AD Secondaire fonctionnement

À quoi sert un AD secondaire en RODC :

- **Alléger la charge du serveur primaire :** Le serveur secondaire va permettre d'alléger la charge du serveur primaire dans différents besoins. Par exemple pour un site distant, économiser la bande passante et améliorer les performances. Il utilise un mécanisme de mise en charge pour stocker une copie partielle des données Active Directory. Cela inclut notamment les informations d'identification des utilisateurs (sous forme de cache de mot de passe restreint) et d'autres données couramment consultées. Si les données ne sont pas disponibles localement, le RODC transmet la demande au contrôleur de domaine principal pour traitement.

- **Redondance du serveur primaire :** Le déploiement de plusieurs contrôleurs de domaine dans un domaine Active Directory permet d'assurer la redondance. Si un contrôleur de domaine tombe en panne, les autres contrôleurs de domaine peuvent continuer à fournir des services d'annuaire aux clients. Comment fonctionne un AD secondaire en RODC :

Comment fonctionne un AD secondaire en RODC :

- **Réplication des données :** Le RODC stocke une copie partielle de la base de données Active Directory. Le RODC n'a pas de réplication bidirectionnelle complète avec les autres contrôleurs de domaine. Il ne reçoit que des données en lecture seule, ce qui signifie qu'il n'est pas autorisé à écrire des données sur le réseau Active Directory.

- **Couche applicative :** Le serveur secondaire RODC, utilise les mêmes applications que le serveur primaire, c'est-à-dire le Service de domaine Active Directory ainsi que d'autres services liés à la gestion des utilisateurs, des groupes, des politiques de sécurité, etc.

- **Sécurité :** Le RODC n'authentifie pas directement les utilisateurs. Au lieu de cela, il transmet les demandes d'authentification aux contrôleurs de domaine en lecture-écriture. Cache de mot de passe restreint : Le RODC stocke un cache restreint des informations d'identification des utilisateurs, limitant ainsi l'exposition potentielle des mots de passe en cas de compromission du serveur.
  Contrôle d'accès : Il limite l'accès aux données de manière que seuls certains administrateurs autorisés puissent accéder au serveur et à ses données.

Fonctionnement de la redondance :

Niveau Serveur :

- **Réplication active directory :** Utilisation du protocole LDAP pour la réplication de données entre les contrôleurs de domaine

- **DNS :** Utilisation du service DNS pour résoudre le nom des contrôleurs et d'autres services Active Directory en adresse IP. La redondance DNS peut être assurée en configurant plusieurs serveurs DNS et en utilisant des zones de recherche directe et inverse pour la résolution des noms.

- **Sécurité :** Active Directory utilise le protocole Kerberos pour l'authentification des utilisateurs et des services. La redondance est assurée en ayant plusieurs contrôleurs de domaine qui peuvent authentifier les utilisateurs et délivrer des tickets Kerberos en cas de panne d'un serveur.

Niveau Client :

- **Configuration DNS :** Les clients doivent être configurés pour utiliser plusieurs serveurs DNS pour la résolution des noms, afin de garantir la redondance en cas de panne d'un serveur DNS.
- **Stratégies de site :** Active Directory utilise des stratégies de site pour déterminer quel contrôleur de domaine un client doit contacter en fonction de son emplacement physique. En configurant correctement les sites Active Directory, les clients peuvent être dirigés vers un contrôleur de domaine fonctionnel dans leur site local en cas de panne d'un serveur distant.

Active Directory utilise des stratégies de site pour détÀ l'exception des mots de passe de compte, un RODC contient tous les objets et attributs Active Directory qu'un contrôleur de domaine accessible en écriture contient. En revanche, aucune modification ne peut être apportée à la base de données stockée sur le contrôleur de domaine en lecture seule.

Mot de passe en cache