MICROSOFT OFFICIAL COURSE

Chapitre 1 : Exploration des rôles Active Directory Windows Server 2008

Vue d'ensemble du module

- Vue d'ensemble des services de domaine Active Directory
- Vue d'ensemble des services AD LDS (Active Directory Lightweight Directory Services)
- Vue d'ensemble des services de certificats Active Directory
- Vue d'ensemble des services AD RMS (Active Directory Rights Management Services)
- Vue d'ensemble des services ADFS (Active Directory Federation Services)

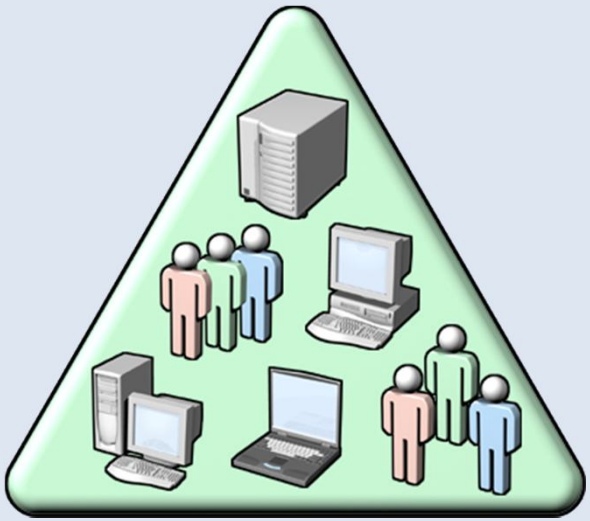
Leçon 1 : Vue d'ensemble des services de domaine Active Directory

- Qu'est-ce qu'un service d'annuaire ?
- Que sont les services AD DS ?
- Comment fonctionne AD DS ?
- Intégration des services de domaine Active Directory avec d'autres rôles serveur Active Directory

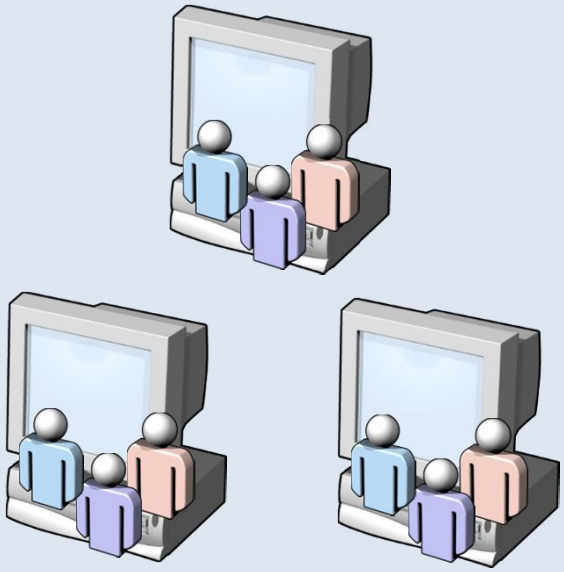
Qu'est-ce qu'un service d'annuaire ?

Un service d'annuaire est à la fois la source d'informations d'annuaire et le service qui rend ces informations disponibles et utilisables

Administration centralisée



Administration dispersée

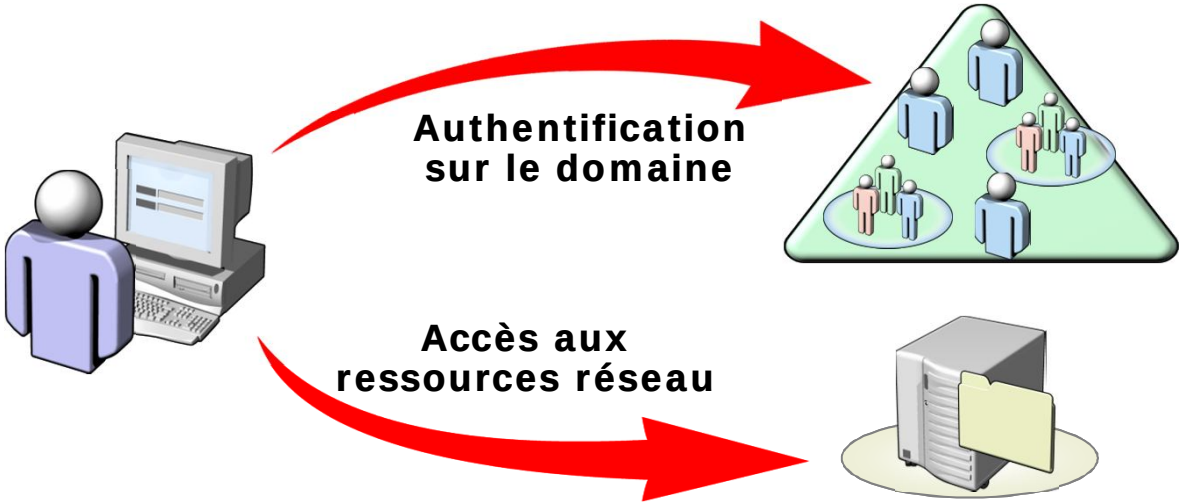


Que sont les services AD DS ?

AD DS est un service d'annuaire qui fournit les services suivants dans un réseau Windows Server 2008 :

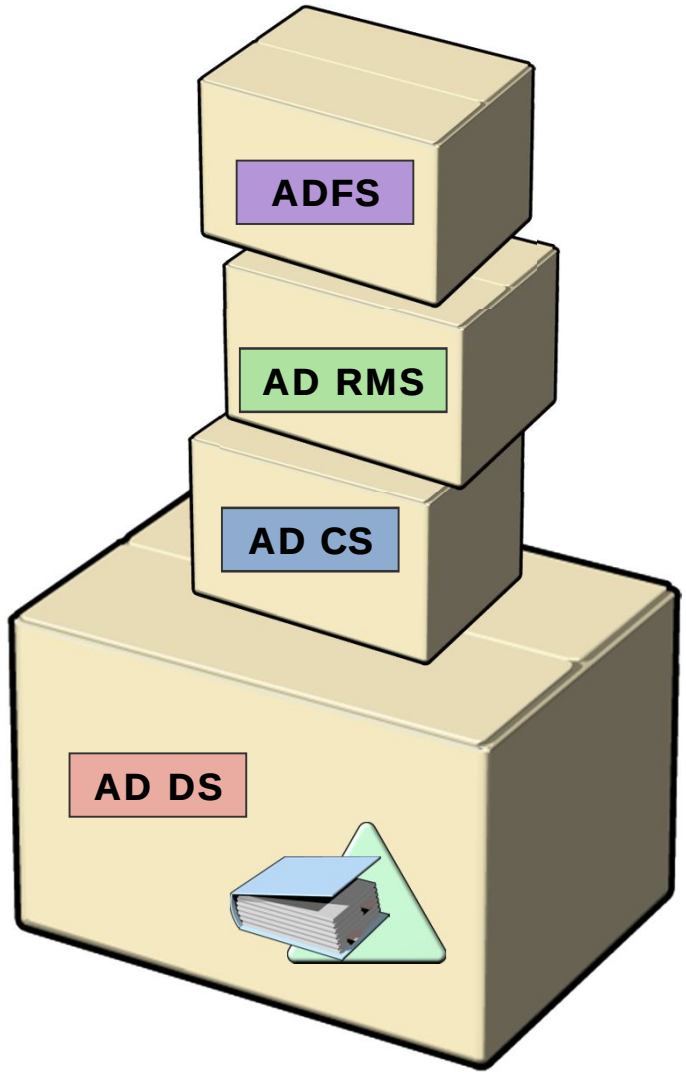
- **Gestion des comptes d'utilisateurs**
- **Authentification utilisateur**
- **Gestion des comptes d'ordinateur**
- **Accès aux ressources réseau**
- **Services de domaine**

Comment fonctionne AD DS ?



1. Les objets utilisateur et ordinateur sont créés dans l'annuaire
2. Ces objets peuvent ensuite être regroupés
3. Un client peut utiliser le compte d'utilisateur pour l'authentification AD DS
4. L'utilisateur peut essayer d'accéder aux ressources réseau
5. Les ressources valideront de nouveau l'utilisateur authentifié avec AD DS

Intégration des services de domaine Active Directory avec d'autres rôles serveur Active Directory



- **AD DS est la base d'un réseau fonctionnel**
- **La plupart des rôles serveur dépendent d'AD DS pour fournir les informations sur les utilisateurs et les ressources aux autres rôles serveur**
- **AD DS fournit également les services d'authentification et d'autorisation**

Leçon 2 : Vue d'ensemble des services AD LDS (Active Directory Lightweight Directory Services)

- Qu'est-ce que LDAP ?
- Qu'est-ce qu'AD LDS ?
- Exemples d'implémentation AD LDS

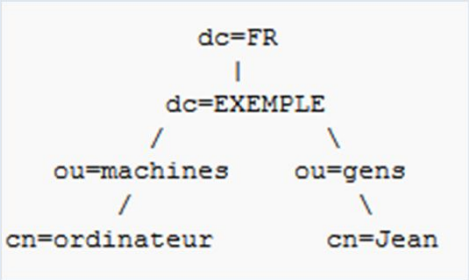
Qu'est-ce que LDAP ?

Le protocole LDAP est :

- **Un protocole de service d'annuaire**
- **Basé sur TCP / IP**
- **Une méthode pour accéder, rechercher, et modifier un service d'annuaire**
- **Un modèle client / serveur**
- **Un annuaire LDAP respecte généralement le modèle X.500 : c'est une structure arborescente dont chacun des nœuds est constitué d'attributs associés à leurs valeurs.**

Qu'est-ce que LDAP ?

Le protocole LDAP :

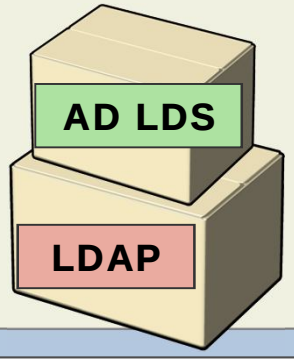



```
cn=ordinateur,ou=machines,dc=EXEMPLE,dc=FR
cn=Jean,ou=gens,dc=EXEMPLE,dc=FR
```

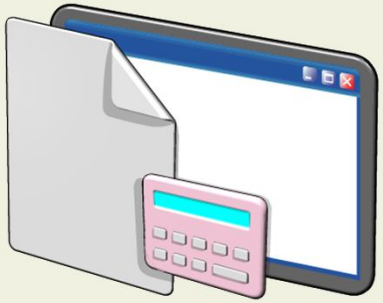
Nom	Exemple
Nom unique relatif LDAP	OU=MonUnitéOrganisation
Nom unique LDAP	OU=MonUnitéOrganisation, DC=microsoft, DC=com
Nom complet	Microsoft.com/MonUnitéOrganisation

Qu'est-ce qu'AD LDS ?

Un service d'annuaire LDAP



Utilisé pour les applications

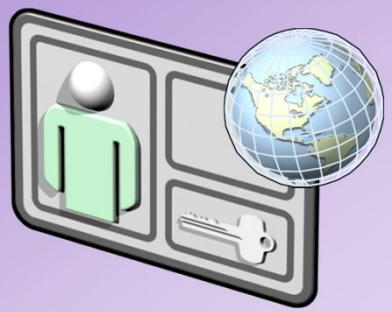


Plus flexible qu'AD DS

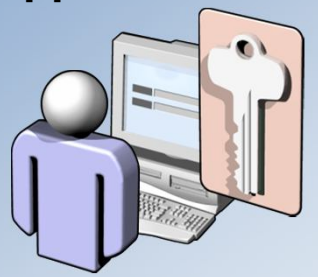
- Plusieurs instances AD LDS peuvent s'exécuter sur un ordinateur
- Ne nécessite pas une infrastructure DNS
- Peut être modifié pour répondre à des besoins d'application spécifiques

Exemples d'implémentation AD LDS

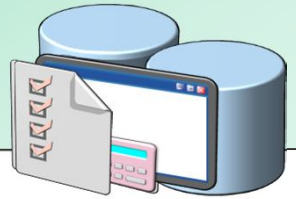
- **Authentification Web**



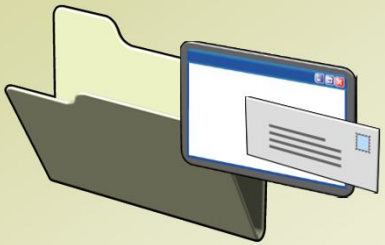
- **Ouverture de session plus sécurisée pour les applications**



- **Stockage de la configuration de l'application qui est située dans un réseau de périmètre et ne peut pas ou ne doit pas accéder à AD DS**



- **Annuaire pour les applications de messagerie**



Leçon 3 : Vue d'ensemble des services de certificats Active Directory

- Discussion : À quoi servent les certificats numériques ?
- Qu'est-ce qu'une infrastructure à clé publique ?
- Qu'est-ce qu'AD CS ?
- Exemples d'implémentation AD CS
- Comment fonctionne AD CS ?
- Intégration d'AD DS et d'AD CS

Discussion : À quoi servent les certificats numériques ?

- Comment les certificats numériques sont-ils utilisés pour fournir le chiffrement ?
- Comment les certificats numériques sont-ils utilisés pour fournir l'authentification ?
- Quelles applications prennent en charge l'utilisation de certificats ?

Qu'est-ce qu'une infrastructure à clé publique ?

Une infrastructure à clé publique est utilisée pour distribuer et gérer les certificats numériques

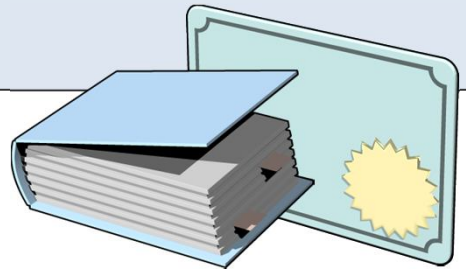
Une infrastructure à clé publique comprend les composants suivants :

- **Autorités de certification**
- **Listes de révocation de certificats**
- **Outils de gestion de l'autorité de certification**
- **Certificats**

Qu'est-ce qu'AD CS ?

AD CS :

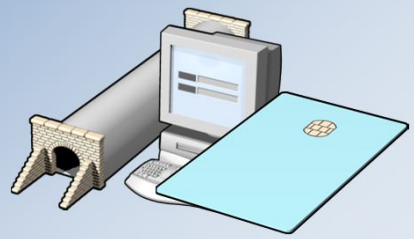
- **Fournit l'autorité de certification**
- **Fournit des outils automatisés et manuels pour la création, la distribution et la révocation de certificats**
- **Fournit des services de révocation de certificat**
- **Intègre les services d'autorité de certification à AD DS**



Exemples d'implémentation AD CS

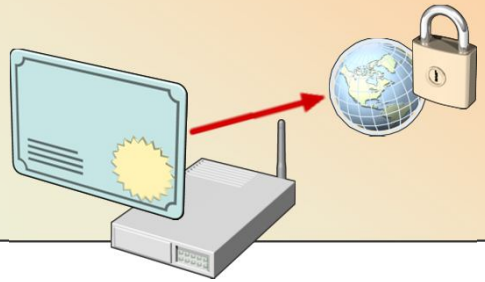
- **Sécurité SSL pour des sites Web internes**

- **Ouverture de session par carte à puce pour des ordinateurs clients et des réseaux VPN**

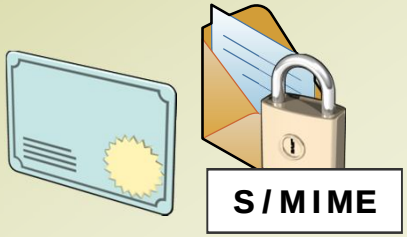


- **Certificats pour les services de fichiers chiffrés**

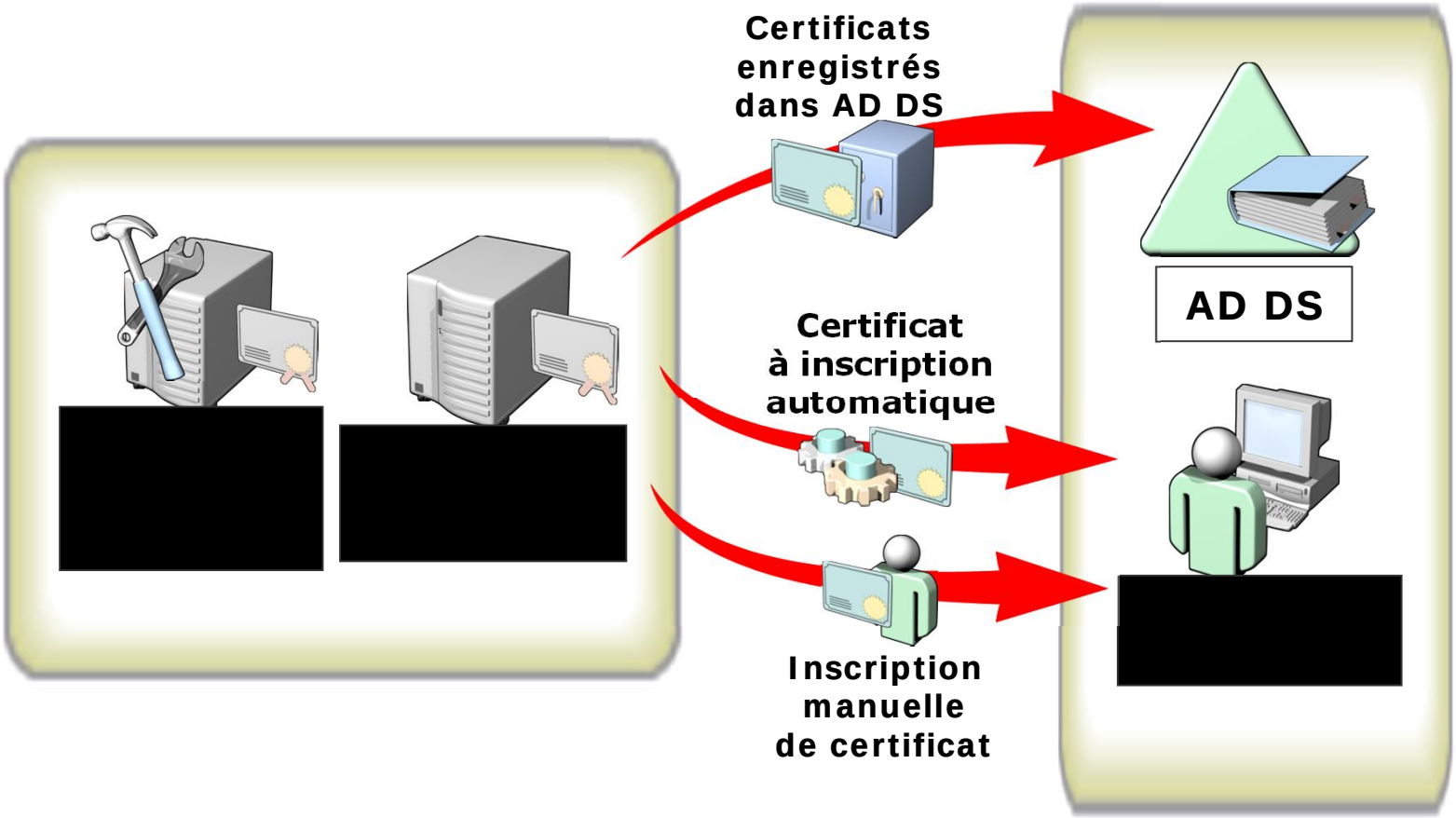
- **Certificats pour les routeurs afin d'établir des communications IPsec**



- **Certificats pour la messagerie S/MIME chiffrée et authentifiée**



Comment fonctionne AD CS ?



Intégration d'AD DS et d'AD CS

AD DS et AD CS sont étroitement intégrés de la façon suivante :

- **Les certificats pour les objets utilisateur et ordinateur peuvent être générés automatiquement**
- **Les certificats pour les objets utilisateur et ordinateur peuvent être stockés dans AD DS**
- **Les stratégies pour accorder et révoquer des certificats, et configurer des certificats de confiance, peuvent être gérées via les paramètres de stratégie de groupe**

Leçon 4 : Vue d'ensemble des services AD RMS (Active Directory Rights Management Services)

- Qu'est-ce qu'une solution ERM (Enterprise Rights Management) ?
- Qu'est-ce qu'AD RMS ?
- Exemples d'implémentation AD RMS
- Intégration d'AD DS et d'AD RMS

Qu'est-ce qu'une solution ERM (Enterprise Rights Management) ?

Une solution qui permet d'empêcher l'affichage, la modification ou l'utilisation non autorisés des informations stockées dans des documents, des messages électroniques et des sites Web

Fonctionnalités :

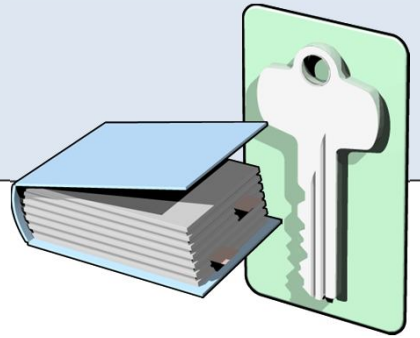
- **D'empêcher les utilisateurs non autorisés de partager ou d'accéder à des informations sensibles**
- **De protéger le contenu, notamment contre la falsification**
- **De contrôler l'expiration des données**

Qu'est-ce qu'AD RMS ?

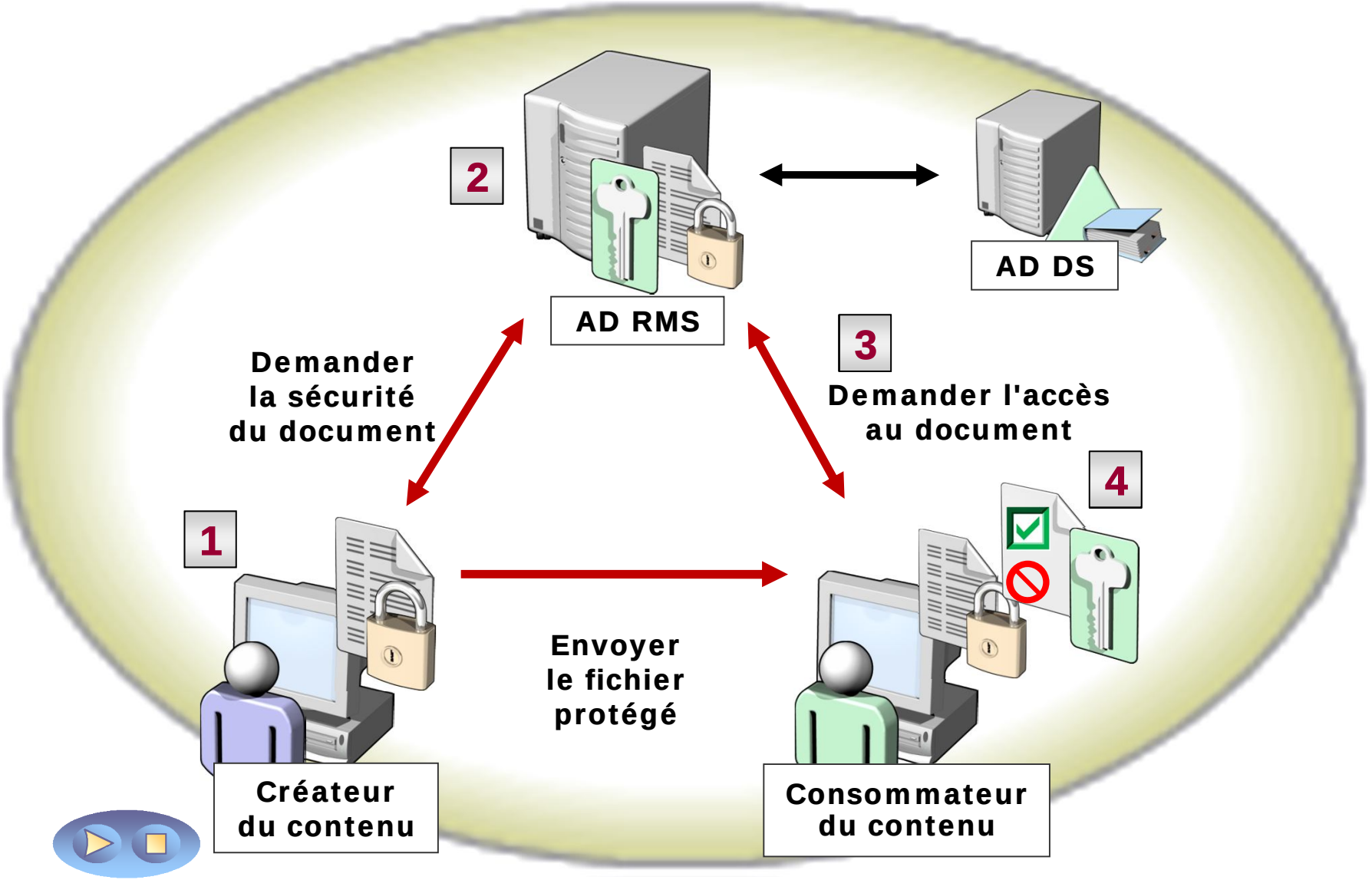
AD RMS (Active Directory Rights Management Services) est l'implémentation Windows Server 2008 d'une solution de gestion des droits d'entreprise

AD RMS :

- **Distribue les certificats clients, met en œuvre les stratégies d'accès au contenu et fournit une gestion centralisée**
- **Requiert l'utilisation d'applications RMS telles que Microsoft Office 2007 ou Internet Explorer® 7.0 et le client RMS**



Exemples d'implémentation AD RMS



Intégration d'AD DS et d'AD RMS

AD RMS est intégré à AD DS de la manière suivante :

- **Tous les utilisateurs AD RMS doivent disposer d'un compte AD DS**
- **AD DS fournit les adresses de messagerie requises pour AD RMS**
- **Les services AD RMS sont inscrits dans AD DS comme point de connexion de service**

Leçon 5 : Vue d'ensemble des services ADFS (Active Directory Federation Services)

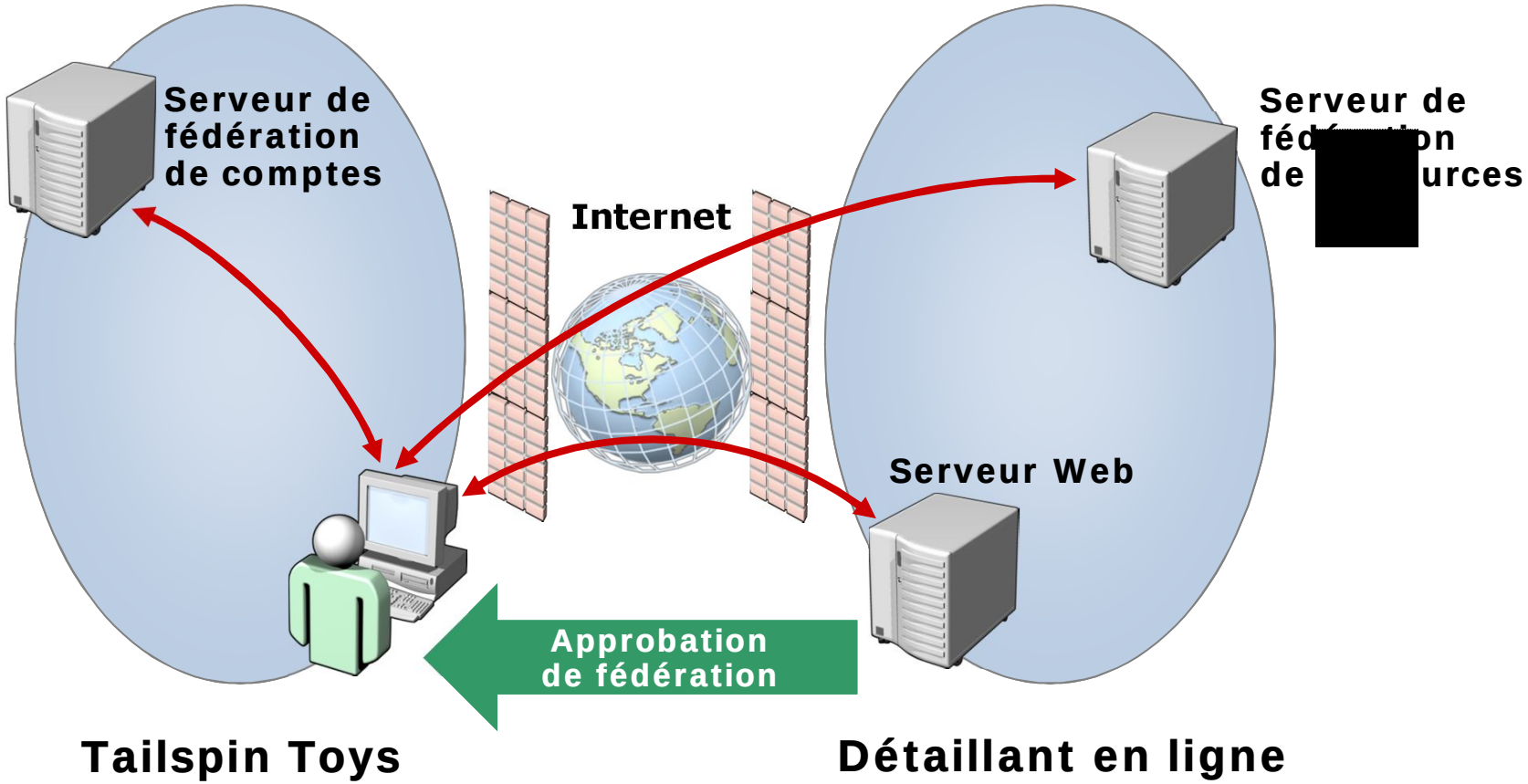
- Qu'est-ce qu'ADFS ?
- Flux du trafic ADFS dans un scénario de fédération B2B
- Comment fonctionne ADFS ?
- Intégration d'AD DS et d'ADFS
- Résumé des rôles serveur Active Directory

Qu'est-ce qu'ADFS ?

ADFS :

- **Permet la création de relations d'approbation entre deux organisations**
- **Fournit l'accès aux applications entre des organisations**
- **Fournit l'authentification unique (SSO) entre deux annuaires différents pour les applications Web**

Flux du trafic ADFS dans un scénario de fédération B2B



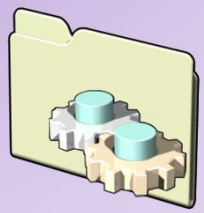
Comment fonctionne ADFS ?

1. Un ordinateur client se connecte à une application Web d'une autre organisation
2. L'application Web redirige la demande d'authentification vers le serveur ADFS
3. Le serveur ADFS du partenaire de ressource répond au client en demandant qu'il obtienne un jeton de sécurité du serveur ADFS dans l'organisation partenaire de compte
4. Le client demande le jeton de sécurité au serveur ADFS du partenaire de compte et repasse le jeton au serveur ADFS du partenaire de ressource
5. Le serveur ADFS de ressources crée un jeton de sécurité pour l'application Web
6. Le client peut désormais accéder à l'application Web

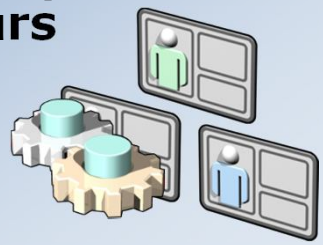
Intégration d'AD DS et d'ADFS

AD DS et ADFS sont intégrés de la façon suivante :

- **ADFS utilise AD DS et AD LDS pour fournir des services d'annuaire**

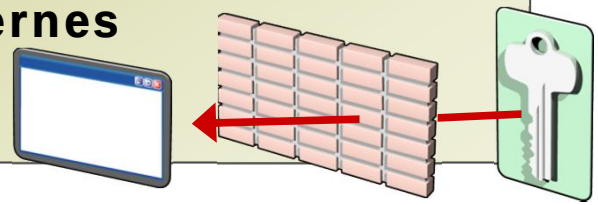


- **Les partenaires de compte ADFS utilisent AD DS pour gérer leurs propres comptes d'utilisateurs**



- **Les partenaires de ressource ADFS peuvent utiliser des comptes AD DS pour fournir l'accès aux applications**

- **ADFS permet aux organisations de fournir un accès externe aux applications pour des comptes AD DS internes**



Résumé des rôles serveur Active Directory

Rôle serveur	Description
Services de domaine Active Directory (AD DS)	Annuaire centralisé pour la gestion et l'authentification des utilisateurs et des ordinateurs sur un réseau Windows Server 2008
Services AD LDS (Active Directory Lightweight Directory Services)	Service d'annuaire LDAP qui fournit un support flexible pour les applications d'annuaire, sans les limitations d'AD DS
Services de certificats Active Directory (AD CS)	Solution utilisée pour empêcher l'affichage, la modification ou l'utilisation non autorisés des informations stockées dans des documents, des messages électroniques et des sites Web
Services AD RMS (Active Directory Rights Management Services)	Technologie de protection d'informations utilisée avec les applications AD RMS pour préserver les informations numériques contre toute utilisation non autorisée
Services ADFS (Active Directory Federation Services)	Rôle serveur dans Windows Server 2008 qui fournit des technologies SSO Web pour authentifier un utilisateur sur plusieurs applications Web pendant une session en ligne

Atelier pratique : Exploration des rôles serveur Active Directory Windows Server 2008

- Exercice 1 : Planification d'implémentations de rôles serveur Active Directory
- Exercice 2 : Présentation de l'intégration des rôles serveur Active Directory avec AD DS

Contrôle des acquis et éléments à retenir

Questions de contrôle des acquis

1. Il vous a été demandé de déployer une solution pour fournir une authentification à 2 facteurs pour les utilisateurs des stations de travail au sein de votre société. Citez deux rôles serveur Active Directory que vous devez déployer pour fournir une solution d'authentification à 2 facteurs gérée de façon centralisée ?

2. De quelle manière AD CS s'appuie-t-il sur AD DS ?

3. De quelles façons les certificats générés par AD CS peuvent-ils être utilisés pour le chiffrement ?

4. Pourquoi déployer AD LDS au lieu d'AD DS ?

5. Quelles sont les fonctions de base fournies par AD RMS ?