STS SIO
Bloc 1 - Déploiement
TD
Session 2024-2025

TD – Déploiement de service « NextCloud »

Contexte

Votre responsable vous demande de déployer un service Nextcloud (solution d'hébergement de fichier et de collaboration en ligne – url : https://nextcloud.com/fr/) sur un nouveau serveur de l'entreprise. Le service devra être déployé de manière sécurisé afin de garantir un degré de protection satisfaisant à la fois du point de vue des accès mais aussi de la confidentialité des données déposé sur le service.

Document n°1 : Configuration du serveur

OS : Debian 12
Version « Nextcloud » : 31
Url de dépôt : wget https://download.nextcloud.com/server/releases/
Nom de domaine : localhost
Infrastructure : Machine virtuelle (cf : Shared > Vms > Cybersécurité > Deb12-Clean.ova)
Le dossier de nextcloud devra se trouver dans le répertoire /var/www/html/nextcloud

Document n°2 : Déploiement "NextCloud"

Pour le déploiement la solution « NextCloud » à besoin d'un certain nombre de dépendances énumérées ci-dessous :

Serveur web apache2
Serveur de base de données MariaDB + Base de données dédiée + Compte applicatif
Php + extensions (php-gd php-json php-mysql php-curl php-mbstring php-intl php-imagick php-xml php-zip)

La solution devra se trouver dans le dossier /var/www/html/ et le dossier NextCloud devra posséder des droits cohérents pour l'ensemble des utilisateurs du serveur.

Voici la procédure pour procéder au téléchargement de « NextCloud »

```
wget https://download.nextcloud.com/server/releases/nextcloud-XX.tar.bz2 tar -xjf nextcloud-XX.tar.bz2 mv nextcloud /var/www/html/nextcloud
```

Document n°3 : Procédure de sécurisation

Afin de pouvoir fournir un degré de protection suffisant sur le serveur afin de le protéger contre les attaques par brute force ou dénie de service il conviendra de configurer les outils suivants :

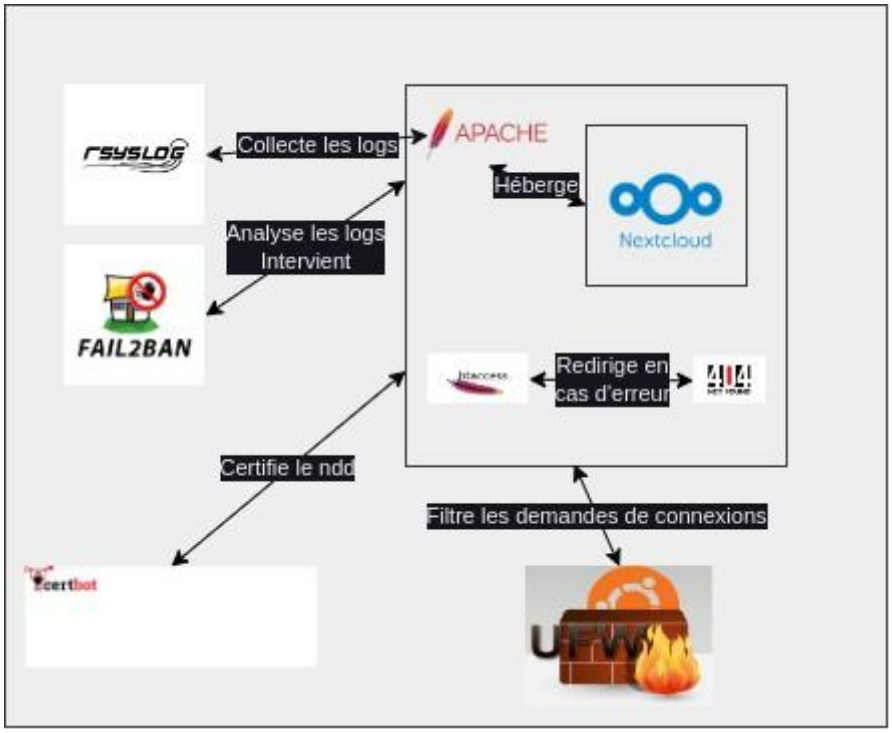
Fail2Ban avec une protection contre les bots, les chargements de scripts et les requêtes non usuelles. L'outil devra être raccordé au serveur web apache.
Rsyslog pour organiser la collecte des connexions et des évènements sur le serveur.
OpenSSL pour la signature du nom de domaine et permettre ainsi la mise en place du protocole HTTPS.
Le pare-feu (ufw) doit être configuré pour n'accepte que les connexions sur les ports HTTP et HTTPS avec une redirection automatique sur le HTTPS. Les services non-essentiels doivent être stoppés..

Document n°4 : Feuille de route

Test	Validé	
	Oui	Non
1 - Installation des dépendances pour « NextCloud »		
2 – Installation du serveur web et du serveur de base de données		
3 – Dépôt de l'application « NextCloud » dans le serveur apache		
4 – Installation des services « Rsyslog » et « Fail2Ban »		
5 – Mise en place d'un certificat « SSL » et activation du protocole « HTTPS »		

6 – Mise en place de la redirection « HTTP » vers « HTTPS »		
8 – Limitation des services activés		
9 – Limitation des ports autorisés (80 et 443)		

Document n°5 : Architecture de la solution



Document n°6 : Documentation Fail2Ban

Fail2ban est une application permettant de gérer les fichiers de journalisations (logs) de services intégrés dans les distributions Linux (apache, nginx…). Elle se repose sur la recherche de motifs sur le contenu des fichiers de journalisation afin de détecter des comportements suspects ou malveillants commis par les utilisateurs d'un service. Ce service permet d'offrir une protection sommaire contre les attaques de type « déni de service » ou « injection de script ».

Voici les commandes préalables pour intégrer le service fail2ban sous Debian

```
apt-get install fail2ban
cp /etc/fail2ban/jail.conf /etc/fail2ban/jail.local
vim /etc/fail2ban/jail.local
```

Pour aller plus loin : https://doc.ubuntu-fr.org/fail2ban

Document n°7 : Documentation openSSL

Ce bloc logiciel permet de générer des certificats SSL autosigné. Cet outil est
Voici les commandes pour implémenter openSSL avec un serveur web apache 2 sous un environnement Debian

```
#Installation des dépendances
sudo apt update && sudo apt install -y openssl apache2

#Génération d'une clé de chiffrement
sudo openssl genpkey -algorithm RSA -out
/etc/ssl/private/apacheselfsigned.key -aes256

#Génération d'un certificat autosigné
sudo openssl req -new -x509 -sha256 -key
/etc/ssl/private/apacheselfsigned.key -out /etc/ssl/certs/apache-selfsigned.crt -
days 365

#Modification ou création d'une configuration pour activer le HTTPS
sudo nano /etc/apache2/sites-available/default-ssl.conf

<IfModule mod_ssl.c>
    <VirtualHost *:443>
        ServerAdmin webmaster@localhost
        DocumentRoot /var/www/html

        SSLEngine on
        SSLCertificateFile      /etc/ssl/certs/apache-selfsigned.crt
        SSLCertificateKeyFile   /etc/ssl/private/apache-selfsigned.key

        <FilesMatch "\.(cgi|shtml|phtml|php)$">
            SSLOptions +StdEnvVars
</FilesMatch>

        <Directory /usr/lib/cgi-bin>
SSLOptions +StdEnvVars
        </Directory>

        ErrorLog ${APACHE_LOG_DIR}/error.log
```

```
        CustomLog ${APACHE_LOG_DIR}/access.log combined
    </VirtualHost>
</IfModule>

sudo a2enmod ssl sudo
a2ensite default-ssl

# Modification du fichier ports.conf pour activer l'écoute sur le port 443 ou vérifier la présence de ces lignes sudo nano /etc/apache2/ports.conf

listen 80
<IfModule ssl_module>
        Listen 443
</IfModule>

<IfModule mods_gnutls.c>
        Listen 443 </IfModule>
sudo systemctl restart
apache2
```

Pour aller plus loin : https://www.kinamo.fr/base-de-connaissanse/opensslcommandes-utiles

Document n°8 : Documentation .htaccess

Les fichiers .htaccess permettent de configurer un serveur avec des droits spécifiques au niveau de chaque répertoire faisant partie de celui-ci. Ce mécanisme permet de définir des comportements spécifiques pour chaque application se trouvant dans le répertoire. On retrouve dans ces fichiers un ensemble de paramétrages possibles comme :

Paramétrage	Opérateur + Exemple
Réécriture d'URL	RewriteRule "^images/(.+)\.jpg" "images/$1.png" Dans cet exemple on change le type de fichier des images.
Gestion des accès Filtrage sur IP	<AuthzProviderAlias ip reject-ips "XXX.XXX.XXX.XXX YYY.YYY.YYY.YYY"> </AuthzProviderAlias> <Directory "/path/to/dir"> <RequireAll>

	Require not reject-ips Require all granted </RequireAll> </Directory> Dans cet exemple deux adresses IP sont rejetées pour l'accès au serveur.
Authentification	AuthType Basic AuthName "Password Required" AuthUserFile "/www/passwords/password.file" AuthGroupFile "/www/passwords/group.file" Require group admins
Redirection	Error 404 /error/pageerreur404.html Dans cet exemple les erreurs 404 seront redirigées vers une page d'erreur dédiée.

Toutefois, la mise en place de cet outil nécessite l'activation de certains paramètres afin d'interagir avec le serveur Apache. Voici les commandes à exécuter pour procéder à l'activation.

```
a2ensite nextcloud
a2enmod rewrite headers env dir mime
systemctl restart apache2
```

Pour aller plus loin : https://httpd.apache.org/docs/2.4/howto/htaccess.html

Document n°9 : Installation de RsysLog

Rsyslog est une couche logicielle permettant de gérer les fichiers de journalisations sur des systèmes Unix. Il permet de mettre rapidement en œuvre un services pour organiser la collecte des évènements sur des technologies natives au sein des environnement Unix (apache, nginx). Quand fail2ban servira à l'analyse des fichiers de journalisation, la plateforme rsyslog assurera la collecte et la mise en place. Voici les commandes pour rattacher Rsyslog sous Apache avec NextCloud

```
echo 'module(load="imfile" PollingInterval="10")' >> /etc/rsyslog.conf echo 'input(type="imfile" File="/var/www/html/nextcloud/data/nextcloud.log" Tag="nextcloud" Severity="error" Facility="local7")' >> /etc/rsyslog.conf
systemctl restart rsyslog
```

Pour aller plus loin : https://www.rsyslog.com/doc/index.html

STS SIO
Bloc 1 - Déploiement
TD
Session 2024-2025

Travail à faire

1. Importez la machine virtuelle « Deb12-Clean » dans « Virtualbox »

2. Installez les dépendances nécessaires à l'installation de « Nextcloud »

3. Installez le serveur web et le serveur de base de données dans la même machine

4. Déployez l'application « Nextcloud » et procédez à son installation (BDD + paramétrage PHP)

5. Déployez les services « Rsyslog » et « Fail2Ban » (**Attention Rsyslog est à installer avant fail2ban).**

6. Déployez un certificat SSL à l'aide de l'outil «openSSL»

7. Installez la redirection des requêtes HTTP vers le trafic HTTPS.
a. Quel est l'objectif de cette démarche ?
b. Quel critère de la sécurité informatique protégez-vous en réalisant cette démarche ?

8. Listez les services actifs sur le serveur
a. Quels sont les services non essentiels ?

9. Stoppez les services précédemment identifiés.
a. Quel est l'objectif de cette démarche ?
b. Quel critère de la sécurité informatique protégez-vous en réalisant cette démarche ?

10. Activez le pare-feu et n'activez que les ports 80 et 443.
a. Pourquoi est-il prudent d'activer le port 80 avec le port 443 ?