

Présentation des Services de domaine Active Directory® (AD DS)

Présenté par :

➤ Pr. Nordine ZIDANE

Creative Commons



MICROSOFT OFFICIAL COURSE

Module 1

Présentation des Services de domaine Active Directory® (AD DS)

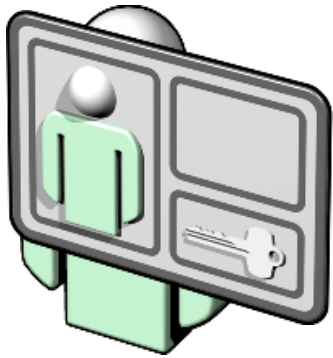
Vue d'ensemble du module

- Présentation d'Active Directory, des identités et des accès
- Composants et concepts d'Active Directory
- Installer les Services de domaine Active Directory
- Étendre IDA avec des services Active Directory

Leçon 1 : Présentation d'Active Directory et des services d'accès et d'identité

- Protection des informations en quelques mots
- Identité et accès (IDA)
- Authentification et autorisation
- Authentification
- Jetons d'accès
- Descripteurs de sécurité, listes de contrôle d'accès et entrées de contrôle d'accès
- Autorisation
- Authentification autonome (groupe de travail)
- Domaines Active Directory : magasin d'identités approuvées
- Active Directory et services d'accès et d'identité

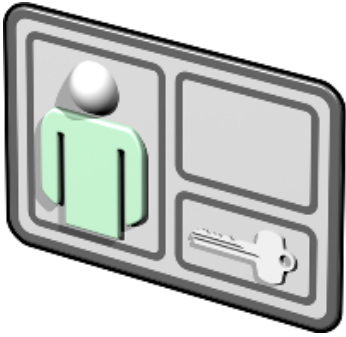
Protection des informations en quelques mots



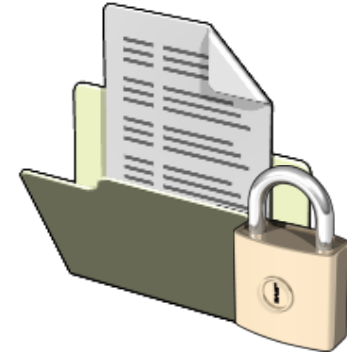
- Il s'agit de connecter des utilisateurs aux données dont ils ont besoin
... EN TOUTE SÉCURITÉ !
- IDA : Identity and Access (identité et accès)
- AAA : Authentication, Authorization, and Accounting (authentification, autorisation et gestion des comptes)
- CIA : Confidentiality, Integrity, and Availability (confidentialité, intégrité et disponibilité) (et authenticité)



Identité et accès (IDA)



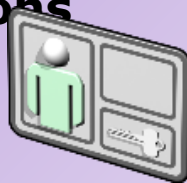
- Identité : compte d'utilisateur
- Enregistré dans un magasin d'identités (base de données d'annuaires)
- Entité de sécurité
- Représenté de manière unique par l'identificateur de sécurité (SID)



- Ressource : dossier partagé
- Sécurisé par un descripteur de sécurité
- Liste de contrôle d'accès discrétionnaire (DACL ou « ACL »)
- Entrées de contrôle d'accès (ACE ou « autorisations »)

Authentification et autorisation

- Un utilisateur présente des informations d'identification qui sont authentifiées à l'aide des informations stockées avec son identité.



- Le système crée un jeton de sécurité qui représente l'utilisateur avec le SID de l'utilisateur et tous les SID de groupe associés.



- Une ressource est sécurisée avec une liste de contrôle d'accès (ACL) : des autorisations correspondant à un SID avec un niveau d'accès.



- Le jeton de sécurité de l'utilisateur est comparé à la liste ACL de la ressource pour autoriser le niveau d'accès demandé.



Authentification

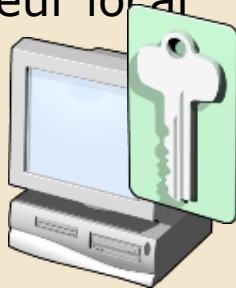
L'authentification est le processus de vérification de l'identité d'un utilisateur.

Informations d'identification : au moins deux composants nécessaires

- Nom d'utilisateur
- Secret, par exemple, un mot de passe

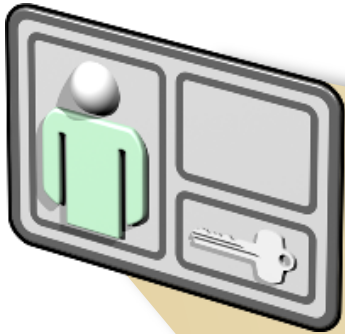
Deux types d'authentification

- Ouverture de session locale (interactive) : authentification d'ouverture de session sur l'ordinateur local



- Ouverture de session à distance (réseau) : authentification pour l'accès aux ressources d'un autre ordinateur





Jeton d'accès de l'utilisateur

SID de l'utilisateur

SID du groupe membre

Privilèges
(« autorisations de
l'utilisateur »)

Autres informations
d'accès

Descripteurs de sécurité, listes de contrôle d'accès et entrées de contrôle d'accès

Descripteur de sécurité

ACL du système
(**SACL**)

ACL discrétionnaire
(DACL ou « **ACL** »)

ACE

Masque d'accès du
client approuvé (SID)

ACE

Masque d'accès du
client approuvé (SID)



Autorisation

L'autorisation est le processus qui détermine s'il faut accorder ou refuser à un utilisateur le niveau d'accès demandé à une ressource.

Trois composants requis pour l'autorisation

- Ressource
- Demande d'accès
- Jeton de sécurité

Jeton d'accès de l'utilisateur

SID de l'utilisateur

SID du groupe

Liste des droits d'utilisateur

Autres informations d'accès

Le système recherche la première ACE dans l'ACL qui autorise ou refuse le niveau d'accès demandé pour tout SID présent dans le jeton de l'utilisateur.

Descripteur de sécurité

ACL du système (**SACL**)

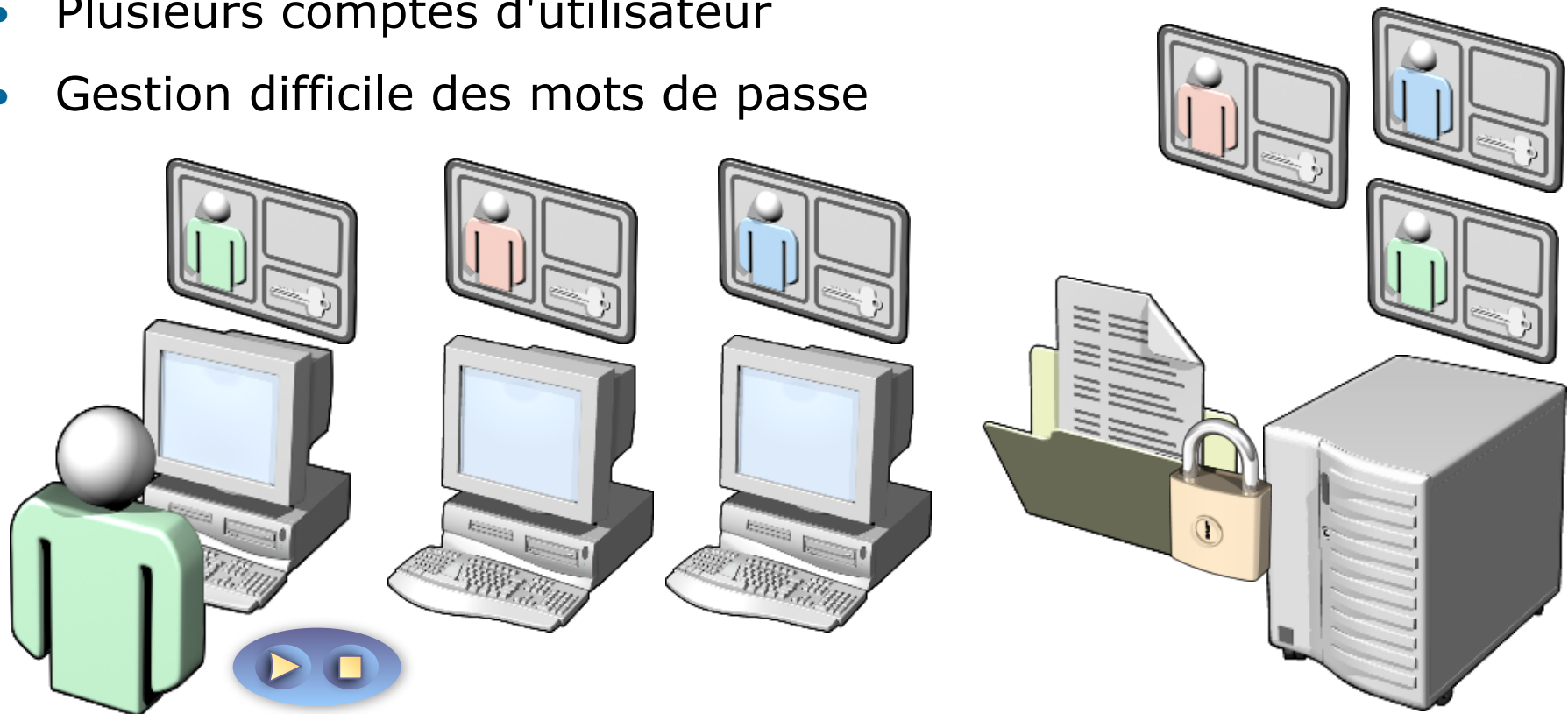
ACL discrétionnaire (DACL ou « **ACL** »)

ACE
Masque d'accès du client approuvé (SID)

ACE
Masque d'accès du client approuvé (SID)

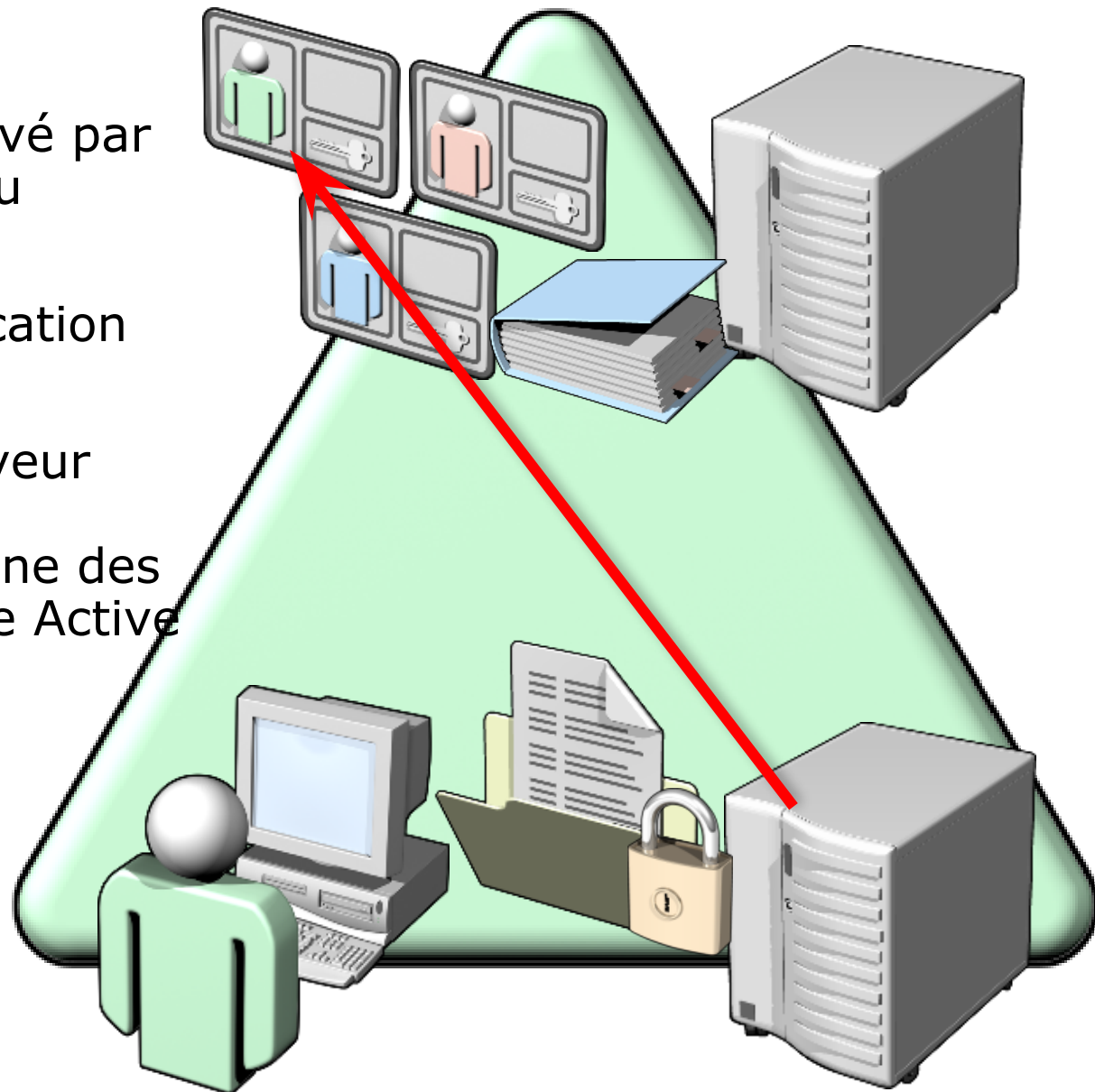
Authentification autonome (groupe de travail)

- Le magasin d'identités est la base de données du Gestionnaire des comptes de sécurité (SAM) dans le système Windows.
- Pas de magasin d'identités approuvées
- Plusieurs comptes d'utilisateur
- Gestion difficile des mots de passe



Domaines Active Directory : magasin d'identités approuvées

- Magasin d'identités centralisé et approuvé par tous les membres du domaine
- Service d'authentification centralisé
- Hébergé par un serveur jouant le rôle d'un contrôleur de domaine des Services de domaine Active Directory (AD DS)



Active Directory et services d'accès et d'identité

- Une infrastructure IDA doit :
 - stocker des informations sur les utilisateurs, les groupes, les ordinateurs et les autres identités ;
 - authentifier une identité ;
 - L'authentification Kerberos utilisée dans Active Directory fournit **l'authentification unique**. Les utilisateurs ne sont authentifiés qu'une fois.
 - contrôler l'accès ;
 - fournir une piste d'audit.
- Services Active Directory
 - Services de domaine Active Directory (AD DS)
 - Services AD LDS (Active Directory Lightweight Directory Services)
 - Services de certificats Active Directory (AD CS)
 - Services AD RMS (Active Directory Rights Management Services)
 - Services ADFS (Active Directory Federation Services)

Leçon 2 : Composants et concepts d'Active Directory

- Active Directory comme base de données
- Démonstration : schéma Active Directory
- Unités d'organisation
- Gestion à base de stratégies
- Banque de données Active Directory
- Contrôleurs de domaine
- Domaine
- Réplication
- Sites
- Arborescence
- Forêt
- Catalogue global
- Niveau fonctionnel
- Partitions d'applications et DNS
- Relations d'approbation

Active Directory comme base de données

- Active Directory est une base de données
 - Chaque « enregistrement » est un objet
 - Utilisateurs, groupes, ordinateurs...
 - Chaque « champ » est un attribut
 - Nom de connexion, SID, mot de passe, description, appartenance...
 - Identités (entités de sécurité ou « comptes »)
- Services : Kerberos, DNS, réplication, etc.

En fin de compte, AD DS est à la fois une base de données et les services qui prennent en charge ou utilisent cette base de données.

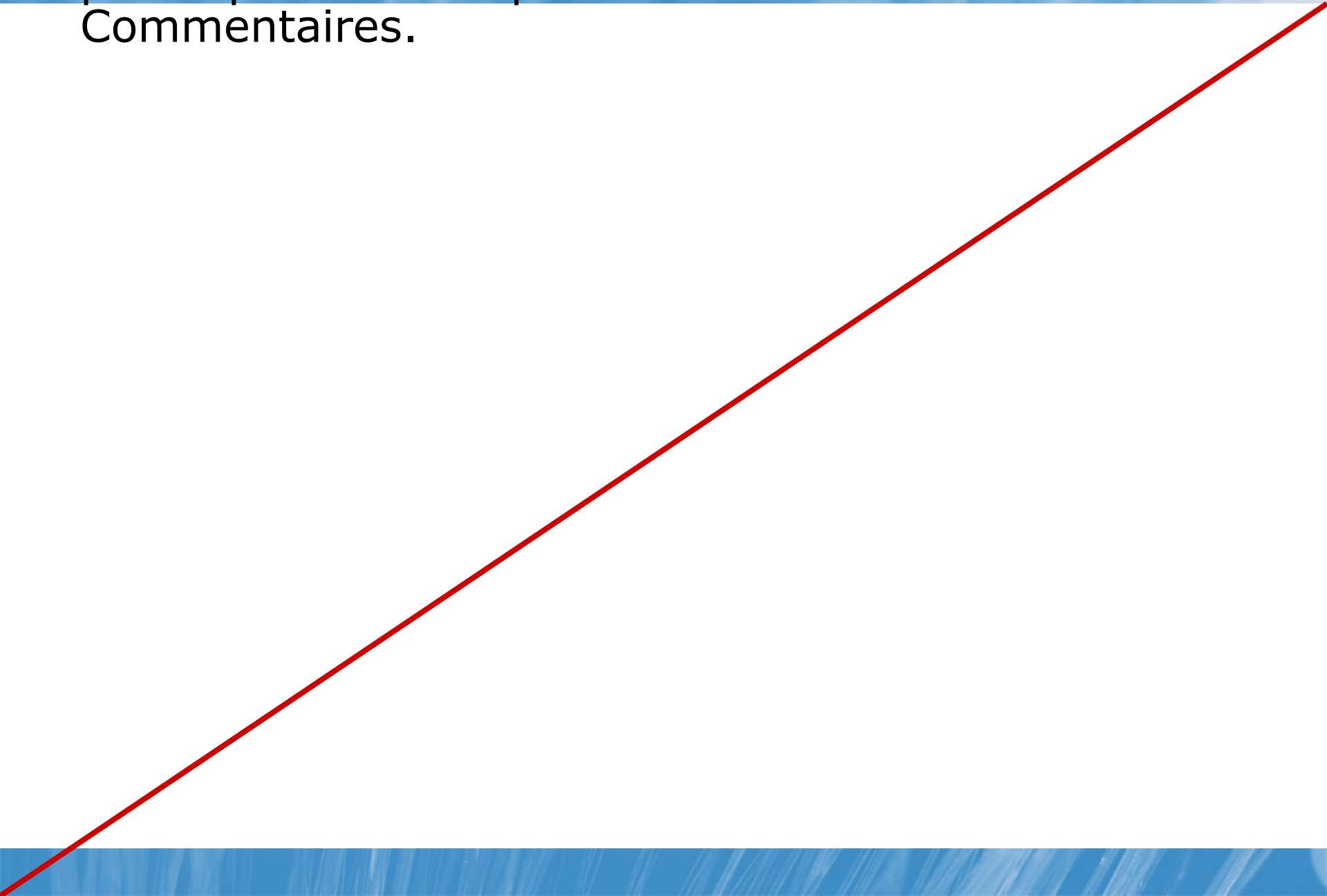
- Accès à la base de données
 - Outils Windows, interfaces utilisateur et composants
 - API (.NET, VBScript, Windows PowerShell)
 - Lightweight Directory Access Protocol (LDAP)

Démonstration : schéma Active Directory

Dans cette démonstration, nous allons :

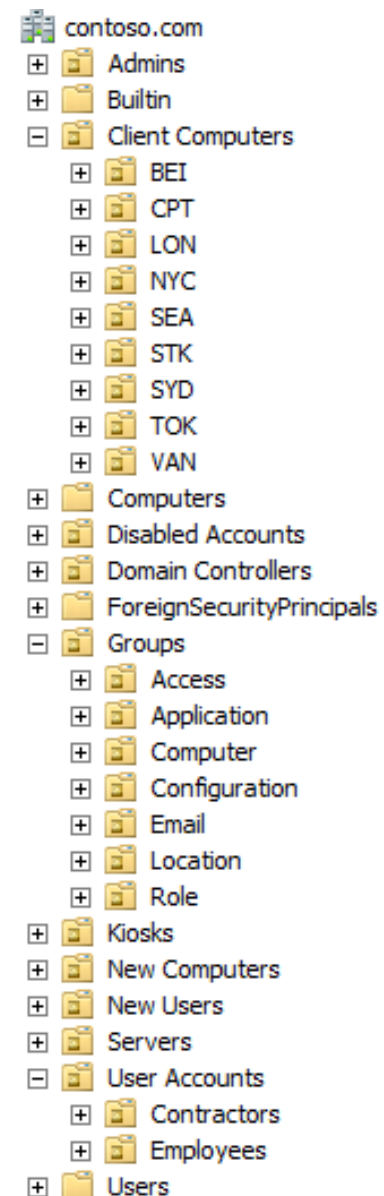
- découvrir comment le schéma agit comme un modèle pour Active Directory en définissant des attributs ;
 - objectSID
 - sAMAccountName
 - unicodePwd
 - member
 - Description
- et les classes d'objets
 - Utilisateur
 - Ventes

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



Unités d'organisation

- Conteneurs
 - Users
 - Computers
- Unités d'organisation
 - Des conteneurs qui prennent également en charge la gestion et la configuration des objets à l'aide d'une stratégie de groupe
 - Elles créent des unités d'organisation pour :
 - déléguer les autorisations administratives ;
 - appliquer la stratégie de groupe.



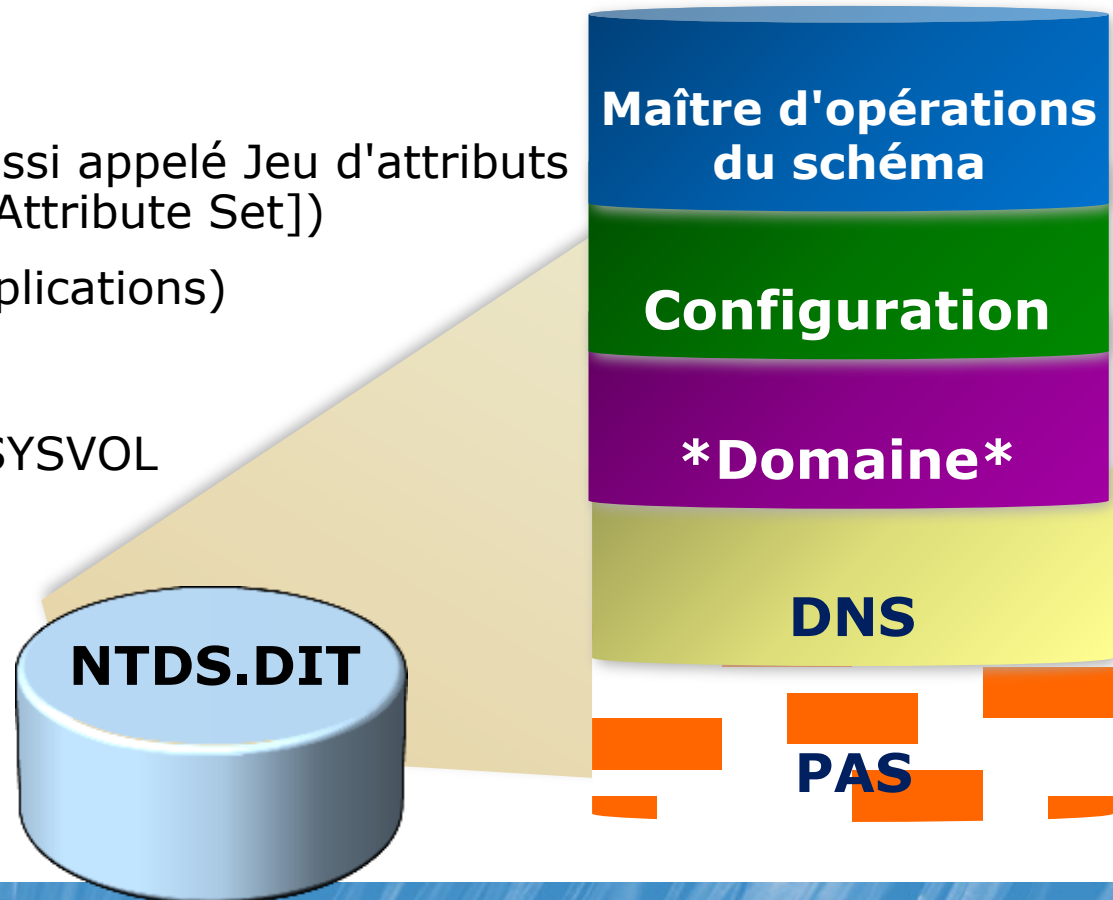
Gestion à base de stratégies

- Active Directory propose un point unique de gestion pour la sécurité et la configuration par des stratégies
 - Stratégie de groupe
 - Stratégie de mot de passe et de verrouillage du domaine
 - Stratégie d'audit
 - Configuration
 - Appliquée aux utilisateurs ou aux ordinateurs par une étendue d'objet de stratégie de groupe contenant des paramètres de configuration
 - Stratégies affinées pour les mots de passe et le verrouillage



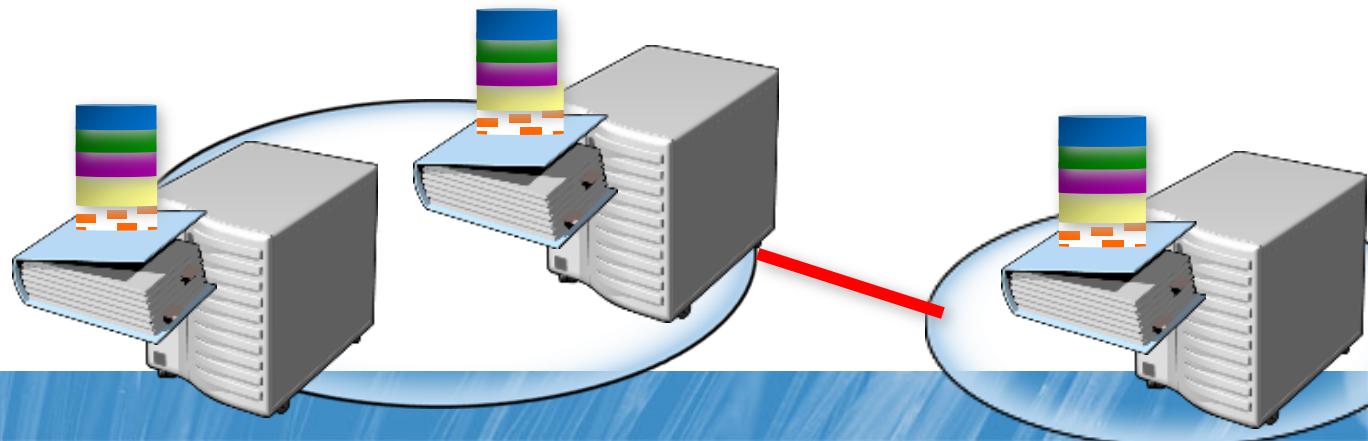
Banque de données Active Directory

- %racinesystème%\NTDS\ntds.dit
- Partitions logiques
 - Contexte d'appellation de domaine
 - Schéma
 - Configuration
 - Catalogue global (aussi appelé Jeu d'attributs partiel [PAS, Partial Attribute Set])
 - DNS (partitions d'applications)
- SYSVOL
 - %racinesystème%\SYSVOL
 - Scripts d'ouverture de session
 - Stratégies



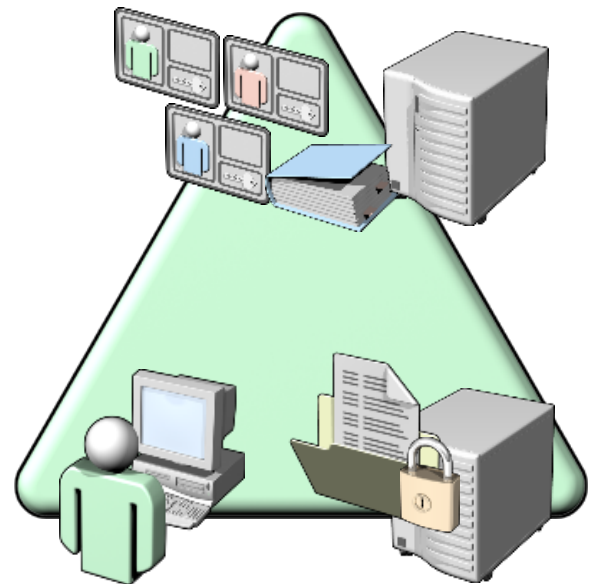
Contrôleurs de domaine

- Les serveurs jouant le rôle AD DS :
 - hébergent la base de données Active Directory (NTDS.DIT) et SYSVOL ;
 - sont répliqués entre les contrôleurs de domaine.
 - Service Centre de distribution de clés Kerberos (KDC) : authentication
 - Autres services Active Directory
- Pratiques recommandées
 - Disponibilité : au moins deux par domaine
 - Sécurité : installation minimale, contrôleurs de domaine en lecture seule



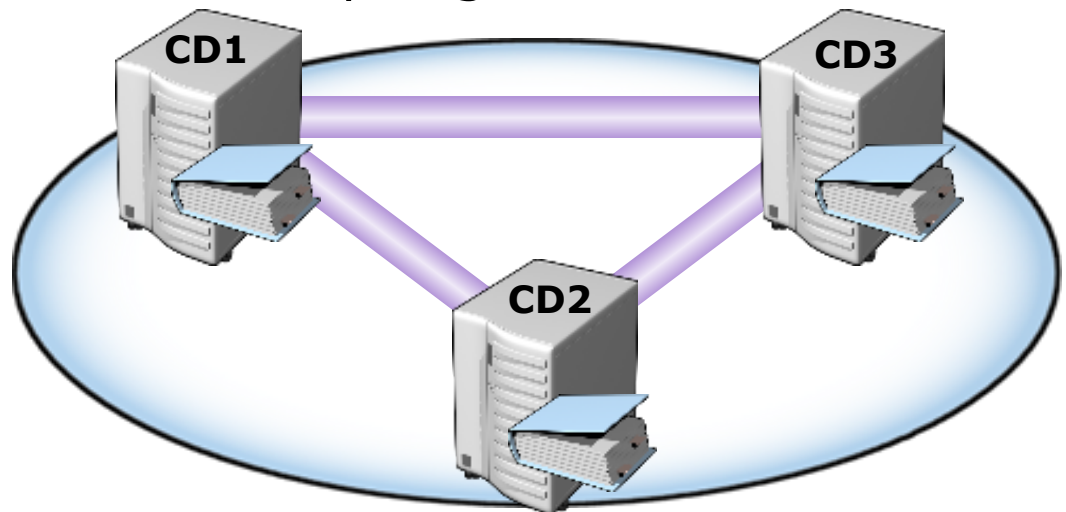
Domaine

- Composé d'un ou plusieurs contrôleurs de domaine
- Tous les contrôleurs de domaine répliquent le contexte d'appellation de domaine
 - Le domaine est le contexte dans lequel sont créés les utilisateurs, les groupes, les ordinateurs, etc.
 - Les « limites de réplication »
- Source d'identité approuvée : tout contrôleur de domaine peut authentifier toute ouverture de session dans le domaine
- Le domaine est l'étendue (limite) *maximale* pour certaines stratégies d'administration
 - Mot de passe
 - Verrouillage



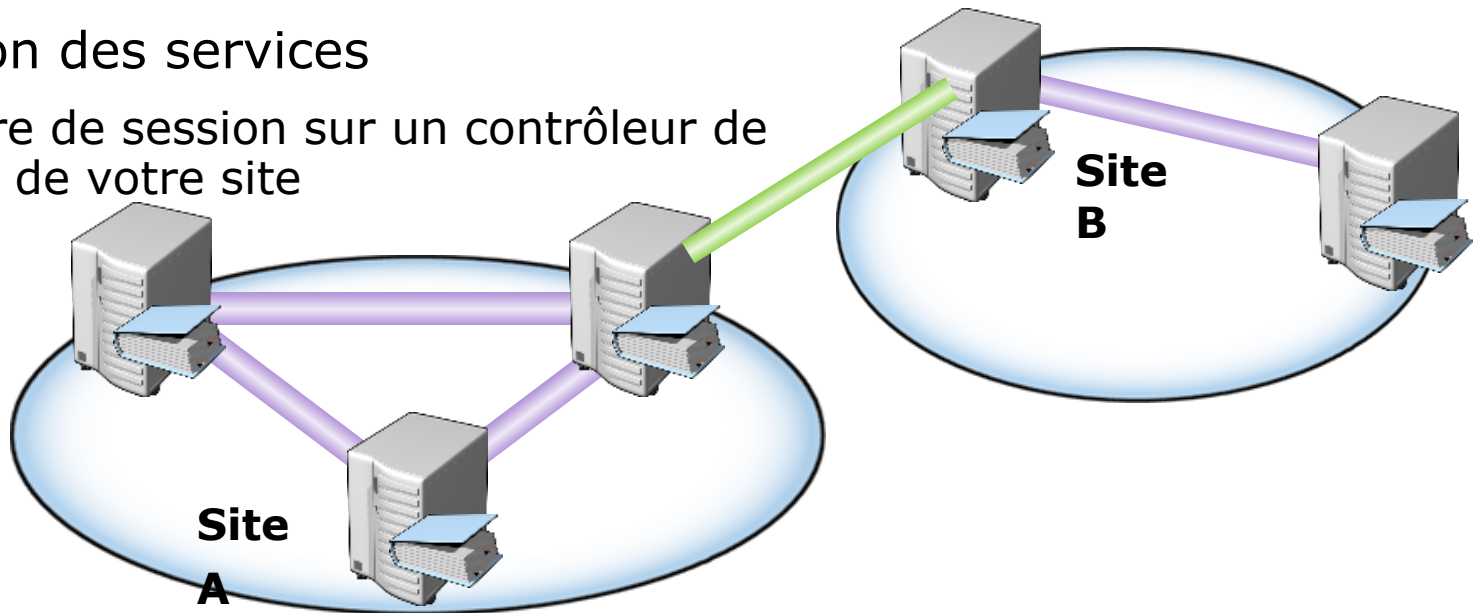
Réplication

- Réplication multimaître
 - Objets et attributs dans la base de données
 - Le contenu de SYSVOL est répliqué.
- Plusieurs composants travaillent pour créer une topologie de réplication robuste et efficace, et pour répliquer les modifications granulaires dans Active Directory.
- La partition de configuration de la base de données stocke des informations sur les sites, la topologie du réseau et la réplication.



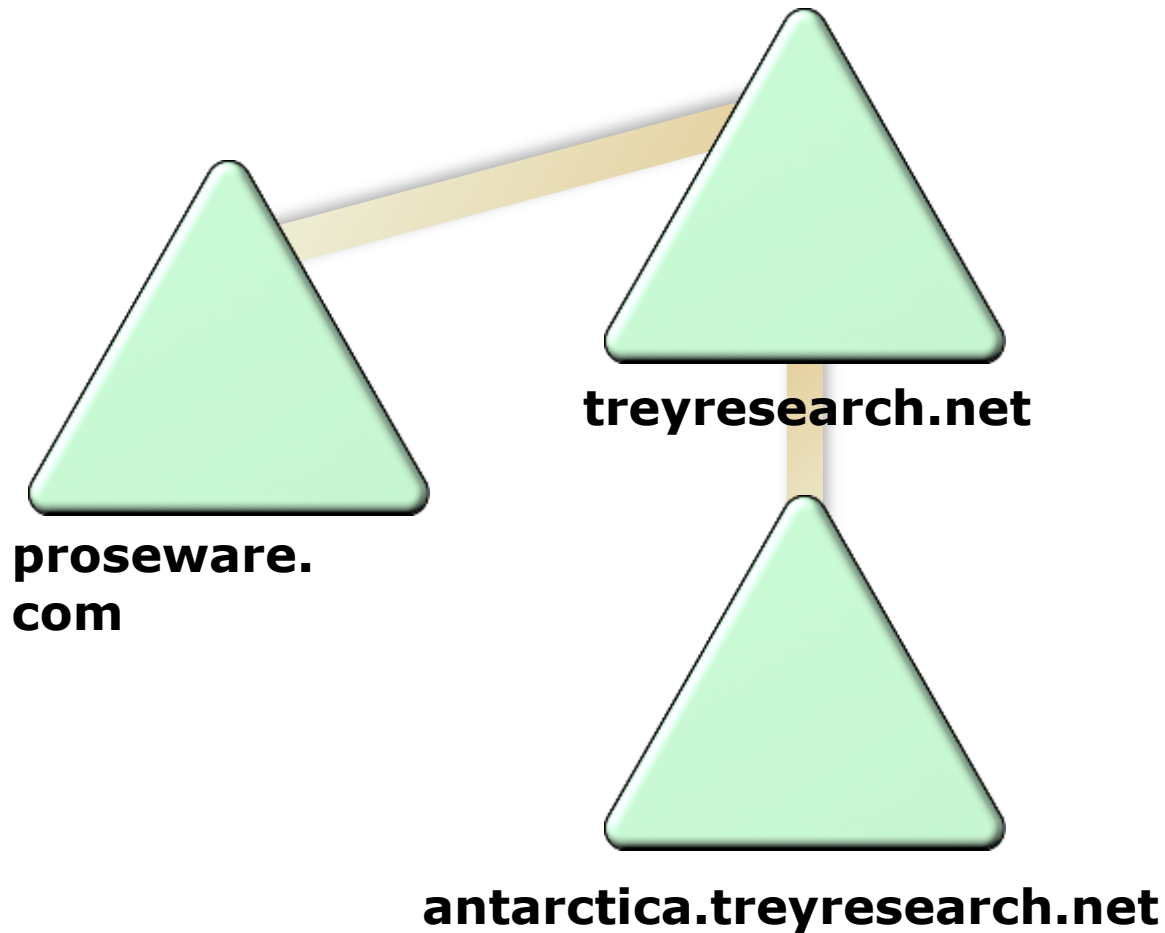
Sites

- Objet Active Directory qui représente une partie bien connectée de votre réseau
 - Associé à des objets de sous-réseau représentant des sous-réseaux IP
- Réplication intrasite/intersites
 - La réplication au sein d'un site se produit très rapidement (15 à 45 secondes).
 - La réplication entre sites peut être gérée.
- Localisation des services
 - Ouverture de session sur un contrôleur de domaine de votre site



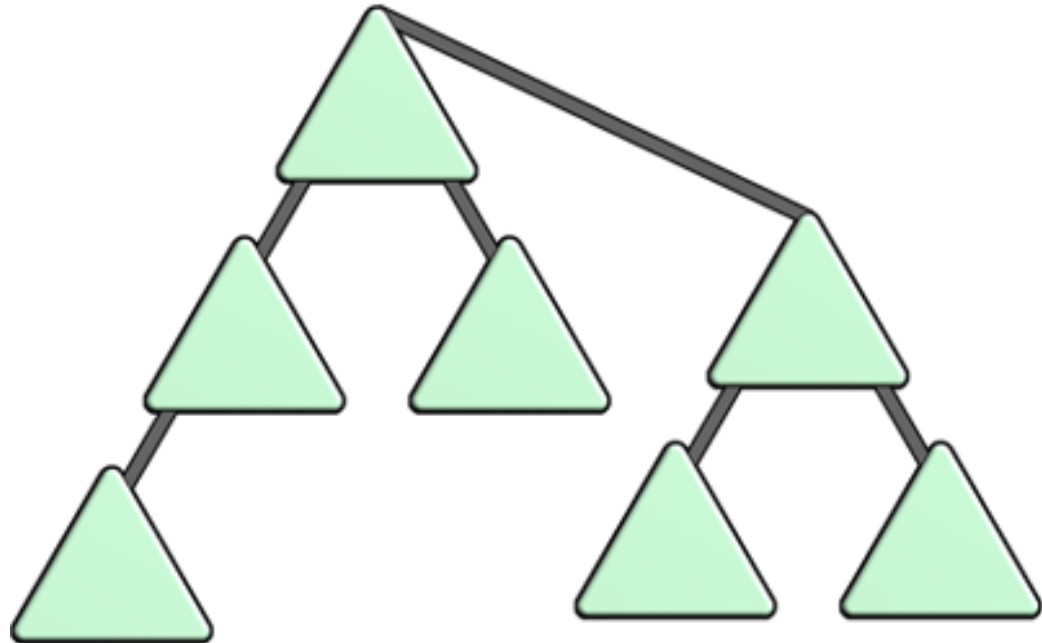
Arborescence

- Un ou plusieurs domaines dans une même instance d'AD DS qui partagent un *espace de noms DNS contigu*



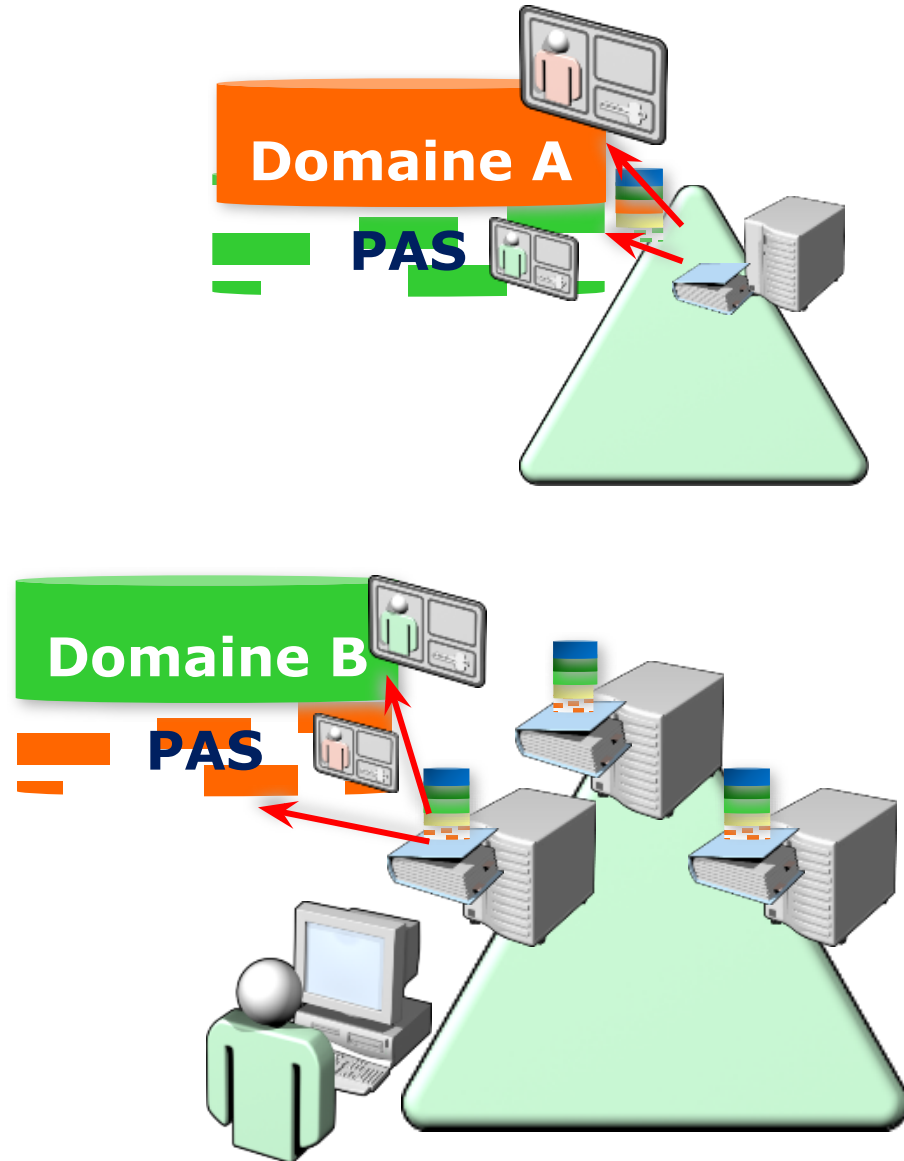
Forêt

- Un ensemble d'une ou plusieurs arborescences de domaines Active Directory
- Le premier domaine est le *domaine racine de la forêt*.
- Une seule configuration et un seul schéma répliqués dans *tous* les contrôleurs de domaine de la forêt
- Une limite de sécurité et de réplication



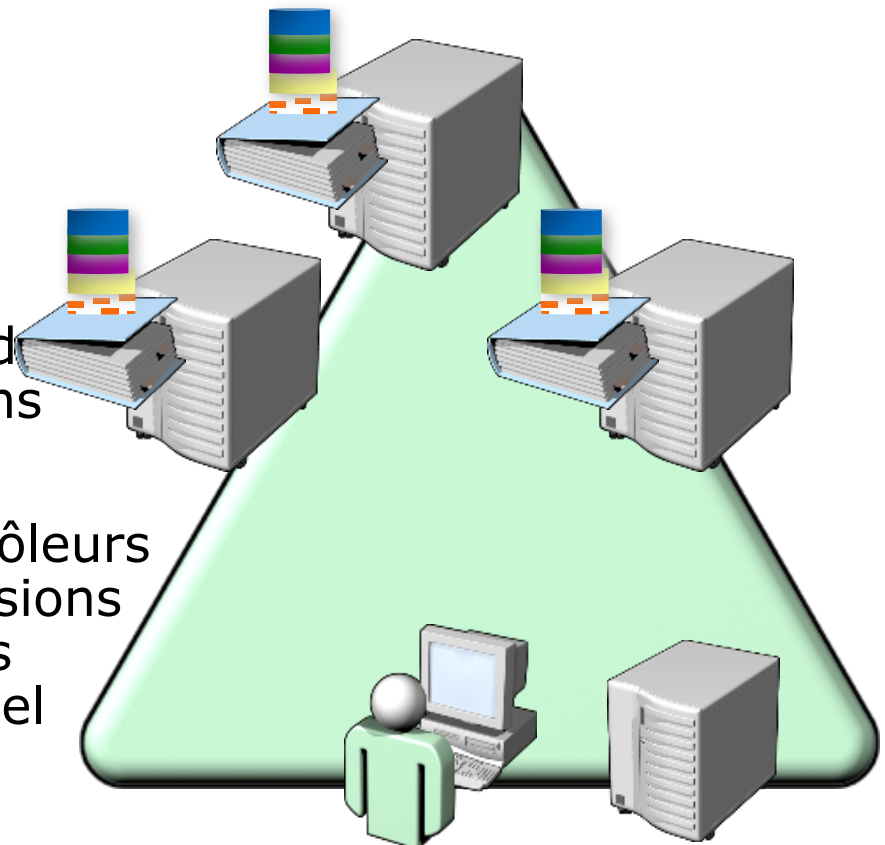
Catalogue global

- Jeu d'attributs partiel (PAS) ou catalogue global
- Contient tous les objets dans chaque domaine de la forêt
- Contient uniquement les attributs sélectionnés
- Un type d'index
- Peut être consulté depuis tout domaine
- Très important pour de nombreuses applications



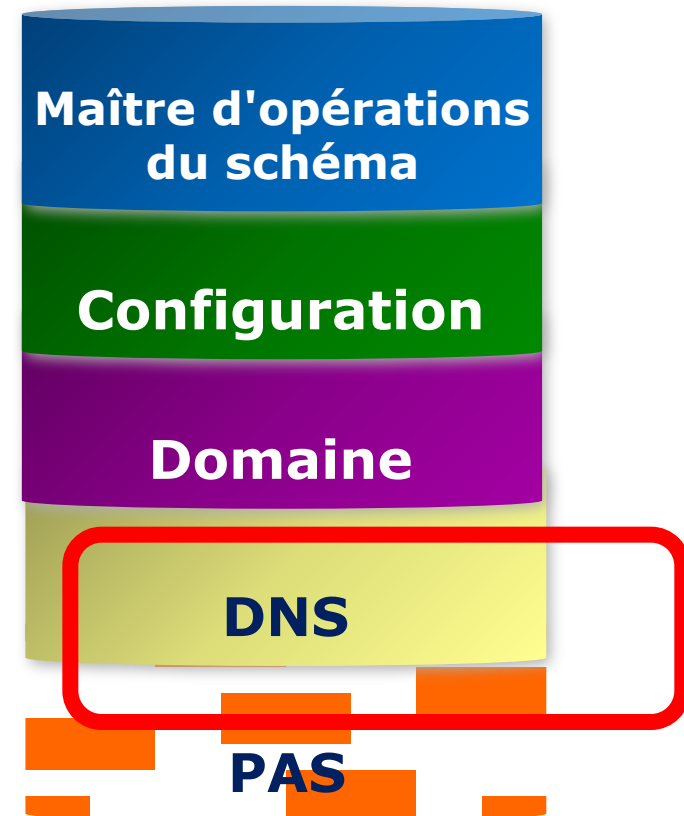
Niveau fonctionnel

- Niveaux fonctionnels de domaine
- Niveaux fonctionnels de forêt
- Nouvelle fonctionnalité qui nécessite que les *contrôleurs de domaine* exécutent une version particulière de Windows
 - Windows 2000
 - Windows Server 2003
 - Windows Server 2022
- Impossible d'élever le niveau fonctionnel si des contrôleurs de domaine exécutent des versions précédentes de Windows
- Impossible d'ajouter des contrôleurs de domaine exécutant des versions précédentes de Windows après avoir élevé le niveau fonctionnel



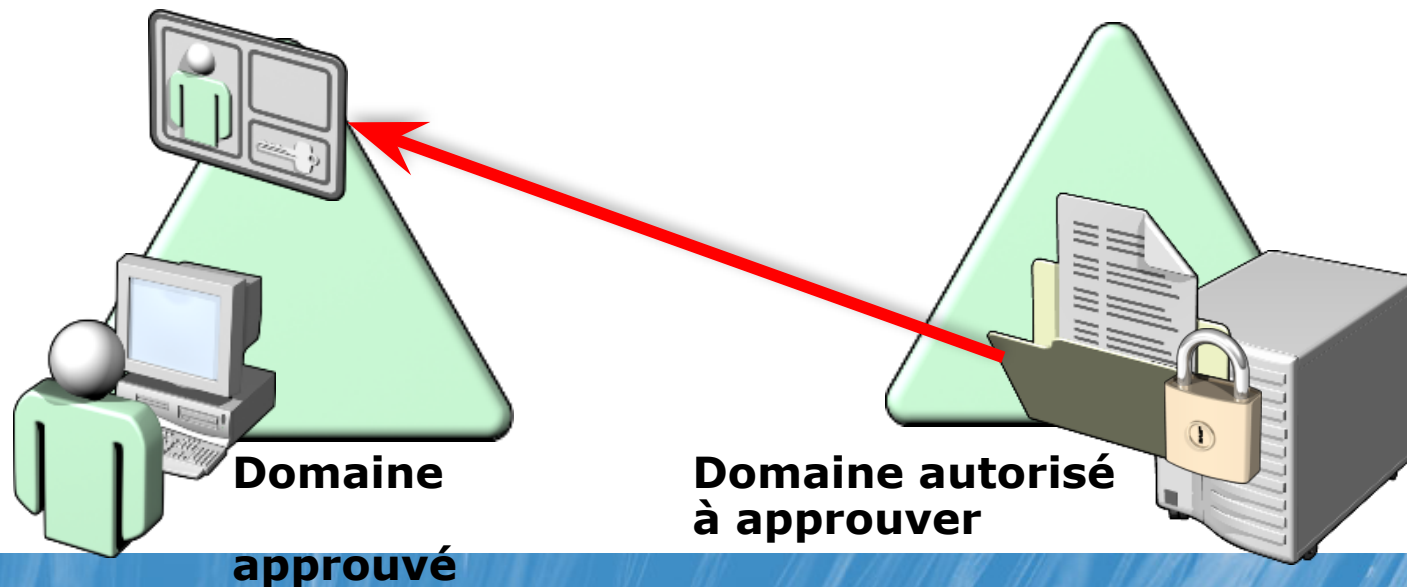
Partitions d'applications et DNS

- Active Directory et DNS sont étroitement intégrés.
- Relation un à un entre le nom de domaine DNS et l'unité de domaine logique d'Active Directory
- Dépendance totale vis-à-vis du DNS pour localiser les ordinateurs et les services dans le domaine
- Un contrôleur de domaine agissant comme serveur DNS peut stocker les données de la zone dans Active Directory même, dans une *partition d'applications*.



Relations d'approbation

- Étend le concept de magasin d'identités approuvées à un autre domaine
- Le domaine d'approbation (avec les ressources) approuve les services de magasin d'identités et d'authentification du domaine approuvé.
- Un utilisateur approuvé peut s'authentifier auprès du domaine autorisé à approuver et accéder à ses ressources.
- Dans une forêt, chaque domaine approuve tous les autres domaines.
- Il est possible d'établir des relations d'approbation avec des domaines externes.

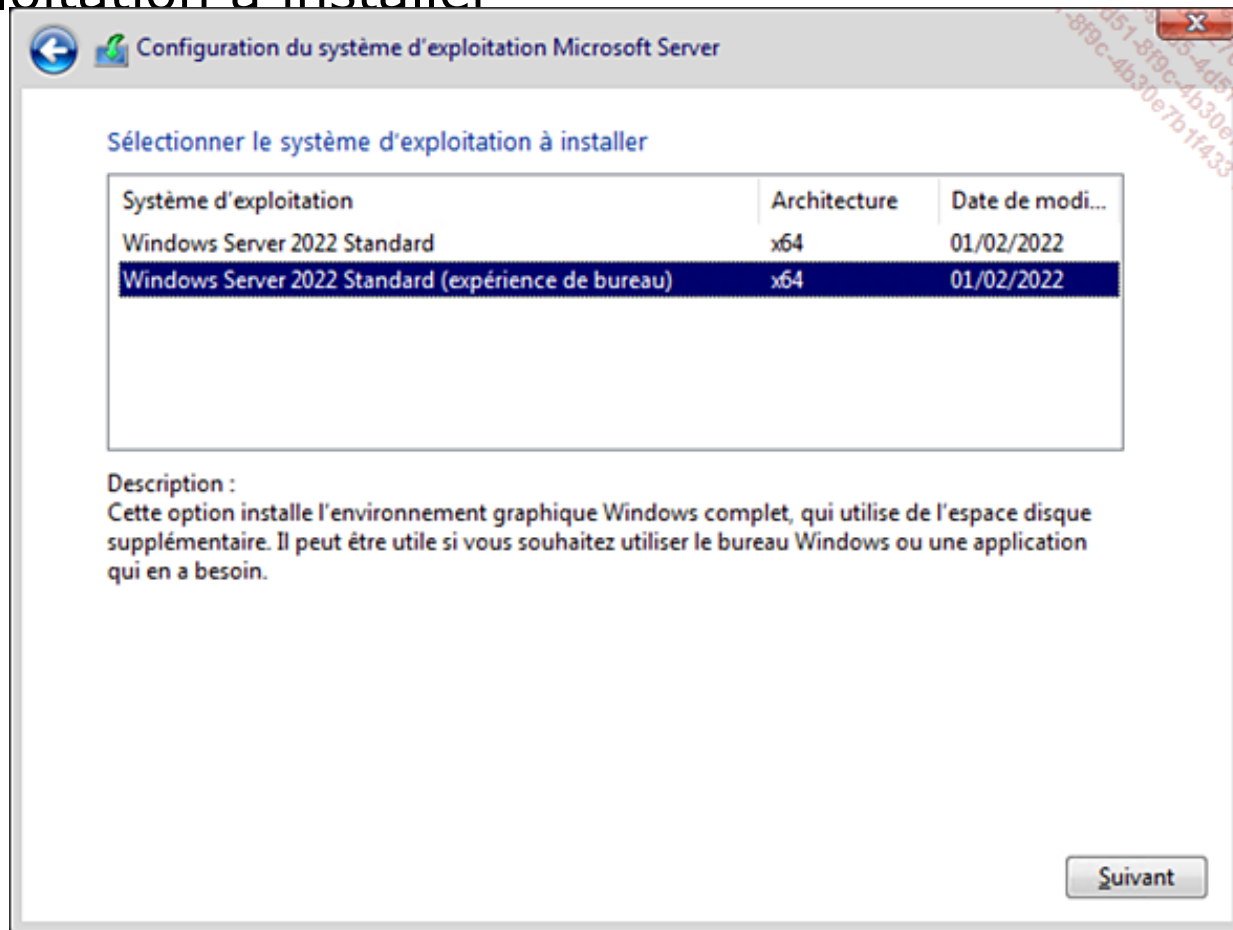


Leçon 3 : Installer les Services de domaine Active Directory

- Installation de Windows Server 2022
- Gestionnaire de serveur et configuration à base de rôles de Windows Server 2022
- Préparation de la création d'une nouvelle forêt avec Windows Server 2022
- Installation et configuration d'un contrôleur de domaine

Installation de Windows Server 2022

- Démarrer avec le support d'installation (DVD)
- Suivre les instructions et sélectionner le système d'exploitation à installer



Gestionnaire de serveur et configuration à base de rôles Windows Server 2022

- Windows Server® 2022 est d'un encombrement minimal.
- Les fonctionnalités sont ajoutées en tant que *rôles* ou *fonctions*.
- Gestionnaire de serveur : configuration des rôles et des fonctions, et des composants logiciels enfichables administratifs courants pour le serveur

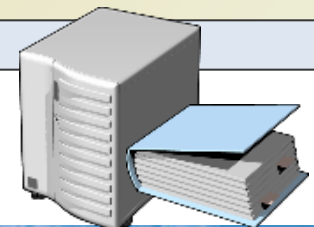


Préparation de la création d'une nouvelle forêt avec Windows Server 2022

- Nom DNS du domaine (contoso.com)
- Nom NetBIOS du domaine (contoso)
- Savoir si la nouvelle forêt devra prendre en charge des contrôleurs de domaine exécutant des versions précédentes de Windows (impact sur le choix du niveau fonctionnel)
- Des détails sur la manière dont DNS sera implémenté pour prendre AD DS en charge
 - Par défaut : la création d'un contrôleur de domaine ajoute aussi le rôle de serveur DNS
- Configuration IP pour le contrôleur de domaine
 - IPv4 et, éventuellement, IPv6
- Le nom d'utilisateur et le mot de passe d'un compte dans le groupe Administrateurs du serveur. Le compte doit avoir un mot de passe.
- Emplacement pour la banque de données (ntds.dit) et SYSVOL
 - Par défaut : %racinesystème% (c:\windows)

Installation et configuration d'un contrôleur de domaine

- 1** Installation du rôle Services de domaine Active Directory à l'aide du Gestionnaire de serveur
- 2** Exécution de l'Assistant Installation des Services de domaine Active Directory
- 3** Choix de la configuration de déploiement
- 4** Sélection des fonctionnalités supplémentaires du contrôleur de domaine
- 5** Sélection de l'emplacement de la base de données, des fichiers journaux et du dossier SYSVOL
- 6** Configuration du mot de passe de l'administrateur du mode de restauration des services d'annuaire



Atelier pratique A : Installation d'un contrôleur de domaine AD DS pour créer une forêt à un seul domaine

- Exercice 1 : Exécution des tâches de configuration après l'installation
- Exercice 2 : Installation d'une nouvelle forêt Windows Server 2022 à l'aide de l'interface Windows

Informations de connexion

Ordinateur virtuel	6238B-HQDC01-D
Nom d'ouverture de session utilisateur	Administrateur
Mot de passe	Pa\$\$w0rd

Durée approximative : 15 minutes

Scénario de l'atelier pratique

- Vous avez été embauché afin d'améliorer la gestion des identités et des accès chez Contoso, Ltd. La société dispose actuellement d'un serveur dans une configuration de groupe de travail. Les employés se connectent au serveur à partir de leurs ordinateurs clients personnels. En prévision d'une croissance à court terme, vous avez été chargé d'améliorer la facilité de gestion et la sécurité des ressources de l'entreprise. Vous décidez d'implémenter une forêt et un domaine AD DS en affectant au serveur le rôle de contrôleur de domaine. Vous venez d'achever l'installation de Windows Server 2022 à partir du DVD d'installation.

Récapitulatif

Au terme de cet atelier pratique, vous aurez :

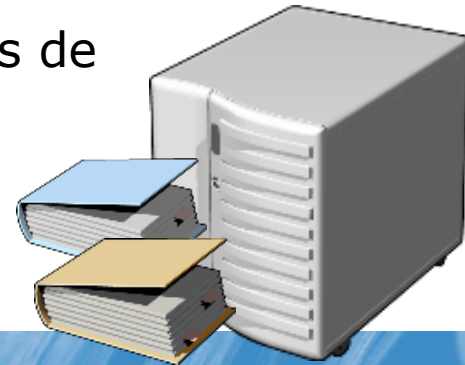
- effectué des tâches post-installation en nommant un serveur HQDC01, en configurant le fuseau horaire correct, avec une résolution d'affichage d'au moins 1024 x 768 pixels et en définissant les informations relatives à son adresse IP ;
- configuré une forêt à un domaine nommée contoso.com avec un contrôleur de domaine unique nommé HQDC01.

Leçon 4 : Étendre IDA avec des services Active Directory

- Services AD LDS (Active Directory Lightweight Directory Services)
- Services de certificats Active Directory (AD CS)
- Services AD RMS (Active Directory Rights Management Services)
- Services ADFS (Active Directory Federation Services)

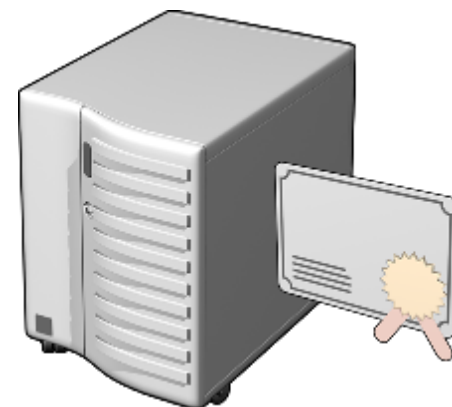
Services AD LDS (Active Directory Lightweight Directory Services)

- Version autonome d'Active Directory
 - Utilisée pour prendre en charge des applications qui nécessitent un magasin d'annuaires
 - Permet de personnaliser sans impact sur Active Directory en production
- Caractéristiques
 - Un sous-ensemble des fonctionnalités AD DS, qui partagent le même code
 - Partitions de schéma, de configuration et d'applications
 - Réplication
 - Indépendant d'AD DS
 - Peuvent utiliser AD DS pour authentifier des entités de sécurité Windows
 - Peuvent exécuter plusieurs instances sur un seul serveur

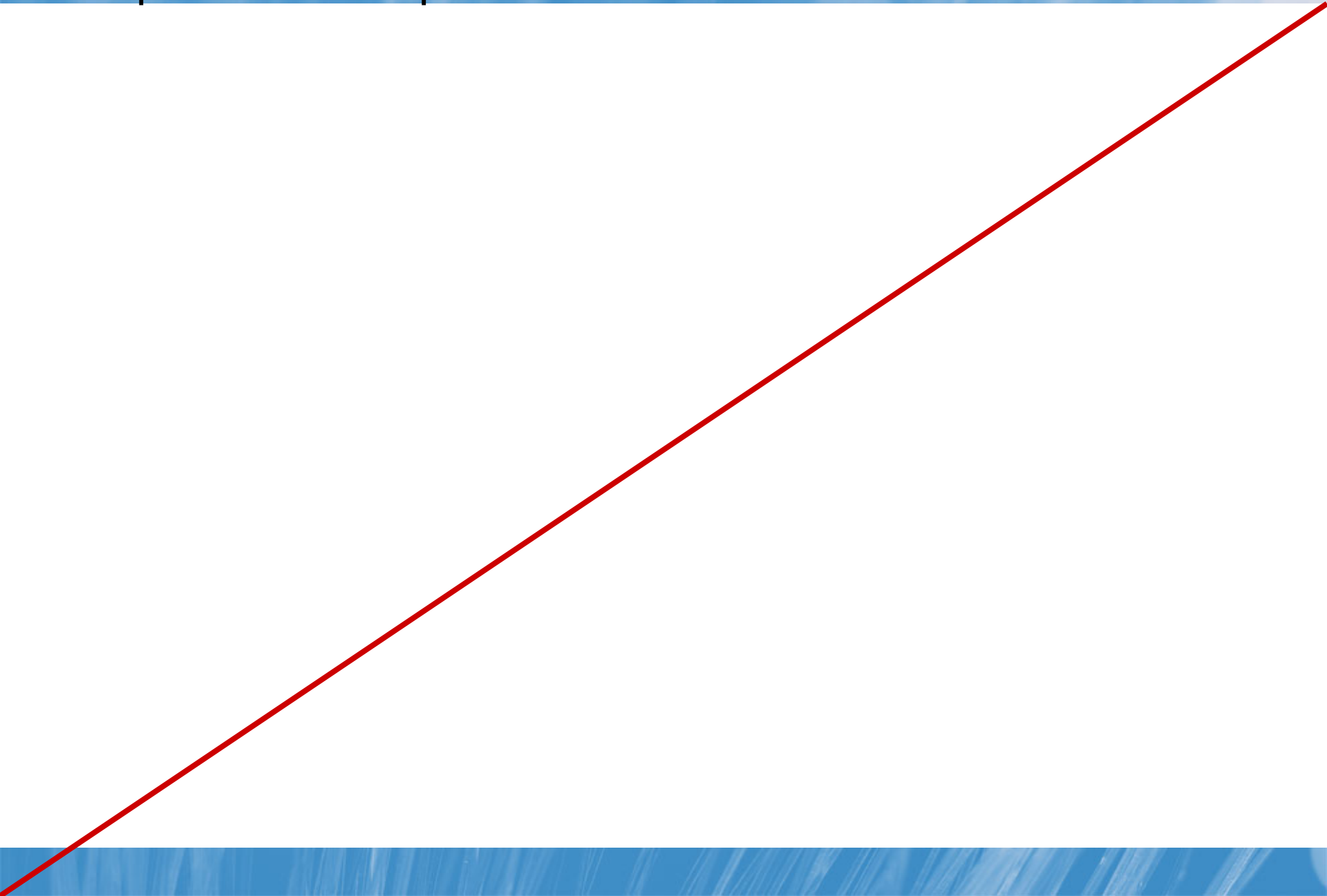


Services de certificats Active Directory (AD CS)

- Étendent le concept d'approbation
 - Un certificat émanant d'une autorité de certification (CA) approuvée garantit l'identité.
 - L'approbation peut être étendue au-delà des limites de votre entreprise, tant que les clients approuvent l'autorité de certification des certificats que vous présentez.
- Créent une infrastructure à clé publique (PKI)
 - Confidentialité, intégrité, authenticité, non-répudiation
- *De nombreuses utilisations*
 - Internes seulement, ou externes
 - Sites Web sécurisés (SSL)
 - Réseau privé virtuel (VPN)
 - Chiffrement et authentification sans fil
 - Authentification par carte à puce
- L'intégration à AD DS est puissante, mais pas obligatoire.



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



Services AD RMS (Active Directory Rights Management Services)

- Vérifie l'intégrité des informations
 - Modèle traditionnel : une ACL détermine l'accès. Aucune restriction d'*utilisation*.
 - AD RMS : s'assure que l'accès est limité et définit l'utilisation.
- Exemples
 - Limiter l'accès à certaines personnes
 - Afficher les e-mails, mais pas les transférer ni les imprimer
 - Afficher et imprimer des documents, mais pas les modifier ou les envoyer par e-mail
- Requiert :
 - AD RMS
 - IIS, base de données (SQL Server ou base de données interne de Windows)
 - AD DS
 - Applications compatibles RMS, dont Microsoft Office, Internet Explorer



Services ADFS (Active Directory Federation Services)

- Étend l'autorité d'AD DS pour authentifier les utilisateurs
- « Approbation » traditionnelle
 - Deux domaines Windows
 - De nombreux ports TCP ouverts dans les pare-feux
 - « Toute personne » du domaine approuvé est approuvée
- AD FS utilise les technologies des services Web pour implémenter l'approbation
 - Un annuaire AD DS/LDS ; de l'autre côté, il peut y avoir Active Directory ou d'autres plateformes.
 - Port 443 : les transactions sont sécurisées et chiffrées.
 - Des règles déterminent quels utilisateurs du domaine approuvé sont approuvés.
- Utilisations
 - B2B : partenariat
 - Authentification unique

