Checklist

Advens
Security for the greater good

Reconstruire son Active Directory : la checklist en 5 étapes

Certaines entreprises mettent en place des processus bien définis pour **reconstruire leur Active Directory** en toute autonomie. Mais il arrive que des étapes clés soient négligées – voire oubliées. Voici donc une checklist qui résume les étapes à suivre pour reconstruire votre Active Directory !

ÉTAPE 1

Créez une zone de confiance et analysez

- ☑ **Isolez le réseau** en empêchant tout accès de et vers l'extérieur
- ☑ Isolez l'Active Directory dans un **VLAN** (segmentation) ou derrière un pare-feu (cloisonnement)
- ☑ Analysez le **comportement** et les traces laissées par l'attaquant

Le saviez-vous ?

Advens dispose d'une équipe d'investigation Forensic dédiée.

Son rôle est :

- d'étudier les preuves laissées par le cyber attaquant (mouvements latéraux, rebonds…) ;
- d'identifier une ou plusieurs portes d'entrée, ainsi que les vulnérabilités exploitées ;
- de rédiger un rapport avec des informations sur la nature de l'attaque.

ÉTAPE 2

Installez un nouveau DC et migrez les objets de l'annuaire

- ☑ Installez un nouveau contrôleur de domaine (DC) en repartant d'une **installation saine**, depuis un système d'exploitation plus récent
- ☑ **Synchronisez** ce nouveau DC avec l'ancien afin de récupérer l'ensemble des objets de l'annuaire, puis rompez la liaison
- ☑ Effectuez une **remédiation des vulnérabilités** identifiées à l'aide d'outils spécialisés, jusqu'à obtenir un niveau de sécurité optimal

ÉTAPE 3

Ajoutez les services un à un sur le nouvel annuaire

- Ajoutez les services qui se connectent sur l'annuaire, tout en vérifiant que le niveau de sécurité ne baisse pas
- En parallèle, menez des audits via des outils comme **PurpleKnight** ou **PingCastle** afin de :
  - maintenir un niveau de sécurité optimal à chaque fois que vous ajoutez un nouveau service ;
  - garder une trace écrite de l'opération via un **compte-rendu ad hoc**.

Le Tiering Model : ça vous parle ?

Ce modèle, appliqué chez Advens, est recommandé par l'ANSSI et Microsoft.

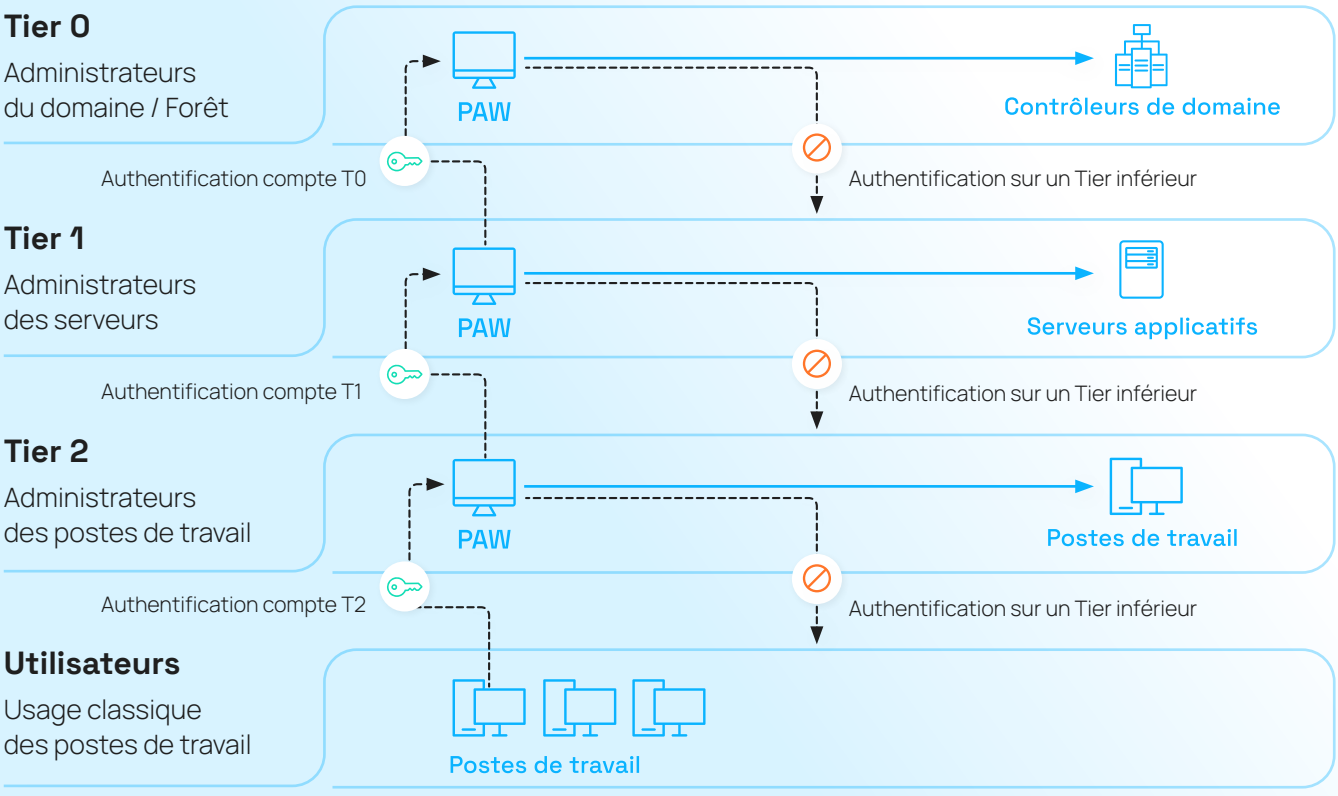
→ **L'objectif ?**

Les objets de l'AD sont répartis en fonction de leur niveau d'importance (et de leurs privilèges), et **ces différentes couches restent hermétiques**. De cette façon, si un compte utilisateur est compromis durant une attaque, l'attaquant ne pourra pas effectuer de mouvement latéral lui permettant de faire des dégâts à grande échelle. L'impact sur l'entreprise sera donc minime.

→ **Comment ça marche ?**

Le principe est de classer les serveurs et les niveaux des postes selon leur utilisation et leur adhérence avec l'Active Directory :

- Premier niveau (T0) : serveurs les plus critiques
- Deuxième niveau (T1) : services et applications destinés aux utilisateurs et aux prestataires
- Troisième niveau (T2) : postes les moins sensibles (ceux des utilisateurs en général)



ÉTAPE 4

Remédiez et appliquez les mesures correctives

- **Si le niveau de sécurité baisse**, appliquez la remédiation nécessaire et menez des actions correctives
- Voici **3 exemples** de situations qui peuvent engendrer une baisse de sécurité :
  - trop de privilèges accordés sur un compte de service (messagerie, par exemple) ;
  - des chemins dangereux tracés entre l'AD et certains services ;
  - un système d'exploitation obsolète ou non à jour.

Quelques bonnes pratiques

- Segmentez votre réseau
- Vérifiez le niveau d'autorisation des utilisateurs et corrigez-le au besoin
- Assurez-vous que chaque administrateur d'un système est administrateur de ce système seulement : un administrateur de messagerie ne doit pas être administrateur du domaine
- Ne restez pas concentré uniquement sur l'Active Directory : revoyez en permanence la sécurité de votre architecture globale (commutateurs, pare-feux…)

ÉTAPE 5

Auditez (encore) votre environnement et ouvrez les flux un à un

Une fois que vous aurez mené à bien la remédiation de votre Active Directory, ainsi qu'une refonte de l'architecture et des différents services, passez à l'audit !

- Auditez la sécurité de **l'ensemble de votre réseau,** pour vous assurer que l'architecture est aux normes et peut s'ouvrir sans aucun risque de sécurité pour l'organisme
- Identifiez les **services prioritaires** à ouvrir vers l'extérieur (par exemple activer le service de messagerie pour que les employés puissent envoyer des mails)
- Rédigez un **rapport technique** pour archiver les mesures correctives appliquées

> « Il ne faut pas attendre de se faire attaquer pour envisager de repenser la structure de son Active Directory et revoir la manière dont elle est sécurisée. Cela fait 25 ans que ce service d'annuaire existe, il y a des améliorations qui sortent en continu mais les risques persistent et les entreprises ne doivent pas les sous-estimer pour rester constamment protégées. Pour cela, le suivi en continu de votre SI au travers d'audits réguliers et de remédiations reste la meilleure procédure. »

Régis Auquier –
Manager au sein du pôle
Architecture et Intégration d'Advens

Acquérir de solides capacités de reconstruction rapide d'un AD n'est donc plus une option – même si elle peut exiger des compétences pointues en la matière.
Vous souhaitez auditer votre Active Directory ?

Advens vous accompagne

Advens
Security for the greater good