CONSTRUISONS ENSEMBLE
LA DÉFENSE DE DEMAIN

COURS
WINDOWS ET LA SÉCURITÉ

DGA

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

MINISTÈRE
DE LA DÉFENSE

INFRASTRUCTURE RÉSEAU

INFRASTRUCTURE RÉSEAU

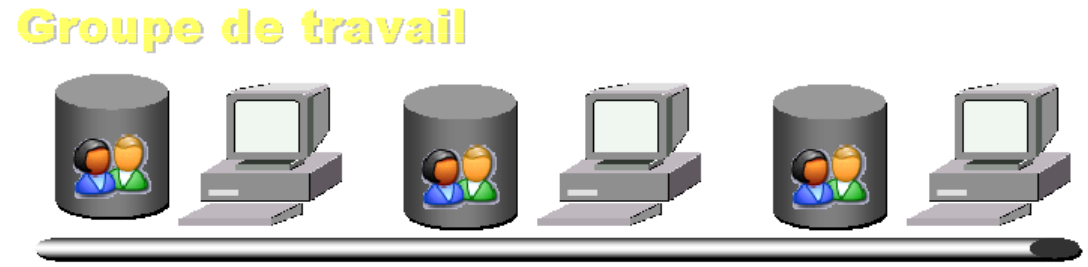
Le réseau

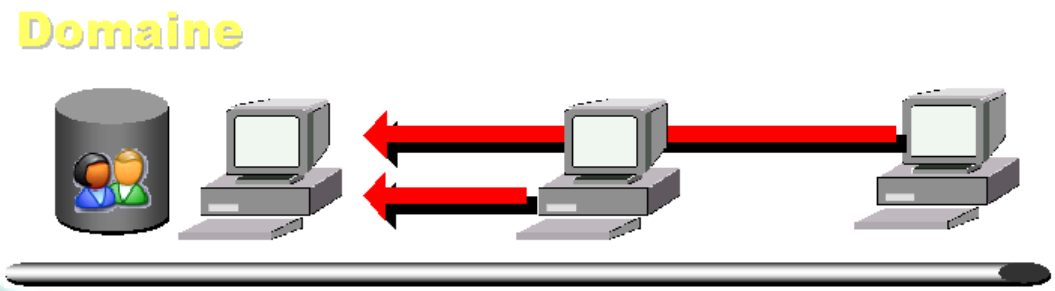
- Les fonctions de réseau sont apparues dès 1992 avec Windows 3.1 Workgroups
- Windows est capable de fonctionner de façon autonome ou intégrée à une infrastructure
- Les principaux services d'une infrastructure réseau sous Windows sont les suivants :
  - L'annuaire d'un domaine
  - L'authentification et la sécurité
  - Le partage de fichiers
  - L'exécution distante
  - La gestion d'une infrastructure

INFRASTRUCTURE RÉSEAU

Groupe de travail vs Domaine

- 2 scénarios sont possibles dans un réseau :
  - Chaque poste est autonome, il fait partie d'un groupe de travail dans lequel il peut échanger facilement
  - Les postes sont associés et dépendants d'un serveur de domaine





INFRASTRUCTURE RÉSEAU

Serveur de domaine

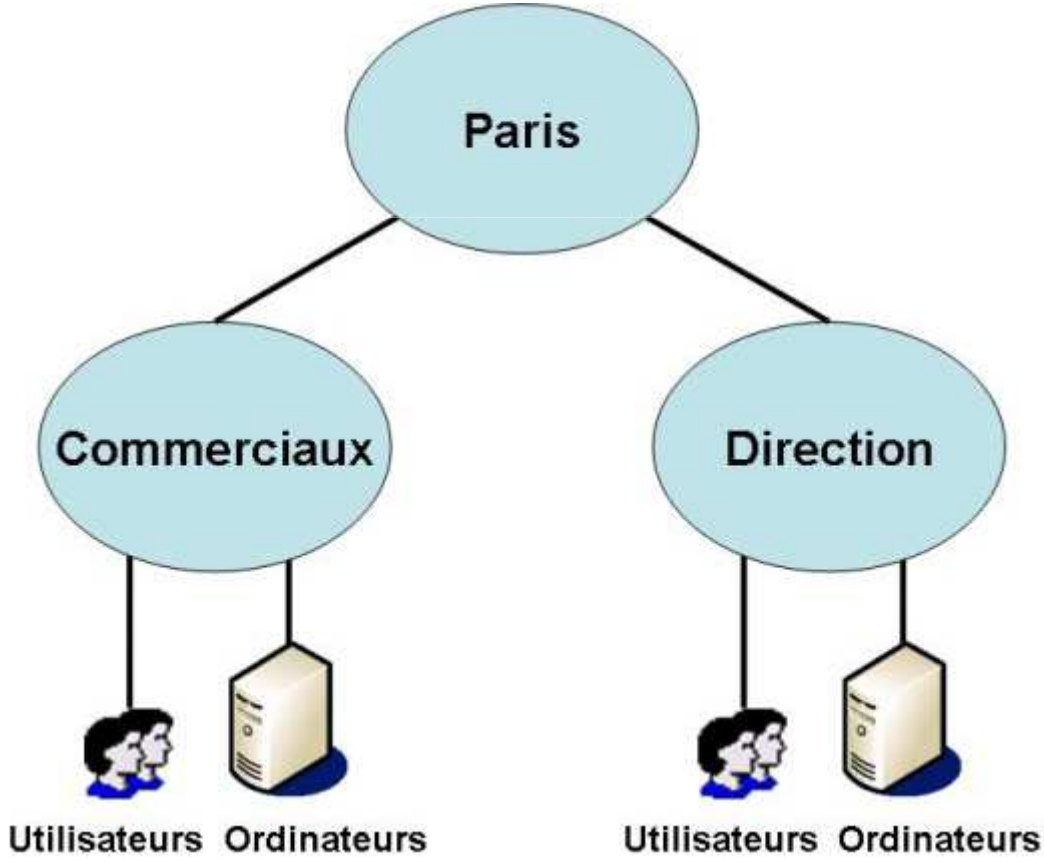
- Le serveur central qui gère un domaine est porté par un service AD (Active Directory)
- AD est un annuaire qui permet de stocker des informations relatives aux ressources réseau d'un domaine
- AD est équivalent à un serveur LDAP avec lequel il est capable de s'interfacer (pour synchroniser des comptes Linux par exemple)
- Le service AD n'est présent que sur les versions de Windows de type « Server » (2000, 2003, 2008, 2012)

INFRASTRUCTURE RÉSEAU
Active Directory

- Une structure AD est une organisation hiérarchisée d'objets classés en trois grandes catégories :
  - Les ressources : imprimantes, les postes, les serveurs, …
  - Les services : partage de fichiers, serveur de mails, …
  - Les utilisateurs : comptes utilisateurs et groupes
- La base SAM n'est plus utilisée pour la gestion des comptes utilisateurs d'un poste appartenant à un AD
- L'AD fournit des informations sur les objets, il les organise et contrôle les accès et la sécurité
- La structure logique de AD est composée de forêts, d'arbres, de domaines, d'unités d'organisation et d'objets

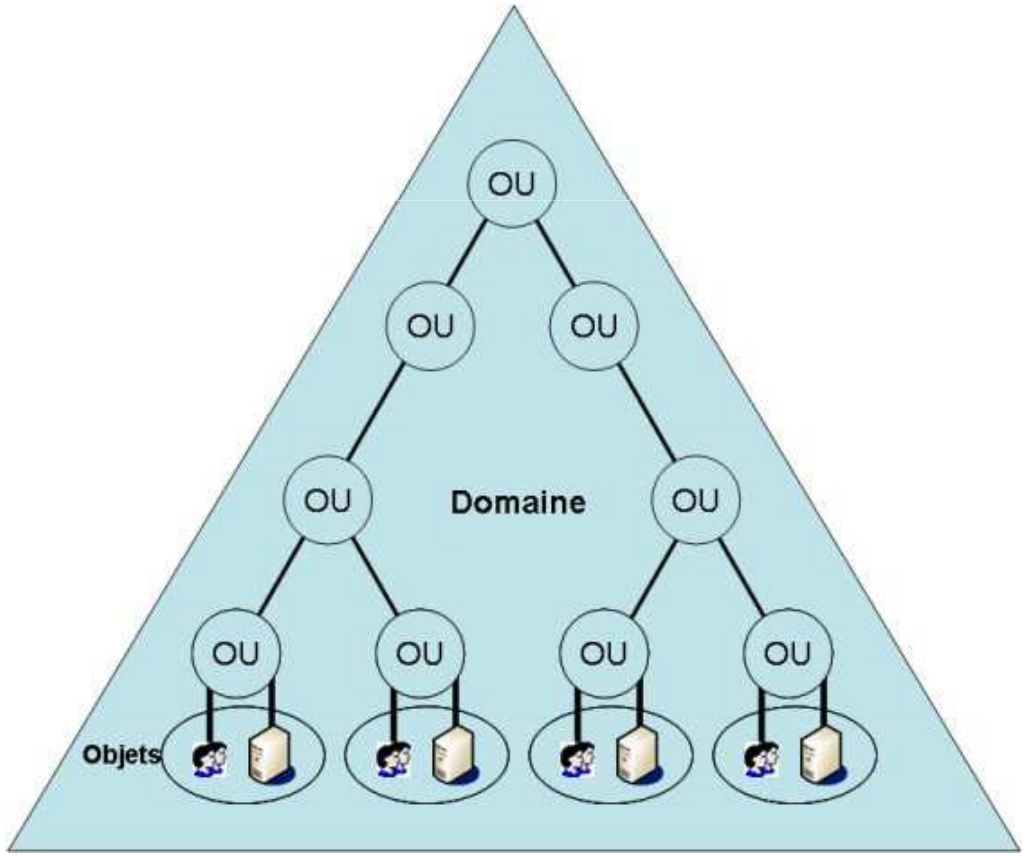
INFRASTRUCTURE RÉSEAU
Unités d'organisation

- Une Unité d'Organisation (OU) est un conteneur utilisé pour organiser les objets d'un domaine en groupes



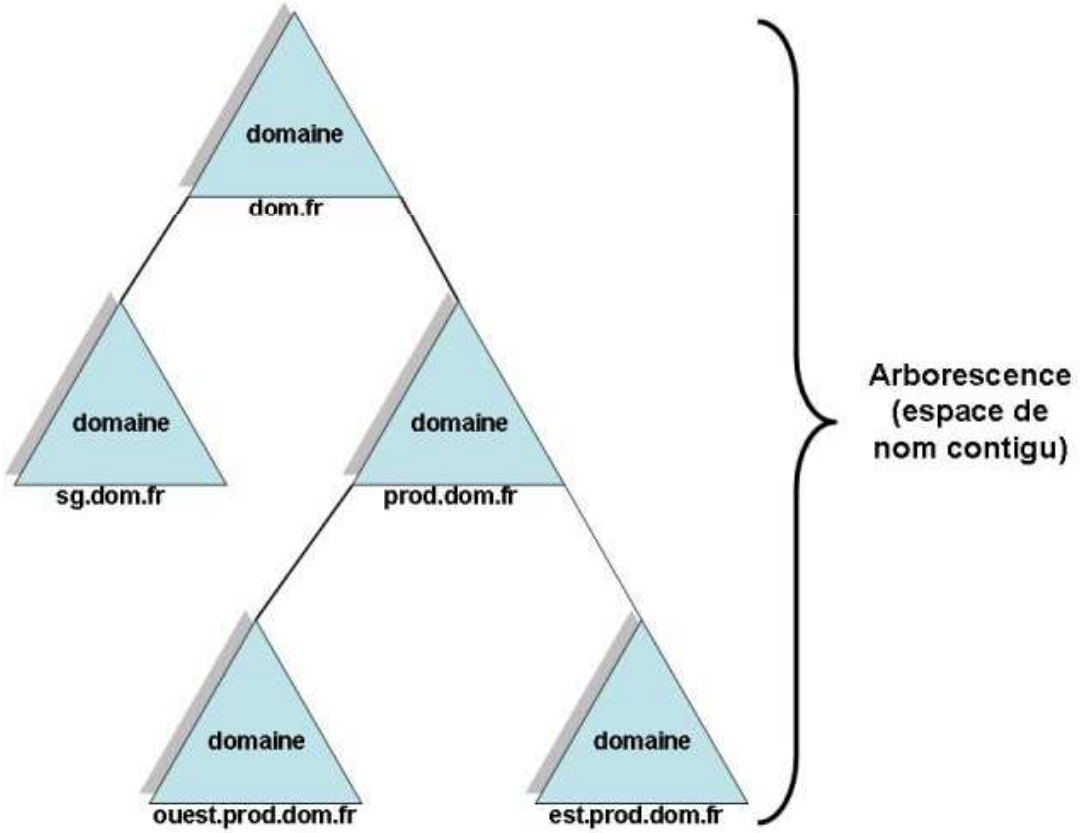
INFRASTRUCTURE RÉSEAU
Domaines

- Un domaine est un regroupement logique de plusieurs « OU » organisés de façon hiérarchique et d'objets



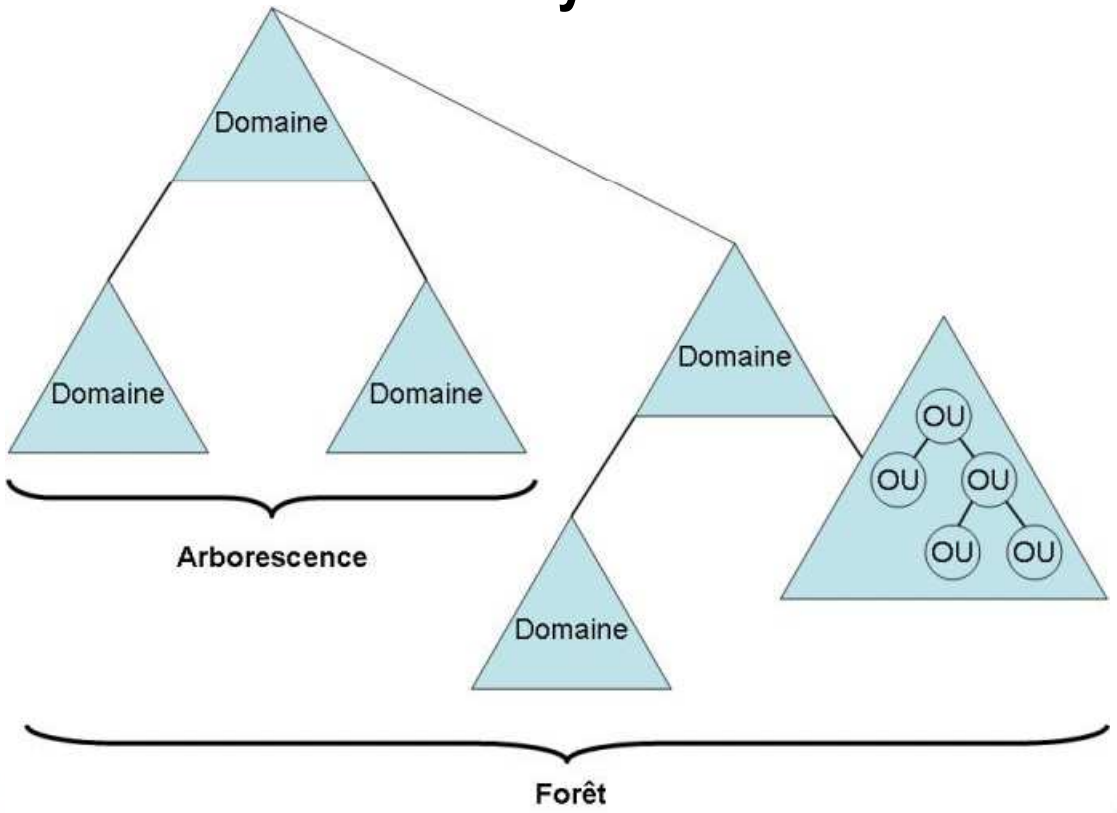
INFRASTRUCTURE RÉSEAU
Arbres

- Un arbre est un regroupement ou une organisation hiérarchisée d'un ou plusieurs domaines



INFRASTRUCTURE RÉSEAU
Forêts

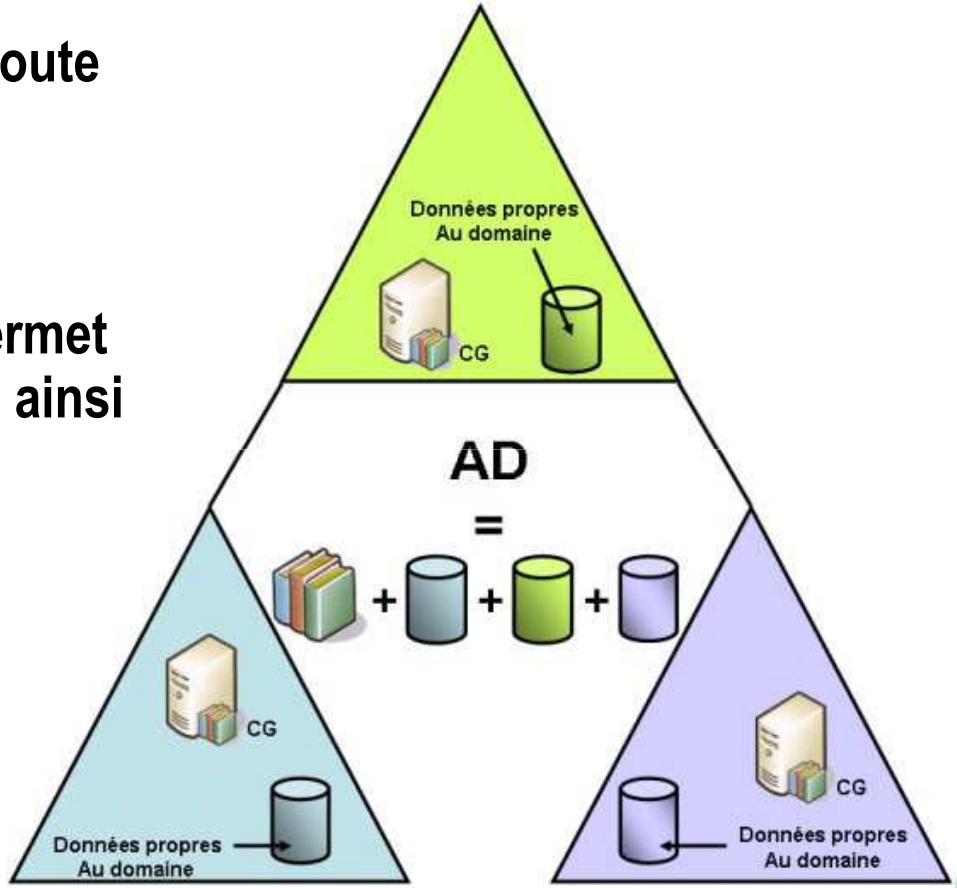
- Une forêt est un regroupement ou une organisation hiérarchisée d'un ou plusieurs arbres
- Une forêt = Un Active Directory



INFRASTRUCTURE RÉSEAU

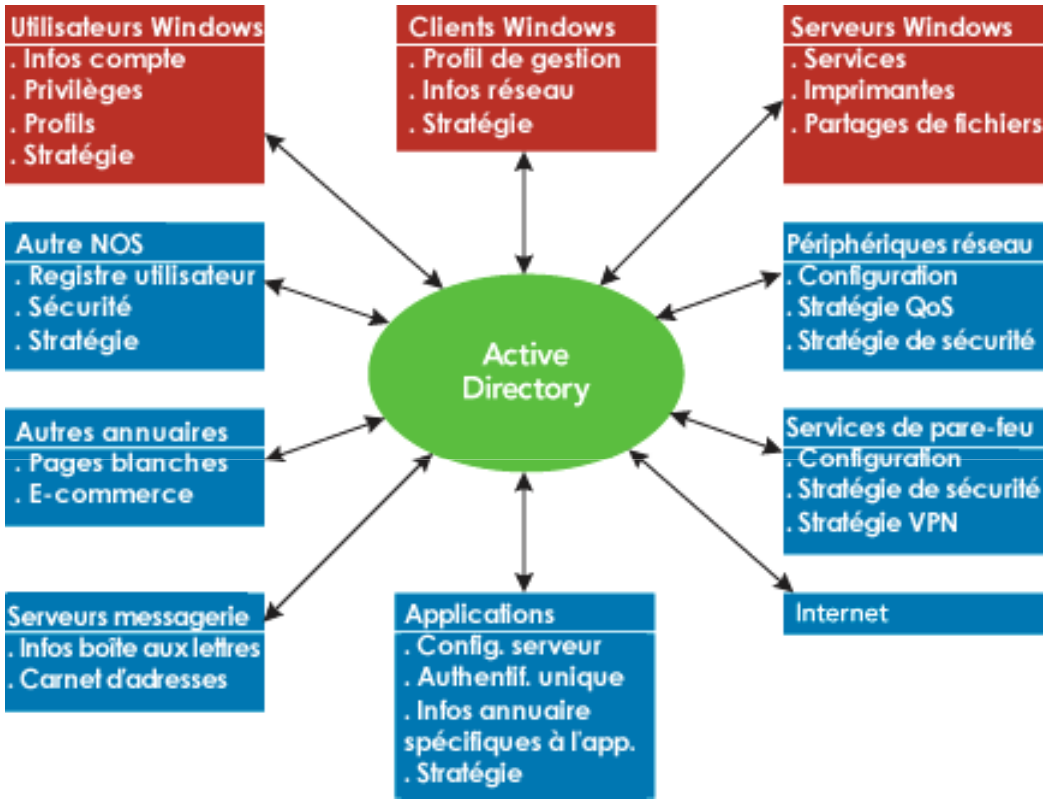
Réplication et catalogue global

- L'AD est partagé dans toute la forêt mais il demeure réparti : tout n'est pas répliqué
- Un Catalogue Global permet de référencer les objets ainsi que leur localisation



INFRASTRUCTURE RÉSEAU

Exemple d'objets stockés dans l'AD



- La clé de récupération de BitLocker est stockée dans AD

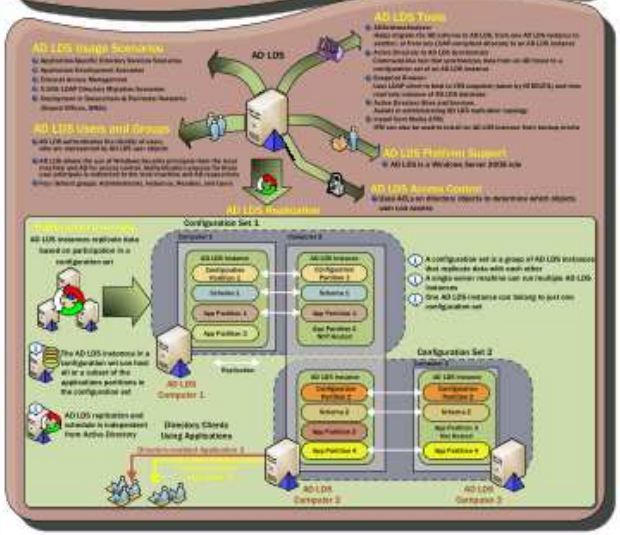
⇒Un attaquant ciblera le fichier NTDS.dit contenant l'AD

Active Directory Lightweight Directory Services

Windows Server 2008

Product Scenario: Enterprise and Branch Office

Active Directory Lightweight Directory Services (AD LDS) provides directory services for directory-enabled applications. AD LDS does not require or rely on Active Directory domains or forests. AD LDS was previously known as Active Directory Application Mode (ADAM).

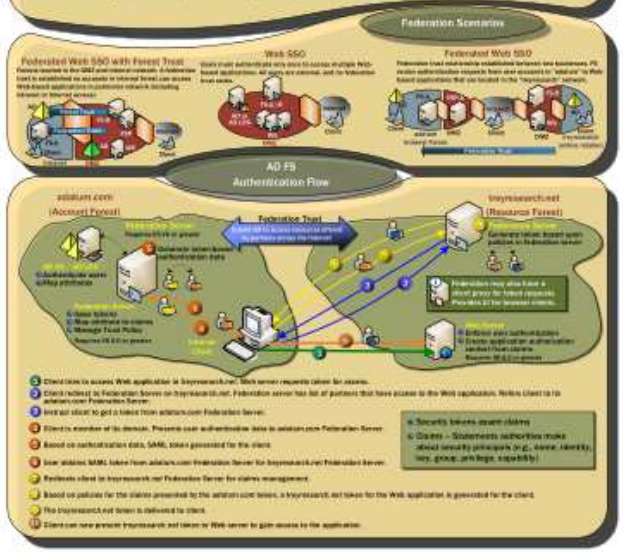


Active Directory Federation Services

Windows Server 2008

Product Scenario: Security and Policy Enforcement

Active Directory Federation Services (AD FS) provides Web single sign-on (SSO) technologies to authenticate a user to multiple Web applications over the life of a single online session. AD FS securely shares digital identity and entitlement rights, or "claims," across security and enterprise boundaries.

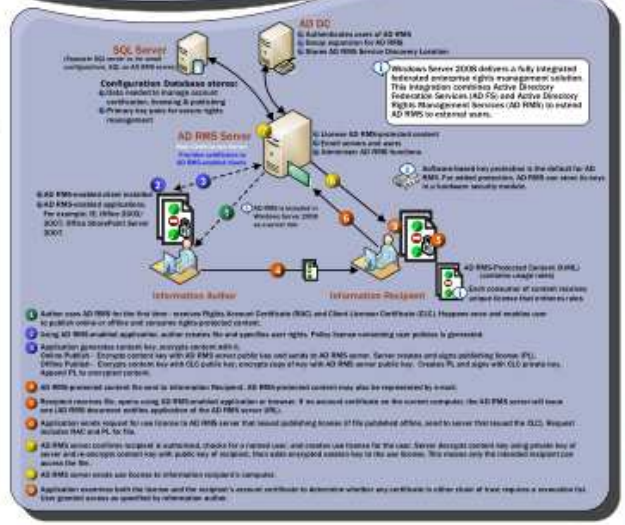


Active Directory Rights Management Services

Windows Server 2008

Product Scenario: Security and Policy Enforcement

Active Directory Rights Management Services (AD RMS) is information protection technology that works with AD RMS-enabled applications to safeguard digital information from unauthorized use – both online and offline – inside and outside of your organization's firewall.

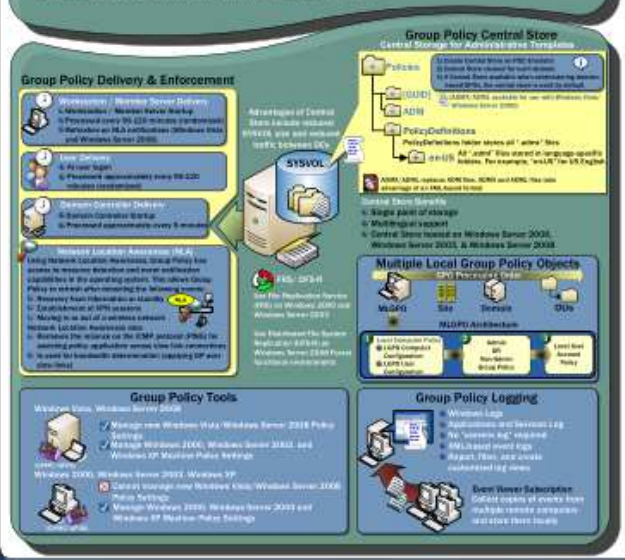


Group Policy

Windows Server 2008

Product Scenario: Server Management

Group Policy delivers and applies configuration or policy settings to targeted users and computers within an Active Directory environment. Windows Server 2008 supports a Central Store for centralized XML based template storage, advanced logging, and enhanced Group Policy delivery and enforcement using Network Location Awareness.

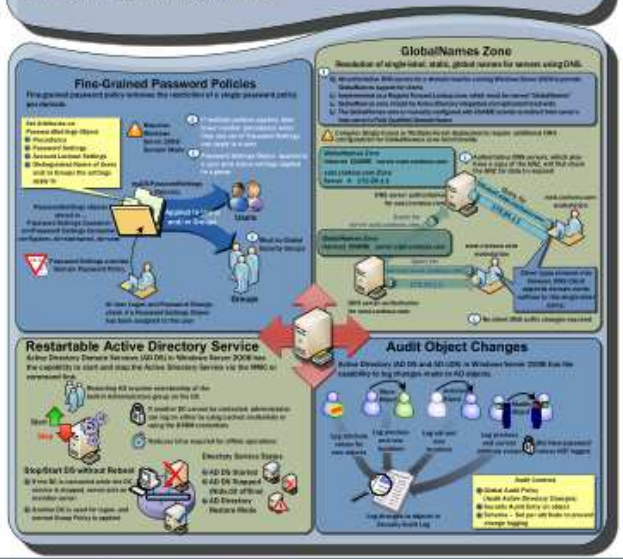


Active Directory Management

Windows Server 2008

Product Scenario: Server Management

Active Directory Domain Services (AD DS) expands auditing capabilities to track changes in the Active Directory objects. Windows Server 2008 has password policy that removes the restriction of a single password policy per domain. AD DS has the capability to stop and restart the Active Directory Service.

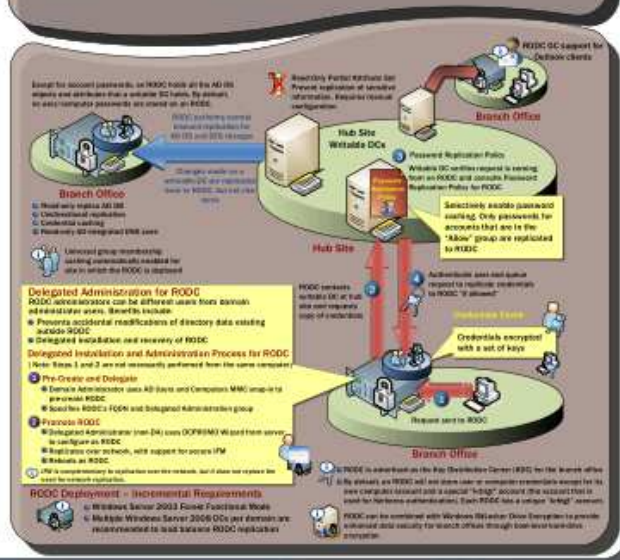


Active Directory Read-Only Domain Controller

Windows Server 2008

Product Scenario: Enterprise and Branch Office

A Read-Only Domain Controller (RODC) allows organizations to easily deploy a DC in locations where physical security cannot be guaranteed. RODC hosts a read-only replica of the database in Active Directory Domain Services (AD DS) for any given domain.



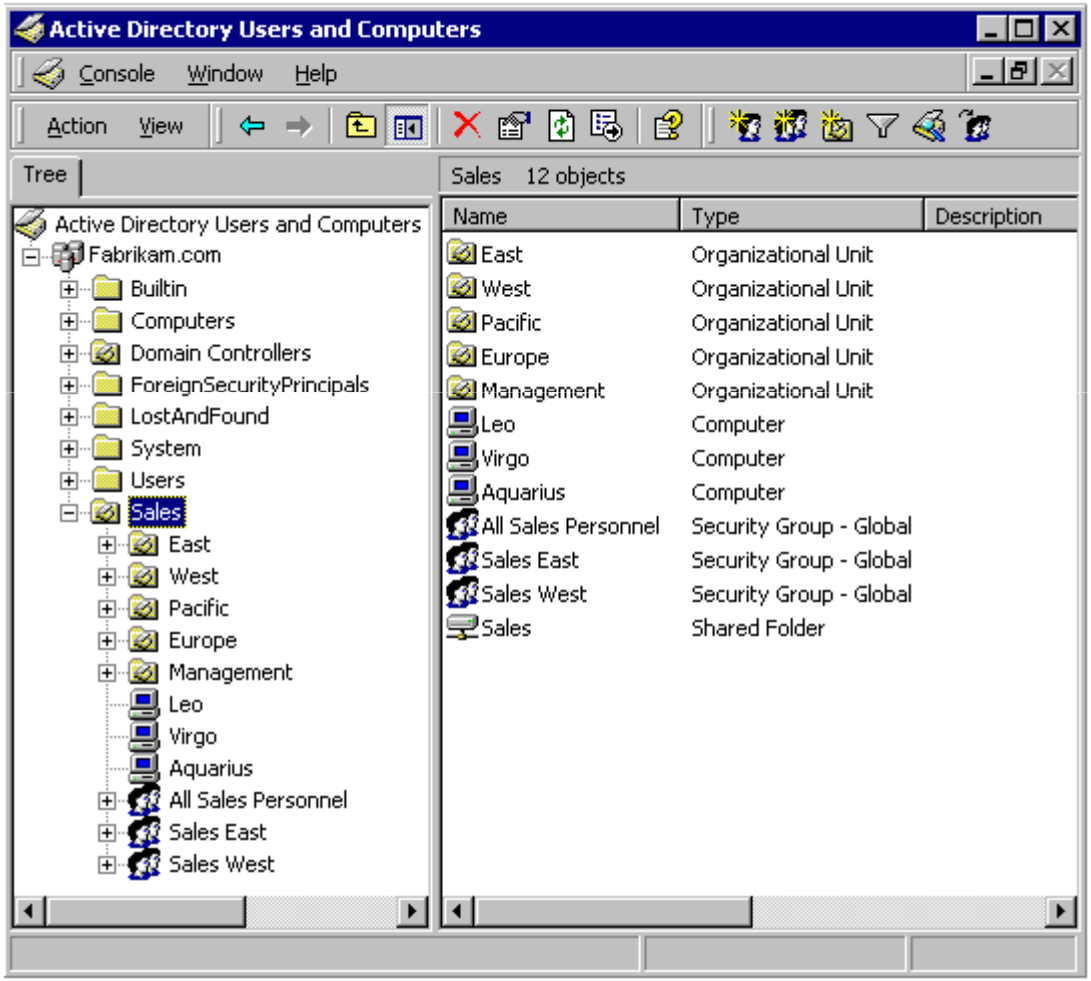
Windows Server 2008 Active Directory Feature Components

This poster is based on a prerelease version of Windows Server 2008. All information herein is subject to change.

Authors: Martin McClean & Astrid McC

INFRASTRUCTURE RÉSEAU

Exemple de vue de l'interface d'administration de AD



INFRASTRUCTURE RÉSEAU

Authentification dans un domaine AD

- AD sécurise les accès aux objets dans sa base de données, l'authentification des utilisateurs est réalisée par le protocole d'authentification Kerberos v5
- Kerberos est un mécanisme d'authentification mutuel entre clients et serveurs ; un client réalise une authentification sur un serveur Kerberos afin d'obtenir un jeton d'accès pour une ressource tierce. Ce jeton d'accès, à validité limitée dans le temps, sert alors de moyen d'authentification pour accéder à la ressource considérée

INFRASTRUCTURE RÉSEAU

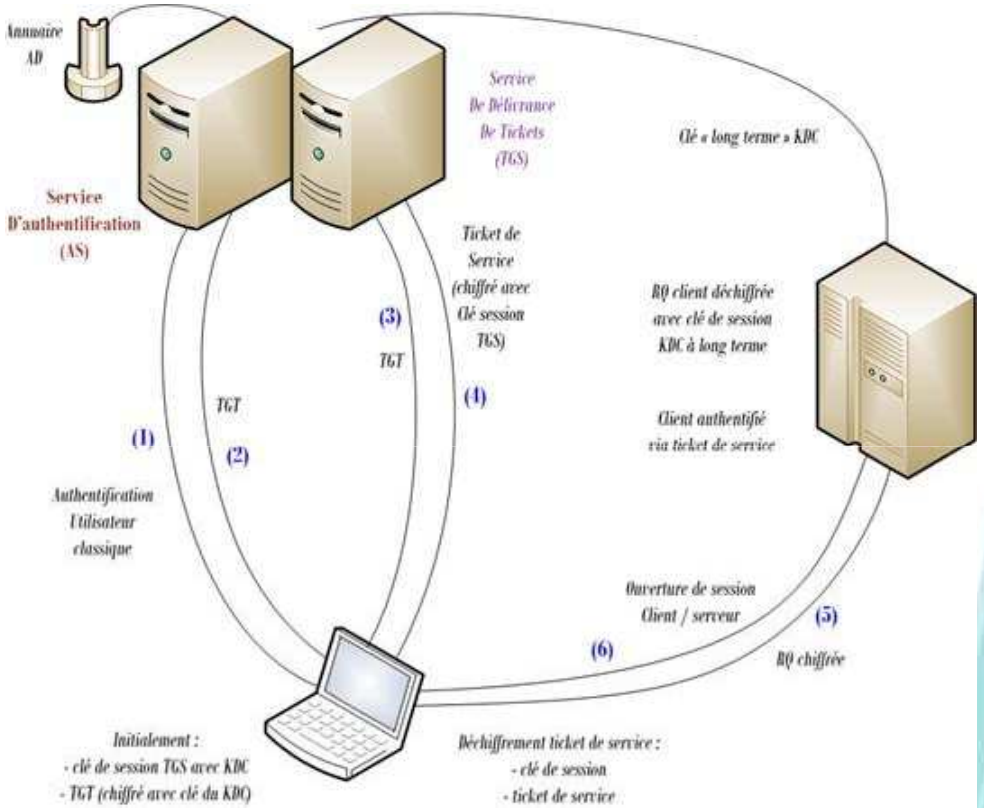
Architecture de Kerberos

- L'architecture de Kerberos est en 3 tiers :
  - un client
  - un serveur de ressources (par exemple une imprimante)
  - une autorité approuvée (KDC)
- L'autorité approuvée :
  - est un serveur dit « de confiance »,
  - reconnu comme tel par le client et le serveur
  - est présupposée parfaitement sécurisée

INFRASTRUCTURE RÉSEAU

Accès à une ressource par Kerberos

- 1 Auth. par mot de passe
- 2 TGT : Ticket Initial
- 3 Envoi du TGT
- 4 Ticket de service
- 5 Envoi clé de session dérivée du ticket de service
- 6 Accès à la ressource



INFRASTRUCTURE RÉSEAU

Partage de fichiers

- Depuis les débuts de Windows, le protocole de SMB (Server Message Block) fournit les fonctions de partage de fichiers et d'imprimantes sur un réseau
- Renommé de nombreuses fois : Lan Manager, CIFS, SMB
- La dernière version 3.02 de SMB est apparue avec Win8.1
- SMB fonctionne en mode client / serveur, il est orienté réseau local car très consommateur en bande passante
- Partage d'une ressource sécurisé par des ACLs

INFRASTRUCTURE RÉSEAU
SMB

- SMB est prévu pour être utilisé au dessus de l'interface NetBIOS
- Utilisation des noms NetBIOS (15 caractères + 1 pour le type)
- Resolution de nom :
  - Broadcast NetBIOS
  - Service Wins (Windows Internet Name Server)
  - DNS
- URI : \\serveur\ressource

<table>
<tr><td colspan="3">Application</td></tr>
<tr><td colspan="3">SMB</td></tr>
<tr><td colspan="3">NetBIOS</td></tr>
<tr><td>TCP/IP</td><td>NetBEUI</td><td>IPX/SPX</td></tr>
<tr><td>802.x</td><td>PPP</td><td>...</td></tr>
</table>

INFRASTRUCTURE RÉSEAU

Système de gestion de Windows

- WMI (Windows Management Instrumentation) est l'implémentation du WBEM (Web-Based Enterprise Management), le standard du DMTF (Distributed Management Task Force). Il prend en charge le modèle de données CIM (Common Information Model), qui décrit les objets d'un environnement de gestion
- WMI est une Framework qui permet aux administrateurs de gérer localement ou à distance les composants du systèmes et les applications
- Il faut les privilèges Administrateur pour utiliser WMI
- WMI est préinstallé depuis Windows Millenium

INFRASTRUCTURE RÉSEAU
WMI

- WMI utilise les technologies COM (Component Object Model) et DCOM (Distributed Component Object Model) qui permettent la programmation d'objets distribués sur la plate-forme Windows
- COM définit un format d'interfaces indépendant des langages utilisés et permet la communication entre applications Windows au niveau des objets
- COM est restreint aux communications inter-processus au sein d'une même machine tandis que DCOM est une extension de COM qui permet la communication entre objets situés sur des machines différentes

INFRASTRUCTURE RÉSEAU

Exemples d'usage de WMI

- Lister les applications installées sur un poste
- Installer une application sur l'ensemble d'un parc de machines dans un AD
- Modifier les paramètres de sécurité (DEP) d'un poste
- Redémarrage d'une machine distante
- Lancer une application à distance
- Effacer le journal d'évènements

⇒WMI fait partie du système Windows et fournit tous les outils pour un attaquant qui pourra agir discrètement

INFRASTRUCTURE RÉSEAU

Ce qu'il faut retenir pour la suite

- L'annuaire AD contient toutes les informations d'un réseau Windows
- Kerberos permet d'accéder aux différentes ressources d'un domaine sans se ré-authentifier à chaque fois
- SMB permet le partage des fichiers et des imprimantes localement
- WMI est un fantastique outil d'administration qui peut être dangereux dans de mauvaises mains