Microsoft® Official Course

Module 3

Gestion des services de domaine Active Directory

Microsoft

Vue d'ensemble du module

- Vue d'ensemble d'AD DS
- Implémentation des contrôleurs de domaine virtualisés
- Implémentation des contrôleurs de domaine en lecture seule
- Administration d'AD DS
- Gestion de la base de données AD DS

Leçon 1: Vue d'ensemble d'AD DS

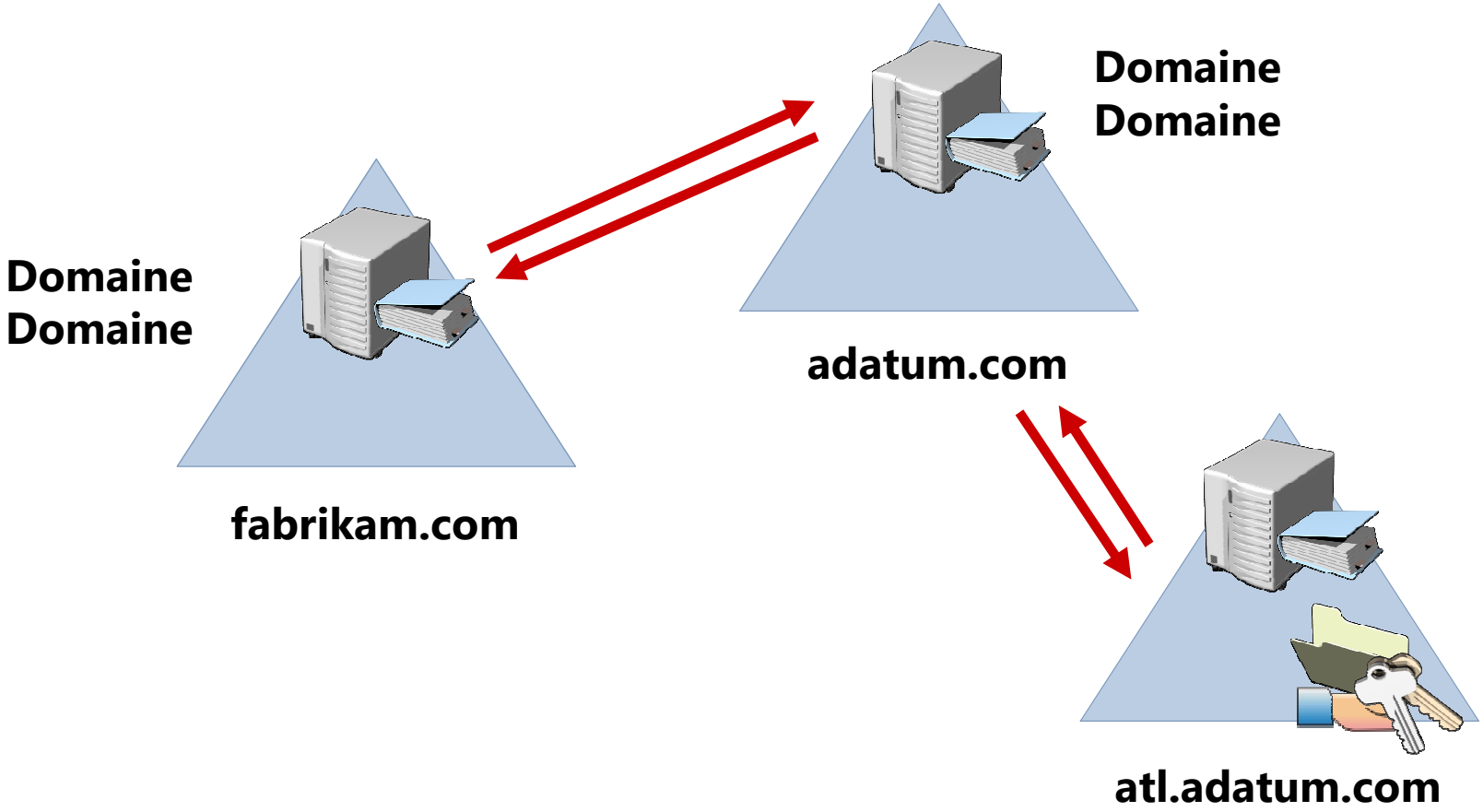
- Vue d'ensemble des composants AD DS
- Présentation de la structure de la forêt et schématique d'AD DS
- Présentation de la structure de domaine AD DS

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 • Contrôleurs de domaine en lecture seule	• Partitions • Schéma • Domaines • Arborescences de domaine • Forêts • Sites • Unités d'organisation

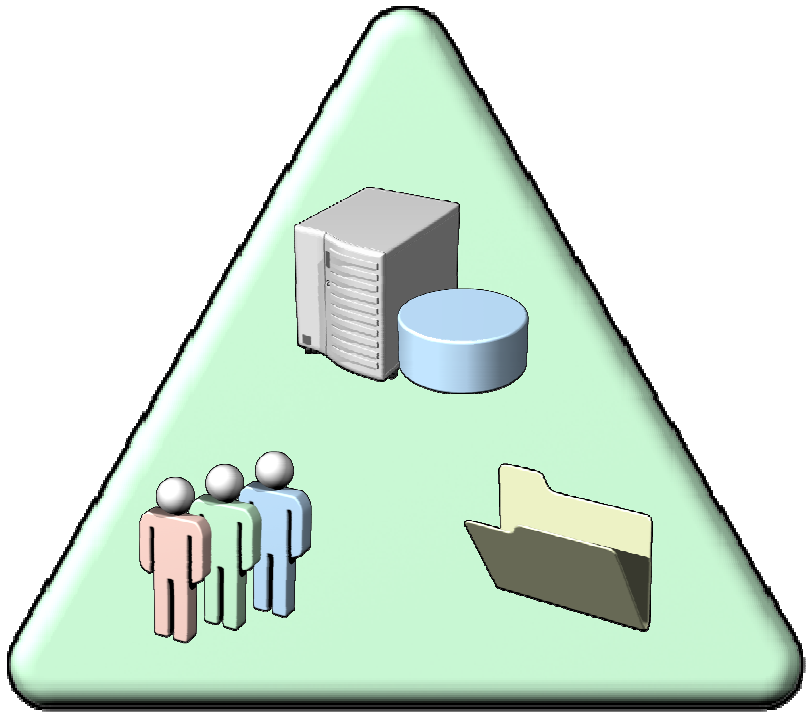
Présentation de la structure de la forêt et schématique d'AD DS



Présentation de la structure de domaine AD DS

- Les services AD DS requièrent un ou plusieurs contrôleurs de domaine
- Tous les contrôleurs de domaine maintiennent une copie de la base de données du domaine synchronisée en permanence

  - Le domaine est le contexte dans lequel des utilisateurs, des groupes et des ordinateurs sont créés
  - Le domaine est une limite de réplication
  - Le domaine est un centre d'administration pour configurer et gérer des objets
  - N'importe quel contrôleur de domaine peut authentifier n'importe quelle connexion au domaine



Leçon 2: Implémentation des contrôleurs de domaine virtualisés

- Présentation des contrôleurs de domaine virtualisés clonés
- Déployer un contrôleur de domaine virtualisé cloné
- Gestion des contrôleurs de domaine virtualisés

Présentation des contrôleurs de domaine virtualisés clonés

Windows Server 2012 fournit les fonctionnalités suivantes pour les contrôleurs de domaine virtualisés :

- Clonage sûr
- Restauration sûre depuis une capture d'écran

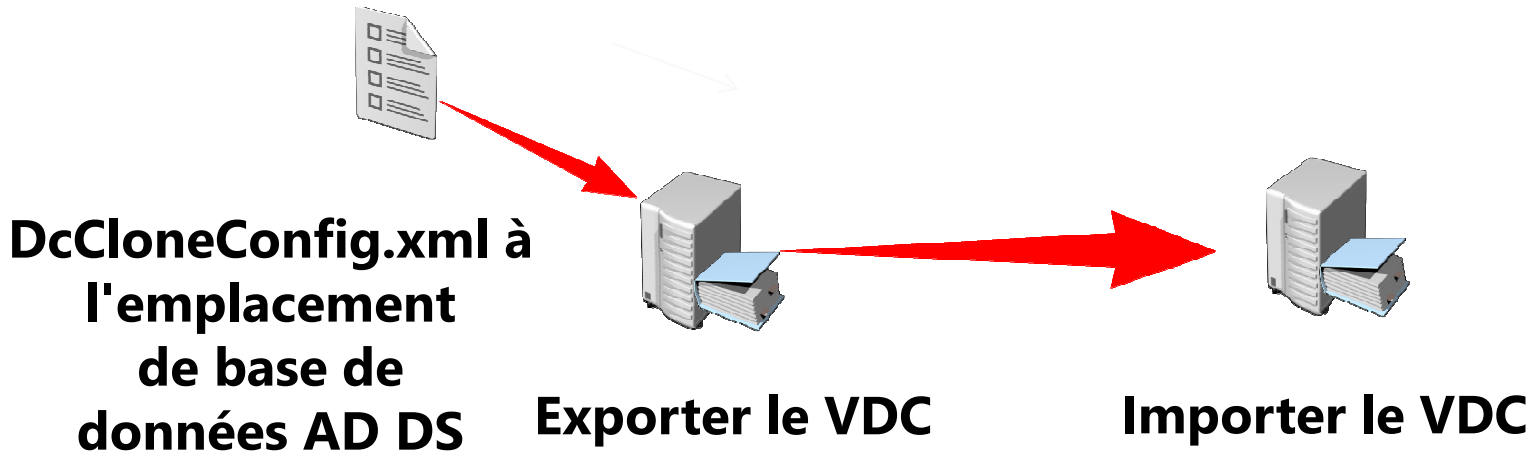
La mise en place des contrôleurs de domaine virtualisés offre les avantages suivants :

- Déploiement rapide des contrôleurs de domaine
- Mise en service évolutive des contrôleurs de domaine
- Remplacement ou récupération rapide des contrôleurs de domaine
- Approvisionnement facile des environnements de test

Déployer un contrôleur de domaine virtualisé cloné

Vous pouvez copier un contrôleur de domaine virtuel existant en toute sécurité en procédant comme suit :

1. créez un fichier DcCloneConfig.xml et enregistrez-le dans l'emplacement de base de données AD DS
2. prenez le VDC hors ligne et exportez-le
3. créez un nouvel ordinateur virtuel en important le VDC exporté



Gestion des contrôleurs de domaine virtualisés

Pour répliquer AD DS correctement, vérifiez les points suivants :

- Un contrôleur de domaine virtuel restauré peut entrer en contact avec un contrôleur de domaine accessible en écriture
- Vous ne restaurez pas tous les contrôleurs de domaine dans un domaine simultanément
- Toutes les modifications apportées depuis la dernière capture d'écran sont répliquées, sans quoi elles seront perdues

Observations concernant la gestion des captures d'écran :

- Les captures d'écran ne remplacent pas les copies de sauvegarde régulières
- Ne restaurez pas les captures d'écran réalisées avant la promotion du contrôleur de domaine
- N'hébergez pas tous les contrôleurs de domaine virtuels sur le même hyperviseur

Leçon 3: Implémentation des contrôleurs de domaine en lecture seule

- Éléments à prendre en compte pour implémenter les contrôleurs de domaine en lecteur seule
- Gestion de la mise en cache des informations d'identification d'un contrôleur de domaine en lecture seule
- Gestion de l'administration locale des contrôleurs de domaine en lecture seule

Éléments à prendre en compte pour implémenter les contrôleurs de domaine en lecteur seule

- Les contrôleurs de domaine en lecture seule fournissent plusieurs fonctions importantes :
  - Mise en cache des informations d'identification
  - Séparation des rôles d'administration
  - DNS en lecture seule

- Pour déployer un contrôleur de domaine en lecture seule :
  1. Assurez-vous qu'il n'y a aucun compte informatique dans AD DS pour le nouveau contrôleur de domaine en lecture seule
  2. Pré-créez le compte de contrôleur de domaine en lecture seule dans AD DS dans le conteneur de contrôleurs de domaine
  3. Exécutez l'assistant d'installation d'AD DS sur le nouveau contrôleur de domaine en lecture seule

Gestion de la mise en cache des informations d'identification d'un contrôleur de domaine en lecture seule

- La mise en cache des informations d'identification est gérée au moyen de stratégies de réplication de mot de passe
- Stratégies de réplication de mot de passe :
  - Déterminez les informations d'identification à mettre en cache sur un contrôleur de domaine en lecture seule
    - Comptes d'utilisateurs
    - Comptes informatiques
  - Présence d'une liste verte et d'une liste d'exclusion
    - Groupe autorisé à la réplication de mot de passe de contrôleur de domaine en lecture seule
    - Groupe exclu de la réplication des mots de passe de contrôleur de domaine en lecture seule
- Ne mettez pas en cache les comptes administratifs de domaine

Gestion de l'administration locale des contrôleurs de domaine en lecture seule

- Déléguez l'administration du contrôleur de domaine en lecture seule aux administrateurs locaux
- Définissez un principal de sécurité unique en tant qu'administrateur
  - Utilisateur
  - Groupe
- Activez à l'aide des méthodes suivantes :
  - Géré par l'onglet du contrôleur de domaine en lecture seule
  - dsmgmt
  - ntsdutil
- Mettez en cache les informations d'identification des administrateurs délégués

Leçon 4: Administration d'AD DS

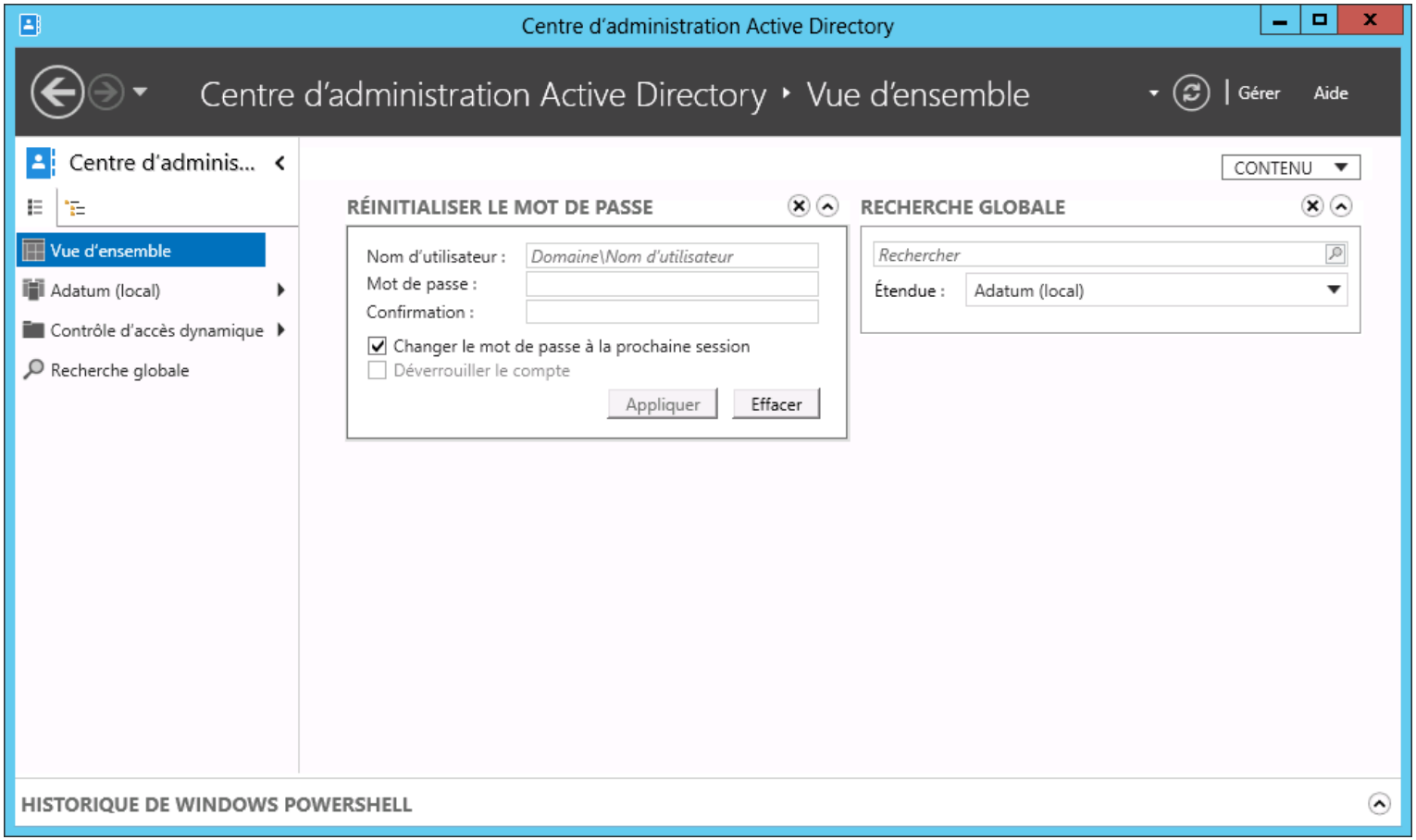
- Vue d'ensemble des composants logiciels enfichables d'administration d'Active Directory
- Vue d'ensemble du centre d'administration d'Active Directory
- Vue d'ensemble du module Active Directory pour Windows PowerShell
- Démonstration : Gestion d'AD DS à l'aide des outils de gestion
- Gestion des rôles des maîtres d'opérations
- Gestion des sauvegardes et des récupérations AD DS

Vue d'ensemble des composants logiciels enfichables d'administration d'Active Directory

- Les composants logiciels enfichables de l'administration d'Active Directory sont composés de quatre consoles différentes de MMC :
  - Utilisateurs et ordinateurs Active Directory
  - Sites et services Active Directory
  - Domaines et approbations Active Directory
  - Schéma Active Directory

Vue d'ensemble du centre d'administration d'Active Directory

- Le centre d'administration Active Directory est un outil adapté à la tâche selon Windows PowerShell



Vue d'ensemble du module Active Directory pour Windows PowerShell

- Le module Active Directory pour Windows PowerShell fournit des fonctionnalités administratives complètes dans les domaines suivants :
  - Gestion des utilisateurs
  - Gestion de l'ordinateur
  - Gestion des groupes
  - Gestion de l'unité d'organisation
  - Gestion de la stratégie de mot de passe
  - Recherche et modification d'objets
  - Gestion des forêts et des domaines
  - Gestion des contrôleurs de domaine et des maîtres d'opérations
  - Gestion des comptes de service gérés
  - Gestion des réplications de site
  - Gestion de l'accès centralisé et des revendications

Démonstration : Gestion d'AD DS à l'aide des outils de gestion

- Dans cette démonstration, vous allez apprendre à :
  - Créer des objets dans Utilisateurs et ordinateurs Active Directory
  - Rechercher des attributs d'objets dans Utilisateurs et ordinateurs Active Directory
  - Naviguer dans le centre d'administration Active Directory
  - Effectuer une tâche administrative dans le centre d'administration Active Directory
  - Utiliser la visionneuse de Windows PowerShell dans le centre d'administration Active Directory
  - Gérer les objets d'Active Directory DS avec Windows PowerShell

Gestion des rôles des maîtres d'opérations

Des rôles de maître d'opérations sont attribués au contrôleur de domaine responsable d'effectuer une tâche spécifique sur la forêt ou le domaine

- Rôles de maître d'opérations dans l'ensemble de la forêt
  - Rôle de maître d'attribution de noms de domaine
  - Rôle de contrôleur de schéma
- Rôles de maître d'opérations dans l'ensemble du domaine
  - Rôle de maître RID
  - Rôle de maître d'infrastructure
  - Rôle d'émulateur PDC

Gestion des sauvegardes et des récupérations AD DS

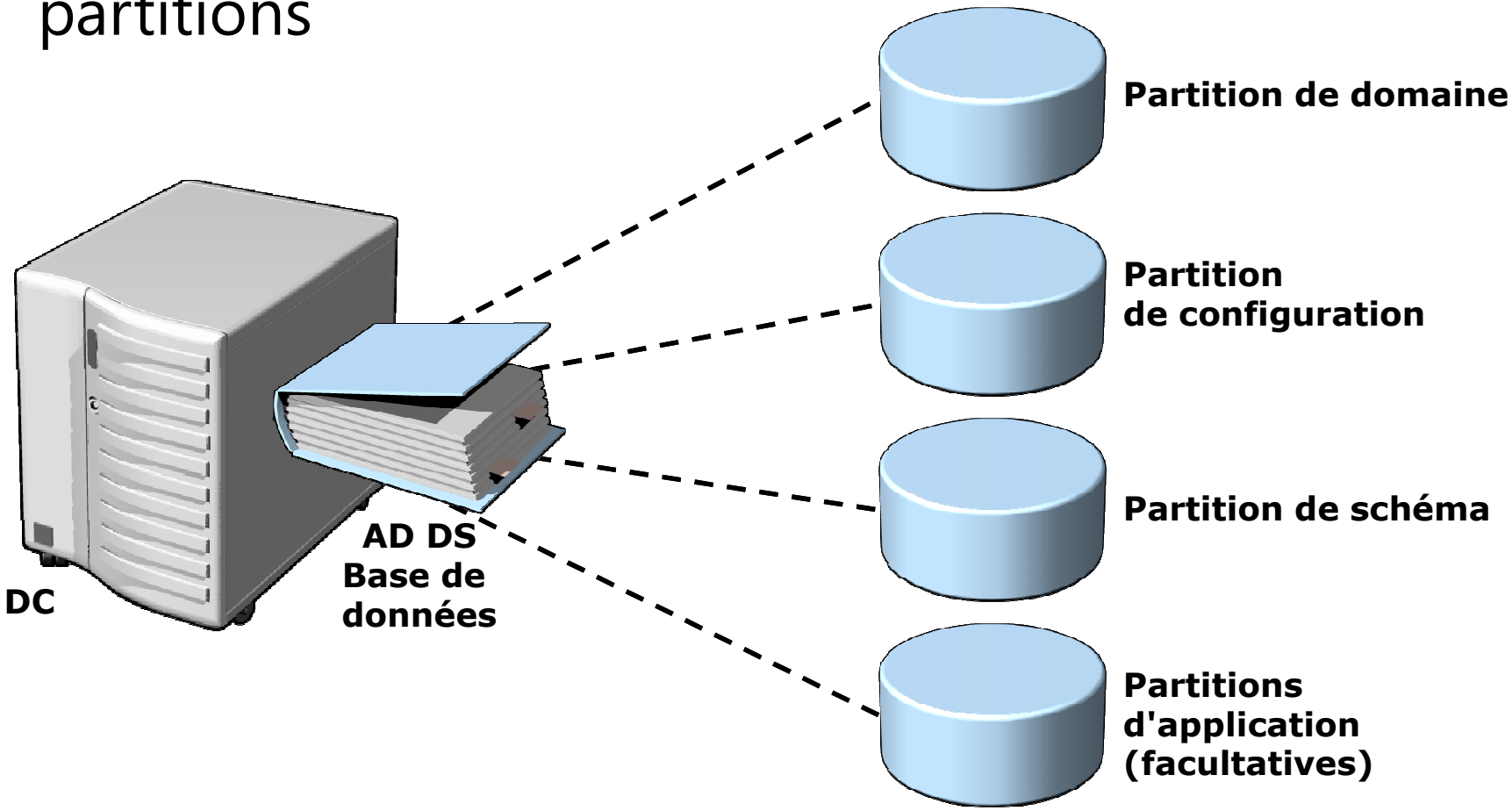
- Restauration ne faisant pas autorité ou normale
  - Restaurer le contrôleur de domaine vers son état valide antérieur connu
  - Le contrôleur de domaine sera mis à jour à l'aide de la réplication standard des partenaires
- Restauration forcée
  - Restaurer le contrôleur de domaine vers son état valide antérieur connu
  - Marquer les objets que vous souhaitez voir faire autorité
  - Le contrôleur de domaine est mis à jour depuis ses partenaires à jour
  - Le contrôleur de domaine envoie des mises à jour faisant autorité à ses partenaires
- Restauration de serveur entier
  - En général effectuée dans l'environnement de récupération Windows
- Restauration d'un autre emplacement

Leçon 5: Gestion de la base de données AD DS

- Présentation de la base de données AD DS
- Qu'est-ce que NTDSUtil ?
- Présentation des services AD DS redémarrables
- Démonstration : Exécution de la maintenance de la base de données AD DS
- Création d'instantanés AD DS
- Présentation de la restauration des objets supprimés
- Configuration de la Corbeille Active Directory

Présentation de la base de données AD DS

- La base de données AD DS maintient toutes les informations basées sur les domaines dans quatre partitions



Qu'est-ce que NTDSUtil ?

Avec NTDSUtil vous pouvez :

- Gérer et contrôler des opérations à maître unique
- Exécuter la maintenance de la base de données AD DS
  - Effectuer une défragmentation hors connexion
  - Créer et monter des captures d'écran
  - Déplacer les fichiers de base de données
- Maintenir les métadonnées de contrôleur de domaine
- Réinitialiser le mot de passe du mode de restauration des services d'annuaire

Présentation des services AD DS redémarrables

- Les services AD DS peuvent être démarrés ou arrêtés à l'aide de la console Services
- Les services AD DS peuvent se trouver dans trois états :
  - AD DS démarrés
  - AD DS arrêtés
  - DSRM
- Il est impossible de restaurer l'état du système lorsque les services AD DS sont à l'état arrêté

Démonstration : Exécution de la maintenance de la base de données AD DS

Dans cette démonstration, vous allez apprendre à :

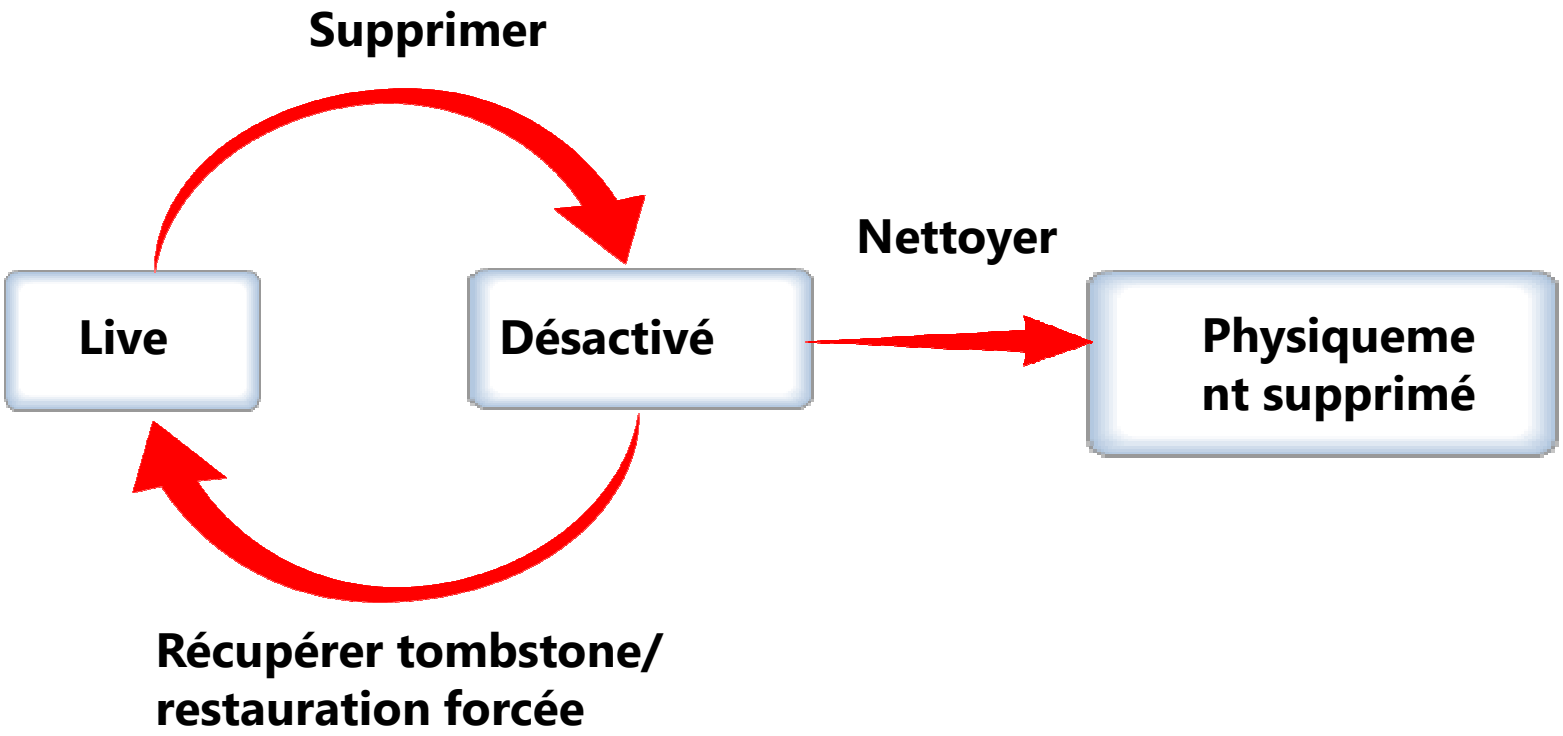
- Arrêter AD DS
- Exécuter une défragmentation hors ligne de la base de données AD DS
- Vérifier l'intégrité de la base de données AD DS
- Démarrer AD DS

Création d'instantanés AD DS

- Créer une capture d'écran d'Active Directory
  - NTDSUtil
- Monter la capture d'écran sur un port unique
  - NTDSUtil
- Exposer la capture d'écran
  - Cliquer avec le bouton droit sur le nœud racine Utilisateurs et ordinateurs Active Directory, puis cliquer sur Se connecter au contrôleur de domaine
  - Saisir serverFQDN:port
- Afficher la capture d'écran (en lecture seule)
  - Impossible de restaurer les données directement depuis la capture d'écran
- Récupérer les données
  - Se connecter à la capture d'écran montée, et exporter/réimporter des objets avec LDIFDE
  - Restaurer une sauvegarde de la même date que la capture d'écran
  - Ressaisir manuellement les données

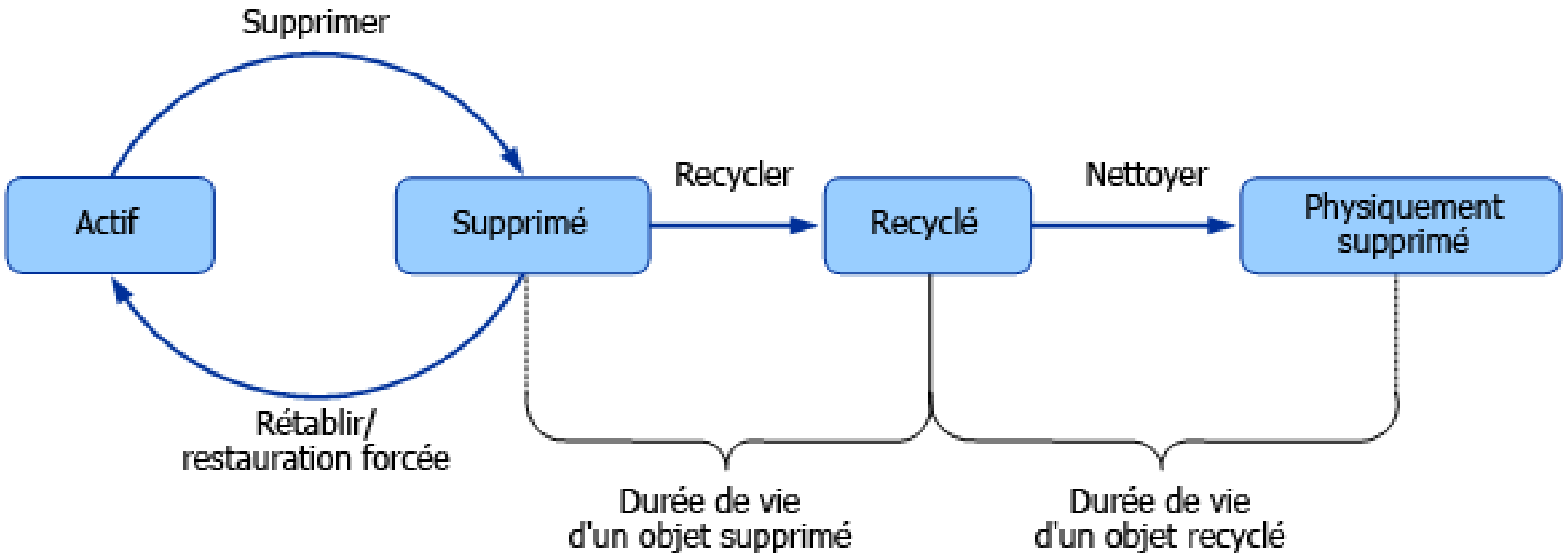
Présentation de la restauration des objets supprimés

- Des objets supprimés sont récupérés grâce à la fonction de récupération de l'objet tombstone
- Quand l'objet est supprimé, la plupart des attributs sont effacés
- La restauration forcée nécessite une interruption d'AD DS



Configuration de la Corbeille Active Directory

- La corbeille d'Active Directory offre un moyen de restaurer des objets supprimés sans interruption d'AD DS
- Elle utilise Windows PowerShell avec le module Active Directory ou le centre d'administration Active Directory pour restaurer des objets



Atelier pratique : Gestion d'AD DS

- Exercice 1 : Installation et configuration d'un contrôleur de domaine en lecture seule (RODC)
- Exercice 2 : Configuration des instantanés d'AD DS
- Exercice 3 : Configuration de la Corbeille Active Directory

Informations d'ouverture de session

Ordinateurs virtuels	22411B-LON-DC1 22411B-LON-SVR1
Nom d'utilisateur	**Administrateur**
Mot de passe	**Pa$$w0rd**

Durée approximative : 75 minutes

Scénario d'atelier pratique

A. Datum Corporation est une société internationale d'ingénierie et de fabrication, dont le siège social est à Londres, au Royaume-Uni. Un bureau informatique et un centre de données sont situés à Londres pour s'occuper du siège social et d'autres sites. A. Datum a récemment déployé une infrastructure serveur et client Windows Server 2012

A. Datum fait plusieurs modifications d'organisation qui requièrent des modifications portant sur l'infrastructure AD DS. Un nouvel emplacement requiert une méthode sécurisée de fournir AD DS sur site et vous avez été invité à étendre les fonctions de la corbeille Active Directory à l'organisation entière

Questions de contrôle des acquis

- Quels objets AD DS doivent avoir leurs informations d'identification mises en cache sur un contrôleur de domaine en lecture seule situé dans un emplacement distant ?
- Quels avantages le centre d'administration Active Directory fournit-il sur les utilisateurs et ordinateurs Active Directory ?

Contrôle des acquis et éléments à retenir

- Questions de contrôle des acquis
- Outils
- Méthode conseillée