

DE LA RECHERCHE À L'INDUSTRIE



Active Directory

Sécurité Windows

Commissariat à l'Énergie Atomique
et aux Énergies Alternatives

13 janvier 2020

1 Introduction**2** Fonctionnement

- Stockage
- Structure logique
- GC et schéma
- Stratégies de groupe
- RéPLICATION

3 Sécurité

- Authentification
- Contrôle d'accès
- Architecture en silo
- Chemins de contrôle

4 Bonus

- WSUS

1 Introduction

2 Fonctionnement

3 Sécurité

4 Bonus

Active Directory

Il s'agit d'un annuaire qui :

- existe depuis **1999** (Windows 2000 Server) ;
- permet de **centraliser des informations** relatives aux utilisateurs et aux ressources d'une entreprise ;
- fournit des mécanismes d'**identification** et d'**authentification** ;
- permet de simplifier et **centraliser l'administration** ;
- **sécurise** l'accès aux données.

> Beaucoup d'évolutions depuis 1999, *Active Directory* est devenu complexe.

Active Directory est central en terme de sécurité :

- c'est une **cible privilégiée** pour un attaquant;
- la compromission d'un **seul compte** avec des droits privilégiés peut faire perdre la maîtrise de la totalité du système d'information.

C'est une technologie complexe :

- des nombreuses techniques de **persistence** existent et certaines sont **difficilement détectables** ;
- en cas de compromission, il peut être impossible de nettoyer un système, il faut alors le reconstruire totalement :
 - > **fort coût financier et humain**

Il est intéressant d'étudier *Active Directory* car c'est une technologie :

- utilisée dans (presque) **toutes les entreprises** ;
- **centrale** en terme de sécurité :
 - > un attaquant qui en prend le contrôle compromet tout le parc.

Connaître *Active Directory* est particulièrement utile pour :

- une équipe d'**audit de sécurité** ;
- une *blue team* ;
- un SIEM.

- Les fonctionnalités d'Active Directory sont regroupés dans *Active Directory Domain Services* (AD DS) :
- Un serveur avec AD DS est un *domain controller* (DC) ou **contrôleur de domaine** ;
- Il peut y avoir plusieurs DC par domaine.

Principaux rôles d'un DC

- Serveur DNS ;
- Annuaire LDAP ;
- Service d'authentification Kerberos ;
- Service de gestion de configuration (GPO).

- Les **machines membres** :

- appartiennent à un domaine ;
- possèdent une base locale de comptes (base SAM) ;
- possibilité d'ouverture de session de comptes locaux ou de domaine.

- Les **contrôleurs de domaine** (*domain controller, DC*) :

- contiennent une copie de la base de domaine (base NTDS) ;
- authentifient les machines et les utilisateurs du domaine.

1 Introduction

2 Fonctionnement

- Stockage
- Structure logique
- GC et schéma
- Stratégies de groupe
- RéPLICATION

3 Sécurité

4 Bonus

Les données d'*Active Directory* sont stockées dans une base de données :

- par défaut contenu dans **C:\Windows\NTDS.DIT** ;

- chemin configuré dans :

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\NTDS\Parameters

- utilise le moteur de base de données **ESE** (*Extensible Storage Engine*) de Microsoft ;
- cette base de données permet de stocker des informations sur les objets tels que :
 - les utilisateurs ;
 - les groupes ;
 - les ordinateurs ;
 - les domaines ;
 - les unités d'organisation ;
 - les stratégies de sécurité.
- on trouve les **empreintes des mots de passe** de tous utilisateurs du domaine (il s'agit donc d'une cible prioritaire en test d'intrusion).

- Un deuxième emplacement est utilisé par *Active Directory*,
C:\Windows\SYSTOL :
 - Contient les GPO et les scripts de connexion s'exécutant à l'ouverture de session des utilisateurs ;
 - Il ne s'agit pas d'une base de données mais d'une arborescence de fichiers ;
 - Accessible via SMB.

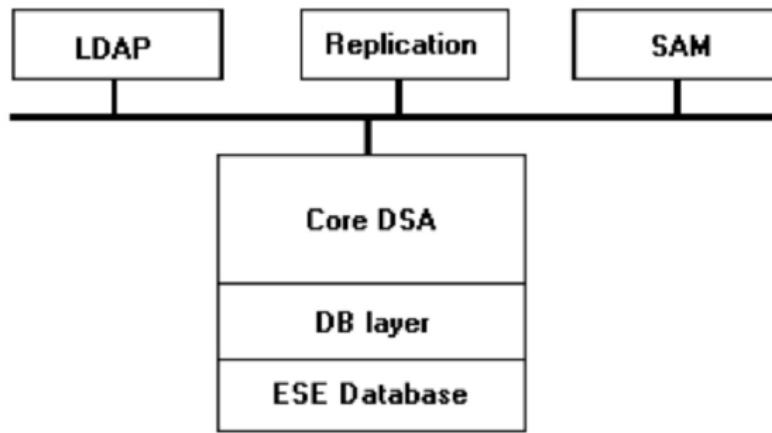


Figure – source : [technet.microsoft.com "Dimensionnement de la base de données Active Directory"](https://technet.microsoft.com/fr-fr/library/bb727005(v=ws.10).aspx)

- L'annuaire dispose d'une racine : *RootDSE* (*root DSA-specific Entry*) :
 - contient des informations sur le domaine et le contrôleur comme par exemple :
 - le niveau de fonctionnalité (c'est-à-dire la version) du domaine (attribut *domainFunctionality*) ;
 - le nom de domaine (attribut *dnsHostName*) ;
 - la version de LDAP supportée (attribut *supportedLDAPVersion*) .
 - ces informations sont accessibles sans authentification.

Structure de l'annuaire

Stockage

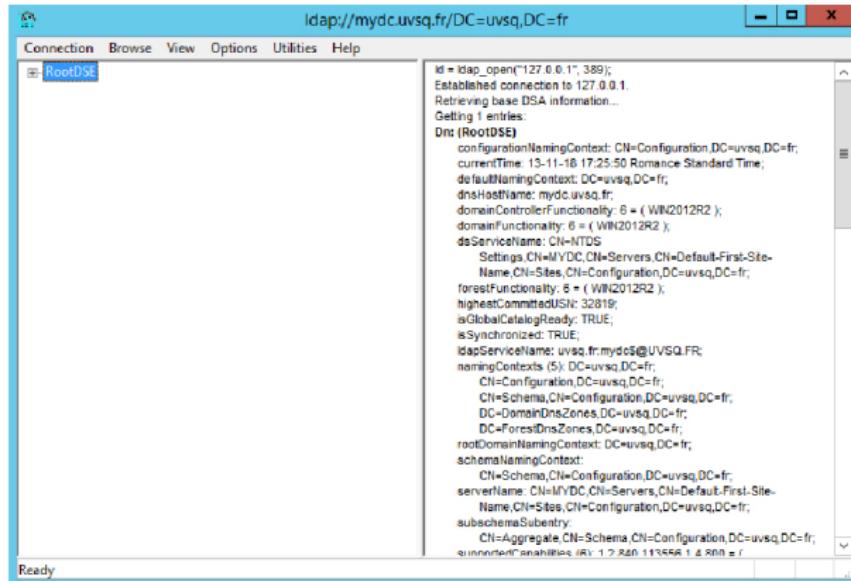


Figure – Visualisation de *RootDSE* avec l'outil *ldap*

- L'annuaire est ensuite séparé en partitions appelées *Naming Context* (NC) ;
- On trouve notamment les NC :
 - **Schema** qui contient la définition de toutes les classes d'objets et leurs attributs ;
 - *ForestDnsZones* et *DomainDnsZones* qui les informations de zone DNS pour la forêt et le domaine ;
 - la **partition du domaine** qui contient tous les objets propres au domaine (utilisateurs, machines, groupes, OU, ...).
- Via l'API LDAP, les objets sont référencés de manière unique par un *Distinguished Name* (DN).

Structure de l'annuaire

Stockage

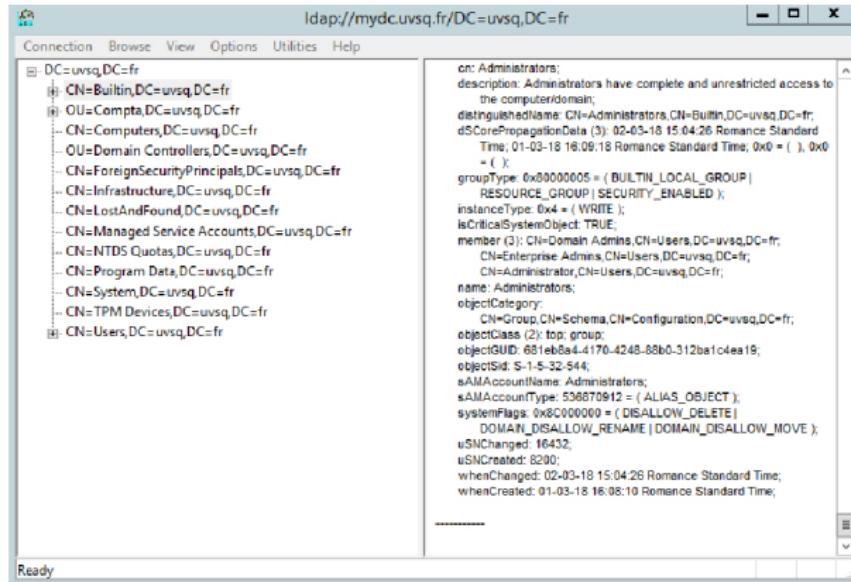


Figure – Visualisation de la partition du domaine avec l'outil *ldap*

Structure de l'annuaire

Stockage

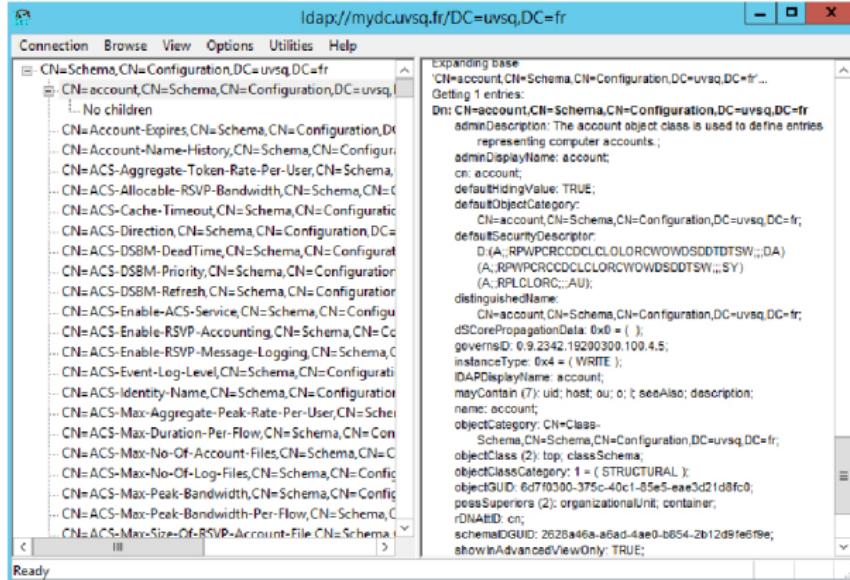


Figure – Visualisation de la partition Schema avec l'outil *ldp*

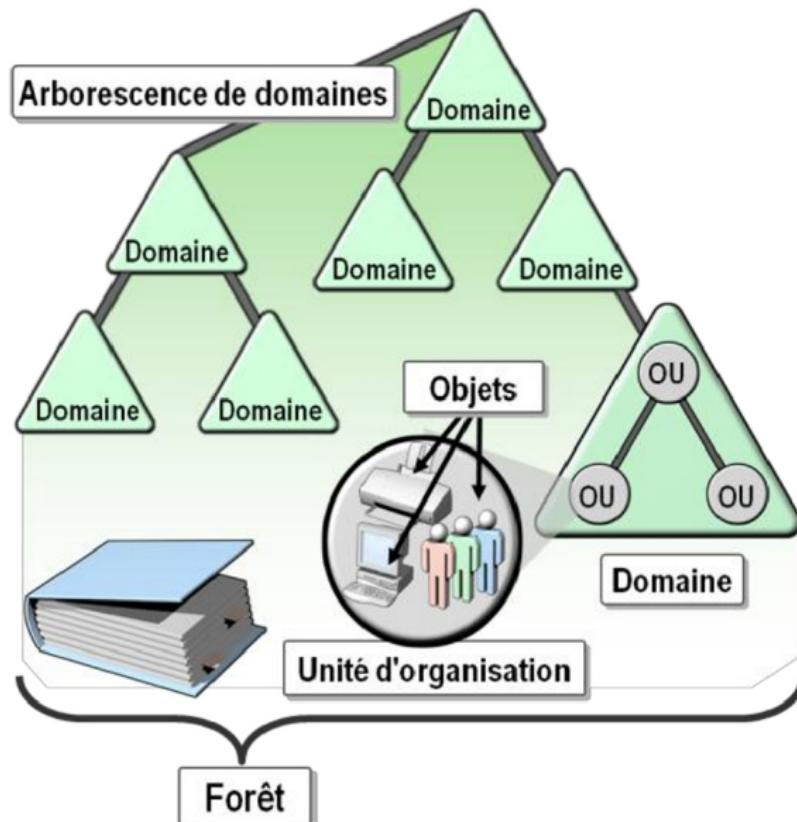
1 Introduction

2 Fonctionnement

- Stockage
- Structure logique
- GC et schéma
- Stratégies de groupe
- RéPLICATION

3 Sécurité

4 Bonus



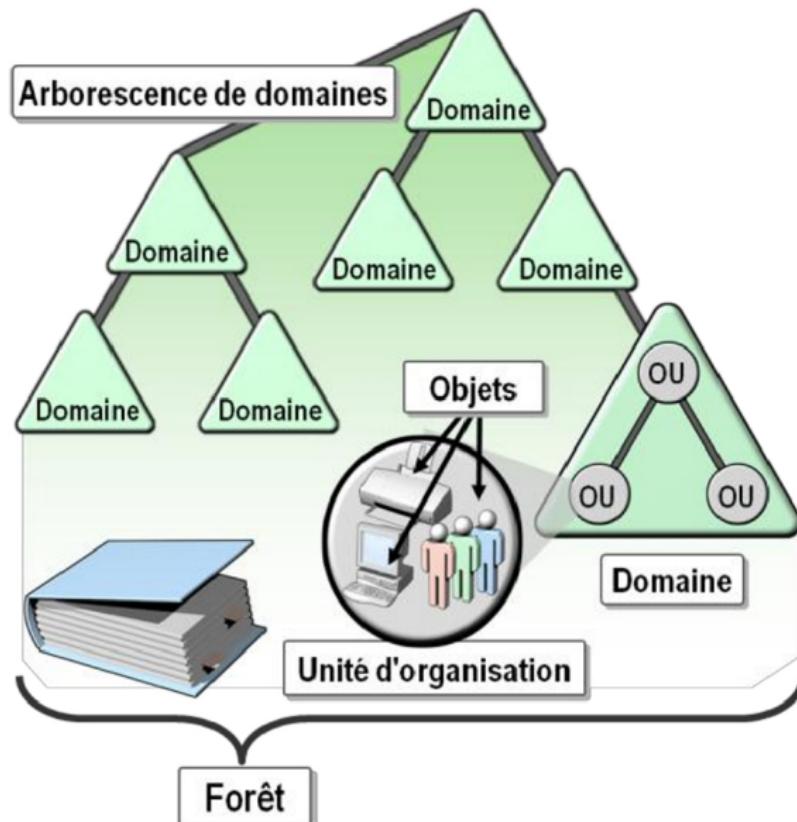
Domaine

- Les domaines sont identifiés par leur nom DNS (uvsq.fr par exemple) que l'on appelle ***namespace***;
- Un domaine contient un ensemble d'**unités d'organisation**.

Unité d'organisation

Une unité d'organisation (*organizational unit*, OU) est un conteneur générique utilisé pour grouper d'autres objets (comme des utilisateurs ou encore d'autres OU) pour faciliter l'administration.

Par analogie, une OU correspondrait à un dossier dans un système de fichier.



Arbre

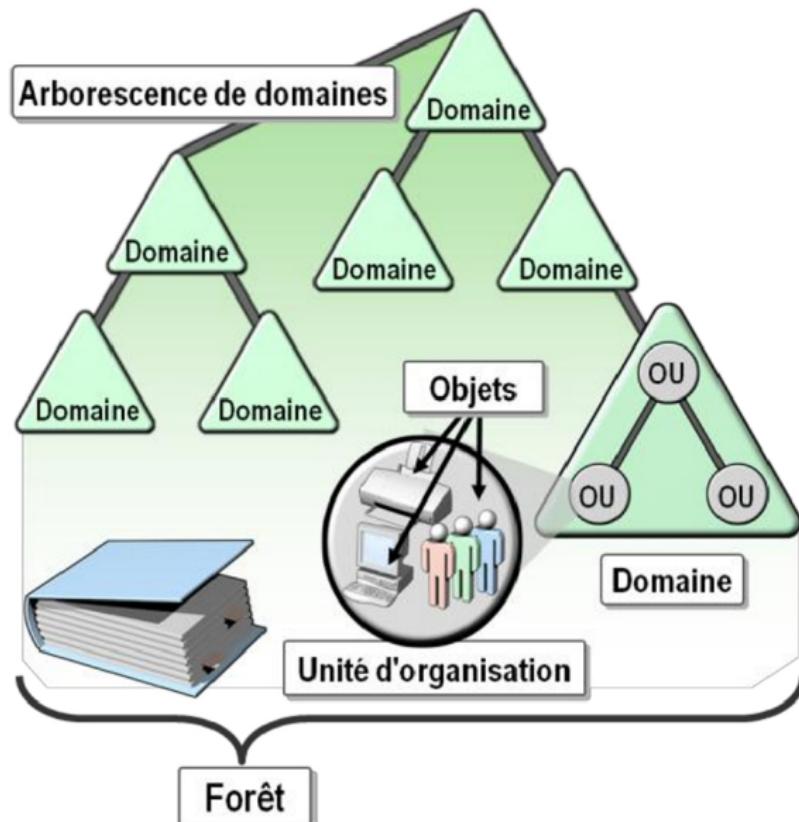
Un arbre est un regroupement hiérarchique de plusieurs domaines. Les domaines d'un même arbre partagent un espace de nom contigu.

Exemple : un arbre avec le domaine racine uvsq.fr et deux domaines feuilles *versailles.uvsq.fr* et *saint-quentin.uvsq.fr*.

Forêt

Une forêt est un regroupement de plusieurs arbres qui ne partagent pas le même espace de nom.

- Tous les domaines d'une forêt partagent un *global catalog* commun.



- Les liens entre les domaines, les arbres et même les forêts sont des **relations d'approbation** ;
- Permet de **mutualiser l'authentification** entre domaines/forêts ;
 - Par exemple, une relation d'approbation entre la forêt A et B peut permettre aux utilisateurs de la forêt A d'accéder aux ressources de la forêt B avec leurs authentifiants de la forêt A ;
- Basée sur la notion de **trust** (d'approbation) ;
- On distingue principalement les relations d'approbation sur deux aspects :
 - La direction ;
 - La transitivité.

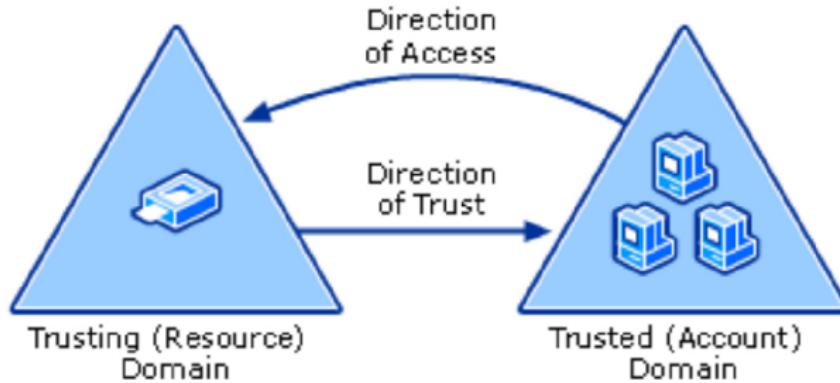


Figure – Extrait de docs.microsoft.com

Direction

- **unidirectionnelle (one-way) :**
 - Le domaine A approuve le domaine B ;
 - A->B
 - Un utilisateur du domaine B peut accéder aux ressources du domaine A.
- **bidirectionnelle (two-way) :**
 - Le domaine A approuve le domaine B et inversement ;
 - A<->B
 - Un utilisateur du domaine B peut accéder aux ressources du domaine A et inversement.

Transitivité

- **transitive** : affecte les domaines reliés par la relation ainsi que ceux ayant des relations d'approbation avec ces deux domaines :
 - par exemple : si $A \rightarrow B$ et $B \rightarrow C$ alors $A \rightarrow C$.
- **non-transitive** : n'affecte que les domaines reliés par la relation.

- Les sites représentent la **structure physique** (par opposition à la structure logique que nous venons de voir) ;
- Les sites regroupent les entités du domaine par rapport à un ou plusieurs sous-réseaux IP ;
- La structure des sites est indépendante de la structure des domaines et des OU ;
- La structure des sites est commune au travers d'une forêt ;
- Les sites permettent de contrôler le trafic généré par la **réPLICATION** et d'identifier le DC le plus proche d'un client ;
- On peut également appliquer des GPO au niveau des sites.

1 Introduction

2 Fonctionnement

- Stockage
- Structure logique
- GC et schéma
- Stratégies de groupe
- RéPLICATION

3 Sécurité

4 Bonus

Global Catalog

- Un DC peut être configuré comme serveur GC (*Global Catalog*) ;
- Les serveurs GC fournissent un listing global de tous les objets dans une forêt ;
- Pour garder une base de GC relativement petite, seulement certains attributs des objets y sont stockés. On appelle cela la PAS (*partial attributes set*) ;
- On peut modifier la PAS en marquant les attributs à répliquer vers le GC via une modification du schéma.

Schéma

Le schéma contient la définition de toutes les classes d'objets que l'on peut créer dans une forêt ainsi que la définition de tous les attributs que peut avoir un objet.

- Tous les objets ont un (ou plusieurs) type défini dans leur attribut *objectClass* ;
- Les classes sont construites avec un système d'héritage :
 - une classe hérite des attributs de ses classes mères ;
 - chaque classe rajoute ses propres attributs.
- Exemple de la classe *Computer* :
 - hérite de *User* (qui hérite de *Organizational-Person* puis de *Person* et enfin de *Top*) ;
 - elle hérite entre autres de l'attribut *Unicode-Pwd* de *User* et *name* de *Top* ;
 - elle définit entre autres l'attribut *dNSHostName*.
- Il est possible d'étendre le schéma :
 - modification de classes existantes ;
 - ajout de nouvelles classes.

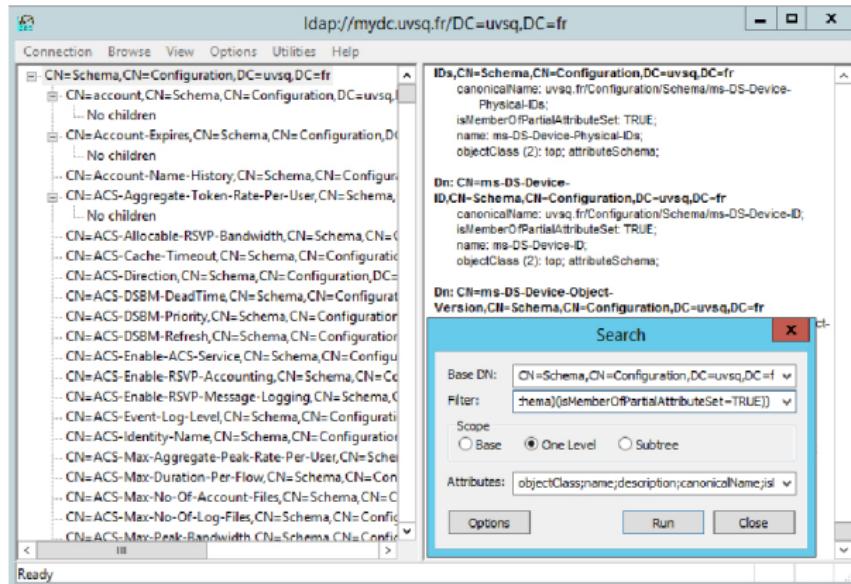


Figure – Recherche dans le Schéma avec *ldp*

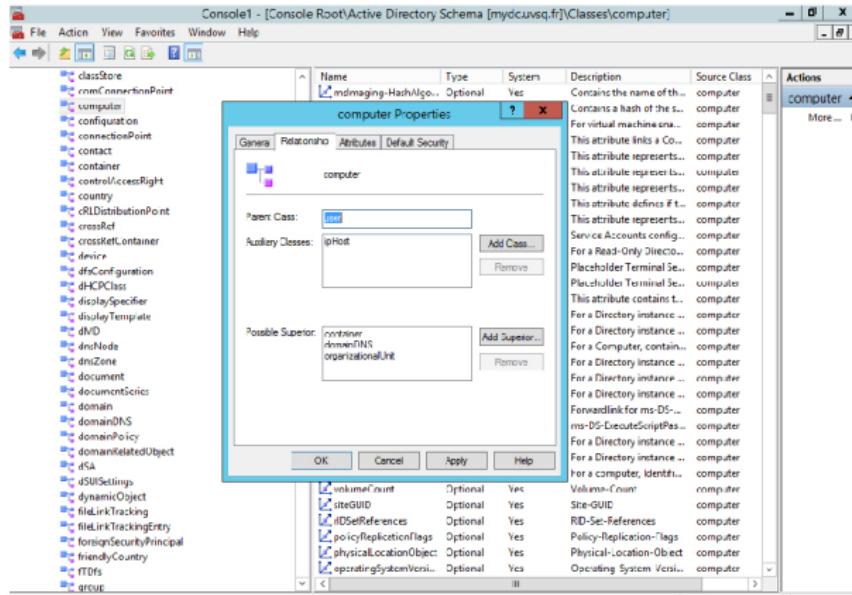


Figure – Manipulation du Schéma avec *Active Directory Schema*

1 Introduction

2 Fonctionnement

- Stockage
- Structure logique
- GC et schéma
- Stratégies de groupe
- RéPLICATION

3 Sécurité

4 Bonus

Stratégies de groupe

- Les stratégies de groupe (*Group Policy*) permettent de gérer la configuration des machines, des applications et des utilisateurs sur l'ensemble d'un domaine ;
- Les stratégies de groupe sont identifiées par un GUID ;
- Les stratégies de groupe peuvent être appliquées à des OU ;
- Ces stratégies se présentent sous la forme d'objet que l'on appelle GPO (*Group Policy Object*) :
- Il existe une version locale de ces GPO : les LGPO (*Local Group Policy Object*) ;
- Avec une GPO on peut :
 - définir la longueur minimale des mots de passe ;
 - bloquer l'accès au gestionnaire de tâches ;
 - restreindre l'accès à certains dossiers ;
 - installer un logiciel ;
 - modifier la base de registre ;
 - modifier la politique de conservation de logs.

Les informations des GPO sont stockés à trois emplacements :

- dans un objet de GPO appelé GPC (*Group Policy Container*) ;
 - stocké dans l'annuaire (CN=<GUID>,CN=Policy,CN=System,DC=<domaine>) ;
 - on y trouve les métadonnées de la GPO.
- dans le dossier C:\Windows\SYSVOL :
 - stocké dans C:\Windows\SYSVOL\<domaine>\Policy\{<GUID>} ;
 - contient une arborescence de fichiers qui définissent les paramètres de la GPO et les scripts ou exécutables à appliquer.
- dans l'attribut GPLink des objets où s'applique la GPO :
 - contient une liste d'élément de la forme [<DN de la GP01>;<enforcement>][<DN de la GP02>;<enforcement>]....

- Les GPO s'appliquent dans l'ordre suivant¹ :
 - local;
 - site;
 - domaine;
 - OU.
- Les GPO sont actualisées toutes les 90 minutes avec un offset aléatoire de 30 minutes;
- Quelques commandes utiles :
 - `gpresult /V` : donne l'ensemble des stratégies de groupe appliquées sur une machine ou à un utilisateur (appelé **Resultant Set of Policy**, RSoP);
 - `gpupdate` : met à jour les stratégies de groupe sur une machine.

1. Quand les GPO sont *enforced*, ce comportement change

1 Introduction

2 Fonctionnement

- Stockage
- Structure logique
- GC et schéma
- Stratégies de groupe
- RéPLICATION

3 Sécurité

4 Bonus

- Les modifications des informations du domaine sont synchronisées via un mécanisme de réPLICATION ;
- Cette réPLICATION fonctionne en ***pull***, c'es-à-dire que les modifications ne sont pas envoyées par le serveur où la modification a été effectuée mais récupérées par les autres serveurs.

- *Knowledge Consistency Checker* (KCC) : processus tournant sur tous les DC qui définit une topologie de réPLICATION en fonction des liens entre les sites ;
 - > cette topologie permet de distinguer deux cas :
 - la réPLICATION intrasite, qui est fréquente et automatique ;
 - la réPLICATION intersite, qui est moins fréquente et n'est pas automatique.
- La réPLICATION se fait principalement en *Remote Procedure Calls* (RPC) sur IP ;
- Pour certains types de modification, la réPLICATION entre sites peut se faire via SMTP ;
- Des attaques se basent sur le mécanisme de réPLICATION :
 - DCSync ;
 - DCShadow.

1 Introduction

2 Fonctionnement

3 Sécurité

- Authentification
- Contrôle d'accès
- Architecture en silo
- Chemins de contrôle

4 Bonus

- Par défaut, l'authentification se fait via le protocole Kerberos ;
 - pour l'authentification Kerberos, il y a trois partis :
 - le client ;
 - le serveur ;
 - le KDC.
 - différentes DLL sont utilisées :
 - kerberos.dll sur le client et le serveur ;
 - kdcsvc.dll sur le KDC.
- Pour la rétrocompatibilité, le protocole NTLM peut être utilisé.

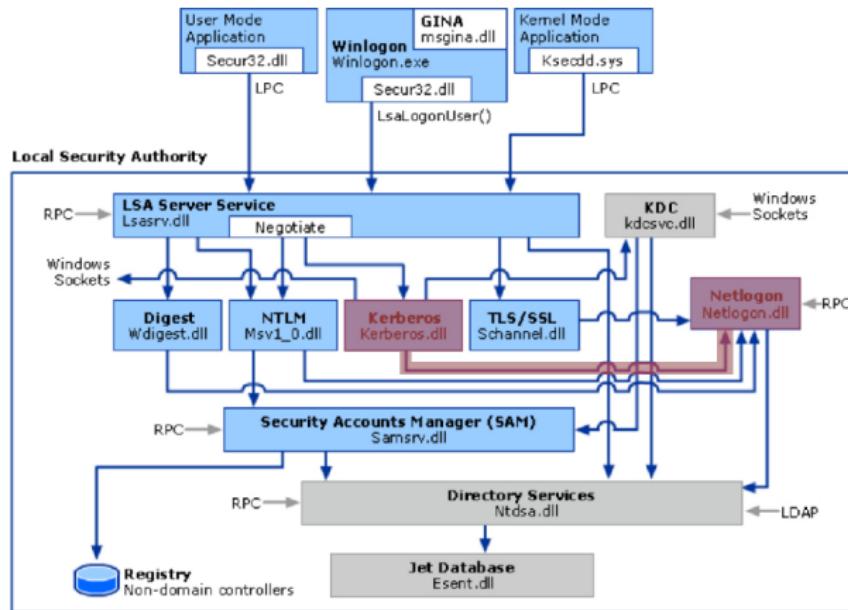


Figure – Extrait de docs.microsoft.com

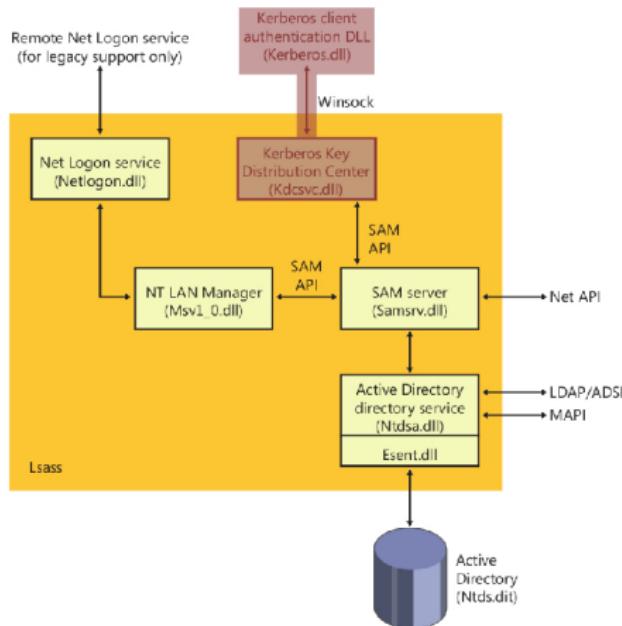
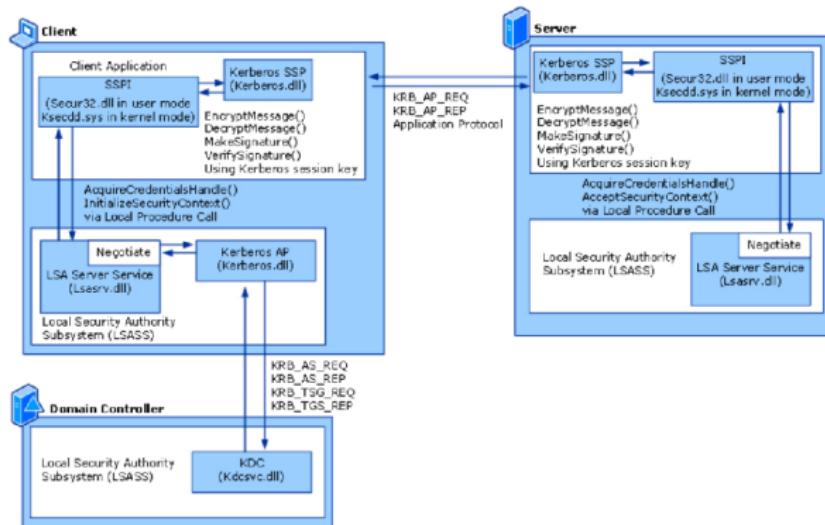


Figure – Extrait de *Windows Internals, 6th edition, part 1*

Vue d'ensemble



1 Introduction

2 Fonctionnement

3 Sécurité

- Authentification
- Contrôle d'accès
- Architecture en silo
- Chemins de contrôle

4 Bonus

- Le contrôle d'accès d'*Active Directory* se base sur le contrôle d'accès discrétionnaire de Windows ;
- Tous les objets de l'annuaire AD possède un **descripteur de sécurité** ;
- Le système de contrôle d'accès est étendu pour AD :
 - notamment par l'ajout de droits (comme DS_READ_PROP).

Groupe de sécurité

- Les groupes de sécurité, ou tout simplement les groupes, permettent d'organiser les utilisateurs et d'autres objets du domaine pour faciliter l'administration des **permissions d'accès** ;
- Il existe des groupes *built-in* comme :
 - *Everyone* ;
 - *Administrators*.

Groupe de distribution

Les groupes de distribution sont seulement utilisés pour la **distribution des mails**, ils ne permettent pas de gérer les permissions.

Quelle est la différence par rapport aux OU ?

- Les groupes :
 - peuvent être utilisés pour définir les permissions ;
 - un utilisateur peut appartenir à plusieurs groupes.
- Les OU :
 - ne peuvent pas être utilisées pour définir les permissions ;
 - un utilisateur peut être contenu que dans une OU.

- Un privilège est le droit d'un compte, comme un utilisateur ou un groupe, de faire des actions systèmes sur la machine ;
- Par exemple, ces actions peuvent être :
 - éteindre la machine ;
 - charger des drivers ;
 - changer l'heure.
- Il existe des privilèges spécifique à AD comme le privilège d'ajout de machine au domaine (*SeMachineAccountPrivilege*) ;
- Les privilèges diffèrent des permissions par deux aspects :
 - les privilèges sont attribués à un utilisateur ou à un groupe, alors que les permissions sont définies pour un objet ;
 - Les privilèges autorisent un utilisateur à faire des actions système, alors que les permissions contrôlent les actions que l'on peut faire sur un objet.

- La délégation est un mécanisme qui nous permet de mettre en place le principe de **séparation des priviléges** ;
- Ce mécanisme permet à un administrateur de déléguer le contrôle sur des objets à des utilisateurs ou des groupes ;
- La délégation peut se faire au niveau des OU mais aussi au niveau des objets et des attributs de ces objets ;
- Il peut par exemple autoriser un utilisateur d'une OU à créer des comptes dans cette OU.

1 Introduction

2 Fonctionnement

3 Sécurité

- Authentification
- Contrôle d'accès
- Architecture en silo
- Chemins de contrôle

4 Bonus

- Lors d'une attaque sur un domaine Windows, l'attaquant va essayer de récupérer les *credentials* d'un administrateur ;
- Ces *credentials* peuvent se matérialiser de plusieurs façons :
 - le mot de passe ;
 - des secrets stockés en mémoire (le *hash* du mot de passe par exemple) ;
 - *Pass-The-Hash*
 - des traces réseau (élément de défi/réponse par exemple).
- Il faut donc éviter qu'un administrateur qui est administrateur de domaine dissémine ces *credentials* sur tout le parc ;
- On va donc segmenter le domaine pour qu'un attaquant qui aurait compromis un poste de travail ne puisse pas récupérer les *credentials* d'un administrateur de domaine qui lui donnerait le contrôle sur l'ensemble du domaine ;
- > Pour faire ça on va se baser sur le système Windows de silo.

- Les silos vont permettre de restreindre l'authentification sur un groupe de machine à un groupe d'utilisateur;
 - > cela va permettre de définir des zones qui seront cloisonées au niveau de l'authentification.
- On va pouvoir définir trois zones :
 - Une zone DC : la prise de contrôle d'une ressource de ce niveau permet de contrôler toutes les ressources;
 - cette zone comporte principalement les DC.
 - Une zone SERVEUR : les ressources et les serveurs hébergeant les données métier;
 - cette zone comporte tous les serveurs ;
 - on retrouve les serveurs de web, les serveurs de sauvegarde...
 - Une zone STATIONS : les postes de travail et le reste.
- > Pour plus de détails, voir l'article *L'administration en silo* d'Aurélien Bordes du SSTIC 2017.

1 Introduction

2 Fonctionnement

3 Sécurité

- Authentification
- Contrôle d'accès
- Architecture en silo
- Chemins de contrôle

4 Bonus

- Méthode d'analyse d'environnements AD ;
- Analyse les chemins de contrôle entre les objets du domaine ;
- Un chemin de contrôle est une succession de relation de contrôle direct entre objet ;
- Une relation de contrôle direct traduit le contrôle d'un objet sur un autre ;
- Les relations de contrôle direct sont identifiées sur plusieurs critères comme :
 - le contenu des descripteurs de sécurité ;
 - par exemple, le propriétaire de l'objet a le contrôle sur l'objet.
 - l'appartenance à un groupe de sécurité ;
 - l'appartenance à un conteneur (comme les OU) ;
 - les priviléges configurés par les GPO ;
- Il faut donc récolter des informations dans l'annuaire, dans les GPO ainsi que localement sur chaque machine.

- Cette analyse se passe en trois phases :
 - 1 la récolte des informations de l'AD permettant de définir des relations de contrôle ;
 - 2 la génération des relations de contrôle à partir des informations récoltées ;
 - 3 l'extraction de chemins de contrôle (sous forme de graph).
 - Permet par exemple de répondre aux questions :
 - Qui peut contrôler tel groupe ?
 - Qui peut devenir administrateur de domaine ?
 - Quelles ressources sont accessibles à un utilisateur ?
 - Des outils ont été développés pour réaliser cette tâche :
 - AD-control-paths² ;
 - Bloodhound³ ;
 - bta⁴.
- > Pour plus de détails, voir l'article *Chemins de contrôle en environnement Active Directory* de Lucas Bouillot et Emmanuel Gras du SSTIC 2014.

-
2. <https://github.com/ANSSI-FR/AD-control-paths>
 3. <https://github.com/BloodHoundAD/BloodHound>
 4. <https://bitbucket.org/iwseclabs/bta>

Exemple d'un domaine compromis

Analyse de chemins de contrôle

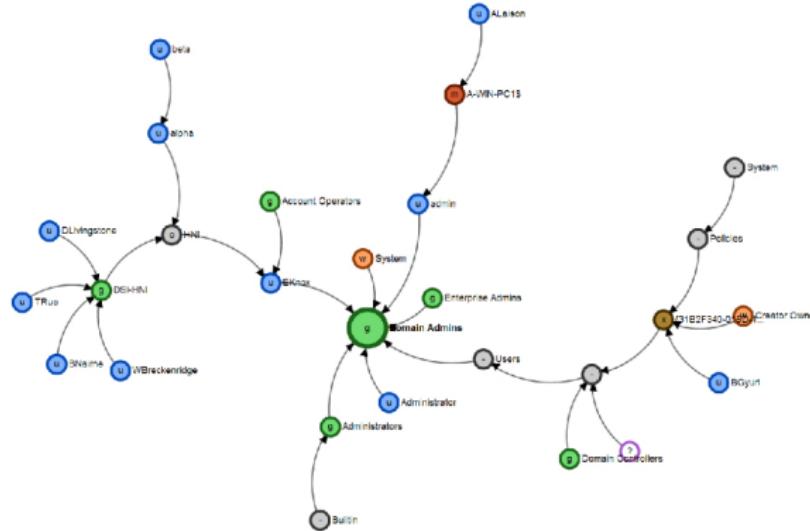


Figure – Extrait de l'article *Chemins de contrôle en environnement Active Directory* du SSTIC 2014

1 Introduction

2 Fonctionnement

3 Sécurité

4 Bonus

■ WSUS

- *Windows Server Update Services (WSUS)* est un service permettant de déployer les mises à jour sur un ensemble de postes Windows ;
- WSUS télécharge les mises à jour depuis le site Microsoft Update puis les redistribue ;
- Peut se paramétrer à l'aide de GPO ;
- Il existe des attaques se basant sur WSUS :
 - WSUSpect ;
 - WSUSpendu.

Commissariat à l'énergie atomique et aux énergies alternatives
Centre de Bruyères-le-Châtel | 91297 Arpajon Cedex
T. +33 (0)1 69 26 40 00 | F. +33 (0)1 69 26 40 00
Établissement public à caractère industriel et commercial
RCS Paris B 775 685 019

CEA