Titre du cours : La sécurisation par des GPO

Contexte : Dans le cadre de la mise en place d'une infrastructure 'client léger', celle-ci ne doit pas vous soustraire à la bonne sécurisation de vos postes utilisateurs, mais aussi des communications.
Dans ce module, vous allez voir comment appliquer les GPO , mais aussi quelle GPO est possible. Un test des GPO doit être fait au cas par cas, afin de vérifier le bon fonctionnement.

PARTIE 1: Pourquoi appliquer une sécurisation par GPO

- **Généralités**

La sécurisation par GPO permet d'établir une uniformisation pour l'ensemble des postes utilisateurs sur le réseau.

Si vous n'en mettez pas en place, le propre de l'être humain étant de toujours fouiller là où il ne faut pas, cela peut rapidement devenir un énorme problème. (Jalousie entre les utilisateurs, modification des paramètres en tout genre, etc…)
C'est pour ce genre de comportement que l'on restreint au maximum l'accès des utilisateurs aux fonctionnalités des postes.

Les GPO offrent un large choix de configuration, mais dans le choix qui vous est proposé, il est facile de s'y perdre. N'hésitez pas à faire des recherches pour cibler la bonne GPO en fonction de vos besoins.
Le site documentaire de Microsoft vous sera d'une grande aide à ce sujet, mais il existe aussi des annuaires de recherche très utiles (en anglais) (https://gpsearch.azurewebsites.net/).

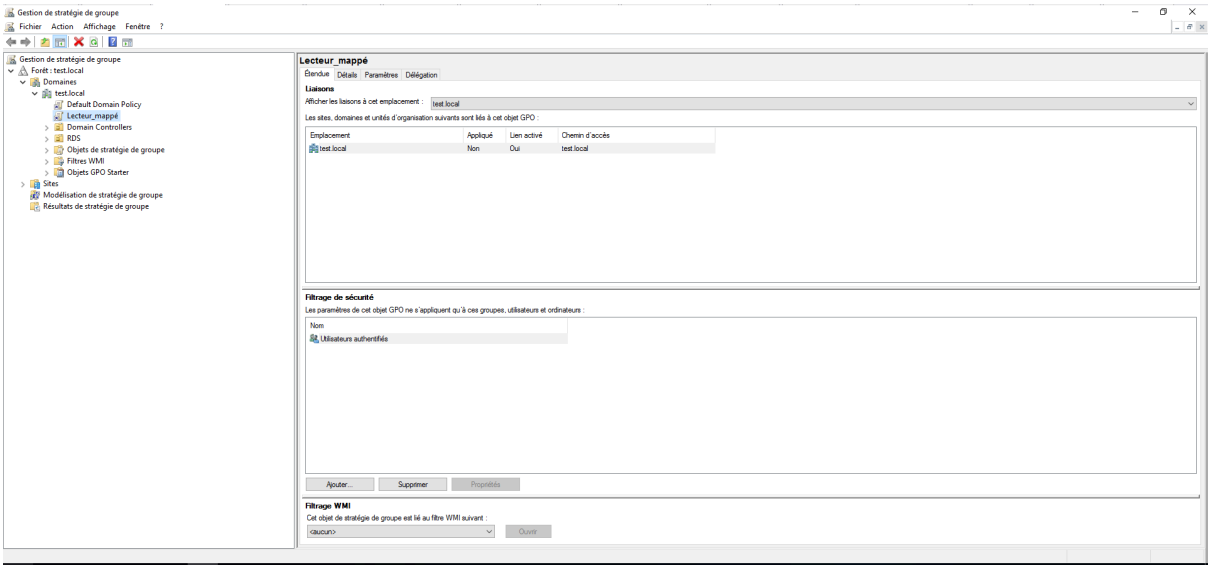
La sécurisation des GPO pourra aussi bien s'appliquer sur l'ordinateur ou sur l'utilisateur, en fonction de la GPO et des besoins. Il faudra choisir si l'une est plus pertinente que l'autre. Mais certaines GPO ne vous laisseront pas le choix, elles seront exclusivement sur l'ordinateur ou sur l'utilisateur.

Appliquer des GPO basiques

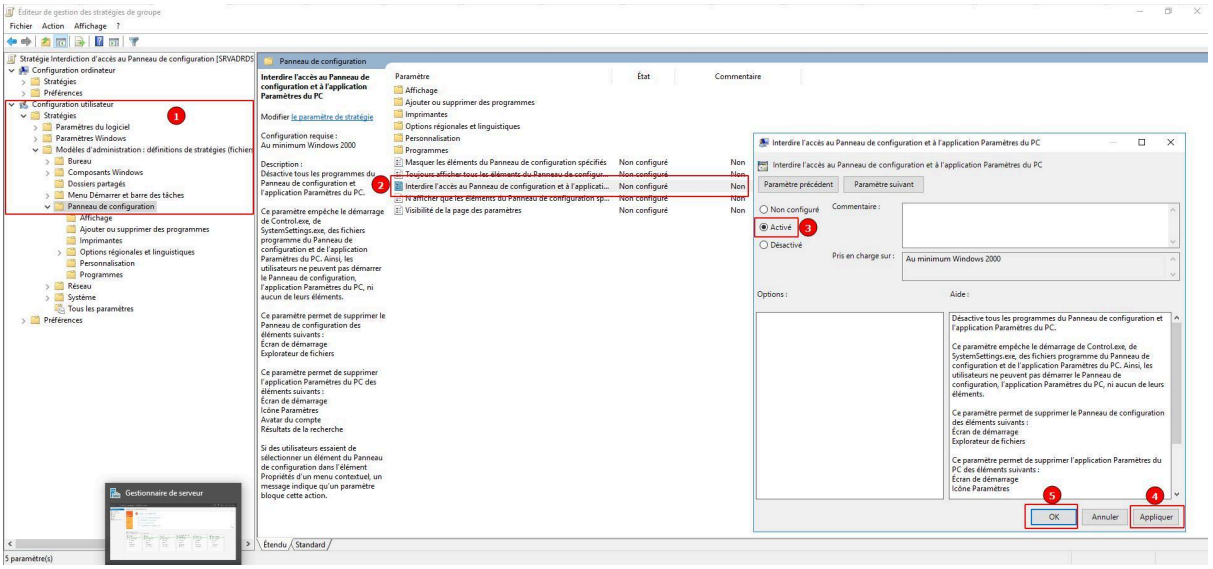
Nous allons appliquer des GPO dites 'basiques'. L'utilisateur n'a pas vocation à administrer lui-même son poste et surtout ne doit pas en avoir l'occasion. Comme expliqué précédemment, ceci est un aspect sécuritaire de votre infrastructure.

Interdiction d'accès au 'Panneau de configuration'

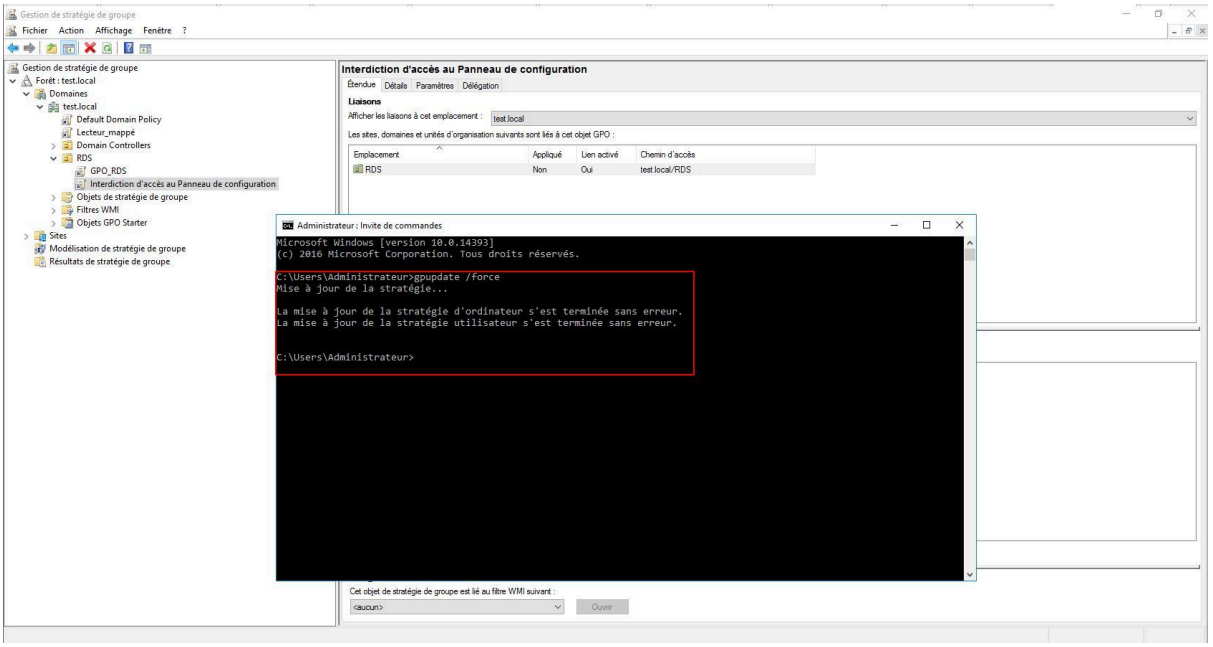
Etape 1: Ouvrez le '**Gestionnaire de stratégie de groupe**' sur le serveur AD.



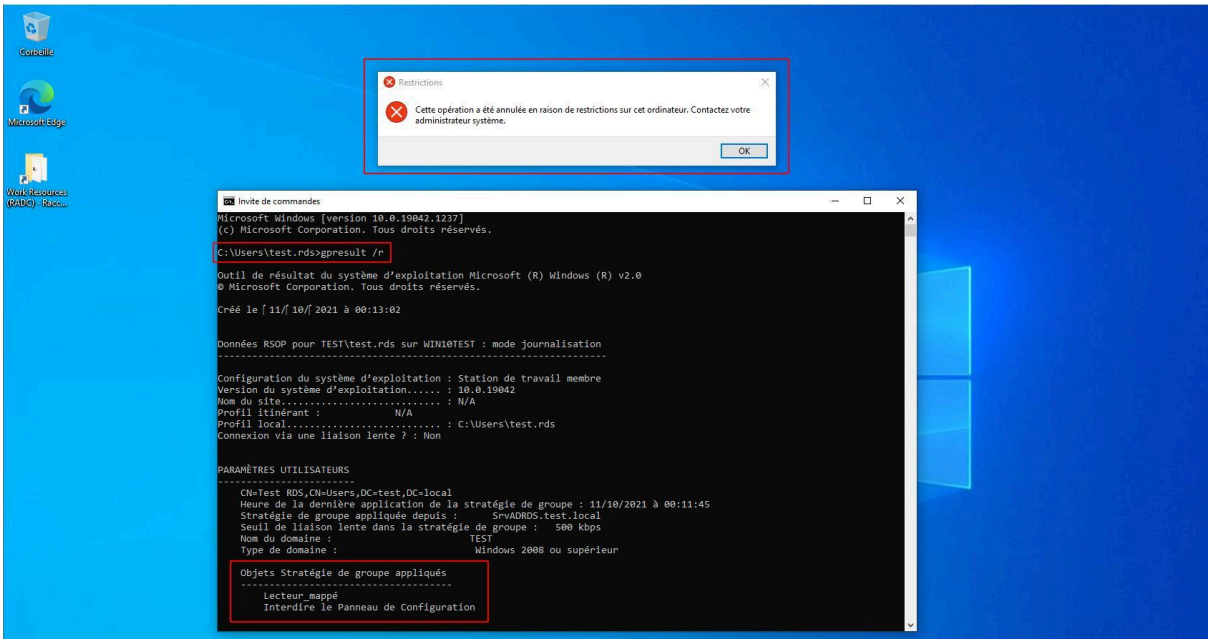
Etape 2: Créez une nouvelle GPO sur l'interdiction d'accès au '**Panneau de configuration**': **Configuration Utilisateur** > **Stratégies** > **Modèles d'Administration** > **Panneau de Configuration** > **Interdire l'accès au Panneau de Configuration et aux paramètres du PC**



Etape 3: Appliquez la GPO, ouvrez un invite de commande et tapez "**gpupdate /force**" pour forcer l'application aux utilisateurs concernés.



Etape 4: Vérifiez la bonne application sur le poste client avec un utilisateur du “**Grp_RDS**”. Ouvrez votre session, allez dans le ‘**Panneau de configuration**’.
Celui-ci doit vous être refusé.
Vous pouvez aussi ouvrir un invite de commande et taper “**gpresult /r**” pour voir si l’utilisateur avec qui vous êtes connecté est bien impacté par cette GPO.

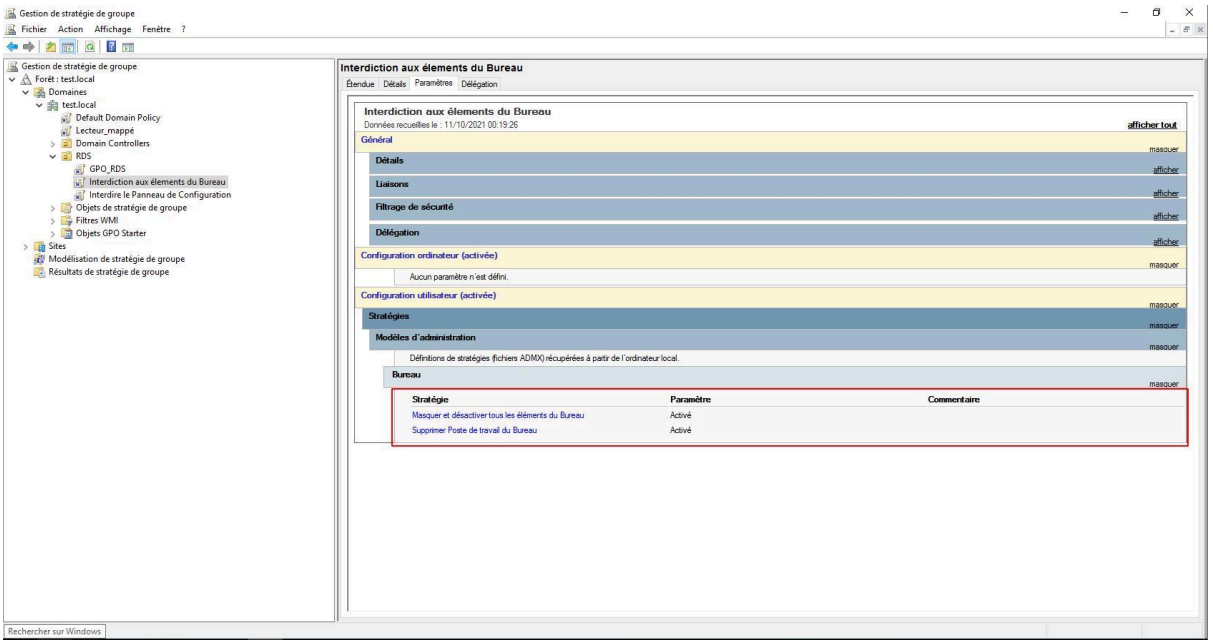


- **Restreindre l’accès au élements du bureau**

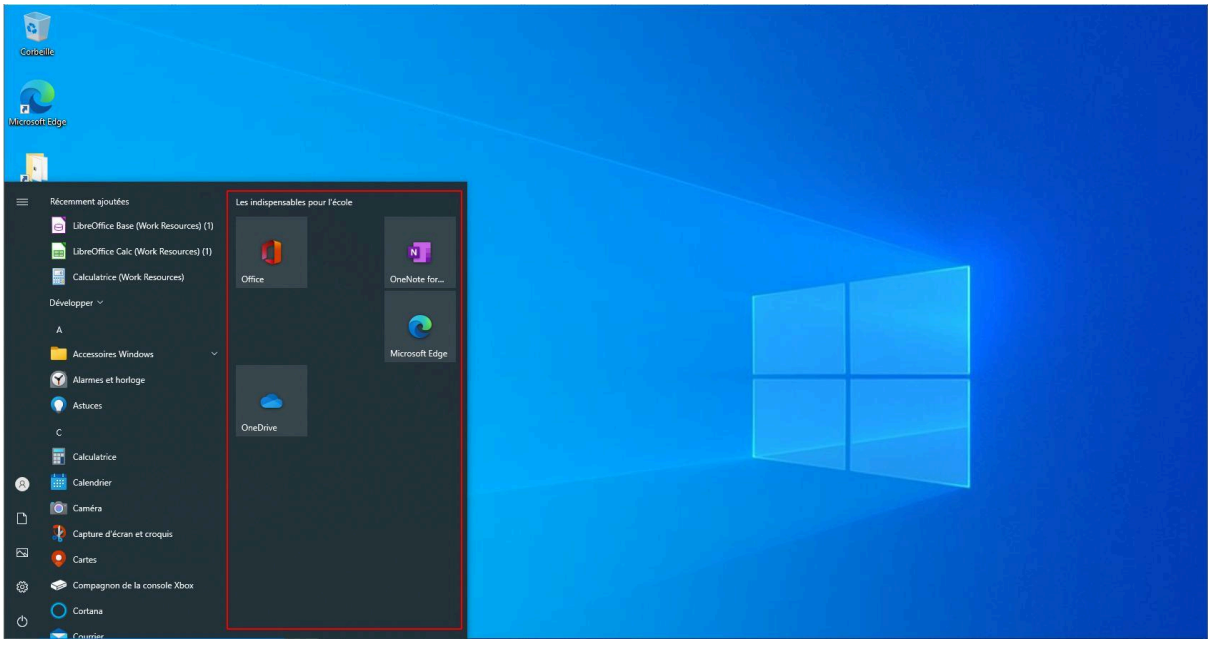
Etape 1: Sur le serveur AD, ouvrez la ‘**Gestion des stratégie de groupe**’ et créez une GPO se nommant “**Interdire l’accès aux éléments du bureau**”.

Configuration Utilisateur > Stratégies > Modèles d’Administration > Bureau Paramètre : Masquer et désactiver tous les éléments du bureau

Configuration Utilisateur > Stratégies > Modèles d'Administration > Bureau Paramètre : Supprimer Poste de Travail du Bureau



Etape 2: Appliquez un "**gpupdate /force**", ensuite passez sur votre VM TEST avec un utilisateur. Constatez les modifications d'application de la GPO. (Vous pouvez toujours faire un "**gpupdate /force**" et un "**gpresult /r**" sur le client.
Certaines fonctionnalités ne seront plus accessibles ainsi que certains logiciels. Ils disparaîtront des éléments de base installés par Windows.



- **Et bien d'autres encore…**

Vous avez la possibilité d'aller plus loin dans la sécurisation de vos postes. N'oubliez pas que moins vous laissez d'accès à vos utilisateurs plus votre infrastructure sera saine et la tentation des utilisateurs à modifier ou à fouiller dans leur machine sera moindre.

Dans le cas où votre GPO ne fonctionne pas, pensez à bien vérifier qu'elle est fonctionnelle, dans la bonne UO par rapport à vos besoins. Il ne faudra pas hésiter à la refaire si besoin. Les GPO peuvent être capricieuses.

PARTIE 2: GPO de sécurisation du protocole RDP

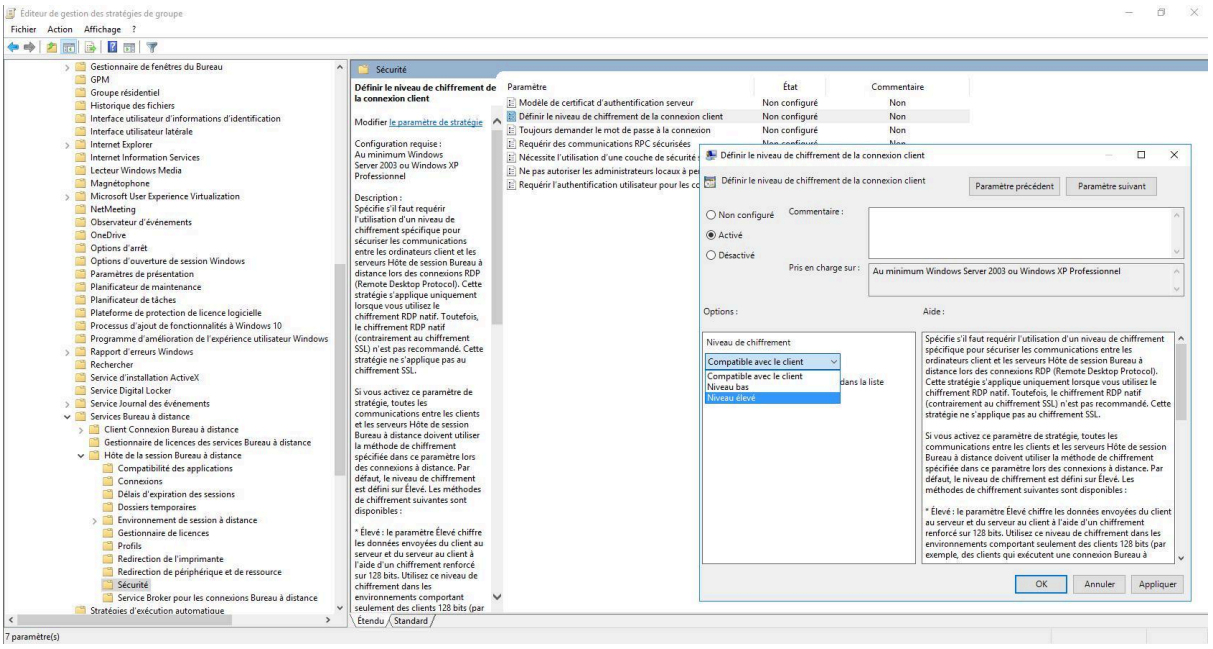
- **Allons plus loin**

Vous allez pouvoir dès à présent appliquer des GPO pour la sécurisation de plusieurs points. Dans le cas où nous sommes dans une infrastructure 'client léger', nous allons devoir proposer une sécurisation des données qui transite par le protocole RDP, mais aussi pour l'authentification au serveur RDS et, par conséquent, aussi sur le réseau.

- **GPO pour sécuriser les données qui transitent par le protocole RDP**

Etape 1: Ouvrez le '**Gestionnaire des stratégies de groupe**' dans le serveur AD.
Créez une nouvelle GPO en donnant un intitulé correct à votre GPO "**Sécurisation des communications client**".
Configuration Ordinateur > Stratégies > Modèles d'Administration > Composants Windows > Service Bureau à Distance > Hôte de la session Bureau à Distance > Sécurité > Paramètre : Définir le niveau de chiffrement de la connexion client.

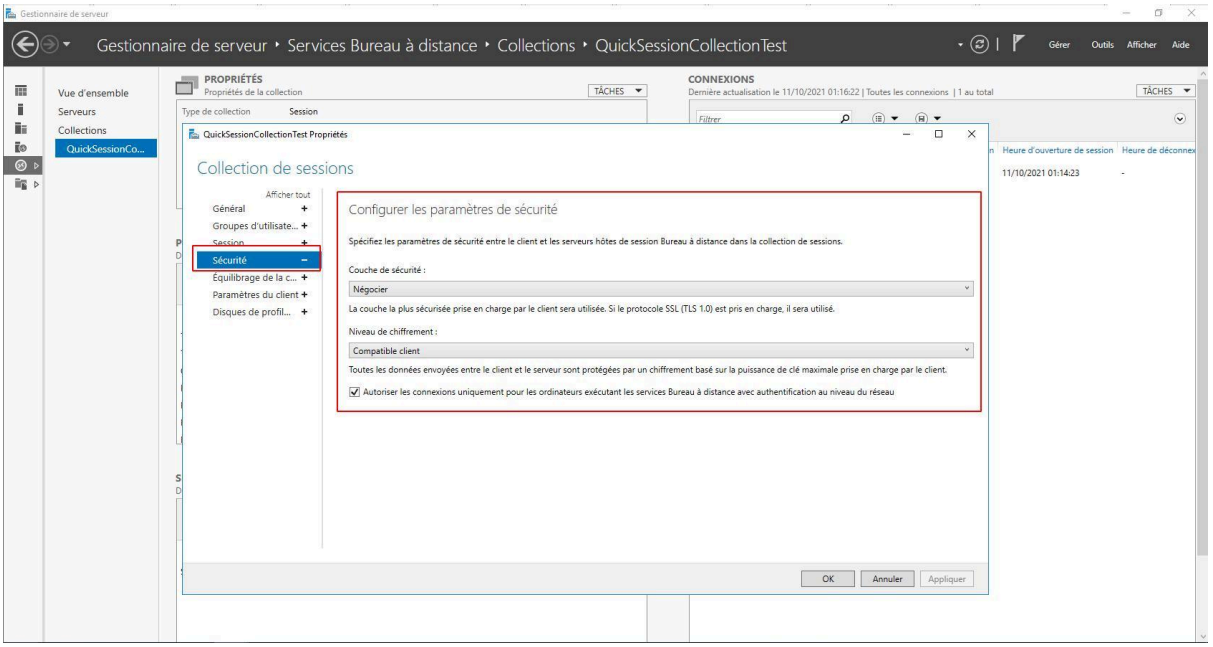
Vous pouvez choisir différents types de chiffrement. Pour vous entraîner, commencez avec "**Compatible avec le client**".



Etape 2: Comme pour les autres manipulations, appliquez cette GPO, puis testez-la depuis un poste client, sans oublier les commandes “**gpupdate /force**” et “**gpresult /r**”.
Vous n’obtiendrez pas un retour visuel de cette GPO, un “**gpresult /r**” vous donnera un premier aperçu de son application. Afin de voir les communications chiffrées, n’hésitez pas à utiliser un logiciel permettant d’analyser vos trames (ex: wireshark).

- **Autres moyens**

Lors des paramétrages sur le Serveur RDS concernant les collections que vous créez, vous pouvez aussi appliquer cette fonctionnalité.



Rappel: Autres GPO possible

Des GPO de d’authentification sont aussi possibles, via certificats pour l’authentification au serveur RDS, mais aussi au niveau des utilisateurs du réseau.
Vous trouverez un récapitulatif de l’ensemble des GPO qui vous sont possibles en fin de module, dans une section dédiée.

PARTIE 3: Surveillance et Contrôle des sessions utilisateurs

- **A quoi cela sert-il ?**

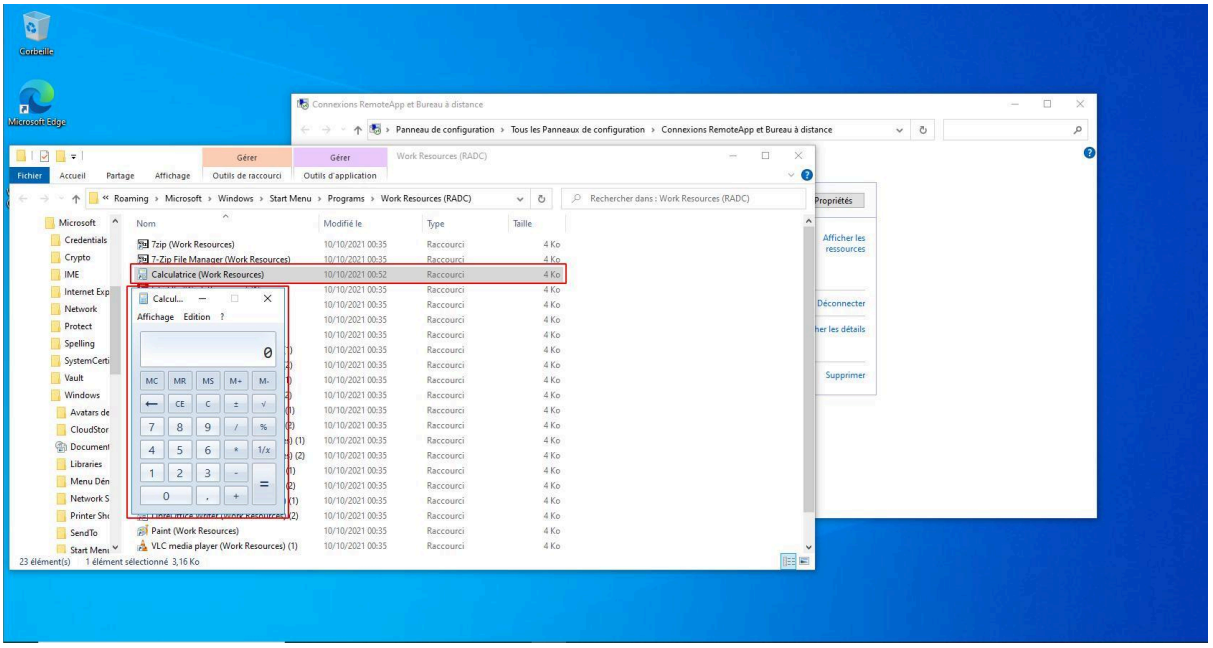
Dans le cas ou l’un de vos utilisateurs rencontre un problème avec un des logiciels ou une méthodologie d’application, vous aurez la possibilité d’afficher son écran et voir ce qu’il s’y passe. De la même façon, il vous sera possible de prendre la main à distance afin de pouvoir résoudre l’incident sur le poste client.
Il n’est pas toujours aisé de se déplacer sur le poste utilisateur directement, pensez que votre interaction avec le serveur RDS et le service IT peut être dans le même bâtiment comme à plusieurs centaines de kilomètres.

Attention: cet accès vous sera possible dans la mesure où l'utilisateur accepte cette

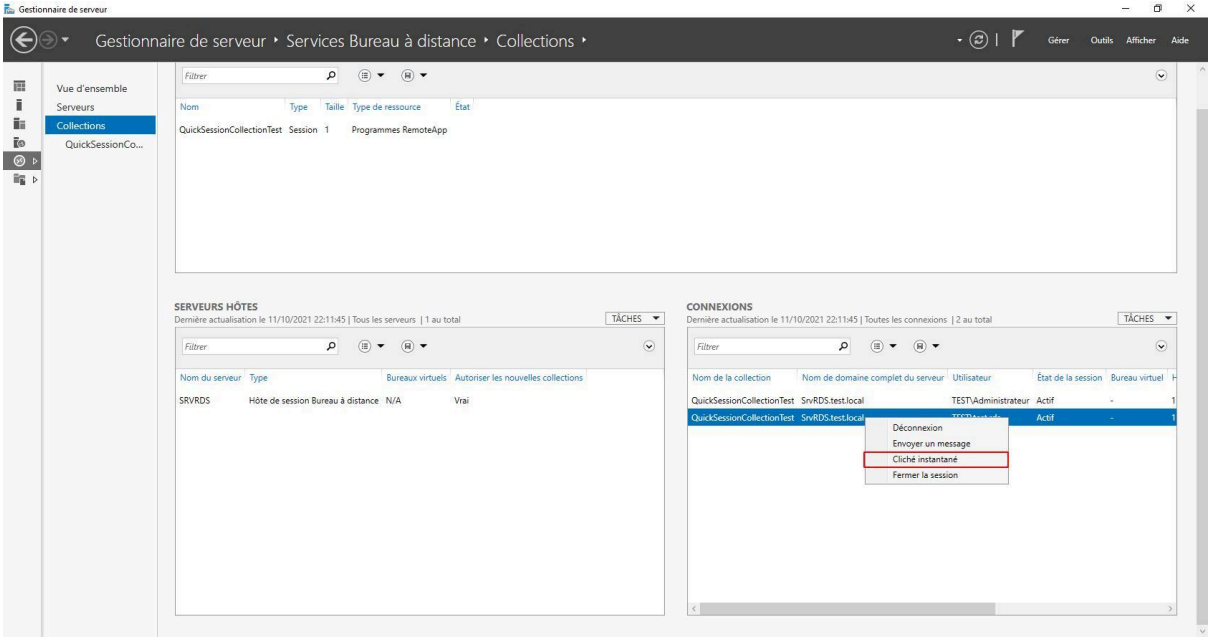
méthode. Dans le cas contraire, un retour de la communication se fera avec un message d'erreur vous empêchant ainsi toute interaction.

- **Établir une surveillance ou un contrôle sur une session utilisateur**

Etape 1: Sur un poste client, initiez une connexion au serveur RDS. Par la calculatrice, par exemple.

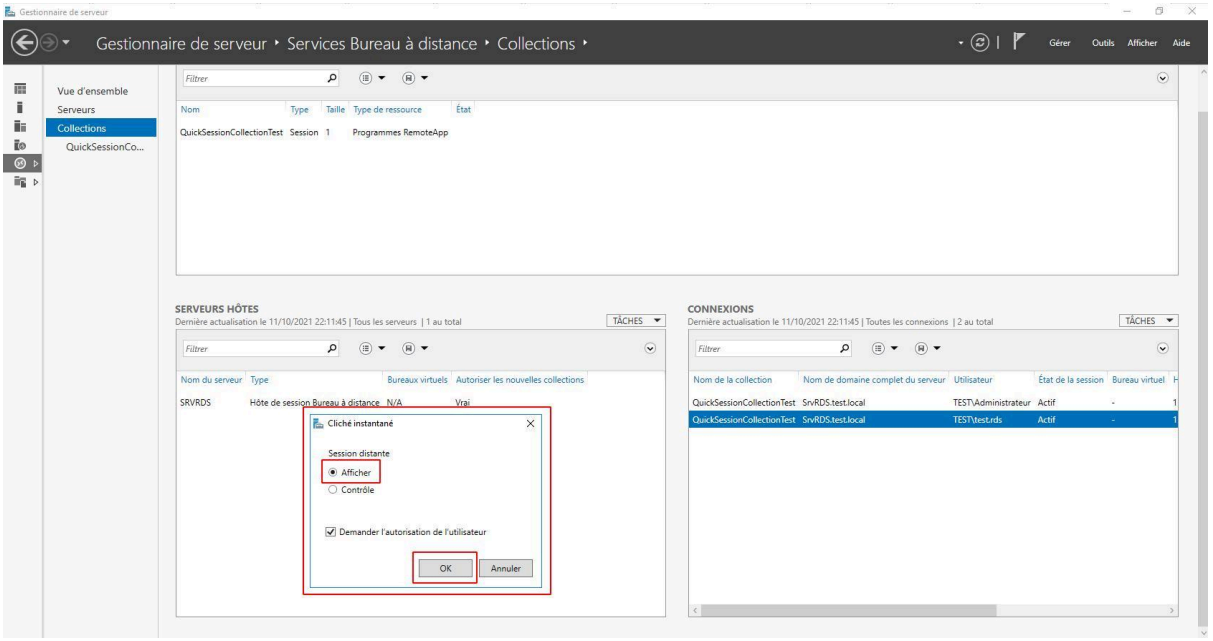


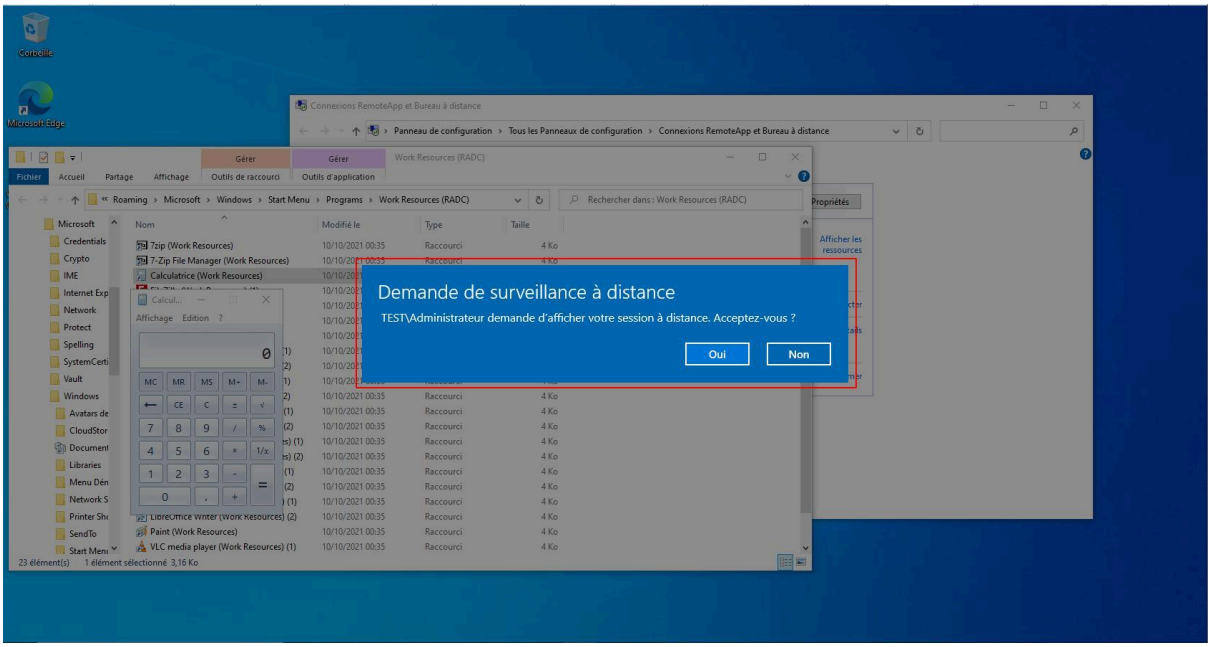
Etape 2: Allez sur votre serveur RDS dans "**Service Bureau à distance" > "Collection" > "Connexions".**
Vous allez voir votre utilisateur qui est connecté.
En cliquant sur l'utilisateur avec un clic-droit, faites "Cliché instantané".

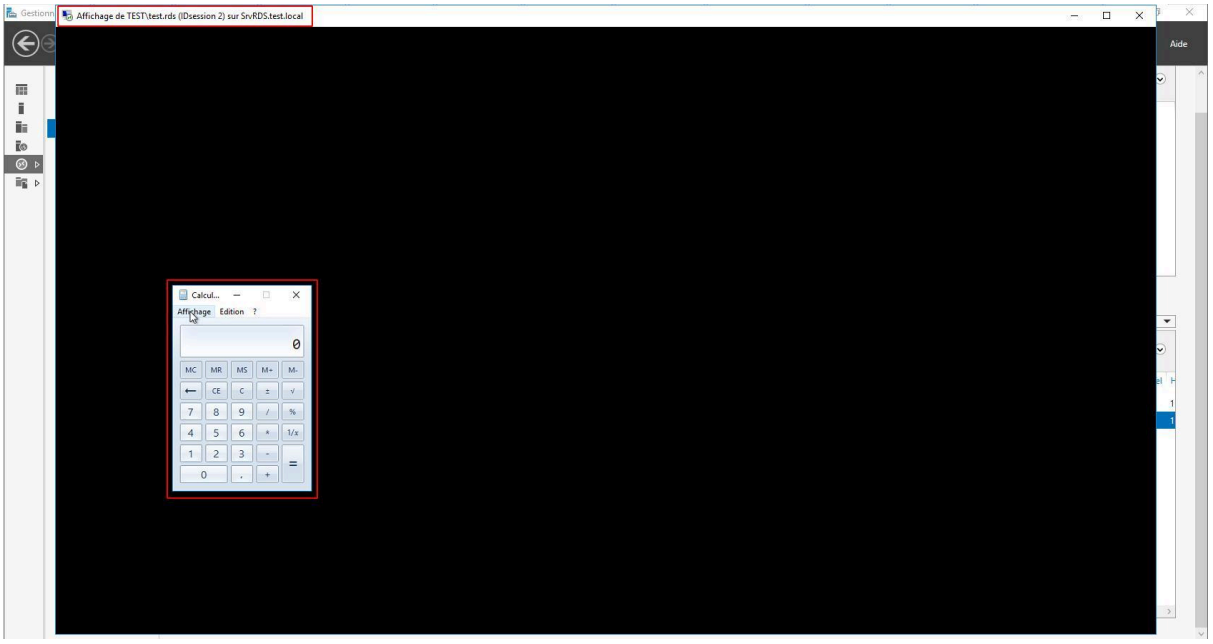


Etape 3: Vous avez ici une fenêtre qui s'ouvre, vous proposant plusieurs choix. "**Afficher**" ou "**Contrôle**".
Laissez la case de demande d'autorisation à l'utilisateur cochée.

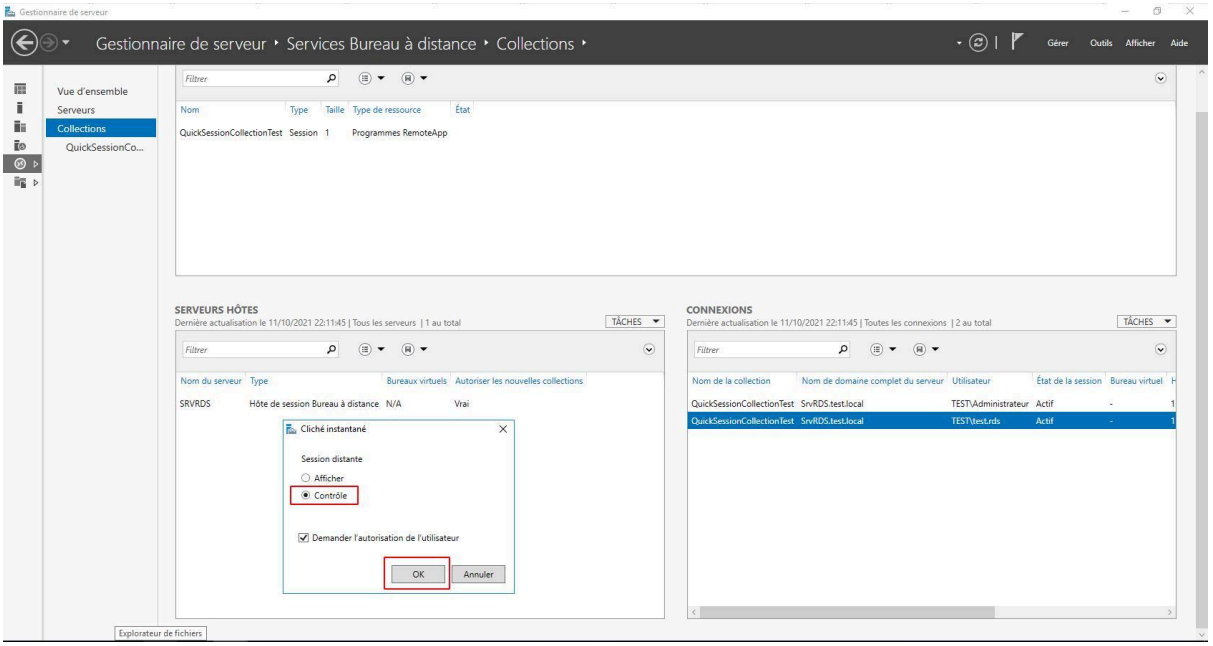
- Laissez "**Afficher**" et faites "**OK**" . Allez sur le poste client, une demande apparaît. Une fois acceptée, revenez sur le serveur RDS et notez l'apparition de votre bureau client.

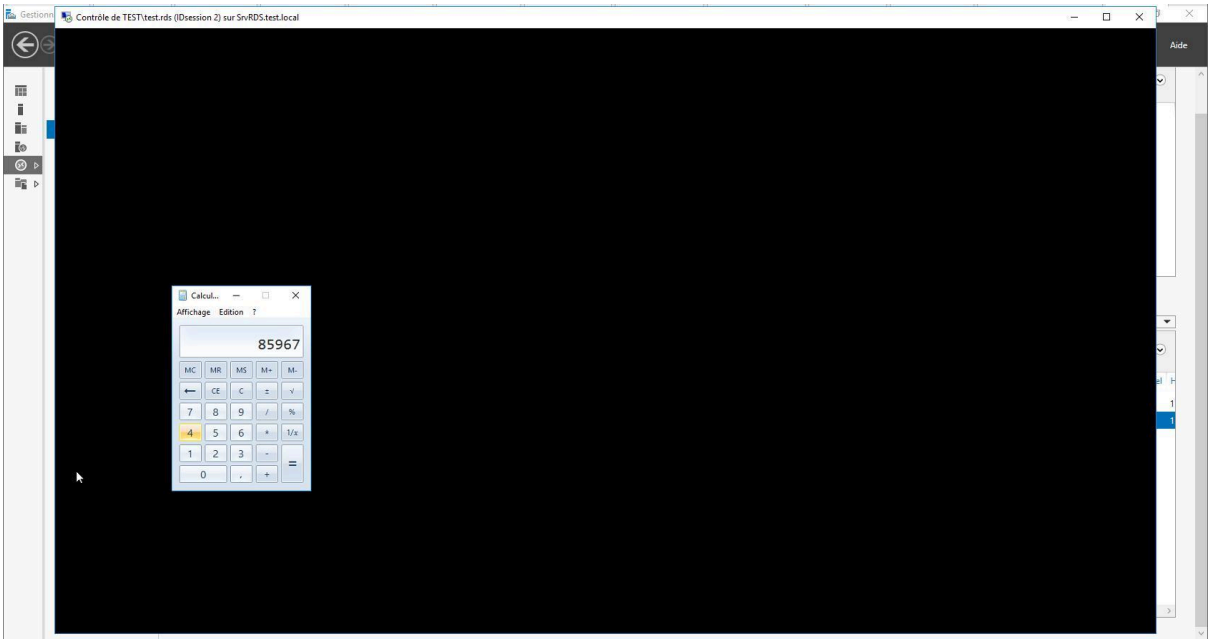






- En sélectionnant “**Contrôle**”, faites “**Ok**”. Répétez l’opération de validation et revenez sur votre serveur pour constater le résultat. En cliquant dans la fenêtre, vous aurez la possibilité de contrôler la souris.





PARTIE 4: Liste de GPO qui est applicable pour la sécurisation.

Les GPO pour restreindre les actes des utilisateurs sur leur poste.

Restreindre l'accès au **panneau de configuration**: Empêche l'utilisateur d'ouvrir son panneau de configuration, ceci évitera des modifications dans les multiples menus qu'il propose.

Restreindre l'accès au menu **Démarrer** et au **options Réseau**: Empêche l'accès à la barre des tâches pour d'éventuelles modifications des options réseau (paramétrable)

Restreindre l'accès au l'**invite de commande**: Empêche l'ouverture de l'invite de commande

Restreindre l'accès au **Registre:** Empêche l'accès au registre via "**regedit.exe**"

Restreindre l'accès aux **Mises à jour automatiques de Windows**: Bloque la possibilité de gérer l'arrêt ou l'installation des mises à jour depuis un poste utilisateur.

Vous avez encore bien d'autres possibilités, comme l'installation de pilotes d'imprimante, de redirection d'imprimantes, ressources périphériques, etc… Cette liste n'est qu'une ébauche de l'ensemble des fonctionnalités.

Sécurisation des communications entre le serveur RDS et le poste client

Définir le niveau de chiffrement de la connexion client: Permet de définir le niveau de chiffrement pour les données qui transitent entre le client et le serveur

Nécessite l'utilisation d'une couche de sécurité spécifique pour les connexions distantes (RDP) : SSL (TLS1.0): Oblige l'utilisation d'une couche de sécurité supplémentaire pour les connexion via RDP entre les clients et les serveurs

Requérir l'authentification utilisateur pour les connexions à distance à l'aide de l'authentification au niveau du réseau: Demande l'authentification de l'utilisateur au niveau du réseau pour les connexions RDP.

Authentification unique Single Sign On (SSO)

Autoriser la délégation d'informations d'identifications par défaut: Vous permettra d'avoir une délégation d'authentification sur les serveurs (qui seront spécifié dans la GPO) via le CredSSP. Une authentification sera alors appliquée via un certificat X509 pour Kerberos.