



# ACTIVE DIRECTORY

# SOMMAIRE

- Annuaire
- Service de domaine
- Architecture Active Directory
- Sécurité informatique
- Gestion des droits
- Gestion des utilisateurs
- Stratégies de groupe
- Service de certificat
- Les protocoles LDAP, DNS et Kerberos



Active Directory

# Annuaire

L'annuaire permet de :

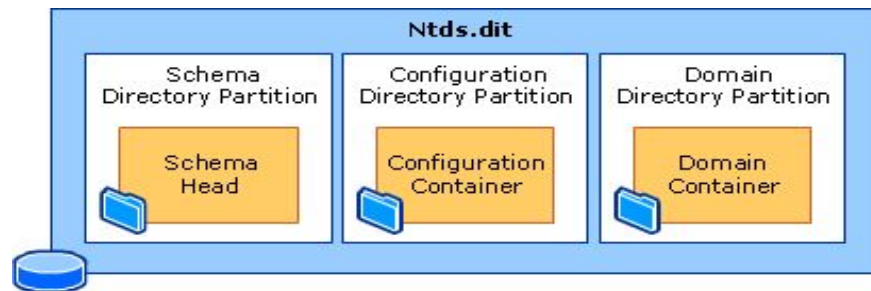
- Administration centralisée et simplifiée
- Unifier l'authentification
- Identifier les objets sur le réseau
- Référencer les utilisateurs et ordinateur

Racine de la console	Nom	Syntaxe	État	Description
Utilisateurs et ordinateurs Act...	accountExpires	Entier long/Intervalle	Actif	Account-Expires
4 Schéma Active Directory [SRV...	accountNameHistory	Chaîne Unicode	Actif	Account-Name-History
Classes	aCSAggregateTokenR...	Entier long/Intervalle	Actif	ACS-Aggregate-Token-...
Attributs	aCSAllocableRSVPBan...	Entier long/Intervalle	Actif	ACS-Allocable-RSVP-Ba...
	aCSCacheTimeout	Entier	Actif	ACS-Cache-Timeout
	aCSDirection	Entier	Actif	ACS-Direction
	aCSDSBMDeadTime	Entier	Actif	ACS-DSBM-DeadTime
	aCSDSBMPriority	Entier	Actif	ACS-DSBM-Priority
	aCSDSBMRefresh	Entier	Actif	ACS-DSBM-Refresh
	aCSEnableACSService	Booléen	Actif	ACS-Enable-ACS-Service
	aCSEnableRSVPAccou...	Booléen	Actif	ACS-Enable-RSVP-Acco...
	aCSEnableRSVPMessa...	Booléen	Actif	ACS-Enable-RSVP-Messa...
	aCSEventLogLevel	Entier	Actif	ACS-Event-Log-Level
	aCSIdentityName	Chaîne Unicode	Actif	ACS-Identity-Name

# Annuaire

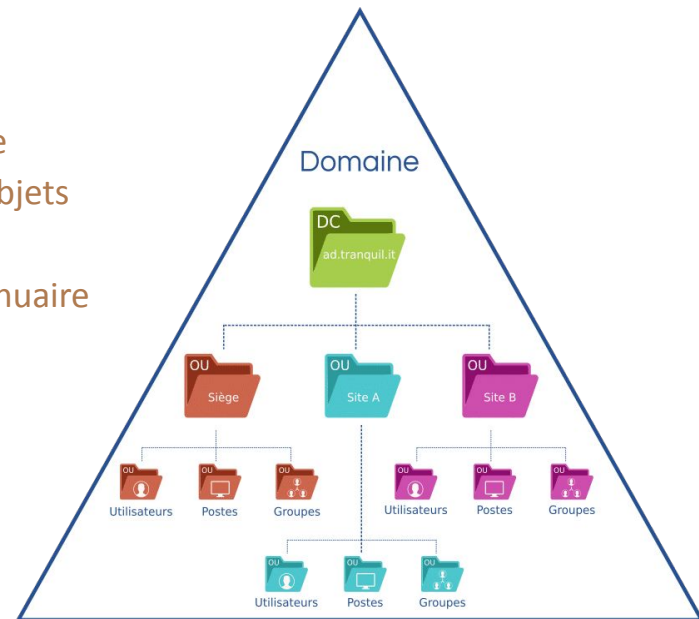
## Structure de l'Active Directory :

- Les classes et les attributs
- Le schéma
- Les partitions d'annuaire :
  - La partition de schéma
  - La partition de configuration
  - La partition de domaine



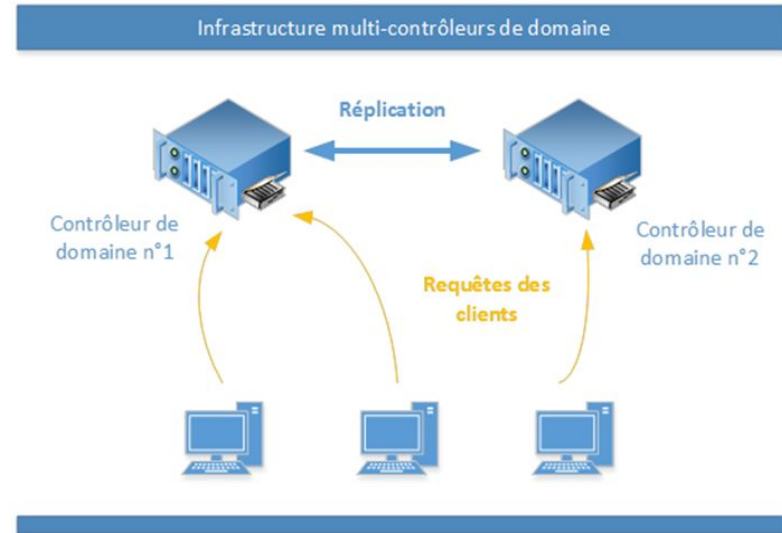
# Service de domaine

- Base d'utilisateurs, de groupes et d'ordinateurs centralisée
- L'annuaire contient toutes les informations relatives aux objets
- Ouverture de session unique par utilisateur
- Chaque contrôleur de domaine contient une copie de l'annuaire
- Administration et gestion de la sécurité centralisée



# Service de domaine

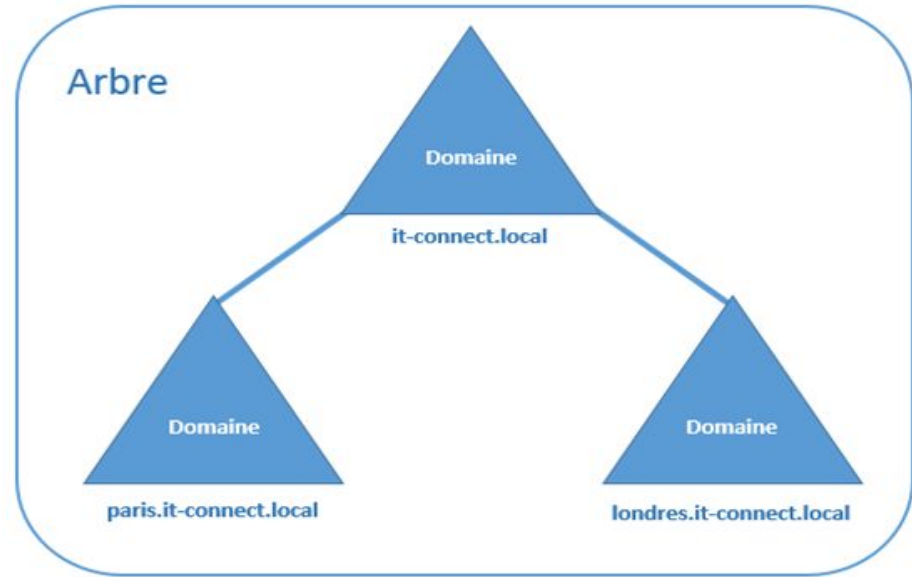
- Contrôleur de domaine
- Le fichier de base de données NTDS.dit
- La réplication des contrôleurs de domaine



# Architecture Active Directory

Un domaine :

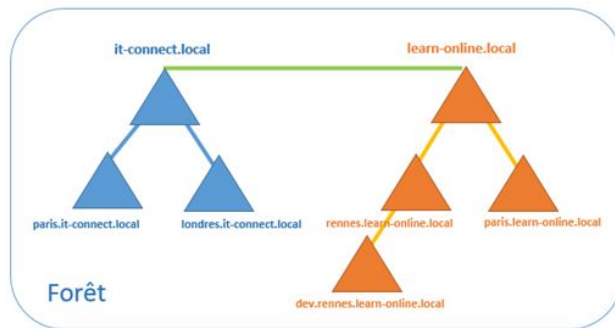
- Domaine principal
- Sous domaine 1
- Sous domaine 2



# Architecture Active Directory

Les forêts :

- Les arbres d'une forêt partagent un schéma d'annuaire commun
- Les domaines d'une forêt partagent un "Catalogue Global" commun
- Les domaines d'une forêt fonctionnent de façon indépendante
- Création de relations entre les différents domaines de la forêt
- Simplification de l'administration et flexibilité

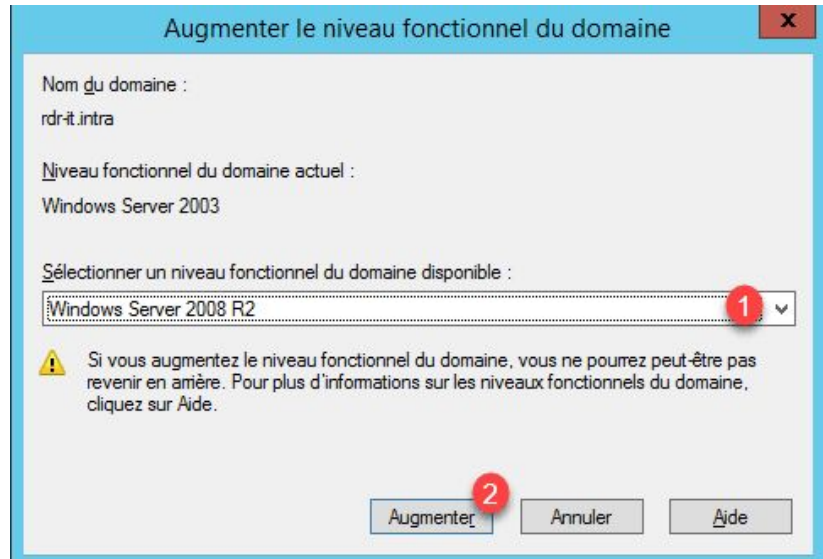




# Architecture Active Directory

Le niveau fonctionnel :

- C'est quoi le niveau fonctionnel ?
- Augmenté le niveau fonctionnel
- La portée d'un niveau fonctionnel

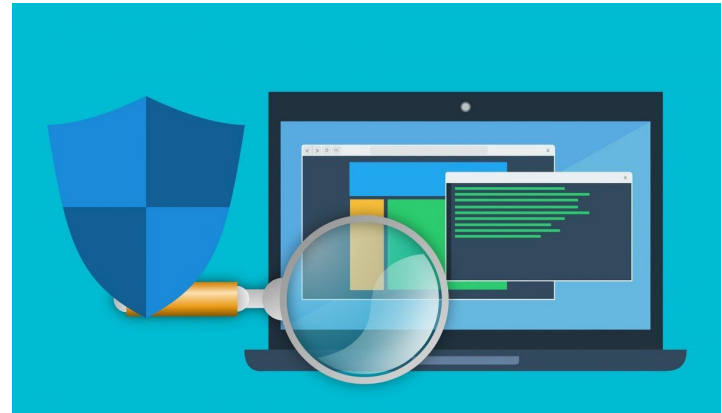


# Sécurité informatique

## *Protection contre les attaques*

Plusieurs mesures de sécurité :

- Les politiques de mot de passe
- Surveillance des événements de sécurité
- Authentification multifacteur
- Pare-feu et isolation de réseau
- Gestion des droits d'accès
- Mises à jour régulières

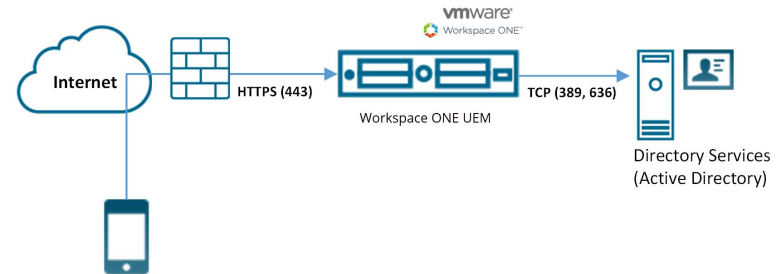


# Sécurité informatique

## *Authentication*

Certificats numériques pour vérifier l'identité des utilisateurs :

- L'utilisateur envoie une demande d'authentification
- Vérification du contrôleur de domaine
- Demande de validation
- Le rôle du contrôleur de domaine

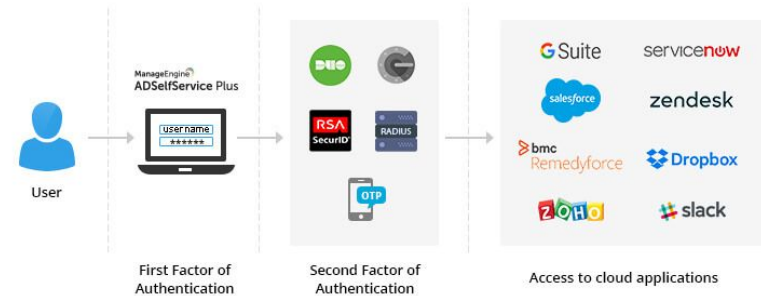


# Sécurité informatique

## *Sécurité multi-facteurs*

Mesures de sécurité complémentaire :

- Configurée la sécurité multi-facteurs
- Configurer l'authentification
- L'authentification supplémentaire
- Gestion des droits d'accès pour l'utilisateurs

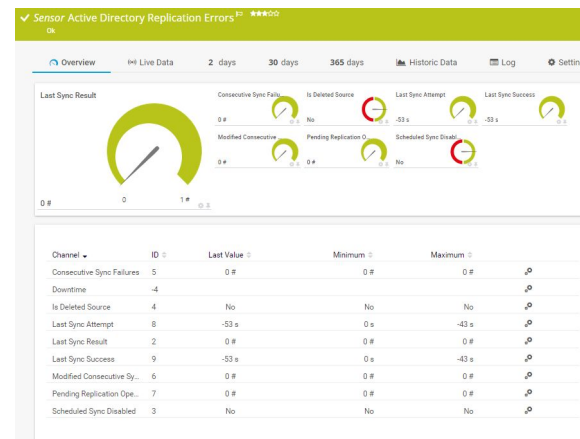


# Sécurité informatique

## Surveillance

La surveillance dans l'Active Directory :

- Les journaux d'audit enregistrent les événements dans l'AD
- Détection d'activités suspectes
- Des alertes de sécurité
- Les rapports de sécurité
- Modification aux objets AD

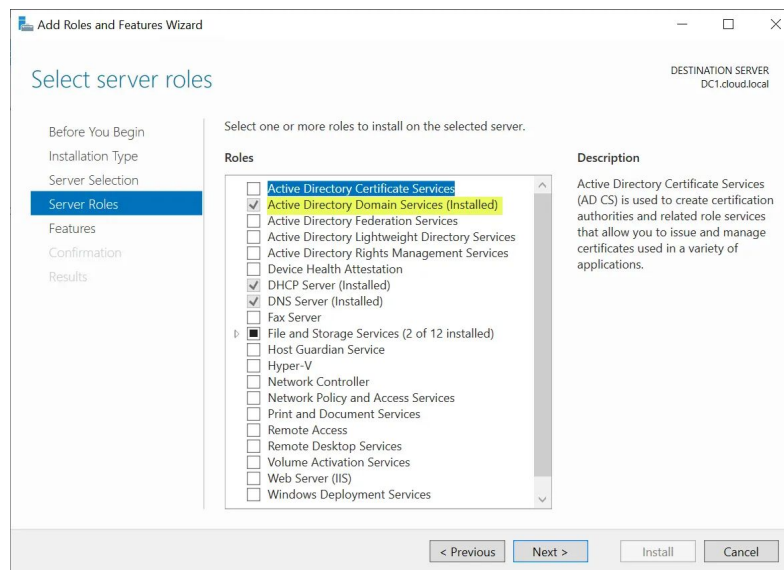


# Sécurité informatique

## *Sécurité basée sur des rôles*

### Gestion des rôles :

- Les groupes utilisateurs
- L'attribution rôles aux utilisateurs
- Les permissions pour chaque rôle
- L'attribution des permissions
- Gérés de manière centralisée



# Sécurité informatique

## Gestion de clés et des certificats

Service de certification (SC) et de chiffrement de fichier (CF) :

- Le SC permet différentes choses dans l'AD
- Chiffrement de données et stockage des clés
- Console de gestion de certificats

The image displays two screenshots of the 'Configuration des services de certificats Active Directory' (Active Directory Certificate Services Configuration) wizard.

**Left Screenshot: 'Nom de l'autorité de certification' (Certificate Authority Name)**

- Navigation pane:** Informations d'identifiants..., Services de rôle, Type d'installation, Type d'AC, Clé privée, Chiffrement (selected), Nom de l'AC, Période de validité, Base de données de certi..., Confirmation, Progression, Résultats.
- Section: 'Nom de l'autorité de certification'**
  - Spécifier le nom de l'AC:** Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.
  - Nom commun de cette AC :** CA-IT-CONNECT-FR
  - Suffixe du nom unique :** DC=it-connect,DC=fr
  - Aperçu du nom unique :** CN=CA-IT-CONNECT-FR,DC=it-connect,DC=fr
- Buttons:** < Précédent, Suivant >, Configurer, Annuler.

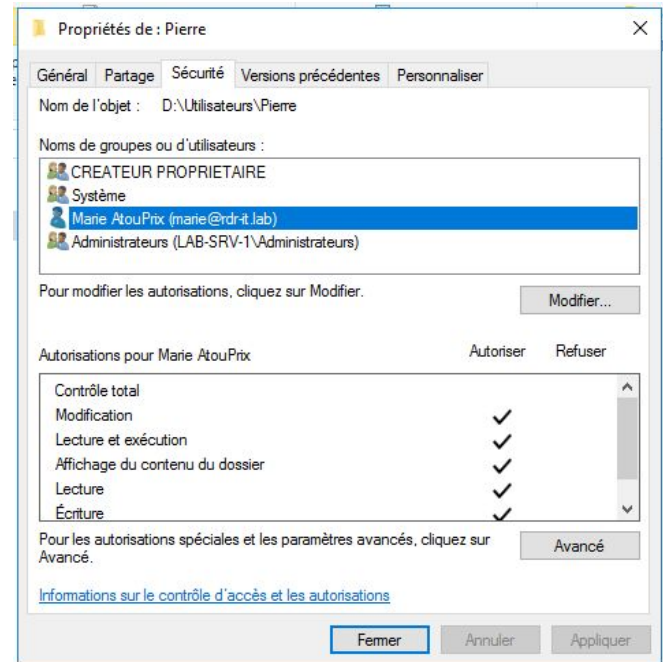
**Right Screenshot: 'Clé privée' (Private Key)**

- Navigation pane:** Informations d'identifiants..., Services de rôle, Type d'installation, Type d'AC, Clé privée (selected), Chiffrement, Nom de l'AC, Période de validité, Base de données de certi..., Confirmation, Progression, Résultats.
- Section: 'Clé privée'**
  - Spécifier le type de la clé privée**
  - Options:**
    - ☒ **Créer une clé privée**  
Utilisez cette option si vous n'avez pas de clé privée ou pour en créer une.
    - ☐ **Utiliser la clé privée existante**  
Utilisez cette option pour garantir la continuité avec les certificats émis antérieurement lors de la réinstallation d'une AC.
      - ☐ Sélectionner un certificat et utiliser sa clé privée associée
      - ☐ Sélectionner une clé privée existante sur cet ordinateur
- Buttons:** < Précédent, Suivant >, Configurer, Annuler.

# Gestion des droits

Les étapes à suivre pour une bonne gestion des droits :

- Identifier les besoins en matière de sécurité
- Créer des groupes de sécurité
- Définir les autorisations
- Utiliser des stratégie de groupe
- Surveiller et auditer les droits d'accès





# Gestion des utilisateurs

Les étapes à suivre pour la gestion des utilisateurs :

- Créer un compte utilisateur
- Modifier les informations de compte
- Désactiver ou supprimer un compte
- Gérer les autorisations d'accès
- Gérer les stratégies de mot de passe
- Suivre les modifications

Nouvel objet - Utilisateur

Créer dans : lab.intra/Services/IT/Users

Prénom :  Initiales :

Nom :

Nom complet :

Nom d'ouverture de session de l'utilisateur :  
 @lab.intra

Nom d'ouverture de session de l'utilisateur (antérieur à Windows 2000) :

< Précédent Suivant > Annuler

# Stratégies de groupe

Des paramètres à configurer :

- Paramètres de sécurité : Mot de passe, droit d'accès, certificats
- Paramètres de configuration du système :  
Paramètres de registre, de pare-feu, de mise à jour et de scripts de connexion/déconnexion
- Paramètres de logiciel :  
Stratégies d'installation, paramètres de comptabilité et de configuration de Microsoft Office.

# Stratégies de groupe

Les étapes à suivre pour créer une stratégie de groupe :

- Accéder au module complémentaire Gestion des stratégies de groupe dans l'Active Directory
- Créez un nouvel objet de stratégie de groupe
- Modifiez la stratégie de groupe en configurant les paramètres du nouvel objet
- Appliquez la stratégie de groupe en la liant à une unité d'organisation, un groupe de sécurité ou un domaine

# Service de certificat

Permet de :

- Déployer
- Gérer
- Distribuer

Pour sécuriser :

- Les communications
- Les transactions
- L'identité

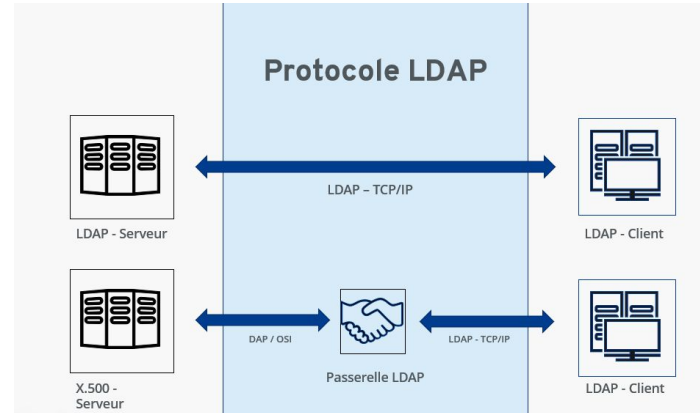
Pour sécuriser les connexions :

- VPN
- Sans fil
- Htpps
- Signature numérique

# Les protocoles LDAP

Comprennent le :

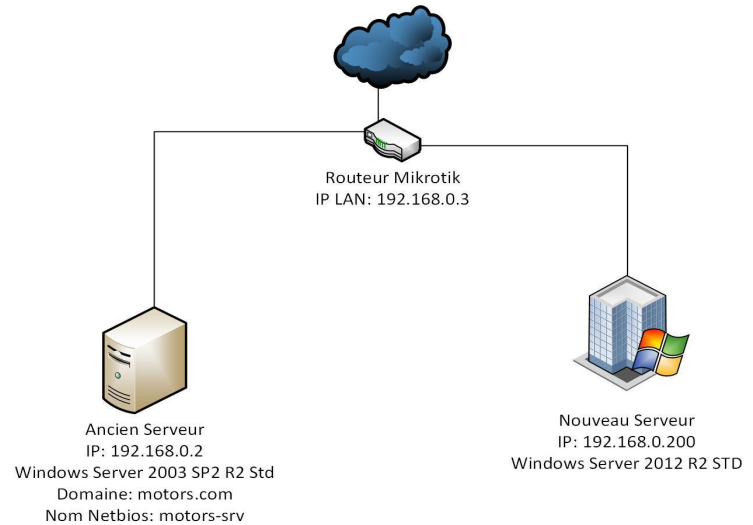
- LDAP Standard
- LDAPS (LDAP sécurisé)
- LDAP sur UDP et TCP
- Global Catalog LDAP
- Active Directory Web Service (ADWS)



# Les protocoles DNS

Comprennent le :

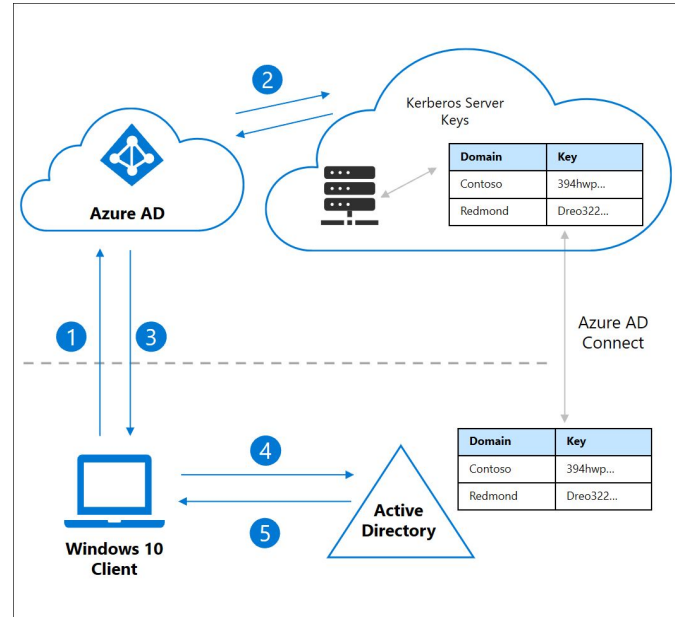
- LDAP
- Kerberos
- Global Catalog
- Dynamic DNS
- Nslookup



# Les protocoles Kerberos

Plusieurs extensions :

- Kerberos Constrained Delegation
- Kerberos Armoring
- Services for User



# FIN DU DIAPORAMA

Merci de nous avoir écoutés

- Florian
- Clément
- Lukas
- Valérien

