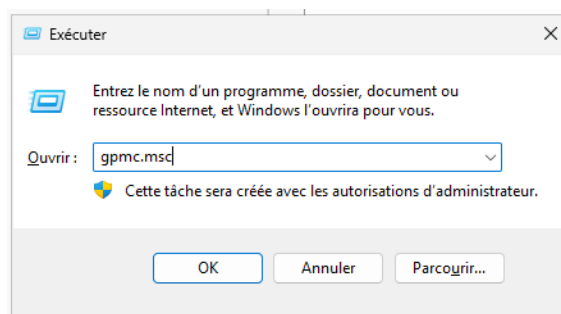


FICHE 4 – DÉPLOIEMENT DE STRATÉGIES DE GROUPE (GPO) SUR LE SERVEUR

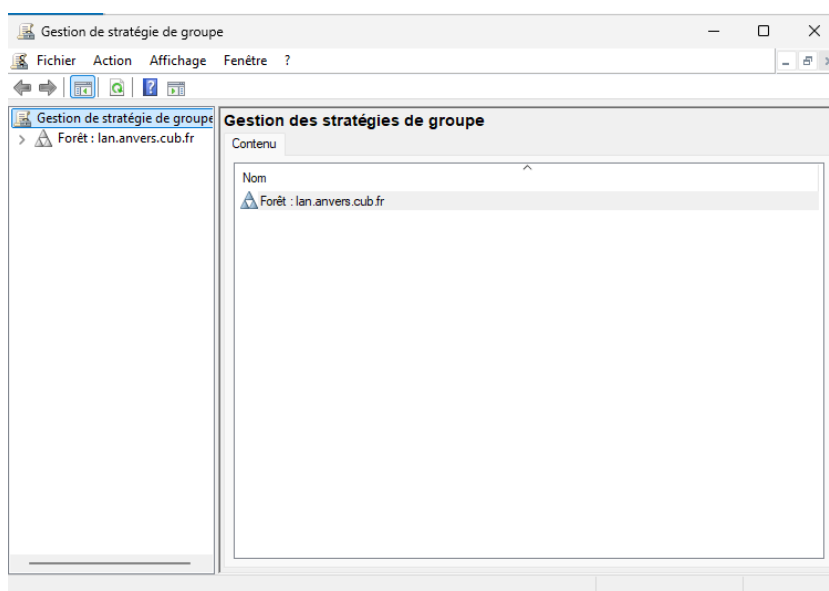
Table des matières

ACTIVER LA PRISE EN CHARGE DES CERTIFICATS ECC (GÉNÉRÉS À PARTIR D'ALGORITHMES DE CHIFFREMENT À COURBES ELLIPTIQUES).....	3
ACTIVER LE VERROUILLAGE DE SESSION LORSQUE QU'UNE CLÉ EST RETIRÉE D'UNE MACHINE.....	5
ACTIVER L'INSCRIPTION AUTOMATIQUE POUR LES MACHINES ET LES UTILISATEURS DU DOMAINE CONCERNÉS.....	9
FORCER L'AUTHENTIFICATION PAR CLÉ UNIQUEMENT.....	12
EMPÊCHER L'AUTHENTIFICATION SUR UNE MACHINE.....	13

Sur le serveur Windows, taper sur les touches "Windows + r" ou faire un clic droit sur l'icône Windows Démarrer puis sélectionner "Exécuter". Enfin, saisir gpmmc.msc et appuyer sur la touche Entrée.



Descendre dans l'arborescence puis choisir une stratégie déjà existante ou créer une nouvelle stratégie de groupe associée à une unité d'organisation.

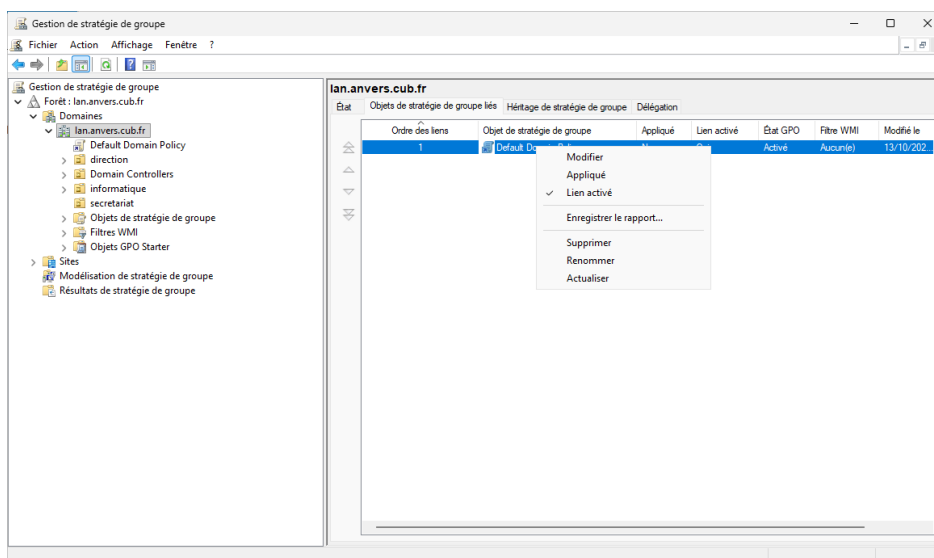
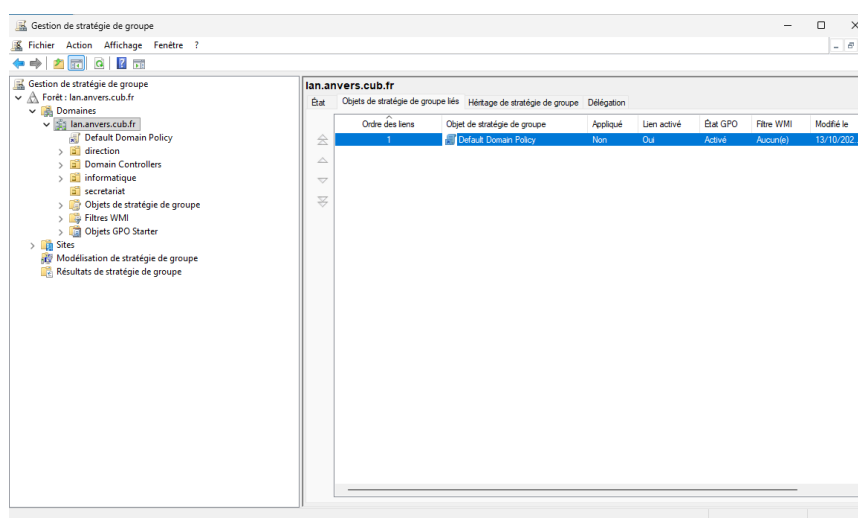


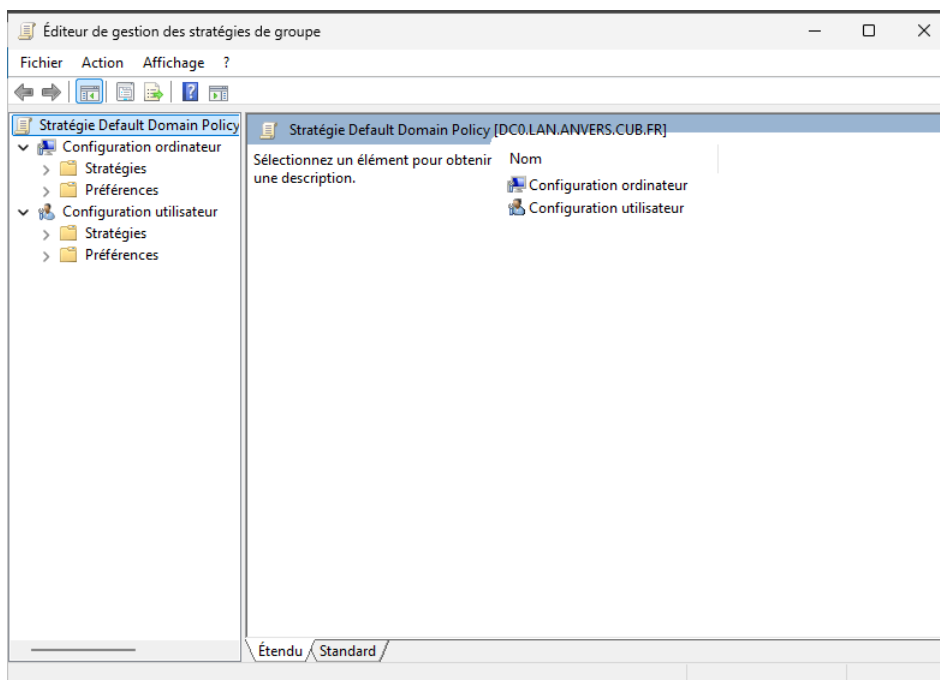
ACTIVER LA PRISE EN CHARGE DES CERTIFICATS ECC (GÉNÉRÉS À PARTIR D'ALGORITHMES DE CHIFFREMENT À COURBES ELLIPTIQUES).



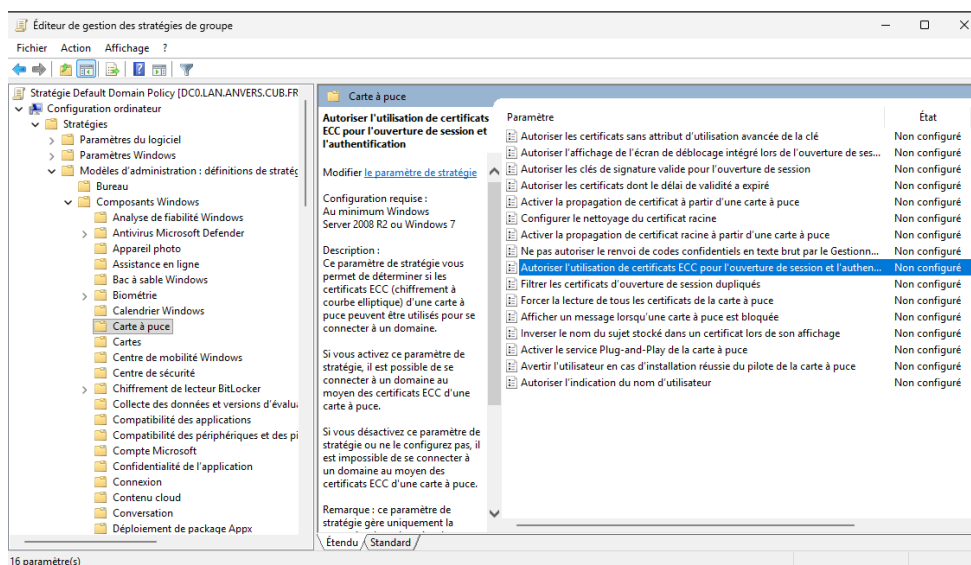
Attention ! Les bonnes pratiques Microsoft recommandent de déployer de façon séparée les stratégies de groupe à appliquer aux machines de celles à appliquer aux utilisateurs.

Ce paramétrage est à appliquer sur les machines concernées par l'authentification SmartCard/PIV. Il est nécessaire de créer une nouvelle stratégie que l'on appliquera sur l'unité d'organisation adéquate. L'exemple fourni ci-dessous est donc à réadapter.

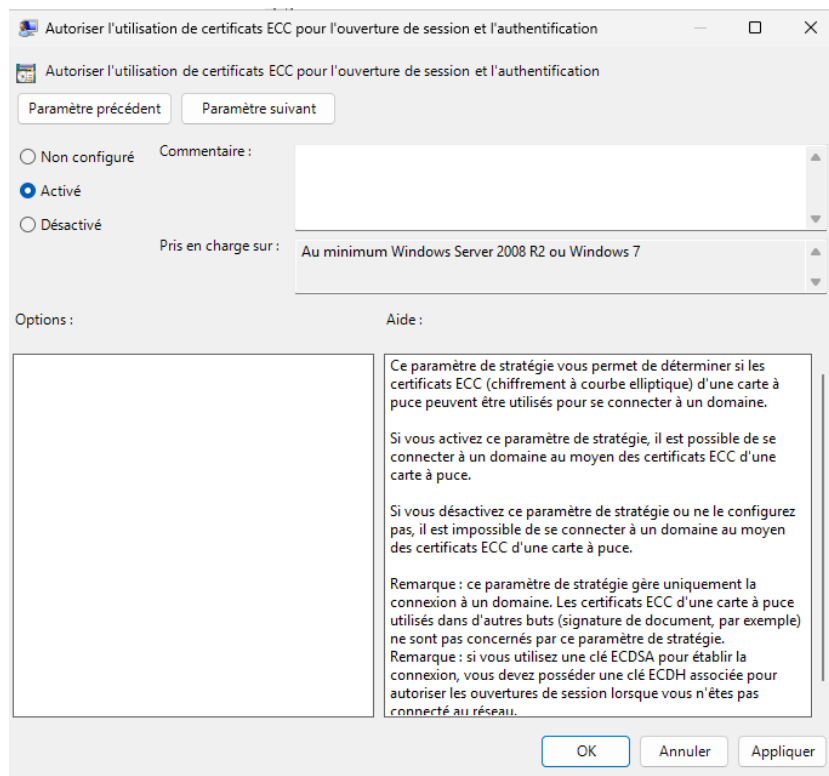




Dans la stratégie de groupe choisie, sélectionner **Configuration Ordinateur > Stratégies > Modèles d'administration > Composants Windows > Carte à puce > Autoriser l'utilisation de certificats ECC pour l'ouverture de session et l'authentification**.

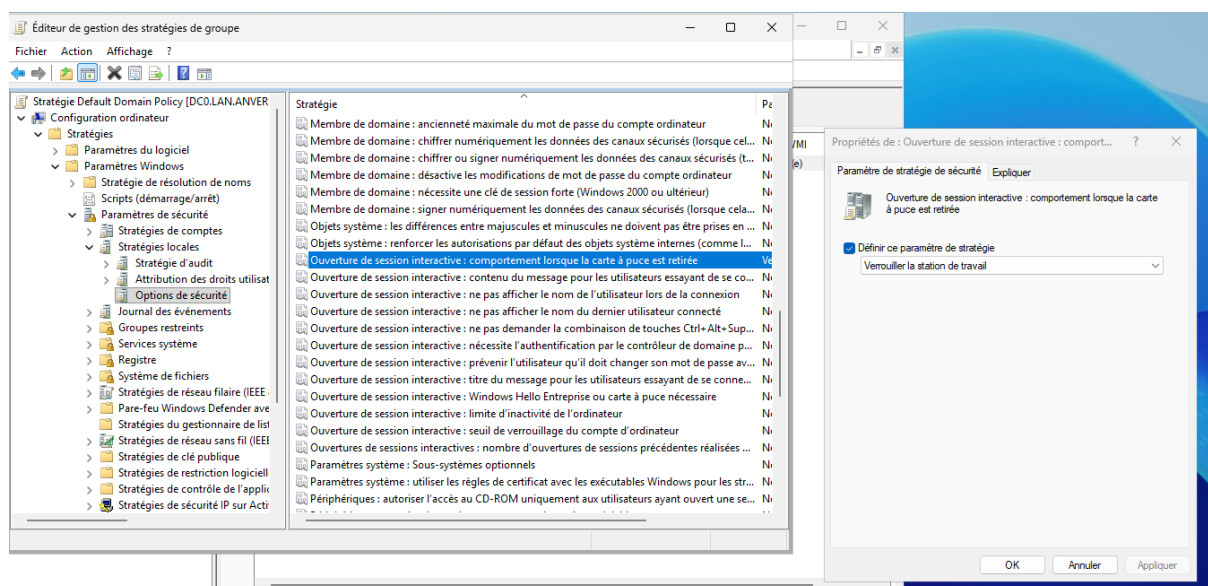


Éditer le paramètre et sélectionner Activer puis Appliquer et OK.



ACTIVER LE VERROUILLAGE DE SESSION LORSQUE QU'UNE CLÉ EST RETIRÉE D'UNE MACHINE

Dans la stratégie choisie, sélectionner **Configuration Ordinateur > Stratégies > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Options de sécurité > Ouverture de session interactive : comportement lorsque la carte à puce est retirée**.



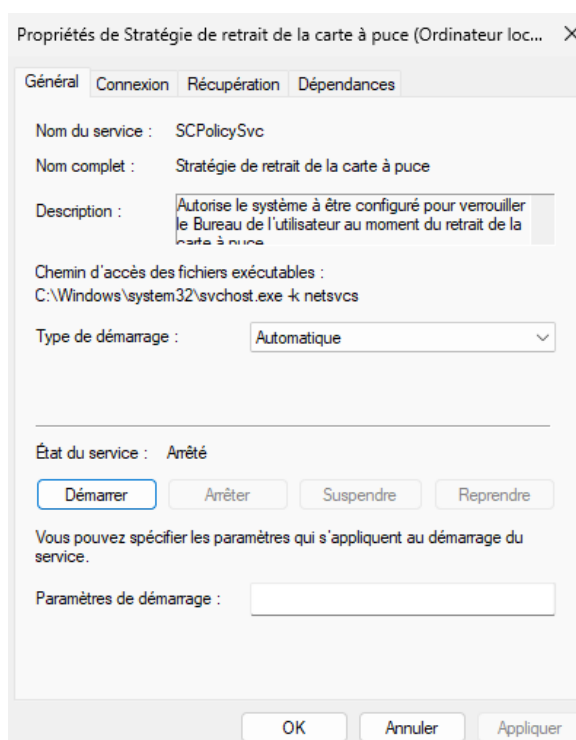
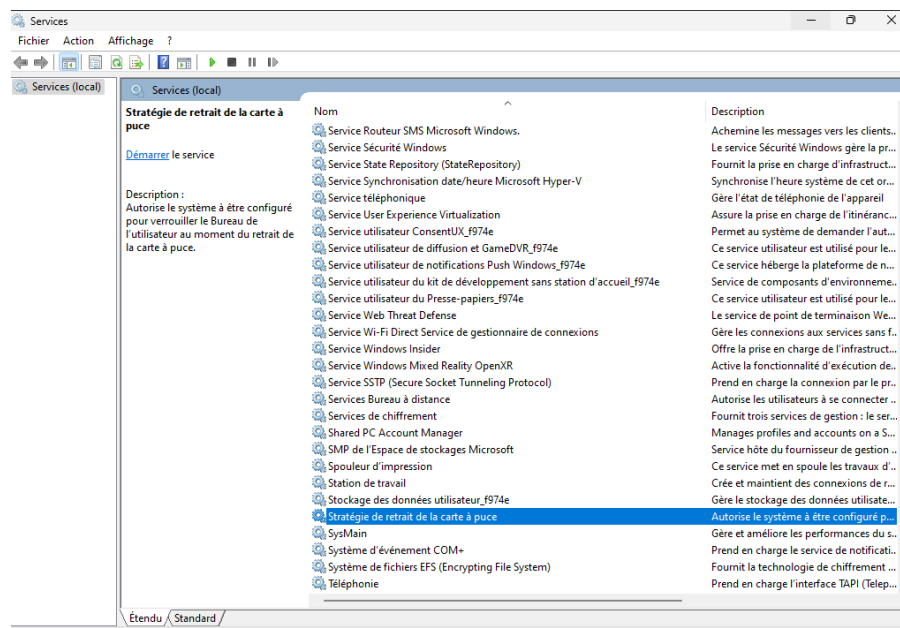
Cocher **Définir ce paramètre de stratégie** et sélectionner **Verrouiller la station de travail**.

Sur les postes clients, il faut également s'assurer que le service « *Stratégie de retrait de la carte à puce* » soit correctement démarré. Pour cela, deux possibilités :

- Se connecter en tant qu'administrateur sous Windows 11 et ouvrir le gestionnaire de services à l'aide du raccourci clavier *Windows+r* puis taper *services.msc*.
- Automatiser le démarrage du service via le contrôleur de domaine Windows et les stratégies de groupe.

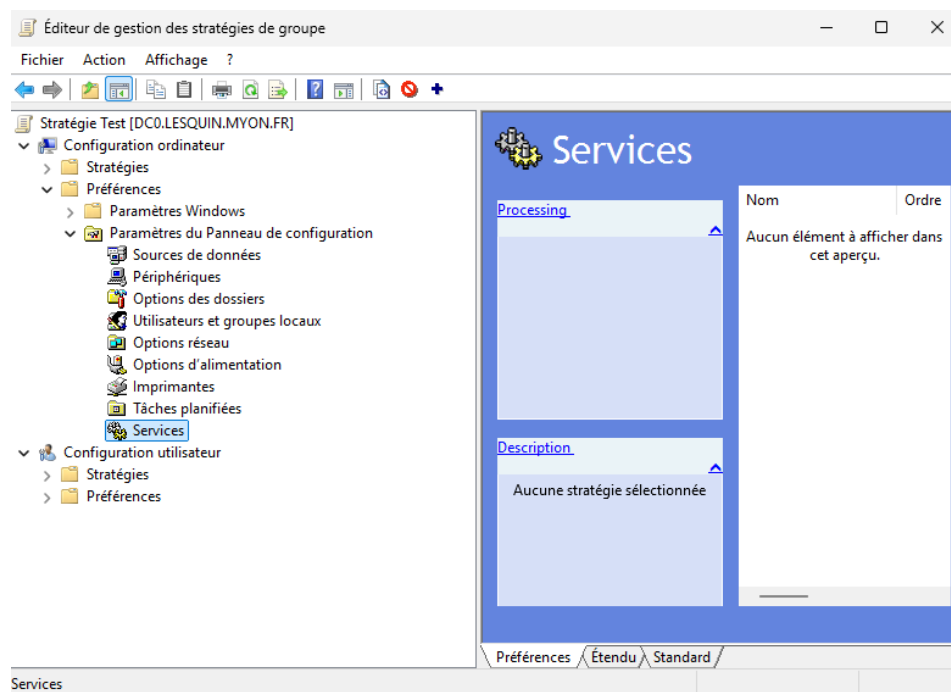
Vérification manuelle du démarrage du service sur le poste

Rechercher le service « *Stratégie de retrait de la carte à puce* » puis double-cliquer dessus et s'assurer que le service est en **démarrage automatique**.

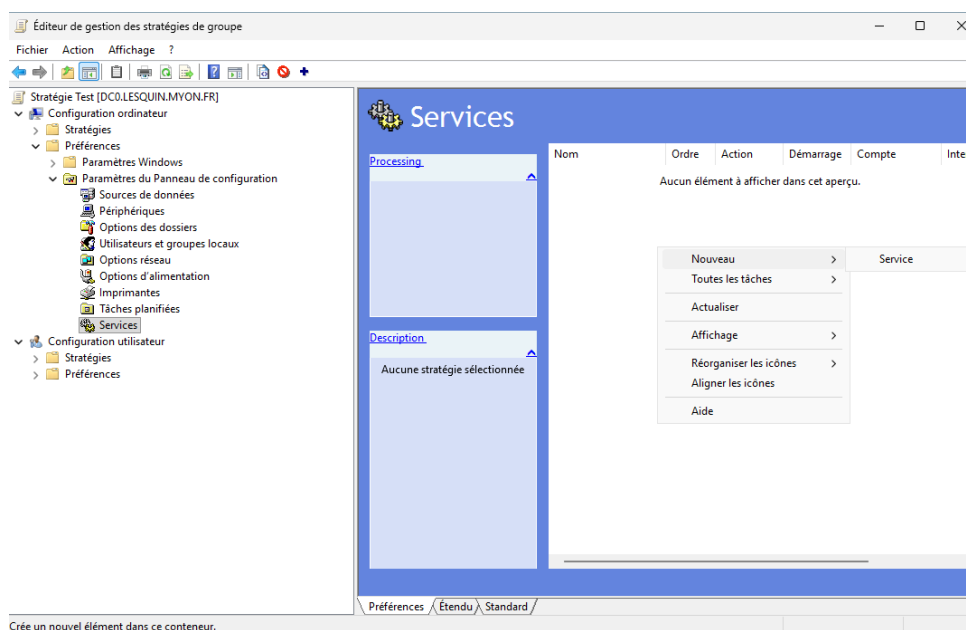


Automatiser le démarrage du service à l'aide des stratégies de groupe du domaine

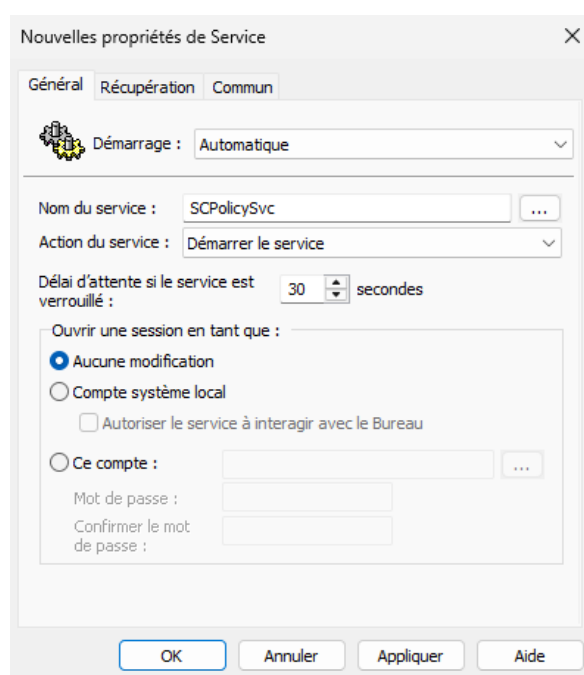
Dans la stratégie de groupe choisie sur le domaine, sélectionner *Configuration Ordinateur > Préférences > Paramètres du panneau de configuration > Services*.



Créer ensuite un nouveau service



Sélectionner Démarrage : Automatique, Nom du service : SCPolicySvc, Action du service : Démarrer le service.



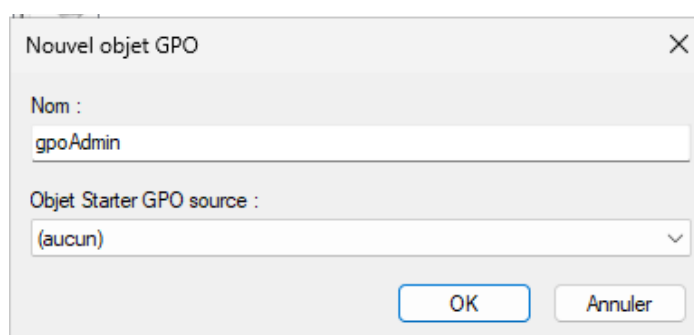
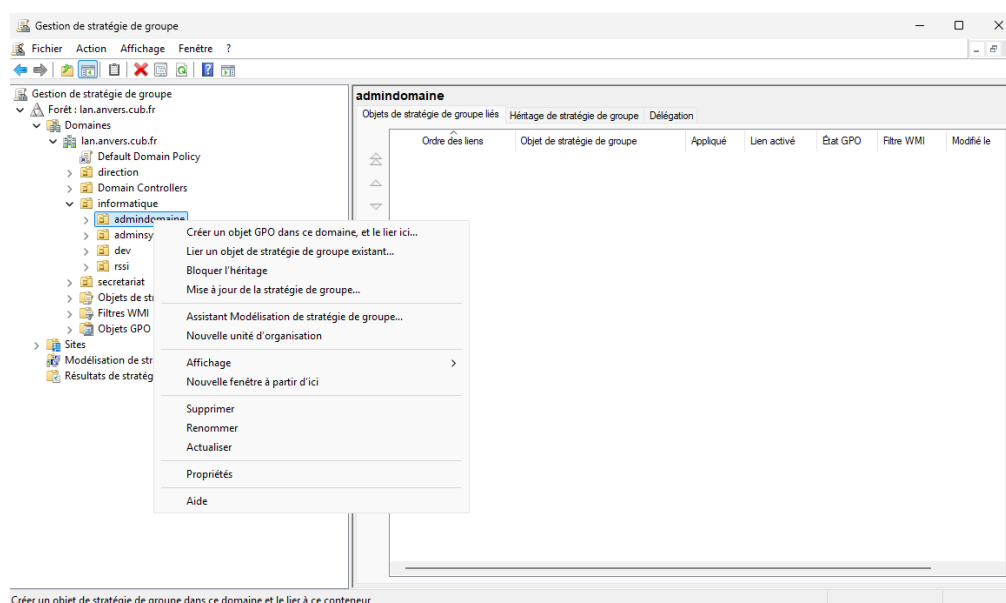
NB : Le nom du service peut être récupéré sur les machines sur lesquelles le logiciel YubiKey-Minidriver a été installé préalablement à l'aide de la commande PowerShell `Get-Service`.

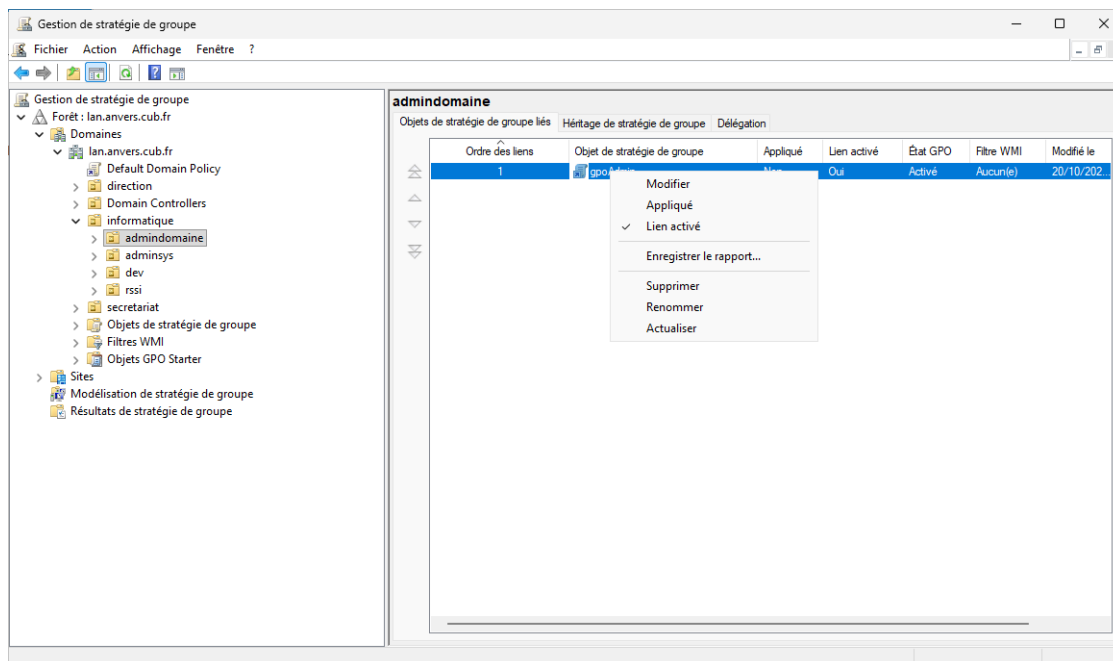
ACTIVER L'INSCRIPTION AUTOMATIQUE POUR LES MACHINES ET LES UTILISATEURS DU DOMAINE CONCERNÉS



Attention ! Ces stratégies doivent être appliquées aux utilisateurs et aux machines. Dans l'exemple ci-dessous, il n'est fait référence qu'à la configuration utilisateurs. Il suffit de réaliser les mêmes opérations dans la stratégie dédiée aux machines.

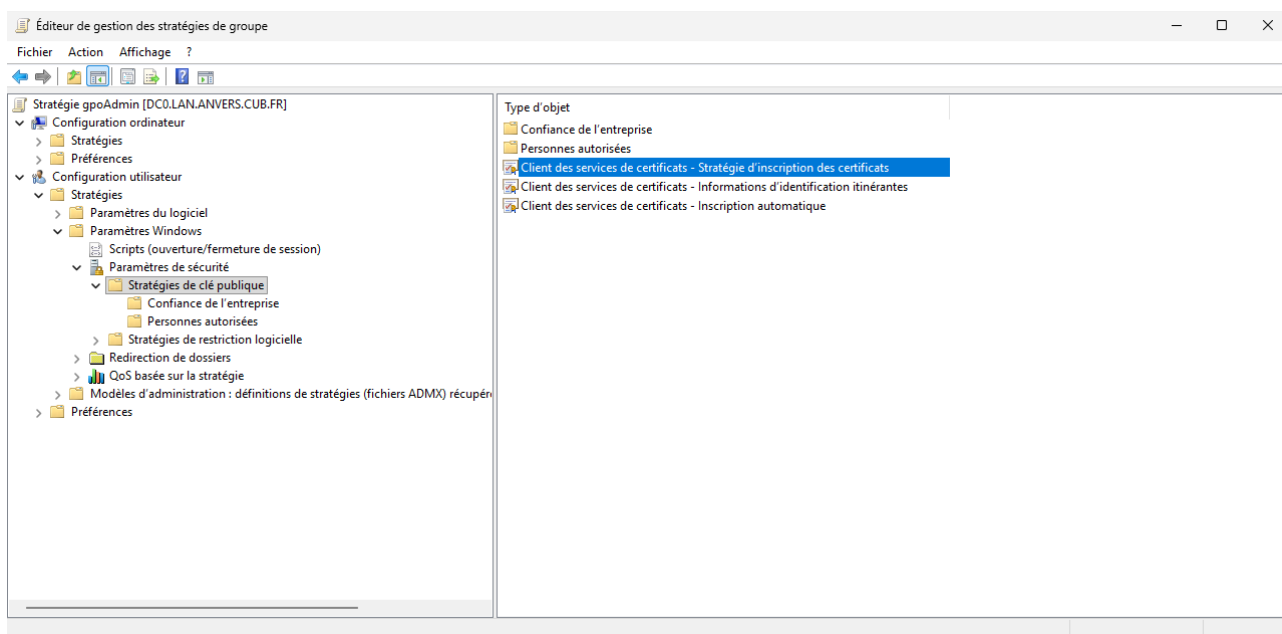
Dans la console Gestion des stratégies de groupe, naviguer dans l'arborescence et choisir l'unité d'organisation contenant les utilisateurs concernés par l'authentification par certificats. Créer une nouvelle GPO à appliquer sur cette unité d'organisation.



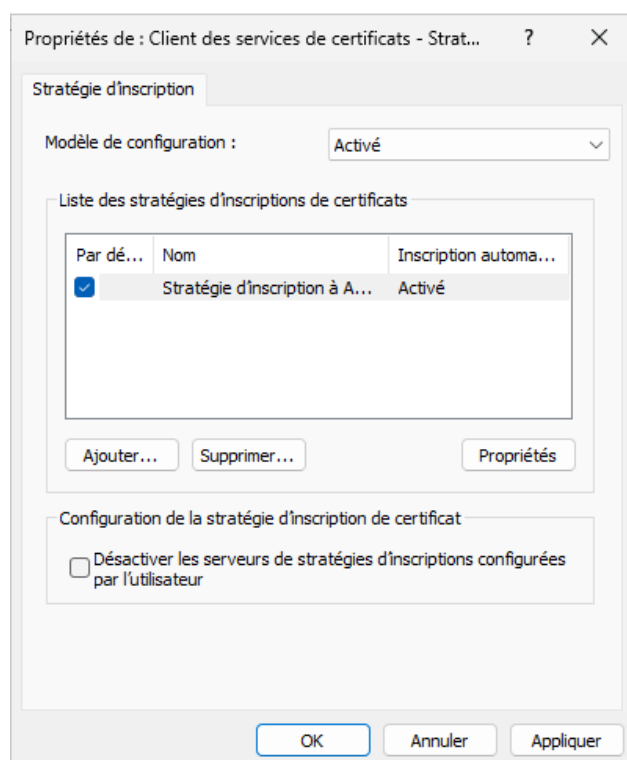


Une fois la nouvelle GPO créée, faire un clic droit dessus et choisir Modifier.

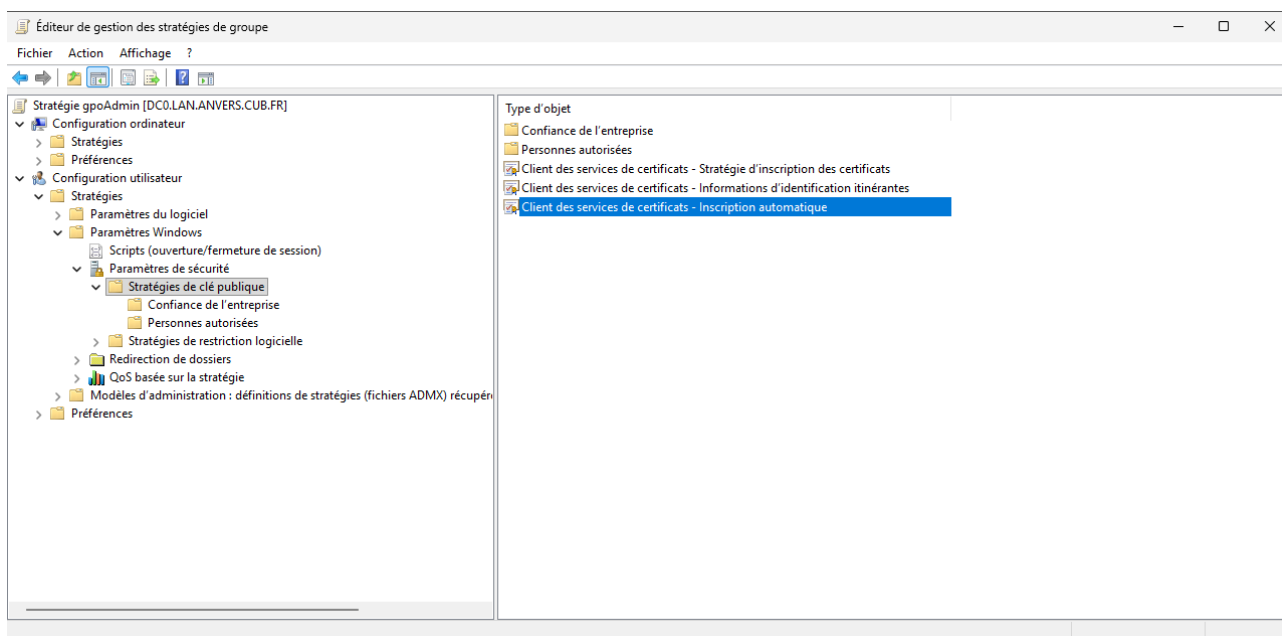
Sélectionner **Configuration utilisateur > Paramètres Windows > Paramètres de sécurité > Stratégie de clé publique > Client de services de certificats – Stratégie d'inscription des certificats.**



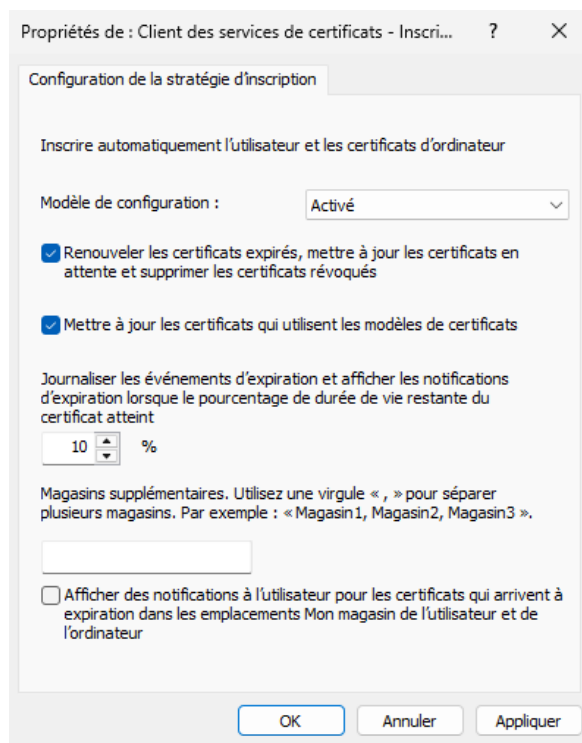
Réaliser un clic droit sur cet objet puis choisir Activé dans Modèle de configuration puis Appliquer et OK.



Sélectionner **Configuration utilisateur > Paramètres Windows > Paramètres de sécurité > Stratégie de clé publique > Client de services de certificats – Inscription automatique.**



Réaliser un clic droit sur cet objet puis choisir **Activé** dans **Modèle de configuration** puis cocher les case **"Renouveler les certificats expirés, mettre à jour les certificats en attente et supprimer les certificats révoqués"** et **"Mettre à jour les certificats qui utilisent les modèles de certificats"**. Cliquer sur **Appliquer** et **OK**.

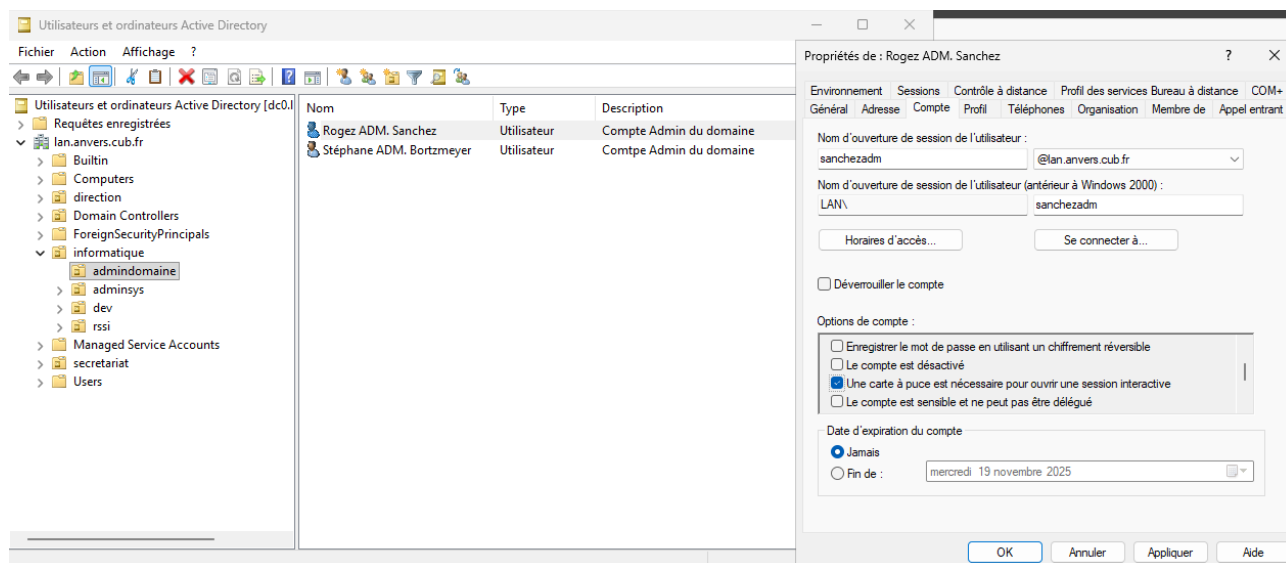


FORCER L'AUTHENTIFICATION PAR CLÉ UNIQUEMENT



Attention ! Cette opération n'est à effectuer qu'après l'auto-inscription et la mise en place du certificat et de la clé privée sur la clé de sécurité.

Par défaut, lorsqu'un utilisateur concerné devra s'authentifier, il aura le choix entre son mot de passe et sa clé de sécurité. Pour renforcer la politique de sécurité et n'autoriser qu'une authentification forte multifacteur, il est possible de configurer le compte concerné en ce sens.



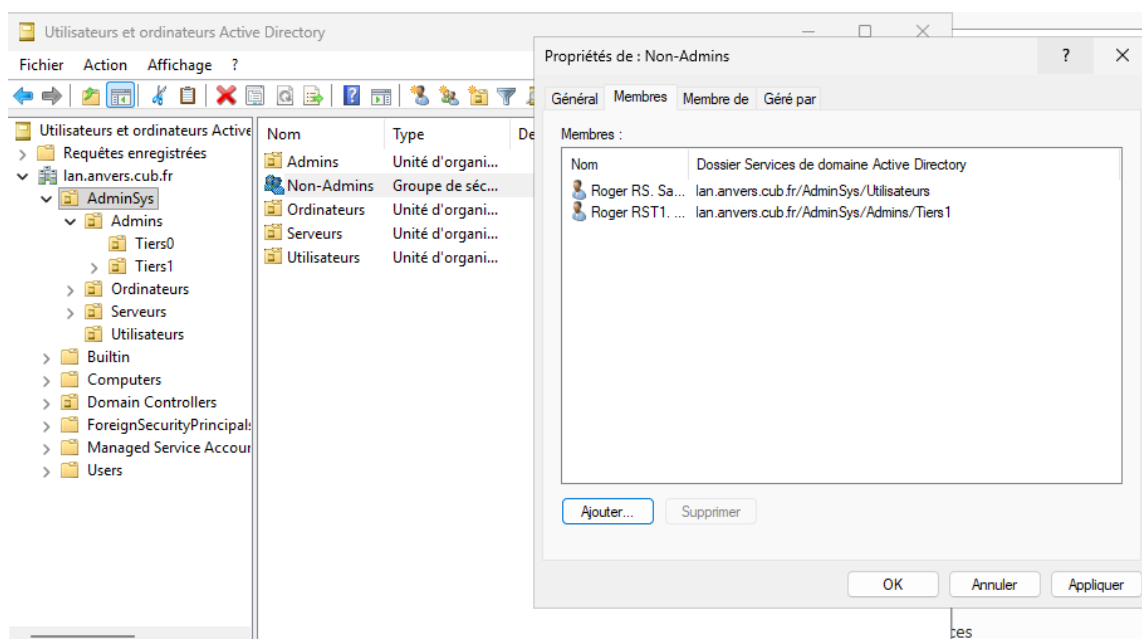
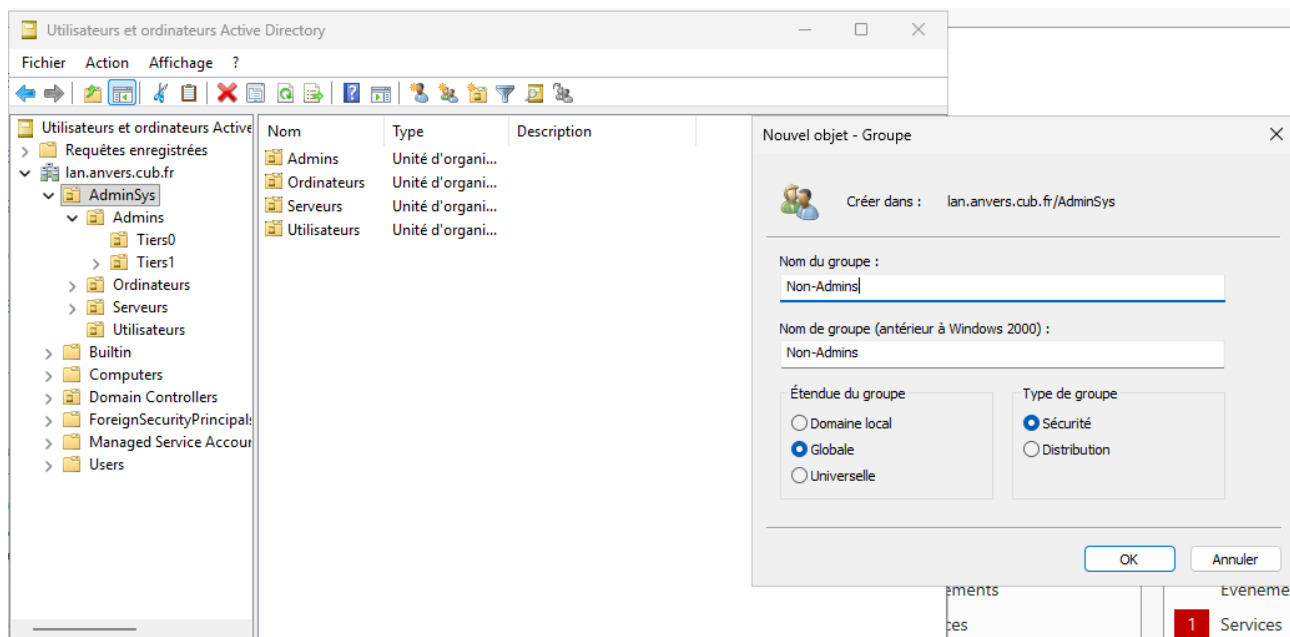
EMPÊCHER L'AUTHENTIFICATION SUR UNE MACHINE

Plusieurs méthodes pour empêcher l'authentification sur une machine sont envisageables. Nous verrons comment le faire via les GPO.

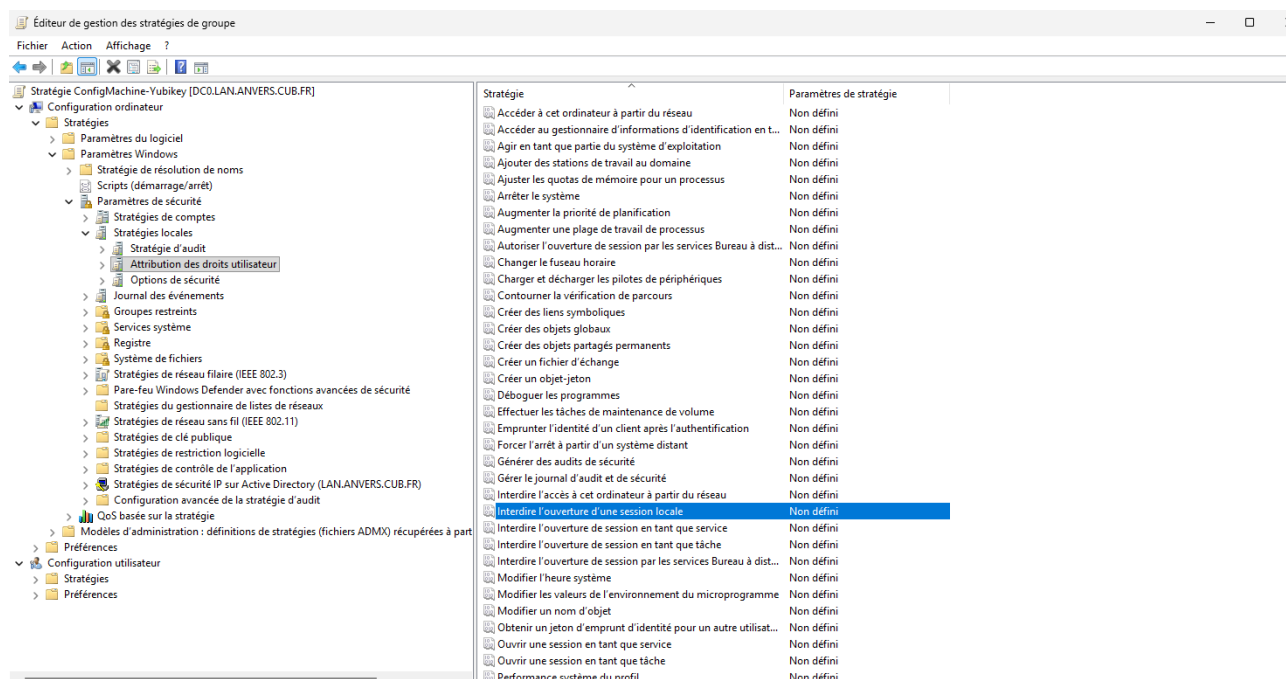


Attention ! Cela ne bloque pas forcément d'autres connexions comme le bureau à distance par exemple.

Tout d'abord, il est nécessaire de créer un groupe contenant les utilisateurs qui seront interdits de connexion sur la ou les machines.



Ensuite, il est nécessaire d'éditer la stratégie de groupe adéquate et de sélectionner **Configuration ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies locales > Attribution des droits utilisateurs > Interdire l'ouverture d'une session locale**.



Sélectionner ensuite le groupe ou l'utilisateur qui ne pourra pas se connecter sur la ou les machines en question.

