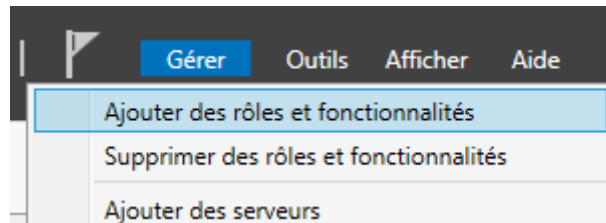


Services Active Directory DS

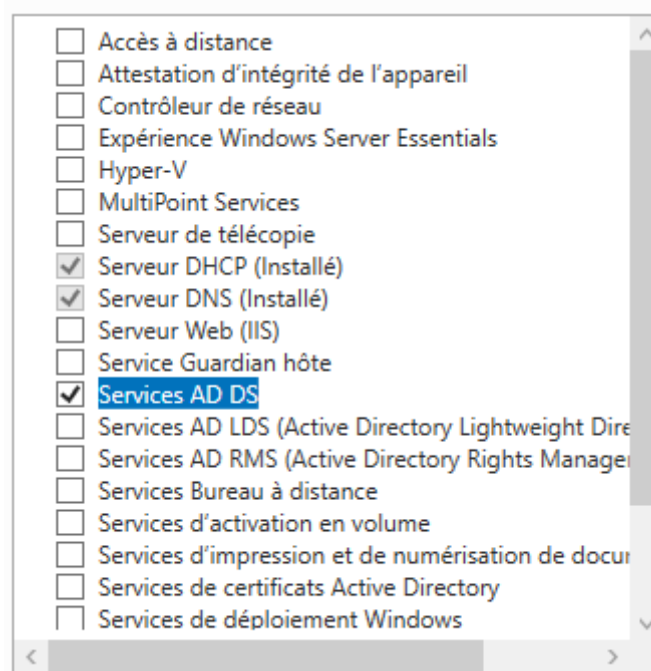
- [Installation du service AD DS](#)
- [Installation du service AD DS redondant](#)
- [Joindre un poste au domaine](#)
- [GPO](#)
 - [Blocage du CMD](#)
 - [Afficher un message avant l'ouverture de session Windows](#)
 - [Stratégie de verrouillage des comptes](#)

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.

Afficher la progression de l'installation

i Installation de fonctionnalité

Configuration requise. Installation réussie sur SRVDC1.

Services AD DS

Des étapes supplémentaires sont requises pour faire de cet ordinateur un contrôleur de domaine.

[Promouvoir ce serveur en contrôleur de domaine](#)

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

Sélectionner l'opération de déploiement

- ☐ Ajouter un contrôleur de domaine à un domaine existant
- ☐ Ajouter un nouveau domaine à une forêt existante
- ☒ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Nom de domaine racine :

- 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 !

Sélectionner le niveau fonctionnel de la nouvelle forêt et du domaine racine

Niveau fonctionnel de la forêt :

Niveau fonctionnel du domaine :

Spécifier les fonctionnalités de contrôleur de domaine

☒ Serveur DNS (Domain Name System)

☒ Catalogue global (GC)

☐ Contrôleur de domaine en lecture seule (RODC)



Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

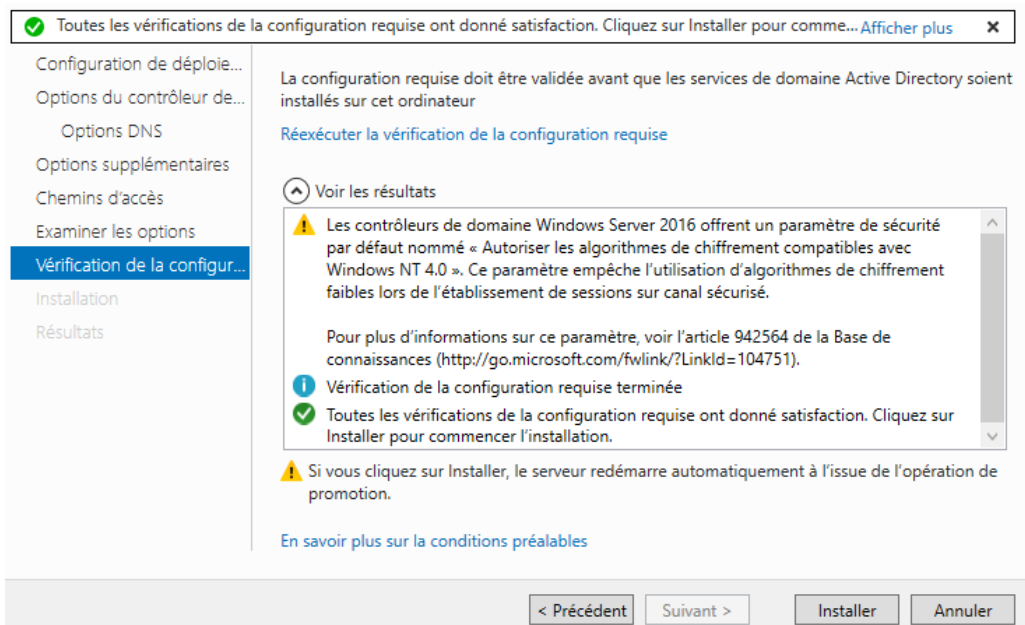
- Au niveau des options de délégation DNS, laisser décocher la case Créer une délégation DNS, ne pas prendre en compte l'erreur qui apparaît.

Spécifier les options de délégation DNS

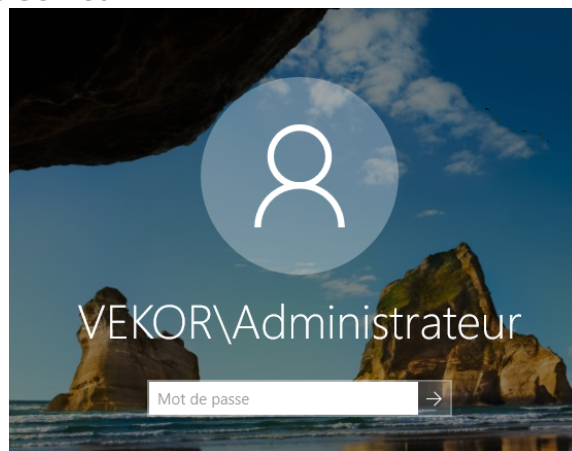
☐ Créer une délégation DNS

- 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 être proposé par défaut.

- Faire suivre jusqu'à atteindre la page de vérification de la configuration requise pour l'installation des services AD.
- Le serveur valide la 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 a été 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

Sélectionner l'opération de déploiement

☒ Ajouter un contrôleur de domaine à un domaine existant
☐ Ajouter un nouveau domaine à une forêt existante
☐ Ajouter une nouvelle forêt

Spécifiez les informations de domaine pour cette opération

Domaine :

Fournir les informations d'identification pour effectuer cette opération

administrateur@vekor.net

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

Spécifier les capacités du contrôleur de domaine et les informations sur le site

☒ Serveur DNS (Domain Name System)
☒ Catalogue global (GC)
☐ Contrôleur de domaine en lecture seule (RODC)

Nom du site :

Taper le mot de passe du mode de restauration des services d'annuaire (DSRM)

Mot de passe :

Confirmer le mot de passe :

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

Spécifier les options d'installation à partir du support (IFM)

☐ Installation à partir du support

Spécifier des options de réplication supplémentaires

Répliquer depuis :

- 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.

Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation. [Afficher plus](#)

Configuration de déploiement...

Options du contrôleur de domaine...

Options DNS

Options supplémentaires

Chemins d'accès

Examiner les options

Vérification de la configuration requise

Installation

Résultats

La configuration requise doit être validée avant que les services de domaine Active Directory soient installés sur cet ordinateur

[Réexécuter la vérification de la configuration requise](#)

Voir les résultats

⚠ Les contrôleurs de domaine Windows Server 2016 offrent un paramètre de sécurité par défaut nommé « Autoriser les algorithmes de chiffrement compatibles avec Windows NT 4.0 ». Ce paramètre empêche l'utilisation d'algorithmes de chiffrement faibles lors de l'établissement de sessions sur canal sécurisé.

Pour plus d'informations sur ce paramètre, voir l'article 942564 de la Base de connaissances (<http://go.microsoft.com/fwlink/?LinkId=104751>).

ℹ Vérification de la configuration requise terminée

✓ Toutes les vérifications de la configuration requise ont donné satisfaction. Cliquez sur Installer pour commencer l'installation.

⚠ Si vous cliquez sur Installer, le serveur redémarre automatiquement à l'issue de l'opération de promotion.

[En savoir plus sur la conditions préalables](#)

< Précédent

Suivant >

Installer

Annuler

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.

Modification du nom ou du domaine de l'ordinateur ✕

Vous pouvez modifier le nom et l'appartenance de cet ordinateur. Ces modifications peuvent influencer sur l'accès aux ressources réseau.

Nom de l'ordinateur :
CLT-B1

Nom complet de l'ordinateur :
CLT-B1

Autres...

Membre d'un

☒ Domaine :
vekor.net

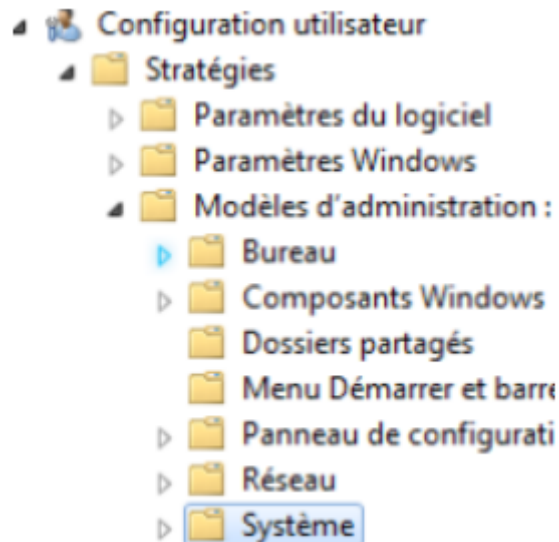
☐ Groupe de travail :
WORKGROUP

OK Annuler


GPO

Blocage du CMD

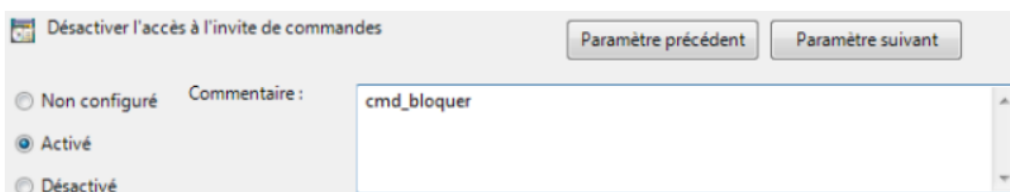
- Modifier la GPO et parcourez l'arborescence des paramètres de cette façon
 - Configuration utilisateur -> stratégie -> modèles d'administration -> système




- 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.

 Désactiver l'accès à l'invite de commandes **désactivé**

- Double cliquer sur cette option et activer le fait que l'accès à 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.

 Désactiver l'accès à l'invite de commandes **Activé**

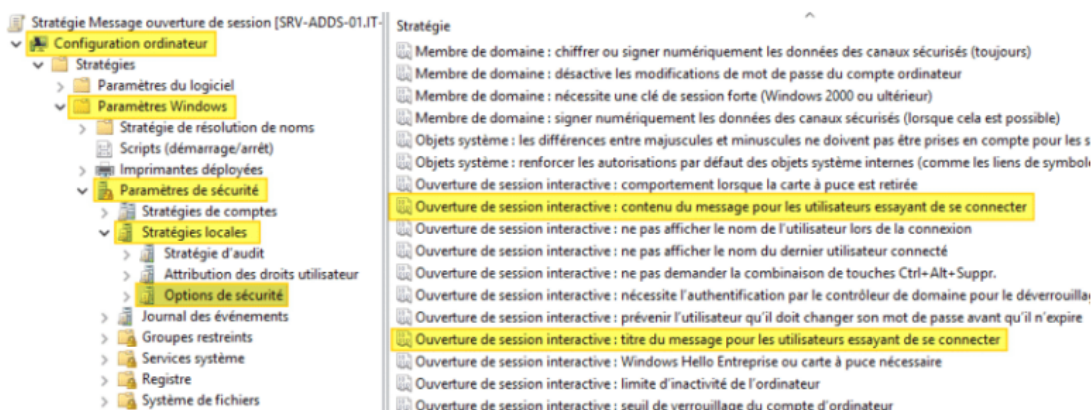
Afficher un message avant l'ouverture de session Windows

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" :

Propriétés de : Ouverture de session interactive : titre du ... ? X

Paramètre de stratégie de sécurité Expliquer

 Ouverture de session interactive : titre du message pour les utilisateurs essayant de se connecter


☒ Définir ce paramètre de stratégie

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."

Propriétés de : Ouverture de session interactive : contenu ... ? X

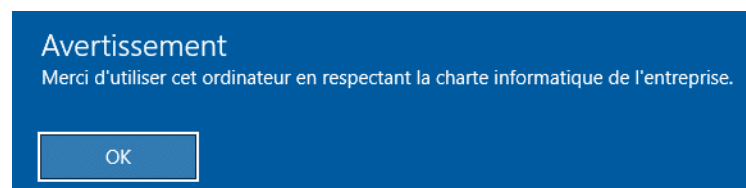
Paramètre de stratégie de sécurité Expliquer

 Ouverture de session interactive : contenu du message pour les utilisateurs essayant de se connecter

☒ Définir ce paramètre de stratégie dans le modèle

Merci d'utiliser cet ordinateur en respectant la charte informatique de l'entreprise

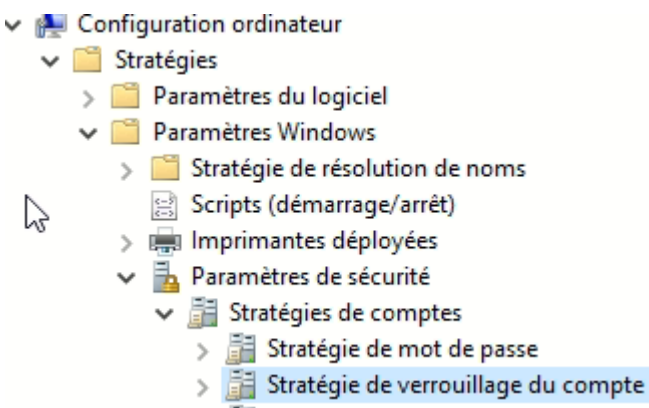
- Vérification :



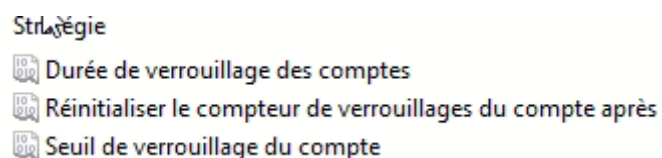
Stratégie de verrouillage des comptes

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

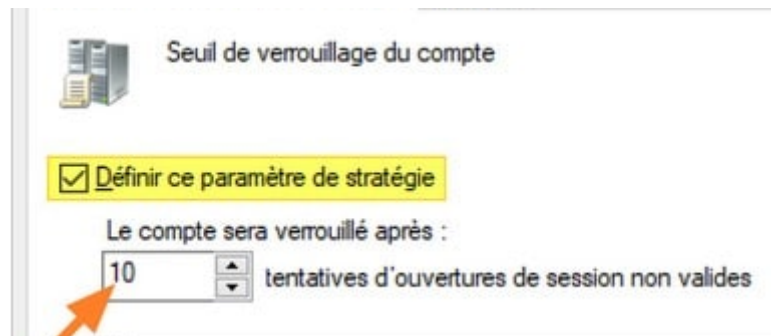
- Modifiez la GPO et parcourez l'arborescence des paramètres de cette façon :
 - Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de verrouillage du compte



- 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 ?



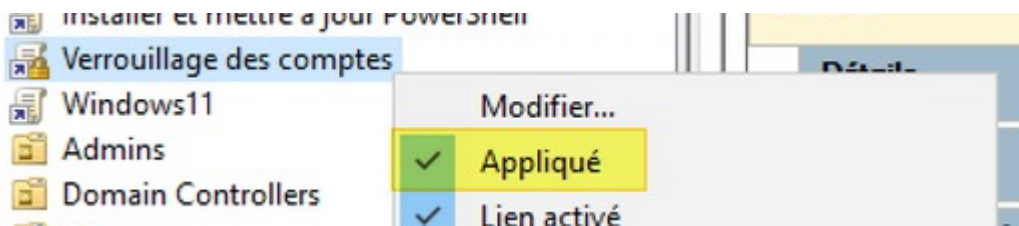
- Modifier le paramètre "Seuil de verrouillage du compte" afin de l'activer en cochant "Définir ce paramètre de stratégie". Ensuite, indiquez "10" pour que le compte soit verrouillé après 10 tentatives en échecs.



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

Stratégie	Paramètres de stratégie
Durée de verrouillage des comptes	15 minutes
Réinitialiser le compteur de verrouillages du compte après	15 minutes
Seuil de verrouillage du compte	10 tentatives d'ouvertures de ses

- 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
```

```
PS C:\Users\guy.mauve> net accounts
Fermeture forcée de la session après expiration ? : Jamais
Durée de vie minimale du mot de passe (jours) : 0
Durée de vie maximale du mot de passe (jours) : Pas de limite
Longueur minimale du mot de passe : 8
Nombre de mots de passe antérieurs à conserver : Aucune
Seuil de verrouillage : 10
Durée du verrouillage (min) : 15
Fenêtre d'observation du verrouillage (min) : 15
Rôle de l'ordinateur : STATION
La commande s'est terminée correctement.
```

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.

lockoutTime	132890901190781735
-------------	--------------------

Ce timestamp peut-être converti avec la commande suivante :

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

