Rapport SR2I309: Projet Cloud Public/Privé

Lucas MARACINE, Loic TESTA
Institut Mines Télécom-Télécom Paris Tech

19 janvier 2025

Résumé

Ce rapport propose la conception et la mise en œuvre d'une architecture cloud hybride pour une entreprise souhaitant sécuriser ses données critiques en tenant compte de leur sensibilité. L'objectif est de segmenter les données selon les niveaux de classification TLP (Traffic Light Protocol), permettant de définir leur emplacement de stockage approprié entre un cloud public et un cloud privé.

Une instance Nextcloud a été déployée pour gérer les données à faible sensibilité (TLP :WHITE et TLP :GREEN) dans un environnement public, tandis qu'une machine virtuelle dédiée gère les données sensibles (TLP :AMBER et TLP :RED) dans un environnement privé. La connexion entre les deux environnements est sécurisée à l'aide d'un VPN WireGuard, renforcé par des règles de pare-feu restrictives.

Un contrôle d'accès strict est mis en place, avec une gestion fine des utilisateurs et des groupes, garantissant que seuls les utilisateurs habilités accèdent aux ressources correspondantes. Par ailleurs, des mécanismes de journalisation avancés de NextCloud permettent de surveiller en temps réel la sécurité et les performances de l'architecture. Cette solution répond aux exigences de protection des données critiques tout en maintenant une accessibilité optimisée pour les utilisateurs autorisés.

L'entièreté du code et des implémentations sont disponibles à l'adresse suivante :
A DEFINIR

Table des matières

1 Installation Rapide et Automatisée de Debian **3**
1.1 Script de Déploiement 3
1.2 Configuration par Défaut 3

2 Classification TLP : Traffic Light Protocol **3**
2.1 Les Niveaux de Classification TLP 3
2.2 Utilisation Pratique dans ce Projet 4
2.3 Illustration Visuelle de la Classification TLP 5

3 Création de deux VM distinctes **5**
3.1 VM Nextcloud . . . 5
3.2 VM Stockage Privé . . . 5

4 Connexion WireGuard entre les Deux VMs **5**
4.1 Configuration du Côté Proxmox . . . 6
4.2 Configuration de WireGuard sur les VMs . . . 6
4.2.1 VM-NAS (cloud privé) . . . 6
4.2.2 VM-Nextcloud (cloud public) . . . 7

5 Setup de Nextcloud (VM Nextcloud) et du cloud privé (VM NAS) **7**
5.1 Installation des Dépendances . . . 7
5.2 Configuration d'Apache . . . 8
5.3 Activation de la Configuration Apache . . . 8
5.4 Configuration des Identifiants Nextcloud . . . 8
5.5 Résolution des Erreurs Potentielles . . . 8
5.6 Installation de Modules PHP Requis . . . 9
5.7 Configuration des Habilitations TLP . . . 9
5.7.1 Création des Dossiers . . . 9
5.7.2 Création des Groupes . . . 9
5.7.3 Ajout des Utilisateurs . . . 9
5.7.4 Ajout vers les Niveaux Inférieurs d'Habilitation . . . 9
5.7.5 Liste et Informations sur les Utilisateurs . . . 10
5.8 Gestion des Fichiers et Accès . . . 10
5.8.1 TLP_WHITE : Lecture Universelle sans Modification . . . 10
5.8.2 TLP_GREEN : Lecture/Écriture pour le Personnel Interne . . . 10
5.8.3 Journalisation des Modifications . . . 11
5.8.4 TLP_AMBER : Lecture/Écriture et Consultation Treemap pour le Personnel Habilité 11
5.9 Configuration SFTP pour le Stockage Externe . . . 12
5.9.1 Configuration sur `VM-NAS` . . . 12
5.9.2 Configuration sur `VM-NEXTCLOUD` . . . 13
5.10 TLP_RED : Consultation Treemap et Lecture/Écriture avec Jetons pour le Personnel Habilité 14
5.10.1 Préparation de la VM-NAS . . . 14
5.10.2 Configuration d'un Second Service SSH pour TLP_RED . . . 15
5.10.3 API Python pour Treemap et Téléchargement avec Jetons . . . 16
5.10.4 Points à Noter . . . 16

6 Améliorations Possibles et Recommandations de Sécurité **17**
6.1 Examen et Réduction des Failles Potentielles . . . 17
6.2 Amélioration de la Gestion des Mots de Passe . . . 17
6.3 Gestion des Utilisateurs et Groupes . . . 17
6.4 Renforcement des Règles de Pare-feu (iptables) . . . 17
6.5 Génération et Exploitation des Logs . . . 17
6.6 Sécurisation du Stockage des Données . . . 17
6.7 Gestion des Partages et des Accès . . . 18
6.8 Autres Axes de Sécurisation . . . 18

7 Accès à l'Environnement de POC **18**
7.1 Accès SSH aux Machines Virtuelles . . . 18
7.2 Accès à l'Instance Nextcloud . . . 18
7.3 Notes Importantes . . . 19

Expression du besoin

La gestion efficace des fichiers dans une entreprise, notamment dans des environnements nécessitant une segmentation stricte des données en fonction de leur sensibilité, est essentielle pour garantir la sécurité et la conformité des systèmes d'information. Ce projet vise à fournir une solution à déployer sur deux machines virtuelles (VM) dédiées :

— Une VM Nextcloud pour gérer les fichiers classifiés comme **TLP :WHITE** et **TLP :GREEN**.

— Une VM pour le stockage privé destinée aux fichiers sensibles **TLP :AMBER** et **TLP :RED**.

Nous reviendrons plus loin sur la signification de ces niveaux de sensiblité.
L'approche proposée repose sur une installation rapide et automatisée de Debian, configurée pour être immédiatement fonctionnelle. Cela permet de minimiser l'effort manuel, lors de la conception du POC. En Production, cela est géré par des solutions comme Ansible ou autre.

1 Installation Rapide et Automatisée de Debian

Le déploiement des machines virtuelles est géré par un script qui automatise l'installation de Debian sans interface utilisateur graphique (UIX). Ce script configure également les sources et les outils nécessaires pour une utilisation prête à l'emploi.

1.1 Script de Déploiement

Le script se trouve dans le répertoire `vm_auto_deploy` et peut être exécuté avec la commande suivante :

Listing 1 – Exécution du script de création de VM

```
./create_vm_debian.sh 102 192.168.100.3 test test
./create_vm_debian.sh <IP> <USER> <PASSWORD>
```

1.2 Configuration par Défaut

— Le script crée un utilisateur par défaut qui appartient au groupe `sudoers`.

— L'utilisateur peut exécuter `sudo bash` sans mot de passe.

— L'environnement inclut `zsh` et `oh-my-zsh` pour une expérience utilisateur améliorée.

2 Classification TLP : Traffic Light Protocol

La classification TLP (Traffic Light Protocol) est un standard de classification des informations basé sur des niveaux de sensibilité. Il est conçu pour faciliter le partage contrôlé d'informations en indiquant clairement les restrictions d'utilisation et de diffusion. Chaque niveau est représenté par une couleur, avec des règles spécifiques associées.

2.1 Les Niveaux de Classification TLP

— **TLP :RED** :

  — **Description** : Les informations classifiées en TLP :RED sont extrêmement sensibles. Leur diffusion est strictement limitée à l'audience présente au moment de leur partage.

  — **Exemples** : Discussions stratégiques confidentielles, informations critiques concernant la sécurité.

  — **Règles de Diffusion** : Ne peut être partagé avec aucune personne extérieure, même de manière informelle.

— **TLP :AMBER** :
  — **Description** : Les informations classifiées en TLP :AMBER sont sensibles mais peuvent être partagées avec des membres spécifiques d'une organisation ou d'un groupe.
  — **Exemples** : Alertes de sécurité nécessitant une action limitée à une équipe interne.
  — **Règles de Diffusion** : Diffusion limitée à ceux qui ont besoin de connaître l'information pour leur rôle spécifique.
— **TLP :GREEN** :
  — **Description** : Les informations TLP :GREEN peuvent être partagées à l'intérieur d'une communauté, mais pas rendues publiques.
  — **Exemples** : Bonnes pratiques de sécurité, rapports non sensibles à partager dans un cadre professionnel restreint.
  — **Règles de Diffusion** : Partage autorisé avec les membres de la communauté, mais diffusion publique interdite.
— **TLP :WHITE** :
  — **Description** : Les informations TLP :WHITE ne sont soumises à aucune restriction de diffusion. Elles peuvent être partagées librement.
  — **Exemples** : Communiqués de presse, rapports publics.
  — **Règles de Diffusion** : Partage sans aucune restriction.

2.2 Utilisation Pratique dans ce Projet

Dans ce projet, le TLP est utilisé pour classifier les fichiers et structurer les accès en fonction des niveaux de sensibilité :

— **TLP :WHITE** : Accès universel en lecture seule. Utilisé pour des fichiers à diffusion publique tels que des annonces ou des communiqués.
— **TLP :GREEN** : Lecture et écriture pour le personnel interne. Réservé à des fichiers non publics mais partageables à l'intérieur de l'organisation.
— **TLP :AMBER** : Lecture et écriture pour les membres habilités. Les fichiers sont stockés dans des environnements sécurisés avec des règles strictes d'accès.
— **TLP :RED** : Lecture et écriture restreinte avec contrôle par jeton. Les fichiers sont hautement sécurisés avec une gestion stricte des permissions et un contrôle précis des accès.

2.3 Illustration Visuelle de la Classification TLP

FIGURE 1 – Classification TLP. Source : `https://kravensecurity.com/traffic-light-protocol/`.

3 Création de deux VM distinctes

Deux machines virtuelles doivent être créées pour répondre aux besoins du projet :

3.1 VM Nextcloud

Cette VM sera utilisée pour stocker et gérer les fichiers classifiés comme **TLP :WHITE** et **TLP :GREEN**. Nextcloud offre une solution sécurisée et intuitive pour le partage et la gestion des fichiers.

3.2 VM Stockage Privé

Cette VM sera dédiée au stockage des données sensibles classifiées comme **TLP :AMBER** et **TLP :RED**. Elle devra être configurée avec des mesures de sécurité renforcées pour prévenir tout accès non autorisé. Cette VM est nottament sur un réseau Proxmox isolé (interface vmbr). En prod (MEP de la solution), l'unique accès se fait par tunnel VPN.

4 Connexion WireGuard entre les Deux VMs

Comme dit plus haut, pour sécuriser les communications entre les deux machines virtuelles, WireGuard sera utilisé pour établir une connexion VPN.

4.1 Configuration du Côté Proxmox

— Routage entre `vmbr1` et `vmbr3` :

```
ip route add 192.168.100.200 via 192.168.100.1 dev vmbr1
ip route add 10.20.10.10 via 10.20.10.1 dev vmbr3
```

— Configuration des `iptables` pour le trafic WireGuard et ICMP (uniquement debug avant MEP) :

```
# Autoriser ICMP entre 192.168.100.200 et 10.20.10.2
iptables -A FORWARD -i vmbr1 -s 192.168.100.200 -d 10.20.10.2 -p icmp \
-j ACCEPT

iptables -A FORWARD -o vmbr3 -s 10.20.10.2 -d 192.168.100.200 -p icmp \
-j ACCEPT

# Autoriser WireGuard (UDP) entre 192.168.100.200 et 10.20.10.2
iptables -A FORWARD -i vmbr1 -s 192.168.100.200 -d 10.20.10.2 -p udp \
--dport 51820 -j ACCEPT

iptables -A FORWARD -o vmbr3 -s 10.20.10.2 -d 192.168.100.200 -p udp \
--sport 51820 -j ACCEPT

# Bloquer le reste
iptables -A FORWARD -i vmbr3 ! -s 10.20.10.2 -j DROP
iptables -A FORWARD -o vmbr3 ! -d 10.20.10.2 -j DROP
iptables -A FORWARD -i vmbr1 ! -s 192.168.100.200 -j DROP
iptables -A FORWARD -o vmbr1 ! -d 192.168.100.200 -j DROP
```

— Les règles `INPUT` et `OUTPUT` restent inchangées pour permettre une gestion centralisée via Proxmox. Nottament les connexion SSH depuis l'extérieur. Mais dans l'absolu, il faudriat appliquer des règles de filtrage similaires !

4.2 Configuration de WireGuard sur les VMs

4.2.1 VM-NAS (cloud privé)

Dans la suite, vous pourrez parfois trouver la nomination de NAS pour la VM de cloud privé...

— Installation de WireGuard :

```
sudo apt update
sudo apt install wireguard
wg genkey | tee privatekey | wg pubkey > publickey
```

— Configuration dans `/etc/wireguard/wg0.conf` :

```
[Interface]
Address = 10.0.0.1/24
PrivateKey = <cle_privee_NAS>
ListenPort = 51820

[Peer]
PublicKey = <cle_publique_Nextcloud>
AllowedIPs = 10.0.0.2/32
Endpoint = 192.168.100.200:51820
PersistentKeepalive = 25
```

— Activation de WireGuard :

```
sudo systemctl start wg-quick@wg0
sudo systemctl enable wg-quick@wg0
```

4.2.2 VM-Nextcloud (cloud public)

— Installation de WireGuard :

```
sudo apt update
sudo apt install wireguard
wg genkey | tee privatekey | wg pubkey > publickey
```

— Configuration dans `/etc/wireguard/wg0.conf` :

```
[Interface]
Address = 10.0.0.2/24
PrivateKey = <cle_privee_Nextcloud>
ListenPort = 51820

[Peer]
PublicKey = <cle_publique_NAS>
AllowedIPs = 10.0.0.1/32
Endpoint = 10.20.10.2:51820
PersistentKeepalive = 25
```

— Activation de WireGuard :

```
sudo systemctl start wg-quick@wg0
sudo systemctl enable wg-quick@wg0
```

5 Setup de Nextcloud (VM Nextcloud) et du cloud privé (VM NAS)

La configuration de Nextcloud est effectuée sur la VM Nextcloud pour offrir une solution de gestion et de partage de fichiers sécurisée.

5.1 Installation des Dépendances

```
sudo apt update
sudo apt install wget git
wget https://download.nextcloud.com/server/releases/latest-9.zip

sudo apt install apache2 unzip
unzip latest-9.zip
sudo mv nextcloud /var/www/html/

sudo chown -R www-data:www-data /var/www/html/nextcloud
sudo chmod -R 750 /var/www/html/nextcloud
```

5.2 Configuration d'Apache

Modifiez le fichier `/etc/apache2/sites-available/nextcloud.conf` :

```
<VirtualHost *:80>
    ServerAdmin test@test.fr
    DocumentRoot /var/www/html/nextcloud
    ServerName localhost

    <Directory /var/www/html/nextcloud/>
        Require all granted
        AllowOverride All
        Options FollowSymLinks MultiViews
    </Directory>

    ErrorLog ${APACHE_LOG_DIR}/nextcloud_error.log
    CustomLog ${APACHE_LOG_DIR}/nextcloud_access.log combined
</VirtualHost>
```

5.3 Activation de la Configuration Apache

```
sudo a2dissite 000-default.conf
sudo a2ensite nextcloud.conf
sudo a2enmod rewrite headers env dir mime
sudo systemctl restart apache2
```

5.4 Configuration des Identifiants Nextcloud

Les identifiants et paramètres de base pour la configuration de Nextcloud sont les suivants :

- **Login** : `admin`
- **Password** : `ProxmoxGNS3_`
- **Nom de la base de données** : `nextcloud_db`
- **Compte utilisateur de la base de données** : `nextcloud_user@ProxmoxGNS3!`

5.5 Résolution des Erreurs Potentielles

En cas d'erreur lors de la connexion à la base de données :

```
sudo mysql -u root -p
SELECT user, host FROM mysql.user WHERE user = 'nextcloud_user';
DROP USER 'nextcloud_user'@'localhost';

# Creer un nouvel utilisateur sans afficher le mot de passe en clair
CREATE USER 'nextcloud_user'@'localhost' IDENTIFIED BY 'ProxmoxGNS3!';
GRANT ALL PRIVILEGES ON nextcloud_db.* TO 'nextcloud_user'@'localhost';
FLUSH PRIVILEGES;

# Verification de la connexion
mysql -u nextcloud_user -p -D nextcloud_db
```

5.6 Installation de Modules PHP Requis

```
sudo apt install php-xml
sudo apt install php-zip php-mbstring php-gd php-curl
```

5.7 Configuration des Habilitations TLP

Pour segmenter les données selon les habilitations TLP, les étapes suivantes sont effectuées sur la VM Nextcloud :

5.7.1 Création des Dossiers

```
sudo -u www-data mkdir -p /var/www/html/nextcloud/data/admin/files/TLP_WHITE
sudo -u www-data mkdir -p /var/www/html/nextcloud/data/admin/files/TLP_GREEN

# Reindexation des fichiers
sudo -u www-data php /var/www/html/nextcloud/occ files:scan --all
```

5.7.2 Création des Groupes

```
# Creer les groupes TLP_WHITE, TLP_GREEN, TLP_AMBER et TLP_RED
sudo -u www-data php /var/www/html/nextcloud/occ group:add TLP_WHITE_GROUP
sudo -u www-data php /var/www/html/nextcloud/occ group:add TLP_GREEN_GROUP
sudo -u www-data php /var/www/html/nextcloud/occ group:add TLP_AMBER_GROUP
sudo -u www-data php /var/www/html/nextcloud/occ group:add TLP_RED_GROUP
```

5.7.3 Ajout des Utilisateurs

```
# Ajouter des utilisateurs a chaque groupe
sudo OC_PASS="password_white" -u www-data php /var/www/html/nextcloud/occ \
user:add journaliste --password-from-env --group=TLP_WHITE_GROUP

sudo OC_PASS="password_drh" -u www-data php /var/www/html/nextcloud/occ \
user:add drh --password-from-env --group=TLP_GREEN_GROUP

sudo OC_PASS="password_amber" -u www-data php /var/www/html/nextcloud/occ \
user:add manager --password-from-env --group=TLP_AMBER_GROUP

sudo OC_PASS="password_red" -u www-data php /var/www/html/nextcloud/occ \
user:add directeur --password-from-env --group=TLP_RED_GROUP
```

5.7.4 Ajout vers les Niveaux Inférieurs d'Habilitation

```
# Ajouter des utilisateurs a des groupes inferieurs
sudo -u www-data php /var/www/html/nextcloud/occ group:adduser \
TLP_AMBER_GROUP directeur
sudo -u www-data php /var/www/html/nextcloud/occ group:adduser \
TLP_GREEN_GROUP directeur
```

```
sudo -u www-data php /var/www/html/nextcloud/occ group:adduser \
TLP_WHITE_GROUP directeur

sudo -u www-data php /var/www/html/nextcloud/occ group:adduser \
TLP_GREEN_GROUP manager
sudo -u www-data php /var/www/html/nextcloud/occ group:adduser \
TLP_WHITE_GROUP manager

sudo -u www-data php /var/www/html/nextcloud/occ group:adduser \
TLP_WHITE_GROUP drh
```

Toutes ces étapes sont évidemment voués à être automatisée dans un environement en Production

5.7.5 Liste et Informations sur les Utilisateurs

```
# Lister tous les utilisateurs
sudo -u www-data php /var/www/html/nextcloud/occ user:list

# Obtenir des informations sur un utilisateur specifique
sudo -u www-data php /var/www/html/nextcloud/occ user:info directeur
```

5.8 Gestion des Fichiers et Accès

5.8.1 TLP_WHITE : Lecture Universelle sans Modification

— **Création du dossier TLP_WHITE** :

```
sudo -u www-data \
mkdir -p /var/www/html/nextcloud/data/admin/files/TLP_WHITE

sudo -u www-data php /var/www/html/nextcloud/occ files:scan --all
```

— **Partage avec tous les utilisateurs** :

```
curl -X POST \
'http://127.0.0.1/nextcloud/ocs/v2.php/apps/files_sharing/api/v1/shares' \
-H 'OCS-APIRequest: true' \
-u 'admin:ProxmoxGNS3_' \
-d 'path=/TLP_WHITE&shareType=1&shareWith=TLP_WHITE_GROUP&permissions=1'
```

— `shareType=1` : Partage avec un groupe.
— `shareWith=TLP_WHITE_GROUP` : Groupe destinataire.
— `permissions=1` : Accès en lecture seule.

5.8.2 TLP_GREEN : Lecture/Écriture pour le Personnel Interne

— **Création du dossier TLP_GREEN** :

```
sudo -u www-data \
mkdir -p /var/www/html/nextcloud/data/admin/files/TLP_GREEN
sudo -u www-data php /var/www/html/nextcloud/occ files:scan --all
```

— **Partage avec les groupes TLP_GREEN_GROUP et supérieurs** :

```
curl -X POST \
'http://127.0.0.1/nextcloud/ocs/v2.php/apps/
files_sharing/api/v1/shares' \
-H 'OCS-APIRequest: true' \
-u 'admin:ProxmoxGNS3_' \
-d 'path=/TLP_GREEN&shareType=1&shareWith=TLP_GREEN_GROUP&permissions=15'

curl -X POST \
'http://127.0.0.1/nextcloud/ocs/v2.php/apps/files_sharing/api/v1/shares' \
-H 'OCS-APIRequest: true' \
-u 'admin:ProxmoxGNS3_' \
-d 'path=/TLP_GREEN&shareType=1&shareWith=TLP_AMBER_GROUP&permissions=15'

curl -X POST \
'http://127.0.0.1/nextcloud/ocs/v2.php/apps/files_sharing/api/v1/shares' \
    -H 'OCS-APIRequest: true' \
    -u 'admin:ProxmoxGNS3_' \
    -d 'path=/TLP_GREEN&shareType=1&shareWith=TLP_RED_GROUP&permissions=15'
```

— `path=/TLP_GREEN` : Chemin du dossier.`shareType=1` : *Partageavecungroupe.*
— `shareWith=TLP_GREEN_GROUP, TLP_AMBER_GROUP, TLP_RED_GROUP` : Groupes autorises.
— `permissions=15` : Acces en lecture, écriture, création et suppression.

5.8.3 Journalisation des Modifications

Pour suivre les modifications apportées aux fichiers (ajouts, suppressions, modifications), activez les applications de journalisation dans Nextcloud :

— **Activez les modules nécessaires** :

```
sudo -u www-data php /var/www/html/nextcloud/occ app:enable activity
sudo -u www-data php /var/www/html/nextcloud/occ app:enable \
files_accesscontrol
```

— **Configurez les notifications d'activité dans Nextcloud** :

```
sudo -u www-data php /var/www/html/nextcloud/occ activity:settings \
--user '*' --enable-email --type file_changed file_deleted \
file_restored file_created
```

Cela envoie des notifications pour les modifications des fichiers.

— **Pour propager les modifications** (normalement fait via l'interface Web) :

```
sudo -u www-data php /var/www/html/nextcloud/occ files:scan --all
```

5.8.4 TLP_AMBER : Lecture/Écriture et Consultation Treemap pour le Personnel Habilité

— **Point de Montage dédié** : On fait en sorte d'utiliser `/mnt` dans l'optique d'un NAS dédié à ce niveau. Tous les fichiers seront placés sous `/mnt/private/TLP_AMBER`.

— **Création du dossier** :

```
sudo -u www-data mkdir -p /mnt/private/TLP_AMBER
sudo -u www-data php /var/www/html/nextcloud/occ files:scan --all
```

— **Partage avec les groupes habilités** :

```
curl -X POST \
'http://127.0.0.1/nextcloud/ocs/v2.php/apps/files_sharing/api/v1/shares' \
    -H 'OCS-APIRequest: true' \
    -u 'admin:ProxmoxGNS3_' \
    -d 'path=/mnt/private/ \
    TLP_AMBER&shareType=1&shareWith=TLP_AMBER_GROUP&permissions=15'

curl -X POST \
'http://127.0.0.1/nextcloud/ocs/v2.php/apps/files_sharing/api/v1/shares' \
    -H 'OCS-APIRequest: true' \
    -u 'admin:ProxmoxGNS3_' \
    -d 'path=/mnt/private/ \
    TLP_AMBER&shareType=1&shareWith=TLP_RED_GROUP&permissions=15'
```

- `path=/mnt/private/TLP_AMBER` : Définit le chemin du dossier.
- `shareType=1` : Partage destiné à un groupe.
- `shareWith=TLP_AMBER_GROUP, TLP_RED_GROUP` : Groupes autorisés à accéder.
- `permissions=15` : Lecture, écriture, création et suppression.

5.9 Configuration SFTP pour le Stockage Externe

5.9.1 Configuration sur `VM-NAS`

- **Création et Configuration du Répertoire TLP_AMBER** :

```
sudo mkdir -p /mnt/private/TLP_AMBER

sudo groupadd tlp_amber
sudo chown -R root:tlp_amber /mnt/private/TLP_AMBER
sudo chmod -R 770 /mnt/private/TLP_AMBER
```

- **Configuration du Serveur SFTP dans `/etc/ssh/sshd.conf`** :

```
PermitRootLogin yes
PasswordAuthentication yes
ChallengeResponseAuthentication no

Subsystem sftp internal-sftp

Match Group tlp_amber
    ChrootDirectory /mnt/private/TLP_AMBER
    ForceCommand internal-sftp -u 002
    AllowTcpForwarding no
    X11Forwarding no
```

Cette configuration :

- Permet la connexion des utilisateurs appartenant au groupe `tlp_amber`.
- Restreint l'accès à SFTP uniquement (grâce à `internal-sftp` et `ForceCommand`).
- Applique un umask de `002` pour garantir que les fichiers créés ont les permissions appropriées.
- Désactive le forwarding et le X11 pour limiter les vecteurs d'attaque.

- **Ajout de Nouveaux Utilisateurs SFTP** : Pour chaque nouvel utilisateur, utilisez les commandes suivantes :

```
sudo useradd -m -G tlp_amber user_amber
sudo passwd user_amber
```

Ces commandes :
— Ajoutent l'utilisateur au groupe `tlp_amber`.
— Assurent que l'utilisateur puisse se connecter avec un mot de passe.

— **Création et Configuration du Sous-Dossier `/data` :**

```
sudo mkdir -p /mnt/private/TLP_AMBER/data
sudo chown root:tlp_amber /mnt/private/TLP_AMBER/data
sudo chmod g+s /mnt/private/TLP_AMBER
```

Cette configuration garantit que tous les fichiers créés dans le dossier `/data` hériteront des permissions du groupe.

— **Redémarrage du Serveur SSH :**

```
sudo systemctl restart sshd
```

5.9.2 Configuration sur `VM-NEXTCLOUD`

— **Activation de l'Application `files_external` :**

```
sudo -u www-data php /var/www/html/nextcloud/occ app:enable files_external
```

— **Création d'une Connexion SFTP :**

```
sudo -u www-data php /var/www/html/nextcloud/occ \
files_external:create /TLP_AMBER_SFTP \
sftp password::userprovided > VA RENVOYER UN IDENTIFIANT <ID>

sudo -u www-data php /var/www/html/nextcloud/occ \
files_external:config <ID> host "10.0.0.1"

sudo -u www-data php /var/www/html/nextcloud/occ \
files_external:config <ID> root "/data"

sudo -u www-data php /var/www/html/nextcloud/occ \
files_external:config <ID> port "22"
```

Ces commandes configurent l'accès SFTP pour le stockage TLP_AMBER depuis Nextcloud :
— `host "10.0.0.1"` : L'adresse IP de la VM-NAS.
— `root "/data"` : Le répertoire cible sur la VM-NAS.
— `port "22"` : Le port utilisé pour la connexion SFTP.

— **Activation du Partage des Fichiers via le GUI** : Dans l'interface administrateur de Nextcloud :
  — Allez dans **Administration** > **External storage**.
  — Activez l'option `Enable_sharing`.
  — Vérifiez que le mécanisme d'authentification est réglé sur `"User entered, store in database"`.

Cette configuration simplifie l'authentification des utilisateurs mais nécessite de synchroniser les mots de passe entre les utilisateurs sur les deux VM.

— **Permissions et Problèmes Courants :**
  — Assurez-vous que les permissions des fichiers créés dans `/data` sont correctes :
    — Permissions : `660`.
    — Propriétaire : `createur:tlp_amber`.
  — Si des problèmes d'accès surviennent, vérifiez les permissions sur le répertoire `/data`.

5.10 TLP_RED : Consultation Treemap et Lecture/Écriture avec Jetons pour le Personnel Habilité

Pour le niveau `TLP_RED` dans notre démonstration, la configuration sera similaire à celle de `TLP_AMBER`, mais indépendante. Cependant, Nextcloud nous impose des limitations techniques pour ce niveau.

Nous allons devoir reconnecter temporairement la VM-NAS à Internet pour installer certaines dépendances nécessaires. En production, assurez-vous de tous les aspects de sécurité (fichiers de configuration, pare-feu, etc.) avant cette étape.

5.10.1 Préparation de la VM-NAS

— **Connexion temporaire à Internet** :

1. Ajoutez une interface `virtio` connectée au NAT `vmbr1` dans Proxmox.
2. Assignez une IP dans le réseau `192.168.100.0/24`.
3. Ajoutez la route par défaut via la passerelle NAT :

```
ip route add default via 192.168.100.1
```

4. Vérifiez que la VM peut accéder à Internet avant de poursuivre.

— **Mise à jour et installation des dépendances nécessaires** :

```
sudo apt update
sudo apt install python3-pip
sudo python3 -m pip install flask paramiko
```

— **Configuration des Répertoires et des Permissions** :

```
sudo mkdir -p /mnt/private/TLP_RED
sudo mkdir -p /mnt/private/tokens
sudo touch /mnt/private/whitelist_tlp_red.txt
sudo chmod 660 /mnt/private/whitelist_tlp_red.txt
sudo chown root:tlp_red_group /mnt/private/whitelist_tlp_red.txt

echo "manager" | sudo tee -a /mnt/private/whitelist_tlp_red.txt
echo "directeur" | sudo tee -a /mnt/private/whitelist_tlp_red.txt

sudo chown -R root:tlp_red_group /mnt/private/TLP_RED
sudo chmod -R 750 /mnt/private/TLP_RED
```

— **Gestion des Groupes et des Utilisateurs** :

```
sudo groupadd tlp_red
sudo usermod -a -G tlp_red directeur
```

Ces étapes permettent :

— De restreindre l'accès au répertoire `/mnt/private/TLP_RED`.

— De gérer les utilisateurs autorisés à accéder via le groupe `tlp_red`.

Comme vous pourrez le constater dans le code de l'API, celle-ci fonctionne de la manière suivante :

— **1ère fonctionnalité : consultation du "tree" du répertoire TLP_RED**
Afin de consulter les répertoires disponibles dans le partage, un utilisateur doit être habilité `TLP:RED` (être dans le groupe `tlp_red`) et il doit également être explicitement cité dans le fichier `whitelist_tlp_red.txt` (accessible uniquement par les administrateurs).
— **2ème fonctionnalité : téléchargement de fichier**
Pour télécharger un fichier, un utilisateur doit non seulement satisfaire aux exigences de la première fonctionnalité, mais également disposer d'un token unique pour lui et le fichier. Ce token est généré (côté admin) par le script situé dans `/mnt/private/generate_tlp_red_token.py`.

Le point intéressant est ici de voir la forme du token :

{user} :{file_path} :{timestamp} :{SECRET_KEY}

Où `{user}` est l'utilisateur ayant explicitement besoin d'accéder au fichier, `{file_path}` représente le fichier en question, `{timestamp}` est le timestamp lors de l'émission du token, et `{SECRET_KEY}` est une clé secrète détenue par l'administrateur.

Vous le verrez dans le code, cette clé secrète est pour le moment stockée en clair, dans le code, pour les besoins du POC. Il est évident qu'un stockage robuste (saisie manuelle, token USB, etc.) est nécessaire dans un environnement en production.

5.10.2 Configuration d'un Second Service SSH pour TLP_RED

— **Configuration du Second SSHD** : Modifiez ou créez le fichier `/etc/ssh/sshd_config_red` :

```
Port 2223
PermitRootLogin no
Subsystem sftp internal-sftp

Match Group tlp_red
    ChrootDirectory /mnt/private/TLP_RED
    ForceCommand internal-sftp -u 002
    AllowTcpForwarding no
    X11Forwarding no
```

— **Création et Activation du Service SSH Secondaire** : Ajoutez un nouveau service pour SSH destiné à `TLP_RED` :

```
sudo nano /lib/systemd/system/ssh-red.service
```

Contenu du fichier `ssh-red.service` :

```
[Unit]
Description=OpenBSD Secure Shell server (TLP_RED)
After=network.target auditd.service

[Service]
EnvironmentFile=-/etc/default/ssh
ExecStart=/usr/sbin/sshd -D -f /etc/ssh/sshd_config_red
ExecReload=/bin/kill -HUP $MAINPID
KillMode=process
Restart=on-failure
RestartSec=42s
```

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

Redémarrez le service pour l'activer :

```
sudo systemctl daemon-reload
sudo systemctl enable ssh-red
sudo systemctl start ssh-red
```

5.10.3 API Python pour Treemap et Téléchargement avec Jetons

— **Test de l'API avec `curl` :**

```
curl -v -X POST http://10.0.0.1:5000/api/access_file \
    -H "Content-Type: application/json" \
    -d '{
        "user": "directeur",
        "password": "password_red",
        "file_path": "/data/TLP_RED1.txt",
        "token": "5f04298e0e29ff8dadb2b0ade3f6e69520913d58601ea74e479fd85c6b
    }' \
    -O -J
```

Explications :

— `user` : L'utilisateur effectuant la requête (`directeur` dans cet exemple).
— `password` : Mot de passe de l'utilisateur.
— `file_path` : Chemin complet du fichier demandé.
— `token` : Jeton valide généré par l'administrateur.

Cette requête retourne le fichier demandé en fonction des permissions et de la validité du jeton.

— **Test de treemap avec `curl` :**

```
curl -X POST http://10.0.0.1:5000/api/tlp_red_tree \
-H "Content-Type: application/json" \
-d '{
  "user": "directeur",
  "password": "password_red"}'
```

Explications :

— `user` : L'utilisateur effectuant la requête (`directeur` dans cet exemple).
— `password` : Mot de passe de l'utilisateur.

Cette requête retourne la liste (treemap) des fichiers présents sur le partage (cela ne veut pas dire que l'utilisateur y a accès !).

5.10.4 Points à Noter

— La VM-NAS doit être reconnectée temporairement à Internet pour installer les dépendances nécessaires.
— Assurez-vous de vérifier toutes les configurations de sécurité avant de reconnecter la machine à Internet en environnement de production.
— Si des problèmes d'accès surviennent, vérifiez les permissions des fichiers et dossiers (`750` pour `/mnt/private/TLP_RED` et `660` pour `/mnt/private/whitelist_tlp_red.txt`).
— Cette solution pour le niveau TLP :RED est difficlement implémentable dans la GUI NextCloud. IL faut donc passer en ligne de commande...

6 Améliorations Possibles et Recommandations de Sécurité

Pour garantir un niveau de sécurité informatique optimal et aligné avec les meilleures pratiques, plusieurs axes d'amélioration peuvent être explorés. Ces recommandations permettent d'atténuer les risques identifiés dans cette démonstration et d'adapter la solution à un environnement de production sécurisé.

6.1 Examen et Réduction des Failles Potentielles

— **Audit du Code pour Détecter les Fuites de Sécurité** : Vérifiez si des informations sensibles, comme des mots de passe, apparaissent en clair dans les scripts ou les configurations. Ces pratiques doivent être strictement évitées en production.

6.2 Amélioration de la Gestion des Mots de Passe

— **Stockage des Mots de Passe dans la Base de Données** : Vérifiez que les mots de passe sont hachés avec des algorithmes sécurisés (comme bcrypt ou Argon2) au lieu d'être stockés en clair. Cela reste acceptable dans notre démonstration pour simplifier le proof of concept (POC).
— **SSO et Authentification Forte** : Implémentez un système de Single Sign-On (SSO) pour l'authentification, avec des mécanismes avancés comme des clés USB d'authentification ou un badge RFID pour renforcer la sécurité.
— **Gestion des Comptes Administrateurs** : Stockez les mots de passe administrateurs dans un coffre-fort numérique sécurisé (comme HashiCorp Vault). Centralisez les comptes administrateurs et attribuez plusieurs comptes avec des rôles bien définis pour éviter les dépendances à un seul compte.

6.3 Gestion des Utilisateurs et Groupes

— **Centralisation des Utilisateurs et Groupes** : Synchronisez les utilisateurs et groupes entre les différentes instances Nextcloud et les services associés. Cette gestion asynchrone peut entraîner des divergences et des failles potentielles.

6.4 Renforcement des Règles de Pare-feu (iptables)

— **Affinement des Règles iptables** : Assurez-vous que les règles iptables sont strictement restrictives en environnement de production. Supprimez les exceptions ICMP (ping) après les phases de test.
— **Segmentation Réseau** : Isolez les VMs entre elles et limitez les communications aux seuls services nécessaires.

6.5 Génération et Exploitation des Logs

— **Génération de Logs Centralisés** : Configurez un système de journalisation centralisé pour capturer les logs des VMs, des applications et des événements réseau. Ces logs sont essentiels pour la détection d'intrusions et le reporting pour un Security Operations Center (SOC).

6.6 Sécurisation du Stockage des Données

— **Utilisation d'un NAS Sécurisé** : Envisagez de déplacer les fichiers sensibles (TLP_AMBER et TLP_RED) vers un NAS sécurisé avec des mécanismes de redondance et de résilience (RAID).
— **Protection des Endpoints Publics** : Sécurisez l'instance Nextcloud publique (TLP_WHITE et TLP_GREEN) pour éviter les exfiltrations accidentelles des fichiers sensibles. Cela inclut des

règles de pare-feu adaptées, des scans de vulnérabilité réguliers, et l'activation de la vérification des signatures de fichiers.

6.7 Gestion des Partages et des Accès

— **Mise en Place des ACLs (Access Control Lists)** : Implémentez des ACLs fines pour les partages. Cela permet d'assurer que les utilisateurs n'accèdent qu'aux ressources explicitement autorisées.
— **Jetons pour les Partages Temporaires** : Renforcez les mécanismes de contrôle d'accès en utilisant des jetons uniques pour les partages temporaires, en complément des ACLs.

6.8 Autres Axes de Sécurisation

— **Protection Contre les Exfiltrations de Données** : Envisagez des solutions DLP (Data Loss Prevention) pour surveiller les activités suspectes sur les endpoints publics.
— **Mécanismes de Supervision** : Implémentez un monitoring en temps réel pour détecter les anomalies (ex : requêtes massives, erreurs d'accès).

Ces recommandations constituent une base solide pour adapter la solution actuelle à un environnement de production sécurisé. L'objectif est de minimiser les risques tout en garantissant un système robuste et évolutif.

7 Accès à l'Environnement de POC

Cette section présente les informations nécessaires pour accéder à l'environnement de Proof of Concept (POC), incluant les connexions SSH aux machines virtuelles et l'accès à l'instance Nextcloud. Les identifiants utilisateurs et mots de passe sont également détaillés. Les 2 VM sont hebergés sur un proxmox qu'on appelle apr la suite "proxmox_bebou_js" (nom défini dans notre config SSH)

7.1 Accès SSH aux Machines Virtuelles

Pour accéder aux machines virtuelles utilisées dans l'environnement de POC, utilisez les commandes suivantes :

— **VM-NAS (Cloud Privé)** :

```
ssh -J proxmox_bebou_js test@10.20.10.2
```

Utilisateur : `test`
Mot de Passe : `test`

— **VM-Nextcloud (Cloud Public)** :

```
ssh -J proxmox_bebou_js test@192.168.100.200 \
-L 127.0.0.1:8080:192.168.100.200:80
```

Utilisateur : `test`
Mot de Passe : `test`

7.2 Accès à l'Instance Nextcloud

L'instance Nextcloud est accessible via un navigateur web à l'URL suivante :
URL : `http://127.0.0.1:8080/nextcloud` ou **URL** : `http://127.0.0.1:8080/`
Pour accéder à l'interface Nextcloud, utilisez les identifiants ci-dessous :

Nom d'utilisateur	Mot de Passe	Rôle / Groupe
admin	ProxmoxGNS3_	Administrateur
journaliste	password_white	TLP_WHITE_GROUP
drh	password_drh	TLP_GREEN_GROUP
manager	password_amber	TLP_AMBER_GROUP
directeur	password_red	TLP_RED_GROUP

Table 1 – Liste des utilisateurs et mots de passe Nextcloud

7.3 Notes Importantes

— Veillez à sécuriser les accès en production en changeant les mots de passe par défaut et en activant des mécanismes d'authentification renforcée.
— Les mots de passe présentés ici sont uniquement valides pour l'environnement de POC et ne doivent pas être utilisés en environnement réel.