TP08. 22 : Administration et Utilisation de NextCloud

Objectifs pédagogiques :

1. Maîtriser les fonctionnalités d'administration de NextCloud.
2. Configurer les utilisateurs, groupes, quotas, alertes et restrictions.
3. Tester les configurations pour valider leur mise en œuvre.
4. Découvrir d'autres fonctions administratives comme les journaux d'activité, le chiffrement et les applications.

Contexte :

Vous travaillez comme administrateur système pour l'entreprise **CloudCorp**, qui utilise NextCloud pour le partage et la collaboration. Votre mission est de gérer et configurer NextCloud afin de répondre aux besoins de l'organisation tout en assurant la sécurité des données et la conformité aux politiques internes.

Partie 1 : Administration de NextCloud

Exercice 1 : Gestion des utilisateurs et des groupes

1. Connectez-vous à l'interface d'administration de NextCloud avec vos identifiants administrateur GLPI/GLPI.
2. Rendez-vous dans la section **Utilisateurs** du menu d'administration.
3. Créez les groupes Marketing, Développement et Administration.
4. Ajoutez les utilisateurs suivants :
    - **Alice** : Membre du groupe *Marketing*.
    - **Bob** : Membre du groupe *Développement*.
    - **Claire** : Membre des groupes *Marketing* et *Développement*.
5. Attribuez à chaque utilisateur un mot de passe temporaire qu'ils devront modifier lors de leur première connexion.
6. Ajoutez un avatar à chaque utilisateur pour faciliter leur identification.
7. Explorez les options avancées comme la définition d'une date d'expiration pour l'accès d'un utilisateur.
8. Quelle est l'utilité de structurer les utilisateurs en groupes ?
9. Dans quels scénarios professionnels la définition d'une date d'expiration pourrait-elle être particulièrement utile ?

Exercice 2 : Configuration des quotas

1. Accédez aux paramètres de **Stockage & quotas** pour chaque utilisateur.
2. Appliquez les quotas suivants :
    - **Alice** : 2 Go.
    - **Bob** : 1 Go.
    - **Claire** : 3 Go.
3. Activez l'option pour informer les utilisateurs de leur utilisation actuelle de l'espace disque.

4. Configurez un quota par défaut pour tout nouvel utilisateur (ég. : 500 Mo).
5. Testez la création d'un utilisateur supplémentaire pour vérifier l'application du quota par défaut.
6. Que se passe-t-il lorsque l'espace alloué est saturé ?
7. Comment les quotas peuvent-ils aider à prévenir une surcharge du serveur ?

Exercice 3 : Restrictions et règles de sécurité

1. Rendez-vous dans la section **Paramètres** → **Partage** :
    a. Désactivez le partage de fichiers avec des utilisateurs externes pour tous les utilisateurs sauf ceux du groupe *Développement*.
    b. Autorisez uniquement les administrateurs à partager des dossiers avec des permissions d'écriture.
2. Accédez à **Paramètres** → **Flux d'activités** :
    a. Activez une alerte par email lorsque :
        a. Un fichier est supprimé.
        b. Un quota est atteint à 80 %.
3. Interdisez le téléchargement des types de fichiers suivants : *.exe*, *.bat* pour le groupe *Marketing*.
4. Configurez des règles de déconnexion automatique après 15 minutes d'inactivité pour tous les utilisateurs.

Exercice 4 : Sécurité et automatisation :

Expérimentez avec les **Règles d'automatisation** pour implémenter des politiques avancées telles que Le verrouillage de fichiers sensibles en fonction de l'adresse IP, l'heure de connexion ou même le type de périphérique utilisé. Pour ce faire vous devriez installer les plugins (**"File Access Control", "Security", …)**

1. Configurez une règle d'automatisation pour bloquer l'accès aux fichiers d'un utilisateur si :
    - L'accès se fait depuis un pays non autorisé (par exemple, hors de l'Union Européenne).
    - L'utilisateur tente d'accéder à un fichier en dehors des heures de travail (8h-18h).
2. Testez ces configurations avec un utilisateur test et vérifiez leur comportement.
3. Quels cas d'utilisation spécifiques dans une entreprise peuvent justifier de telles restrictions ?
4. Comment les règles d'automatisation influencent-elles la gestion des accès en temps réel ?

Exercice 5 : Audit log

1. Installez et configurez l'application **Audit Log** depuis la section **Applications**.

2. Accédez aux journaux d'activité et analysez :
    - Les fichiers récemment téléchargés ou supprimés.
    - Les connexions échouées des utilisateurs.
    - Les modifications des paramètres système.
3. Créez un rapport hebdomadaire automatisé pour les administrateurs contenants :
    - La liste des 10 activités les plus fréquentes.
    - Les tentatives de connexion suspectes.
4. Quels avantages l'utilisation de l'Audit Log apporte-t-elle en termes de suivi et de conformité ?
5. Comment ces journaux peuvent-ils être exploités pour améliorer la sécurité globale ?

Exercice 6 : Intégration d'applications

1. Accédez à la section **Applications** et installez les modules suivants :
    - **Collabora Online** ou **OnlyOffice** : Pour la collaboration en temps réel sur les documents.
    - **Tasks** : Pour la gestion de projets.
    - **Workflow OCR** : Pour automatiser la reconnaissance de texte dans les documents téléversés.
    - **Two-Factor Authentication** : Pour la double authentification.
2. Configurez une application pour un groupe spécifique uniquement (ex. : Tasks pour *Marketing*).
3. Quels modules considérez-vous comme essentiels pour une entreprise comme CloudCorp ?

Exercice 7 : Importation des utilisateurs depuis Active Directory

1. Accédez à l'interface d'administration de Nextcloud et ouvrez la section **LDAP/AD Integration** dans les paramètres.
2. Configurez une connexion avec un serveur Active Directory (AD) en renseignant les informations suivantes :
    - **Adresse IP ou nom de domaine du serveur AD**.
    - **Port** : Utilisez le port 389 pour une connexion standard ou 636 pour une connexion sécurisée (LDAPS).
    - **Base DN** : Chemin de l'arbre LDAP (exemple : dc=example,dc=com).
    - **Compte administrateur AD** : Fournissez les identifiants d'un utilisateur avec des droits de lecture sur l'AD.
3. Testez la connexion pour vérifier que Nextcloud peut accéder à l'AD.
4. Une fois la connexion établie, configurez les options de synchronisation :

- Synchronisez les utilisateurs des groupes *Marketing* et *Développement* uniquement.
- Attribuez des quotas par défaut pour les utilisateurs importés (exemple : 1 Go).

5. Vérifiez que les utilisateurs importés apparaissent dans la liste des utilisateurs Nextcloud.
6. Utilisez les filtres LDAP pour inclure ou exclure des utilisateurs ou groupes spécifiques (exemple : importer uniquement les utilisateurs ayant un attribut employeeType=active).
7. Quels avantages apporte l'intégration de Nextcloud avec Active Directory pour la gestion des utilisateurs ?

Partie 2 : Tests utilisateurs

Exercice 1 : Vérification des quotas

1. Connectez-vous avec l'utilisateur **Bob**.
2. Essayez de téléverser plusieurs fichiers jusqu'à atteindre et dépasser son quota (1 Go).
3. Supprimez un fichier pour libérer de l'espace et recommencez.

Questions :

- Que se passe-t-il lorsqu'un utilisateur atteint son quota ?
- Comment un utilisateur peut-il gérer son espace disque efficacement ?

Exercice 2 : Validation des restrictions

1. Connectez-vous avec l'utilisateur **Alice**.
2. Essayez :
    - De partager un fichier avec une adresse email externe.
    - De téléverser un fichier exécutable (*example.exe*).
3. Observez et notez les messages ou comportements du système.