



DOSSIER PROFESSIONNEL (DP)

Nom de naissance ▶ Malet
Nom d'usage ▶ Malet
Prénom ▶ Raphaël
Adresse ▶ 27 avenue talabot 13007, Marseille

Titre professionnel visé

Administrateur d'infrastructures sécurisées

MODALITÉ D'ACCÈS :

- ☐ Parcours de formation
- ☐ Validation des Acquis de l'Expérience (VAE)

Présentation du dossier

Le dossier professionnel (DP) constitue un élément du système de validation du titre professionnel. **Ce titre est délivré par le Ministère chargé de l'emploi.**

Le DP appartient au candidat. Il le conserve, l'actualise durant son parcours et le présente **obligatoirement à chaque session d'examen.**

Pour rédiger le DP, le candidat peut être aidé par un formateur ou par un accompagnateur VAE.
Il est consulté par le jury au moment de la session d'examen.

Pour prendre sa décision, le jury dispose :

1. des résultats de la mise en situation professionnelle complétés, éventuellement, du questionnaire professionnel ou de l'entretien professionnel ou de l'entretien technique ou du questionnement à partir de productions.
2. du **Dossier Professionnel** (DP) dans lequel le candidat a consigné les preuves de sa pratique professionnelle
3. des résultats des évaluations passées en cours de formation lorsque le candidat évalué est issu d'un parcours de formation
4. de l'entretien final (dans le cadre de la session titre).

[Arrêté du 22 décembre 2015, relatif aux conditions de délivrance des titres professionnels du ministère chargé de l'Emploi]

Ce dossier comporte :

- pour chaque activité-type du titre visé, un à trois exemples de pratique professionnelle ;
- un tableau à renseigner si le candidat souhaite porter à la connaissance du jury la détention d'un titre, d'un diplôme, d'un certificat de qualification professionnelle (CQP) ou des attestations de formation ;
- une déclaration sur l'honneur à compléter et à signer ;
- des documents illustrant la pratique professionnelle du candidat (facultatif)
- des annexes, si nécessaire.

DOSSIER PROFESSIONNEL ^(DP)

Pour compléter ce dossier, le candidat dispose d'un site web en accès libre sur le site.



<http://travail-emploi.gouv.fr/titres-professionnels>

Sommaire

Exemples de pratique professionnelle

Administrer et sécuriser les infrastructures

p.2

- Installation et configuration de wazuh pour administrer une infrastructure.

p.2

Concevoir et mettre en œuvre une solution en réponse à un besoin d'évolution

p.14

- Mise en place d'un serveur de supervision pour une parc informatique, utilisation de prometheus et Graphana

p.14

Participer à la gestion de la cybersécurité

p.36

- Analyse de risque d'une entreprise plus mise en place de plan de remédiation

p.36

Déclaration sur l'honneur

p.

Documents illustrant la pratique professionnelle (facultatif)

p.

Annexes (Si le RC le prévoit)

p.

EXEMPLES DE PRATIQUE PROFESSIONNELLE

Activité-type 1 Administrer et sécuriser les infrastructures

Exemple n°1 - Mise en place d'un EDR dans un parc informatique

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Dans ce projet, nous allons utiliser une machine tournant sous debian, dans mon cas, j'ai utilisé une machine virtuelle.

Pour installer l'agent wazuh sur notre machin, nous allons avoir besoin de télécharger les deux paquets suivant :

curl -sO <https://packages.wazuh.com/4.9/wazuh-install.sh>

curl -sO <https://packages.wazuh.com/4.9/config.yml>

Ces fichiers nous permettent d'avoir un script pour nous faciliter l'installation de notre agent sur notre machine, et une fichiers de configuration.

une fois ces deux fichier télécharger, on va éditer le fichier **config.yml**

une fois dans le fichier, on va renseigner les ip de nos différents services, dans notre cas, on utilise l'ip de notre machine :

```
nodes:
  # Wazuh indexer nodes
  indexer:
    - name: node-1
      ip: "ip-machine"
    #- name: node-2
    # ip: "<indexer-node-ip>"
    #- name: node-3
    # ip: "<indexer-node-ip>"

  # Wazuh server nodes
  # If there is more than one Wazuh server
  # node, each one must have a node_type
  server:
```

```
- name: wazuh-1
  ip: "ip-machine"
# node_type: master
#- name: wazuh-2
# ip: "<wazuh-manager-ip>"
# node_type: worker
#- name: wazuh-3
# ip: "<wazuh-manager-ip>"
# node_type: worker

# Wazuh dashboard nodes
dashboard:
  - name: dashboard
    ip: "ip-machine"
```

une fois notre fichier de configuration, correctement configuré, on peut générer nos fichier de config, si on a plusieurs node, pour la suite le transférer sur les autres serveur, pour se faire, on utilise la commande suivante :

```
sudo bash wazuh-install.sh --generate-config-files
```

On peut copier ce fichier **.tar** sur nos autres serveurs au besoin.

Nous pouvons maintenant passer à l'installation de wazuh indexer :

On installe wazuh-install.sh avec la commande suivante :

```
#Facultatif
curl -sO https://packages.wazuh.com/4.9/wazuh-install.sh
```

Une fois cela fait, on peut lancer l'installation avec :

```
sudo bash wazuh-install.sh --wazuh-indexer node-1
```

```
raph@Ubuntu:~/wazuh$ ls
wazuh-install-files.tar wazuh-install.sh
raph@Ubuntu:~/wazuh$ sudo bash wazuh-install.sh --wazuh-indexer node-1
28/10/2024 11:45:53 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.1
28/10/2024 11:45:53 INFO: Verbose logging redirected to /var/log/wazuh-install.log
28/10/2024 11:45:57 INFO: --- Dependencies ---
28/10/2024 11:45:57 INFO: Installing gawk.
28/10/2024 11:46:01 INFO: Verifying that your system meets the recommended minimum hardware requirements.
28/10/2024 11:46:05 INFO: --- Dependencies ---
28/10/2024 11:46:05 INFO: Installing apt-transport-https.
28/10/2024 11:46:12 INFO: Wazuh repository added.
28/10/2024 11:46:12 INFO: --- Wazuh indexer ---
28/10/2024 11:46:12 INFO: Starting Wazuh indexer installation.
28/10/2024 11:47:49 INFO: Wazuh indexer installation finished.
28/10/2024 11:47:49 INFO: Wazuh indexer post-install configuration finished.
28/10/2024 11:47:49 INFO: Starting service wazuh-indexer.
28/10/2024 11:48:08 INFO: wazuh-indexer service started.
28/10/2024 11:48:08 INFO: Initializing Wazuh indexer cluster security settings.
28/10/2024 11:48:11 INFO: Wazuh indexer cluster initialized.
28/10/2024 11:48:11 INFO: --- Dependencies ---
28/10/2024 11:48:11 INFO: Removing gawk.
28/10/2024 11:48:16 INFO: Installation finished.
raph@Ubuntu:~/wazuh$
```

Si on a plusieurs indexer-nodes, il faut répéter cette action sur tous nos index.

Nous allons maintenant passer à l'initialisation d'un cluster :

La dernière étape de notre installation pour notre node, est de lancer le script de sécurité d'admin.

On doit lancer l'assistant d'installation avec l'option `--start-cluster` sur tous nos index node avec la commande :

```
sudo bash wazuh-install.sh --start-cluster
```




```
raph@Ubuntu:~/wazuh$ sudo bash wazuh-install.sh --start-cluster
28/10/2024 11:53:15 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.1
28/10/2024 11:53:15 INFO: Verbose logging redirected to /var/log/wazuh-install.log
28/10/2024 11:53:19 INFO: --- Dependencies ---
28/10/2024 11:53:19 INFO: Installing gawk.
28/10/2024 11:53:23 INFO: Verifying that your system meets the recommended minimum hardware requirements.
28/10/2024 11:53:27 INFO: Wazuh indexer cluster security configuration initialized.
28/10/2024 11:53:39 INFO: Updating the internal users.
28/10/2024 11:53:41 INFO: A backup of the internal users has been saved in the /etc/wazuh-indexer/internalusers-backup folder.
28/10/2024 11:53:50 INFO: --- Dependencies ---
28/10/2024 11:53:50 INFO: Removing gawk.
28/10/2024 11:53:54 INFO: Wazuh indexer cluster started.
raph@Ubuntu:~/wazuh$
```

On peut maintenant tester si notre cluster est fonctionnel :

On doit dans un premier temps, lancer cette commande pour obtenir le MDP Admin :

```
sudo tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "'admin'" -A 1
```

```
raph@Ubuntu:~/wazuh$ sudo tar -axf wazuh-install-files.tar wazuh-install-files/wazuh-passwords.txt -O | grep -P "'admin'" -A 1
indexer_username: 'admin'
indexer_password: '6r?d+A3hr1BRUluJw7y7WebuoxBNr2T9'
raph@Ubuntu:~/wazuh$
```

Une fois le password obtenu, on peut lancer cette commande pour voir si notre node est correctement lancé :

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200
```

```
raph@Ubuntu:~/wazuh$ curl -k -u admin:6r?d+A3hr1BRUluJw7y7WebuoxBNr2T9 https://192.168.61.190:9200

{
  "name" : "node-1",
  "cluster_name" : "wazuh-indexer-cluster",
  "cluster_uuid" : "x0rA3sLsR9KnB0reFRVBZw",
  "version" : {
    "number" : "7.10.2",
    "build_type" : "deb",
    "build_hash" : "df77813b351f3b8729809c90f18e6f4509e045f5",
    "build_date" : "2024-10-15T17:46:28.890396Z",
    "build_snapshot" : false,
    "lucene_version" : "9.10.0",
    "minimum_wire_compatibility_version" : "7.10.0",
    "minimum_index_compatibility_version" : "7.0.0"
  },
  "tagline" : "The OpenSearch Project: https://opensearch.org/"
}
raph@Ubuntu:~/wazuh$
```

On peut lancer cette commande pour voir si notre cluster fonctionne correctement :

```
curl -k -u admin:<ADMIN_PASSWORD> https://<WAZUH_INDEXER_IP>:9200/_cat/nodes?v
```

```
raph@Ubuntu:~/wazuh$ curl -k -u admin:6r?d+A3hr1BRUluJw7y7WebuoxBNr2T9 https://192.168.61.190:9200/_cat/nodes?v
ip      heap.percent ram.percent cpu load_1m load_5m load_15m node.role node.roles cluster_manager name
192.168.61.190 42      92      0      0.00    0.18    0.27 dimr   data,ingest,master,remote_cluster_client * node-1
```

Nous allons passer à l'installation de notre service Serveur.

Une fois cela fait, on peut lancer l'installation de wazuh serveur, faites attention, regardez bien que vous avez votre fichier `.tar`` dans votre dossier actuel d'installation.

```
sudo bash wazuh-install.sh --wazuh-server wazuh-1
```

```
raph@Ubuntu:~/wazuh$ ls
wazuh-install-files.tar wazuh-install.sh
raph@Ubuntu:~/wazuh$ sudo bash wazuh-install.sh --wazuh-server wazuh-1
[sudo] Mot de passe de raph :
28/10/2024 12:45:07 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.1
28/10/2024 12:45:07 INFO: Verbose logging redirected to /var/log/wazuh-install.log
28/10/2024 12:45:12 INFO: --- Dependencies ---
28/10/2024 12:45:12 INFO: Installing gawk.
28/10/2024 12:45:16 INFO: Verifying that your system meets the recommended minimum hardware requirements.
28/10/2024 12:45:23 INFO: Wazuh repository added.
28/10/2024 12:45:24 INFO: --- Wazuh server ---
28/10/2024 12:45:24 INFO: Starting the Wazuh manager installation.
28/10/2024 12:47:16 INFO: Wazuh manager installation finished.
28/10/2024 12:47:16 INFO: Wazuh manager vulnerability detection configuration finished.
28/10/2024 12:47:16 INFO: Starting service wazuh-manager.
28/10/2024 12:47:36 INFO: wazuh-manager service started.
28/10/2024 12:47:36 INFO: Starting Filebeat installation.
28/10/2024 12:47:50 INFO: Filebeat installation finished.
28/10/2024 12:47:51 INFO: Filebeat post-install configuration finished.
28/10/2024 12:47:55 INFO: The filebeat.yml file has been updated to use the Filebeat KeyStore username and password.
28/10/2024 12:48:17 INFO: Starting service filebeat.
28/10/2024 12:48:20 INFO: filebeat service started.
28/10/2024 12:48:20 INFO: --- Dependencies ---
28/10/2024 12:48:20 INFO: Removing gawk.
28/10/2024 12:48:28 INFO: Installation finished.
raph@Ubuntu:~/wazuh$
```

Bravo, vous venez d'installer wazuh serveur sur votre machine, on va maintenant passer à l'installation de l'interface graphique :

On peut maintenant passer à l'installation de wazuh-dashboard, avec la commande :

```
sudo bash wazuh-install.sh --wazuh-dashboard dashboard
```

par défaut, le serveur utilise le port 443, mais on peut changer ce port avec l'option : **-p** ou **--port <port-number>**

Dans notre cas, on va garder le port par défaut.

```
raph@Ubuntu:~/wazuh$ sudo bash wazuh-install.sh --wazuh-dashboard dashboard
28/10/2024 12:52:57 INFO: Starting Wazuh installation assistant. Wazuh version: 4.9.1
28/10/2024 12:52:57 INFO: Verbose logging redirected to /var/log/wazuh-install.log
28/10/2024 12:53:04 INFO: --- Dependencies ---
28/10/2024 12:53:04 INFO: Installing gawk.
28/10/2024 12:53:11 INFO: Verifying that your system meets the recommended minimum hardware requirements.
28/10/2024 12:53:11 INFO: Wazuh web interface port will be 443.
28/10/2024 12:53:18 INFO: --- Dependencies ---
28/10/2024 12:53:18 INFO: Installing debhelper.
28/10/2024 12:53:38 INFO: Wazuh repository added.
28/10/2024 12:53:38 INFO: --- Wazuh dashboard ---
28/10/2024 12:53:38 INFO: Starting Wazuh dashboard installation.
28/10/2024 12:54:55 INFO: Wazuh dashboard installation finished.
28/10/2024 12:54:55 INFO: Wazuh dashboard post-install configuration finished.
28/10/2024 12:54:55 INFO: Starting service wazuh-dashboard.
28/10/2024 12:54:56 INFO: wazuh-dashboard service started.
28/10/2024 12:55:20 INFO: Initializing Wazuh dashboard web application.
28/10/2024 12:55:20 INFO: Wazuh dashboard web application initialized.
28/10/2024 12:55:20 INFO: --- Summary ---
28/10/2024 12:55:20 INFO: You can access the web interface https://192.168.61.190:443
    User: admin
    Password: 6r?d+A3hr1BRUluJw7y7WebuoxBNr2T9
28/10/2024 12:55:20 INFO: --- Dependencies ---
28/10/2024 12:55:20 INFO: Removing gawk.
28/10/2024 12:55:25 INFO: Installation finished.
raph@Ubuntu:~/wazuh$
```

Ici, on voit toutes les informations pour accéder à notre interface web :

lien : <https://192.168.61.190:443>

User : admin

Password : 6r?d+A3hr1BRUluJw7y7WebuoxBNr2T9

Nous allons maintenant mettre en place un agent sur une machine. Pour ce faire, nous allons nous rendre sur notre interface web, et nous rendre dans la section suivante :

Wazuh > Menu > Server Management > Endpoints Summary > Deploy New Agent

DOSSIER PROFESSIONNEL (DP)

Deploy new agent

Close

1

Select the package to download and install on your system:

LINUX

☐ RPM amd64

☐ RPM aarch64

☐ DEB amd64

☐ DEB aarch64

WINDOWS

☒ MSI 32/64 bits

macOS

☐ Intel

☐ Apple silicon

For additional systems and architectures, please check our [documentation](#).

2

Server address:

This is the address the agent uses to communicate with the server. Enter an IP address or a fully qualified domain name (FQDN).

Assign a server address

10.0.0.198

☐ Remember server address

3

Optional settings:

By default, the deployment uses the hostname as the agent name. Optionally, you can use a different agent name in the field below.

Assign an agent name

Windows

The agent name must be unique. It can't be changed once the agent has been enrolled.

Select one or more existing groups

default

4

Run the following commands to download and install the agent:

```
Invoke-WebRequest -Uri https://packages.wazuh.com/4.x/windows/wazuh-agent-4.8.0-1.msi -OutFile $(env:tmp)\wazuh-agent.msi; msisec.exe /i $(env:tmp)\wazuh-agent /q WAZUH_MANAGER=10.0.0.198 WAZUH_AGENT_GROUP="default" WAZUH_AGENT_NAME="Windows"
```

Requirements

- You will need administrator privileges to perform this installation.
- PowerShell 3.0 or greater is required.

Keep in mind you need to run this command in a Windows PowerShell terminal.

5

Start the agent:

```
NET START WazuhSvc
```

Close

Une fois l'agent télécharger, nous allons maintenant installer l'agent sur notre machine.

DOSSIER PROFESSIONNEL-Version du 01/06/2016

Page 9

```
debian@debian:~$ wget https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.1-1_amd64.deb && sudo WAZUH_MANAGER='192.168.0.128' dpkg -i ./wazuh-agent_4.9.1-1_amd64.deb
--2024-10-29 18:46:01-- https://packages.wazuh.com/4.x/apt/pool/main/w/wazuh-agent/wazuh-agent_4.9.1-1_amd64.deb
Résolution de packages.wazuh.com (packages.wazuh.com)... 3.165.136.37, 3.165.136.126, 3.165.136.42, ...
Connexion à packages.wazuh.com (packages.wazuh.com)|3.165.136.37|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 10767678 (10M) [application/vnd.debian.binary-package]
Sauvegarde en : « wazuh-agent_4.9.1-1_amd64.deb »

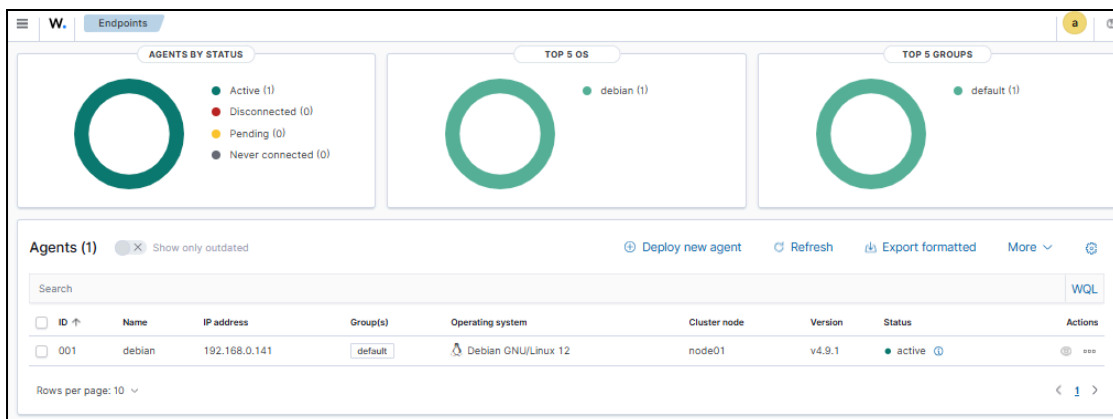
wazuh-agent_4.9.1-1_amd 100%[=====>] 10,27M 46,1MB/s ds 0,2s

2024-10-29 18:46:01 (46,1 MB/s) - « wazuh-agent_4.9.1-1_amd64.deb » sauvegardé [10767678/10767678]

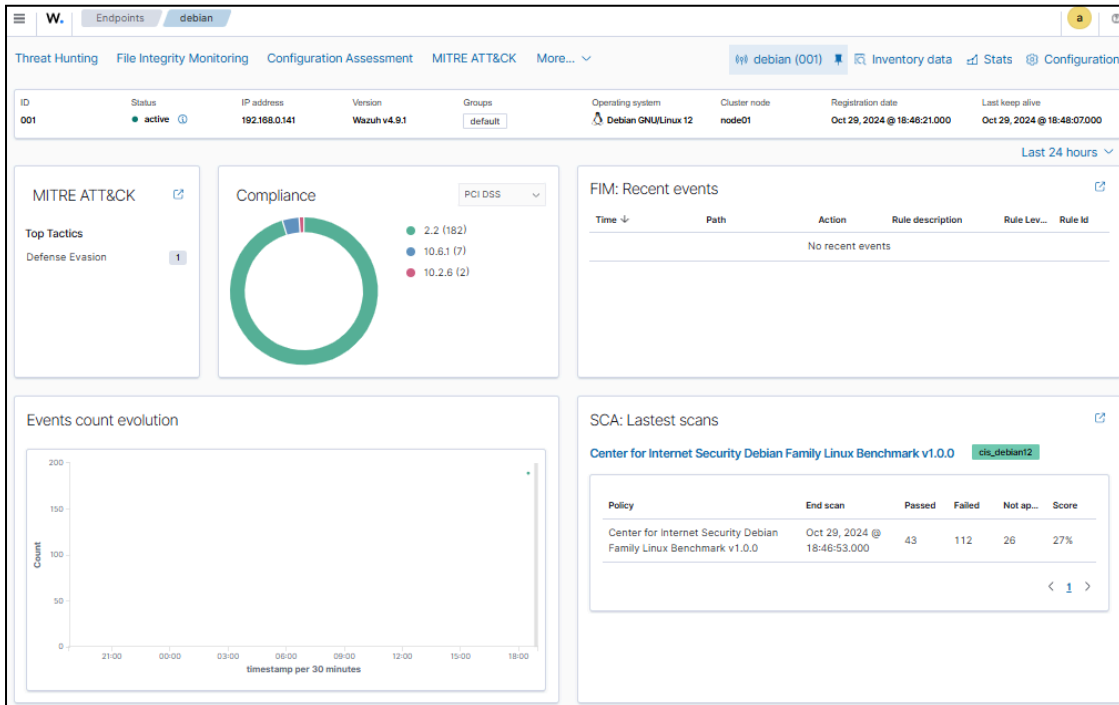
[sudo] Mot de passe de debian :
Sélection du paquet wazuh-agent précédemment désélectionné.
(Lecture de la base de données... 154980 fichiers et répertoires déjà installés.)
Préparation du dépaquetage de ../wazuh-agent_4.9.1-1_amd64.deb ...
Dépaquetage de wazuh-agent (4.9.1-1) ...
Paramétrage de wazuh-agent (4.9.1-1) ...
debian@debian:~$ sudo systemctl daemon-reload
sudo systemctl enable wazuh-agent
sudo systemctl start wazuh-agent
Created symlink /etc/systemd/system/multi-user.target.wants/wazuh-agent.service → /lib/systemd/system/wazuh-agent.service.
debian@debian:~$ |
```

Une fois l'agent installé sur notre machine, nous n'avons pas à faire de configuration supplémentaire, car toutes les informations et configuration sont dans l'agent d'installation que nous avons téléchargé.

Nous pouvons maintenant nous reconnecter à notre interface web, pour vérifier que notre agent est détecté correctement sur notre machine.



DOSSIER PROFESSIONNEL (DP)



Nous pouvons maintenant configurer des règles de détection personnalisées, pour surveiller et faire de la réponse à incident sur nos machines.

Sur la VM sur laquelle est installé l'agent, on veut surveiller le Desktop. Pour cela, on va créer quelques fichiers, puis les modifier et les supprimer, pour voir ce que ça fait.

Sur l'agent, on accède au fichier `ossec.conf` : **`sudo nano /var/ossec/etc/ossec.conf`**

Puis, on ajoute une ligne pour surveiller le bureau : **`<directories check_all="yes" report_changes="yes" realtime="yes">/home/debian/Bureau</directories>`**

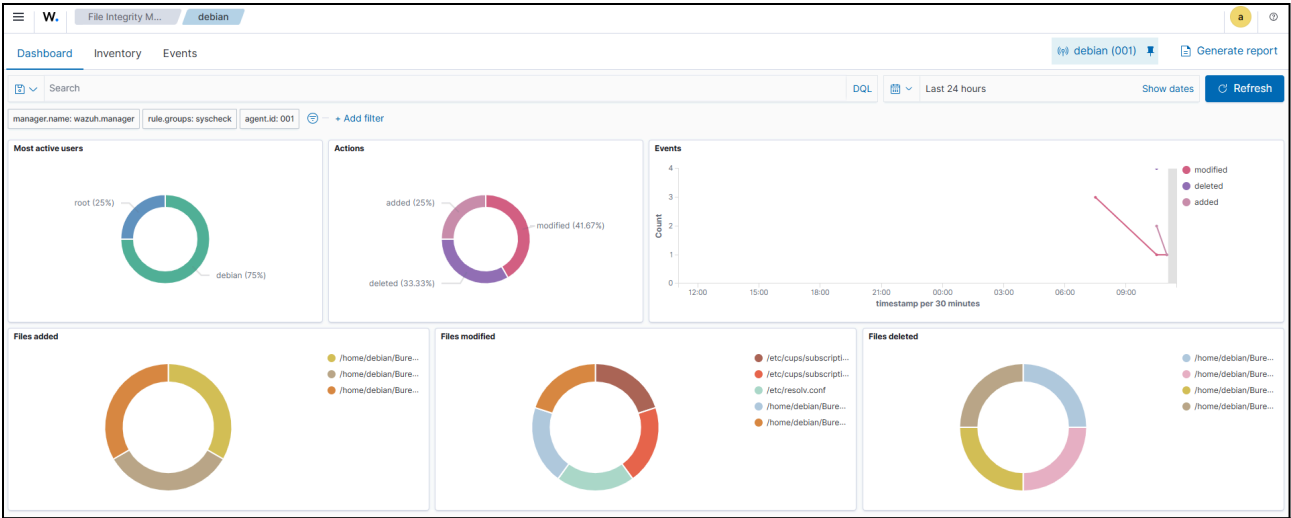
On redémarre l'agent : **`systemctl restart wazuh-agent`**

DOSSIER PROFESSIONNEL (DP)

Last 24 hours ▾

FIM: Recent events 🔗

Time ▾	Path	Action	Rule description	Rule Lev...	Rule Id
Oct 30, 2024 @ 11:01:11.483	/home/debian/Bureau/test3.txt	modified	Integrity checksum changed.	7	550
Oct 30, 2024 @ 11:00:34.930	/home/debian/Bureau/test3.txt	added	File added to the system.	5	554
Oct 30, 2024 @ 10:58:35.762	/home/debian/Bureau/test2.txt	deleted	File deleted.	7	553
Oct 30, 2024 @ 10:58:35.718	/home/debian/Bureau/test1.txt	deleted	File deleted.	7	553
Oct 30, 2024 @ 10:56:47.924	/home/debian/Bureau/test2.txt	added	File added to the system.	5	554



PS : Le File integrity monitoring (FIM) est un processus qui implique la vérification et le suivi réguliers des fichiers afin de détecter toute modification non autorisée.

DOSSIER PROFESSIONNEL ^(DP)

2. Précisez les moyens utilisés :

Machine VM tournant sous debian, pour notre serveur wazuh.

Une VM debian qui nous sert de client.

Une connexion internet pour télécharger les différents paquet sur nos machines.

3. Avec qui avez-vous travaillé ?

Travaille en groupe.

4. Contexte

Nom de l'entreprise, organisme ou association ▶ La Plateforme_

Chantier, atelier, service ▶ Lors de ma formation.

Période d'exercice ▶ Du 2025 au 2025

5. Informations complémentaires (facultatif)

Activité-type 2

Concevoir et mettre en œuvre une solution en réponse
à un besoin d'évolution

Exemple n°1 - Mise en place d'un serveur de supervision pour un parc de machines industrielles.

Dans un premier temps, il faut créer un utilisateur et un groupe prometheus qui seront dédié à l'utilisation de prometheus. pour assurer une bonne sécurité et isolation de notre système de monitoring.

On créer notre groupe prometheus avec la commande :

```
sudo groupadd --system prometheus
```

Shell

Une fois que nous avons créé notre groupe prometheus, il nous faut maintenant créer notre utilisateur prometheus qu'on va aussi ajouter au groupe prometheus par la même occasion.

```
sudo useradd -s /sbin/nologin --system -g prometheus prometheus
```

Shell

On peut maintenant passer au téléchargement de prometheus.

1. Téléchargement de prometheus.

Maintenant que nous avons configuré notre user et notre groupe pour l'utilisation de prometheus, il faut installer l'application, pour ce faire on va prendre la dernière version se trouvant sur github.

```
wget https://github.com/prometheus/prometheus/releases/download/v2.54.0/prometheus-2.54.0.linux-386.tar.gz
```

Shell

```
raph@Raphdebian:~/Téléchargements$ wget https://github.com/prometheus/prometheus/releases/download/v2.54.0/prometheus-2.54.0.linux-386.tar.gz
--2024-08-27 10:28:08-- https://github.com/prometheus/prometheus/releases/download/v2.54.0/prometheus-2.54.0.linux-386.tar.gz
Résolution de github.com (github.com)... 140.82.121.4
Connexion à github.com (github.com)|140.82.121.4|:443... connecté.
requête HTTP transmise, en attente de la réponse... 302 Found
Emplacement : https://objects.githubusercontent.com/github-production-release-asset-2e65be/6838921/14c48c0f-2d5a-4a7d-b630-83399c5dce91?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240827%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240827T082808Z&X-Amz-Expires=300&X-Amz-Signature=4d7ed274dcace6ef94cde27daf4a1e43be77ad1c508b23ebce1feed9c2d576ee&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=6838921&response-content-disposition=attachment%3B%20filename%3Dprometheus-2.54.0.linux-386.tar.gz&response-content-type=application%2Foctet-stream [suivant]
--2024-08-27 10:28:09-- https://objects.githubusercontent.com/github-production-release-asset-2e65be/6838921/14c48c0f-2d5a-4a7d-b630-83399c5dce91?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=releaseassetproduction%2F20240827%2Fus-east-1%2Fs3%2Faws4_request&X-Amz-Date=20240827T082808Z&X-Amz-Expires=300&X-Amz-Signature=4d7ed274dcace6ef94cde27daf4a1e43be77ad1c508b23ebce1feed9c2d576ee&X-Amz-SignedHeaders=host&actor_id=0&key_id=0&repo_id=6838921&response-content-disposition=attachment%3B%20filename%3Dprometheus-2.54.0.linux-386.tar.gz&response-content-type=application%2Foctet-stream
Résolution de objects.githubusercontent.com (objects.githubusercontent.com)... 185.199.108.133, 185.199.111.133, 185.199.110.133, ...
Connexion à objects.githubusercontent.com (objects.githubusercontent.com)|185.199.108.133|:443... connecté.
requête HTTP transmise, en attente de la réponse... 200 OK
Taille : 97816713 (93M) [application/octet-stream]
Sauvegarde en : « prometheus-2.54.0.linux-386.tar.gz »

prometheus-2.54.0.linux- 100%[=====] 93,29M 3,33MB/s ds 27s

2024-08-27 10:28:36 (3,51 MB/s) - « prometheus-2.54.0.linux-386.tar.gz » sauvegardé [97816713/97816713]

raph@Raphdebian:~/Téléchargements$

raph@Raphdebian:~/Téléchargements$ ls
prometheus-2.54.0.linux-386.tar.gz
raph@Raphdebian:~/Téléchargements$
```

Maintenant que nous avons correctement téléchargé la dernière version de prometheus, on va de déTAR, pour son installation avec la commande :

```
tar -xvf prometheus-2.54.0.linux-386.tar.gz
```

Shell

2. Configuration de prometheus

Dans un premier temps, on va créer deux dossier prometheus, un premier dans le repertoire **/etc** de notre machine et un deuxième dans le répertoire **/var/lib** de notre machine avec la commande

```
sudo mkdir /etc/prometheus
```

```
sudo mkdir /var/lib/prometheus
```

Une fois cela fait, on peut se rendre dans le dossier **prometheus-2.54.0.linux-386** que l'on vient de décompresser, puis on va déplacer son contenu dans le dossier **/etc/prometheus** que l'on vient de créer.

```
raph@Raphdebian:~/Téléchargements$ sudo mv prometheus-2.54.0.linux-386 /etc/prometheus/
raph@Raphdebian:/etc/prometheus$ ls
console_libraries  consoles  data  LICENSE  NOTICE  prometheus  prometheus.yml  promtool
```

Maintenant, on va donner les droits au groupe et user prometheus que l'on a créée précédemment. au deux dossier que l'on vient de créer

```
sudo chown prometheus:prometheus /etc/prometheus
sudo chown -R prometheus:prometheus /etc/prometheus/consoles
```

Shell

```
sudo chown -R prometheus:prometheus /var/lib/prometheus
sudo chmod -R 775 /var/lib/prometheus
```

Shell

On va maintenant configurer certains de ses scripts et outils en les copiant dans le répertoire **bin** de l'utilisateur système.

```
sudo cp /etc/prometheus/prometheus /usr/local/bin/
sudo cp /etc/prometheus/promtool /usr/local/bin/
```

Shell

Maintenant que nous avons correctement configuré prometheus, on va le configurer en tant que service pour qu'il puisse démarrer directement au boot de notre machine.

3. Configurer prometheus comme systemd ou service sur notre machine.

pour configurer prometheus soit considéré comme un service que notre machine, il faut créer un fichier **prometheus.service** dans le répertoire **/etc/systemd/system** avec la commande suivante :

```
sudo nano /etc/systemd/system/prometheus.service
```

Shell

une fois dans l'éditeur de fichier, il faut rajouter cette configuration :

```
[Unit]
Description=Prometheus
Documentation=https://prometheus.io/docs/introduction/overview/
Wants=network-online.target
After=network-online.target
[Service]
User=prometheus
Group=prometheus
Type=simple
ExecStart=/usr/local/bin/prometheus \
--config.file /etc/prometheus/prometheus.yml \
--storage.tsdb.path /var/lib/prometheus/ \
--web.console.templates=/etc/prometheus/consoles \
--web.console.libraries=/etc/prometheus/console_libraries
[Install]
WantedBy=multi-user.target
```

service

Maintenant que notre service prometheus est bien configuré il faut initialiser notre service, pour qu'il puisse démarrer au boot de notre machine :

```
sudo systemctl daemon-reload
sudo systemctl enable --now prometheus
sudo systemctl start prometheus
sudo systemctl enable prometheus
```

Shell

une fois cela fait, on peut faire la commande **sudo systemctl status prometheus** pour vérifier qu'il tourne correctement.

4. Configuration de notre Firewall (Optionnel)

si on utilise un firewall sur notre machine (toujours bon d'en avoir un :)), on doit ouvrir le port 9090 qui est utilisé par notre service prometheus.

5. Test de la connexion au service prometheus sur notre navigateur web

Pour accéder à l'interface web de prometheus, il faut taper l'adresse suivante : <http://ip-pc:9090>

http://192.168.61.178:9090

si notre service est bien configuré et qu'on a vérifié qu'il est bien up on devrait arriver sur cette page :

The screenshot shows the Prometheus web interface. At the top, there's a navigation bar with 'Prometheus', 'Alerts', 'Graph', 'Status', and 'Help'. Below this, there are several checkboxes: 'Use local time' (checked), 'Enable query history' (unchecked), 'Enable autocomplete' (checked), 'Enable highlighting' (checked), and 'Enable linter' (checked). A warning message is displayed: 'Warning: Error fetching server time: Detected 114.82099986076355 seconds time difference between your browser and the server. Prometheus relies on accurate time and time drift might cause unexpected query results.' Below the warning, there's a search bar with the placeholder 'Expression (press Shift+Enter for newlines)' and an 'Execute' button. The interface is currently in 'Table' view, but 'Graph' is also visible. A message 'No data queried yet' is shown in the main area. At the bottom, there's an 'Add Panel' button and a 'Remove Panel' link. The bottom part of the screenshot shows the same search bar with the query 'process_virtual_memory_max_bytes' entered.

On peut ensuite faire des recherches de base sur notre système, que l'on peut visionner en Table, ou en Graph :

On peut ensuite faire des recherches de base sur notre système, que l'on peut visionner en Table, ou en Graph :

On peut donc voir qu'on reçoit bien une valeur, ici on a juste pris le max de mémoire virtuelle disponible sur notre machine.

6. Définition de nos jobs scrape pour les différents systèmes :

On se rend dans le fichier `/etc/prometheus/prometheus.yml` et on y ajoute la configuration suivante :

```
global:
  scrape_interval: 15s
  evaluation_interval: 15s

scrape_configs:
  - job_name: 'vaisseau_cpu'
    static_configs:
      - targets: ['localhost:9100']

  - job_name: 'vaisseau_memory'
    static_configs:
      - targets: ['localhost:9200']

  - job_name: 'vaisseau_network'
    static_configs:
      - targets: ['localhost:9300']

  - job_name: 'vaisseau_disk'
    static_configs:
      - targets: ['localhost:9400']
```

```
global:
  scrape_interval: 15s # Set the scrape interval to every 15 seconds. Default is every 1 minute.
  evaluation_interval: 15s # Evaluate rules every 15 seconds. The default is every 1 minute.
  # scrape_timeout is set to the global default (10s).

# Alertmanager configuration
alerting:
  alertmanagers:
    - static_configs:
      - targets:
        # - alertmanager:9093

# Load rules once and periodically evaluate them according to the global 'evaluation_interval'.
rule_files:
  # - "first_rules.yml"
  # - "second_rules.yml"

# A scrape configuration containing exactly one endpoint to scrape:
# Here it's Prometheus itself.
scrape_configs:
  # The job name is added as a label 'job=<job_name>' to any timeseries scraped from this config.
  - job_name: "prometheus"

    # metrics_path defaults to '/metrics'
    # scheme defaults to 'http'.

    static_configs:
      - targets: ["localhost:9090"]

  - job_name: 'vaisseau_cpu'
    static_configs:
      - targets: ['localhost:9100']

  - job_name: 'vaisseau_memory'
    static_configs:
      - targets: ['localhost:9200']

  - job_name: 'vaisseau_network'
    static_configs:
      - targets: ['localhost:9300']

  - job_name: 'vaisseau_disk'
    static_configs:
      - targets: ['localhost:9400']
```

7. Ajouter des exporter pour chaque système :

Maintenant que nous avons configuré notre serveur Prometheus, ce serait bien de pouvoir avoir des infos sur d'autres systèmes. Pour ce faire, on va utiliser des "Exporters", qui collectent des données (CPU, RAM, Réseau ...), pour ensuite les exposer à Prometheus.

8. Installation de Node Export :

Dans un premier temps, il faut installer Node Export sur notre machine, on passe pour cela par un repo Github, qu'on va par la suite installer sur notre machine.

```
wget
https://github.com/prometheus/node_exporter/releases/download/v1.6.1/node_exporter-1.6.1.linux-amd64.tar.gz
tar xvf node_exporter-1.6.1.linux-amd64.tar.gz
sudo mv node_exporter-1.6.1.linux-amd64/node_exporter /usr/local/bin/
```

Maintenant que nous avons installé Node Exporter, on va créer un user pour utiliser le service et mettre les droits sur les dossiers que l'on vient d'installer et de move dans /usr/local/bin


```
sudo useradd --no-create-home --shell /bin/false nodeusr  
sudo chown nodeusr:nodeusr /usr/local/bin/node_exporter
```

On va maintenant créer un fichier `node_exporter.service`, pour que notre node exporter, puisse être directement lancer au boot de notre machine.

```
sudo nano /etc/systemd/system/node_exporter.service
```

et on y ajoute la configuration suivante :

```
[Unit]  
Description=Node Exporter  
Wants=network-online.target  
After=network-online.target  
  
[Service]  
User=nodeusr  
Group=nodeusr  
Type=simple  
ExecStart=/usr/local/bin/node_exporter  
  
[Install]  
WantedBy=multi-user.target
```

Maintenant que nous avons configuré notre service node Exporte, on peut reload nos daemon sur notre machine, et enable le service au boot de la machine :

```
sudo systemctl daemon-reload  
sudo systemctl start node_exporter  
sudo systemctl enable node_exporter
```

Pour être sûr que toutes notre configuration fonctionne correctement, on peut effectuer un reboot de la machine.

9. Installation de grafana :

<https://grafana.com/grafana/download/11.1.5?platform=linux&edition=oss>

Maintenant que nous avons installé prometheus sur notre machine, on va maintenant installer grafana pour avoir une meilleur interface utilisateur.

```
sudo apt-get install -y adduser libfontconfig1 musl
wget
[https://dl.grafana.com/oss/release/grafana_11.1.5_amd64.deb](https://dl.grafana.com/oss
/release/grafana_11.1.5_amd64.deb)
sudo dpkg -i grafana_11.1.5_amd64.deb
```

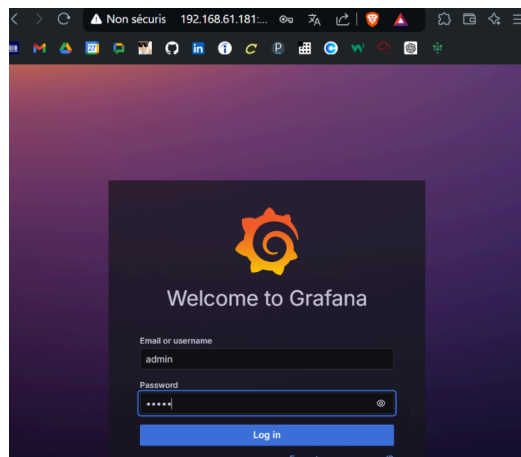
Avant de lancer notre serveur grafana, on doit reload nos deamond, et lancer le service grafana.

```
sudo /bin/systemctl daemon-reload
sudo /bin/systemctl enable grafana-server
sudo /bin/systemctl start grafana-server
```

On peut maintenant se connecter à notre page web grafana avec l'adresse suivante :

<http://ip-pc:3000>

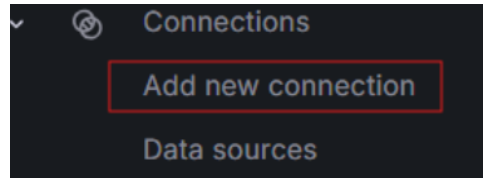
Si on à configurer un firewall sur notre machine, il ne faut pas oublier de laisser passer le trafique sur le port **3000** de notre machine.



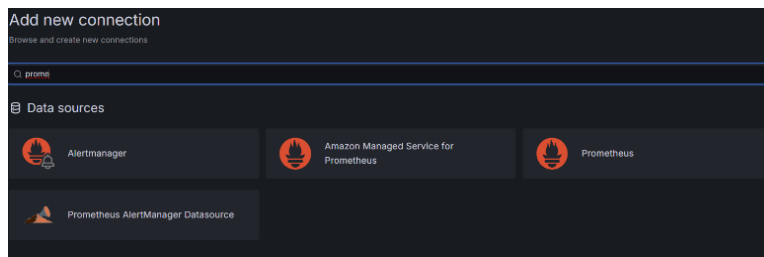
Le log par défaut sont admin admin. On peut les modifier après notre première connexion.

10. Connecter notre serveur prometheus à grafana :

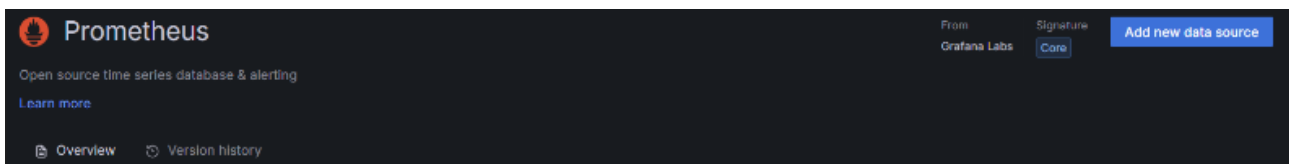
on va se rendre sur l'onglet à droite puis dans **Connections>Add new connection** :



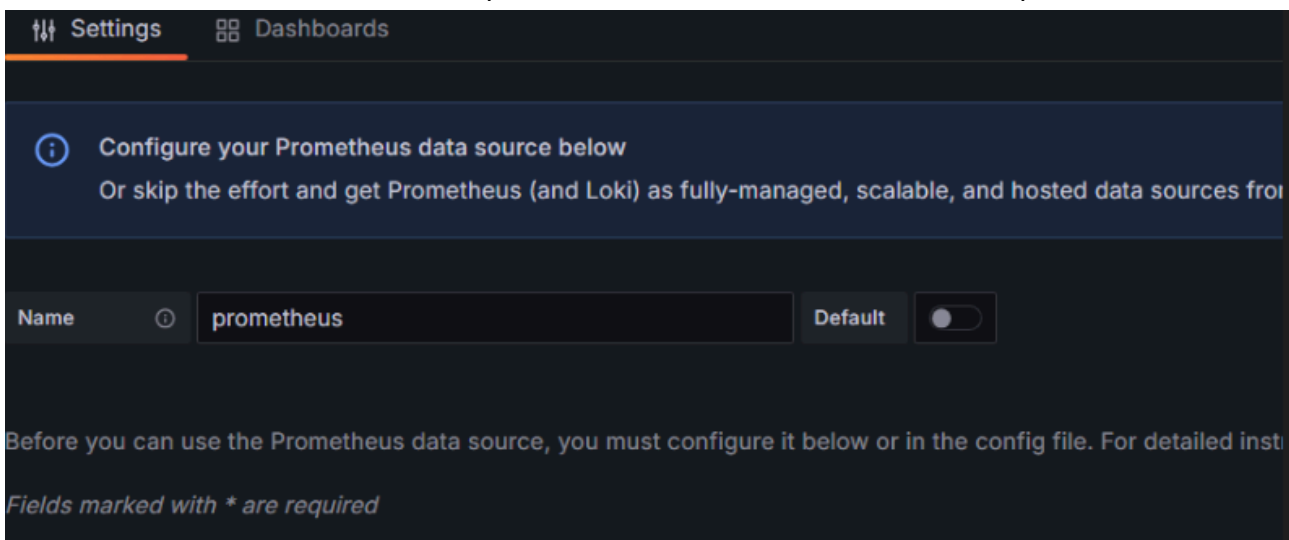
On va ensuite chercher prometheus :



on clique ensuite sur le bouton add new data source :



on entre ensuite un nom et on oublie pas de mettre l'adresse de notre serveur prometheus :

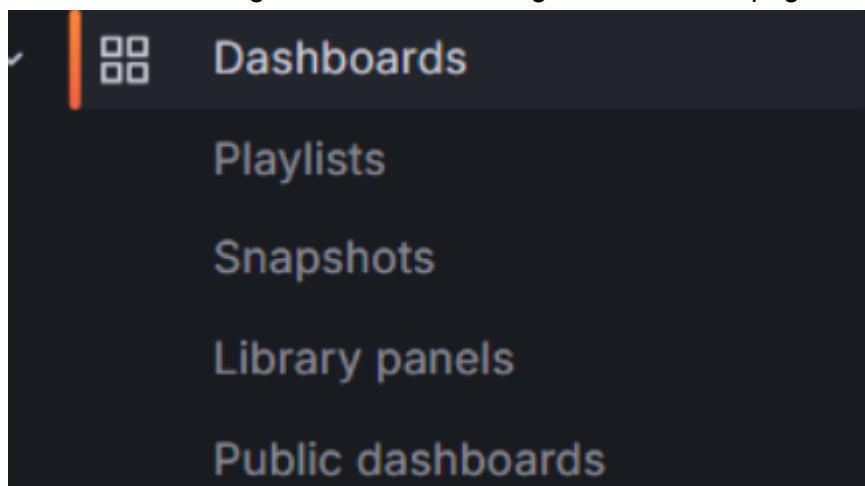


on peut ensuite cliquer sur save and test, si on arrive à arriver sur l'interface web de notre serveur prometheus, alors la connexion se fera sans soucis. :)

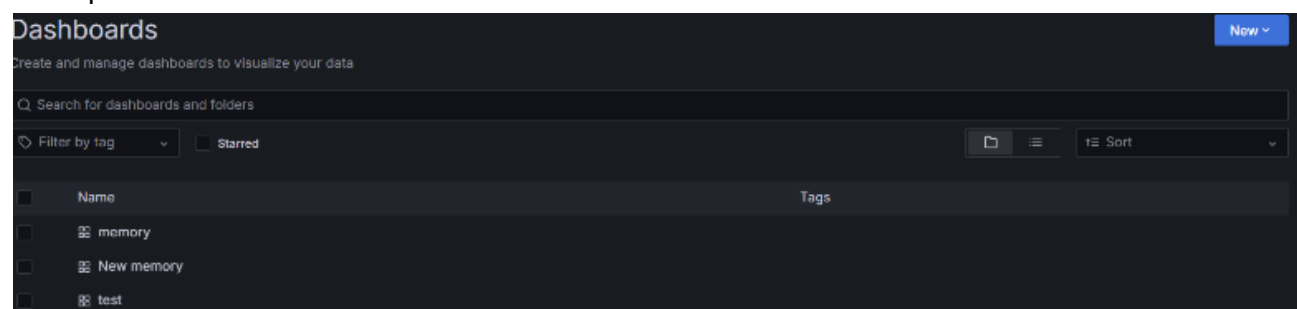
11. Configuration de quelques graphique pour grafana :

On va maintenant configurer quelque graph pour avoir des informations sur la ou les machines monitorer.

pour ce faire on se rends dans l'onglet dashboard sur la gauche de notre page web :



on clique ensuite sur le bouton new :



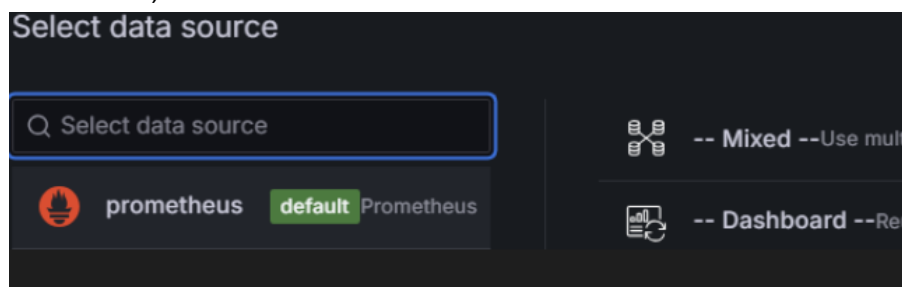
On part de 0 donc on clique sur le bouton add visualization :

Start your new dashboard by adding a visualization

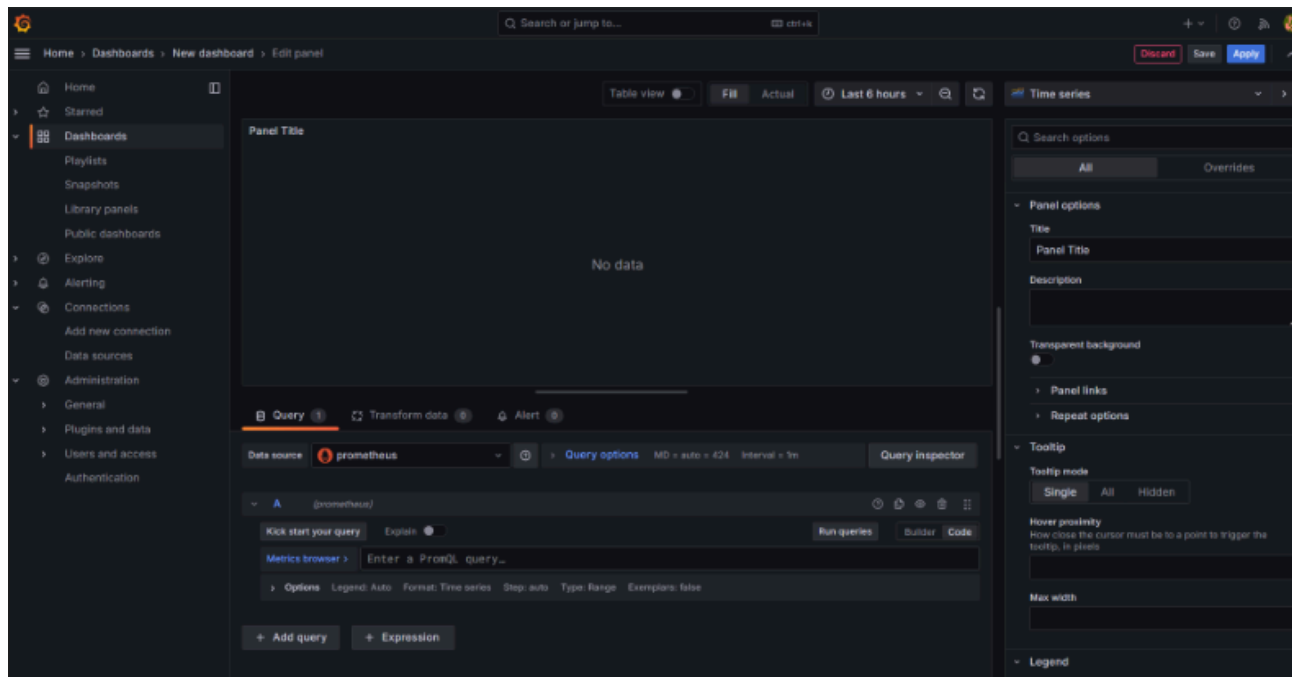
Select a data source and then query and visualize your data with charts, stats and tables or create lists, markdowns and other widgets.

+ Add visualization

on choisit ensuite notre data source donc dans notre cas prometheus (ou un autre nom en fonction de celui qu'on lui a donné)



On devrait normalement arriver sur cet interface :

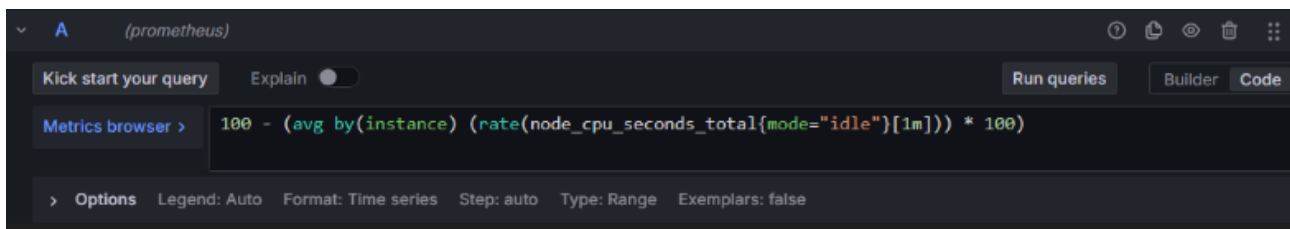


12. Configuration de notre graph pour CPU usage :

on va maintenant configurer un graph pour pouvoir surveiller l'usage de notre CPU sur notre machine.

Dans la partie ou l'on doit rentrer les infos que l'on veut annalyser, on choisit l'option code, et on entre cette ligne de code.

```
100 - (avg by(instance) (rate(node_cpu_seconds_total{mode="idle"}[1m])) * 100)
```

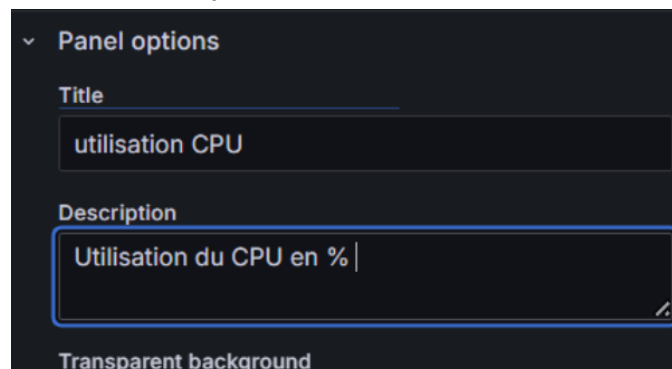


une fois cette ligne entrer, on peut faire run queries, pour voir l'appercu sur notre graph :



on pourrait le laisser comme cela, mais on va changer un peu le graphique d'un point de vu visuel pour qu'il soit plus agréable à regarder .

On se rend dans le panneau de configuration sur la gauche, et on entre dans un premier temps, le titre de notre graph, et l'on peut aussi ajouter une petite description.



Panel options

Title

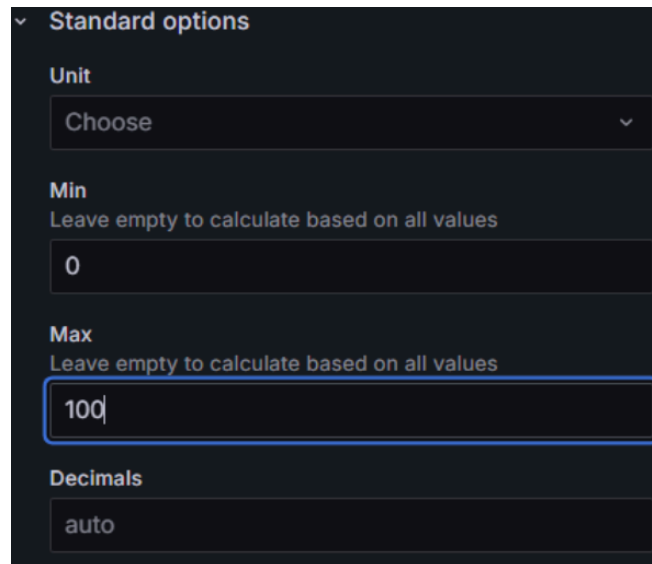
utilisation CPU

Description

Utilisation du CPU en %

Transparent background

Dans standard options, on peut aussi ajouter une valeur maximal et minal, dans notre cas on va mettre 0 et 100, car on est en pourcentage.



Standard options

Unit

Choose

Min

Leave empty to calculate based on all values

0

Max

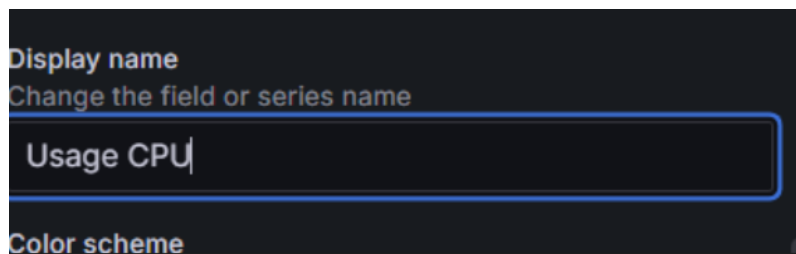
Leave empty to calculate based on all values

100

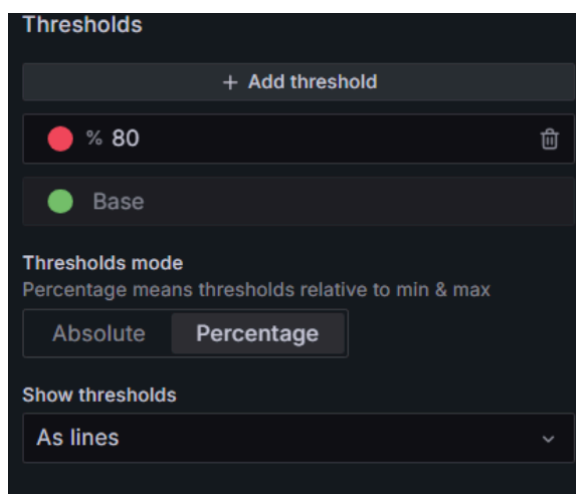
Decimals

auto

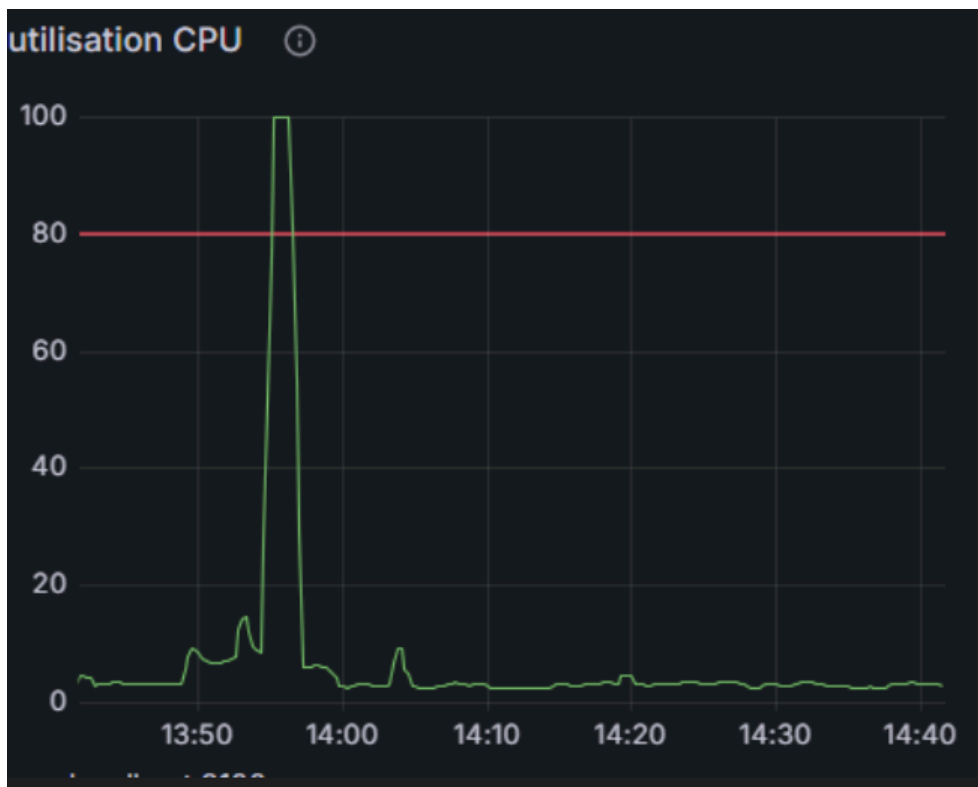
On peut aussi ajouter une valeur dans display name, pour donner un nom à notre courbe, dans notre cas, on va l'appeler simplement Usage CPU.



On peut aussi ajouter une valeur critique, que nous permet de voir facilement quand la charge à dépasser la limite que l'on a fixé :



On devrait à la fin avoir un graphique qui ressemble à celui-ci :



Voila votre graph sur l'usage du CPU est créer !!!

13. Utilisation de notre disque :

On va maintenant faire un graph pour voir l'utilisation de notre disque, je vais vous montrer le résultat souhaiter et on vas voir comment on peut obtenir ce résultat :

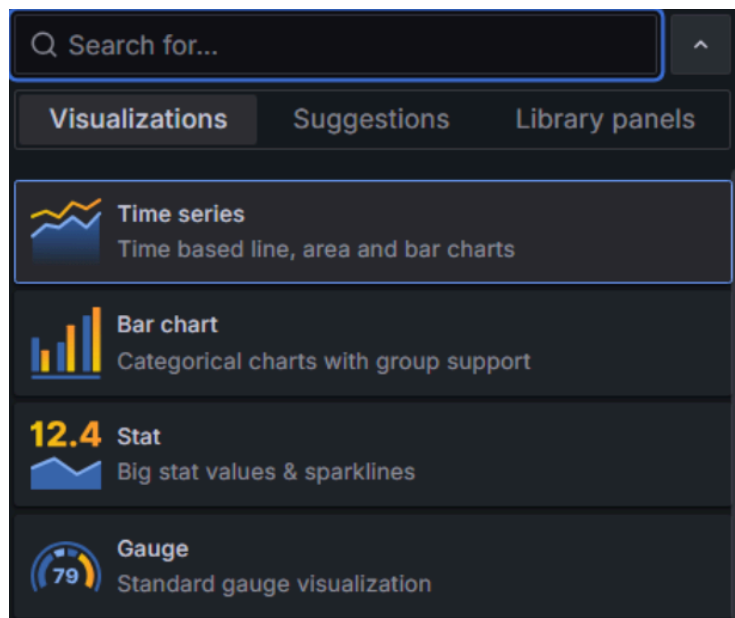


Pour se faire, on se rends sur notre dash board, et on va ajouter une nouvelle visualisation en appuyant sur le bouton Add.

comme pour le graph sur l'usage de notre CPU, on va se mettre en mode code et ajouter cette ligne de code :

```
100 * (node_filesystem_size_bytes{fstype!~"tmpfs|devtmpfs", mountpoint="/" } -  
node_filesystem_avail_bytes{fstype!~"tmpfs|devtmpfs", mountpoint="/" }) /  
node_filesystem_size_bytes{fstype!~"tmpfs|devtmpfs", mountpoint="/" }
```

pour mettre notre graph en mode jauge, on se rend dans l'onglet sur la droite et on choisit le graphique jauge :



On devrait arriver sur un résultat qui devrait avoir après être passer en mode jauge :



Comme on rentre des pourcentage dans notre metric, on voudrait que notre jauge monte jusqu'à 100, donc pour se faire on va dans les options sur la gauche de notre page web et on cherche l'onglet standard options, pour rentrer en valeur min 0 et en valeur max 100 :

Standard options

Unit
Choose

Min
Leave empty to calculate based on all values
0

Max
Leave empty to calculate based on all values
100

on devrait maintenant avoir un graphique qui ressemble à ceci :



Si vous le voulez vous pouvez aussi personnaliser le graphique, dans notre cas cela ressemble fortement au résultat voulu.

14. Trafic réseau :

15.1. Trafic entrant

pour notre dernier graphique, on va afficher le trafic réseau entrant et sortant de notre machine linux, cela va un peu changer des graphiques précédents, car on aura deux courbes sur notre graphique.

On va s'occuper dans un premier du trafic sortant sur notre machine, pour ce faire, on utilise cette ligne de calcul :

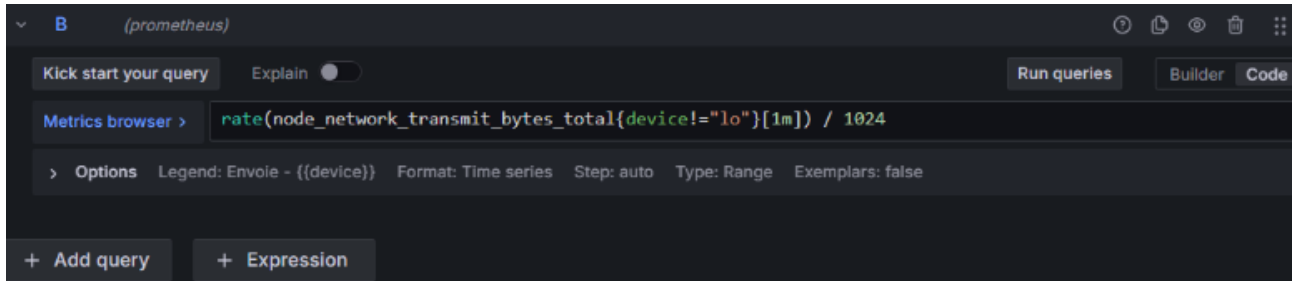
```
rate(node_network_receive_bytes_total{device!="lo"}[1m]) / 1024
```

ensuite on se rends dans options pour donner un nom à notre courbe, on choisit une valeur custom, et on met cette valeur, qui nous indiquera l'interface sur laquelle on analyse le trafic :

Réception - {{device}}

15.2. Trafic sortant

On va maintenant faire une courbe qui va analyser le trafic sortant de notre machine, pour ce faire, on clique sur le bouton add query :



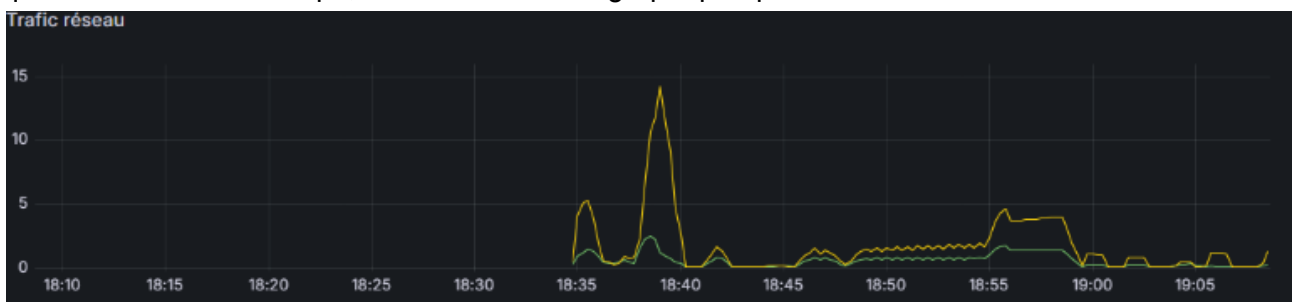
ensuite on entre cette ligne de calcul :

```
rate(node_network_transmit_bytes_total{device!="lo"}[1m]) / 1024
```

cette ligne nous permet de voir le trafic sortant de notre port d'écoute, on ajoute ensuite comme pour le trafic entrant la ligne qui permet de donner un nom à notre courbe :

Envoie - {{device}}

quand on a fini cette étape, on devrait avoir un graphique qui ressemble à cela :



voilà vous venez de finir la configuration pour une machine en combinant prometheus et grafana, notre dash board devrait ressembler à cela :



Voilà la configuration de monitoring de notre machine est enfin terminée, si vous voulez obtenir la configuration complète du dash board, un import json se trouve en ANNEXE.

2. Précisez les moyens utilisés :

Machine VM tournant sous debian, pour notre serveur prometheus et graphana.

Une VM debian qui nous sert de client et une machine windows qui nous sert également de client .

Une connexion internet pour télécharger les différents paquet sur nos machine.

DOSSIER PROFESSIONNEL (DP)



3. Avec qui avez-vous travaillé ?

Travaille en groupe.

4. Contexte

Nom de l'entreprise, organisme ou association ▶ La Plateforme_

Chantier, atelier, service ▶ Lors de ma formation.

Période d'exercice ▶ Du 2025 au 2025

5. Informations complémentaires (facultatif)*

<https://linux.how2shout.com/how-to-install-prometheus-in-debian-11-or-ubuntu-20-04/>

Activité-type 3 Participer à la gestion de la cybersécurité

Exemple n°1 - Analyse de risque pour une entreprise fictive, plus mise en place de plan de remédiation

1. Décrivez les tâches ou opérations que vous avez effectuées, et dans quelles conditions :

Introduction du sujet

"TechSecure" est une PME spécialisée dans le développement de solutions logicielles de cybersécurité. Elle dispose d'une équipe de 50 employés et gère des données sensibles pour ses clients.

- **Infrastructure** : Serveurs cloud, bases de données clients, site web dématérialisé.
- **Données critiques** : Informations clients, codes sources de logiciels de sécurité.
- **Menaces potentielles** : Phishing, ransomware, attaque DDoS, vol de données internes.

Vous avez pour mission d'évaluer les risques , pour cela « TechSecure » fournis le schéma de l'infrastructure de son réseau , ainsi que la configuration des équipements réseau (voir annexes, les mots de passes ont volontairement été changés)

- Vous devez évaluer la probabilité et l'impact des risques en utilisant une matrice des risques.
- Identifier les faiblesses potentielles dans l'architecture réseau (segmentation inadéquate, points de défaillance uniques, etc.).
- Créer une liste des menaces spécifiques à cette infrastructure, classées par type d'attaquant (interne, externe, sophistiqué, opportuniste).
- Évaluation des contrôles de sécurité : Analysez les configurations pour identifier les contrôles manquants ou mal configurés (règles de pare-feu trop permissives, mauvaise ségrégation des VLANs, etc.).
- Plan de remédiation : Création d'un plan hiérarchisé pour corriger les vulnérabilités identifiées.
- Étude d'impact business : Identifiez les actifs critiques sur ce réseau et évaluez l'impact business en cas de compromission.
- Élaboration d'un plan de continuité : Conception de stratégies pour maintenir les services essentiels en cas d'incident.

- Analyse de conformité : Vérifiez si la configuration respecte les normes pertinentes (RGPD, etc.).
- Élaboration de règles adaptées à cette infrastructure.
- Identification des points de surveillance et des alertes à implémenter.
- Analysez les configurations pour identifier les contrôles manquants ou mal configurés (règles de pare-feu trop permissives, mauvaise ségrégation des VLANs, etc.).

1) Adressage IP

Réseau principal : 10.0.0.0/16

VLAN 10 (Administration) : 10.0.10.0/24

VLAN 20 (Développement) : 10.0.20.0/24

VLAN 30 (Commercial) : 10.0.30.0/24

VLAN 40 (Serveurs internes) : 10.0.40.0/24

VLAN 99 (Management) : 10.0.99.0/24

DMZ : 172.16.0.0/24

2) Routeur R1 (Cisco 2911)

```
enable
```

```
configure terminal
```

```
hostname R1
```

```
enable secret TechSecure@2025
```

```
interface GigabitEthernet0/0
```

```
description Connexion WAN
```

```
ip address dhcp
```

```
no shutdown
```

```
interface GigabitEthernet0/1
```

```
description Connexion LAN
```

```
ip address 10.0.0.1 255.255.0.0
```

```
no shutdown
```

```
ip nat inside source list 1 interface GigabitEthernet0/0 overload
```

```
access-list 1 permit 10.0.0.0 0.0.255.255
```

```
ip route 172.16.0.0 255.255.255.0 10.0.0.2
```

3) Pare-feu ASA 5506-X (FW1)

```
enable
```

```
configure terminal
```

```
hostname FW1
```

```
interface GigabitEthernet1/1
```

```
nameif outside
```

```
security-level 0
```

```
ip address 10.0.0.2 255.255.0.0
```

```
interface GigabitEthernet1/2
```

```
nameif inside
security-level 100
ip address 10.0.1.1 255.255.0.0
interface GigabitEthernet1/3
nameif dmz
security-level 50
ip address 172.16.0.1 255.255.255.0
```

3) Switch Principal (S1 - L3)

```
enable
configure terminal
hostname S1
vlan 10
name Administration
vlan 20
name Developpement
vlan 30
name Commercial
vlan 40
name Serveurs_Internes
vlan 99
name Management
```

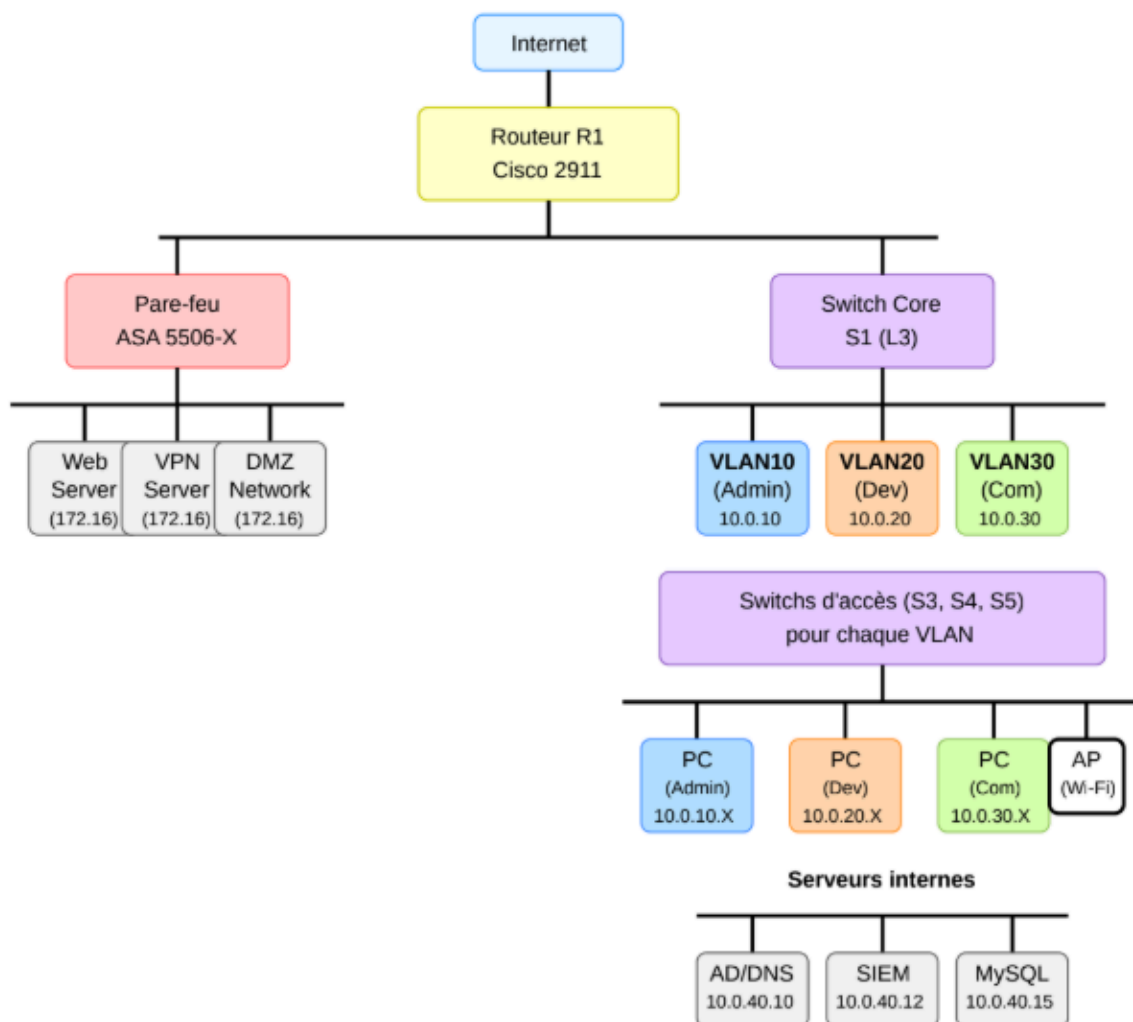
4) Configuration des Points d'Accès (AP1 et AP2 VLAN30)

```
enable
configure terminal
hostname AP1 ou AP2
interface Dot11Radio0
ssid TechSecure-WiFi
authentication open
encryption mode ciphers aes-ccm
wpa-psk ascii TechSecure@2025!
interface GigabitEthernet0
switchport mode access
switchport access vlan 30
no shutdown
```

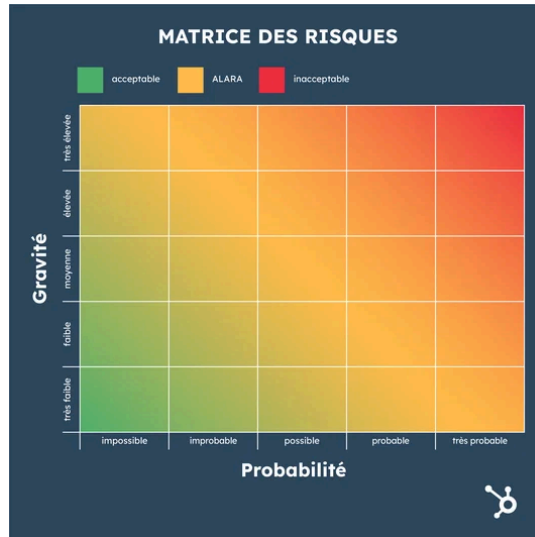
5) Configuration du Serveur MySQL/MariaDB (VLAN 40)

```
CREATE USER 'dev_user'@'10.0.20.0%' IDENTIFIED BY 'DevPass123!';
GRANT ALL PRIVILEGES ON *.* TO 'dev_user'@'10.0.20.0%' WITH GRANT OPTION;
FLUSH PRIVILEGES;
```

Schéma du réseau



1. Evaluation des risques



Menace	Probabilité	Impact	Niveau de risque
Phishing	Élevé	Élevé	Critique
Ransomware	Moyen	Élevé	Critique
Attaque DDoS	Moyen	Moyen	Élevé
Vol de données internes	Faible	Élevé	Moyen

2. Identification des faiblesses potentielles

Segmentation réseau insuffisante : L'accès à la DMZ est trop ouvert, permettant un accès facile aux ressources internes. Le filtrage inter-VLAN est trop permissif. **Action** : Restreindre les flux entre VLANs et sécuriser l'accès à la DMZ en limitant les services exposés.

Pare-feu ASA mal configuré : Les règles sont trop permissives, ne filtrant pas certains types de trafic. Il manque un contrôle applicatif et les logs ne sont pas suffisamment détaillés pour une détection efficace des attaques. **Action** : Appliquer une politique "deny-all", activer l'inspection DPI (Deep Packet Inspection) et configurer les alertes de sécurité.

Wi-Fi non sécurisé : Le Wi-Fi utilise un protocole WPA-PSK vulnérable aux attaques par force brute, et il n'y a pas de séparation entre les utilisateurs du réseau sans fil. **Action** : Passer à WPA2-Enterprise avec des contrôles d'accès renforcés et isoler les connexions Wi-Fi des

autres segments du réseau (utilisation de VLAN dédiés).

Accès trop permissif à la base de données : L'utilisateur dev_user dispose de privilèges trop larges et peut se connecter à partir d'un large sous-ensemble d'adresses IP. De plus, la connexion n'est pas chiffrée, ce qui expose les données à des risques d'interception. **Action :** Restreindre l'accès au strict minimum nécessaire (privilège minimal), et activer TLS pour sécuriser les connexions.

3. Menaces par type d'attaquant

Interne : Employé malveillant, vol de données internes (accès non autorisé aux ressources sensibles).

Externe : Attaques par phishing, ransomware, DDoS, compromission via une faille réseau.

Sophistiqué : Attaques ciblées (exploitation de vulnérabilités, espionnage industriel).

Opportuniste : Attaques par force brute, scanning des ports, exploitation de failles de sécurité non patchées.

4. Evaluation des contrôles de sécurité

Pare-feu : Il est nécessaire de restreindre les flux entre VLANs et d'appliquer des règles plus strictes. Actuellement, trop de ports sont ouverts, ce qui expose le réseau à des risques accrus. **Action :** Appliquer une politique "deny-all" avec des règles restrictives, n'autorisant que les flux nécessaires entre les différents segments.

Wi-Fi : Le protocole WPA-PSK est vulnérable aux attaques par force brute et ne garantit pas une isolation adéquate des utilisateurs. **Action :** Passer à WPA2-Enterprise et isoler les connexions Wi-Fi en utilisant des VLANs dédiés.

Contrôle des accès à la base de données : Le compte dev_user possède des privilèges trop élevés et des restrictions d'accès insuffisantes. **Action :** Appliquer le principe du moindre privilège et utiliser TLS pour sécuriser les connexions.

5. Plan de remédiation

VLAN séparé pour Wi-Fi : Créer un VLAN dédié pour les accès sans fil afin d'isoler les utilisateurs du réseau interne.

Renforcement des règles de pare-feu : Modifier les règles pour restreindre l'accès à la DMZ et interdire les flux inutiles entre les VLANs.

Authentification forte : Implémenter une authentification forte (2FA) pour les accès internes et gérer les privilèges de manière stricte.

6. Étude d'impact business

Confidentialité des données : Une violation de la confidentialité des données sensibles des clients (codes sources, informations personnelles) aurait des conséquences graves sur la réputation de l'entreprise et la confiance des clients.

Réputation : La perte de confiance des clients pourrait entraîner une réduction des ventes et des partenariats.

Conformité réglementaire : Non-respect des réglementations comme le RGPD entraînerait des sanctions financières importantes et des coûts de gestion de crise.

Pertes financières : Outre les amendes, des poursuites judiciaires et des compensations seraient possibles pour les victimes de la fuite.

Impact sur la détection des menaces : Sans un système de détection efficace, les menaces ne seraient pas repérées à temps, ce qui augmenterait la probabilité de dommages importants.

7. Elaboration d'un plan de continuité (PCA)

Sauvegarde : Mise en place de sauvegardes régulières, y compris des sauvegardes hors ligne.

Redondance des services critiques : Assurer la redondance des services essentiels pour garantir leur disponibilité en cas d'incident majeur.

8. Analyse de conformité

RGPD : Renforcer la protection des données clients en appliquant des mesures de sécurité adaptées à la nature des données traitées (cryptage, gestion des accès).

ISO 27001 : Renforcer la gestion des accès et mettre en place des audits réguliers pour assurer la conformité avec la norme ISO 27001.



9. Elaboration de règles de sécurité

Segmentation stricte des VLANs : Assurer une séparation rigoureuse des VLANs pour isoler les différents types de trafic.

Renforcement des configurations de pare-feu : Mettre en place des règles plus restrictives pour limiter l'accès non autorisé aux ressources internes.

10. Surveillance et alertes

SIEM : Implémenter un système de surveillance centralisée pour détecter les tentatives de connexion suspectes et les comportements anormaux sur le réseau.

IDS/IPS : Mettre en place des systèmes de détection et de prévention des intrusions pour surveiller les attaques réseau.

EDR : Déployer un système de détection et de réponse sur les postes de travail pour surveiller les comportements malveillants.

UEBA (user and entity behavior analytics) : Implémenter un logiciel de sécurité qui utilise l'analyse comportementale et le machine learning pour identifier les comportements anormaux.

2. Précisez les moyens utilisés :

~Besoin d'un plan d'entreprise fictive pour notre analyse de risque

DOSSIER PROFESSIONNEL (DP)

3. Avec qui avez-vous travaillé ?

Travaille en groupe.

4. Contexte

Nom de l'entreprise, organisme ou association ▶ La Plateforme_

Chantier, atelier, service ▶ Lors de ma formation.

Période d'exercice ▶ Du 2025 au 2025

5. Informations complémentaires (facultatif)

Titres, diplômes, CQP, attestations de formation

(facultatif)

Intitulé	Autorité ou organisme	Date
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.
Cliquez ici.	Cliquez ici pour taper du texte.	Cliquez ici pour sélectionner une date.

Déclaration sur l'honneur

Je soussigné(e) [prénom et nom] *Cliquez ici pour taper du texte.* ,
déclare sur l'honneur que les renseignements fournis dans ce dossier sont exacts et que je
suis l'auteur(e) des réalisations jointes.

Fait à **Marseille** le *Cliquez ici pour choisir une date*
pour faire valoir ce que de droit.

Signature :

Cliquez ici pour taper du texte.

Documents illustrant la pratique professionnelle

(facultatif)

Intitulé
Cliquez ici pour taper du texte.

DOSSIER PROFESSIONNEL ^(DP)

ANNEXES

(Si le RC le prévoit)

