Services Active Directory DS

Présentation de l'Active Directory

L'Active Directory

C'est une solution propriétaire Microsoft. Cela permet de centraliser les identités, objets et les accès aux ressources d'une organisation (ordinateurs, imprimantes, partage de fichiers...).

Aujourd'hui il existe une version alternative "Cloud" ou plutôt SaaS appelée **Microsoft Entra ID**.

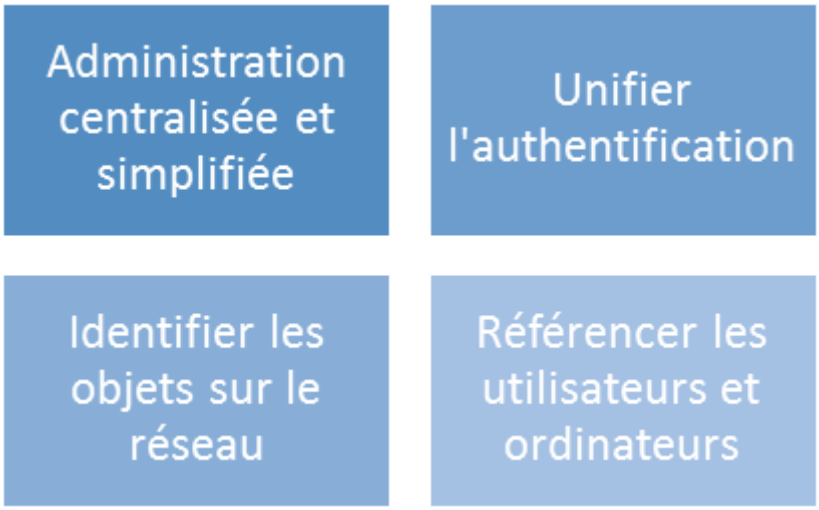
Ce service d'annuaire utilise le protocole LDAP (Lightweight Directory Access Protocol) de la couche 7 du modèle OSI.

Ce protocole s'appuie sur TCP/IP et par défaut il utilise les ports 389 et 3268.

Active Directory utilise également le protocole **DNS** afin d'identifier et enregistrer les objets. Il est donc primordiale de disposer d'une structure DNS stable et fiable pour son fonctionnement.

Les intérêts de l'annuaire

Présent dans la plupart des entreprises, les avantages de l'Active Directory ne sont plus un débat.



- **Centralisation et simplification de l'administration**

La création des utilisateurs, des permissions d'accès aux ressources et la gestion de politiques de configuration (GPO) sont définies et maintenues au niveau du domaine. Donc à partir d'un seul endroit, ce qui évite les répétition de configuration.

- **Authentification**

Les objets "utilisateurs" s'authentifient sur des objets "ordinateurs" qui sont eux même authentifié au domaine AD. Cela leur permet d'accéder (ou non en fonction des autorisations) à des ressources partagés sur d'autres ordinateurs/serveurs du domaine.

Egalement, un seul compte est utile pour se connecter sur des ordinateurs du domaine différents.

Autre point important, il existe de nombreuses applications qui permettent de s'appuyer sur l'authentification Active Directory et donc de simplifier encore plus la gestion des accès en entreprise !

- **Identification**

Comme indiquer précédemment, chaque objet est enregistré dans l'annuaire AD. Ces objets sont unique et facilement identifiables.

Toutes les ressources sont listées et il est très simple de "couper les accès" à une ressource en la désactivant par exemple.

- **Référencement**

L'annuaire AD étant une énorme base de données où tous les utilisateurs et ordinateurs de l'entreprise sont référencés, on s'appuie dessus pour réaliser les opérations d'authentification, d'identification, les déploiements de logiciels, les politiques de mot de passe...

La structure logique

- **Objets**

Les éléments utilisateurs, ordinateurs, serveurs ou encore les unités d'organisations, sont des **Objets** de l'annuaire.

Ces objets correspondent à des **classes** et chaque classe dispose **d'attributs**.

Exemple : un ordinateur est un objet de la classe Ordinateurs. Il dispose d'attributs spécifiques qu'un objet de la classe Utilisateur ne dispose pas et inversement.

- **Conteneurs**

Les conteneurs sont également des objets de l'annuaire, ces derniers servent à l'organisation et peuvent donc contenir d'autre objets.

Les groupes contiendront donc des objets de la classe Utilisateur ou Ordinateur par exemple.

Les Unités d'Organisations (OU) sont également des conteneurs d'objet. Par défaut, des OU sont présentes dans l'annuaire. Il convient à l'administrateur d'en ajouter afin de créer une structure avec plusieurs niveaux qui simplifieront l'administration générale de l'Active Directory.

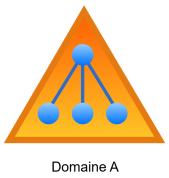
Il faut voir les OU comme des dossiers qui permettent de ranger les objets.

- **Domaine**

Un domaine est une zone d'administration regroupant plusieurs objets et ressources qui partagent un annuaire commun.

Dans le même principe que DNS, Active Directory utilise le principe de l'arborescence inversée. Ainsi, un domaine ajouté à un domaine existant sera "enfant" du premier.

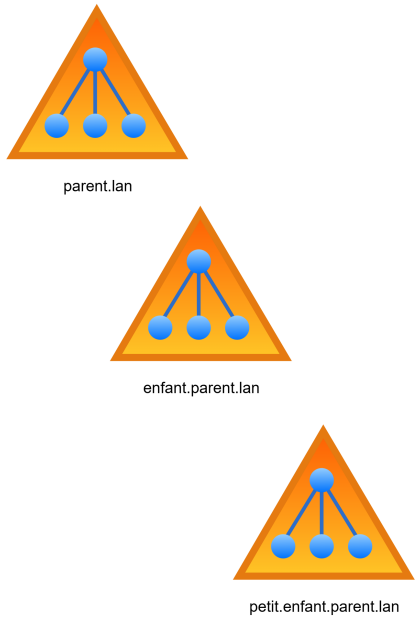
Conventionnellement, les domaine Actives Directory sont représenté par des triangles.



- **Arbre**

L'arbre représente l'ensemble hiérarchique des domaine parent + enfant. Il est possible pour un domaine enfant d'avoir lui aussi un ou plusieurs autres domaine enfant. Cela formera donc une hiérarchie de domaine dont la base du nom reprendra toujours celle du domaine racine/parent : domaineEnfant.domaineParent.lan

Cette ensemble forme donc l'arbre Active Directory.



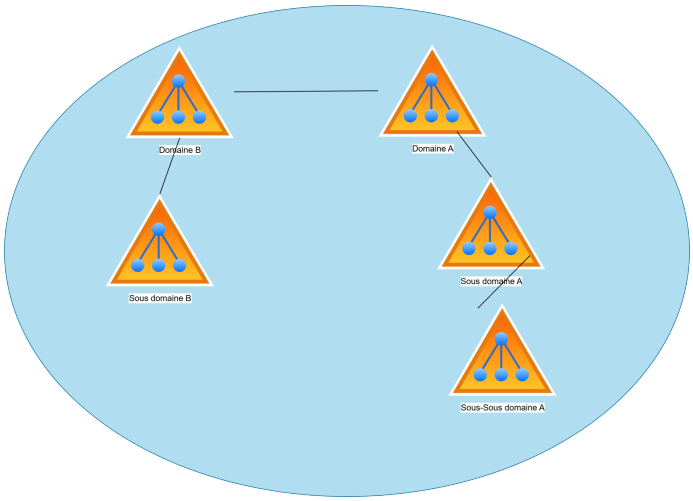
- **Forêt**

C'est la représentation complète de tous les arbres représentant eux mêmes tous les domaine parents + enfants.

Tous les domaines d'une forêt partagent :

- Une configuration commune
- Une étendue de recherche global
- Des relations d'approbations

Lorsque l'on crée un nouveau domaine dans un nouvelle forêt, on crée ce que l'on appelle le **domaine racine**.



- **Le schéma**

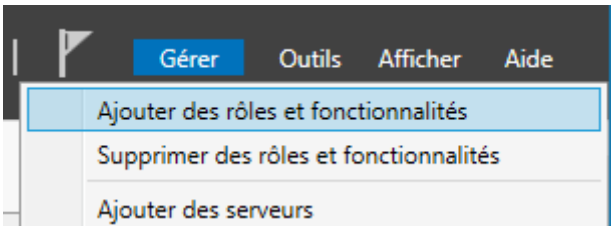
Le schéma Active Directory contient toutes les définitions de tous les objets de l'annuaire. Un schéma est créé par défaut à la création d'un domaine, il évoluera au fil du temps en fonction des besoins ou pour répondre à des prérequis d'applications (exemple Microsoft Exchange).

Attention toutefois, la modification du schéma doit être réalisé avec précaution car tous les objets seront impactés par les modifications.

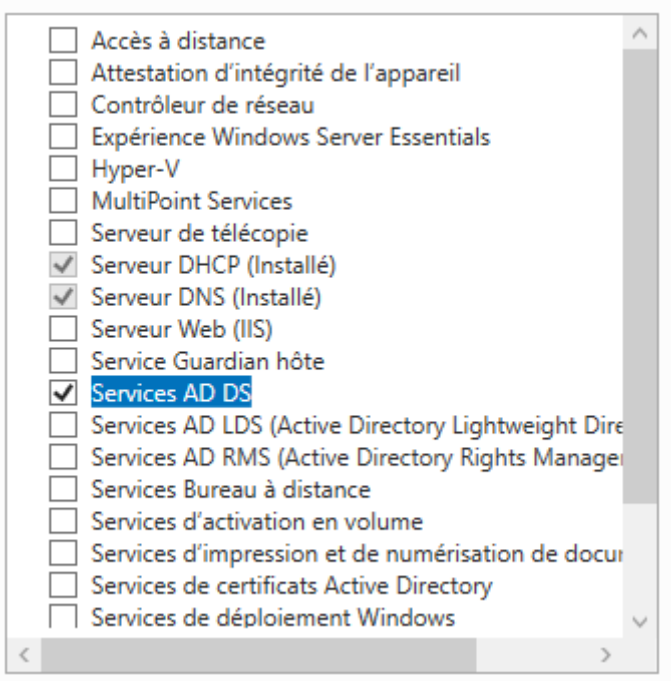
Il existe d'ailleurs un groupe de sécurité "Administrateur du schéma" dont il faut être membre afin de réaliser les modifications.

Installation du service AD DS

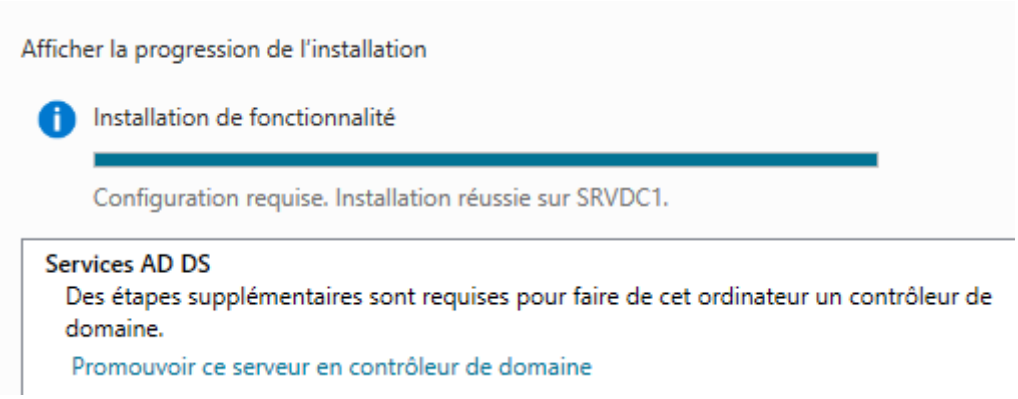
- Dans le gestionnaire de serveur, ajouter des rôles et fonctionnalités.
  - Dans cette situation le serveur a déjà été renommé et configuré avec un adresse IP statique, nous n'avons donc pas besoins de le faire.



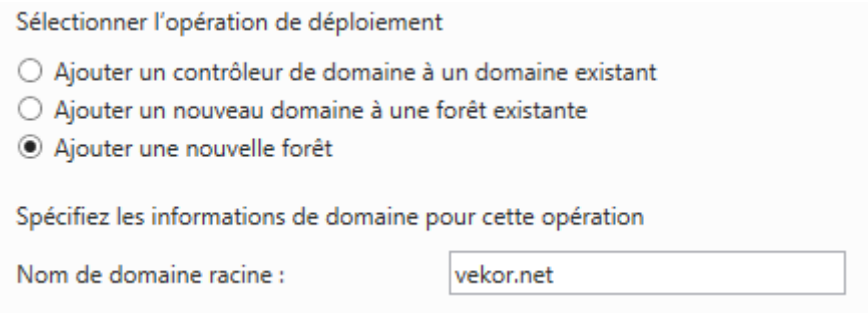
- Sélectionner : Services AD DS puis suivant jusqu'à pouvoir installer le rôle.



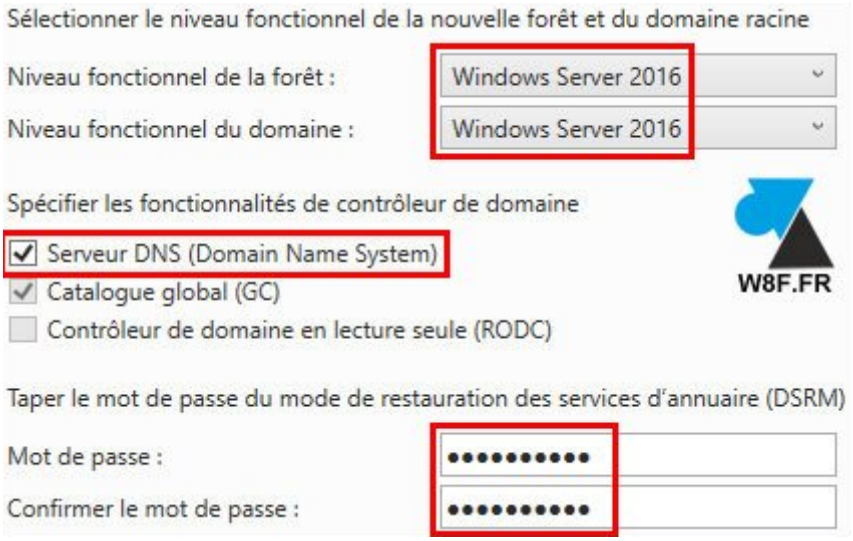
- Lorsque l'installation du service est terminée, cliquer sur Promouvoir ce serveur en contrôleur de domaine.



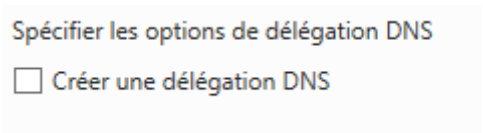
- Sélectionner Ajouter une nouvelle forêt puis indiquer le nom de domaine, ici : vekor.net.
  - Ensuite faire suivant.



- Ensuite configurer les options comme ci-contre :
  - Niveau fonctionnel : Correspond à la version Windows des postes qui seront membres du domaine. Laisser Windows Server 2016 pour un parc sous Windows 10
  - Garder la fonctionnalité Serveur DNS
  - Indiquer un mot de passe qui servira à entrer en mode DSRM (Mode de récupération des services d'annuaire). Utile pour restaurer une sauvegarde, le mot de passe ne doit surtout pas être perdu !

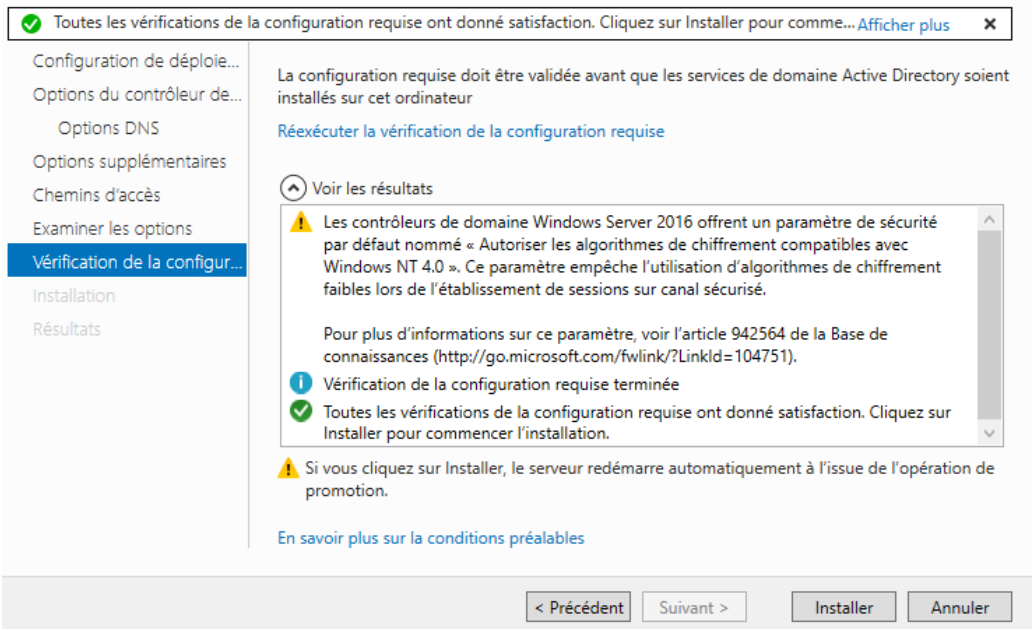


- Au niveau des options de délégation DNS, laisser décocher la case Créer une délégation DNS, ne pas prendre en compte l'erreur qui apparait.

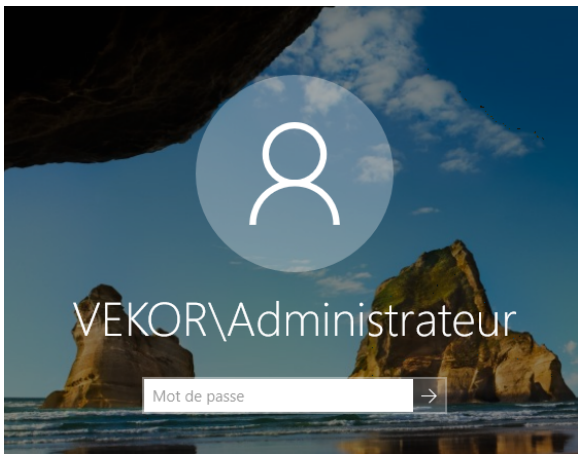


- Ensuite, il faut indiquer l'équivalent NetBIOS pour les anciens appareils qui ne gèrent pas les noms de domaines qualifiés. Par exemple, pour « vekor.local » on choisit le NetBIOS « VEKOR ». C'est le choix qui doit vous etre proposer par défaut.

- Faire suivant jusqu’à atteindre la page de vérification de la configuration requise pour l’installation des services AD.
- Le serveur valide la alors configuration, cliquer sur installer.
- Le serveur redémarre à la fin de l’installation.



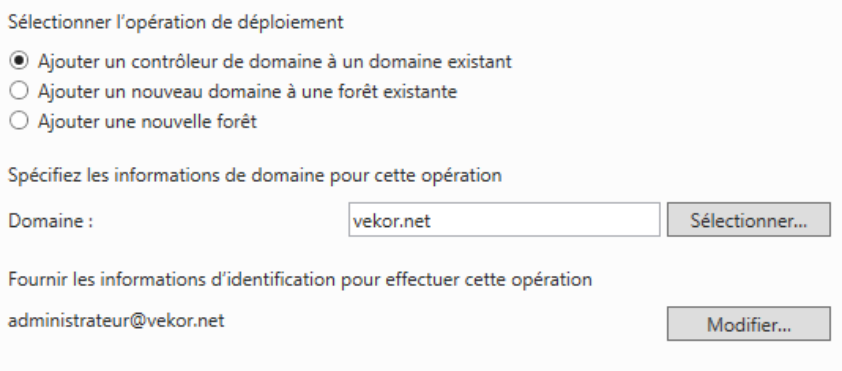
- Une fois que le serveur a redémarré, on peut maintenant se connecter sur le domaine.
- Le mot de passe du compte Administrateur du domaine est celui qui créé lors de l’installation du Windows Serveur.



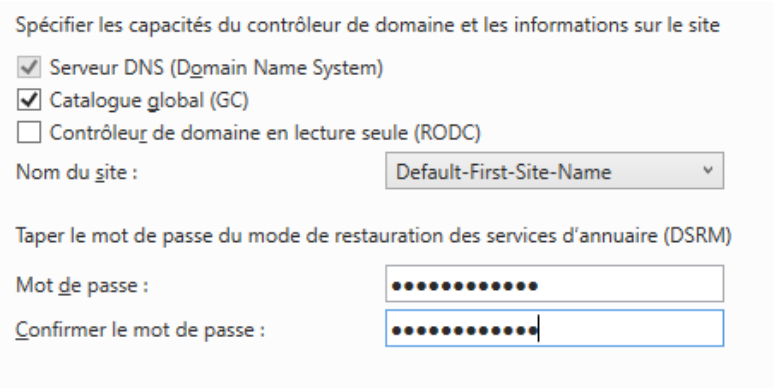
Installation du service AD DS redondant

Maintenant que le service principal est en place sur le serveur principale, nous allons voir l'installation du service AD DS sur le serveur secondaire, ici SRVDC2. Pour l'installation, il faut suivre la même procédure que pour le serveur principal jusqu'au niveau de la promotion du serveur en contrôleur de domaine.

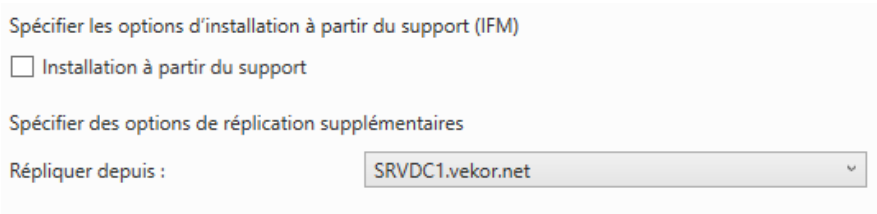
- Opération de déploiement : Choisir "Ajouter un contrôleur de domaine à un domaine existant".
  - Indiquer le domaine existant, ici vekor.net
  - Indiquer les informations d'identifications de l'administrateur du domaine vekor.net



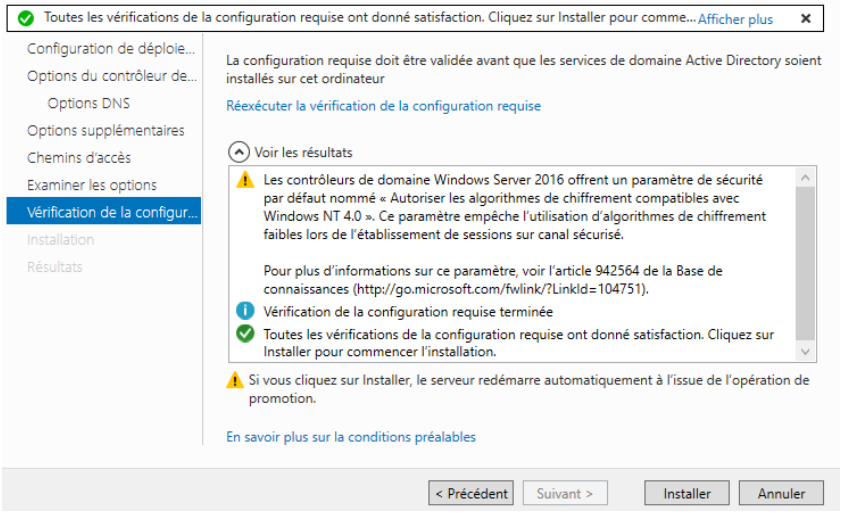
- On indique de nouveau un mot de passe pour le mode de restauration de l'annuaire puis suivant.



- Pour les options de réplications, on indique de répliquer depuis le serveur principal.
  - Ici : SRVDC1.vekor.net

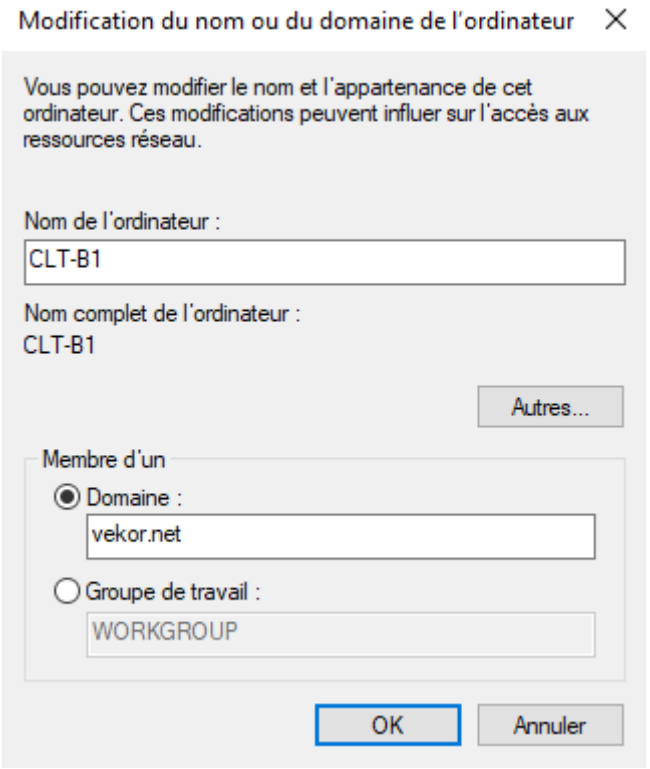


- Enfin, le serveur effectue des vérifications avant de valider l'installation.
  - A la fin de l'installation, le serveur va redémarrer et sera joint automatiquement au domaine.



Joindre un poste au domaine

S’assurer que le poste communique bien avec le serveur AD (ping FQDN)
- Aller dans les propriétés système (touche Windows + pause) → Modifier les paramètres → Modifier… → Sélectionner membre d’un domaine → Entrer le nom du domaine.
- Le contrôleur de domaine indique alors de s’identifier avec un compte administrateur du domaine pour valider l’intégration.
- Ensuite le client redémarre, on se connecte avec un utilisateur du domaine pour vérifier.

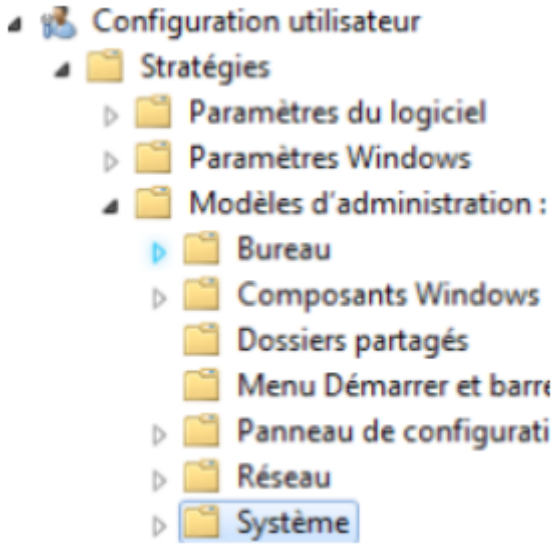


GPO

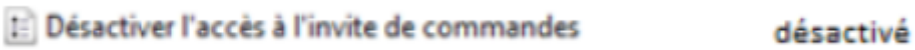
GPO

Blocage du CMD

- Modifier la GPO et parcourez l'arborescence des paramètres de cette façons
  - Configuration utilisateur -> stratégie -> modèles d'administration -> système

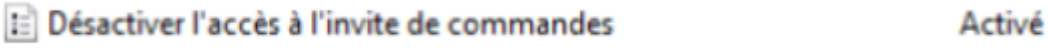


- Une liste d'options s'affiche sur une colonne à droite, dans cette liste est présent l'option désactiver l'accès à l'invite de commandes.



- Double cliquer sur cette option et activer le fait que l'accès a l'invite de commande soit désactiver.
  - Vous pouvez également ajouter une description renseignant le but de cette option.

- l'option est maintenant activée dans la liste précédente.



GPO

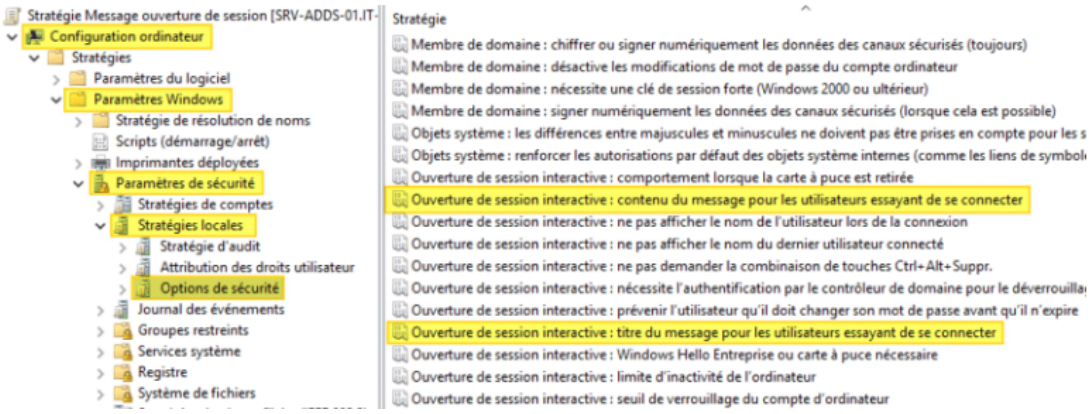
Afficher un message avant l’ouverture de session Windows

Afficher un message d'avertissement sur les postes de votre domaine pour rappeler quelques règles de bonne conduite sur l'utilisation des postes informatiques ou pour avertir les utilisateurs d'un changement ?

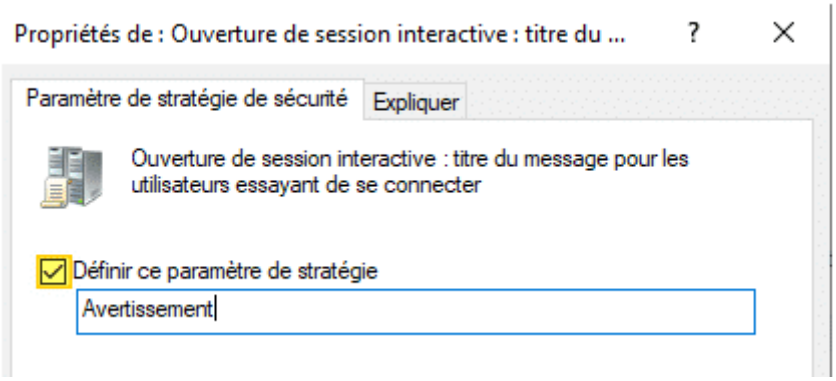
Fonctionne sur les différentes versions de Windows : Windows 7, Windows 10 ou encore Windows 11 (mais aussi les versions "Server").

À partir de la console de gestion des stratégies de groupe, créez une nouvelle GPO nommée "**Message ouverture de session**" liée directement à l’OU sur la quel vous souhaitez que cela s’applique.

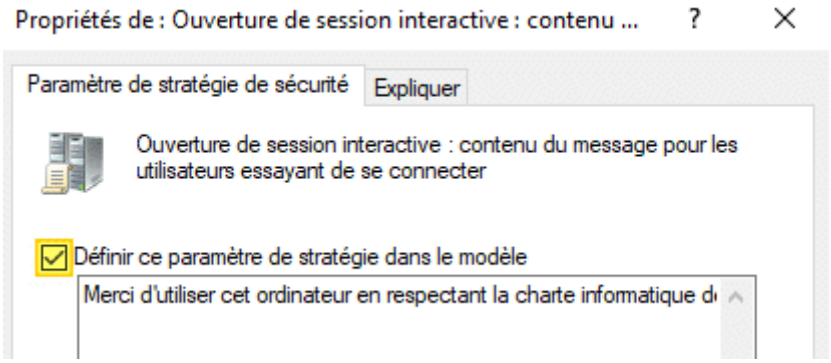
- Modifiez la GPO et parcourez l'arborescence des paramètres de cette façon
  - Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Option de sécurité



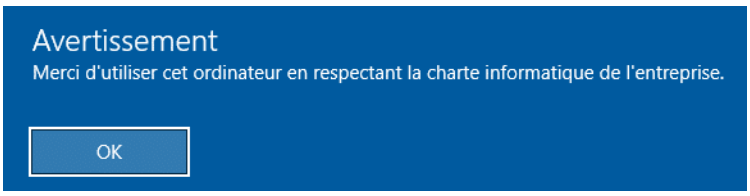
- Commençons par le paramètre permettant de configurer le titre,
  - Editer et activer en cochant l'option "Définir ce paramètre de stratégie" et de renseigner en indiquant le titre dans la zone de saisie. Par exemple : "Avertissement" :



- Le second paramètre va permettre de définir le contenu du message.
  - Par exemple : "Merci d'utiliser cet ordinateur en respectant la charte informatique de l'entreprise.".



- Vérification :

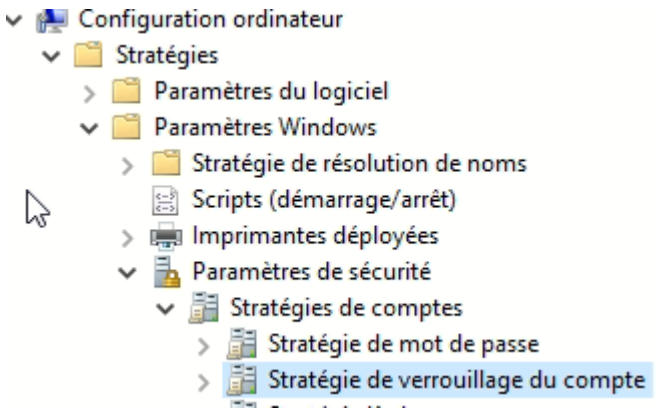


GPO

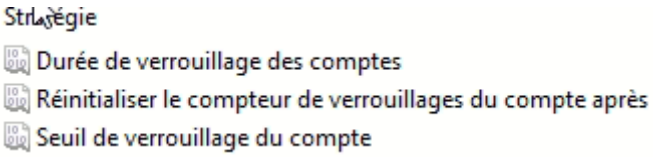
Stratégie de verrouillage des comptes

À partir de la console de gestion des stratégies de groupe, créez une nouvelle GPO nommée "**Verrouillage des comptes**" liée directement à la racine de votre domaine afin de sécuriser l'ensemble des utilisateurs

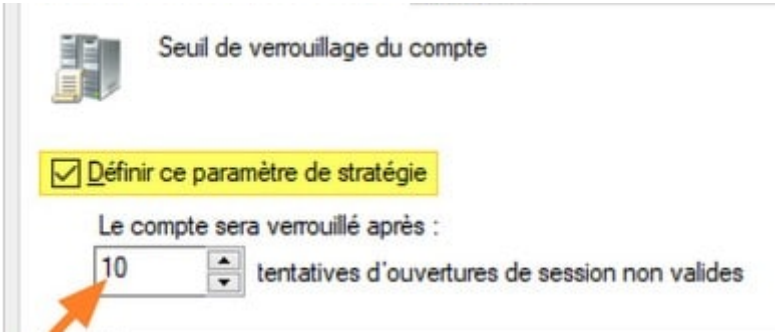
- Modifiez la GPO et parcourez l'arborescence des paramètres de cette façon :
  - Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de verrouillage du compte



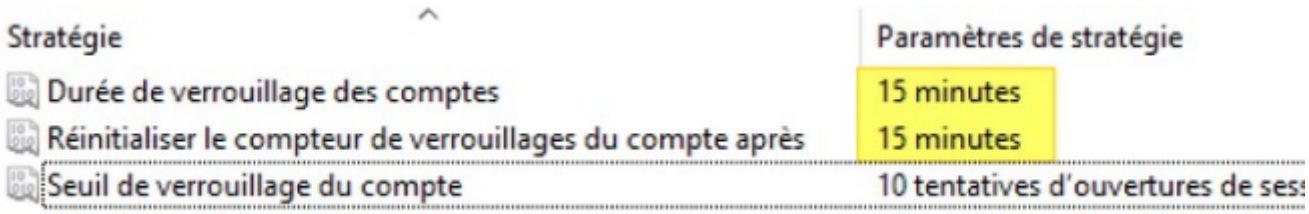
- Seuil de verrouillage du compte : au bout de combien de tentatives d'ouvertures de session non valides faut-il verrouiller le compte ?
- Réinitialiser le compteur de verrouillages du compte après : ce paramètre détermine l'intervalle de temps pendant lequel on doit compter les tentatives en échecs avant de remettre le compte à zéro. L'idée étant de ne pas compter indéfiniment, car sinon le compte finira forcément par se verrouiller si l'utilisateur se trompe de mot de passe une fois de temps en temps.
- Durée de verrouillage de comptes : pendant combien de temps faut-il verrouiller le compte ?



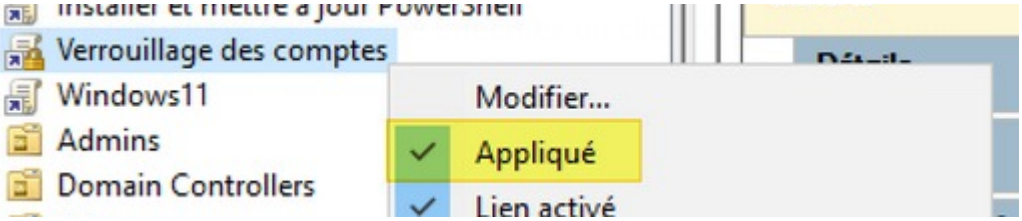
- Modifier le paramètre "Seuil de verrouillage du compte" afin de l'activer en cochant "Définir ce paramètre de stratégie". Ensuite, indiquez "10" pour que le compte soit verrouillé après 10 tentatives en échecs.



- Modifiez les deux autres paramètres en mettant 15 minutes à chaque fois. Vous devez obtenir cette configuration :



- La GPO est "Appliqué".

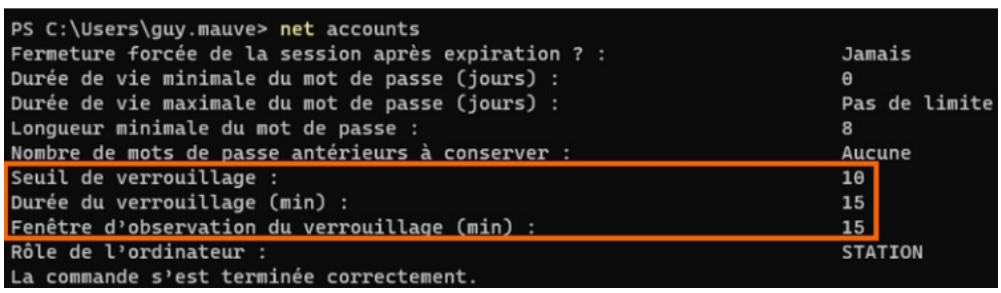


Vérifier que la GPO s'applique bien

Rendez-vous sur un poste de travail où s'applique la GPO afin de se connecter avec un utilisateur. Avant toute chose, il faut effectuer un "gpupdate /force" et redémarrer la machine (Non obligatoire sur cette GPO).

Ouvrir une fenetre CMD est exécuter

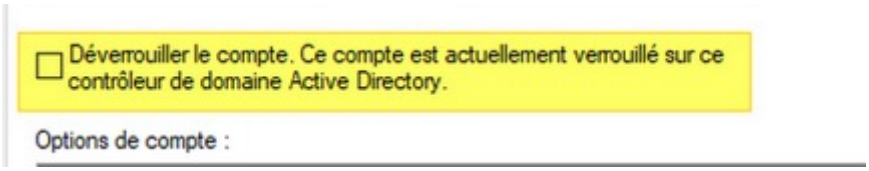
```
net accounts
```



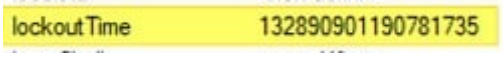
Déverrouillée un compte dans l'AD

Au bout de X tentatives en échecs, le compte va se verrouiller. Windows affichera un message pour préciser que le compte est verrouillé. "Par mesure de sécurité, le compte de l'utilisateur a été verrouillé suite à un nombre excessif de tentatives de connexion ou de modification du mot de passe. Attendez un peu avant de réessayer, ou contactez votre administrateur système ou votre service de support technique."

Dans les propriétés du compte utilisateur, dans l'onglet « Compte » :
"Déverrouiller le compte. Ce compte est actuellement verrouillé sur ce contrôleur de domaine Active Directory".
Pour déverrouiller le compte sans attendre la fin du temps imparti, il faut cocher l'option et valider.



Si l'on veut en savoir un peu plus sur ce verrouillage de compte, il faut basculer sur l'éditeur d'attributs. L'attribut "lockoutTime" indique la date et l'heure à laquelle a eu lieu cet incident de sécurité.



Ce timestamp peut-être converti avec la commande suivante :

```
w32tm.exe /ntte 132890901190781735
```