MICROSOFT OFFICIAL COURSE

Chapitre 2 : Présentation des services de domaine Active Directory

Vue d'ensemble du module

- Vue d'ensemble d'AD DS
- Vue d'ensemble des composants logiques AD DS
- Vue d'ensemble des composants physiques AD DS

Leçon 1 : Vue d'ensemble d'AD DS

- Pourquoi déployer AD DS ?
- Qu'est-ce que l'authentification ?
- Qu'est-ce qu'une autorisation ?
- Utilisation d'AD DS pour centraliser la gestion réseau
- Vue d'ensemble des composants AD DS

Pourquoi déployer AD DS ?

AD DS fournit un système centralisé pour la gestion des utilisateurs, des ordinateurs et d'autres ressources sur un réseau

Les fonctionnalités AD DS sont les suivantes :

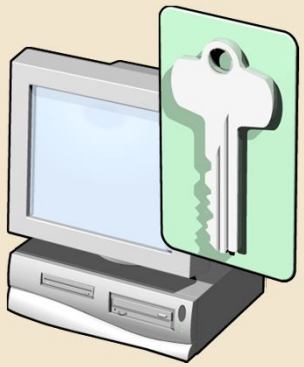
- **Annuaire centralisé**
- **Accès via authentification unique**
- **Sécurité intégrée**
- **Évolutivité**
- **Interface de gestion commune**

Qu'est-ce que l'authentification ?

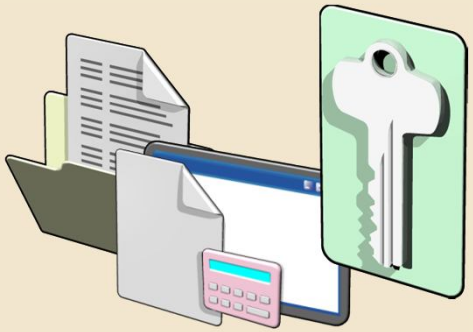
L'authentification est un processus qui consiste à vérifier l'identité d'un utilisateur sur un réseau

L'authentification comporte deux composants :

- **Ouverture de session interactive : autorise l'accès à l'ordinateur local**



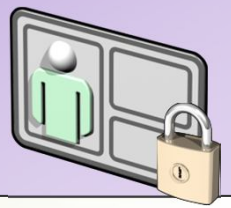
- **Authentification réseau : autorise l'accès aux ressources réseau**



Qu'est-ce qu'une autorisation ?

L'autorisation est un processus qui consiste à vérifier qu'un utilisateur authentifié a l'autorisation d'exécuter une action

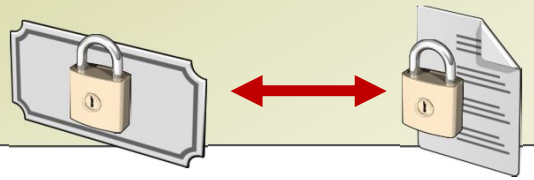
- **Les entités de sécurité sont émises en tant qu'identificateurs de sécurité (SID) lorsque le compte est créé**



- **Des jetons de sécurité sont émis pour les comptes d'utilisateurs au cours de l'authentification et ils incluent le SID de l'utilisateur ainsi que les SID de tout groupe connexe**

- **Les ressources partagées sur un réseau incluent des listes de contrôle d'accès (ACL) qui définissent qui peut accéder à la ressource**

- **Le jeton de sécurité est comparé à la liste DACL sur la ressource et l'accès est accordé ou refusé**



Utilisation d'AD DS pour centraliser la gestion réseau

AD DS permet de centraliser la gestion réseau en fournissant les éléments suivants :

- **Emplacement unique et jeu d'outils pour la gestion des comptes d'utilisateurs et des comptes de groupes**
- **Emplacement unique pour l'autorisation d'accès à des ressources réseau partagées**
- **Service d'annuaire pour les applications utilisées avec AD DS**
- **Options pour la configuration de stratégies de sécurité qui s'appliquent à tous les utilisateurs et à tous les ordinateurs**
- **Stratégies de groupe pour la gestion des bureaux d'utilisateurs et des paramètres de sécurité**

Vue d'ensemble des composants AD DS

AD DS se compose à la fois de composants physiques et logiques

Composants physiques	Composants logiques
• Magasin de données • Contrôleurs de domaine • Serveur de catalogue global • Contrôleur de domaine en lecture seule	• Partitions • Schéma • Domaines • Arborescences de domaine • Forêts • Sites • Unités d'organisation

Leçon 2 : Vue d'ensemble des composants logiques AD DS

- Qu'est-ce que le schéma AD DS ?
- Qu'est-ce qu'un domaine ?
- Que sont les approbations AD DS ?
- Qu'est-ce qu'une arborescence de domaine ?
- Qu'est-ce qu'une forêt ?
- Qu'est-ce qu'une unité d'organisation ?
- Discussion : Scénarios pour l'implémentation de composants logiques AD DS
- Que sont les objets AD DS ?
- Démonstration : Outils pour la gestion du composant logique AD DS

Qu'est-ce que le schéma AD DS ?

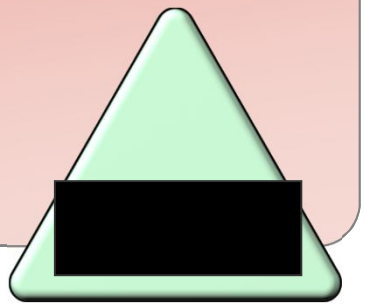
Le schéma AD DS :

- **Définit chaque type d'objet qui peut être stocké dans AD DS**
- **Applique des règles relatives à la création et la configuration d'objet**

Types d'objet	Fonction	Exemples
Objet de classe	Définit les nouveaux objets qui peuvent être créés dans l'annuaire	• Classe utilisateur • Classe ordinateur
Objet attribut	Définit les informations qui peuvent être stockées pour chaque classe d'objet	• Nom complet

Qu'est-ce qu'un domaine ?

Les domaines sont des composants d'annuaire logiques qui permettent de regrouper et de gérer les objets AD DS dans une organisation

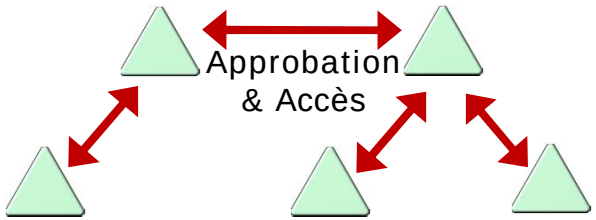


Les domaines fournissent :

- Une limite administrativepour l'application de stratégies à des groupes d'objets
- Une limite de réplicationpour la réplication de données entre des contrôleurs de domaine
- Une limite d'authentification et d'autorisationqui constitue un moyen de limiter l'étendue de l'accès aux ressources

Que sont les approbations AD DS ?

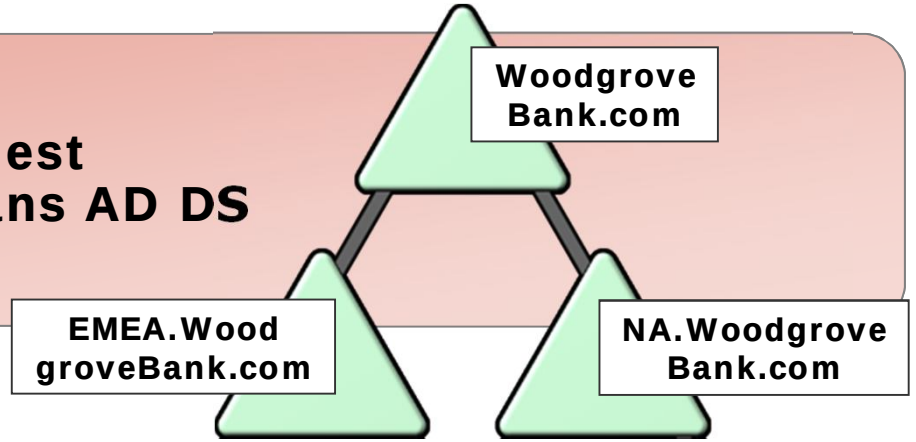
Les approbations fournissent un mécanisme qui permet aux utilisateurs d'accéder aux ressources d'un autre domaine

Types d'approbations	Description	Diagramme
Directionnelle	La direction de l'approbation va du domaine approuvé vers le domaine d'approbation	
Transitive	La relation d'approbation s'étend au-delà d'une approbation à deux domaines pour inclure d'autres domaines approuvés	

- Tous les domaines d'une forêt approuvent toutes les autres domaines de la forêt
- Les approbations peuvent s'étendre en dehors de la forêt

Qu'est-ce qu'une arborescence de domaine ?

Une arborescence de domaine est une hiérarchie de domaines dans AD DS

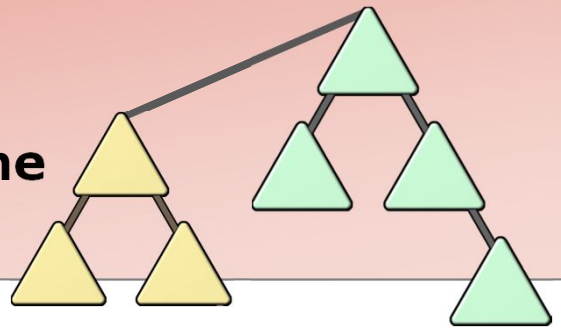


Tous les domaines de l'arborescence de domaine :

- **Possèdent un espace de noms contigu avec le domaine parent**
- **Peuvent avoir des domaines enfants supplémentaires ajoutés à l'espace de noms**
- **Possèdent une approbation transitive bidirectionnelle avec d'autres domaines de l'arborescence**

Qu'est-ce qu'une forêt ?

Une forêt est une collection d'une ou de plusieurs arborescences de domaine

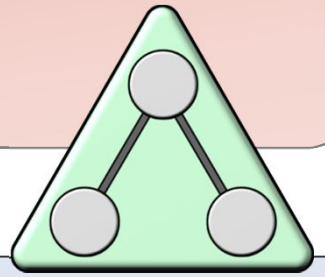


Les forêts :

- **Partagent un schéma commun**
- **Partagent une partition de configuration commune**
- **Partagent un catalogue global commun pour permettre les recherches**
- **Permettent les approbations entre tous les domaines de la forêt**
- **Partagent les groupes Administrateurs de l'entreprise et Administrateurs du schéma**

Qu'est-ce qu'une unité d'organisation ?

Les unités d'organisation sont des conteneurs Active Directory qui peuvent contenir des utilisateurs, des groupes, des ordinateurs et d'autres unités d'organisation



Les unités d'organisation peuvent être utilisées pour :

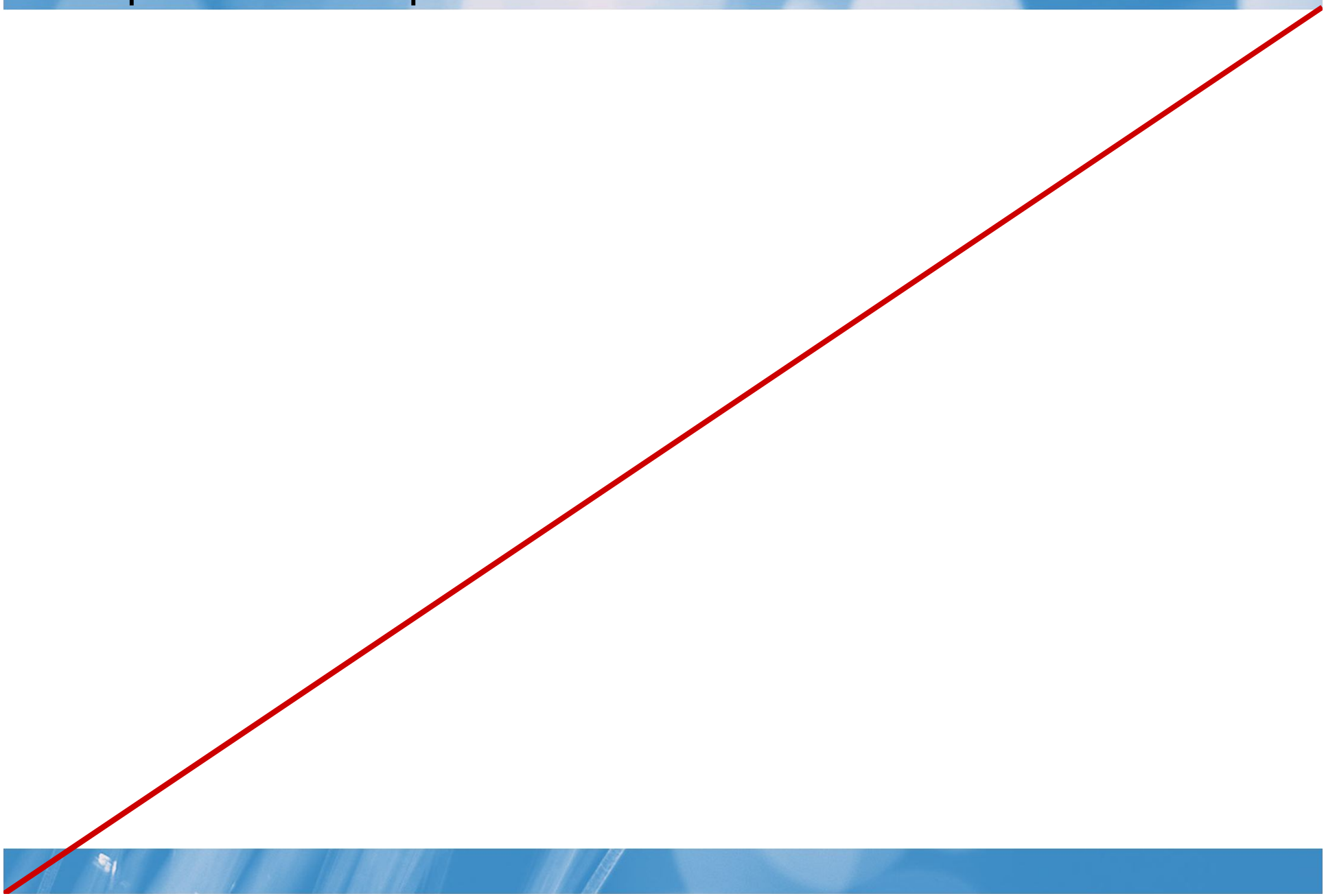
- **Représenter votre organisation sous forme hiérarchique et logique**
- **Gérer une collection d'objets de manière cohérente**
- **Déléguer des autorisations pour l'administration de groupes d'objets**
- **Appliquer des stratégies**

Discussion : Scénarios pour l'implémentation de composants logiques AD DS

Pour chaque scénario, décrivez les composants logiques AD DS qui devront être implémentés :

- Scénario 1 : Petite organisation
- Scénario 2 : Organisation moyenne
- Scénario 3 : Organisation d'étude
- Scénario 4 : Organisation d'entreprise

Diapositive annexe de la page Commentaires. Ne pas imprimer la diapositive. Voir le volet Commentaires



Que sont les objets AD DS ?

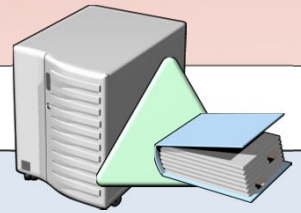
Objet	Description
Utilisateur	• Permet l'accès aux ressources réseau pour un utilisateur
InetOrgPerson	• Similaire à un compte d'utilisateur • Utilisé à des fins de compatibilité avec d'autres services d'annuaire
Contacts	• Utilisé essentiellement pour affecter des adresses de messagerie à des utilisateurs externes • Ne permet pas l'accès réseau
Groupes	• Utilisé pour simplifier l'administration du contrôle d'accès
Ordinateurs	• Permet l'authentification et l'audit de l'accès d'un ordinateur aux ressources
Imprimantes	• Utilisé pour simplifier le processus de localisation et de connexion aux imprimantes
Dossiers partagés	• Permet aux utilisateurs de rechercher des dossiers partagés à partir de propriétés

Leçon 3 : Vue d'ensemble des composants physiques AD DS

- Que sont les contrôleurs de domaine AD DS ?
- Vue d'ensemble du service DNS et d'AD DS
- Que sont les serveurs de catalogue global ?
- Qu'est-ce que le magasin de données AD DS ?
- Qu'est-ce que la réplication AD DS ?
- Que sont les sites ?
- Discussion : Scénarios pour l'implémentation de composants physiques AD DS
- Démonstration : Outils pour la gestion des composants physiques AD DS

Que sont les contrôleurs de domaine AD DS ?

Un contrôleur de domaine est un serveur sur lequel le rôle serveur AD DS est installé



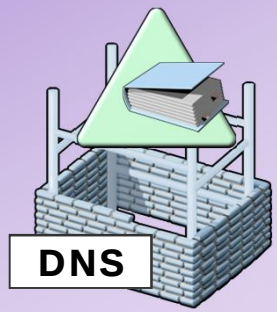
Les contrôleurs de domaine :

- **Hébergent une copie du magasin d'annuaire AD DS**
- **Fournissent des services d'authentification et d'autorisation**
- **Répliquent les mises à jour sur d'autres contrôleurs de domaine dans le domaine et la forêt**
- **Autorisent l'accès d'administration pour la gestion des comptes d'utilisateurs et des ressources réseau**

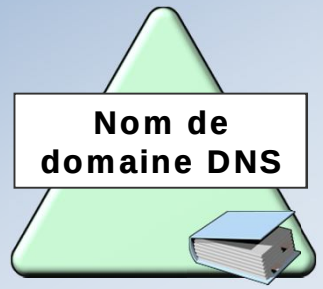
Windows Server 2008 AD DS prend en charge les contrôleurs de domaine en lecture seule

Vue d'ensemble du service DNS et d'AD DS

- **AD DS requiert une infrastructure DNS**

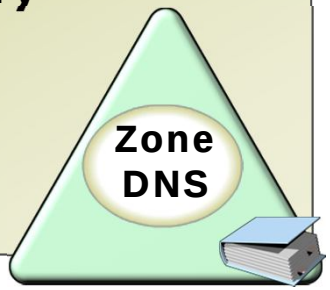


- **Les noms de domaine AD DS doivent être des noms de domaine DNS**



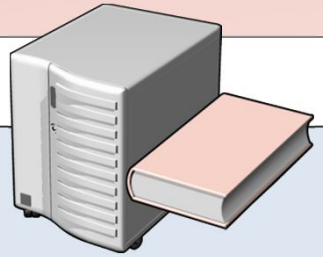
- **Les enregistrements de contrôleur de domaine AD DS doivent être inscrits dans DNS afin de permettre aux autres contrôleurs de domaine et aux ordinateurs clients de localiser les contrôleurs de domaine**

- **Les zones DNS peuvent être stockées dans AD DS comme les zones intégrées à Active Directory**



Que sont les serveurs de catalogue global ?

Les serveurs de catalogue global sont des contrôleurs de domaine qui stockent également une copie du catalogue global



Le catalogue global :

- **Contient une copie de tous les objets AD DS dans une forêt qui inclut uniquement certains attributs pour chaque objet de la forêt**
- **Améliore l'efficacité des recherches d'objet en évitant les référence inutiles aux contrôleurs de domaine**
- **Est requis pour que les utilisateurs puissent ouvrir une session sur un domaine**

Qu'est-ce que le magasin de données AD DS ?

Le magasin de données AD DS contient les fichiers de base de données et les processus qui stockent et gèrent les informations d'annuaire relatives aux utilisateurs, aux services et aux applications

Le magasin de données AD DS :

- **Comporte le fichier Ntds.dit**
- **Est stocké par défaut dans le dossier %SystemRoot%\NTDS sur tous les contrôleurs de domaine**
- **Est uniquement accessible à partir des processus et des protocoles de contrôleur de domaine**

Qu'est-ce que la réplication AD DS ?

La réplication AD DS copie toutes les mises à jour de la base de données AD DS sur tous les autres contrôleurs de domaine dans un domaine ou une forêt

La réplication AD DS :

- **Vérifie que tous les contrôleurs de domaine disposent des mêmes informations**
- **Utilise un modèle de réplication multimaître**
- **Peut être gérée par la création de sites AD DS**

La topologie de réplication AD DS est créée automatiquement au fur et à mesure que de nouveaux contrôleurs de domaine sont ajoutés au domaine

Que sont les sites ?

Un site AD DS est utilisé pour représenter un segment réseau dans lequel tous les contrôleurs de domaine sont connectés via une connexion réseau rapide et fiable

Les sites sont :

- **Associés à des sous-réseaux IP**
- **Utilisés pour gérer le trafic de réplication**
- **Utilisés pour gérer le trafic d'ouverture de session client**
- **Utilisés par des applications orientées site telles que le système de fichiers DFS (Distributed File Systems) ou Exchange Server 2007**
- **Utilisés pour attribuer des objets de stratégie de groupe à tous les utilisateurs et à tous les ordinateurs sur un site d'entreprise**

Discussion : Scénarios pour l'implémentation de composants physiques AD DS

Pour chaque scénario, décrivez les composants physiques AD DS qui devront être implémentés :

- Scénario 1 : Petite organisation
- Scénario 2 : Organisation moyenne
- Scénario 3 : Organisation d'étude
- Scénario 4 : Organisation d'entreprise

Atelier pratique : Exploration des composants et des outils AD DS

- Exercice 1 : Examen des composants logiques AD DS
- Exercice 2 : Examen des composants physiques AD DS

Informations d'ouverture de session

Ordinateur virtuel	**6857A-NYC-DC1, 6857A-LON-DC1**
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Ordinateur virtuel	**6857A-NYC-CL1**
Nom d'utilisateur	**Thomas**
Mot de passe	**Pa$$w0rd**

Durée approximative : 45 minutes

Contrôle des acquis de l'atelier pratique

- Dans cet atelier pratique, vous avez administré l'environnement AD DS à l'aide des outils d'administration et vous avez utilisé Bureau à distance. Quels sont les avantages de chaque approche pour l'administration d'un ordinateur qui exécute Windows Server 2008 ? Quelle option préféreriez-vous utiliser ?
- Comment pourriez-vous combiner tous les outils que vous avez utilisés dans cet atelier pratique sur une console de gestion ?

Contrôle des acquis et éléments à retenir

- Questions de contrôle des acquis
- Résumé des services de domaine Active Directory