

# Besoins en Matière de Sécurité et d'Accès pour le Réseau

## Introduction

Salut à tous ! Dans le cadre de notre projet de ville intelligente, il est super important de parler des besoins en matière de sécurité et d'accès pour notre réseau. Avec notre équipe de cinq (Augustin, Koryan, Matteo, Noah et moi, Florian), on doit s'assurer que toutes les données sont bien protégées et que seules les bonnes personnes peuvent y accéder.

### 1. Authentification

D'abord, tous les utilisateurs doivent se connecter via l'Active Directory (AD), que ce soit en local ou central. Ça veut dire que personne ne peut accéder aux applications sans s'identifier. C'est crucial pour éviter que des personnes non autorisées mettent leur nez dans nos affaires. En plus, on doit sauvegarder toutes les données de l'AD régulièrement et appliquer toutes les mesures de sécurité qu'on a vues en cours.

### 2. Contrôle d'Accès

Ensuite, parlons du contrôle d'accès. C'est vraiment important que les permissions soient gérées par groupes dans l'AD. Par exemple, un utilisateur du Groupe 1 ne doit pas pouvoir accéder aux ressources du Groupe 2. Ça aide à éviter les problèmes et à protéger les données de chaque département. De plus, pour les actions critiques comme les modifications ou les transferts, on doit valider selon le rôle de chacun dans l'AD. C'est une bonne manière de s'assurer que tout le monde reste dans son coin.

### 3. Traçabilité

Pour la traçabilité, on doit garder des journaux de connexion sur le serveur AD pour chaque utilisateur. On peut faire ça avec un script PowerShell ou d'autres méthodes. C'est super utile pour suivre ce qui se passe et repérer rapidement toute activité suspecte. En plus, on doit suivre les modifications dans les bases de données avec des triggers, histoire de savoir qui a fait quoi.

### 4. Gestion des Permissions d'Accès

Enfin, la gestion des permissions d'accès doit être bien faite. On doit s'assurer que tout est géré via l'Active Directory et qu'on valide les accès côté serveur (avec PHP ou Python). Ça veut dire que chaque utilisateur ne doit avoir accès qu'aux données et ressources qui lui sont autorisées. C'est essentiel pour renforcer la sécurité de notre système.

## Conclusion

Pour conclure, les besoins en matière de sécurité et d'accès pour notre projet de ville intelligente sont super importants. En mettant en place des mesures d'authentification solides, un contrôle d'accès strict, une bonne traçabilité et une gestion rigoureuse des permissions, on peut garantir la sécurité de notre réseau et la confidentialité des données.