PROJET IT
DOCUMENTATION

Gestion des Utilisateurs et Groupes
(RBAC & Permissions)

MORGAN, HUBERT BURERA

JUILLET 2025

Ubuntu, Terminal

Table des matières

Ce document fait partie d’un cadre personnel de développement de mon portfolio afin de documenter mon apprentissage autodidacte, servant à supplémenter mes futures certifications. Toutes les simulations ont été effectuées dans des environnements de lab controllés.

I. Aperçu du Projet

Ce projet a consisté à mettre en place une infrastructure de gestion des utilisateurs et des groupes sous Linux afin de simuler une organisation composée de plusieurs départements (HR, Finance, IT, Stagiaires).

L'objectif principal était :

- Créer et gérer des utilisateurs et des groupes.
- Implémenter des permissions fines (lecture/écriture).
- Simuler des scénarios courants en entreprise (Nouvel employé, départ d'un employé, mot de passe oublié, etc.).

II. Mise en Place de l'Environnement

Matériel	Détails
OS	VM Linux, ubuntu 22.04.2
Type de réseau	Wi-fi (ens33, domicile)
Outils de utilisés	Terminal Linux (adduser, usermod, chmod, chown, ACL).
Structure des répertoires :	/srv/ ├── HR/ ├── Finance/ └── IT/ └── Stagiaires/

III. Procédure et Étapes Clés

- Création et suppression d'utilisateurs avec **adduser**, **userdel**.
- Gestion des groupes et des permissions avec **usermod -aG**, **chmod**, **chown**.
- Mise en place d'ACL pour les droits lecture/écriture.
- Scénarios testés (ajout d'utilisateur, changement de mot de passe, verrouillage).

IV. Scénarios Simulés

- *Nouvel employé* : ajout d'un stagiaire dans **stagiaires**, lecture seule sur **/IT** et écriture sur **/IT/Stagiaires**. Pour laisser les stagiaires consulter les documentations mais pas les modifier. Cependant ils ont un accès total à leur répertoire **/Stagiaires/**
- *Départ :* suppression d'un employé et suppression automatique de son home directory.
- *Sécurité :* utilisateur malveillant bloqué via **passwd -l** et suppression des droits sur ses fichiers.

V. Résultats et Vérifications

- **ls -l /srv** et **getfacl** ont permis de valider la bonne configuration des droits.
- Test utilisateur avec **sudo -u <user>** pour vérifier lecture/écriture.

VI. Compétences Acquises / Démontrées

- Maîtrise des commandes Linux pour la gestion des utilisateurs et groupes.
- Mise en place d’une structure de permissions basée sur les rôles (RBAC).
- Utilisation des ACL pour une gestion fine des droits.

VII. Améliorations Personnelles

- Meilleure compréhension du **SGID (Le ‘2' dans “2770", aussi appelé ’Sticky Bit’)** et de l’héritage des permissions.

- Pratique des scénarios réels d’entreprise, transférables vers Active Directory.

- Sur une arborescence réelle d’entreprise, l’utilisation de scripts (création, suppression d’utilisateurs…) seraient adoptés pour une fluidité de travail supérieure.

- La gestion d’unités organisationnelles devrait être constamment vérifiée afin de protéger les fichiers qui devraient l’être, voir les séparer de l’environnement professionnel. En somme fluidifier tout sur lequel on travail.