Révision Active Directory

1. Différence et signification entre Active Directory et LDAP

Les annuaires LDAP (**Lightweight Directory Access Protocol**) et AD (**Active Directory**) sont deux technologies distinctes qui servent à stocker et à gérer des informations d'identification et de sécurité pour les utilisateurs et les ordinateurs dans un réseau.

LDAP

LDAP est un protocole ouvert et multiplateforme qui permet de stocker et de récupérer des informations dans un annuaire.

LDAP est un protocole de communication qui permet aux applications de communiquer avec d'autres serveurs de services d'annuaire.

Il est utilisé pour l'authentification, la gestion des groupes et des utilisateurs, ainsi que pour la gestion des stratégies.

Active Directory

Active Directory est une technologie propriétaire développée par Microsoft pour stocker et gérer des informations d'identification et de sécurité pour les utilisateurs et les ordinateurs dans un réseau.

Il est conçu pour être intégré à d'autres produits Microsoft pour fournir un emplacement centralisé pour la gestion de tous les aspects de l'infrastructure technologique d'une organisation.

Active Directory est une implémentation des services d'annuaire qui fournit toutes sortes de fonctionnalités, telles que l'authentification, la gestion des groupes et des utilisateurs, l'administration des stratégies et plus encore.

2. Structure de l'Active Directory

Domaine dans Active Directory

Un domaine dans Active Directory est une unité logique qui regroupe un ensemble d'objets tels que des utilisateurs, des ordinateurs, des imprimantes et d'autres ressources réseau qui partagent la même base de données de comptes et la même politique de sécurité. Chaque domaine possède ses propres contrôleurs de domaine et sa propre base de données Active Directory, appelée base de données NTDS (NT Directory Services). Les domaines sont utilisés pour gérer et organiser les ressources réseau de manière centralisée et pour appliquer des politiques de sécurité spécifiques.

Forêt

Une forêt est l'entité la plus large dans une infrastructure Active Directory. Elle peut contenir plusieurs domaines et représente la frontière de sécurité ultime dans Active Directory. Tous les domaines dans une forêt partagent le même schéma et le même catalogue global. Le schéma définit la structure et les classes d'objets que l'on peut créer dans Active Directory. Le catalogue global contient une copie partielle des informations de chaque domaine de la forêt, ce qui permet aux utilisateurs de rechercher des informations sur les objets dans tous les domaines de la forêt.

Différence entre une Unité d'Organisation (OU) et un Conteneur

Unité d'Organisation (OU)

- Une Unité d'Organisation (OU) est une subdivision au sein d'un domaine Active Directory. Elle permet d'organiser et de regrouper des objets (utilisateurs, groupes, ordinateurs) de manière hiérarchique pour simplifier la gestion administrative.

- Les OU peuvent être imbriquées, ce qui permet de créer une structure d'organisation complexe et refléter l'organisation réelle de l'entreprise.

- Les OU permettent l'application de stratégies de groupe (GPO) spécifiques et la délégation de l'administration.

Conteneur

- Un conteneur est également une unité de regroupement dans Active Directory, mais il s'agit d'un objet plus statique comparé à une OU.

- Les conteneurs par défaut sont créés lors de l'installation d'Active Directory et ne permettent pas de lier des stratégies de groupe ni de déléguer des contrôles administratifs de manière aussi granulaire que les OU.

En résumé, la principale différence entre une OU et un conteneur est que les OU sont plus flexibles et permettent une gestion plus fine des permissions et des stratégies, alors que les conteneurs sont des structures plus simples et statiques.

3. Réplication et sauvegarde

Fonctionnement de la Réplication

La réplication dans Active Directory (AD) permet de synchroniser les bases de données des différents contrôleurs de domaine (DC).

1. Topologie de Réplication : Active Directory utilise le « Knowledge Consistency Checker » (KCC) pour créer une topologie de réplication basée sur un anneau. Cela

garantit que chaque contrôleur de domaine peut communiquer efficacement avec ses voisins.

2. Réplication Multimaître : Tous les DC peuvent recevoir des modifications et répliquent ces modifications aux autres DC. Cela permet une flexibilité et une redondance élevées.

3. Changement de Notification : Lorsqu'un changement est effectué sur un DC, une notification de changement est envoyée à ses partenaires de réplication. Ces partenaires sollicitent ensuite les modifications pour les appliquer localement.

4. Conflits de Réplication : Si des modifications concurrentes sont effectuées sur différents DC, AD utilise des identifiants uniques et des numéros de séquence d'update (USN) pour résoudre les conflits en privilégiant la modification la plus récente.

5. Sites et Liens de Sites : Les entreprises peuvent configurer des sites AD pour optimiser la réplication en fonction de la topologie physique du réseau. Les liens de sites définissent la connectivité et les coûts associés à la réplication entre sites.

Sauvegarder et Restaurer Active Directory

Sauvegarde

1. Utilisation des Outils de Sauvegarde Natifs : Utilisez les outils de sauvegarde intégrés comme Windows Server Backup pour sauvegarder l'état du système, qui inclut Active Directory.

2. Planification Régulière des Sauvegardes : Effectuez des sauvegardes régulières (quotidiennes, hebdomadaires) pour minimiser la perte de données en cas de défaillance.

3.*Test des Sauvegardes : Périodiquement, testez les sauvegardes pour vous assurer qu'elles sont complètes et peuvent être restaurées sans problème.

4. Sécurisation des Sauvegardes : Stockez les sauvegardes dans un emplacement sécurisé, idéalement hors site, pour protéger contre les catastrophes locales.

5. Documenter et Mettre à Jour les Stratégies de Sauvegarde : Maintenez une documentation à jour des processus et des procédures de sauvegarde.

Restauration

1. Restauration Autoritative et Non-Autoritative : La restauration non-autoritative remet le DC dans un état cohérent et laisse la réplication AD mettre à jour les modifications. La restauration autoritative force les modifications restaurées à répliquer sur tous les autres DC.

2. Utilisation du Mode de Récupération des Services Directory (DSRM) : Pour restaurer AD, démarrez le DC en mode DSRM. Cela permet d'effectuer des opérations de restauration sans risque d'interférence avec la réplication.

3. Suivi et Validation : Après la restauration, surveillez le DC restauré et validez que la réplication fonctionne correctement et que les données restaurées sont correctes.

4. Documentation des Processus de Restauration : Ayez une documentation claire et testée des procédures de restauration pour garantir une réponse rapide et efficace en cas de défaillance.

4. Group Policy Object (GPO)

Objet de Stratégie de Groupe (GPO)

Un Objet de Stratégie de Groupe (GPO) est un ensemble de paramètres configurés dans l'Active Directory pour gérer les environnements des utilisateurs et des ordinateurs. Les GPO permettent aux administrateurs de contrôler et d'automatiser diverses configurations et règles, telles que les paramètres de sécurité, les installations de logiciels, les scripts de démarrage et de fermeture de session, et bien plus encore.

Application des GPO aux Utilisateurs et aux Ordinateurs

1. Liens de GPO : Les GPO sont liés à des conteneurs spécifiques dans Active Directory tels que des sites, des domaines ou des unités d'organisation (OU). Un GPO peut être lié à plusieurs conteneurs.

2. Héritage et Priorité

- Ordre d'application : Les GPO sont appliqués dans un ordre spécifique : Local, Site, Domaine, puis OU (LSDOU).

- Héritage : Les GPO peuvent être hérités des conteneurs parents, mais cet héritage peut être bloqué ou forcé par des paramètres spécifiques.

3. Filtrage de Sécurité : Vous pouvez spécifier quels utilisateurs ou groupes d'utilisateurs sont affectés par un GPO en utilisant le filtrage de sécurité. Cela permet une application plus fine des stratégies.

4. Filtrage WM* : Les filtres Windows Management Instrumentation (WMI) peuvent être utilisés pour appliquer des GPO en fonction de critères spécifiques (par exemple, appliquer un GPO uniquement aux ordinateurs avec une certaine version de Windows).

5. Loopback Processing : Cette fonctionnalité permet aux GPO des ordinateurs de prendre le dessus sur ceux des utilisateurs, utile dans des environnements où les

utilisateurs se déplacent entre différents ordinateurs avec des configurations spécifiques.

Étapes pour Créer et Lier un GPO

1. Créer un Nouveau GPO :

- Ouvrez la console de gestion des stratégies de groupe (Group Policy Management Console, GPMC).

- Cliquez avec le bouton droit sur le conteneur (site, domaine ou OU) où vous souhaitez créer le GPO.

- Sélectionnez "Create a GPO in this domain, and Link it here...".

- Donnez un nom descriptif au GPO et cliquez sur "OK".

2. Configurer le GPO :

- Dans la GPMC, localisez le GPO que vous venez de créer.

- Cliquez avec le bouton droit sur le GPO et sélectionnez "Edit".

- La console de gestion des stratégies de groupe (Group Policy Management Editor) s'ouvre.

- Configurez les paramètres souhaités sous les sections "Computer Configuration" et "User Configuration" en fonction des besoins.

3. Lier un GPO Existante à un Conteneur :

- Dans la GPMC, naviguez jusqu'au conteneur où vous souhaitez lier le GPO (site, domaine ou OU).

- Cliquez avec le bouton droit sur le conteneur et sélectionnez "Link an Existing GPO".

- Choisissez le GPO à partir de la liste et cliquez sur "OK".

4. Configurer les Permissions de Sécurité et les Filtres :

- Sélectionnez le GPO dans la GPMC.

- Accédez à l'onglet "Scope" pour configurer le filtrage de sécurité et les filtres WMI si nécessaire.

5. Forcer l'Application des GPO** (si nécessaire) :

- Ouvrez une invite de commande sur un ordinateur cible et exécutez `gpupdate /force` pour forcer l'application immédiate des GPO.

Partit 2

1. Qu'est-ce que l'Active Directory ?

L'Active Directory (AD) est un service de gestion des identités et des accès développés par Microsoft. Il permet de stocker des informations sur les objets d'un réseau (comme les utilisateurs, les groupes et les ordinateurs) et de gérer ces objets de manière centralisée. AD facilite l'administration de la sécurité et l'organisation des ressources dans un environnement Windows Server.

2. Quels sont les principaux composants de l'Active Directory ?

Les principaux composants de l'Active Directory sont :

- Domaine : Un regroupement logique d'objets AD.

- Forêt : Un ensemble de domaines AD qui partagent la même structure logique et le même schéma.

- Unité d'organisation (OU) : Un conteneur permettant de regrouper des objets pour faciliter la gestion.

- Contrôleur de domaine (DC) : Un serveur qui héberge une copie de la base de données AD et fournit des services d'authentification.

- DNS : Le système de noms de domaine utilisé pour localiser les services AD.

3. Qu'est-ce qu'un domaine dans le contexte de l'Active Directory ?

Un domaine dans Active Directory est une unité logique qui regroupe un ensemble d'objets comme les utilisateurs, les groupes et les ordinateurs. Il partage une base de données commune et une politique de sécurité. Les domaines peuvent être organisés en forêts.

4. Comment créez-vous un nouvel utilisateur dans l'Active Directory ?

1. Ouvrez "Active Directory Users and Computers" (ADUC).

2. Naviguez jusqu'à l'OU ou le conteneur où vous voulez créer l'utilisateur.

3. Faites un clic droit, sélectionnez "Nouveaux", puis "Utilisateurs".

4. Remplissez les informations requises (nom, login, mot de passe).

5. Suivez les étapes de l'assistant pour compléter la création.

5. Comment configurez-vous les permissions pour un utilisateur ou un groupe dans l'Active Directory ?

1. Ouvrez ADUC.

2. Naviguez jusqu'à l'objet (par exemple, un fichier ou un dossier) auquel vous voulez appliquer les permissions.

3. Faites un clic droit sur l'objet, sélectionnez "Propriété".

4. Allez à l'onglet "Sécurité".

5. Ajoutez l'utilisateur ou le groupe et configurez les permissions appropriées.

6. Qu'est-ce qu'une unité d'organisation dans l'Active Directory ?

Une unité d'organisation (OU) est un conteneur logique dans un domaine AD qui permet de regrouper des objets pour une gestion administrative plus facile. Les OU peuvent contenir des utilisateurs, des groupes, des ordinateurs, et d'autres OU.

7. Comment créez-vous une unité d'organisation dans l'Active Directory ?

1. Ouvrez ADUC.

2. Faites un clic droit sur le domaine ou l'OU parent où vous voulez créer la nouvelle OU.

3. Sélectionnez "Nouveau" puis " Unité d'Organisation ".

4. Entrez un nom pour l'OU et cliquez sur "OK".

8. Qu'est-ce qu'un groupe dans l'Active Directory et quels types de groupes existent ?

Un groupe dans AD est un ensemble d'utilisateurs, d'ordinateurs ou d'autres groupes. Les groupes simplifient la gestion des permissions et des ressources. Il existe deux types principaux de groupes :

- Groupes de sécurité : Utilisés pour attribuer des permissions aux ressources.

- Groupes de distribution : Utilisés pour créer des listes de distribution de courrier électronique.

9. Comment ajoutez-vous un ordinateur à un domaine Active Directory ?

1. Allez dans les paramètres système (Panneau de configuration > Système et sécurité > Système).

2. Cliquez sur "Modifier les paramètres".

3. Sous l'onglet "Nom de l'ordinateur", cliquez sur "Modifier".

4. Sélectionnez "Domaine", entrez le nom du domaine, et cliquez sur "OK".

5. Entrez les informations d'un compte utilisateur ayant les droits d'ajouter des ordinateurs au domaine.

6. Redémarrez l'ordinateur pour appliquer les changements.

10. Qu'est-ce qu'un contrôleur de domaine ?

Un contrôleur de domaine (DC) est un serveur qui héberge les services Active Directory et la base de données. Il authentifie les utilisateurs et les ordinateurs sur le réseau et applique les politiques de sécurité.

11. Qu'est-ce que le DNS et comment est-il utilisé avec l'Active Directory ?

Le DNS (Domain Name System) est un système qui traduit les noms de domaine en adresses IP. Dans AD, le DNS est crucial car il permet de localiser les services AD comme les contrôleurs de domaine et les autres ressources réseau.

12. Qu'est-ce que le protocole LDAP et comment est-il utilisé dans l'Active Directory ?

Le LDAP (Lightweight Directory Access Protocol) est un protocole utilisé pour accéder et gérer les services d'annuaire comme Active Directory. LDAP permet aux applications de communiquer avec AD pour effectuer des recherches et des modifications d'objets.

13. Comment sauvegardez-vous l'Active Directory ?

1. Utilisez un outil de sauvegarde comme Windows Server Backup.

2. Sauvegardez l'état du système (Etat du Systeme), qui inclut la base de données AD.

3. Planifiez des sauvegardes régulières pour assurer une protection continue.

14. Comment restaurez-vous l'Active Directory à partir d'une sauvegarde ?

1. Démarrez le contrôleur de domaine en mode de restauration des services directory (DSRM).

2. Utilisez Windows Server Backup pour restaurer l'état du système à partir de la sauvegarde.

3. Redémarrez le serveur en mode normal.

4. Vérifiez la cohérence des données et la réplication.

15. Qu'est-ce que le service de réplication de fichiers (FRS) ou le service de réplication DFS (Distributed File System) dans l'Active Directory ?

Le FRS (File Replication Service) et le DFS (Distributed File System) sont utilisés pour répliquer les données entre les contrôleurs de domaine. DFS est la technologie plus

récente et plus robuste, permettant de répliquer des dossiers partagés et d'assurer la redondance.

16. Qu'est-ce que le catalogue global dans l'Active Directory ?

Le catalogue global est un annuaire contenant une copie partielle de tous les objets dans la forêt AD. Il permet des recherches rapides et complètes dans tous les domaines de la forêt.

17. Qu'est-ce que le protocole Kerberos et comment est-il utilisé dans l'Active Directory ?

Le protocole Kerberos est un protocole d'authentification réseau utilisé dans AD. Il permet des échanges sécurisés et authentifiés entre les utilisateurs et les services. Kerberos est utilisé pour vérifier les identités des utilisateurs et leur fournir des tickets d'accès aux ressources réseau.

18. Comment configurez-vous une stratégie de groupe dans l'Active Directory ?

Pour configurer une stratégie de groupe (GPO) :

1. Ouvrez la console de gestion des stratégies de groupe (GPMC).

2. Créez un nouveau GPO ou modifiez un GPO existant.

3. Configurez les paramètres souhaités sous les sections "Computer Configuration" et "User Configuration".

4. Liez le GPO au conteneur (site, domaine ou OU) approprié.

5. Appliquez et testez la stratégie sur les utilisateurs ou les ordinateurs cibles.