


Ouverture de ports sur serveurs distants

PARCOURS	SISR <input checked="" type="checkbox"/>	SLAM <input type="checkbox"/>
Lieu de réalisation	Sikiwis UERP	 ERP By SIKIWIS
Période de réalisation	Du : 04.11.2024	Au :
Modalité de réalisation	SEUL <input type="checkbox"/>	EN EQUIPE <input checked="" type="checkbox"/>
Intitulé de la mission	Ouverture de ports	
Description du contexte de la mission	Ouverture de ports sur serveur distant à l'aide du protocole SSH	
Contraintes & Résultat	Ressources fournies / contraintes techniques / Résultats attendu	
	Laptop, Putty, nmap, MongoDBCompass	
Productions associées	Liste des documents produits et description	
Modalités d'accès aux productions	Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage	

Ouverture de ports sur serveurs distants

1) Contexte

La société Sikiwis a une plateforme d'applications, hébergée sur un serveur web dédié Server 10-Core du fournisseur Contabo, à l'adresse 173.212.XXX.XXX. Toutefois, des problèmes de connexions apparaissent avec la plateforme. Après une série de tests, Contabo informe Sikiwis dans un mail que certains des ports sont disponibles, notamment le 22 (SSH/FTP), 80 (HTTP), 443 (HTTPS), mais pas d'autres, le 21 (FTP) et le 27017 (MongoDB). Il est donc décidé d'intervenir directement sur le serveur.

2) Ouverture des ports

On se connecte au serveur à l'aide du logiciel Putty en rentrant l'adresse IP publique, en ssh. Une fois la fenêtre ouverte, on rentre les identifiants (connexion en root, superutilisateur). Lorsqu'on y est, on ouvre les ports concernés à l'aide de commandes basées sur iptables :

On sauvegarde les nouvelles règles avec :

On vérifie l'état des ports avec la commande :

On vérifie que la connexion marche avec le logiciel nmap, en rentrant l'IP utilisée (173.212.XXX.XXX) et cette commande :

```
nmap -p 21,22,27017,80,443 173.212.222.196
```

Les ports 21 et 27017 ne sont toujours pas ouverts. On retourne sur le serveur pour vérifier l'état des services liés à ces ports.

3) Installation des services

Il s'avère que les services liés à ces ports (FTP, MongoDB) ne sont pas installés. Il faut donc les installer. Après s'être assuré que les paquets sont à jour (update, upgrade), on installe les services FTP et MongoDB. On rencontre une erreur en installant MongoDB, donc on va s'aider de Docker, en l'installant, en créant une image Docker sur laquelle on va installer MongoDB.

On retourne sur nmap vérifier la connexion :

```
PORT      STATE SERVICE
21/tcp    open  ftp
27017/tcp open  mongod
```

```
Nmap done: 1 IP address (1 host up) scanned in 0.28 seconds
```

La connexion est désormais possible sur les ports concernés.

4) Conclusion

Ouverture de ports sur serveurs distants

1) Contexte

L'année dernière, la société *Sikiwis*, éditrice de logiciels, a configuré une solution de tracking GPS et livrer un ensemble de trackers GPS pour l'institution des *Centres hospitaliers de Mayotte (CHM)*, destiné à équiper leur flotte de véhicules.

Au niveau de l'architecture logicielle, la société *Sikiwis* a une plateforme d'applications, hébergée sur un serveur web dédié, Server 10-Core, auprès d'une société allemande spécialisée dans l'hébergement web et la fourniture de services de cloud computing, *Contabo GmbH*, à l'adresse 173.212.XXX.XXX. Toutefois, des problèmes de connexions apparaissent avec la plateforme, empêchant le client de Sikiwis, CHM, d'accéder à leur plateforme de tracking GPS. La société Sikiwis remonte ce problème à la société Contabo dans un mail.

On Thu, 31 Oct at 11:01 AM, [REDACTED] <[REDACTED]@sikiwis.com> wrote:
@Contabo Support Team

on 173.212.[REDACTED] when trying to connect we get the message

ECONNREFUSED 173.212.[REDACTED] 27017

This affects a critical customer application in production, we must restore this service immediately

Please help us

Thank you

A la suite d'un échange de messages entre la société Sikiwis et Contabo, il s'avère que le problème de connectivité à la plateforme ne concerne que certains ports, et donc que certains services, notamment le port 21, affecté au protocole FTP, permettant l'échange de fichiers, et le port 27017, affecté aux bases de données non relationnelles MongoDB, utilisées dans l'architecture logicielle de la solution utilisée par CHM.

We have checked your Dedicated Server 10-Core (173.212.[REDACTED]) and it is online and responding to ping requests. We can reach the server via SSH, and SFTP on port 22. However, it seems that ports 27017 and 21 are closed as per the nmap result below, which is probably why you are having issues connecting your DB and FTP to it.

Starting Nmap 7.80 (<https://nmap.org>) at 2024-11-04 10:11 CET
Nmap scan report for m4696.contaboserver.net (173.212.[REDACTED])
Host is up (0.047s latency).
Not shown: 997 closed ports
PORT STATE SERVICE
22/tcp open ssh
80/tcp open http
443/tcp open https

La procédure consiste à rétablir l'accès et la connectivité des ports 21 et 27017, afin que les services d'échange de fichiers et de bases de données MongoDB puisse reprendre, et donc que la société CHM puisse réaccéder à sa plateforme de tracking GPS.

Ouverture de ports sur serveurs distants

2) Tests de connectivité

La première action consiste à mener des tests de connectivité à la plateforme, en se basant sur 2 logiciels : Nmap et MongoDBCompass.

a) *Nmap*

Nmap, « Network Mapper », est un logiciel open source, spécialisé dans le scan de ports créé en 1997, permettant de voir quels ports d'une adresse donnée est ouvert ou fermée, et en interface graphique.

On scanne les ports concernés, 21 et 27017, du serveur, en rentrant cette commande dans nmap.

Target: 173.212. [REDACTED]

Command: nmap -p 21,27017 173.212. [REDACTED]

Le logiciel affiche une sortie avec les résultats pour chaque port. Ils sont actuellement fermés.

```
Nmap Output  Ports / Hosts  Topology  Host Details  Scans
nmap -p 21,27017 173.212. [REDACTED]

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-25 16:30 Paris, Madrid
Nmap scan report for m4696.contaboserver.net (173.212. [REDACTED])
Host is up (0.032s latency).

PORT      STATE SERVICE
21/tcp    [REDACTED] ftp
27017/tcp [REDACTED] mongod

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds
```

Ouverture de ports sur serveurs distants

b) MongoDB Compass

MongoDB est un système de gestion de base de données non relationnelles, open source et disponible depuis 2009. Compass est un outil permettant de manipuler MongoDB est interface graphique, et permet de tester la connexion à une base de données MongoDB.

On se connecte à l'aide des identifiants, en super utilisateur (root) et avec un mot de passe, l'IP publique du serveur et le port concerné.

New Connection ✕

Manage your connection settings

URI ⓘ Edit Connection String

mongodb://root:*****@173.212.212.212:27017/

Name **Color**

173.212.212.212:27017 No Color

☐ **Favorite this connection**
Favoriting a connection will pin it to the top of your list of connections

➤ **Advanced Connection Options**

How do I find my connection string in Atlas?
If you have an Atlas cluster, go to the Cluster view. Click the 'Connect' button for the cluster to which you wish to connect.
[See example](#)

How do I format my connection string?
[See example](#)

ⓘ TLS/SSL is disabled. If possible, enable TLS/SSL to avoid security vulnerabilities.

Cancel Save Save & Connect

La connexion est impossible ; le port 27017 ne répond pas.

173.212.212.212:27017 ✕

Manage your connection settings

URI ⓘ Edit Connection String

mongodb://root:*****@173.212.212.212:27017/

Name **Color**

173.212.212.212:27017 No Color

☐ **Favorite this connection**
Favoriting a connection will pin it to the top of your list of connections

➤ **Advanced Connection Options**

How do I find my connection string in Atlas?
If you have an Atlas cluster, go to the Cluster view. Click the 'Connect' button for the cluster to which you wish to connect.
[See example](#)

How do I format my connection string?
[See example](#)

ⓘ TLS/SSL is disabled. If possible, enable TLS/SSL to avoid security vulnerabilities.

⚠ connect ECONNREFUSED 173.212.212.212:27017

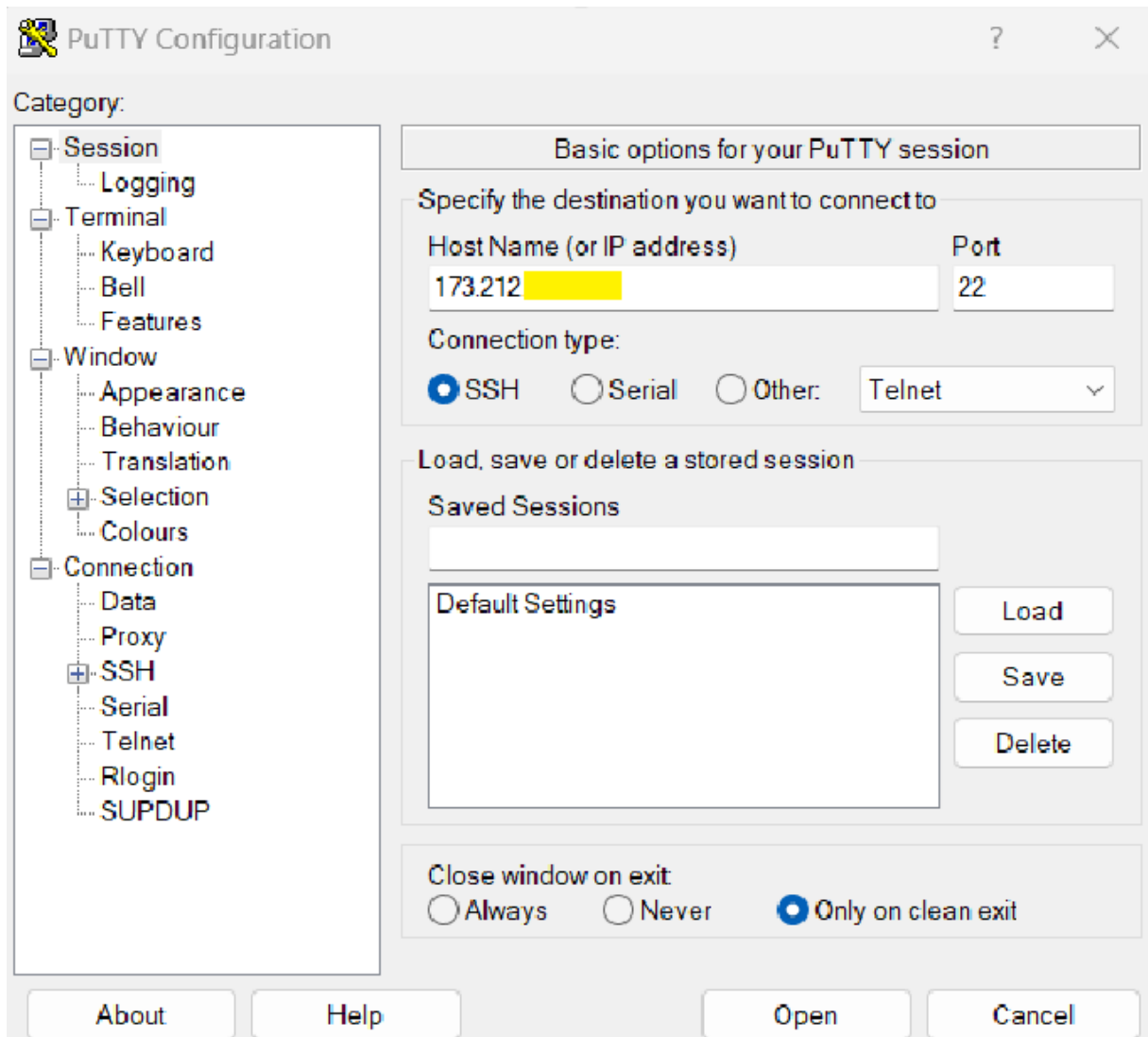
Cancel Save Connect Save & Connect

Ouverture de ports sur serveurs distants

3) Ouverture des ports

a) Vérification des ports

La première étape consiste à se connecter au serveur dysfonctionnant. Il s'agit d'un serveur Linux en ligne de commande, on se connecte en utilisant le logiciel tiers *PuTTY*, spécialisé dans les connexions à distance et prenant en charge divers protocoles, en SSH (port 22) en rentrant l'adresse publique du serveur.



Ouverture de ports sur serveurs distants

On se connecte sur le serveur en entrant les identifiants, en super utilisateur (*root*).

```
login as: root
root@173.212. [REDACTED]'s password:
Access denied
root@173.212. [REDACTED]'s password:
Access denied
root@173.212. [REDACTED]'s password:
Linux m4696.contaboserver.net 5.10.0-28-amd64 #1 SMP Debian 5.10.209-2 (2024-01-31) x86_64

      _ _ _ _ _
     /   /   /   /
    /___/___/___/___/
   /___/___/___/___/
  /___/___/___/___/
 /___/___/___/___/
/___/___/___/___/

Welcome!

This server is hosted by Contabo. If you have any questions or need help,
please don't hesitate to contact us at support@contabo.com.

Last login: Mon Nov  4 14:29:30 2024 from 176.134. [REDACTED]
root@m4696:~#
```

On rentre des commandes pour vérifier l'état des ports, s'ils sont ouverts.

```
root@m4696:~# ss -tuln | grep -E ':21|:27017'
tcp [REDACTED] 4096 0.0.0.0:27017 0.0.0.0:*
tcp [REDACTED] 32 *:21 *:*
```

b) Ouverture des ports

On ouvre les connexions entrantes des ports à l'aide d'iptables.

```
root@m4696:~# iptables -A INPUT -p tcp --dport 21 -j ACCEPT
root@m4696:~# iptables -A INPUT -p tcp --dport 27017 -j ACCEPT
```

On ouvre les connexions sortantes des ports à l'aide d'iptables.

```
root@m4696:~# iptables -A OUTPUT -p tcp --dport 21 -j ACCEPT
root@m4696:~# iptables -A OUTPUT -p tcp --dport 27017 -j ACCEPT
```

Ouverture de ports sur serveurs distants

c) Revérification des ports

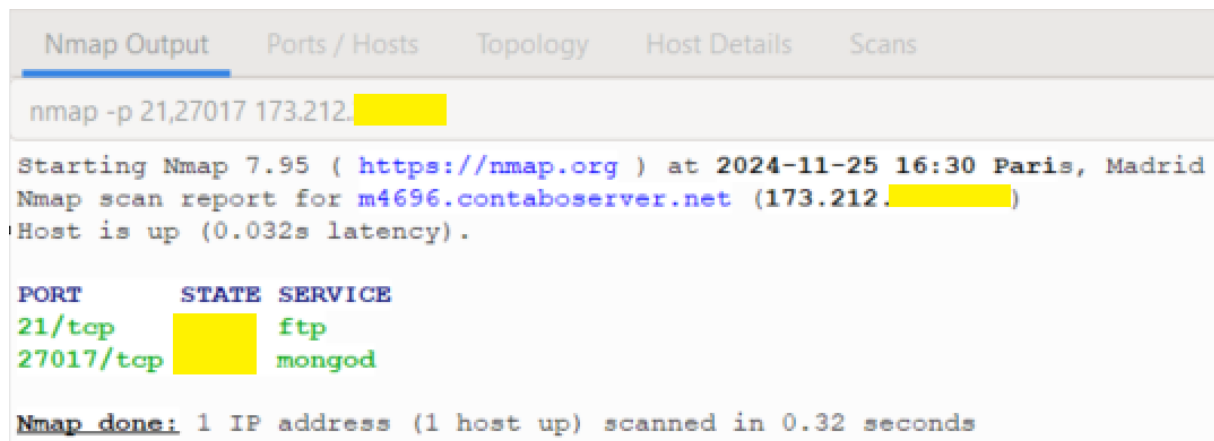
Maintenant que les ports ont été ouverts, on revérifie leur état.

```
root@m4696:~# iptables -L -n
Chain INPUT (policy ACCEPT)
target     prot opt source                destination
ACCEPT     tcp  --  0.0.0.0/0              0.0.0.0/0             tcp dpt:21
ACCEPT     tcp  --  0.0.0.0/0              0.0.0.0/0             tcp dpt:27017
```

Les ports sont bien ouverts.

d) Revérification connectivité

On revérifie la connectivité.



The screenshot shows the Nmap interface with tabs for Nmap Output, Ports / Hosts, Topology, Host Details, and Scans. The Nmap Output tab is active, displaying the command `nmap -p 21,27017 173.212.10.10`. The output text indicates the scan was performed on 2024-11-25 at 16:30 Paris, Madrid, for host `m4696.contaboserver.net` (173.212.10.10). The host is up with a latency of 0.032s. The scan results show two open ports: 21/tcp (ftp) and 27017/tcp (mongod). The scan was completed in 0.32 seconds.

PORT	STATE	SERVICE
21/tcp	open	ftp
27017/tcp	open	mongod

Nmap done: 1 IP address (1 host up) scanned in 0.32 seconds

Ça ne répond toujours pas. Il faut vérifier les services associés aux ports.

Ouverture de ports sur serveurs distants

4) Services

a) Vérification des services

Les services ne sont pas installés.

```
root@m4696:~# mongod --version
-bash: mongod: command not found
root@m4696:~# mongo --version
-bash: mongo: command not found
root@m4696:~# systemctl status mongod
Unit mongod.service could not be found.
root@m4696:~# dpkg -l | grep mongodb
```

Il faut installer les services associés, FTP et MongoDB.

b) Installation des services

Il faut installer le service FTP.

```
root@m4696:~# apt install vsftpd
```

Il faut démarrer le service.

```
root@m4696:~# systemctl start vsftpd
root@m4696:~# systemctl enable vsftpd
Synchronizing state of vsftpd.service with SysV service script with /lib/systemd/systemd-sysv-install.
Executing: /lib/systemd/systemd-sysv-install enable vsftpd
```

On vérifie la connectivité du port.

```
nmap -p 21 173.212.222.196

Starting Nmap 7.95 ( https://nmap.org ) at 2024-11-26 09:34 Paris, Madrid
Nmap scan report for m4696.contaboserver.net (173.212.222.196)
Host is up (0.021s latency).

PORT      STATE SERVICE
21/tcp    open  ftp

Nmap done: 1 IP address (1 host up) scanned in 0.27 seconds
```

La connectivité est établie pour le port 21.

Ouverture de ports sur serveurs distants

5) Relance des conteneurs

a) Relance des images Docker

L'architecture logicielle de la plateforme repose sur Docker, une plateforme de conteneurisation, c'est-à-dire de virtualisation au niveau du système d'exploitation, permettant de faire tourner des applications et d'autres programmes impliqués dans leur fonctionnement.

Ici, la base de données non relationnelle MongoDB est conteneurisée dans une image Docker.

Le fournisseur Contabo, en déménageant ses infrastructures, a interrompu le fonctionnement des images Docker, et donc empêché la plateforme de pouvoir communiquer avec sa base de données MongoDB.

Il faut relancer les images Docker.

On vérifie la version de Docker.

```
root@m4696:~# docker --version
Docker version 20.10.5+dfsg1, build 55c4c88
```

On liste les images Docker tournant actuellement.

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS	NAMES
73f6d97d4ab4	gps-fastapi	"uvicorn api.src.app..."	4 months ago	Up 3 weeks	0.0.0.0:6500->8000/tcp	gps-fastapi
85aa422a5fcc	gps-socket	"python ./socket/src..."	4 months ago	Up 3 weeks	0.0.0.0:6600->6600/tcp	gps-socket
ef5358edb0dc	mongo	"docker-entrypoint.s..."	4 months ago	Up 3 weeks	0.0.0.0:27017->27017/tcp	gps-mongo

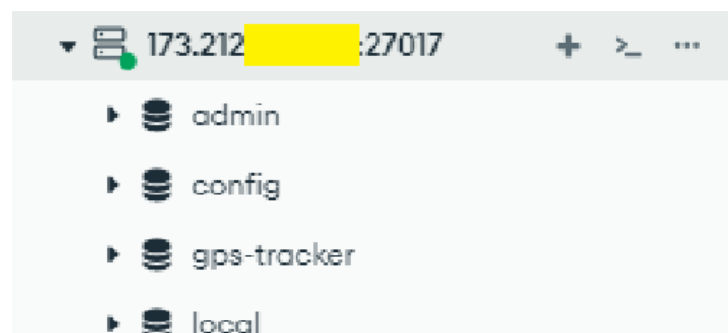
On relance l'image Docker impliquée, celle contenant la base de données MongoDB.

```
root@m4696:~# docker start gps-mongo
gps-mongo
```

L'image est relancée.

b) Vérification connectivité de la base de données

On vérifie la connectivité à la base de données en utilisant MongoDB Compass.



La connectivité est rétablie, on a l'arborescence.

Ouverture de ports sur serveurs distants

Conclusion

Cette mission a permis de résoudre les problèmes de connectivité rencontrés sur le serveur distant hébergé par Contabo pour la société Sikiwis.

À travers une série d'interventions techniques, nous avons :

- Diagnostiqué les ports fermés à l'aide d'outils comme Nmap et MongoDB Compass.
- Ouvert les ports nécessaires (21 pour FTP et 27017 pour MongoDB) en configurant correctement les règles iptables.
- Installé et configuré les services liés aux ports, notamment FTP et MongoDB, pour assurer leur disponibilité.
- Relancé les conteneurs Docker, essentiels au fonctionnement de la base de données MongoDB, pour garantir une connectivité stable.

Ces étapes ont permis de rétablir les services critiques pour le client de Sikiwis, les Centres hospitaliers de Mayotte, notamment l'accès à leur plateforme de tracking GPS. Cette intervention a démontré l'importance de maîtriser les outils réseau, la configuration des pare-feux, et la gestion des services conteneurisés.

En somme, cette mission a non seulement résolu le problème initial, mais également renforcé l'infrastructure pour prévenir de futures interruptions similaires.