Mr ROTH

08/12/2024

Compte rendu TP9

Mise en place d'un serveur de Bureau à distance – RDS avec restrictions via GPO

TEWES Arnaud
BTS SIO SISR 2EME ANNEE

Introduction

Remote Desktop Services (RDS) est une technologie de Microsoft Windows Server qui permet aux utilisateurs d'accéder à des applications et des bureaux à distance sur un réseau. RDS offre une solution centralisée pour héberger des applications et des bureaux, permettant aux utilisateurs d'y accéder depuis divers appareils et emplacements.

Pourquoi utilise-t-on RDS ?

La mise en place de RDS est motivée par plusieurs avantages clés :

- **Centralisation des applications et des données :** RDS permet aux organisations de centraliser le déploiement, la gestion et la maintenance des applications et des données. Cela simplifie l'administration et réduit les coûts.
- **Accès à distance :** RDS offre aux utilisateurs la flexibilité d'accéder à leurs bureaux et applications depuis n'importe où, à partir de divers appareils (ordinateurs portables, tablettes, clients légers). Cela favorise la mobilité et le télétravail.
- **Sécurité améliorée :** En centralisant les applications et les données, RDS peut améliorer la sécurité en réduisant les risques liés au stockage de données sensibles sur les appareils des utilisateurs.
- **Optimisation des ressources :** RDS permet d'optimiser l'utilisation des ressources matérielles en permettant à plusieurs utilisateurs de partager les mêmes serveurs.

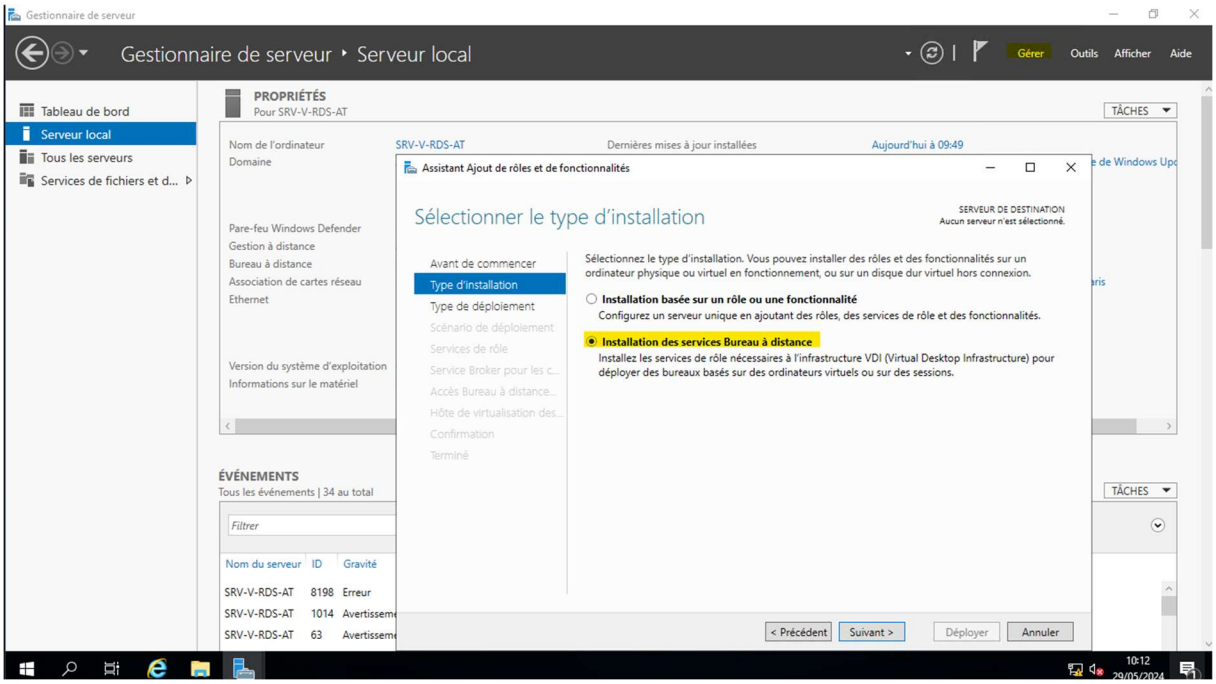
Prérequis :

Avant de déployer RDS, il est important de s'assurer que l'environnement répond aux prérequis suivants :

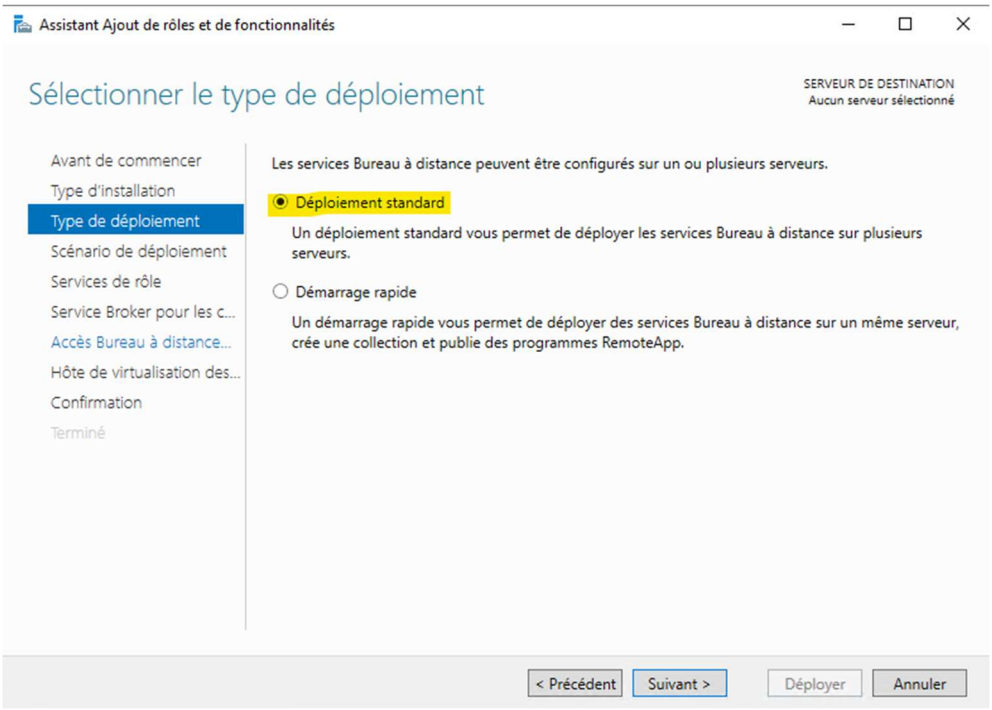
- **Serveur Windows :** Un serveur Windows Server avec une version appropriée (par exemple, Windows Server 2016, 2019, ou 2022) doit être disponible pour héberger les rôles RDS.
- **Matériel adéquat :** Le serveur doit disposer de suffisamment de ressources matérielles (processeur, mémoire, stockage) pour supporter le nombre d'utilisateurs et les applications à héberger.
- **Infrastructure réseau :** Une infrastructure réseau stable et performante est essentielle pour assurer une bonne expérience utilisateur.
- **Considérations de licences :** Les licences RDS doivent être correctement gérées pour être conformes aux exigences de Microsoft.

Procédé de la mise en place pas à pas

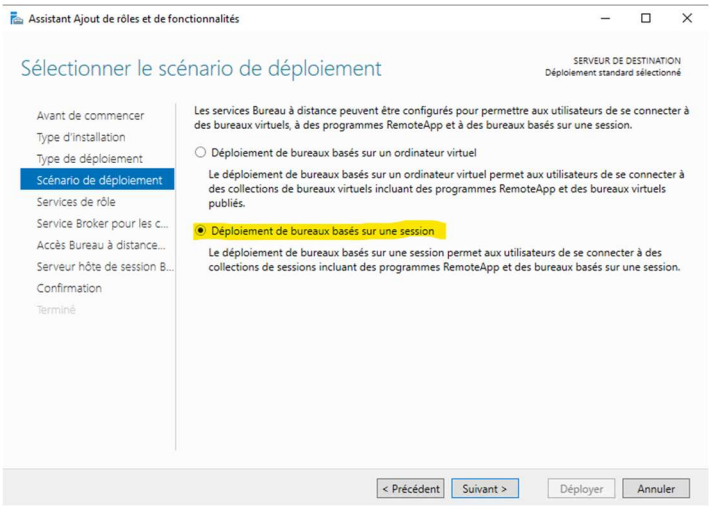
Ouvrez le Gestionnaire de serveur et Cliquez sur "Gérer" > "Ajouter des rôles et des fonctionnalités »

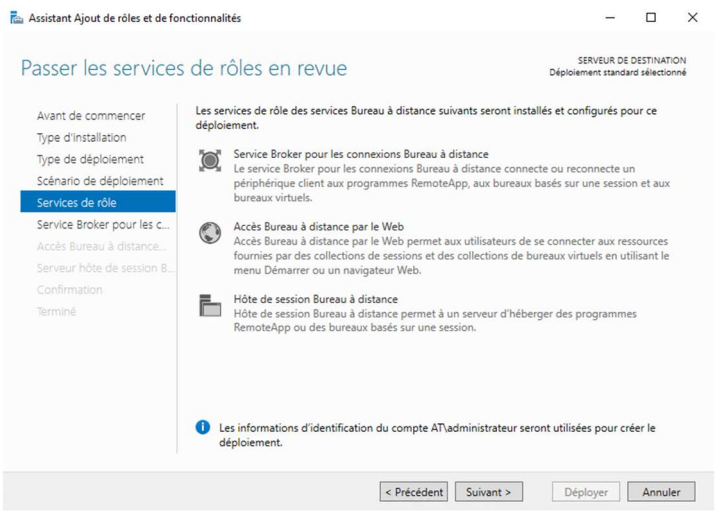


Sélectionner le type de déploiement et choisir "Déploiement standard"

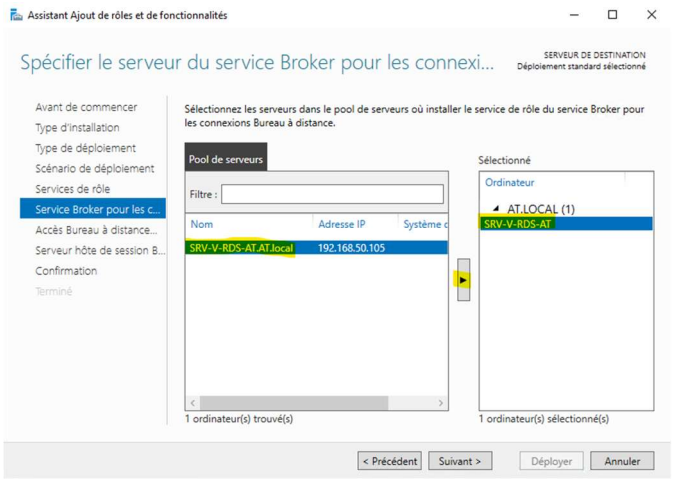


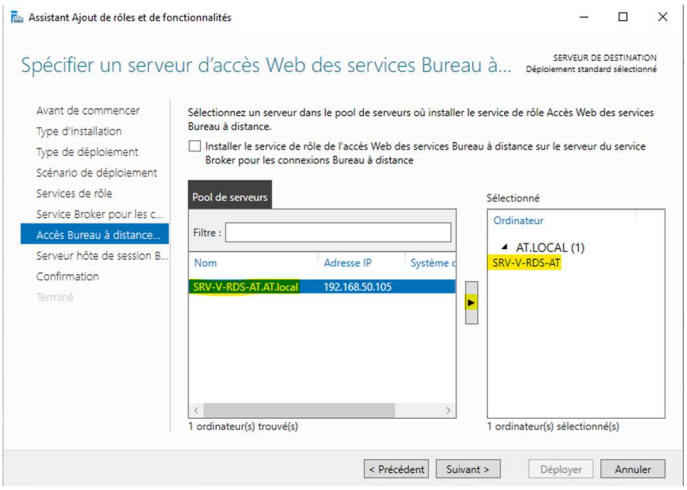
Sélectionner le scénario de déploiement et choisir "Déploiement de bureaux basés sur une session" (pour que chaque utilisateur se partage le même serveur, moins de ressources utilisée)

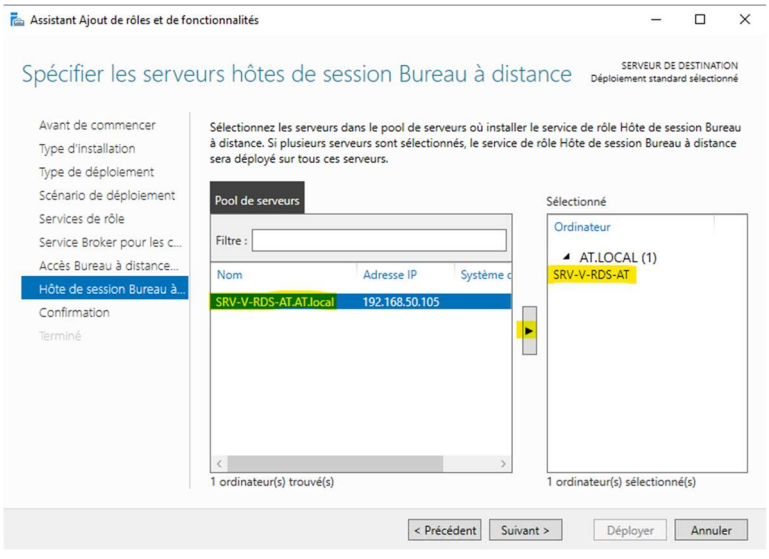




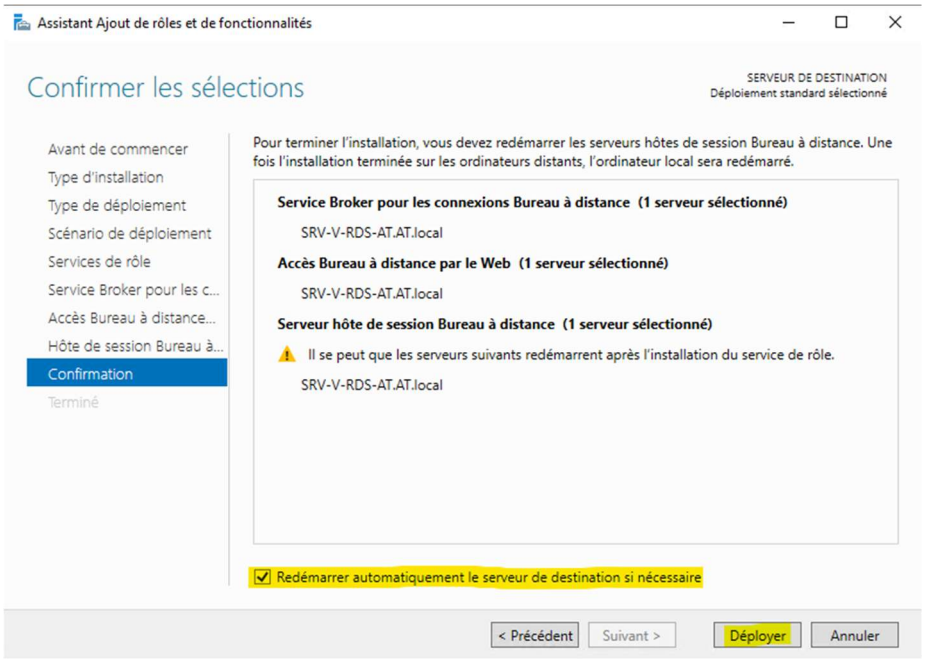
Spécifier le serveur du service Broker pour les connexions, un serveur d'accès Web des services Bureau à distance et les serveurs hôtes de session Bureau à distance



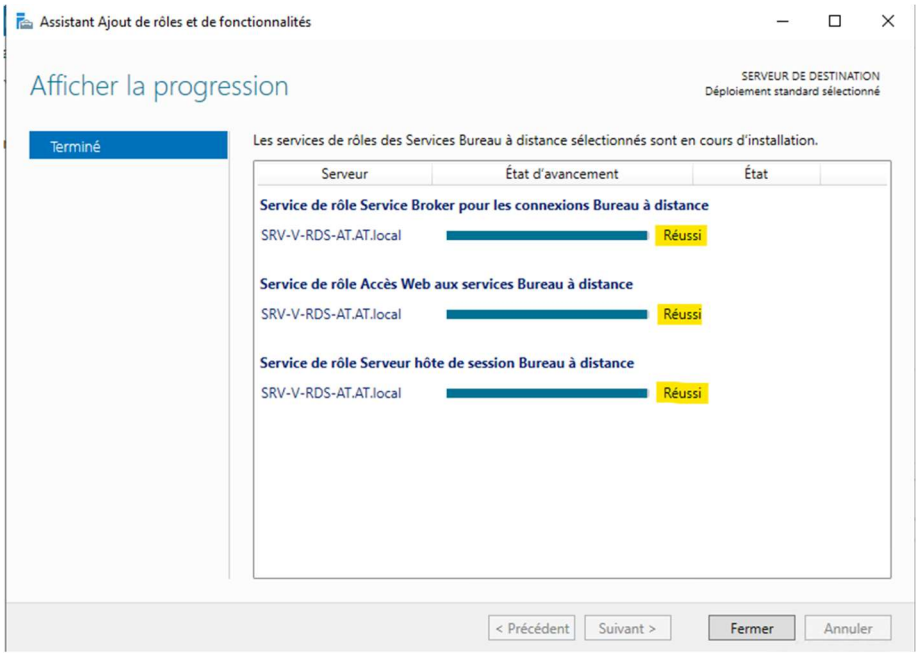




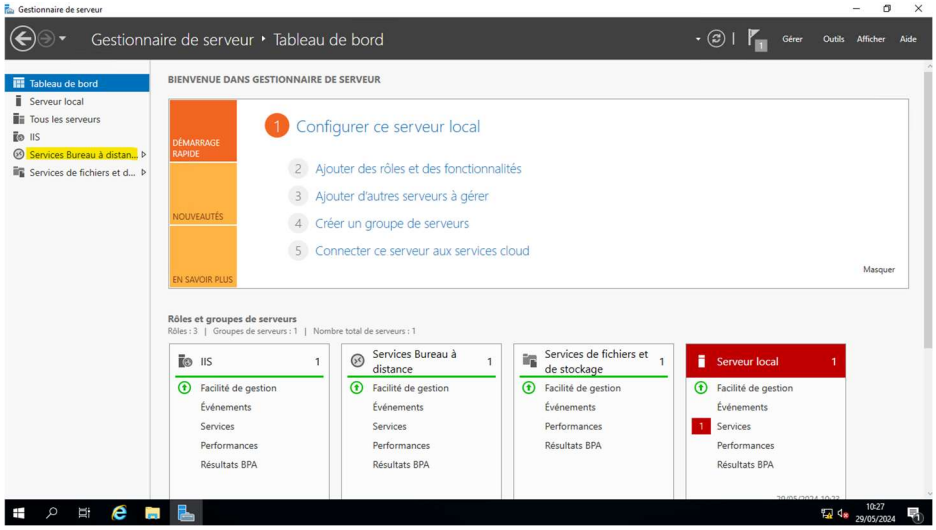
Confirmer les sélections et cocher "Redémarrer automatiquement le serveur de destination si nécessaire"



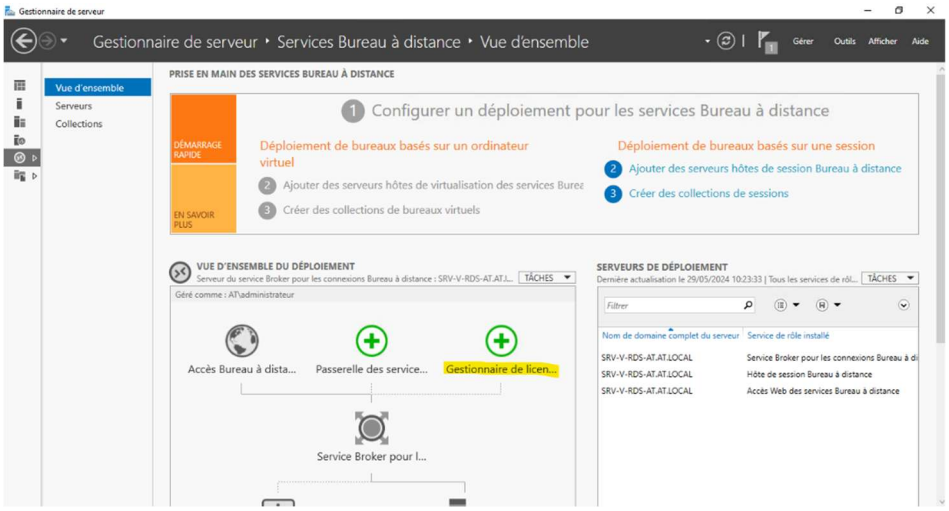
Après un redémarrage, la progression de l'installation des rôles s'affiche



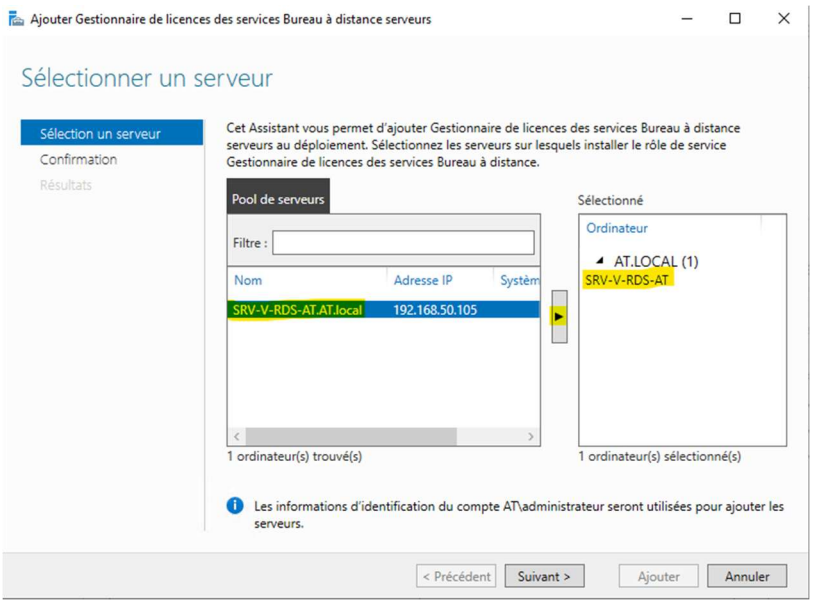
Cliquer sur l'installation des Services Bureau à distance dans le Gestionnaire de serveur



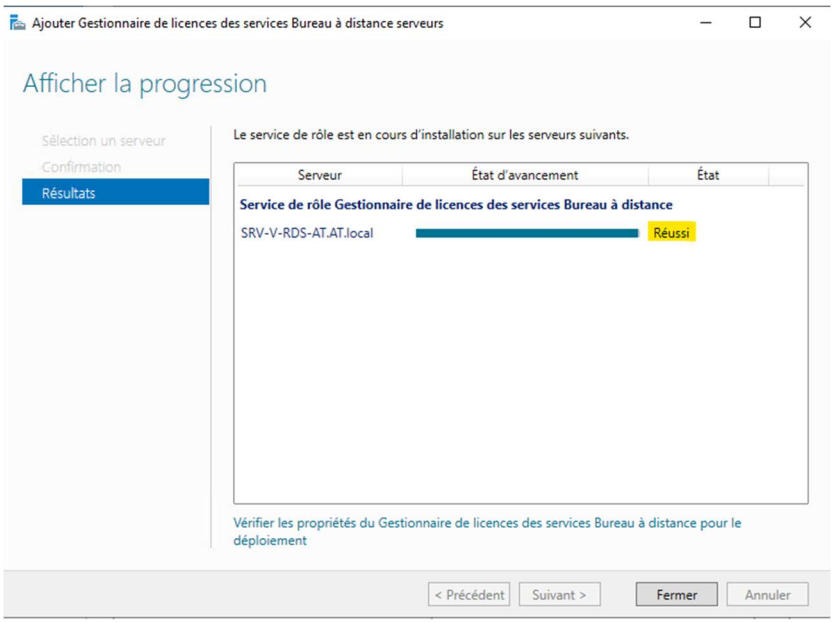
Cliquer sur "Gestionnaire de licences" pour configurer le gestionnaire de licences RDS



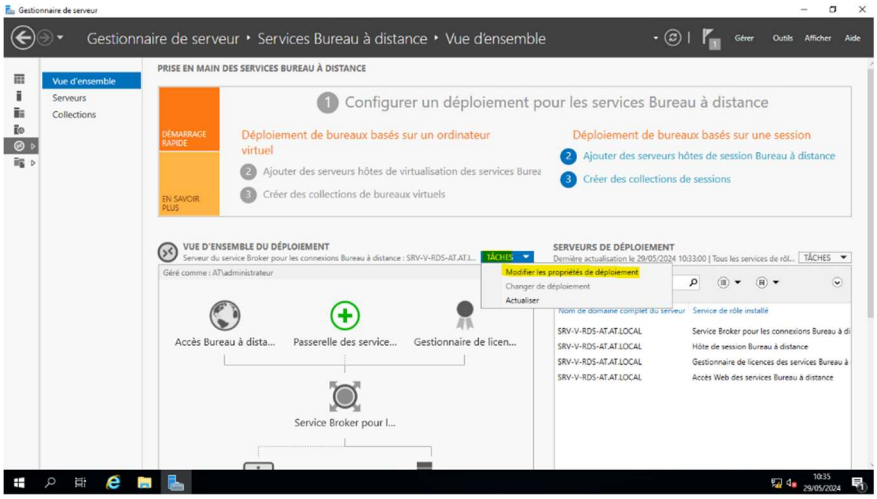
Sélectionner un serveur pour le Gestionnaire de licences des services Bureau à distance



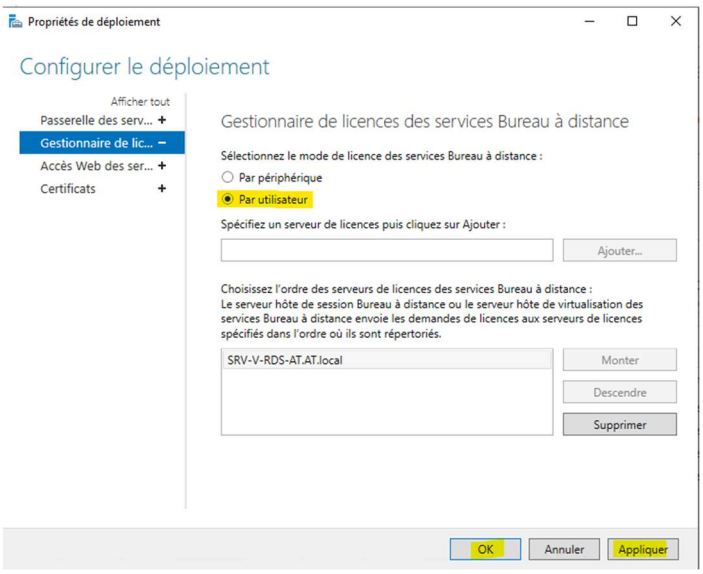
Le gestionnaire s’installe



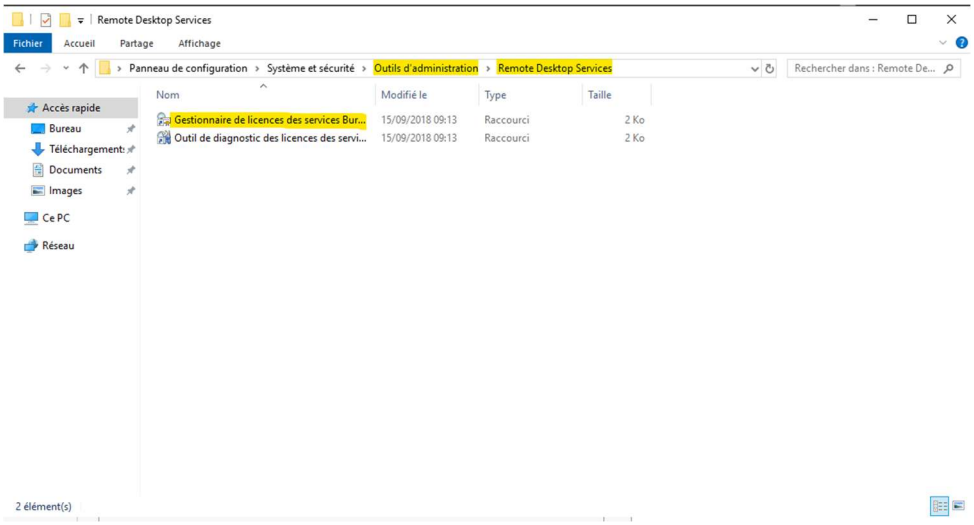
Cliquer sur "Modifier les propriétés de déploiement" pour configurer les paramètres du déploiement RDS



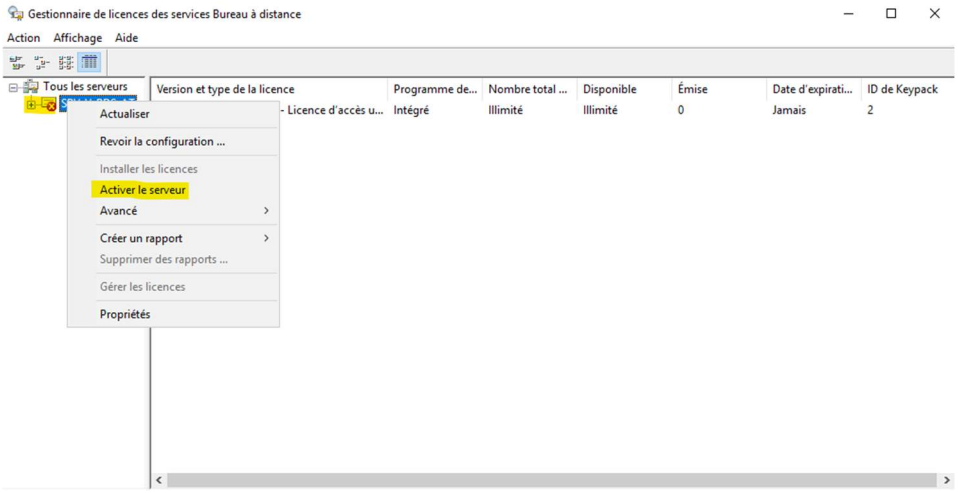
Configurer le mode de licence des services Bureau à distance et choisir "Par utilisateur"



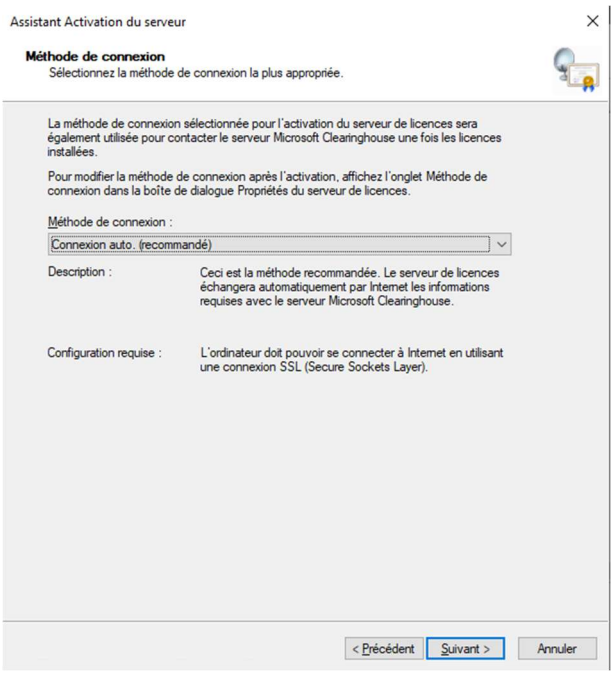
Ouvrir le Gestionnaire de licences des services Bureau à distance depuis les Outils d'administration



Dans le Gestionnaire de licences des services Bureau à distance, cliquer sur "Activer le serveur"

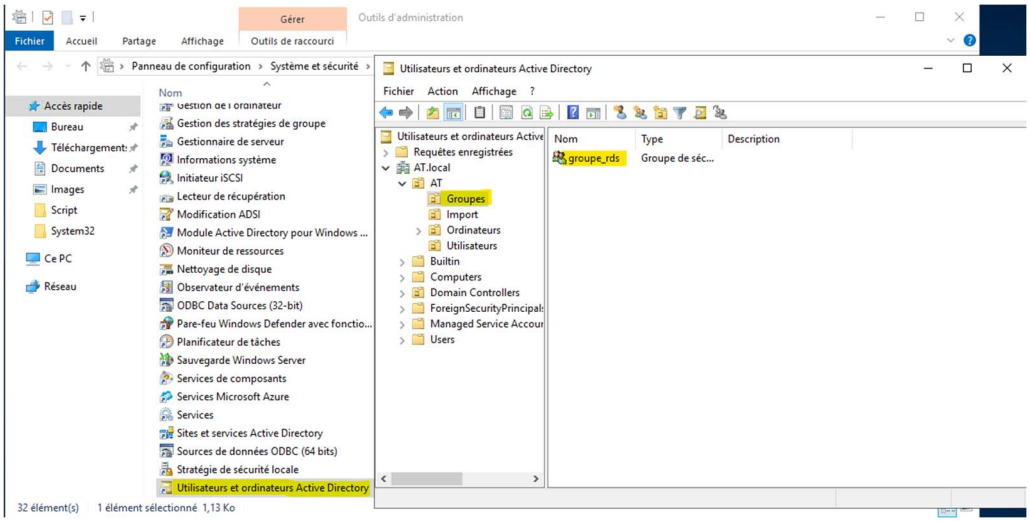


Choisir la méthode de connexion pour l'activation du serveur de licences (Connexion auto. (recommandé)

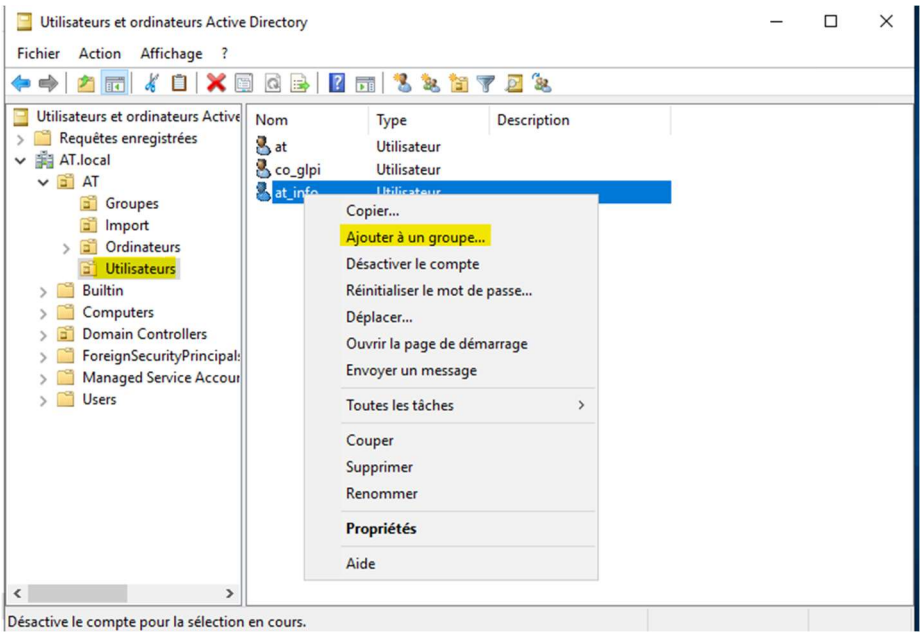


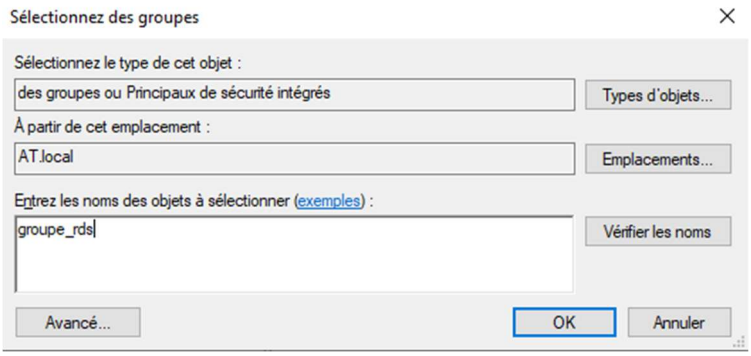
Si on avait des licences RDS, c'est à cette étape qu'on les configurerais. Nous allons maintenant configurer les groupes d'uilisateurs qui auront les droits d'accès au serveur RDS.

Il faut maintenant ouvrir "Utilisateurs et ordinateurs" sur Active Directory depuis les Outils d'administration et créer un groupe RDS.

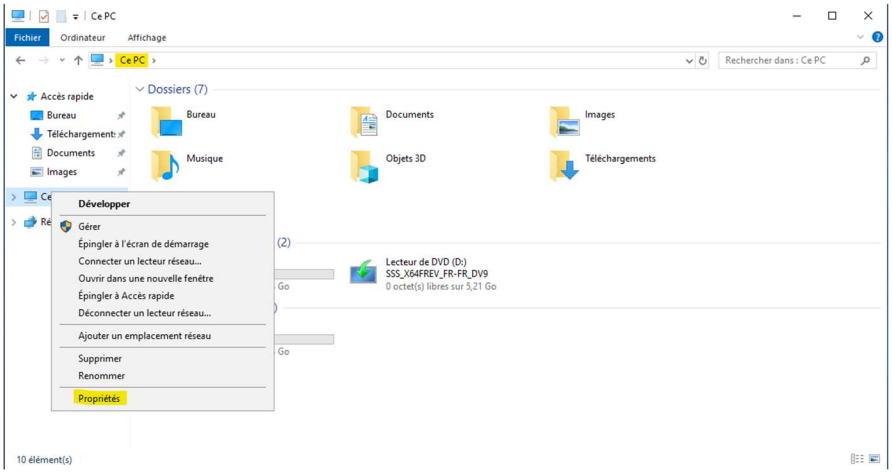


Sur Active Directory, ouvrir "Utilisateurs" et ajouter à un groupe et ajouter les utilisateurs qui auront le droit d'accès a RDS dans le groupe RDS

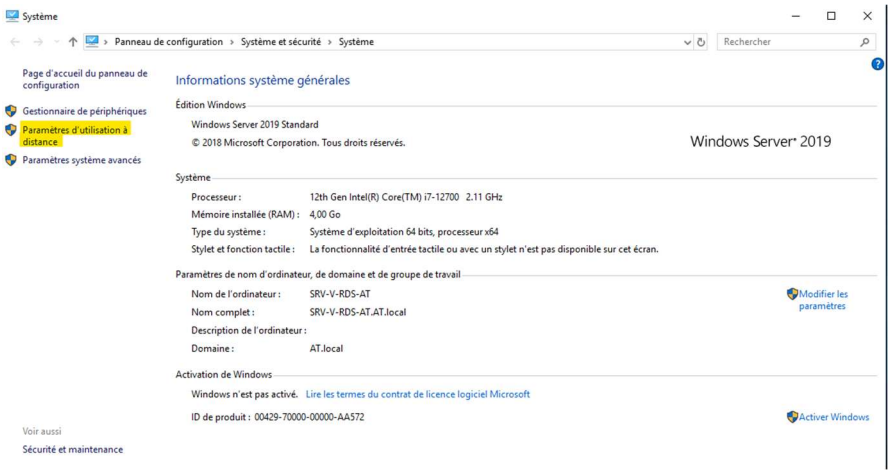




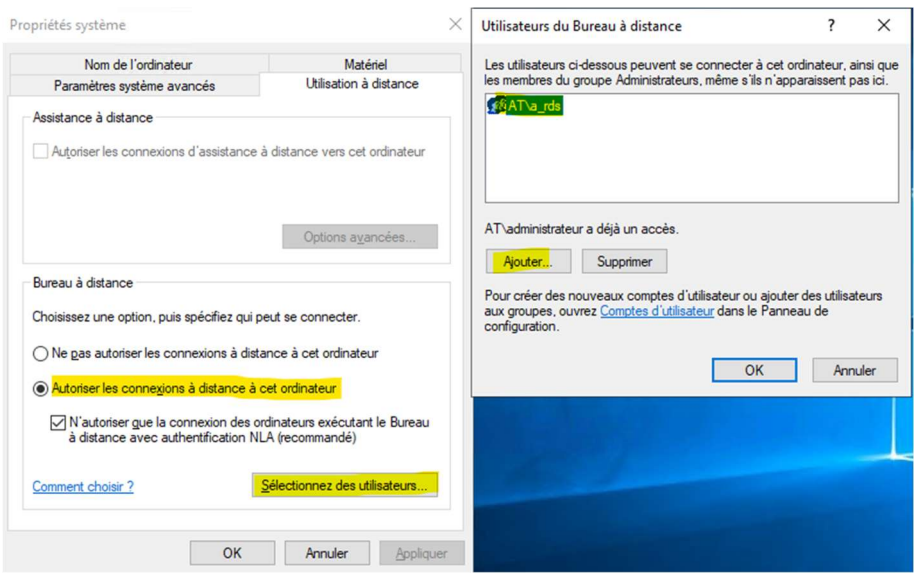
Retourner sur le serveur RDS et ouvrir les propriétés de « ce PC »



Ouvrir les paramètres d'utilisation à distance du système

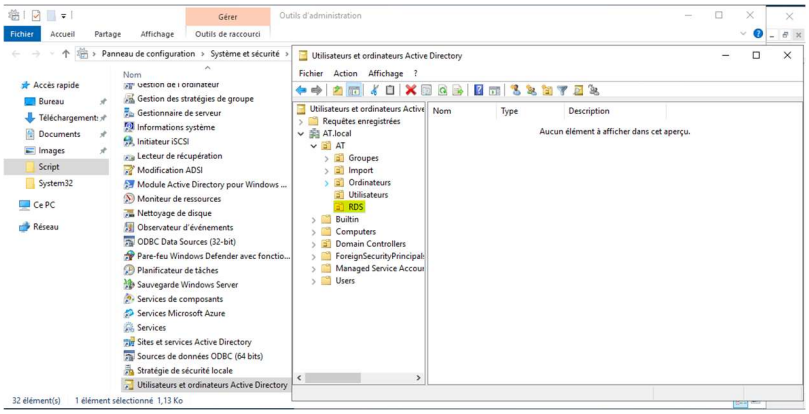


Autoriser les connexions à distance à cet ordinateur et sélectionner le groupe que l'on vient de créer

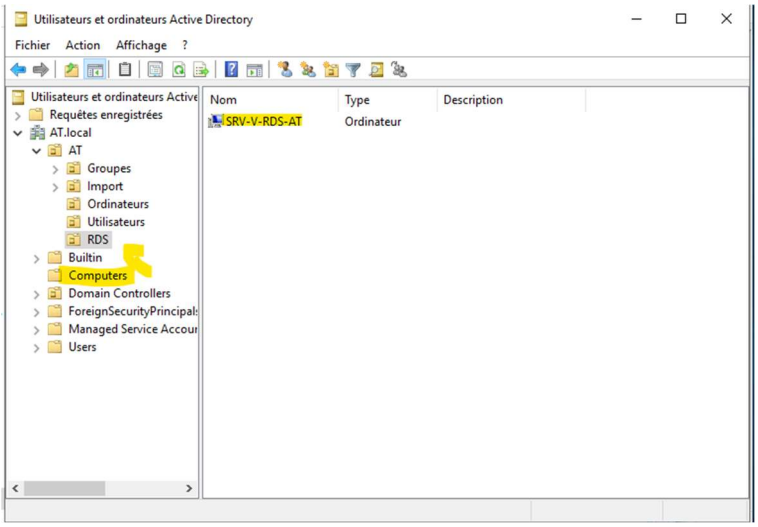


Mise en place de restriction via GPO

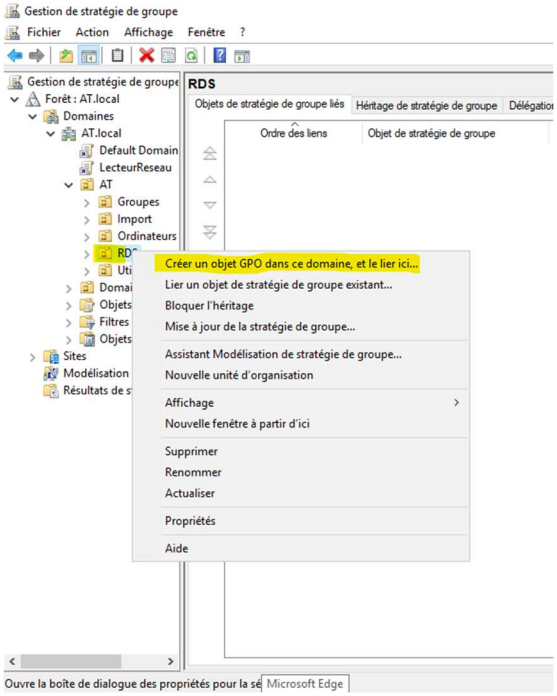
Sur Active Directory, créer une unité d'organisation (UO) pour les services Bureau à distance (RDS)

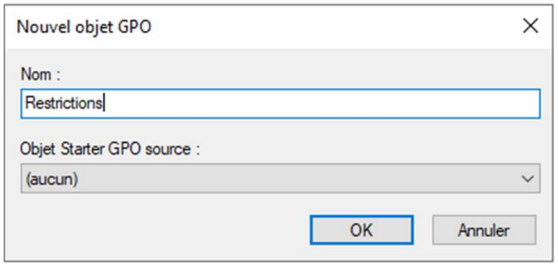


Déplacer le serveur RDS ("SRV-V-RDS-AT") précédemment entré dans le domaine dans l'UO "RDS"

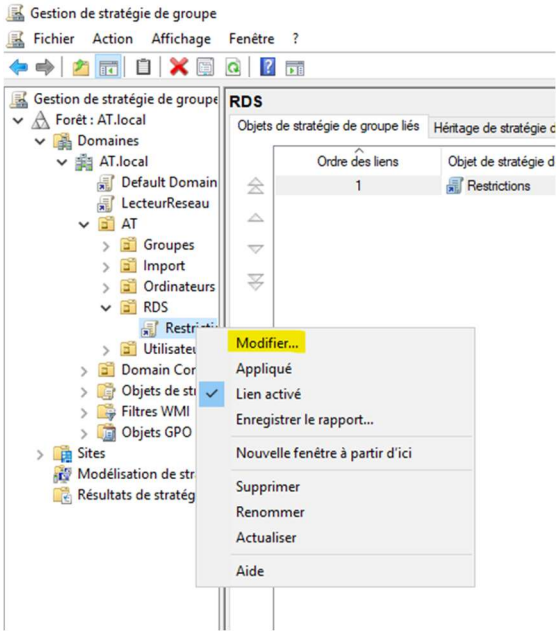


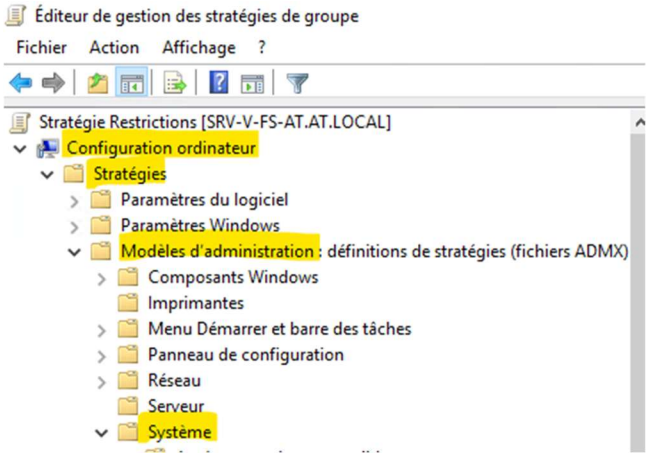
Ouvrir la "Gestion des stratégies de groupe" et sur l'UO RDS, crée un objet GPO dans ce domaine et le lier ici (UO qui ne contient que notre machine RDS) -> La nommer Restrictions



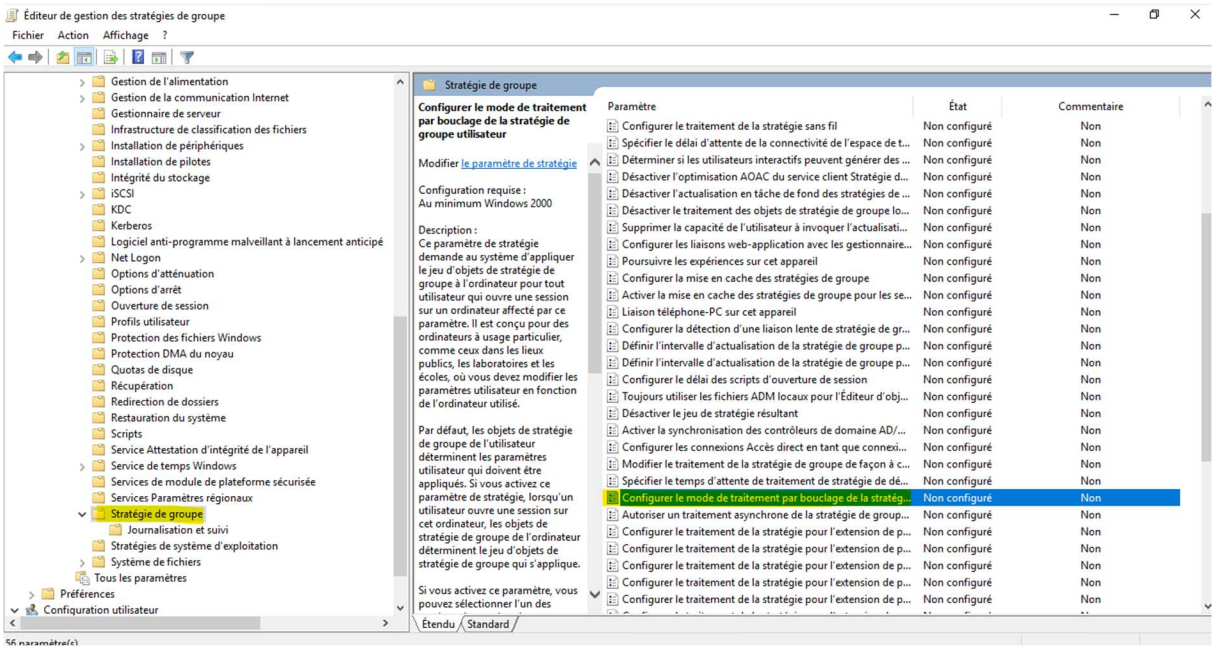


Cliquer sur "Modifier" sur notre GPO et dans l'Éditeur de gestion des stratégies de groupe, aller à "Configuration ordinateur" > "Stratégies" > "Modèles d'administration"

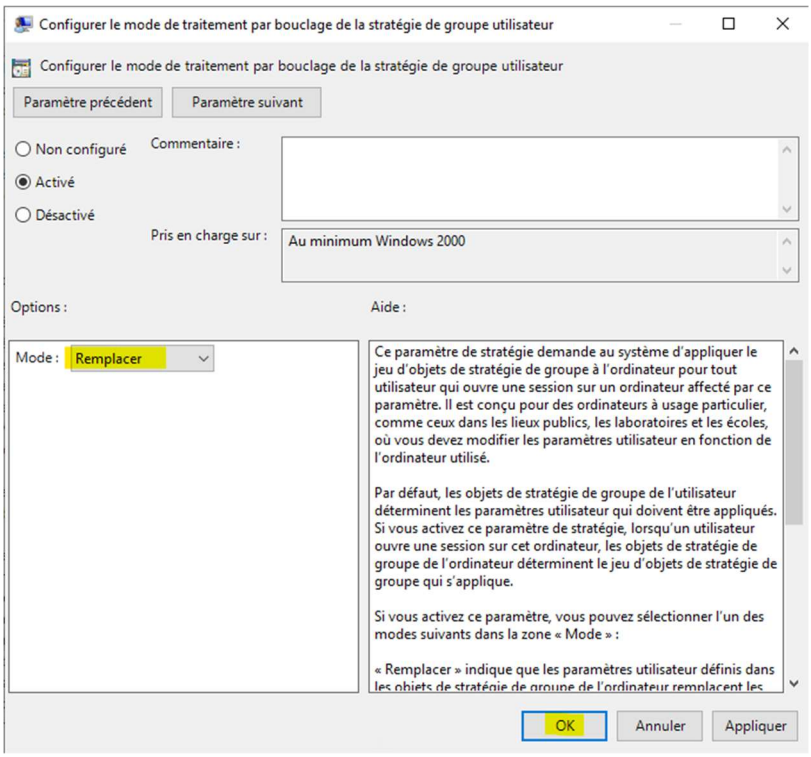




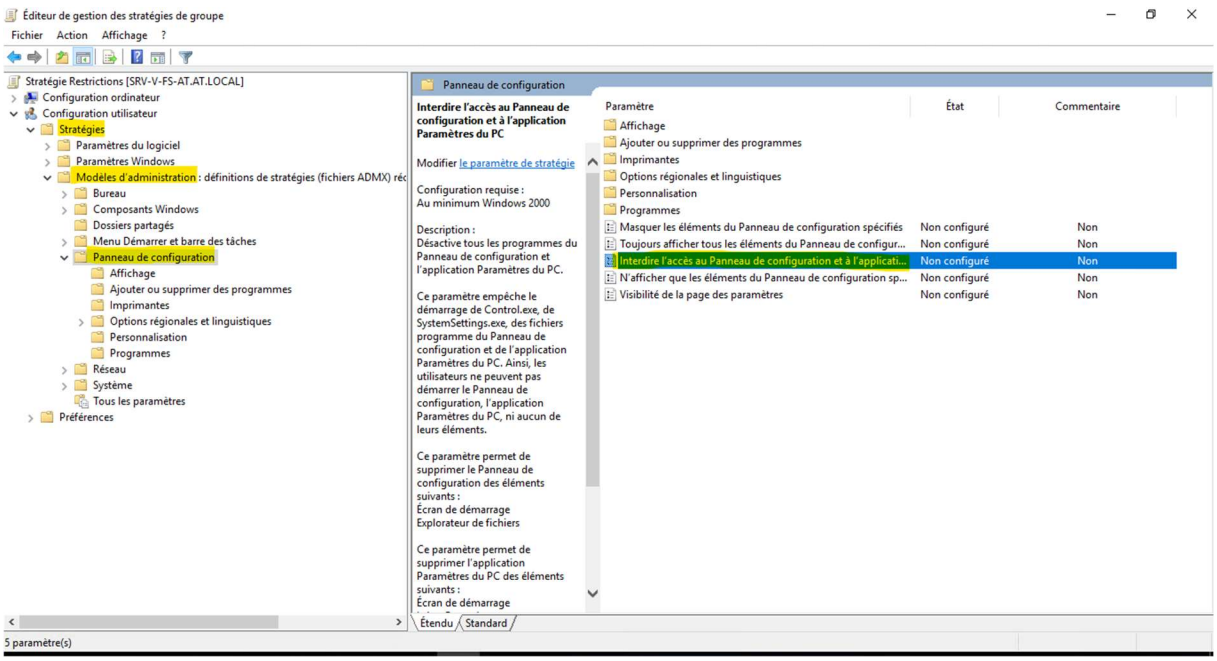
Sous "Modèles d'administration", développer "Composants Windows" et sélectionner "Services Bureau à distance" puis "Hôte de session Bureau à distance" et enfin "Configuration de l'ordinateur \ Configuration du traitement par bouclage de la stratégie de groupe de l'utilisateur"



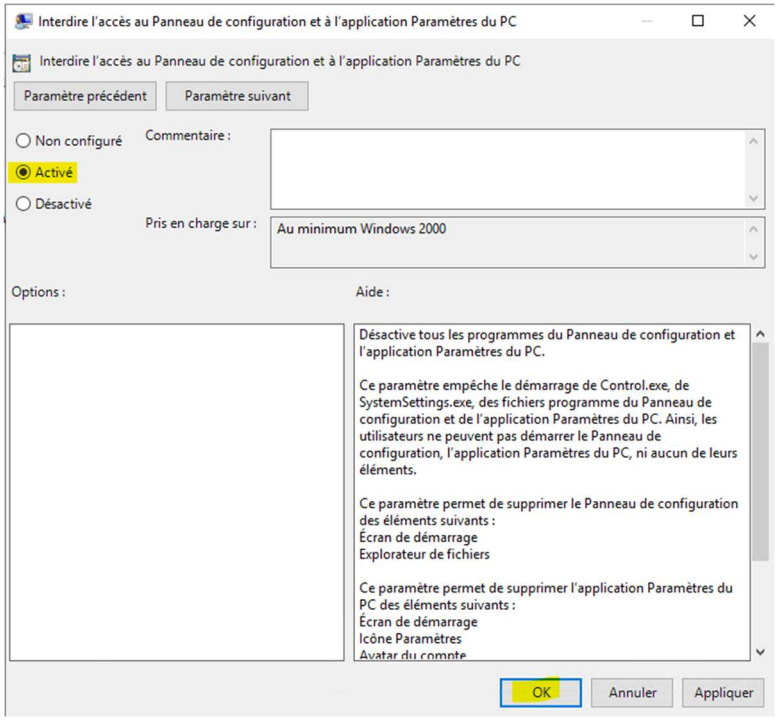
Dans la fenêtre "Configurer le mode de traitement par bouclage de la stratégie de groupe utilisateur", sélectionner "Activé" et choisir le Mode "Remplacer" (pour pouvoir appliquer des GPO utilisateur sur un ordinateur)



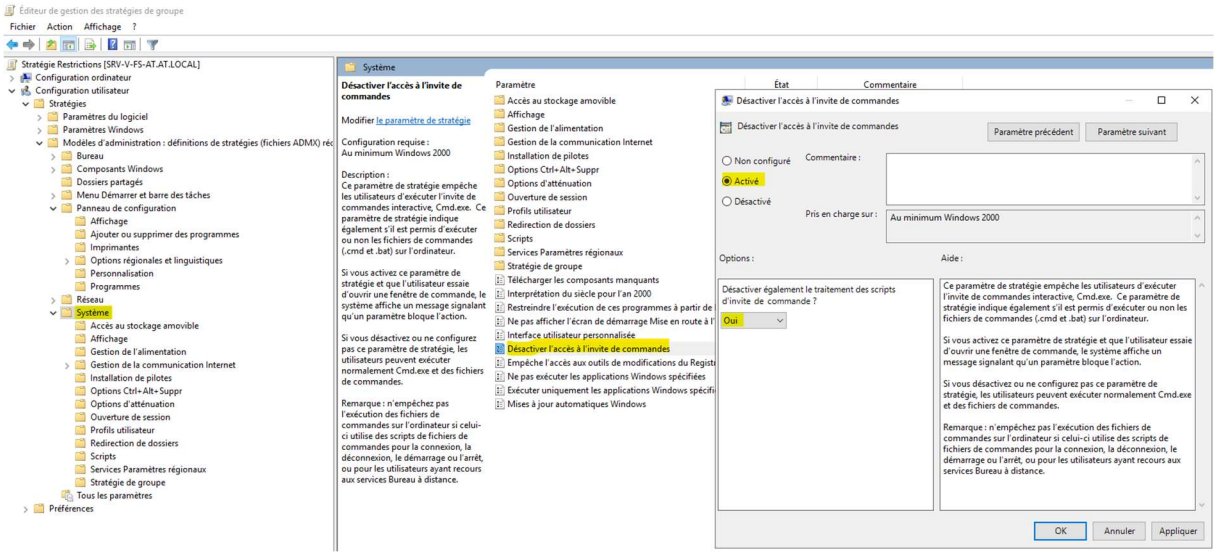
Dans l'Éditeur de gestion des stratégies de groupe, sous "Configuration utilisateur" > "Stratégies" > "Modèles d'administration" > "Panneau de configuration", double-cliquer sur "Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC



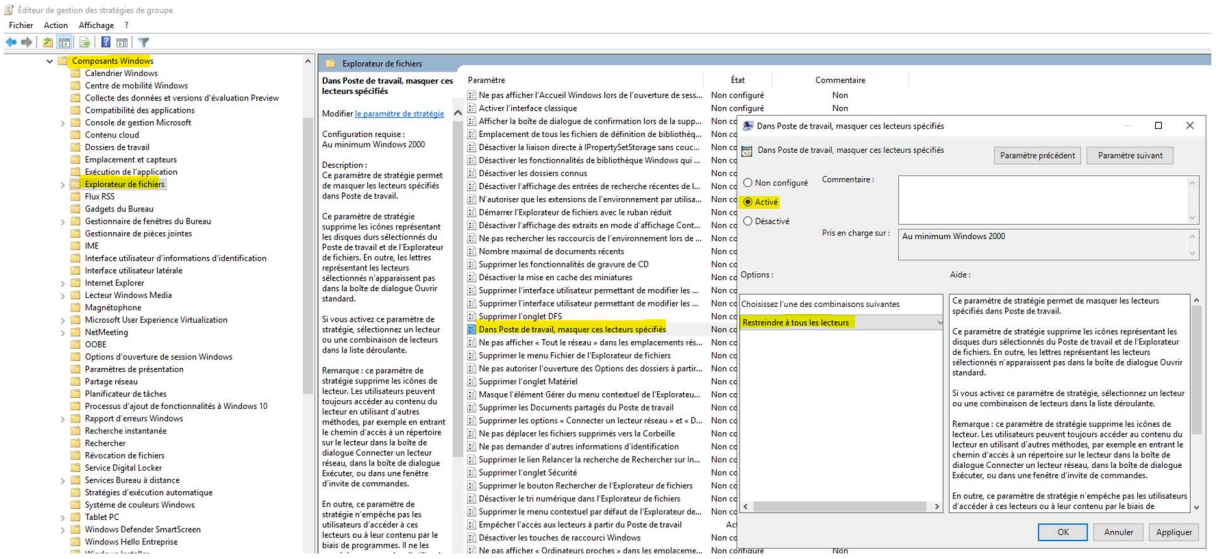
Dans la fenêtre "Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC", sélectionner "Activé" et cliquer sur "OK"



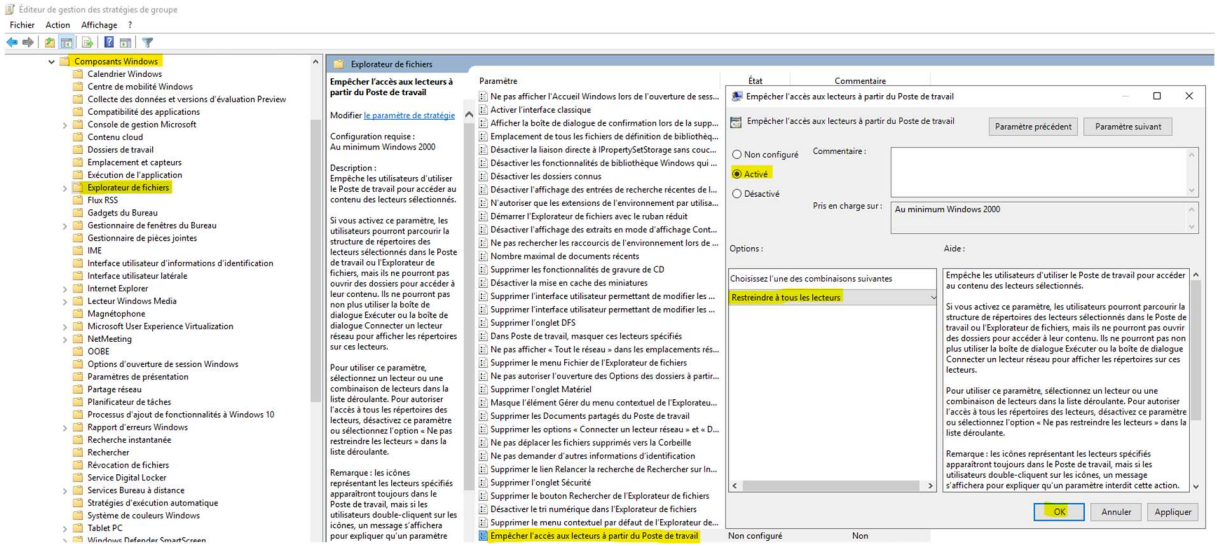
Dans l'Éditeur de gestion des stratégies de groupe, sous "Configuration utilisateur" > "Stratégies" > "Modèles d'administration" > "Système", double-cliquer sur "Désactiver l'accès à l'invite de commandes et dans la fenêtre "Désactiver l'accès à l'invite de commandes", sélectionner "Activé" et cliquer sur "OK"



Dans l'Éditeur de gestion des stratégies de groupe, sous "Configuration utilisateur" > "Stratégies" > "Modèles d'administration" > "Composants Windows" > "Explorateur de fichiers", double-cliquer sur "Masquer les lecteurs spécifiés dans Poste de travail" et dans la fenêtre "Masquer les lecteurs spécifiés dans Poste de travail", sélectionner "Activé" et choisir l'option "Restreindre uniquement les lecteurs A et B". Cliquer ensuite sur "OK"



Dans l'Éditeur de gestion des stratégies de groupe, toujours sous "Configuration utilisateur" > "Stratégies" > "Modèles d'administration" > "Composants Windows" > "Explorateur de fichiers", double-cliquer sur "Empêcher l'accès aux lecteurs à partir de Poste de travail" et dans la fenêtre "Empêcher l'accès aux lecteurs à partir de Poste de travail", sélectionner "Activé" et choisir l'option "Restreindre uniquement les lecteurs A et B". Cliquer ensuite sur "OK"



Dans l'Éditeur de gestion des stratégies de groupe, vous pouvez maintenant voir les stratégies configurées sous l'objet GPO "Restrictions [SRV-V-FS-AT.AT.LOCAL]". Les stratégies activées incluent :

- Configuration ordinateur > Stratégies > Modèles d'administration > Composants Windows > Services Bureau à distance > Hôte de session Bureau à distance > Configuration de l'ordinateur \ Configuration du traitement par bouclage de la stratégie de groupe de l'utilisateur : Activé (Mode : Remplacer)

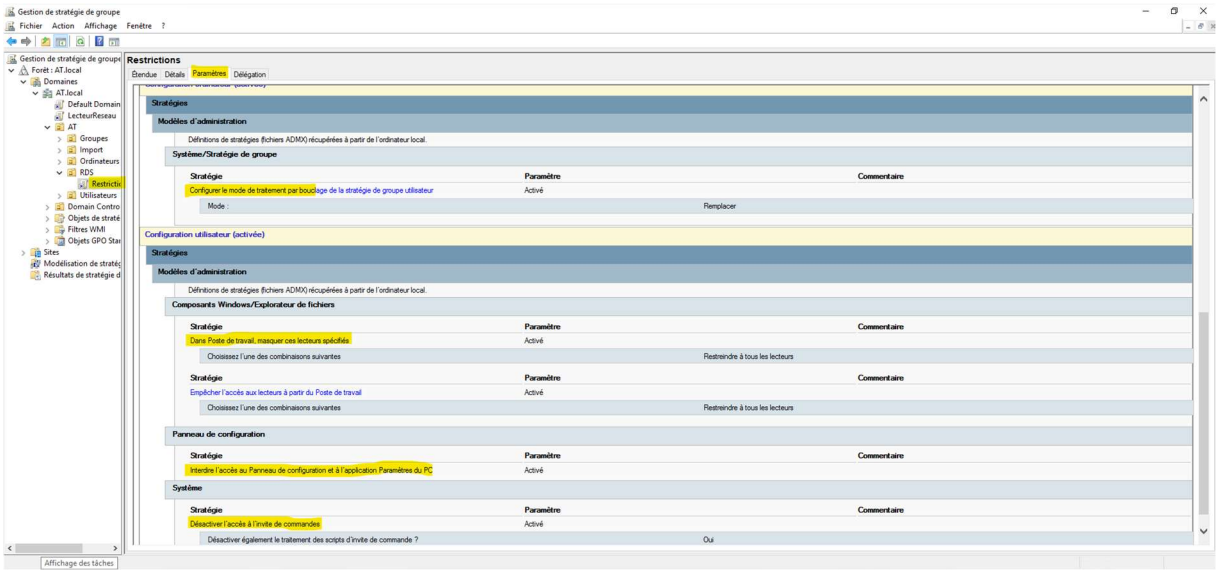
- Configuration utilisateur > Stratégies > Modèles d'administration > Composants Windows > Explorateur de fichiers > Masquer les lecteurs spécifiés dans Poste de travail : Activé (Restreindre uniquement les lecteurs A et B)

- Configuration utilisateur > Stratégies > Modèles d'administration > Composants Windows > Explorateur de fichiers > Empêcher l'accès aux lecteurs à partir de Poste de travail : Activé (Restreindre uniquement les lecteurs A et B)

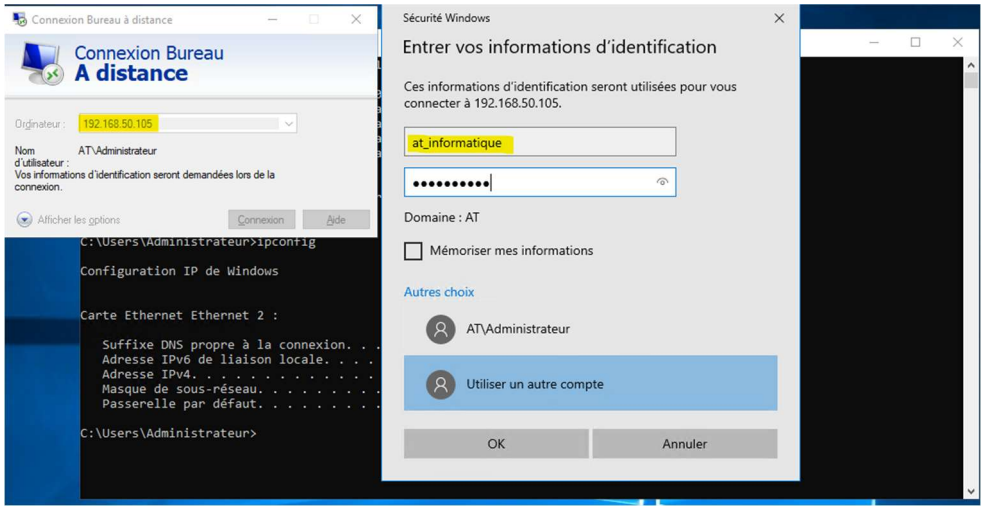
- Configuration utilisateur > Stratégies > Modèles d'administration > Panneau de configuration > Interdire l'accès au Panneau de configuration et à l'application Paramètres du PC : Activé

- Configuration utilisateur > Stratégies > Modèles d'administration > Système > Désactiver l'accès à l'invite de commandes : Activé

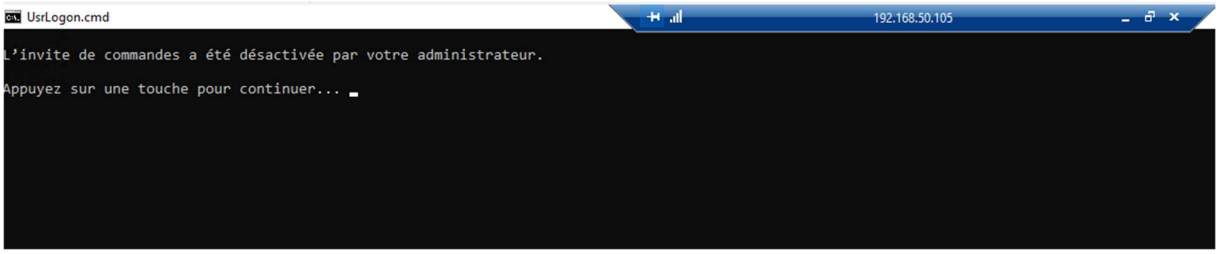
Ces stratégies seront appliquées aux utilisateurs qui se connectent aux serveurs RDS situés dans l'UO "RDS"



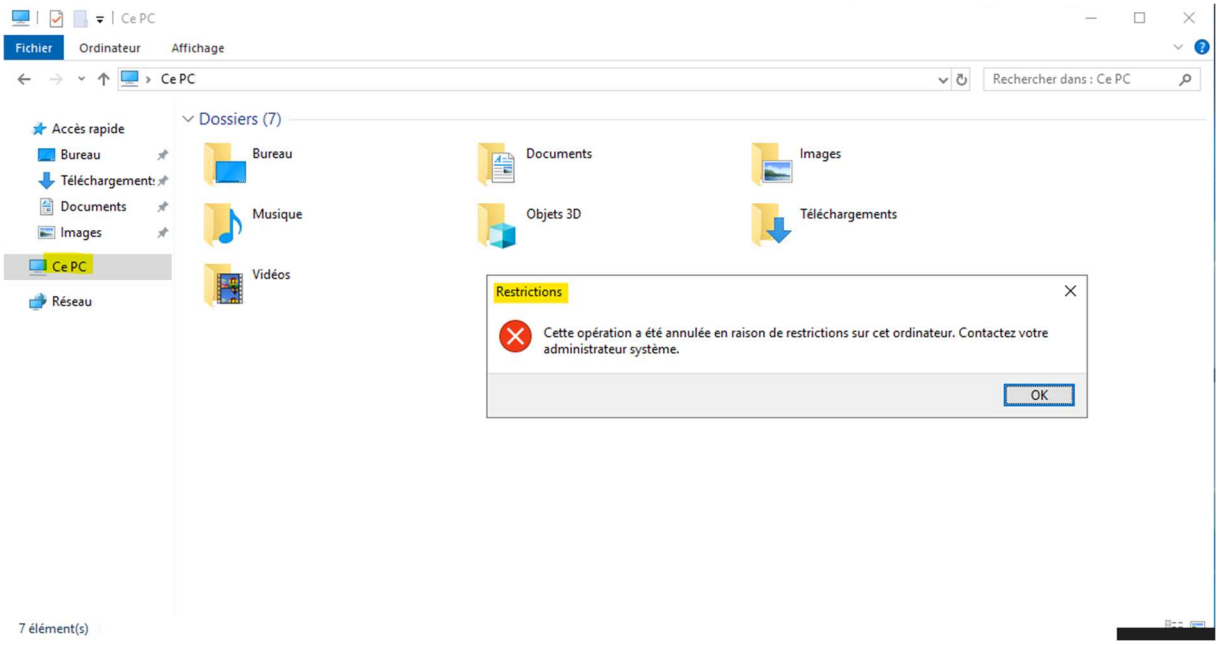
Pour effectuer un test, nous allons essayer avec l'utilisateur « at_informatique » précédemment mis dans le groupe RDS.



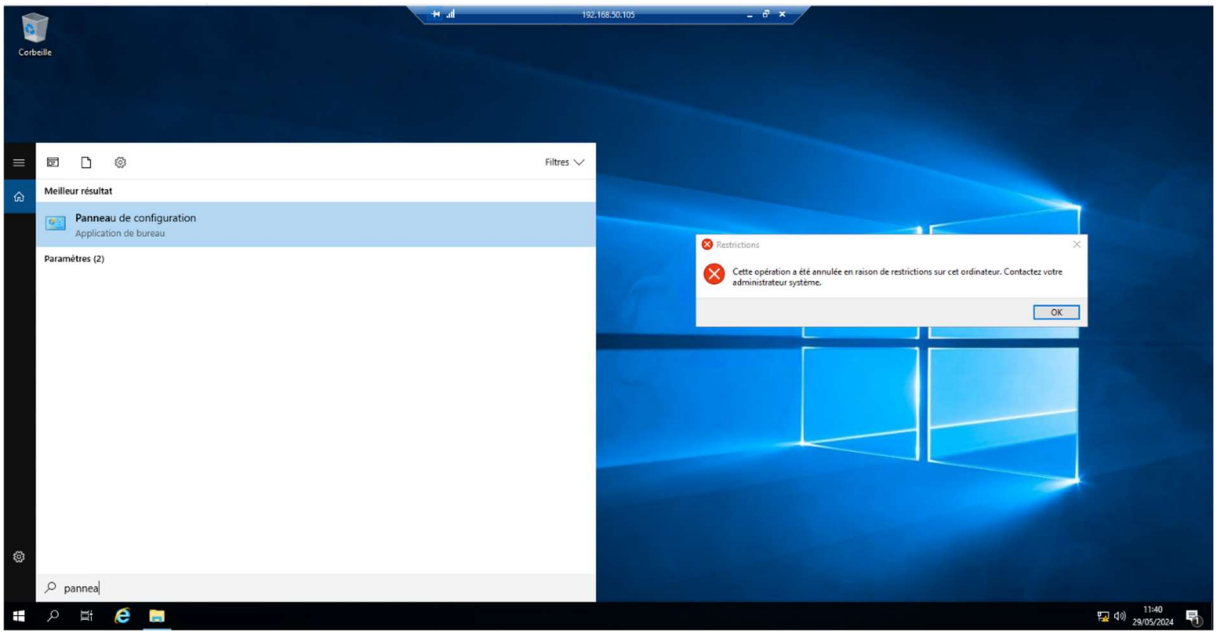
A la connexion, ce message doit apparaitre



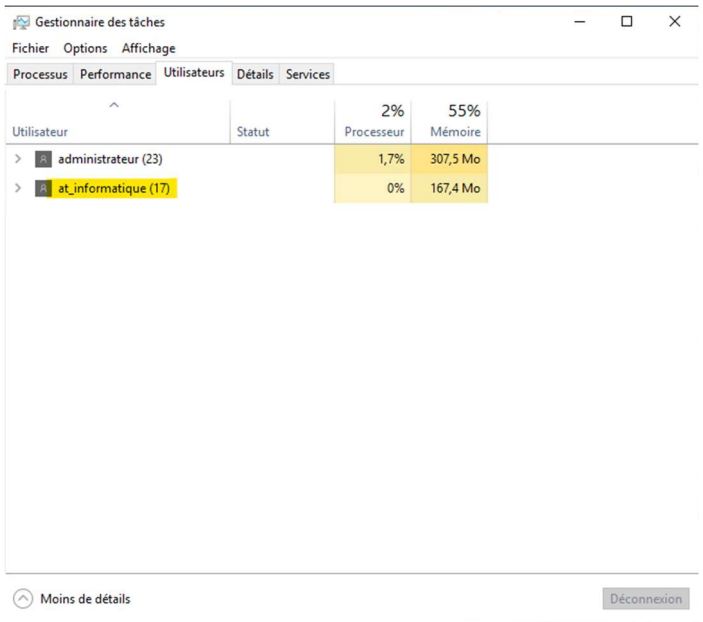
Message d'erreur "Restrictions" : "Cette opération a été annulée en raison de restrictions sur cet ordinateur." lors de l'accès à "Ce PC"

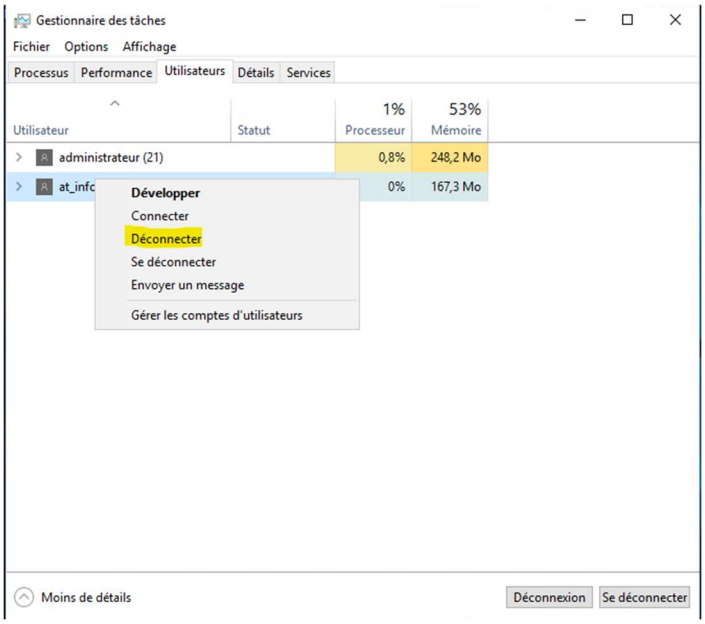


Le panneau de configuration est également bien désactivé



Le gestionnaire des tâches du serveur RDS affiche les utilisateurs connectés. "at_informatique" est connecté et nous avons la possibilité de le deconnecter





Conclusion

Et voilà, nous avons installé les services Bureau à distance (RDS) et mis en place des restrictions d'utilisation via une Stratégie de Groupe (GPO) dans un environnement Active Directory. L'objectif était de sécuriser l'accès au serveur RDS pour les utilisateurs en limitant leurs capacités d'interaction avec le système.

Vérification de bon fonctionnement :

Test utilisateur : Connectez-vous au serveur RDS avec le compte restreint et essayez d'ouvrir l'invite de commandes, d'accéder aux lecteurs A et B dans l'Explorateur, et d'ouvrir le Panneau de configuration. Les messages d'erreur de restriction doivent confirmer l'application des stratégies.

Vérification administrateur : En tant qu'administrateur, utilisez le Gestionnaire des tâches pour voir la session de l'utilisateur et confirmez la possibilité de la gérer (déconnexion).

Confirmation de la GPO : Sur le serveur RDS, connecté avec l'utilisateur restreint, exécutez la commande gpresult /r pour vous assurer que la GPO "Restrictions RDS" est bien appliquée.

Points de vigilance et Conseils de sécurité :

- Portée et ordre des GPO : Vérifiez que la GPO s'applique uniquement aux serveurs RDS via l'UO et que son ordre d'application ne soit pas bloqué par d'autres GPO.
- Tests : Testez les restrictions dans un environnement isolé avant de les appliquer en production pour éviter tout impact inattendu.
- Documentation : Documentez les GPO créées pour faciliter la gestion future.
- Mises à jour : Maintenez les systèmes à jour pour bénéficier des derniers correctifs de sécurité.
- Moindre privilège : Limitez l'accès des utilisateurs au strict nécessaire.
- Surveillance : Surveillez les activités sur le serveur pour détecter toute tentative de contournement.
- Information : Informez les utilisateurs des restrictions.
- Révision : Examinez régulièrement les stratégies pour les adapter aux besoins.
- Sauvegardes : Sauvegardez régulièrement l'environnement AD et la configuration RDS.