

Projet : Mise en place d'une authentification centralisée Active Directory pour systèmes Linux

Contexte

Le projet a été conçu et réalisé de manière autonome dans un environnement de laboratoire personnel, dans une démarche de montée en compétences et de mieux comprendre le rôle d'un Active Directory au sein d'un réseau d'entreprise. Bien que les environnements utilisateurs soient majoritairement Windows, l'intégration de Linux à Active Directory répond à des besoins réels en entreprise, notamment pour la gestion centralisée des accès aux serveurs.

Objectif du projet

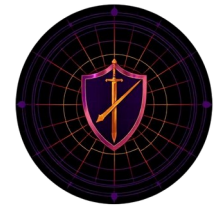
Mettre en place une authentification centralisée Active Directory pour des systèmes Linux, en reproduisant un cas réel d'infrastructure d'entreprise : gestion des comptes, accès SSH et droits administrateur, sans solutions tierces propriétaires.

L'objectif principal était de comprendre et maîtriser les mécanismes sous-jacents (DNS, Kerberos, SSSD, PAM), et pas uniquement d'obtenir un fonctionnement "clé en main".

Architecture mise en place

- Windows Server 2022
 - Active Directory Domain Services
 - DNS
 - Kerberos (KDC)
- Debian GNU/Linux
 - realmd
 - SSSD
 - PAM / NSS
- pfSense pour le routage
- Domaine : homelab.local

Windows Server agit comme autorité d'authentification, Linux délègue l'authentification et le contrôle d'accès à AD.



Principe de fonctionnement

- Authentification Linux via Kerberos
- Résolution des identités et groupes via SSSD
- Contrôle d'accès assuré par PAM
- Accès explicitement filtré par groupes Active Directory
 - linux-users : accès SSH
 - linux-admins : accès SSH + sudo
- Aucun accès implicite via Domain Users

Problèmes rencontrés (principaux)

- DNS : résolution FQDN incomplète, enregistrements AD manquants
→ correction des enregistrements A / PTR / SRV côté AD
- Kerberos : erreurs lors de kinit malgré des identifiants valides
→ incohérences DNS / realm, comptes AD désactivés, configuration krb5.conf
- SSSD / PAM : authentification réussie mais accès SSH refusé
→ filtrage par groupes AD mal appliqué, cache SSSD non purgé
- Home directories : répertoires utilisateurs absents
→ activation de la création automatique via PAM

Ces incidents ont permis de différencier clairement authentification, autorisation et résolution de noms.

Résultat final

- Intégration complète et fonctionnelle entre Active Directory et Linux
- Accès SSH contrôlé par groupes AD
- Gestion des droits sudo via Active Directory
- Création automatique des répertoires utilisateurs
- Infrastructure stable et reproductible

La solution a été validée par des tests fonctionnels incluant des comptes autorisés et non autorisés, ainsi que des vérifications des accès SSH et des droits sudo.



Compétences mises en avant

- Administration Active Directory
- DNS (A, PTR, SRV)
- Kerberos
- Intégration Linux / AD (SSSD, PAM)
- Gestion des accès et des privilèges
- Diagnostic et résolution d'incidents systèmes

Topologie Réseau

