



DESCRIPTION D'UNE SITUATION PROFESSIONNELLE

PARCOURS	SISR <input checked="" type="checkbox"/>	SLAM <input type="checkbox"/>
Lieu de réalisation	Campus Montsouris	 
Période de réalisation	Du :	Au :
Modalité de réalisation	SEUL <input checked="" type="checkbox"/>	EN EQUIPE <input type="checkbox"/>

Intitulé de la mission	Atelier ACL
Description du contexte de la mission	<p>Dans le cadre de la sécurisation des ressources informatiques de l'entreprise simulée, un atelier a été mené pour apprendre à gérer les droits d'accès (ACL) aux dossiers et fichiers partagés sur un serveur Windows. Il s'agissait de mettre en œuvre des règles d'accès spécifiques à chaque utilisateur en fonction de son rôle dans l'organisation.</p>

Contraintes & Résultat	Ressources fournies / contraintes techniques / Résultats attendu
	<p>Limitier les accès aux seules données dont un utilisateur a besoin</p>
Productions associées	Liste des documents produits et description
	<p>Script Batch de création d'arborescence de dossiers.</p> <p>Comptes utilisateurs créés dans l'Active Directory.</p> <p>Paramétrage des ACL via les propriétés de sécurité des dossiers.</p>

Modalités d'accès aux productions	Identifiants, mots de passe, URL d'un espace de stockage et présentation de l'organisation du stockage

Description détaillée de la situation professionnelle retenue et des productions réalisées

L'objectif principal de cet atelier était de maîtriser les bases de la gestion des ACL sous Windows Server. J'ai commencé par créer les utilisateurs requis dans l'Active Directory, en renseignant uniquement leur fonction dans la description. Un mot de passe standard a été défini pour tous.

Ensuite, j'ai rédigé et exécuté un script batch afin de créer automatiquement l'arborescence des dossiers pour chaque service (comptabilité, secrétariat, direction, etc.). Les sous-dossiers ont également été pris en compte selon le modèle fourni.

J'ai ensuite attribué les droits d'accès aux différents dossiers à l'aide des ACL. Par exemple, les chefs de service avaient des droits de modification, tandis que les employés standards n'avaient que des droits de lecture/exécution. Un tableau a été complété pour valider le bon fonctionnement de ces règles avec différents comptes utilisateurs.

Une évolution de la politique d'accès a été mise en œuvre : le directeur a reçu un contrôle total, tandis que les droits de l'administrateur du serveur ont été restreints aux seuls dossiers communs. Deux nouveaux utilisateurs ont été créés, dont Adrien, à qui le directeur a attribué lui-même des droits spécifiques, démontrant ainsi une délégation possible de gestion des ACL.

Ce travail m'a permis d'appliquer une méthodologie claire : analyse des besoins d'accès, création de la structure, attribution des droits, vérification et adaptation. Il s'inscrit pleinement dans les compétences liées à la gestion des ressources et de la sécurité du SISR.