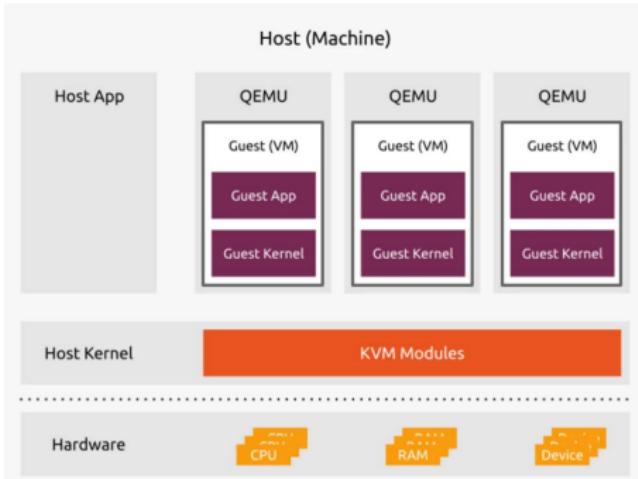
La virtualisation avec KVM et Qemu<sup>2</sup>

KVM (Kernel-based Virtual Machine) est une technologie de virtualisation ouverte intégrée à Linux.

C'est un hyperviseur de type 1, qui négocie directement avec le hardware et offre des performances proches de la machine hôte. Contrairement à un hyperviseur de type 2, qui doit passer par l'OS hôte pour accéder au hardware mais ces derniers ont donc une meilleure portabilité et compatibilité.

Qemu lui peut faire tourner des VM avec ou sans KVM en fonction des besoins.

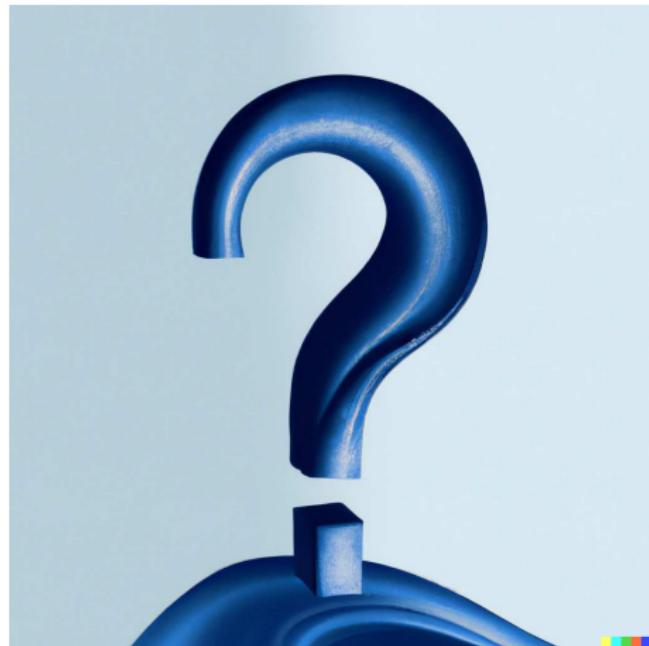
<sup>2</sup>KVM hypervisor: a beginners' guide,  
<https://ubuntu.com/blog/kvm-hypervisor>



# Les ressources partagées

Exercice 1, avec ou sans KVM ?

- Un Windows guest sur un Mac OS hôte?
- Un Alpine Linux sur un Raspberry<sup>3</sup> ?
- VM Ubuntu sur un Ubuntu hôte?
- VM Ubuntu sur un Windows hôte?



---

<sup>3</sup><https://unix.stackexchange.com/questions/340912/qemu-with-kvm-with-differaing-host-guest-architectures>

# Les services

## Définition

Dans les systèmes Windows et Linux, le terme service désigne un programme qui s'exécute en arrière-plan, sans intervention de l'utilisateur. Il faut le configurer pour qu'il démarre automatiquement, dans un certain ordre et avec les bonnes permissions.

La configuration principale consiste à définir une ligne de commande qui sera exécutée au démarrage du service.

Avec `systemd`<sup>4</sup> sous Linux, on peut définir des dépendances entre les services. Limiter les ressources CPU, mémoire, IO, etc. Définir ce qu'il faut faire en cas de crash. Exécuter des scripts avant et après le démarrage du service.

Leur chemin par défaut est `/etc/systemd/system/`.

Ne pas confondre `systemd` qui exécute des tâches en arrière plan et l'ordonnanceur `cron`.

<sup>4</sup>System and Service Manager, <https://systemd.io/>

# Les services

## Exemples

`systemd` est donc l'outil de choix pour lancer en production des applications, des progiciels, etc.

Encore mieux, on peut configurer des services pour qu'ils lancent des VM avec Qemu et les applications tourneraient dans les VM . On profite des avantages de la virtualisation pour isoler les applications et les sécuriser.

Que fait cette configuration ?

```
[Unit]
Description=IN DATA development application
[Service]
RuntimeMaxSec=3600s
Restart=always
WorkingDirectory=/home/debian/dev/IN FRANCE
ExecStart="/home/debian/dev/IN FRANCE/python3-dev/bin/python3" -m gunicorn -w 1
          -b unix:/tmp/in-france-dev-indata-gunicorn.sock application_indata
[Install]
WantedBy=multi-user.target
```

Le chemin de l'exécutable dans `ExecStart` doit être absolu!

# Les services

## Les commandes de base

- `systemctl start <service>` pour démarrer un service.
- `systemctl stop <service>` pour arrêter un service.
- `systemctl restart <service>` pour redémarrer un service.
- `systemctl status <service>` pour afficher le statut d'un service.
- `systemctl enable <service>` pour activer un service au démarrage.
- `systemctl disable <service>` pour désactiver un service au démarrage.
- `systemctl list-units --type=service` pour lister les services.
- `systemctl daemon-reload` pour recharger la configuration de tous les services.
- `systemctl reload <service>` pour recharger la configuration d'un service.

# Les services

Les commandes pour monitorer l'exécution

Pour monitor les logs d'un service, la commande `journalctl` est très utile.

Quelques exemples de commandes utiles :

- `journalctl --unit<service>` pour afficher les logs d'un service.
- `journalctl --unit<service> -f` pour afficher les logs en temps réel.
- `journalctl --unit<service> --since "2024-04-17 00:00:00"` pour afficher les logs depuis une date.
- `journalctl --unit<service> --since "2024-04-17 00:00:00" --until "2024-04-17 23:59:59"` pour afficher les logs entre deux dates.
- `journalctl --unit=<service> -n 100 --no-pager` pour afficher les 100 dernière lignes.

# Exercice pratique 2

Créer une VM avec Qemu et lancer une application avec systemd

Les exigences :

- Créer une VM Linux avec Qemu à l'image d'un VPS OH d'entrée de gamme (1 vCPU, 2 Go de RAM et 10 Go de disque).
- Configurer la machine hôte pour démarrer la VM automatiquement.
- Configurer la VM et Qemu avec une sécurité en accord les bonnes pratiques de sécurité (Clé SSH uniquement, pas de connexion SSH avec le user root, gestion des ports forwardés).
- Démarrer l'application Gunicorn “Hello World”  
<https://gunicorn.org/#quickstart> avec systemd.
- Accès à la VM et à l'application depuis la machine hôte.

# Exercice pratique 3

Une des solutions (commandes à exécuter sur la machine hôte)

```
qemu-img create -f qcow2 linux.qcow2 10G # Create a disk image
# Download a minimal Ubuntu ISO
wget http://archive.ubuntu.com/ubuntu/dists/bionic/main/installer-amd64/current/
    images/netboot/mini.iso
# Install the OS using a virtual CDROM
qemu-system-x86_64 -m 2G -smp 1 -nic user -boot d -cdrom mini.iso -hda linux.
    qcow2 -k fr -enable-kvm
# Run the VM to configure and test SSH
qemu-system-x86_64 -m 2G -smp 1 -nic user,hostfwd=tcp::5022-:22,hostfwd=tcp
    ::5080-:80 -display none -hda linux.qcow2 -k fr -enable-kvm
```

Expliquez chacune des lignes de commande ci-dessus.

Ressources utiles :

- Similaire mais avec Alpine Linux
- Page d'installation Ubuntu du “MinimalCD”
- Configuration des login SSH sur Ubuntu

# Exercice pratique 4

## Une des solutions

Le service de la machine hôte :

```
[Unit]
Description=Qemu Ubuntu VM for St-Michel classes
After=network.target
StartLimitIntervalSec=0

[Service]
Restart=always
WorkingDirectory=/home/chrichri/Documents/Campus-St-Michel-IT/production-
    deployment
ExecStart=/usr/bin/qemu-system-x86_64 -m 2G -smp 1,maxcpus=1 -nic user,hostfwd=
    tcp::5022-:22,hostfwd=tcp::5080-:8080 -display none -hda linux.qcow2 -k fr
    -enable-kvm

[Install]
WantedBy=multi-user.target
```

Expliquez chaque option de la configuration du service.

# Exercice pratique 5

## Une des solutions

Le service de la machine hôte :

```
[Unit]
Description=Qemu Ubuntu VM for St-Michel classes
After=network.target
StartLimitIntervalSec=0

[Service]
Restart=always
WorkingDirectory=/home/chrichri/Documents/Campus-St-Michel-IT/production-
    deployment
ExecStart=/usr/bin/qemu-system-x86_64 -m 2G -smp 1,maxcpus=1 -nic user,hostfwd=
    tcp::5022-:22,hostfwd=tcp::5080-:8080 -display none -hda linux.qcow2 -k fr
    -enable-kvm

[Install]
WantedBy=multi-user.target
```

Expliquez chaque option de la configuration du service.

**-enable-kvm** si l'hôte est un Linux également.

**-display none** pour ne pas afficher la console graphique.

# Exercice pratique 6

Une des solutions

Le service dans la VM :

```
[Unit]
Description=St-Michel Hello World
After=network.target
StartLimitIntervalSec=0

[Service]
Restart=always
WorkingDirectory=/home/chrichri
ExecStart=/usr/bin/gunicorn -w 1 hello:app -b 0.0.0.0:8080

[Install]
WantedBy=multi-user.target
```

Expliquez chaque option de la configuration du service.

# Exercice pratique 7

Une des solutions (commande à exécuter sur la VM)

Commande pour configurer la VM :

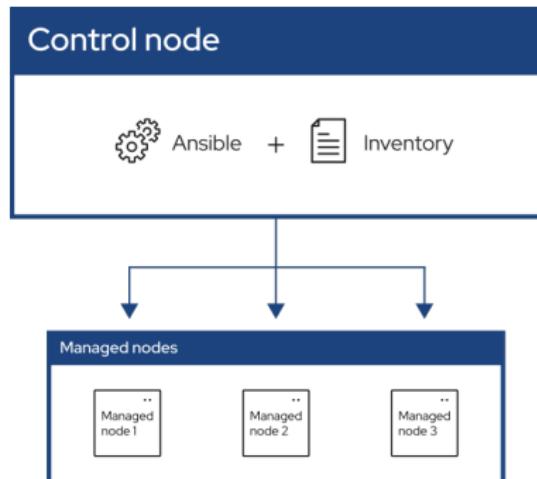
```
# Install gunicorn, pip install gunicorn is no longer recommended
sudo apt-get install python3-gunicorn
# Configure SSH
sudo sed -i 's/PermitRootLogin yes/PermitRootLogin no/' /etc/ssh/sshd_config
sudo sed -i 's/PasswordAuthentication yes/PasswordAuthentication no/' /etc/ssh/
    sshd_config
# Restart SSH with the new configuration
sudo systemctl restart sshd
# Create the .ssh directory and the authorized_keys file
mkdir -p ~/.ssh
touch ~/.ssh/authorized_keys
# Add the public key to the authorized_keys file
echo "ssh-rsa AAAAB3NzaC1yc2EAAAQABAAQgQDQ8z4... chrichri@localhost" >> ~/.ssh/authorized_keys
```

Expliquez chaque commande.

# Automatisation de la configuration avec Ansible

Définition<sup>5</sup>

Ansible est un outil d’automatisation de la configuration des machines physiques ou virtuelles. Il permet de définir des “playbooks” qui décrivent une configuration à appliquer aux machines qui sont dans l’“inventory” .



<sup>5</sup>Ansible Community Documentation,

[https://docs.ansible.com/ansible/latest/getting\\_started/index.html](https://docs.ansible.com/ansible/latest/getting_started/index.html)

# Automatisation de la configuration avec Ansible

## Example d'inventaire

Pour accéder à la VM créée précédemment dans Qemu, il faut définir un inventaire avec les données dont on aurait besoin pour y accéder en SSH .

```
$ ssh chrlichri@localhost -p 5022 -v -i /home/chrlichri/Documents/Campus-St-Michel-IT/production-deployment/virt-ubuntu
```

La commande ci-dessus, devient dans l'inventaire (on peut créer des variables) :

```
[gunicorn]
localhost:5022 ansible_ssh_private_key_file=/home/chrlichri/Documents/Campus-St-Michel-IT/production-deployment/virt-ubuntu ansible_ssh_user=chrlichri
```

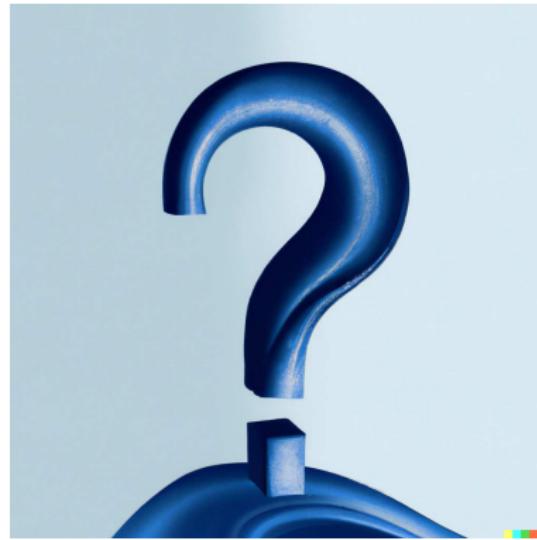
On utilise le module ping pour vérifier que l'accès SSH est correctement configuré.

```
$ ansible gunicorn -m ping -i inventory.ini
localhost | SUCCESS => {
    "ansible_facts": {
        "discovered_interpreter_python": "/usr/bin/python3"
    },
    "changed": false,
    "ping": "pong"
```

# Automatisation de la configuration avec Ansible

Aucune installation côté client ❤️

Pourquoi Ansible n'a aucun client sur les machines de l'inventaire ?



# Automatisation de la configuration avec Ansible

Aucune installation côté client ❤️

Pourquoi Ansible n'a aucun client sur les machines de l'inventaire ?



Avec le seul accès SSH, il exécute les commandes qu'il faut. Il est agnostique à l'OS !

# Automatisation de la configuration avec Ansible

Example de “playbook”

Qu'a-t-on installé sur un Ubuntu *base server* comme package(s) pour pouvoir exécuter l'application gunicorn Hello World ?

# Automatisation de la configuration avec Ansible

Example de “playbook”

Qu'a-t-on installé sur un Ubuntu *base server* comme package(s) pour pouvoir exécuter l'application gunicorn Hello World ?

```
sudo apt-get install python3-gunicorn
```

Commande qui devient dans un playbook Ansible `unicorn.yml` :

```
---
- name: gunicorn
  hosts: gunicorn
  become: yes # Run as root
  tasks:
    - name: Install gunicorn
      apt:
        name: gunicorn # Le package à installer
        state: present
```

À lancer avec la commande :

```
$ ansible-playbook -i inventory.ini unicorn.yml
```

# Automatisation de la configuration avec Ansible

Example de “playbook”

Le résultat de l'exécution du playbook `gunicorn.yml` :

```
$ ansible-playbook -i inventory.ini gunicorn.yml
...
localhost : ok=2 changed=1 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0

$ ansible-playbook -i inventory.ini gunicorn.yml
...
localhost : ok=2 changed=0 unreachable=0 failed=0 skipped=0 rescued=0 ignored=0
```

A la première exécution, le package est installé, à la seconde il est déjà installé, aucun changement.

# Automatisation de la configuration avec Ansible

Commande pour exécuter un programme

Une fois les dépendances requises installées, on peut exécuter un programme avec le module `shell`.

Si il faut copier un ou plusieurs fichiers, on peut utiliser le module `copy`.

Par exemple :

```
---
- hosts: gunicorn # Groupe de host de l'inventory
  vars:
    - EXEC_ABS_PATH: /home/chrichri/helloworld # Utilisé 2 fois donc dans une
      variable
...
- name: Copy Application
  copy:
    src: /home/chrichri/Documents/Campus-St-Michel-IT/production-deployment/
          helloworld/build/helloworld # Le build de ma machine
    dest: "{{ EXEC_ABS_PATH }}"
...
- name: Run Application
  shell: nohup {{ EXEC_ABS_PATH }} & # nohup pour exécuter en arrière plan
```

# Automatisation de la configuration avec Ansible

## La Ansible Galaxy

Comme souvent, inutile de tout recoder. Ansible est modulaire grâce aux “roles” et aux “playbooks” qui sont eux-mêmes des modules<sup>6</sup>.

La communauté Ansible a packagé des modules et des playbooks pour les tâches les plus courantes<sup>7</sup>. Ils sont disponibles sur la [Ansible Galaxy](#). Et peuvent être installés avec la commande `ansible-galaxy install <module>`, commande issue du package `ansible-core`.

---

<sup>6</sup>Roles, [https://docs.ansible.com/ansible/latest/playbook\\_guide/playbooks\\_reuse\\_roles.html](https://docs.ansible.com/ansible/latest/playbook_guide/playbooks_reuse_roles.html)

<sup>7</sup>Ansible Galaxy, <https://galaxy.ansible.com/ui/>

# Automatisation de la configuration avec Ansible

## Ansible et Windows

Sur la machine hôte, on ne peut l'installer que depuis un WSL .

Si la machine cliente est un Windows, attention au package manager et aux séparateurs de chemin, voir [https://docs.ansible.com/ansible/latest/os\\_guide/windows\\_usage.html](https://docs.ansible.com/ansible/latest/os_guide/windows_usage.html).



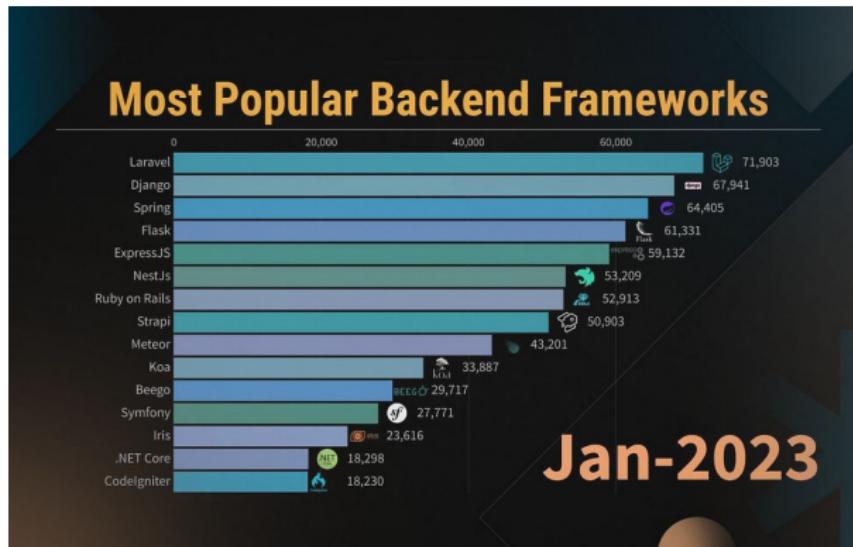
L'idéal reste quand même de ne pas utiliser Windows...

# Automatisation de la configuration avec Ansible

## Exercice 8

En utilisant la VM créée à l'exercice précédent, configurer un inventaire et un playbook pour installer l'application Spring Boot.

Vous pouvez vous aider du [tutoriel officiel](#).



# Automatisation de la configuration avec Ansible

Solution à l'exercice précédent

De nombreuses solutions sont valides. Mais avec Java il est plus simple de profiter du “Write once, run anywhere”.

Ce n'est donc pas obligé d'utiliser un système de build comme Maven ou Gradle sur la VM, Java suffit pour exécuter une JAR .

Une JAR (Java ARchive) est un exécutable qui contient toutes les classes zippées et qui se lance avec `java -jar <JAR file>`. Il suffit donc d'installer Java sur la JVM .

# Automatisation de la configuration avec Ansible

Solution à l'exercice précédent

Par exemple, une solution avec uniquement Java 17 :

```
---
- hosts: gunicorn
  vars:
    - JAR_DEST_PATH: /home/chrichri/helloworld-0.0.1-SNAPSHOT.jar
    become: yes
  tasks:
    - name: Install Java 17
      apt:
        name: openjdk-17-jdk
        state: present

    - name: Copy Spring Boot Application
      copy:
        src: /home/chrichri/Documents/Campus-St-Michel-IT/production-deployment/helloworld/build/libs/
              helloworld-0.0.1-SNAPSHOT.jar
        dest: "{{ JAR_DEST_PATH }}"

    - name: Run Spring Boot Application
      shell: nohup java -jar {{ JAR_DEST_PATH }} &
```

# Conclusion sur la virtualisation d'application dans un OS

- On sait créer et configurer une VM avec Qemu.
- On sait créer un service avec systemd pour automatiser des tâches dans la machine hôte ou la VM .
- On sait automatiser la configuration des VMs avec Ansible.

Dans la plus part des clouds privés comme OVH on peut uploader des images de VMs et les lancer.

Ces technologies sont donc compatibles avec le cloud et le on-premise.  
On a donc un déploiement sécurisé et agnostique à une infrastructure.

# Docker

## Définition

“Accelerate how you build, share, and run applications”<sup>8</sup>.

C'est un outil qui permet de créer des conteneurs qui sont des environnements isolés pour exécuter des applications.

Cet environnement portable est défini dans la `Dockerfile`.

Un autre fichier de configuration le `docker-compose.yml` permet de définir comment un ou plusieurs conteneurs communiquent entre eux et avec la machine.



9

Il utilise des outils de la machine, du kernel, `chroot` et des bibliothèques de la machine hôte pour fonctionner mais ne fait pas tourner un autre OS contrairement à la virtualisation.

<sup>8</sup>What is Docker, <https://www.docker.com/>

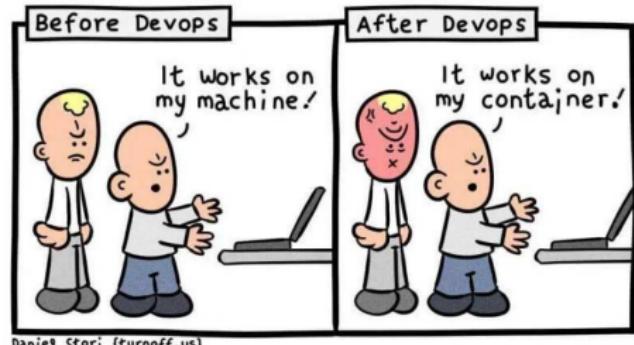
<sup>9</sup>Containers vs. virtual machines, <https://www.atlassian.com/microservices/cloud-computing/containers-vs-vms>

# Docker

## Définition

Il permet, en théorie, le déploiement de n'importe quelle application sur n'importe quelle architecture (OS, ISA)<sup>10</sup> :

- ARMv6 32-bit (arm32v6)
- ARMv7 32-bit (arm32v7)
- ARMv8 64-bit (arm64v8)
- Linux x86-64 (amd64)
- Windows x86-64 (windows-amd64)
- ARMv5 32-bit (arm32v5)
- IBM POWER LE (ppc64le)
- IBM z Systems (s390x)
- MIPS64 LE (mips64le)
- RISC-V 64-bit (riscv64)
- x86/i686 (i386)



Daniel Storii ([turnoff.us](http://turnoff.us))

<sup>10</sup>Docker official Images, <https://github.com/docker-library/official-images#architectures-other-than-amd64>

# Docker, créer une image

Définir l'image dans un Dockerfile

L'essentiel de la Dockerfile :

- Le nom de fichier par convention est `Dockerfile` mais peut être différent.
- Il vient surcharger une image de base définie dans `FROM`.
- On peut y définir des variables d'environnement avec `ENV`.
- La commande `RUN` permet d'exécuter des commandes dans l'image.  
Comme par exemple pour ajouter des dépendances dans l'étape de build de l'image.
- La commande `CMD` définit la commande qui sera exécutée au démarrage du conteneur.
- La commande `EXPOSE` définit les ports qui seront exposés par le conteneur.
- La commande `COPY` permet de copier des fichiers dans l'image.
- La commande `ADD` permet de copier des fichiers dans l'image et de les décompresser.
- *Many more...*<sup>11</sup>

<sup>11</sup>Dockerfile reference, <https://docs.docker.com/reference/dockerfile/>

# Docker, créer une image

Définir l'image dans un Dockerfile

## Que fait cette Dockerfile ?

```
FROM mysql:8-debian

ENV RNCS_PATH=/root/rncs

COPY ./ ${RNCS_PATH}
WORKDIR ${RNCS_PATH}

RUN apt-get update && \
apt-get install -y jq python3 python3-pip moreutils wget unzip libcairo2-dev && \
apt-get clean && \
apt-get autoclean && \
apt-get autoremove -y && \
python3 -m pip install --no-cache-dir -r requirements.txt && \
python3 -m pip install --no-cache-dir -r dev-requirements.txt

EXPOSE 3000/tcp
EXPOSE 5000/tcp
```

Dans la vraie vie tout est très clair grâce à des commentaires explicites 😊.



# Le Docker hub

*Docker Hub is the world's easiest way to create, manage, and deliver your team's container applications*

Encore une fois, inutile de tout recoder. On vient en premier lieu trouver une image la plus complète possible pour son application.

Il y a probablement une image pour quasi toutes les stacks existantes.

En terme de cybersécurité, veillez à auditer les développeurs des images pour ne pas subir une *supply chain attack*.

Une des bonnes pratiques est d'utiliser des images officielles. Par exemple pour Tensorflow, le développeur est Google, etc.

Concernant les performances, les images basées sur Alpine Linux sont souvent plus légères car l'OS est développées autour de `musl` `libc` et `busybox`.

# Les commandes Docker

Builder, lancer et stopper une image

Ci-dessous, quelques commandes Docker de base :

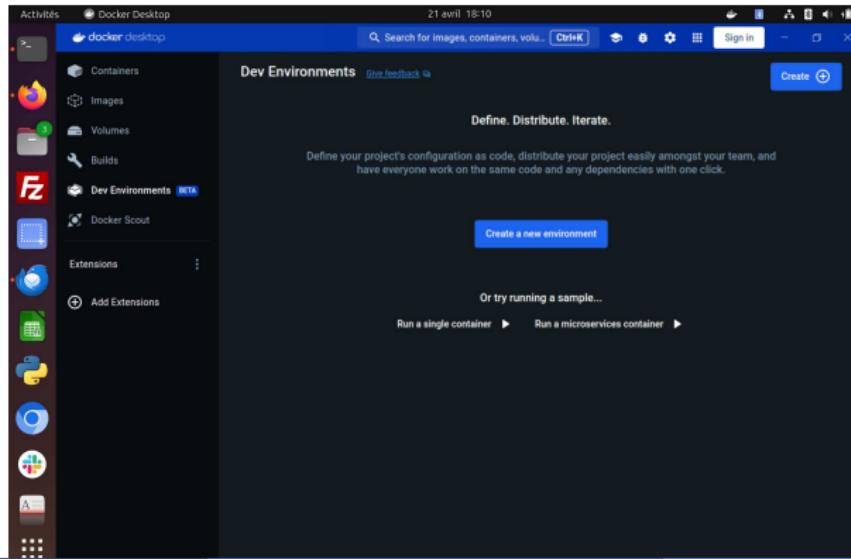
- `docker build -t <image-name>` . pour construire une image Docker.
- `docker run <image-name>` pour lancer une image Docker.
- `docker stop <container-id>` pour arrêter un conteneur.
- `docker ps` pour lister les conteneurs en cours d'exécution.
- `docker ps -a` pour lister tous les conteneurs.
- `docker images` pour lister les images.
- `docker rmi <image-id>` pour supprimer une image.
- `docker rm <container-id>` pour supprimer un conteneur.
- `docker exec -it <container-id> /bin/bash` pour accéder à un conteneur.

# Docker, créer une image

Installation d'un environnement de développement Docker

Comme le dit le site Docker, *Build, Share, Run, verify.* Tout cela est possible avec Docker Desktop. Un GUI qui centralise la plupart des fonctionnalités de Docker.

Sur la machine de production le Docker Engine suffit.



# Docker, trouver la bonne image

## Exercice 9

Sur le Docker Hub, trouvez les images pour les applications suivantes:

- Une application NodeJS .
- Une application Flask.
- OpenJDK 17.
- Alpine Linux

# Docker, créer une image

## Exercice 10

Développer une image Docker pour une application Spring Boot, la même qu'à l'exercice précédent.

Pensez à optimiser l'image pour qu'elle soit la plus légère possible et le plus sécurisé possible...



# Docker, créer une image

Une solution possible de l'exercice

Avec uniquement une image Eclipse Temurin basée sur une distribution Alpine Linux comme par exemple l'image Docker officielle `eclipse-temurin:17-alpine` on génère une image de “seulement” 360 Mo....

Eclipse Temurin est une JVM maintenue par la Fondation Eclipse, elle offre des performances élevées, la compilation en exécutable et est Java SE TCK (Technology Compatibility Kit).

C'est donc une image de choix en terme de taille, sécurité et performance.

```
FROM eclipse-temurin:17-alpine # L'image de base
EXPOSE 8081 # Le port du serveur Spring
# Le fichier JAR
COPY helloworld/build/libs/helloworld-0.0.1-SNAPSHOT.jar /app/spring-boot.jar
# Exécution de la JAR
CMD ["java", "-jar", "/app/spring-boot.jar"]
```

# Docker compose

## Le fichier de configuration Docker Compose<sup>12</sup>

Le fichier `docker-compose.yml` permet de définir comment les conteneurs communiquent entre eux et avec la machine. Limiter les ressources CPU et mémoire prise sur la machine.

Pour les applications web par exemple, il faut définir les ports qui seront exposés par les conteneurs :

```
services:  
  web:  
    build: .  
    ports:  
      - "8000:8000"  
  db:  
    image: postgres  
    ports:  
      - "8001:5432"
```

---

<sup>12</sup>Networking in Compose, <https://docs.docker.com/compose/networking/>

# Docker compose

Le fichier de configuration Docker Compose<sup>13</sup>

On y définit aussi le(s) Dockerfile(s) :

```
version: "3"

services:
  client:
    build:
      context: ../
      dockerfile: docker/Dockerfile.production
```

---

<sup>13</sup>Compose Build Specification,

<https://docs.docker.com/compose/compose-file/build/>

# Docker compose

Le fichier de configuration Docker Compose<sup>14</sup>

Les commandes pour builder, lancer et stopper les conteneurs définis dans le fichier `docker-compose.yml` :

- `docker compose build` pour construire les images.
- `docker compose up` pour lancer les conteneurs.
- `docker compose down` pour arrêter les conteneurs.
- `docker compose ps` pour lister les conteneurs en cours d'exécution.
- `docker compose ps -a` pour lister tous les conteneurs.
- `docker compose images` pour lister les images.
- `docker compose exec <container-name> /bin/bash` pour accéder à un conteneur.

Elles sont très similaires aux commandes Docker.

---

<sup>14</sup> docker compose, <https://docs.docker.com/reference/cli/docker/compose/>

# Docker compose

Exercice 11, développer une configuration Docker Compose

Un Docker compose pour un site Wordpress, ce dernier a besoin d'une base de données MySQL .

# Docker compose

Exercice 12, développer une configuration Docker Compose

Un Docker compose pour un site Wordpress, ce dernier a besoin d'une base de données MySQL .

```
services:
  db:
    image: 'mysql:8'
    env_file:
      - .env
    volumes:
      - 'db_data:/var/lib/mysql'
    restart: always
    environment:
      MYSQL_ROOT_PASSWORD: k36FbP3NH3J8
      MYSQL_DATABASE: ${WORDPRESS_DB_USER}
      MYSQL_USER: ${WORDPRESS_DB_USER}
      MYSQL_PASSWORD: ${WORDPRESS_DB_PASSWORD}
  wordpress:
    depends_on:
      - db
    image: 'wordpress:latest'
    ports:
      - '8000:80'
    restart: always
    environment:
      WORDPRESS_DB_HOST: 'db:3306'
      WORDPRESS_DB_USER: ${WORDPRESS_DB_USER}
      WORDPRESS_DB_PASSWORD: ${WORDPRESS_DB_PASSWORD}
volumes:
  db_data: null
```

# Docker compose

Exercice 13, développer une configuration Docker Compose

Des variables d'environnement comme les mots de passe, etc, sont définies dans un fichier `.env`.

Pas de build de Dockerfile donc une seule commande suffit pour lancer Wordpress :

```
$ docker compose up
```

# Kubernetes

Définition et histoire<sup>15</sup>

Kubernetes est un orchestrateur de conteneurs open-source. Il permet de déployer, de gérer et de scaler des applications conteneurisées.

Créé et libéré en open source par Google en 2014, il est maintenant maintenu par la Cloud Native Computing Foundation (CNCF) de la Linux Foundation.

Aussi appelé par son abréviation “K8s” comme k de K, 8 lettres puis un s.



<sup>15</sup>Qu'est ce que Kubernetes,

<https://kubernetes.io/fr/docs/concepts/overview/what-is-kubernetes/>

# Kubernetes

Les termes clés<sup>16</sup>

- **Cluster** : Ensemble de machines, appelées individuellement « nœuds », utilisées pour exécuter des applications conteneurisées gérées par Kubernetes.
- **Node** : Il s'agit d'une machine virtuelle ou physique. Un cluster se compose d'un nœud maître et de plusieurs nœuds de travail.
- **Pod** : Conteneur unique ou ensemble de conteneurs s'exécutant sur un cluster Kubernetes.
- **Volume** : Un répertoire qui contient des données accessibles par les conteneurs.
- **Deployment** : Objet qui gère les applications répliquées représentées par des pods. Les pods sont déployés sur les nœuds d'un cluster.

---

<sup>16</sup>Qu'est-ce que Kubernetes ?, <https://www.oracle.com/fr/cloud/cloud-native/container-engine-kubernetes/what-is-kubernetes/>

# Kubernetes

## Kubernetes Components<sup>17</sup>

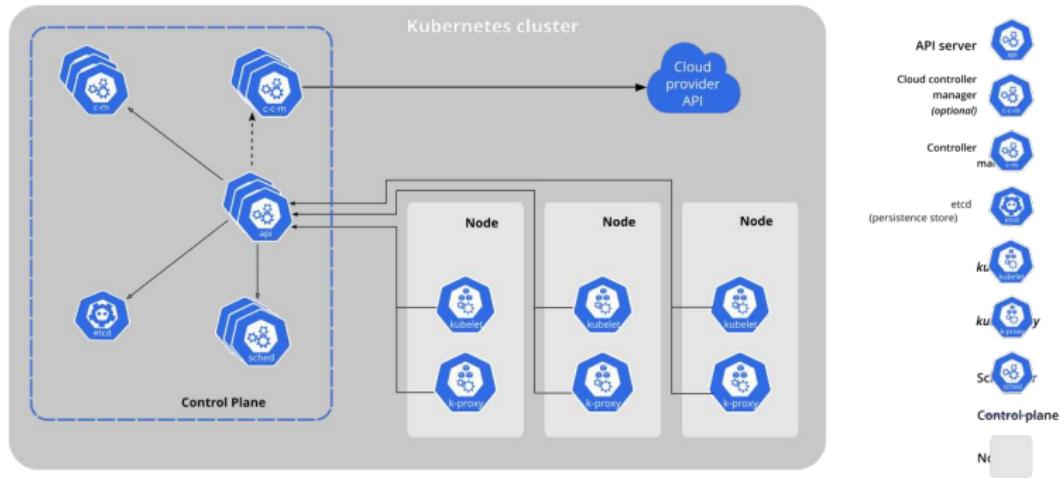
- **kube-apiserver** : Composant central qui fournit l'API Kubernetes.
- **etcd** : Stockage de données clé-valeur.
- **kube-scheduler** : Ordonnanceur qui distribue les pods sur les nœuds.
- **kube-controller-manager** : Composant qui exécute les contrôleurs.
- **kubelet** : Agent qui s'exécute sur chaque nœud du cluster. Il s'assure que les conteneurs sont en cours d'exécution dans un pod.
- **Kube-proxy** : Proxy réseau qui s'exécute sur chaque nœud du cluster.
- **Container runtime** : Gère les exécutions de manière “efficace” et leur cycle de vie des conteneurs dans l'environnement K8s.

---

<sup>17</sup>Kubernetes – Introduction à l'architecture et aux composants,  
<https://kubernetes.io/docs/concepts/overview/components/>

# Kubernetes

## Architectures<sup>17</sup>



# Kubernetes

## Addons et third party<sup>19</sup>

Développé par la communauté Kubernetes, ils apportent des fonctionnalités supplémentaires à Kubernetes. Comme par exemple l'add-on registry qui permet de stocker les images des conteneurs<sup>18</sup>.

Ceux proposés par la documentation officielle <https://kubernetes.io/docs/concepts/cluster-administration/addons/>.

D'autres sont disponibles sur le [Kubeapps](#) une application Kubernetes.

Mais bien d'autres ont été mis en open source, pas de ledger unique trouvé à l'heure actuelle.

---

<sup>18</sup> How to use the built-in registry, <https://microk8s.io/docs/registry-built-in>

<sup>19</sup> Installing Addons,

<https://kubernetes.io/docs/concepts/cluster-administration/addons/>

# Kubernetes

Les types de conteneurs supportés<sup>20</sup>

Kubernetes supporte plusieurs runtimes de conteneurs :

- Docker
- Containerd
- CRI-O
- Mirantis Container Runtime

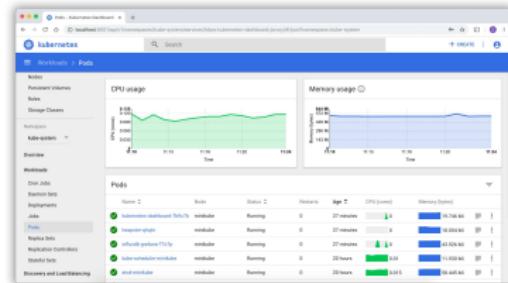
---

<sup>20</sup>Container Runtimes, <https://kubernetes.io/docs/setup/production-environment/container-runtimes/>

# Kubernetes

## Les interfaces

Le dashboard Kubernetes est une interface web qui permet de gérer les ressources du cluster<sup>21</sup>.



Il existe également une CLI, `kubectl` qui permet de gérer le cluster, elle utilise la Kubernetes API<sup>22</sup>.

La Kubernetes API qui rend le cluster accessible depuis la plupart des langages de programmation.

<sup>21</sup>Container Runtimes, <https://kubernetes.io/fr/docs/tasks/access-application-cluster/web-ui-dashboard/>

<sup>22</sup><https://kubernetes.io/docs/reference/kubectl/>

# Kubernetes

Les différentes versions<sup>23</sup>

Il existe plusieurs distributions de Kubernetes :

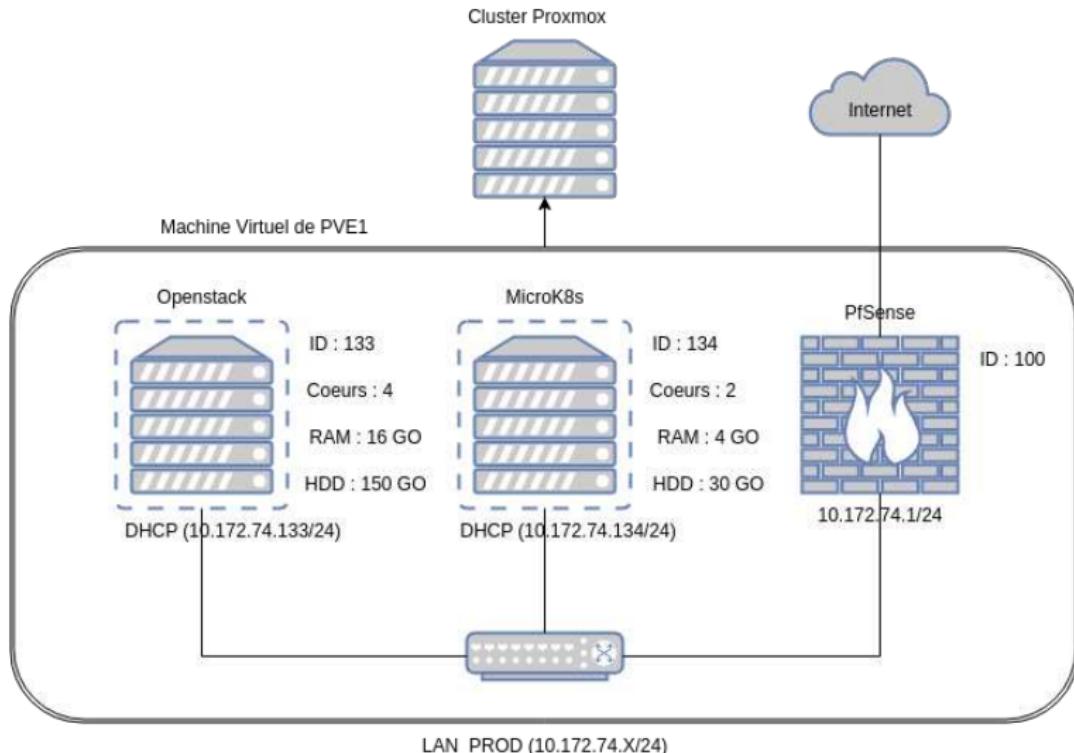
- **MicroK8s** pour des clusters de petites et moyenne taille.
- **Charmed Kubernetes** pour des cluster moyen et gros.
- **Kubeadm** un DIY Kubernetes configurable.
- Many more...

---

<sup>23</sup>How to deploy Kubernetes, <https://ubuntu.com/kubernetes/install>

# Infrastructure Kubernetes de St-Michel

Instance Micro-K8s dédiée aux exercices

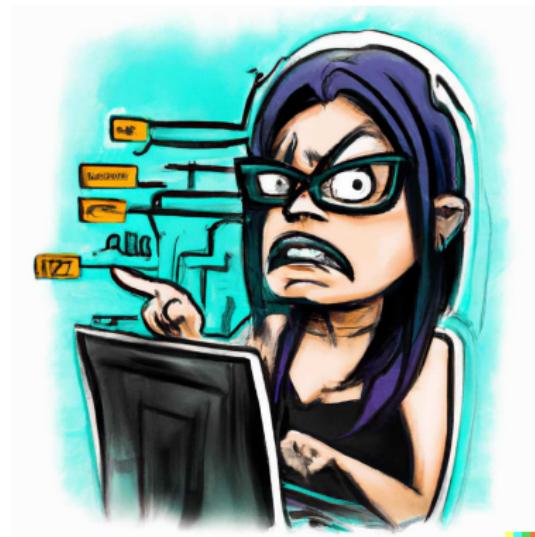


# Exercice 14 de déploiement dans Kubernetes

Exercice évalué sur le déploiement d'une application Spring Boot dans Kubernetes

Pousser l'image sur le registry de MicroK8s et exécuter l'application Spring Boot "Dockerisée" de l'avant dernier exercice dans le MicroK8s de la VM du cluster Proxmox.

L'application doit être accessible sur le réseau de St-Michel.



# Déploiement dans Kubernetes

Solution de l'exercice précédent

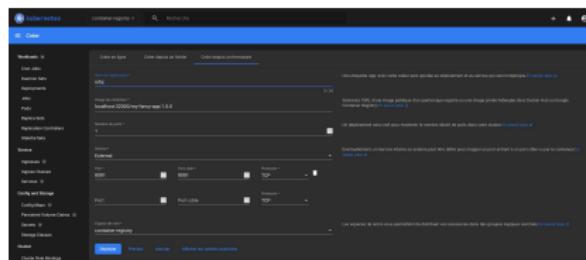
L'image est buildée et tagger sur la machine du développeur :

```
$ docker build -t 10.172.74.134:32000/my-fancy-app:1.0.0 .
```

Poussée sur le registry de MicroK8s :

```
$ docker push 10.172.74.134:32000/my-fancy-app:1.0.0
The push refers to repository [10.172.74.134:32000/my-fancy-app]
0c4cac1d4e27: Pushed
5a8f0ac5756e: Pushed
...
```

Configuration du déploiement dans la web UI :



Nom	Type	Etat	IP	Port(s)	Conditions actives	Conditions échouées
my-fancy-app	Container	En cours d'exécution	10.101.182.200	8080:80	podScheduled	
nginx-ingress-controller	Deployment	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-service	Service	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-controller-0	Container	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-controller-1	Container	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-controller-2	Container	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-service-0	Service	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-service-1	Service	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-service-2	Service	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-controller-0-0	Container	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-controller-1-0	Container	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	
nginx-ingress-controller-2-0	Container	En cours d'exécution	10.101.182.191	80:80,443:443	podScheduled	

# OpenStack

Définition<sup>24</sup>

C'est un logiciel de gestion de cloud, un “Cloud software”. On peut aussi dire que c'est un OS de cloud.

“OpenStack is a set of software components that provide common services for cloud infrastructure.”

“Cloud Infrastructure for Virtual Machines, Bare Metal, and Containers”.

“OpenStack controls large pools of compute, storage, and networking resources, all managed through APIs or a dashboard.”

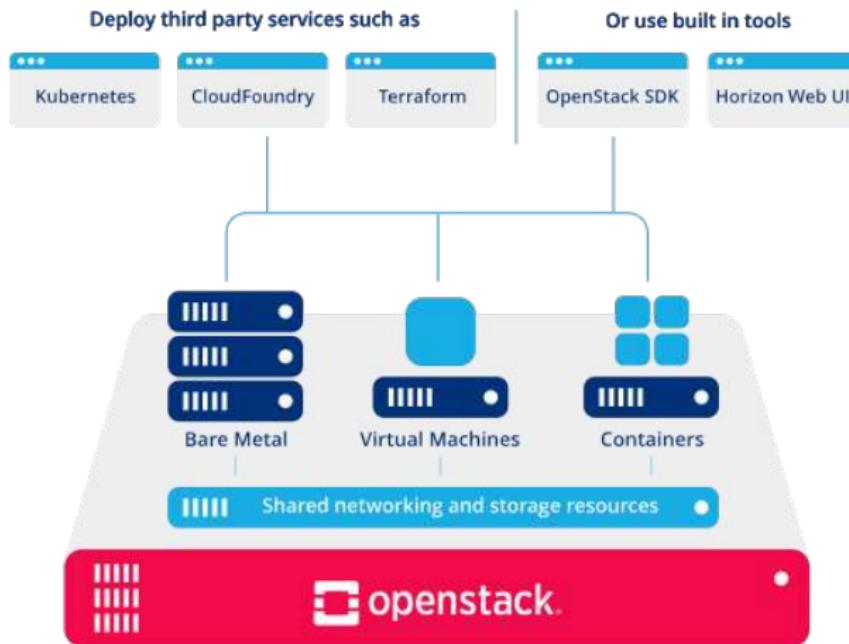
Il est en open source sous licence Apache 2.0 “OpenStack is developed by the community. For the community...”.

---

<sup>24</sup>OpenStack, <https://www.OpenStack.org/>

# OpenStack

Définition<sup>24</sup>



# OpenStack

## Histoire<sup>25</sup>

Né de la convergence des travaux de Rackspace Technology et de la NASA en 2010.

La mission initiale est “to produce a ubiquitous Open Source Cloud Computing platform that is easy to use, simple to implement, interoperable between deployments, works well at all scales, and meets the needs of users and operators of both public and private clouds”.



Une partie des supports en 2024

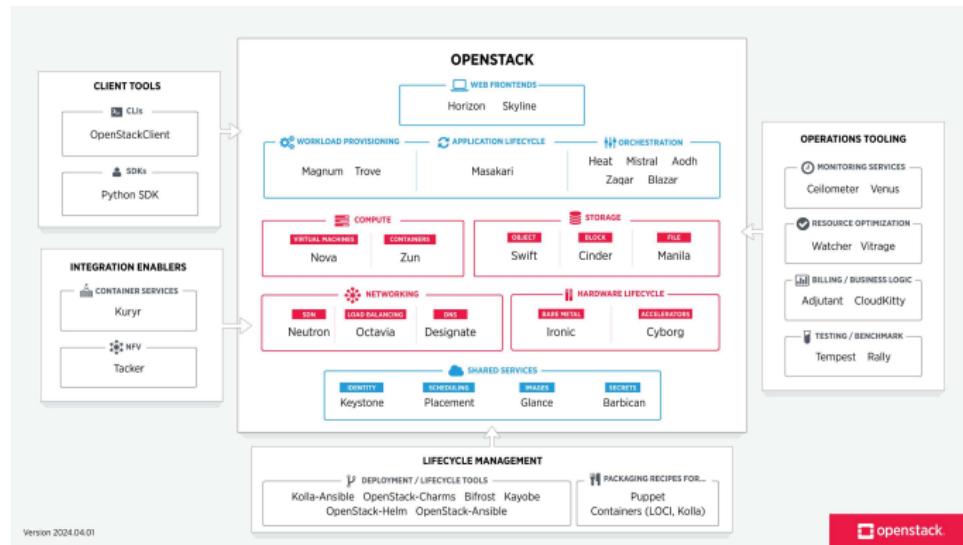
<sup>25</sup>Introduction: A Bit of OpenStack History,

<https://docs.OpenStack.org/project-team-guide/introduction.html>

# OpenStack

Les composants principaux

C'est un ensemble de services, de composants qui s'assemblent de manière "plug and play" en fonction des besoins. Encore une fois, c'est modulaire...



La liste complète des composants est sur le [site officiel](https://www.openstack.org/learn/architecture/).

# OpenStack

Les interfaces<sup>2627</sup>

Les UI web :

- **Horizon** : Le tableau de bord web d'OpenStack.
- **Skyline** : “Next generation dashboard”.

Une CLI à installer avec `pip install python-OpenStackclient`.

Un SDK Python pour les APIs OpenStack.

---

<sup>26</sup>OpenStack Services, <https://www.OpenStack.org/software/project-navigator/OpenStack-components#OpenStack-services>

<sup>27</sup>Client tools, <https://www.OpenStack.org/software/project-navigator/sdks>

# OpenStack

Résumé des fonctionnalités<sup>28</sup>

- Permet de gérer des clouds privés ou publics.
- Virtualisation des ressources.
- Stockage objet, bloc et fichier avec **Swift** et **Cinder**.
- L'authentification et les autorisations avec **Keystone**.
- Le réseau avec **Neutron**.
- Les ressources de calcul avec **Nova**.
- Gestion des conteneurs (Docker entre autre) avec **Zun**.

---

<sup>28</sup>OpenStack, qu'est-ce que c'est ?, <https://www.redhat.com/fr/topics/OpenStack>

# OpenStack

Commandes de base<sup>29</sup>

Pour ajouter une image à OpenStack :

```
$ OpenStack image create <IMAGE> --disk-format raw \
--container-format bare --public \
--file ~/images/cirros-0.3.5-x86_64-disk.img
```

Pour créer un type d'instance, appelé “flavor” : Pour lancer une instance :

```
OpenStack flavor create --ram 512 --disk 1 --vcpus 1 <FLAVOR INSTANCE_NAME>
```

Pour lancer une instance :

```
$ OpenStack server create --image <IMAGE> --flavor <FLAVOR INSTANCE_NAME>
```

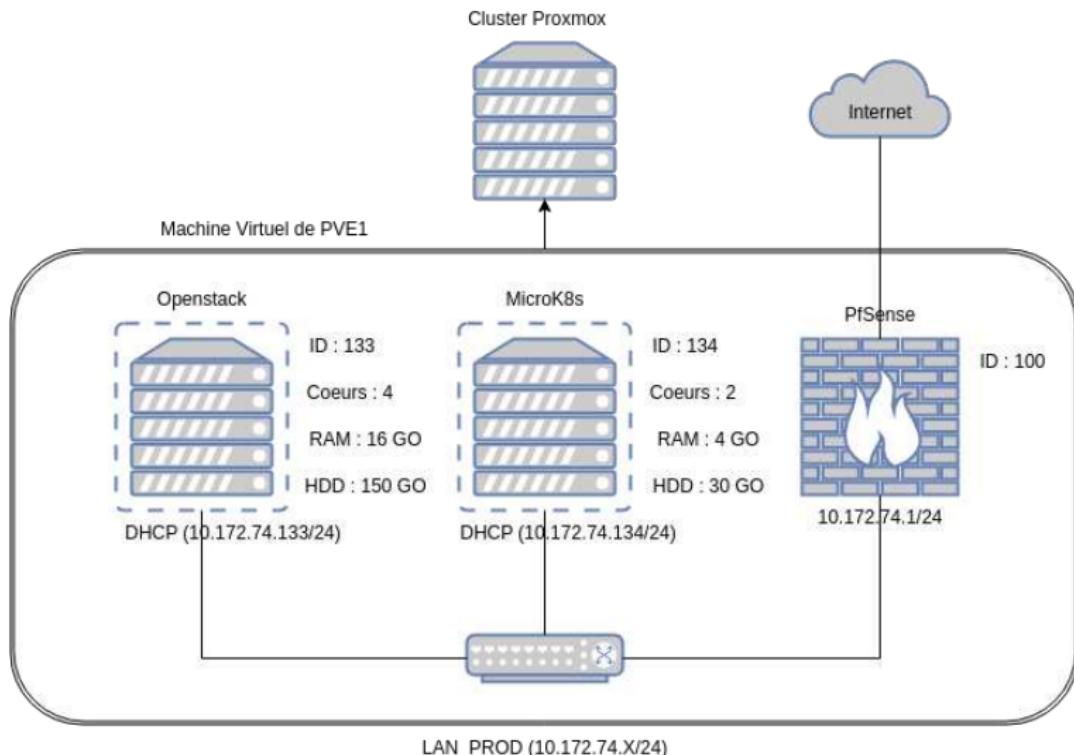
Toutes les commandes dans la [documentation officielle](#).

---

<sup>29</sup>OpenStack, qu'est-ce que c'est ?, <https://www.redhat.com/fr/topics/OpenStack>

# Infrastructure OpenStack de St-Michel

Instance OpenStack dans une VM dédiée aux exercices



# OpenStack

## Exercice 15

- Créer l'image de l'application Spring Boot dans OpenStack.
- Créer un flavor de 1 vCPU et 1 Go de RAM .
- Lancer une instance de l'application Spring Boot.
- Faire un snapshot de l'instance.
- Stopper l'instance.
- Relancer l'instance.

Réalisez ces tâches avec la CLI OpenStack et listez les commandes pour l'évaluation.

# OpenStack

## Exercice 16

- Créer un registre de conteneur dans OpenStack.
- Pousser le conteneur de l'application Spring Boot dans le registre OpenStack.
- Lancer un conteneur de l'application Spring Boot avec 1 vCPU et 1 Go de RAM maximum.
- Stopper le conteneur.

Réalisez ces tâches avec la CLI OpenStack et listez les commandes pour l'évaluation.

# Serveur Web Apache et Nginx

## Généralités

Sont souvent appelés serveur web mais font en réalité bien plus que serveur HTTP de contenu statique.

Apache peut servir du contenu dynamique grâce aux modules `mod_cgi/mod_cgid`<sup>30</sup>. De même sous Nginx (*ɛndʒin'ɛks*) avec le package `fcgiwrap`<sup>31</sup>.

Apache peut-être programmer en Python grâce à son API Python disponible dans le module `mod_cgi`<sup>32</sup>. Similaire au module `ngx_python_module` de Nginx<sup>33</sup>.

<sup>30</sup> Contenu dynamique basé sur CGI,

<https://httpd.apache.org/docs/2.4/fr/howto/cgi.html>

<sup>31</sup> Serving CGI Scripts With Nginx On Debian Squeeze/Ubuntu 11.04,

<https://www.howtoforge.com/>

[serving-cgi-scripts-with-nginx-on-debian-squeeze-ubuntu-11.04-p3](https://www.howtoforge.com/serving-cgi-scripts-with-nginx-on-debian-squeeze-ubuntu-11.04-p3)

<sup>32</sup> Mod\_python Documentation, Tutorial,

<https://modpython.org/live/current/doc-html/tutorial.html>

<sup>33</sup> Nginx Python Module,<sup>34</sup>

# Serveur Web Apache et Nginx

## Généralités

Les moyens utilisés ont les mêmes capacités, servir du contenu dynamique, mais les performances diffèrent<sup>35</sup>.

Server	Version	Req/s	% of httpd static	Notes
<a href="#">nxweb static file</a>	3.2.0-dev	512,767	347.1 %	“memcache”:false. (626,270 if true)
<a href="#">nginx static file</a>	1.0.15	430,135	291.1 %	stock CentOS 6.3 rpm
<a href="#">httpd static file</a>	2.4.4, mpm_event	147,746	100.0 %	
<a href="#">mod_python handler</a>	3.5, Python 2.7.5	125,139	84.7 %	
<a href="#">uWSGI</a>	1.9.18.2	119,175	80.7 %	-p 16 –threads 1
<a href="#">mod_python wsgi</a>	3.5, Python 2.7.5	87,304	59.1 %	
<a href="#">mod_wsgi</a>	3.4	76,251	51.6 %	embedded mode
<a href="#">nxweb wsgi</a>	3.2.0-dev, Python 2.7.5	15,141	10.2 %	possibly misconfigured?

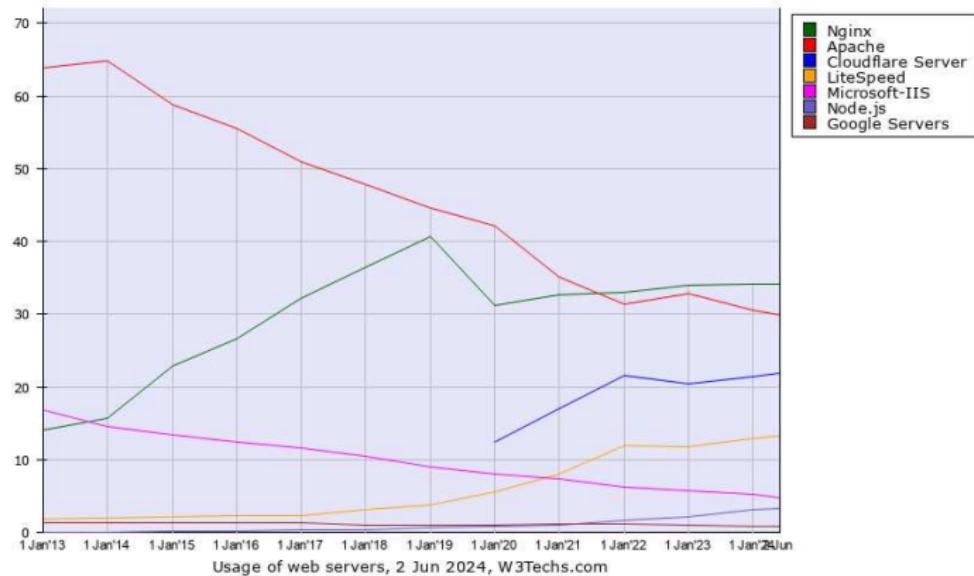
<sup>35</sup>Mod\_python Performance Part 2,

<https://grisha.org/blog/2013/11/07/mod-python-performance-revisited/>

# Serveur Web Apache et Nginx

## Généralités

Apache et Nginx dominent le monde des serveurs web<sup>36</sup>.



<sup>36</sup>Historical yearly trends in the usage statistics of web servers,  
[https://w3techs.com/technologies/overview/web\\_server](https://w3techs.com/technologies/overview/web_server)

# Serveur Web Apache et Nginx

## Généralités

Exécuter du PHP, Apache est souvent utilisé avec `mod_php`<sup>37</sup> et Nginx avec `php-fpm`<sup>38</sup> par exemple.

Dans tous ces cas vus précédemment, Apache et Nginx sont utilisés comme serveur web que ce soit pour du contenu statique ou dynamique.

Mais dans de nombreux cas, ils sont utilisés comme reverse proxy. Les technologies vues aux chapitres précédents comme Spring et Flask/Gunicorn ont déjà un serveur web intégré. Spring a un serveur Tomcat embarqué et Flask/Gunicorn utilise Gunicorn comme serveur HTTP de production.

---

<sup>37</sup> How to install and configure PHP,

<https://ubuntu.com/server/docs/how-to-install-and-configure-php>

<sup>38</sup> PHP FPM pour Nginx, <https://grafikart.fr/tutoriels/php-fpm-nginx-693>

# Serveur Web Apache et Nginx

## Exercices 17 et 18

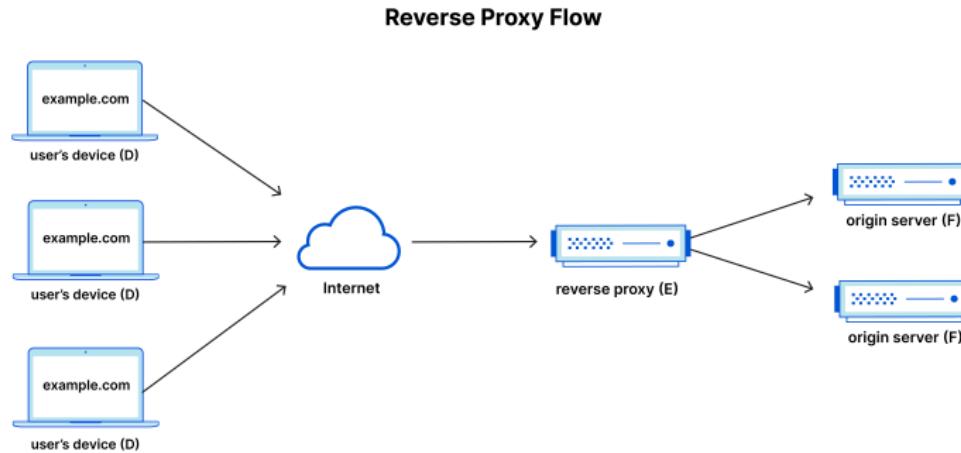
Servir sur un port/domaine des pages statiques avec Apache ou Nginx.

Servir sur un autre port/domaine, du contenu dynamique avec l'autre serveur un script CGI minimaliste. Par exemple, servir sous la même URL “Hello World” ou “Bonjour le monde” ou “Hola a todos” de manière pseudo-aléatoire.

# Apache et Nginx

## Reverse Proxy<sup>39</sup>

Un Reverse Proxy est un serveur qui reçoit des requêtes de clients et les redirige vers un autre serveur. Il permet d'avoir moins de points d'entrée dans le réseau, d'IP par exemple, que de serveurs.



<sup>39</sup>What is a reverse proxy?,

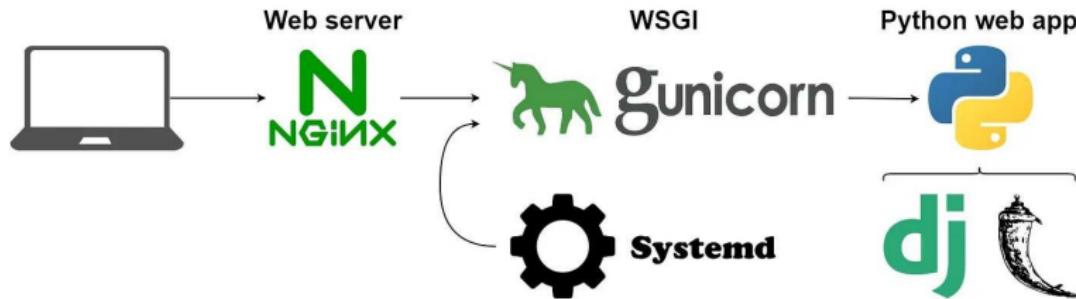
<https://www.cloudflare.com/learning/cdn/glossary/reverse-proxy/>

# Apache et Nginx

## Exemple de configuration de Reverse Proxy

Par exemple, pour limiter les besoins en infra, le Reverse Proxy redirige les requêtes vers les serveurs d'application. De telle manière qu'on peut avoir plusieurs services sur un même VPS et avec une seul IP pour diminuer les coûts.

La configuration du Reverse Proxy consiste à faire correspondre un domaine à un port. Comme on a de nombreux ports sur une machine peut s'adresser à plusieurs domaines alors qu'on a qu'une IP .



# Apache et Nginx

Exemple de configuration de Reverse Proxy sur un port

Les configurations Nginx sont dans le dossier `/etc/nginx/sites-available/`.  
On peut ajouter le fichier `yourdomain` suivant :

```
server {
    listen 80;
    listen [::]:80;

    server_name your_domain;

    location / {
        proxy_pass http://localhost:8001;
        include proxy_params;
    }
}
```

Cette configuration associe les domaines `your_domain` au serveur d'application bindé au port 8001.

# Apache et Nginx

## Exemple de configuration de Reverse Proxy sur un socket Unix

Pour plus de performances et de sécurité, quand c'est possible, il est recommandé d'utiliser un Unix Domain Socket. C'est une communication inter-processus qui ne passe pas par le réseau mais par le file system, donc plus rapide. Par contre il est limité à une machine, car on a un file system par machine.

```
server {
    listen 80;
    listen [::]:80;

    server_name your_domain;

    location / {
        proxy_pass http://unix:/var/run/sock-guni;
        include proxy_params;
    }
}
```

De son côté, Gunicorn est bindé sur ce même socket Unix :

```
gunicorn app.py -b /var/run/sock-guni
```

# Apache et Nginx

Exercice 19 et 20, développer une configuration de Reverse Proxy

Dans la VM de l'exercice précédent, configurer un Reverse Proxy pour servir l'application Gunicorn. Le Reverse Proxy et l'application doivent communiquer par un socket Unix.

A l'aide d'un `docker-compose.yml` déployer un serveur Nginx et l'application Spring déjà conteneurisée dans un précédent exercice. Les deux doivent communiquer par TCP/IP .

# Apache et Nginx

## Exemple de configuration avec un certificat SSL

Les standards modernes de sécurité web recommandent très fortement le HTTPS et l'utilisation de certificat SSL . Les clients de votre application en sont demandeur aussi.

On peut l'acheter chez une autorité (CA) de certification comme Comodo ou autre. Pour seulement quelques centaines ou milliers d'Euros par an  . Ou on peut utiliser Let's Encrypt qui est gratuit.

Let's Encrypt est un projet de CA de la "Internet Security Research Group" (ISRG) qui fournit des certificats SSL gratuits. Il est sponsorisé par de nombreuses entreprises du numérique.

Le moyen le plus simple de l'installer sur votre serveur, dans votre configuration Nginx ou Apache est d'utiliser certbot<sup>40</sup>.

---

<sup>40</sup>Certbot, <https://certbot.eff.org/>

# Apache et Nginx

Exemple de configuration avec un certificat SSL

Avec les droits root ou en sudoer, certbot installe le certificat et modifie la configuration Nginx ou Apache.

La commande suivante :

```
$ sudo certbot --nginx -d your_domain
```

Modifie la configuration comme suit :

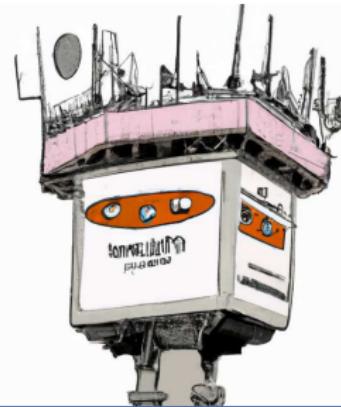
```
server {  
    listen 443 ssl; # Managed by Certbot  
  
    ssl on; # Managed by Certbot  
    ssl_certificate /etc/letsencrypt/live/your_domain/fullchain.pem; # Managed by Certbot  
    ssl_certificate_key /etc/letsencrypt/live/your_domain/privkey.pem; # Managed by Certbot  
  
    server_name your_domain;  
  
    location / {  
        proxy_pass http://unix:/var/run.sock-guni;  
        include proxy_params;  
    }  
}  
  
server {  
    listen 80 default_server; # Managed by Certbot  
    server_name your_domain; # Managed by Certbot  
    return 301 https://$host$request_uri; # Managed by Certbot  
}
```

# Apache et Nginx

Exemple de configuration avec un certificat SSL

Les outils présentés dans ce chapitre ont pour but de mesurer les performances des systèmes, réseaux et applications web. Ils permettent de collecter des données pour d'être plus réactif face à un incident passé ou à venir.

C'est une liste non exhaustive, celle du programme officiel 3IL . Mais il en existe bien d'autres comme Graphana, Prometheus, Naemon, journalctl, grep, etc.



# Syslog

Créer une journalisation sur mesure

Protocole de transmission de messages de journalisation. Crée haut dessus d'autres protocoles comme UDP ou TCP .

Il est utilisé pour centraliser les logs des serveurs, des applications, des équipements réseaux, du noyau, etc.

Il a une partie serveur, le démon `syslogd`, et une partie client, `syslog` . `syslog` envoie les messages à `syslogd` qui les centralise ou les envoie à un autre serveur à la façon d'un proxy.

Il a plus de sources de messages que `journalctl` vu précédemment.

Il est disponible sur les OS Linux et Unix...

# Syslog

Paramétrer la journalisation<sup>41</sup>

Le fichier de configuration est `/etc/rsyslog.conf` .

On peut y sélectionner 8 niveaux de priorité :

- **debug** : Messages de débogage.
- **info** : Messages d'information.
- **notice** : Messages normaux mais significatifs.
- **warning** : Messages d'avertissement.
- **err** : Messages d'erreur.
- **crit** : Messages critiques.
- **alert** : Messages d'alerte.
- **emerg** : Messages d'urgence.

---

<sup>41</sup>Les événements système de syslog,

<https://debian-handbook.info/browse/fr-FR/stable/sect.syslog.html>

# Syslog

Paramétrer la journalisation<sup>41</sup>

Et ce pour les catégories suivantes :

- **auth** : Authentification.
- **authpriv** : Authentification privée.
- **cron** : Tâches planifiées.
- **daemon** : Démon système.
- **kern** : Noyau.
- **lpr** : Impression.
- **mail** : Mail.
- **news** : News.
- **syslog** : Syslog.
- **user** : Utilisateur.
- **uucp** : UUCP.
- **local0 à local7** : Utilisateurs.

# Syslog

Exemple de configuration<sup>42</sup>

Et ce pour les catégories suivantes :

```
# On va sauvegarder les logs de tous les niveaux de priorité des "daemons" dans
# le fichier "daemons-tout.log" dans "/var/log/".
daemon.* /var/log/daemons-tout.log
# On va sauvegarder que les messages "d'erreurs d'authentification" dans le
# fichier "login-erreur.log" dans "/var/log/".
auth.err /var/log/login-erreur.log
# On va mettre plusieurs "services" pour une même destination en utilisant le
# ";".
daemon.*; auth.err /var/log/test.log
# On va mettre plusieurs "catégories" pour le même niveau de "priorité » avec le
# signe « , ».
kern,daemon.info /var/log/mail_news
```

---

<sup>42</sup>Configurer la gestion du serveur de logs,

[http://www.octetmalin.net/linux/tutoriels/  
syslog-configurer-gestion-serveur-logs-fichier-syslog.conf.php](http://www.octetmalin.net/linux/tutoriels/syslog-configurer-gestion-serveur-logs-fichier-syslog.conf.php)