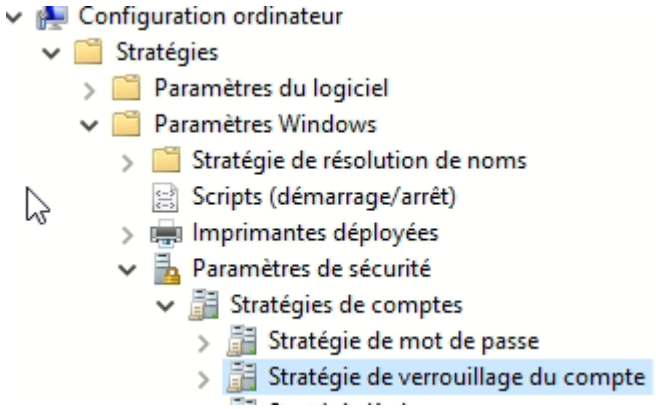
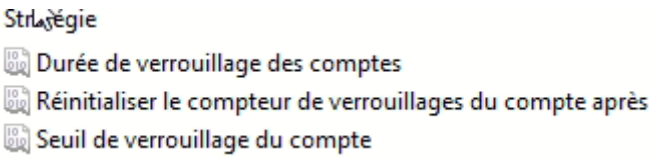
Stratégie de verrouillage des comptes

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

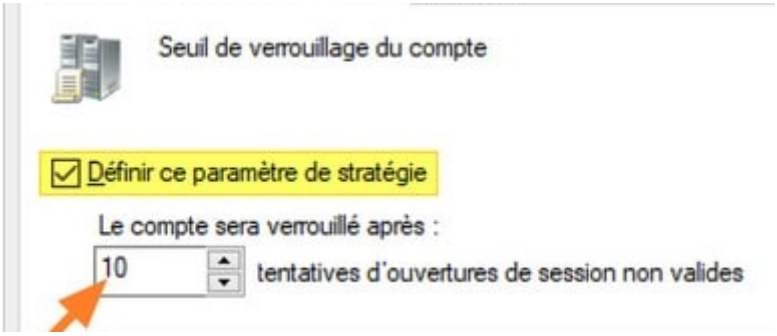
- Modifiez la GPO et parcourez l'arborescence des paramètres de cette façon :
  - Configuration ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies de comptes > Stratégie de verrouillage du compte



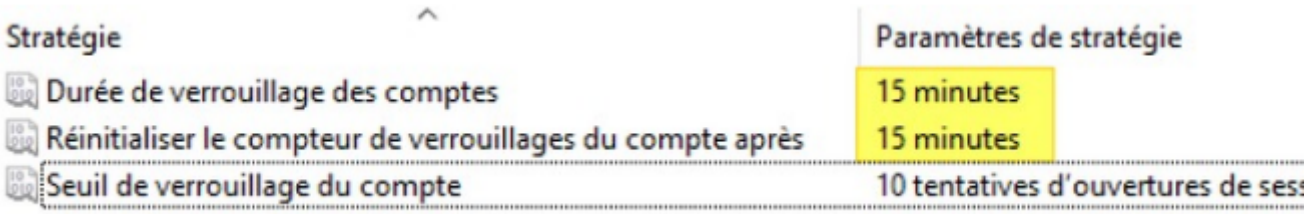
- Seuil de verrouillage du compte : au bout de combien de tentatives d'ouvertures de session non valides faut-il verrouiller le compte ?
- Réinitialiser le compteur de verrouillages du compte après : ce paramètre détermine l'intervalle de temps pendant lequel on doit compter les tentatives en échecs 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 ?



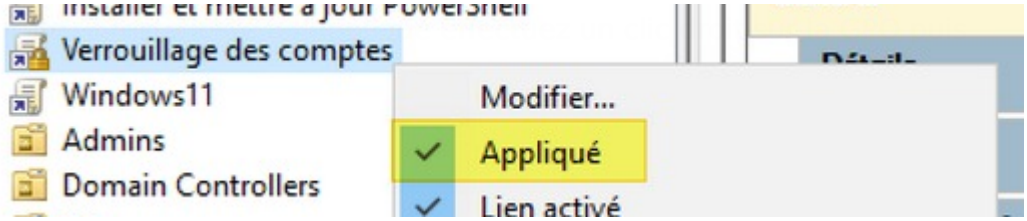
- Modifier le paramètre "Seuil de verrouillage du compte" afin de l'activer en cochant "Définir ce paramètre de stratégie". Ensuite, indiquez "10" pour que le compte soit verrouillé après 10 tentatives en échecs.



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



- La GPO est "Appliqué".

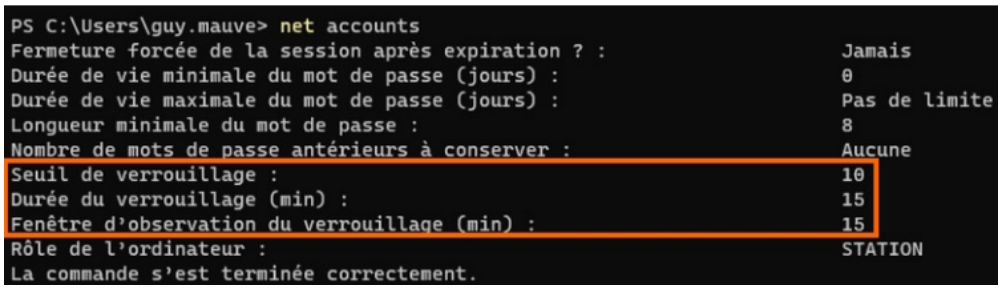


Vérifier que la GPO s'applique bien

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

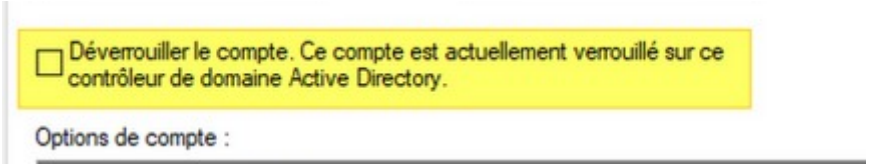
```
net accounts
```



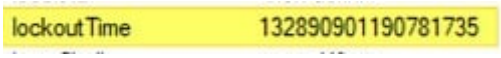
Déverrouillée un compte dans l'AD

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.

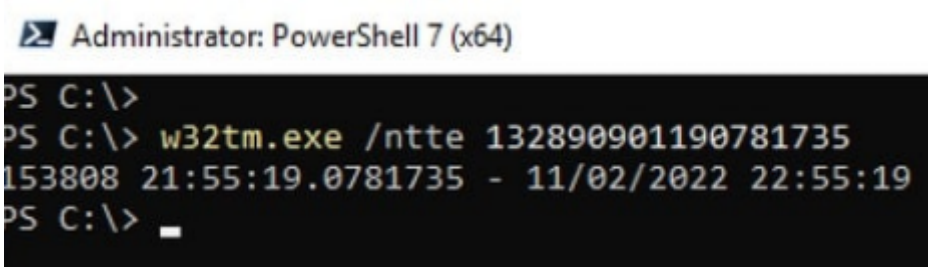


Si l'on veut en savoir un peu plus sur ce verrouillage de compte, il faut basculer sur l'éditeur d'attributs. L'attribut "lockoutTime" indique la date et l'heure à laquelle a eu lieu cet incident de sécurité.



Ce timestamp peut-être converti avec la commande suivante :

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



Revision #1
Created 2024-04-18 07:51:48 UTC by Corentin Roche
Updated 2024-04-18 07:52:53 UTC by Corentin Roche