AP 1.2 Phase 1

Mise en place d'une plateforme collaborative CLOUD

Elaboré par

Yann Duffay

Promotion

1 TSIO Groupe 1

Année scolaire

2023-2024

SOMMAIRE

I. Introduction..... 3
II. Installation de Nextcloud.....4
III. Installation et configuration de Fail2ban pour SSH.....7
IV. Installation et configuration de l'application Nextcloud sur un client Windows & smartphone.....8
V. SAUVEGARDE de la SOLUTION Automatisation / Sauvegarde & Restauration.....9
VI. Fiche de configuration du SERVEUR et du CLIENT.....10
6.1. Configuration Serveur..... 10
6.2. Configuration Client.....10
VII. Conclusion..... 11

I. Introduction

Dans cette première phase d'AP 1.2 l'objectif sera de mettre en place une plateforme collaborative CLOUD. La société "SIO Communication"désire de mettre à disposition de l'ensemble de ses salariés un service sécurisé de stockage de fichiers en ligne accessible depuis un navigateur de type Nextcloud.

II. Installation de Nextcloud

Dans un premier temps il faut installer un serveur LAMP et des paquets nécessaires pour le fonctionnement :

```
apt install curl apache2 php php-mysql php-mbstring php-gd
php-json phpcurl php-intl mcrypt php-imagick php-xml php-zip
php-ldap mariadb-server fail2ban ssh
```

```
mysql
```

On créé la base de donnée nextcloud:

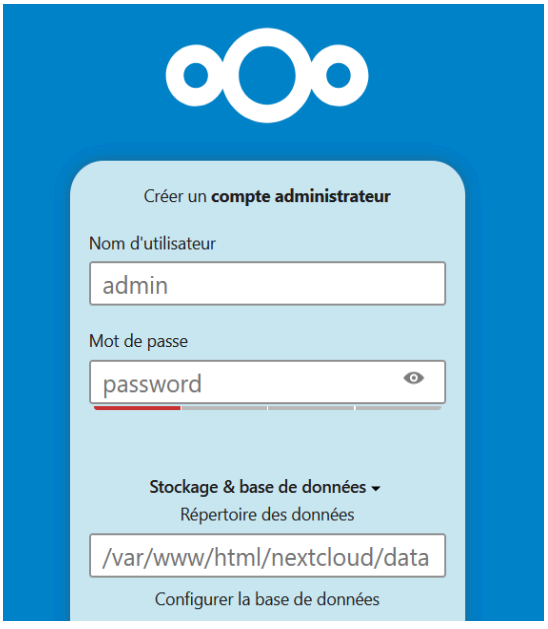
```
create database nextcloud;
```

```
grant all privileges on nextcloud.* to 'nextcloud'@'localhost'
identified by 'password';
```

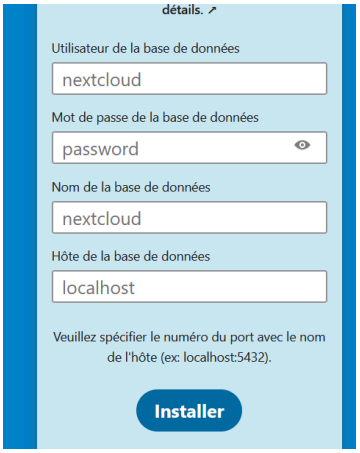
```
flush privileges;
```

Afin de pouvoir administrer le serveur Nextcloud il faut connaître l'@ip configurer sur la vm :

➥ http://192.168.69.3/nextcloud/index.php



Une fois sur le site, il faut créer un compte utilisateur. Dans ce cas on choisit 'admin' comme login et en mot de passe 'password'.



Sur notre vm on peut visualiser l'espace de stockage des fichiers partagés par Nextcloud:

```
root@debian-yduffay:/var/www/html/nextcloud/data# ls
admin  appdata_oc6g0hjnwhg7  files_external  index.html  nextcloud.log
```

Fail2Ban est un outil de sécurité permettant d'empêcher une attaque par force brute. Pour ce faire, Il analyse les fichiers journaux **/var/log/auth.log** et interdit les adresses IP qui effectuent trop de tentatives de connexion infructueuses.

Il prend en compte toutes les @ips, c'est pourquoi il faut ajouter à la liste blanche notre @ip pour éviter de bloquer l'accès à son serveur.

On édite le fichier /etc/fail2ban/jail.conf :

```
ignoreip = 127.0.0.1/8 ::1 192.168.69.3
```

Solution pour le Fail2Ban :
On ajoute la commande
`backend = systemd`
Le paquet rsyslog doit être installé.

`systemctl restart fail2ban.service` permet de redémarrer le service pour qu'il puisse prendre en considération les modifications effectuées.

`systemctl status fail2ban.service` si l'on souhaite visualiser si le service est actif ou non.

III. Installation et configuration de Fail2ban pour SSH

Après avoir installé Fail2ban, il faut créer un paragraphe qui va décrire la surveillance de SSH. Cette configuration spécifique s'ajoute dans le fichier /etc/fail2ban/.

Tout d'abord, on procède à la suppression du fichier `defaults-debian.conf` qui se trouve dans le répertoire /etc/fail2ban/jail.d, la commande `rm` permet de supprimer un fichier.

```
root@debian-yduffay:/etc/fail2ban# cd jail.d/
root@debian-yduffay:/etc/fail2ban/jail.d# ls
defaults-debian.conf
root@debian-yduffay:/etc/fail2ban/jail.d# rm defaults-debian.conf
root@debian-yduffay:/etc/fail2ban/jail.d# ls
root@debian-yduffay:/etc/fail2ban/jail.d# _
```

Maintenant nous créons un fichier "monsshd" avec la commande `cat` :

```
root@debian-yduffay:/etc/fail2ban/jail.d# cat > monsshd.conf
^C
root@debian-yduffay:/etc/fail2ban/jail.d# ls
monsshd.conf
```

On configure le fichier :

```
[sshd]
backend = auto
enabled = true
maxretry = 3
```

Puis on vérifie que la configuration dédiée à ssh fonctionne :

```
root@debian-yduffay:/etc/fail2ban# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

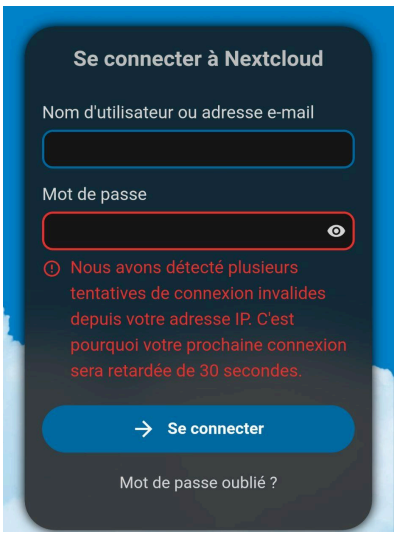
IV. Installation et configuration de l'application Nextcloud sur un client Windows & smartphone

4.1. Configuration de l'application Nextcloud sur un Smartphone

Pour installer l'application nextcloud, il faut se rendre directement sur le Playstore ou l'Appstore et rechercher "nextcloud".

Une fois installer et bien connecté au wifi BTS-SIO, il suffit de rentrer l'adresse de notre serveur: http://192.168.69.3/nextcloud/index.php

Il suffit plus qu'à nous connecter avec l'utilisateur 'admin' et le mot de passe 'password'.

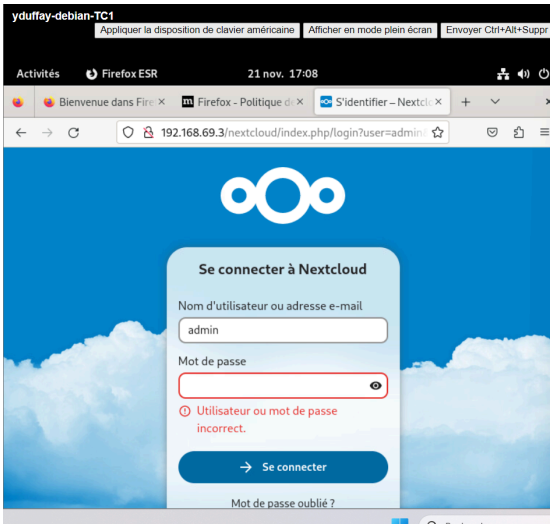


4.1. Windows

Mon jail est bien actif :

```
root@debian-yduffay:/etc/fail2ban/jail.d# fail2ban-client status
Status
|- Number of jail:      1
`- Jail list:   sshd
```

Depuis ma vm (192.168.69.2) je vais essayer de me connecter au nextcloud en me trompant successivement plusieurs fois afin de tester si le ban mis en place fonctionne.



Avant	Après
`root@debian-yduffay:/etc/fail2ban/jail.d# fail2ban-client status sshd` `Status for the jail: sshd` `|- Filter` `|  |- Currently failed: 0` `|  |- Total failed:  0` `|  `- File list: /var/log/auth.log` ``- Actions` ` |- Currently banned: 0` ` |- Total banned: 0` ` `- Banned IP list:`	

V. SAUVEGARDE de la SOLUTION Automatisation / Sauvegarde & Restauration

Script :

```
sudo mysqldump --databases nextcloud> saveNC_$(date
+'%Y-%m-%d_%H-%M').sql
mv saveNC_$(date + '%Y-%m-%d_%H-%M').sql /root/save
```

VI. Fiche de configuration du SERVEUR et du CLIENT

6.1. Configuration Serveur

Paramètres	Valeurs
Nom de la machine	yduffay-Linux-AP2
Système d'exploitation	Linux Debian sans interface graphique
Adresse IP	192.168.69.3
Masque de sous-réseaux	255.255.255.0
Passerelle	192.168.69.254
VLAN	469
DNS	192.168.10.1

6.2. Configuration Client

Paramètres	Valeurs
Nom de la machine	yduffay-debian-TC1
Système d'exploitation	Linux Debian
Adresse IP	192.168.69.2
Masque de sous-réseaux	255.255.255.0
Passerelle	192.168.69.254
VLAN	469
DNS	192.168.10.1

VII. Conclusion