Documentation technique
Déploiement et sécurisation d'un serveur Nextcloud

MP POUR A LA VM: aqw
MP POUR NEXTCLOUD :admin
Azerty1234

1. Introduction

Dans un contexte professionnel, le partage de fichiers et la collaboration sont devenus essentiels. Les entreprises doivent disposer de solutions sécurisées permettant :

- le stockage des données
- le partage de documents
- la synchronisation entre plusieurs appareils
- la gestion centralisée des utilisateurs

La solution retenue est **Nextcloud**, une plateforme open-source permettant de créer un cloud privé.

Toutefois, la mise en place d'un service cloud nécessite une **sécurisation complète de l'infrastructure**, afin de protéger :

- les données sensibles
- les comptes utilisateurs
- les accès au serveur
- la disponibilité du service

Cette documentation décrit la mise en place des mesures suivantes :

- authentification via Active Directory
- authentification multifacteur (MFA)

- chiffrement des communications
- protection contre les attaques brute force
- sauvegardes sur NAS
- principe du moindre privilège
- plan de reprise d'activité (PRA)
- inventaire des versions

2. Présentation de la solution Nextcloud

Nextcloud est une plateforme open-source permettant de créer un service de stockage et de collaboration similaire à Google Drive ou OneDrive, mais hébergé sur une infrastructure interne.

Fonctionnalités principales :

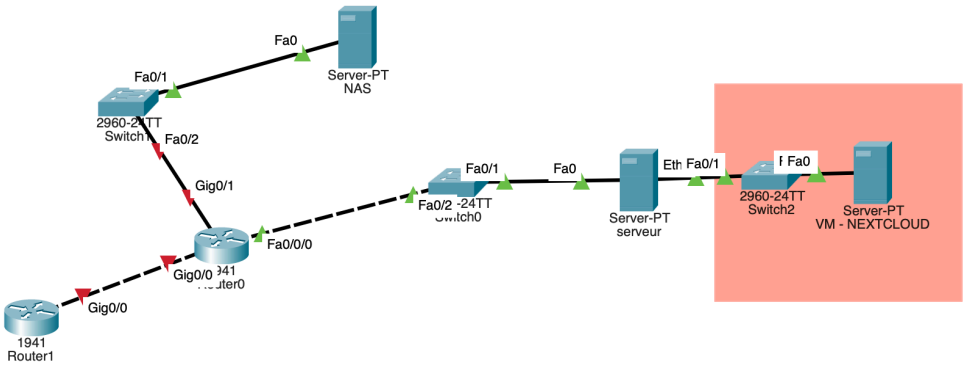
- stockage et synchronisation de fichiers
- partage sécurisé de documents
- gestion des utilisateurs
- calendrier et contacts
- applications collaboratives
- contrôle total des données

Avantages :

- solution open source
- contrôle des données
- extensible via applications
- intégration avec Active Directory
- haut niveau de sécurité

3. Architecture de l'infrastructure

L'infrastructure mise en place repose sur plusieurs composants :



4. Installation du serveur Nextcloud

Le serveur Nextcloud est installé sur une machine Linux.

Packages nécessaires :

- Apache
- PHP
- MariaDB
- Nextcloud

Installation des dépendances :

```
sudo apt update
sudo apt install apache2 mariadb-server php php-mysql php-xml
php-mbstring php-curl php-zip
```

Téléchargement de Nextcloud :

```
wget https://download.nextcloud.com/server/releases/latest.zip
unzip latest.zip
```

Déplacement dans le répertoire web :

```
sudo mv nextcloud /var/www/
```

Configuration des permissions :

```
sudo chown -R www-data:www-data /var/www/nextcloud
```

5. Sécurisation des communications (TLS)

Pour sécuriser les communications entre les utilisateurs et le serveur, le protocole **Transport Layer Security** est utilisé.

Ce protocole permet :

- le chiffrement des données
- l'authentification du serveur
- la protection contre l'interception

Les certificats SSL sont générés via **Certbot** et **Let's Encrypt**.

Installation :

```
sudo apt install certbot python3-certbot-apache
```

Obtention du certificat :

```
sudo certbot --apache
```

Renouvellement automatique :

```
sudo certbot renew
```

6. Authentification via LDAP et Active Directory

Afin de centraliser la gestion des comptes utilisateurs, Nextcloud est connecté à **Active Directory** via le protocole **LDAP**.

Cette configuration permet :

- d’utiliser les comptes AD existants
- d’éviter la création de comptes locaux
- d’appliquer les politiques de sécurité de l’entreprise

7. Configuration côté Active Directory

Création d’un utilisateur de service

Un compte spécifique est créé pour permettre à Nextcloud d’interroger l’annuaire LDAP.

Exemple :

```
Utilisateur : nextcloud-ldap
```

Ce compte doit posséder uniquement les permissions suivantes :

- lecture des utilisateurs
- lecture des groupes

Principe appliqué : **moindre privilège**.

Ports LDAP

Les ports utilisés sont :

Protocole	Port
LDAP	389
LDAPS	636

qPour une meilleure sécurité, l’utilisation de **LDAPS (LDAP sécurisé)** est recommandée.

Base DN

Le Base DN correspond à la racine de l’annuaire.

Exemple :

```
DC=entreprise,DC=local
```

8. Configuration LDAP dans Nextcloud

Dans l'interface administrateur Nextcloud :

Applications
→ LDAP user and group backend
→ Activer

Ensuite :

Paramètres
→ Administration
→ LDAP / AD Integration

Configuration :

Paramètre	Valeur exemple
Serveur LDAP	192.168.1.10
Port	389
Base DN	DC=entreprise,DC=local
Utilisateur DN	CN=nextcloud-ldap,CN=Users,DC=entreprise,DC=local

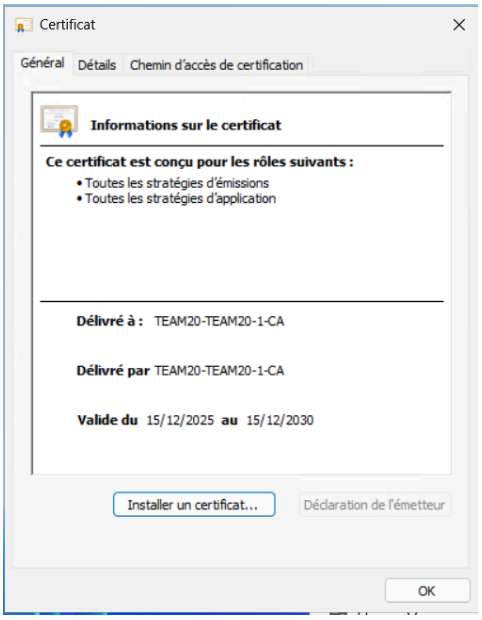
Filtre utilisateur :

```
(&(objectClass=user))
```

Test de connexion :

Test connection

Si la configuration est correcte, les utilisateurs Active Directory apparaissent dans Nextcloud.



9. Authentification multifacteur (MFA)

Pour renforcer la sécurité des comptes utilisateurs, l'authentification multifacteur est activée.

Le MFA nécessite :

1. mot de passe
2. code temporaire généré par une application mobile

Activation dans Nextcloud :

Applications
→ Two-Factor TOTP Provider

Applications compatibles :

- Google Authenticator
- Microsoft Authenticator
- Authy

Processus d'activation :

1. l'utilisateur accède aux paramètres de sécurité
2. il scanne le QR code

3. l’application génère un code temporaire

10. Protection contre les attaques brute force

Nextcloud possède une protection brute force intégrée.

Cette protection :

- détecte les tentatives de connexion répétées
- bloque temporairement l’adresse IP
- ralentit les tentatives d’attaque

Configuration dans l’interface administrateur :

Administration
→ Security
→ Brute Force Protection

11. Sécurisation du serveur avec Fail2ban

En complément, l’outil **Fail2ban** peut être utilisé.

Fail2ban surveille les fichiers logs et bloque les adresses IP malveillantes via le pare-feu.

Installation :

```
sudo apt install fail2ban
```

Configuration :

```
/etc/fail2ban/jail.local
```

Exemple :

```
[nextcloud]
enabled = true
port = http,https
maxretry = 5
bantime = 3600
```

12. Principe du moindre privilège

Le principe du moindre privilège consiste à accorder uniquement les droits nécessaires aux utilisateurs et aux services.

Application dans le projet :

Active Directory

- compte LDAP avec accès lecture uniquement

Nextcloud

- séparation des rôles :
    - administrateurs
    - utilisateurs
    - support

Serveur Linux

Le service Nextcloud fonctionne avec l'utilisateur :

```
www-data
```

Permissions :

```
chmod 750
```

13. Sauvegarde des données sur NAS

Les données doivent être sauvegardées régulièrement afin de prévenir toute perte.

Les sauvegardes sont stockées sur un **NAS (Network Attached Storage)**.

Exemples :

- Synology
- QNAP

Éléments sauvegardés :

- base de données
- fichiers utilisateurs
- configuration Nextcloud

Sauvegarde base de données

```
mysqldump -u root -p nextcloud > backup.sql
```

Sauvegarde fichiers

```
rsync -av /var/www/nextcloud /backup/
```

Planification

Les sauvegardes sont automatisées via **cron** :

crontab -e

Exemple :

```
0 2 * * * /scripts/backup.sh
```

Sauvegarde tous les jours à 2h.

14. Inventaire automatique des versions

Afin de maintenir la sécurité du système, il est important de surveiller les versions des logiciels.

Vérification version Nextcloud :

```
php occ status
```

Version PHP :

```
php -v
```

Version Apache :

```
apache2 -v
```

Ces vérifications permettent d'identifier :

- les mises à jour nécessaires
- les failles de sécurité potentielles

15. Plan de reprise d'activité (PRA)

Le **PRA** permet de restaurer le service en cas d'incident.

Exemples d'incidents :

- panne serveur
- corruption des données
- cyberattaque

Étapes de restauration

1. réinstallation du serveur Linux
2. installation de Nextcloud
3. restauration de la base de données

```
mysql -u root -p nextcloud < backup.sql
```

4. restauration des fichiers

```
rsync -av /backup/nextcloud /var/www/
```

5. redémarrage des services

```
systemctl restart apache2
```

16. Tests de sécurité

Plusieurs tests doivent être réalisés après la mise en place.

Test MFA

Connexion avec :

- mot de passe
- code TOTP

Test LDAP

Connexion avec un compte Active Directory.

Test brute force

Plusieurs tentatives de connexion incorrectes doivent déclencher un blocage.

Test restauration

Simulation d'une panne serveur et restauration via les sauvegardes.

17. Conclusion

La mise en place de Nextcloud au sein de l'infrastructure permet de fournir une solution de stockage et de collaboration sécurisée.

Les mesures mises en place garantissent :

- la protection des comptes utilisateurs
- la sécurisation des communications
- la résilience du système
- la protection des données

L'intégration avec Active Directory facilite la gestion centralisée des identités, tandis que les sauvegardes et le PRA assurent la continuité du service en cas d'incident.

Ces mesures constituent une base solide pour une infrastructure cloud privée sécurisée.

Rapport de test

ID Test	Description	Action réalisée	Résultat attendu	Résultat obtenu	Statut
1	Vérification de l'installation de Nextcloud	Accès via navigateur à l'URL du serveur Nextcloud	Interface d'installation ou de connexion affichée	Interface Nextcloud accessible	OK
2	Vérification des services Apache et MariaDB	`systemctl status apache2` / `systemctl status mariadb`	Services actifs	Services actifs et fonctionnels	OK
3	Vérification de la connexion HTTPS	Accès au site via `https://`	Certificat TLS valide et connexion sécurisée	Connexion HTTPS fonctionnelle	OK
4	Vérification du certificat Let's Encrypt	`certbot certificates`	Certificat valide et non expiré	Certificat actif	OK
5	Vérification de l'intégration LDAP	Test de connexion LDAP dans l'interface admin Nextcloud	Connexion LDAP réussie	Connexion établie avec Active Directory	OK
6	Vérification de l'import des utilisateurs AD	Consultation des utilisateurs dans Nextcloud	Utilisateurs Active Directory visibles	Comptes AD synchronisés	OK
7	Test d'authentification utilisateur AD	Connexion avec un compte Active Directory	Connexion autorisée	Authentification réussie	OK
8	Vérification MFA (TOTP)	Activation MFA et connexion avec code OTP	Demande du code MFA	Authentification double facteur fonctionnelle	OK
9	Test protection brute force	Plusieurs tentatives de connexion incorrectes	Blocage temporaire de l'IP	Blocage détecté	OK

10	Vérification Fail2ban	Analyse des logs Fail2ban après tentatives	IP bannie après plusieurs essais	Adresse IP bloquée	OK
11	Vérification sauvegarde base de données	Exécution `mysqldump`	Fichier backup.sql généré	Sauvegarde créée	OK
12	Vérification sauvegarde fichiers Nextcloud	Exécution `rsync` vers NAS	Copie des fichiers réalisée	Données sauvegardées sur NAS	OK
13	Test automatisation sauvegarde	Vérification tâche cron	Sauvegarde lancée automatiquement	Tâche planifiée fonctionnelle	OK
14	Vérification inventaire des versions	`php occ status`, `php -v`, `apache2 -v`	Versions affichées	Versions correctement détectées	OK
15	Test Plan de Reprise d'Activité	Simulation restauration base + fichiers	Service restauré	Nextcloud opérationnel après restauration	OK