**Gestion des objets dans l’Active Directory**

Ce laboratoire doit être fait individuellement sur l'ordinateur virtuel 2

**Objectifs**

* Utiliser la console "Utilisateurs et ordinateurs Active Directory"
* Comprendre les règles dans la nomenclature des objets et les restrictions
* Comprendre plusieurs attributs des objets

**Étape 1 - La console "Utilisateurs et ordinateurs Active Directory"**

Dans tous les laboratoires à partir de maintenant nous nommerons la console "Utilisateurs et ordinateurs Active Directory" par l’acronyme **UOAD**.

Épingler un raccourci de la console UOAD à la barre des tâches

Ouvrir la console UOAD

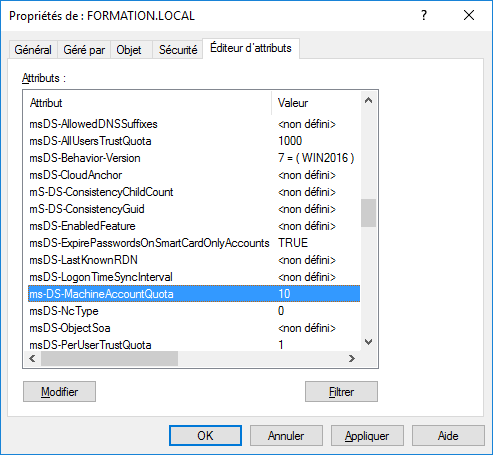
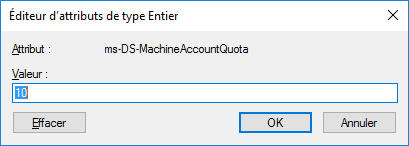
* Dans le menu Affichage, choisir l’option Fonctionnalités avancées
* Dans la rubrique "Requêtes enregistrées" créez une requête qui cherche tous les utilisateurs dont le nom commence par la lettre "a".

**Étape 2 - Empêcher un utilisateur de joindre un ordinateur au domaine**

Par défaut, un utilisateur authentifié qui n'est pas membre du groupe Administrateurs peut joindre 10 ordinateurs au domaine.

Dans la console **UOAD**

* Afficher les attributs du domaine **FORMATION.LOCAL** et sélectionner l'onglet "Éditeur d'attributs"
* Sélectionner l'attribut **ms-DS-MachineAccountQuota**
* La valeur par défaut de l'attribut **ms-DS-MachineAccountQuota** est **10**

Pour empêcher un utilisateur authentifié de joindre des ordinateurs au domaine on doit modifier la valeur de l'attribut **ms-DS-MachineAccountQuota** pour **0**.

**Étape 3 - Création d’objets**

**Protection des UO**

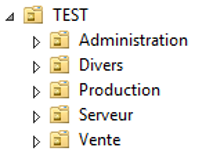
Dans la console **UOAD**

* Créer une unité d’organisation portant le nom TEST directement sous le domaine
* Dans l'onglet "Objet" de votre OU, enlever la protection contre la suppression accidentelle

**Création des UO et d’utilisateurs**

Créer la structure d’unités d’organisation suivante sous l’unité d'organisation TEST.

Pour chaque UO enlever la protection contre la suppression accidentelle.



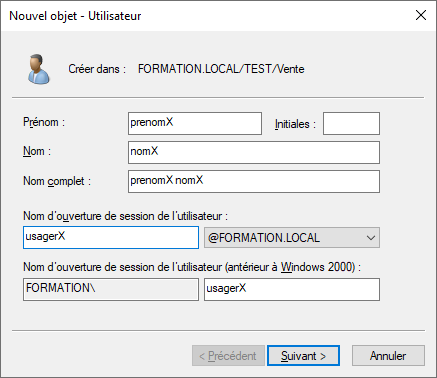
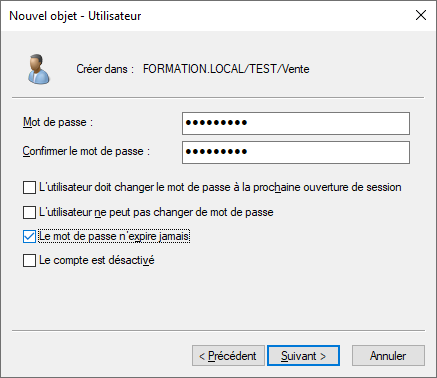
Créer trois utilisateurs dans l’unité d'organisation Vente.

**Vos trois utilisateurs auront les caractéristiques suivantes:**

* Prénom: **PrenomX**
* Nom: **NomX**
* Nom complet: **prenomX nomX**

note: par défaut, le nom complet est complété automatiquement par le système

* Nom d'ouverture de session de l'utilisateur: **usagerX**
* Donner un mot de passe complexe
* Décocher "**L'utilisateur doit changer le mot de passe à la prochaine ouverture de session**"
* Cocher "**Le mot de passe n'expire jamais**"

**Étape 4 - Modification d’objets**

Déplacer les utilisateurs **usager1, usager2 et usager3** de l’unité d’organisation Vente vers Administration.

Changer le nom de l’unité d'organisation Serveur pour Achat.

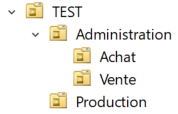
Déplacer les unités d'organisation Vente et Achat sous l'unité d'organisation Administration.

* note: ne fonctionne pas si la protection est activée

Supprimer l’unité d'organisation Divers.

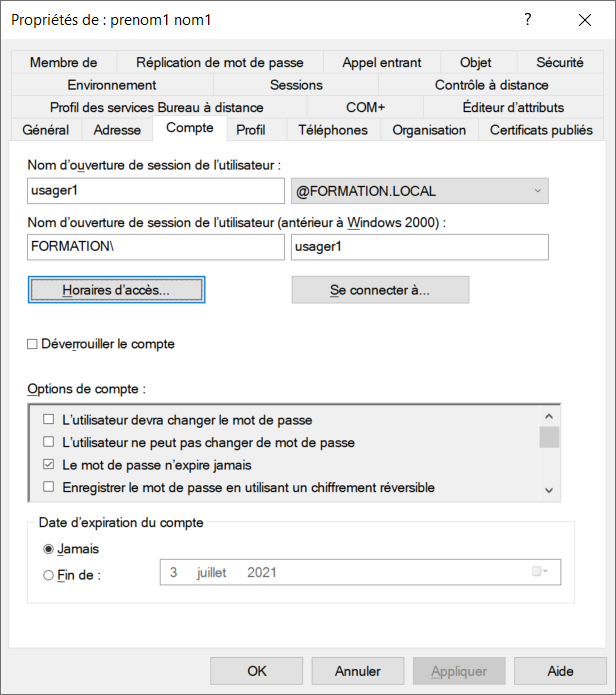
* note: ne fonctionne pas si la protection est activée

**Voici le résultat final**



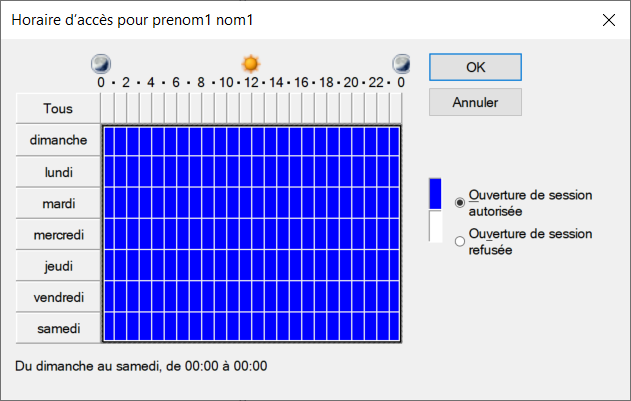
**Étape 5 - Modification des propriétés des utilisateurs**

Voici l'onglet "**Compte**" pour l'utilisateur usager1

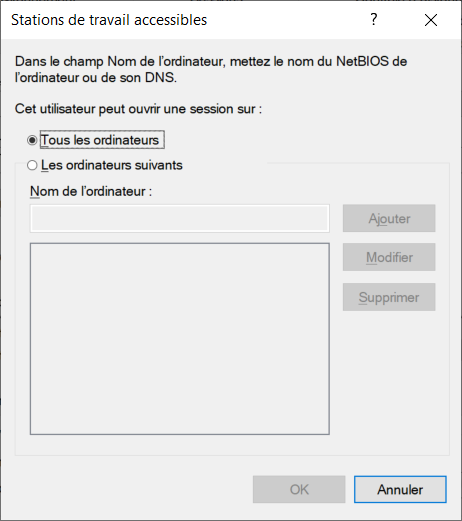


"**Date d'expiration du compte**" Par défaut, le compte d'un utilisateur n'expire jamais.

"**Horaire d'accès…**" Par défaut, un utilisateur n'a pas de restriction pour les heures d'accès.



"**Se connecter à…**" Par défaut, un utilisateur peut ouvrir une session sur tous les ordinateurs.



Autoriser l’utilisateur **usager1** de se connecter seulement sur le serveur virtuel "**SERVEUR2**".

Modifier les heures d'ouverture de session de l’utilisateur **usager2** pour 08h00 à 16h00 du lundi au vendredi seulement.

Faire expirer le compte de l’utilisateur **usager3** en date d’hier.

**Étape 6 - Critères pour la création d'un compte utilisateur**

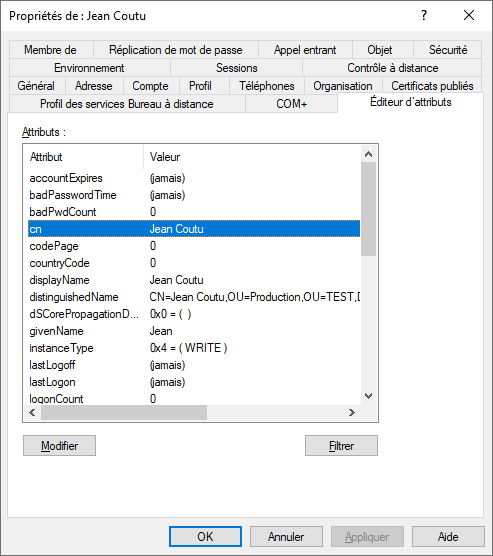
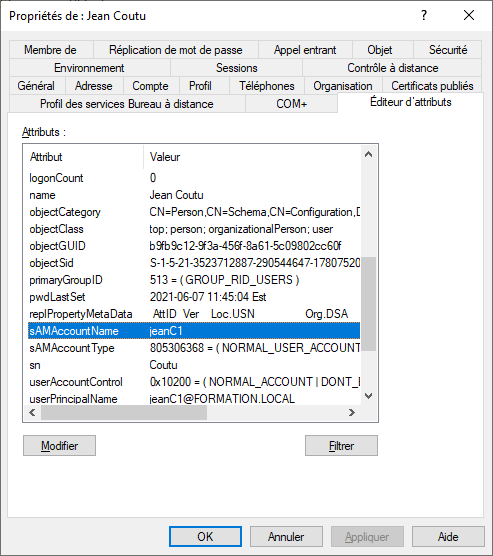
Créer un utilisateur dans l'unité d'organisation Production en indiquant les propriétés suivantes:

* Prénom: **Jean**, Nom: **Coutu**
* Nom d'ouverture de session de l'utilisateur: **jeanC1**
* Donner un mot de passe complexe et cocher "**Le mot de passe n'expire jamais**"

**Lors de la création d'un utilisateur en utilisant l'environnement graphique**

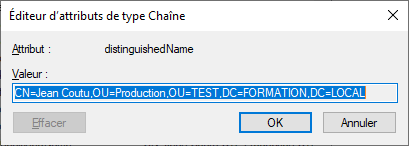
**1 – l'attribut CN contient le nom complet de l'utilisateur**

**2 – l'attribut sAMAccountName contient le nom d'ouverture de session de l'utilisateur**

L'attribut cn est identique aux attributs displayName et name.

L'attribut **distinguishedName** pour l'utilisateur **jeanC1**.

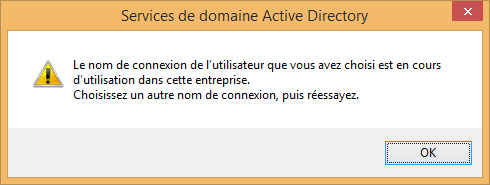


**Mise en situation des deux erreurs possibles lors de la création d'un compte utilisateur**

**Cas 1**

Si on veut créer un autre utilisateur dans l'unité d'organisation Production avec les propriétés suivantes:

* Prénom: **Jean**, Nom: **Couturier**
* Nom d'ouverture de session de l'utilisateur: **jeanC1**
* Donner un mot de passe complexe et cocher "**Le mot de passe n'expire jamais**"

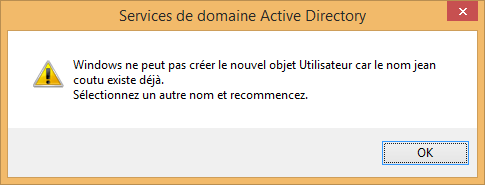


**Le nom de connexion de l'utilisateur (nom d'ouverture de session) doit être unique dans tout le domaine.**

**Cas 2**

Si on veut créer un autre utilisateur dans l'unité d'organisation Production avec les propriétés suivantes:

* Prénom: **Jean**, Nom: **Coutu**
* Nom d'ouverture de session de l'utilisateur: **jeanC2**
* Donner un mot de passe complexe et cocher "**Le mot de passe n'expire jamais**"



**Le nom de l'utilisateur doit être unique dans une OU.**

C'est parce que le nom de l'utilisateur correspond à l'attribut CN ce qui fait que l'attribut distinguishedName serait identique.

**Pour être capable de créer un utilisateur qui a le même prénom et le même nom qu'un autre utilisateur d'une OU, il faut simplement modifier le nom complet.**

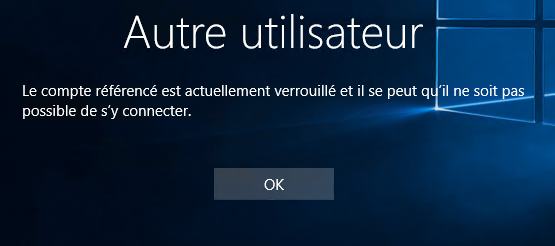
**ANNEXE**

**Exemples de problèmes d’ouverture de session**

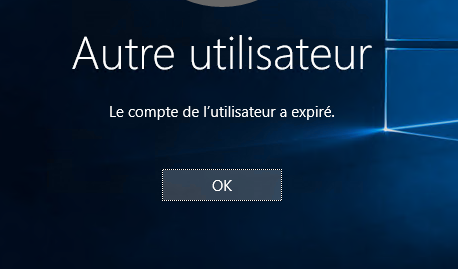
1. **Ce message s'affiche si la configuration réseau de l'ordinateur client ne permet pas de rejoindre le contrôleur de domaine.**
2. **Ce message s'affiche si la différence de temps entre l'ordinateur client et le contrôleur de domaine dépasse cinq minutes.**



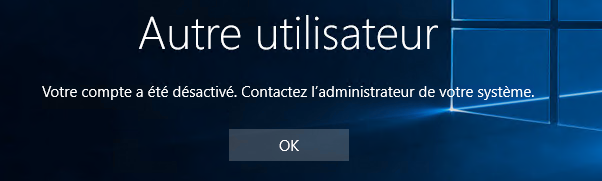
**Le compte de l'utilisateur est verrouillé.**



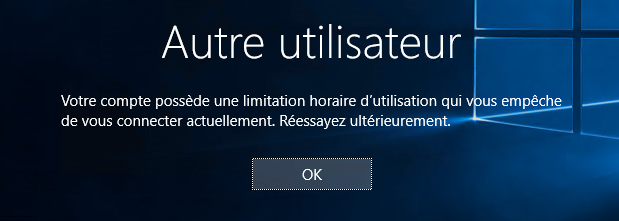
**Le compte de l'utilisateur est expiré.**



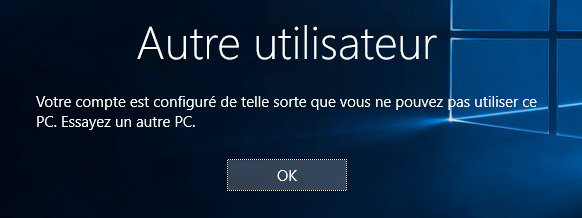
**Le compte de l'utilisateur est désactivé.**



**Le compte de l'utilisateur a été configuré avec des restrictions horaires.**



**Le compte de l'utilisateur a été configuré avec une limitation sur les postes sur lesquels il peut ouvrir une session.**



**Le message suivant indique que l'utilisateur n'est pas autorisé à se connecter localement sur ce poste.**

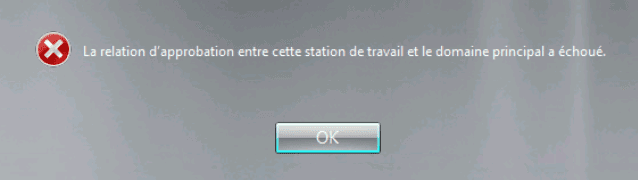
1. **Ce message s'affiche si un utilisateur tente de se connecter sur le contrôleur de domaine.**
2. **Ce message s'affiche si la paramètre "Interdire l'ouverture d'une session locale" de la GPO**

**"Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Attribution des droits utilisateur" est configuré.**



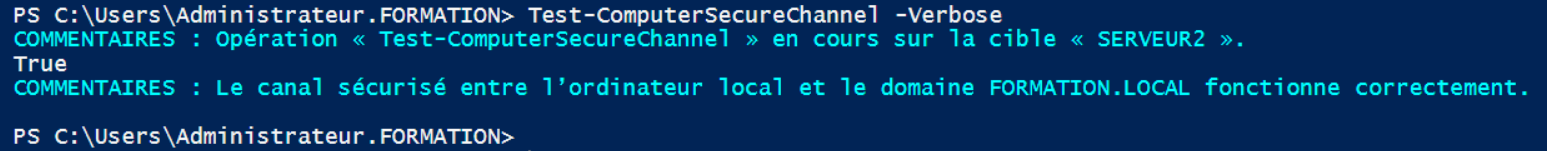
**La relation d'approbation entre cette station de travail et le domaine principal a échoué.**

* **Le compte de l'ordinateur n'est plus authentifié et il est impossible d'ouvrir une session sur le domaine.**
* **Une des raisons est probablement que l'ordinateur a été supprimé dans l'Active Directory.**



Vérification du canal sécurisé entre l'ordinateur client et le domaine FORMATION.LOCAL

L'exécution de la commande s'effectue directement sur l'ordinateur client.



**Voici plusieurs manières de régler le problème de relation d'approbation.**

**Méthode 1a**

**Il faut exécuter Test-ComputerSecureChannel sur l'ordinateur local dont la relation d'approbation n'est plus valide.**

**# Exemple simple**

**# L'exécution du code se fait sur l'ordinateur client avec un compte administrateur local**

**Test-ComputerSecureChannel -Repair `**

**–Verbose**

**# La relation d'approbation est réparée seulement si c'est nécessaire.**

**# L'exécution du code se fait sur l'ordinateur client avec un compte administrateur local**

**if (-not(Test-ComputerSecureChannel))**

**{**

**Test-ComputerSecureChannel -Repair `**

**–Verbose**

**}**

**Méthode 1b**

**Si la méthode précédente ne fonctionne pas.**

**# L'exécution du code se fait sur l'ordinateur client avec un compte administrateur local**

**$cred = Get-Credential –Username "FORMATION\Administrateur" `**

**–Message "Domaine FORMATION.LOCAL"**

**Test-ComputerSecureChannel -Credential $cred `**

**-Repair`**

**–Verbose**

**# L'exécution du code se fait sur le contrôleur de domaine**

**$ordinateur = "SERVEUR2"**

**$ localAdminCredential = Get-Credential**

**$domainCredential = Get-Credential**

**$code = { Test-ComputerSecureChannel -Repair `**

**-Credential $using:domainCredential**

**}**

**Invoke-Command -Computername $ordinateur `**

**-Credential $localAdminCredential `**

**-ScriptBlock $code**

**Méthode 2**

**Il faut exécuter Reset-ComputerMachinePassword sur l'ordinateur local dont la relation d'approbation n'est plus valide.**

**# L'exécution du code se fait sur l'ordinateur client avec un compte administrateur local**

**$cred = Get-Credential –Username "FORMATION\Administrateur" `**

**–Message "Domaine FORMATION.LOCAL"**

**Reset-ComputerMachinePassword -Server "SERVEUR1" `**

**-Credential $cred**

**Notez que cela fonctionne également même si le compte d’ordinateur a été supprimé de Active Directory.**

**Créez un compte d’ordinateur avec le même nom et Reset-ComputerMachinePassword s’assurera que le mot de passe est synchronisé.**

**# L'exécution du code se fait sur le contrôleur de domaine**

**$ordinateur = "SERVEUR2"**

**$localAdminCredential = Get-Credential**

**$domainCredential = Get-Credential**

**$code = { Reset-ComputerMachinePassword -Server "SERVEUR1" `**

**-Credential $using:domainCredential**

**}**

**Invoke-Command -Computername $ordinateur `**

**-Credential $localAdminCredential `**

**-ScriptBlock $code**

**Méthode 3**

1. Il faut sortir l'ordinateur du domaine.
2. Il faut joindre l'ordinateur au domaine.