

Documentation Technique : Déploiement AD DS Sécurisé

Projet : Mise en place d'un contrôleur de domaine durci (Hardening)

Outil utilisé : Script PowerShell "Hello My DIR!" (v1.1.0)

Référence : [Bonnes pratiques de sécurité AD - IT-Connect](#)

1. Introduction

L'objectif de cette mission est d'installer un rôle **AD DS (Active Directory Domain Services)** sur Windows Server en suivant les recommandations de sécurité de l'ANSSI. L'utilisation du script "Hello My DIR!" permet d'automatiser la configuration et de corriger les vulnérabilités natives dès l'installation.

2. Étape 1 : Configuration de la Forêt et du Domaine

Le premier lancement du script permet de définir les paramètres logiques de l'infrastructure :

- **Création de forêt** : Installation d'un nouveau domaine dans une nouvelle forêt.
- **Niveau fonctionnel** : Sélection de **Windows Server 2016** pour la forêt et le domaine.
- **Options activées** : Activation de la **Corbeille Active Directory** (Recycle Bin).
- **Emplacements système** : Configuration personnalisée des dossiers SYSVOL et NTDS.
- **Comptes de délégation** : Création du compte de service DLGUSER01 et du groupe de délégation associé.

3. Étape 2 : Installation des Rôles (Binaires)

Le second lancement installe les composants Windows nécessaires :

- **Rôles installés** : AD-Domain-Services, RSAT (outils AD et DNS), RSAT-DFS-Mgmt-Con et GPMC (Gestion des GPO).
- **Sécurité DSRM** : Génération aléatoire du mot de passe de restauration des services d'annuaire.
- **Finalisation** : Redémarrage automatique du serveur pour appliquer les modifications.

4. Étape 3 : Post-Installation et Hardening (Durcissement)

Après redémarrage, le script est exécuté une troisième fois pour sécuriser l'annuaire en corrigeant les alertes de sécurité (basées sur PingCastle et PurpleKnight) :

- **Corrections réseau** : Configuration des sous-réseaux manquants (SubnetMissing IPv4/IPv6).
- **Gestion des comptes** : Protection des utilisateurs sensibles via le groupe **Protected Users** et exigence du protocole **LDAPS**.
- **Hygiène de l'AD** : Activation de la protection des Unités d'Organisation (OU) contre la suppression accidentelle.
- **Stratégies de Groupe** : Déploiement automatique de GPO durcies :
 - *Default Domain Security*
 - *Default Domain Controllers Security*

5. Conclusion

Le domaine est désormais opérationnel et sécurisé avec un score de risque optimisé. L'étape suivante consiste à intégrer les périphériques et serveurs membres au domaine.