Mise en place d'un serveur RDS en RemoteApp avec une GPO

1. Introduction :

Dans un environnement professionnel moderne, l'accès distant aux applications est un enjeu stratégique pour garantir la flexibilité des employés tout en centralisant les ressources informatiques. Remote Desktop Services (RDS) est une solution permettant d'exécuter des applications sur un serveur distant et de les mettre à disposition des utilisateurs via le protocole RDP (Remote Desktop Protocol). Grâce à la fonctionnalité RemoteApp, il est possible de publier ces applications de manière transparente, comme si elles étaient exécutées localement sur les postes clients.

Ce projet consiste à déployer un serveur RDS en RemoteApp, avec une gestion centralisée des accès via une stratégie de groupe (GPO). Cette maquette reproduit l'infrastructure que j'ai eu l'occasion de mettre en place en entreprise durant ma formation. Elle repose sur l’architecture existante du Projet 1, comprenant un Active Directory répliqué et des UTM DynFi en haute disponibilité (HA). L'objectif est de démontrer comment intégrer un serveur RDS de manière sécurisée et optimisée.

Ce document détaille les étapes nécessaires à l’installation et à la configuration d’un serveur RDS sous Windows Server 2022, en intégrant la gestion des accès via Active Directory et en optimisant la sécurité grâce au pare-feu DynFi. Enfin, nous verrons comment automatiser le déploiement des applications RemoteApp sur les postes clients grâce aux stratégies de groupe.

Prérequis et architecture réseau

Avant d’entamer l’installation et la configuration de RDS, plusieurs éléments doivent être en place :

- Un Active Directory fonctionnel avec réplication (AD01 et AD02) afin de centraliser la gestion des utilisateurs et des autorisations d’accès.
- Un pare-feu DynFi en HA, assurant la protection des flux réseau entrants et sortants.
- Un serveur Windows Server 2022 dédié à l’hébergement de RDS.
- Des postes clients sous Windows, compatibles avec le déploiement des stratégies de groupe (GPO).

Stratégie de Groupe

Une Stratégie de Groupe (GPO) est un outil permettant d'appliquer des configurations et des politiques de sécurité de manière centralisée sur un réseau. Elle est utilisée pour définir des règles qui affectent les utilisateurs ou les ordinateurs dans un environnement Active Directory. Cela permet aux administrateurs d’imposer des paramètres systèmes, des restrictions d'accès, ou de déployer des applications sur plusieurs machines à la fois.

Rôle des GPO dans un Déploiement RDS

Dans le cadre de Remote Desktop Services (RDS), les GPO permettent de gérer les accès et les configurations de manière centralisée. Elles facilitent le déploiement des applications RemoteApp, en assurant que les utilisateurs y accèdent.

Configuration du Dynfi

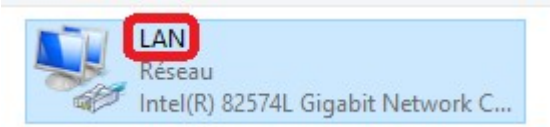
Une partie essentielle de l'implémentation d'un serveur RDS est la gestion de la sécurité du réseau. Le protocole RDP, utilisé pour accéder aux bureaux distants ou aux applications RemoteApp, fonctionne par défaut sur le port 3389. Dans un environnement sécurisé, il est nécessaire de configurer le pare-feu pour permettre le passage des connexions RDP tout en assurant que seules les connexions autorisées peuvent atteindre le serveur.

Dans notre infrastructure, nous utilisons un pare-feu DynFi en haute disponibilité (HA) pour protéger les flux réseau entrants et sortants. Pour permettre la communication RDP entre les sous-réseaux, nous devons ajouter une règle spécifique au niveau du pare-feu pour autoriser le trafic sur le port 3389 entre le LAN serveur et le LAN utilisateurs.

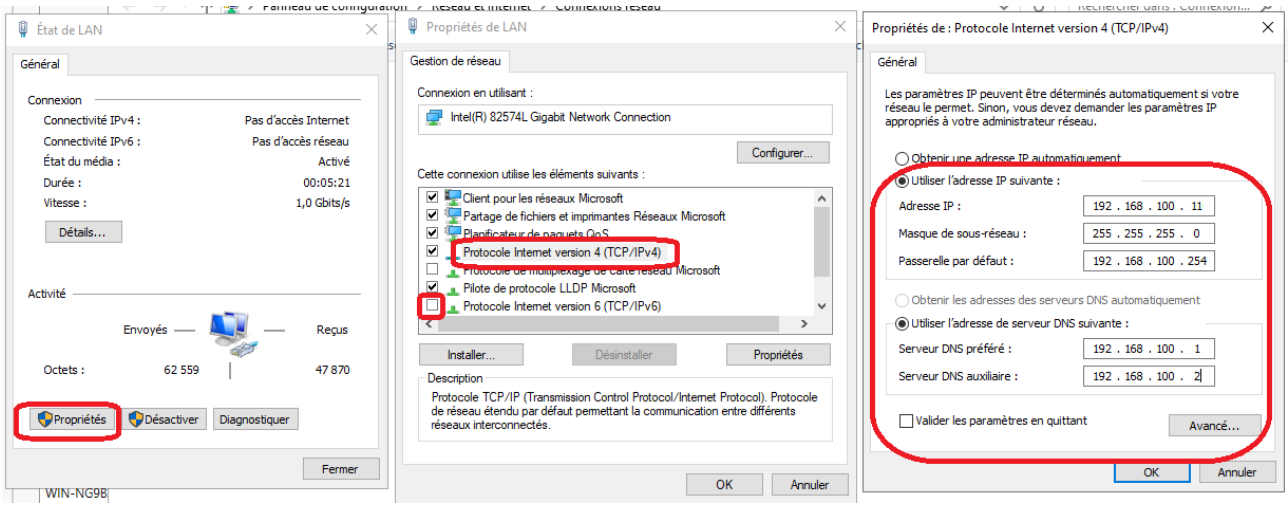
Installation du serveurs RDS

Pour commencer, Après avoir monté l'ISO de Windows Server 2022 sur l'hyperviseur et lancé l'installation, nous arrivons à une fenêtre nous permettant de sélectionner la langue du système. Une fois cette étape validée, nous cliquons sur "Suivant", puis choisissons "Reporter à plus tard" avant de définir le mot de passe du compte administrateur du contrôleur de domaine. Une fois connecté au serveur, nous ouvrons le Gestionnaire de serveur pour configurer la carte réseau, notamment en modifiant son nom et en attribuant une adresse IP statique. Pour cela, nous accédons aux paramètres de l'adressage IP du serveur.

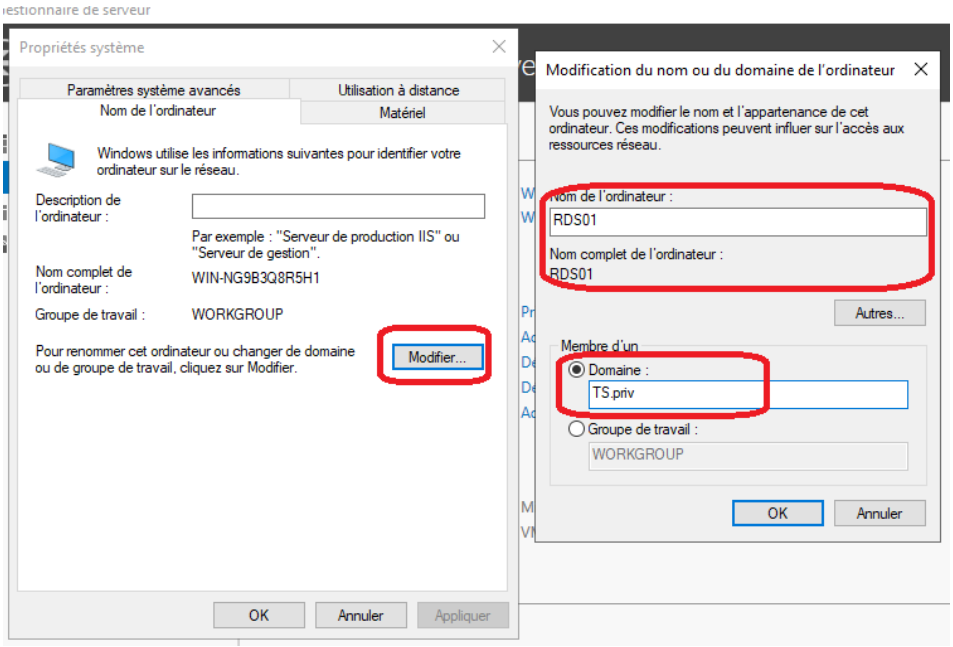
La première action consiste à renommer la carte réseau en "LAN" afin d'en faciliter l'identification.



Ensuite, nous configurons l'adresse IP de la machine en lui attribuant 192.168.100.11/24. La passerelle par défaut est définie sur 192.168.100.254, correspondant à l'adresse de nos Dynfi. Pour les serveurs DNS, nous spécifions 192.168.100.1 et 192.168.100.2, représentant les deux contrôleurs de domaine responsables de la réplication DNS.

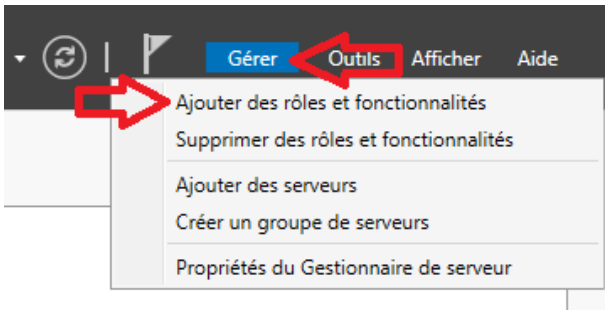


Une fois ces paramètres enregistrés, nous revenons dans le Gestionnaire de serveur, puis nous accédons à la section "Serveur local" pour renommer le serveur. Il suffit de cliquer sur "Modifier", d'entrer le nouveau nom (RDS01), puis d'adhérer le serveur au domaine en lui indiquant TS.priv, et enfin de valider en cliquant sur "OK". Afin de prendre en compte le changement de nom et l'adhésion au domaine, un redémarrage du serveur sera nécessaire.

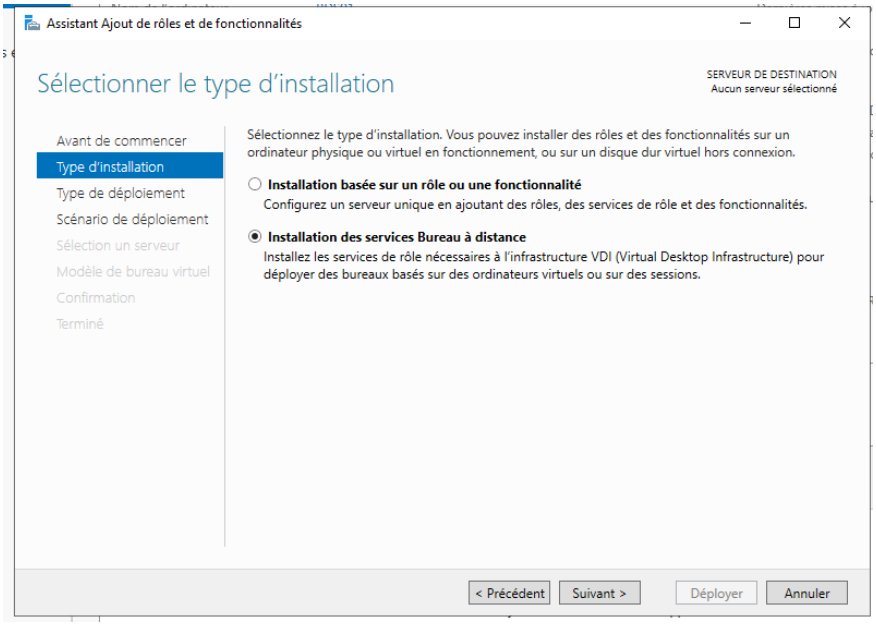


Déploiement et configuration de RDS

Une fois connectés au serveur avec un compte disposant des droits d'administration, nous ouvrons le Gestionnaire de serveur. Ensuite, nous cliquons sur "Gérer" en haut à droite, puis sélectionnons "Ajouter des rôles et fonctionnalités".



Plutôt que de choisir l'option par défaut, nous sélectionnons "Installation des services Bureau à distance". Puis, nous poursuivons ensuite l'assistant.



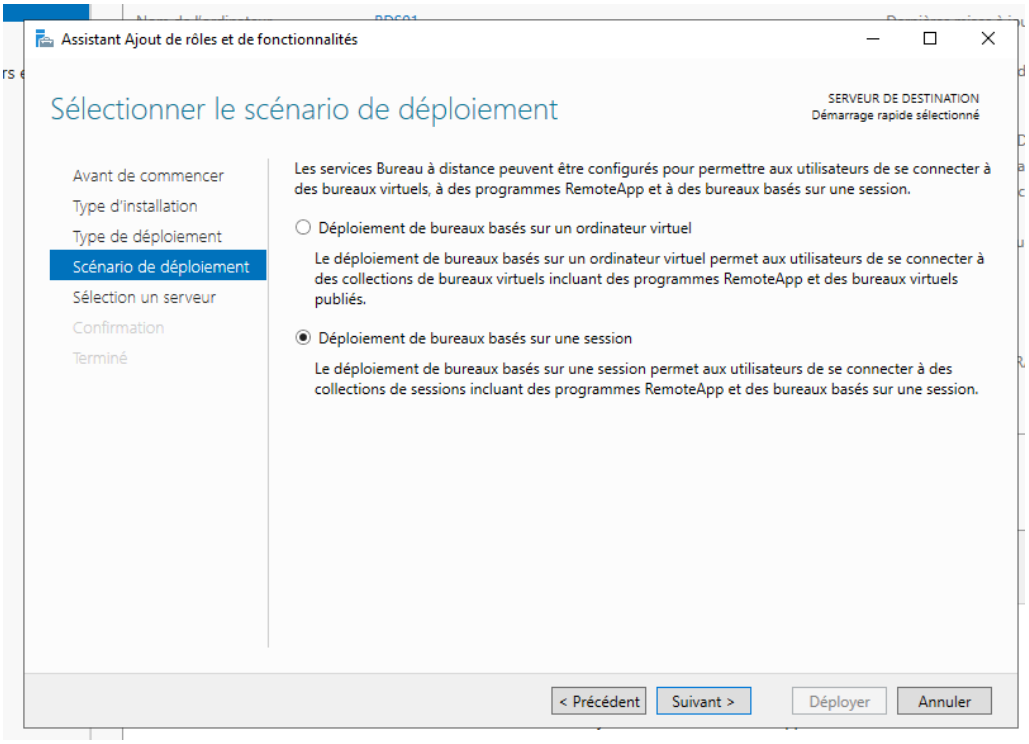
Lorsque nous déployons le rôle RDS sur un seul serveur, nous pouvons opter pour le "Démarrage rapide", ce qui permet d'installer et de pré-configurer les composants nécessaires. Toutefois, nous reviendrons ensuite sur la configuration pour personnaliser davantage l'installation.

Trois rôles seront automatiquement installés sur le serveur :

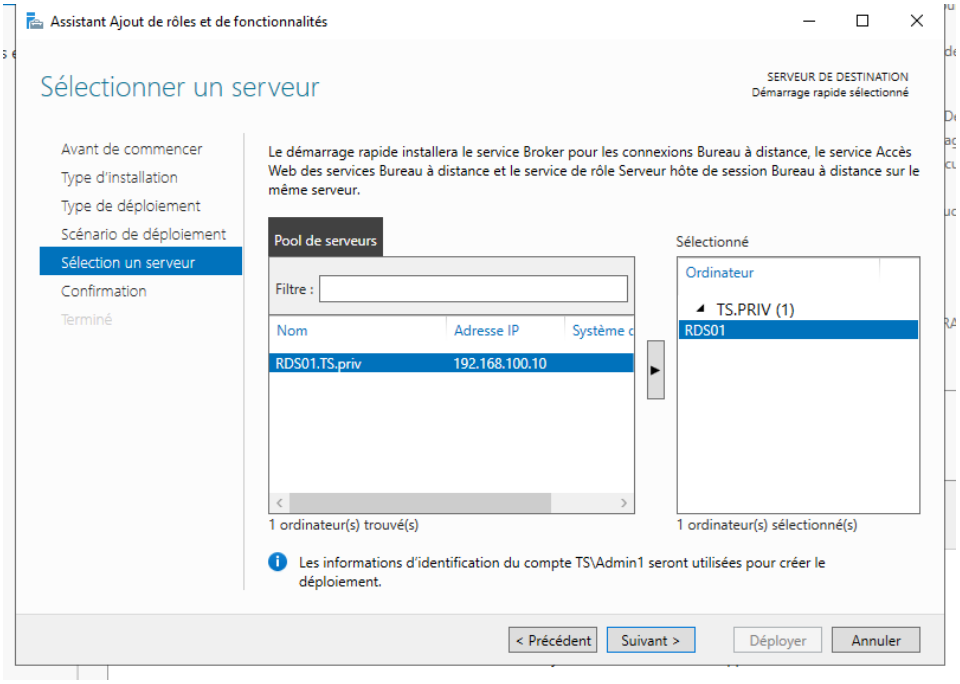
- Le Broker RDS : Ce rôle permet de répartir les utilisateurs entre plusieurs serveurs (lorsqu'il y en a plusieurs) et gère également les sessions, qu'il stocke dans une base de données. Cela permet aux utilisateurs de se reconnecter à leur session sur le bon serveur en cas de coupure.

- L'accès RDS via le portail web : Ce rôle permet aux utilisateurs d'accéder aux applications publiées (RemoteApp) directement à partir de leur navigateur web.
- Le rôle RDS : C'est le rôle principal pour la gestion des connexions à distance et l'exécution des applications publiées.

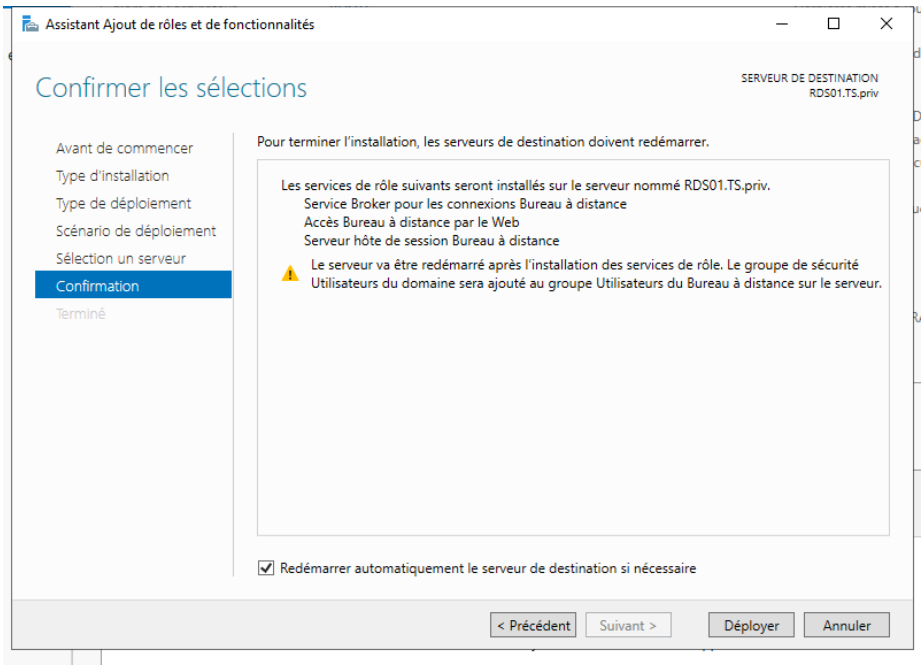
Nous avons désormais le choix entre deux scénarios de déploiement : le déploiement basé sur des sessions ou le déploiement basé sur des ordinateurs virtuels. Nous allons opter pour le déploiement basé sur des sessions, car cela permettra aux utilisateurs d’accéder à un bureau ou à des applications via une session sur un serveur, plutôt que d'utiliser des machines virtuelles dédiées. Pour ce faire, sélectionnons l'option "Déploiement de bureaux basés sur une session".



Sélectionnons maintenant le serveur sur lequel nous allons réaliser l'installation. Dans notre cas, il s'agit de "RDS01". Ce serveur sera l'hôte sur lequel les rôles RDS seront installés.

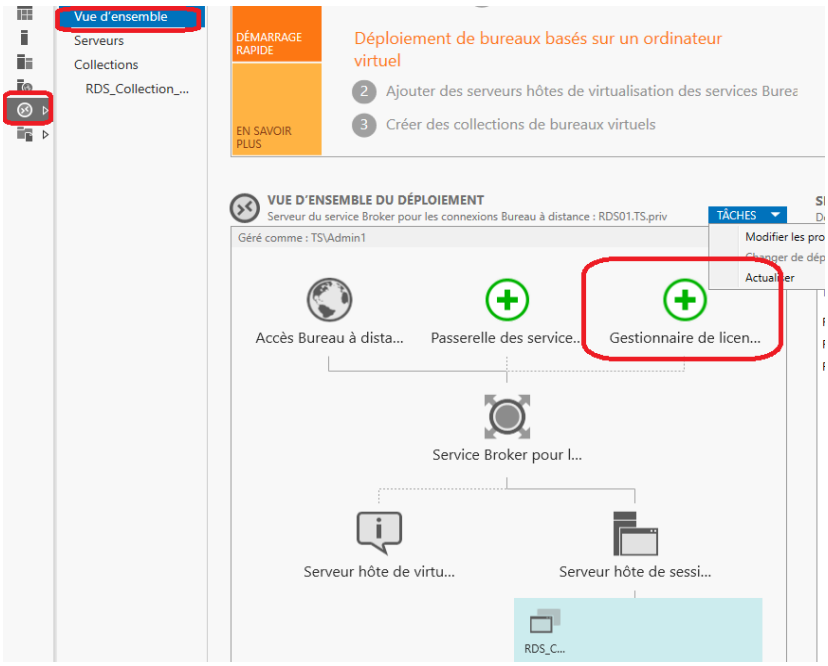


Pour commencer l'installation des rôles, cochez la case "Redémarrer automatiquement le serveur de destination si nécessaire", puis cliquez sur "Déployer". Cela permettra à l'assistant de procéder à l'installation des composants nécessaires, et redémarrera automatiquement le serveur si cela est requis pour terminer le processus.

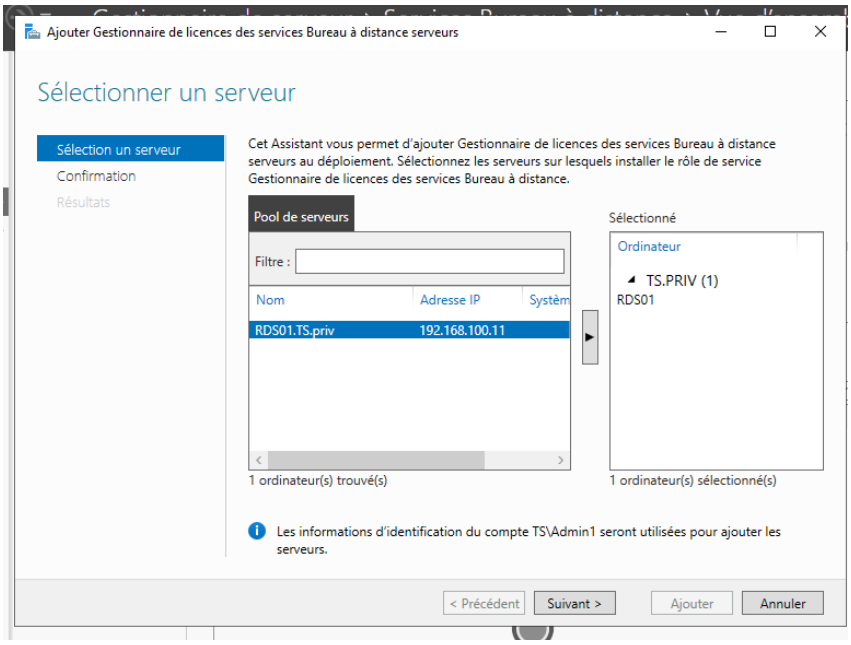


Par le biais du Gestionnaire de serveur, nous pouvons accéder à la gestion des services Bureau à distance. Dans la Vue d'ensemble du déploiement, il vous suffit de double-cliquer sur le "Gestionnaire de licence" pour démarrer l'installation de ce composant.

Il est essentiel de disposer d'un gestionnaire de licence RDS pour pouvoir intégrer vos CAL RDS (Client Access Licenses). Ces licences seront ensuite attribuées à vos utilisateurs ou périphériques pour permettre l'accès aux services Bureau à distance.

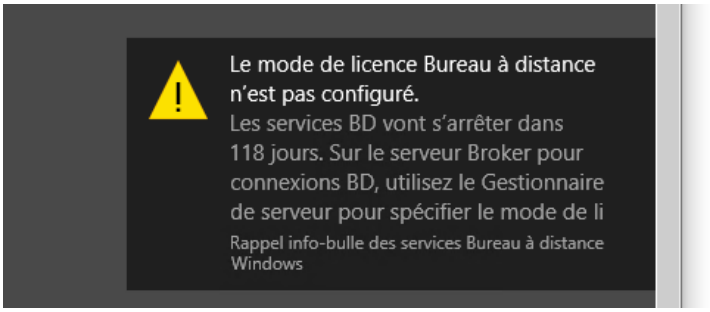


L'assistant va se lancer et vous proposer l'installation du Gestionnaire de licences RDS. Sélectionnez simplement votre serveur dans la liste et continuez en cliquant sur Suivant pour poursuivre l'installation.

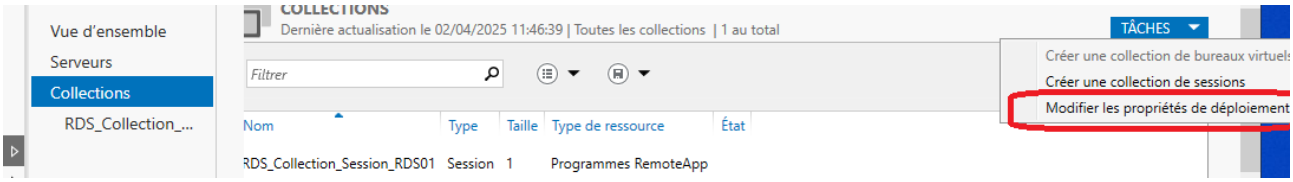


Lorsque nous ouvrons une session sur notre serveur RDS (même si notre licence est présente), il se peut que nous recevions le message suivant : "Le mode de licence Bureau à distance n'est pas configuré. Les services BD vont s'arrêter dans X jours...".

Cela signifie que notre serveur RDS ne sait pas s'il doit fonctionner en attribuant des licences (CAL RDS) par utilisateur ou par périphérique qui se connecte.

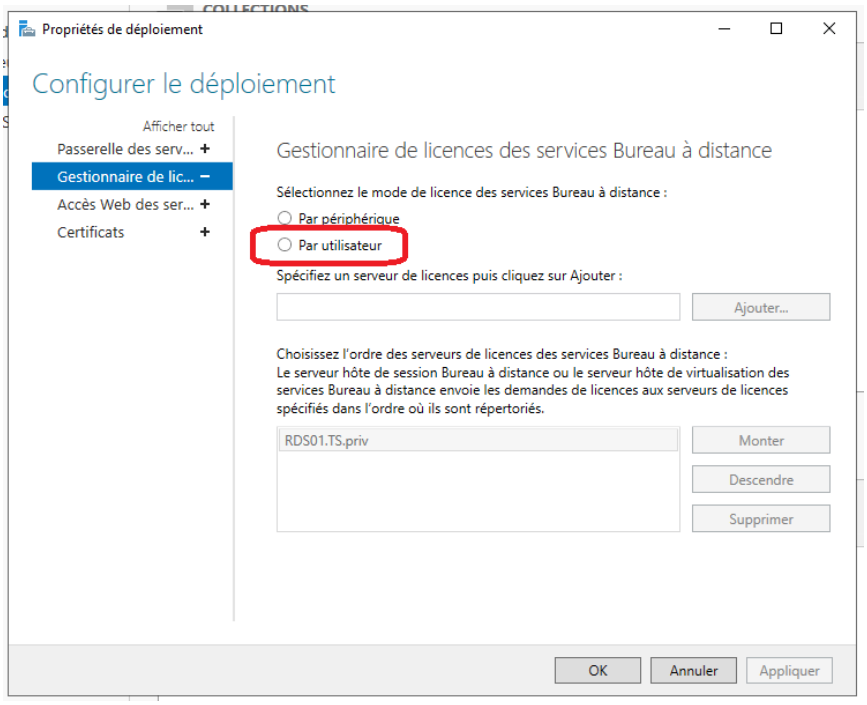


Pour rectifier la situation, accédons à la console de gestion RDS, puis, dans le menu de gauche, cliquons sur "Collections". Ensuite, dans la partie droite, cliquons sur "Tâches", puis sélectionnons "Modifier les propriétés de déploiement".

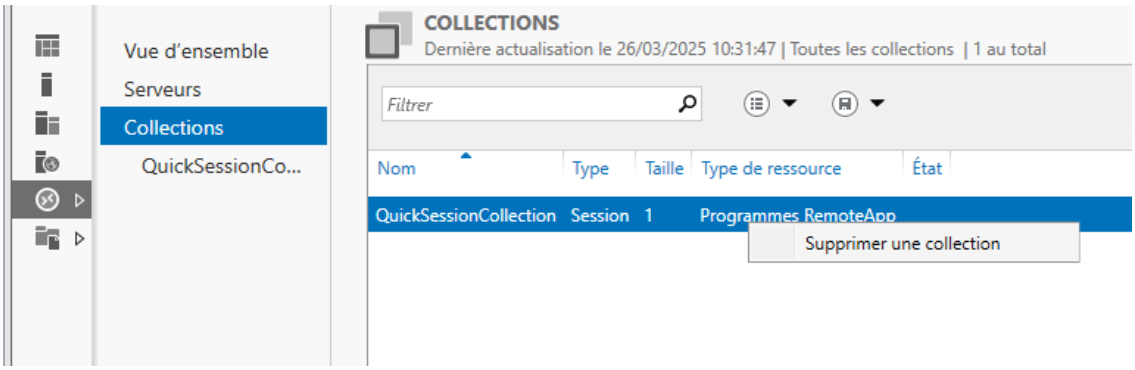


Sur la gauche, cliquons sur "Gestionnaire de licence" et sélectionnons le mode qui nous convient : par utilisateur

Si le serveur de licence n'apparaît pas dans la liste en bas de la fenêtre, nous devons l'ajouter. Cependant, comme le rôle est installé sur le serveur local, il devrait remonter par défaut.



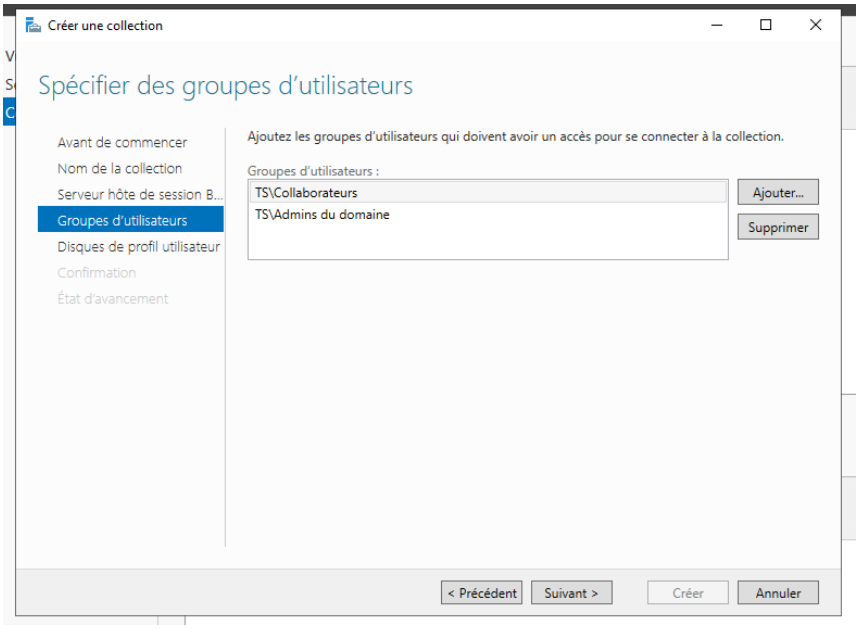
Nous allons maintenant créer et configurer la collection RDS. Tout d'abord, il est nécessaire de supprimer la collection par défaut. Pour ce faire, rendez-vous dans "Service Bureau à distance", puis dans "Collections". Faites un clic droit sur "QuickSessionCollection" et sélectionnez Supprimer. Cela permettra de libérer l'espace pour la création de la nouvelle collection personnalisée.



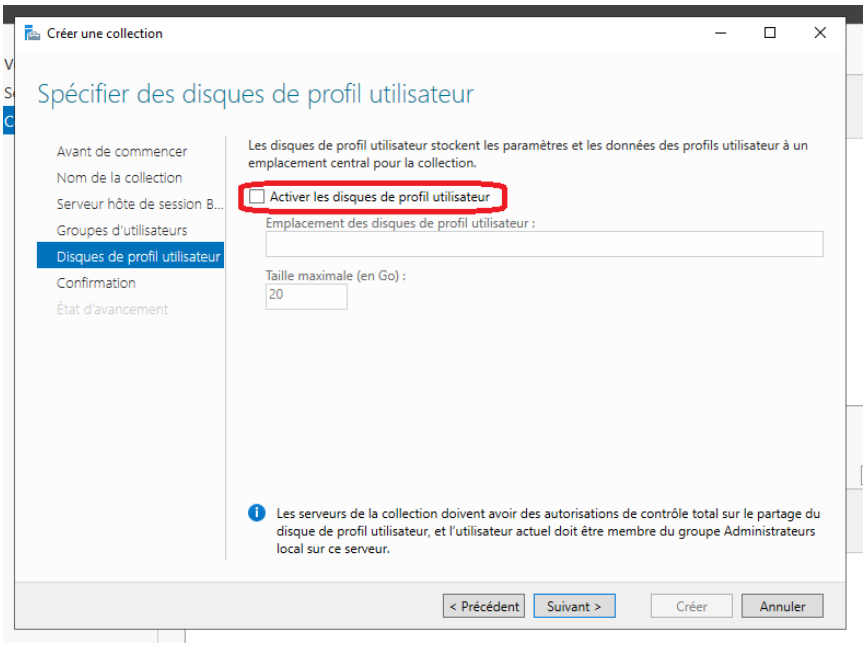
Nous allons maintenant créer une nouvelle collection de sessions RDS. Pour cela, nous nous rendons dans Service Bureau à distance, puis dans Collections, là où nous avons précédemment supprimé la collection par défaut. Ensuite, dans le menu à droite sous Tâches, nous cliquons sur Créer une collection de sessions. Nous suivons ensuite les étapes de l'assistant pour configurer la collection selon nos besoins.

Les deux premières fenêtres de l'assistant nous demandent de définir un nom pour la collection. Nous allons nommer cette collection Collection_Session_RDS01. Ensuite, dans la fenêtre suivante, on nous demande de sélectionner un serveur hôte, où nous choisirons RDS01.

Nous arrivons ensuite à la fenêtre où il faut spécifier les groupes d'utilisateurs autorisés à se connecter aux applications. Nous allons ajouter les groupes Collaborateurs et Admin du domaine, tout en supprimant le groupe Utilisateurs authentifiés.

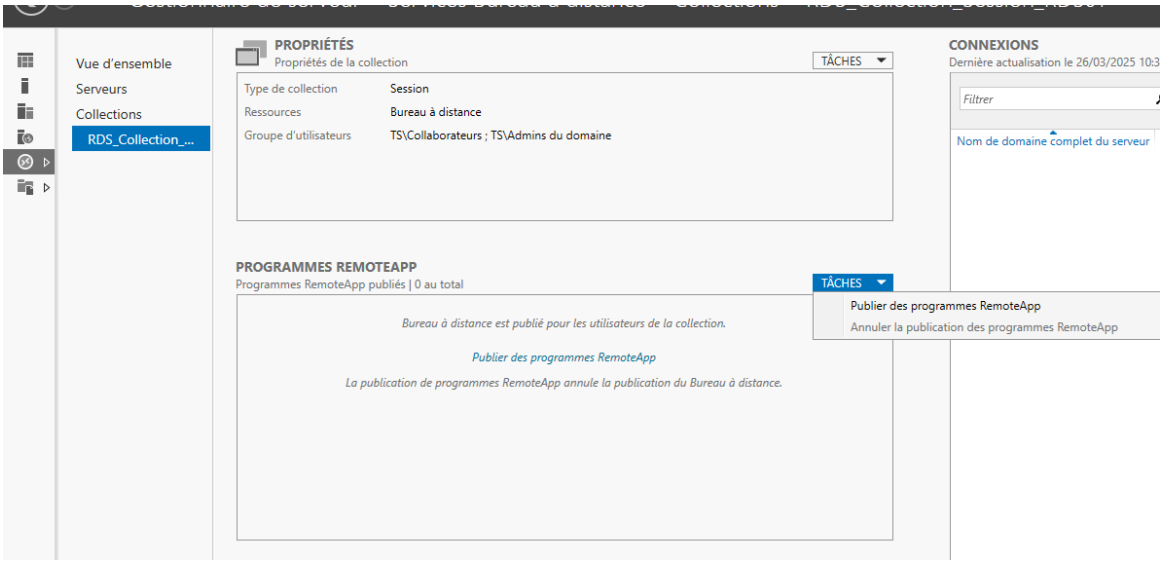


Dans l'onglet "Disques de profil utilisateur", nous décocherons l'option "Activer les disques de profil utilisateur". Une fois cette option désactivée, il ne nous restera plus qu'à confirmer la création de la collection. Nous pourrons ensuite passer à la configuration de celle-ci.

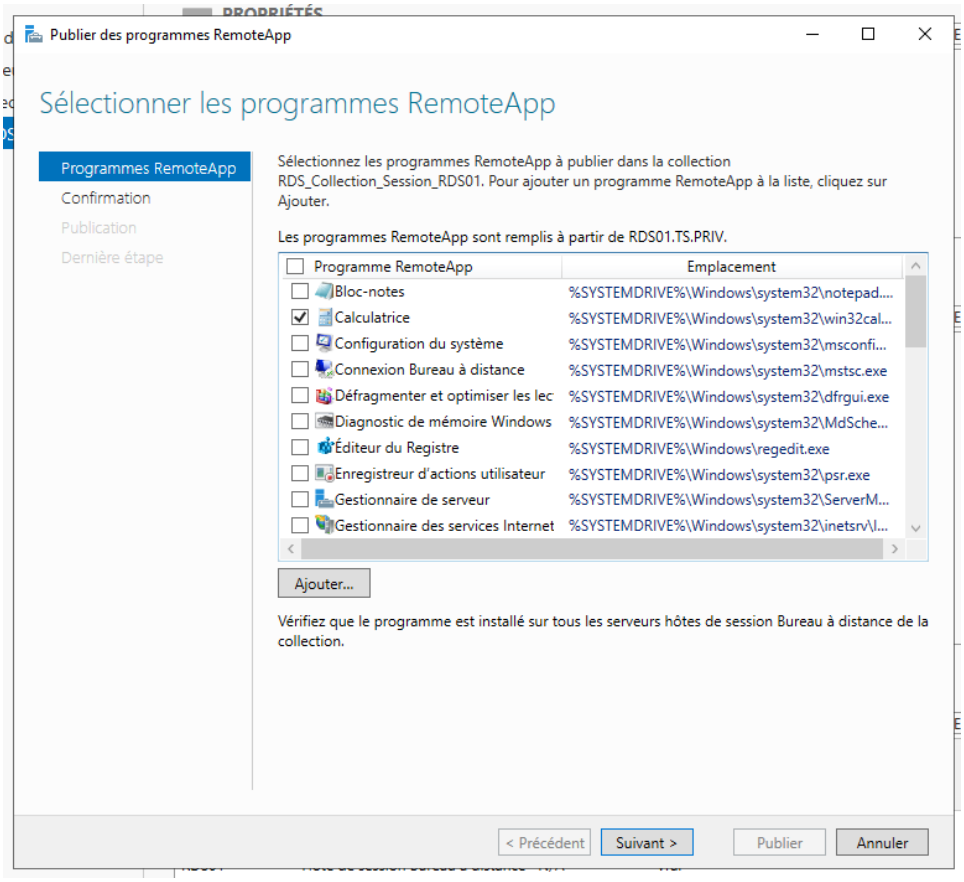


Nous allons maintenant choisir les applications à déployer. Pour cet exemple, nous allons publier Calculatrice, WordPad et Informations système. Dans un cas concret, il suffit d'ajouter les applications nécessaires selon les besoins.

Pour spécifier quelles applications seront déployées, nous accédons à la collection que nous venons de créer. Ensuite, dans l'onglet Tâches, nous sélectionnons "Publier des programmes RemoteApp".



L'assistant s'ouvre et nous demande de sélectionner les applications à publier. Nous choisissons alors Calculatrice, WordPad et Informations système, ainsi que toute autre application souhaitée. Un récapitulatif des applications sélectionnées s'affiche, il ne reste plus qu'à confirmer pour finaliser la publication.

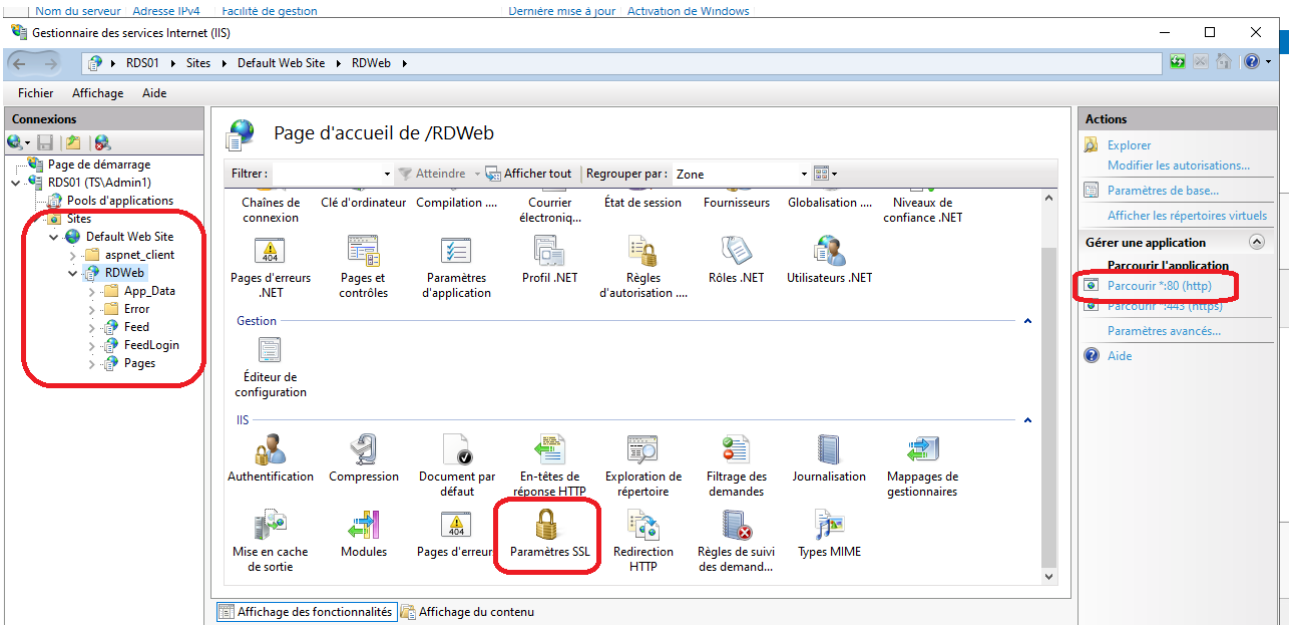


Configuration IIS

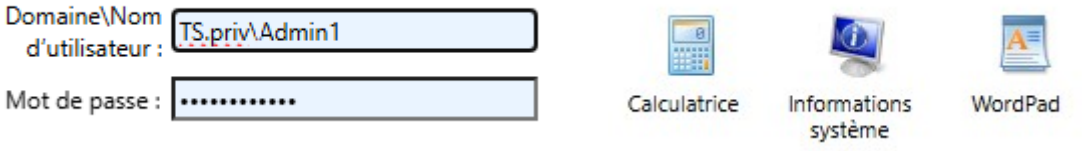
Nous allons maintenant tester l'accès aux applications via le portail web. Avant cela, nous devons désactiver l'exigence du certificat SSL, car sans un certificat valide, la page serait inaccessible. Cependant, comme l'accès via la page web ne sera pas essentiel pour la connexion aux applications, nous ne créerons pas de certificat.

Pour désactiver l'exigence SSL, nous ouvrons le Gestionnaire IIS, accédons à la page RDWeb, puis dans Paramètres SSL, nous décochons l'option "Exiger SSL".

Ensuite, nous accédons à la page web en effectuant un clic droit sur "Parcourir :80 (HTTP)" dans le Gestionnaire IIS. Cela ouvre le portail web RDS où nous pourrons tester l'accès aux applications publiées.

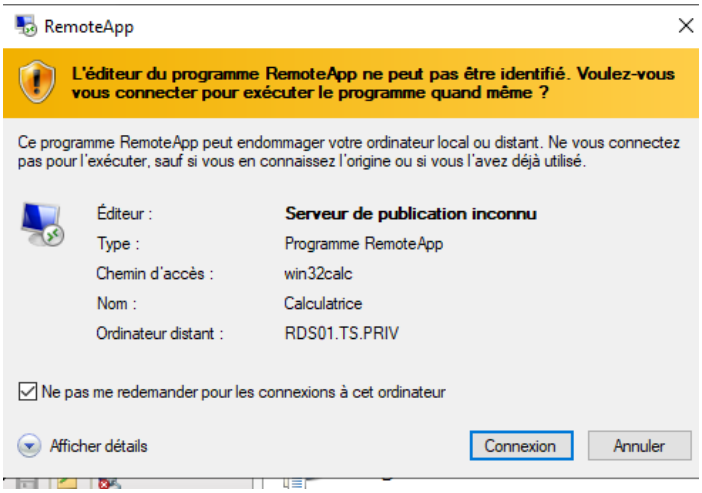


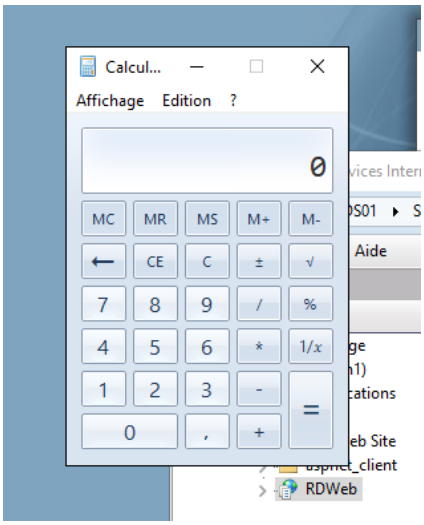
Une fois sur la page de connexion, nous entrons les identifiants d'un utilisateur autorisé, comme un membre du groupe "Collaborateurs" ou "Admin du domaine". Après validation, nous accédons à l'interface où sont affichées les applications publiées, telles que la Calculatrice, WordPad et Informations système. Nous pouvons alors tester leur lancement pour vérifier que la configuration est fonctionnelle.



Pour ce test, nous l'effectuons avec un poste situé dans le LAN serveur, ce qui rend la configuration de DynFi non nécessaire pour le moment. Toutefois, nous y reviendrons un peu plus tard pour compléter la mise en place.

Lorsque nous lançons la calculatrice, un message d’alerte apparaît pour demander la confirmation de connexion. Nous l’acceptons, ce qui permet l’exécution de l’application à distance. Si tout fonctionne correctement, cela confirme que notre configuration RDS est opérationnelle. Si nécessaire, nous pouvons tester d'autres applications pour s'assurer que tout est bien configuré.





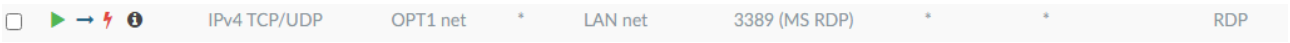
Configuration du Dynfi

Avant de passer à la configuration de la GPO, nous devons d'abord autoriser le port 3389, utilisé par le service Bureau à distance, à travers le pare-feu du DynFi. Cela permettra aux machines du LAN utilisateur d'accéder au LAN serveur via le service RDP (Remote Desktop Protocol).

Pour ce faire, nous commençons par accéder à la configuration du DynFi. Nous ouvrons un navigateur et saisissons l'adresse IP du DynFi, 192.168.100.253. Une fois connectés à l'interface de gestion, nous naviguons vers l'onglet Firewall, puis vers Rules. Dans cette section, nous sélectionnons la règle associée au réseau OPT1, qui correspond à notre réseau LAN utilisateur.

Ensuite, nous ajoutons une nouvelle règle en cliquant sur Add. Nous configurons cette règle pour autoriser le protocole TCP/UDP sur le port 3389 afin de permettre la communication vers le LAN Serveur. Une fois la règle correctement définie, nous enregistrons les modifications en cliquant sur Save.

Cela permettra d'assurer que les connexions RDP entre le LAN utilisateur et le LAN serveur soient autorisées, en passant par le port 3389.



Passons maintenant à la configuration de la GPO pour déployer l’accès aux applications publiées via RemoteApp.

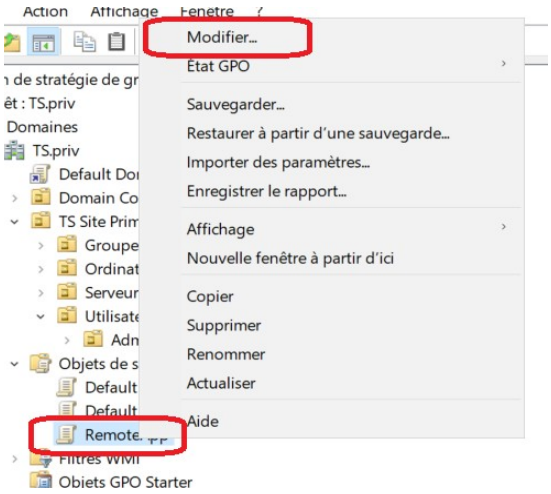
Configuration de la GPO

Tout d'abord, nous devons récupérer le fichier .rdp permettant de lancer l'application. Lors de notre précédent test de lancement via la page web, un fichier de connexion .rdp a été téléchargé. Nous allons le récupérer et le stocker dans un emplacement accessible à tous les postes du réseau. Un emplacement idéal est le SYSVOL du contrôleur de domaine AD01, situé dans :

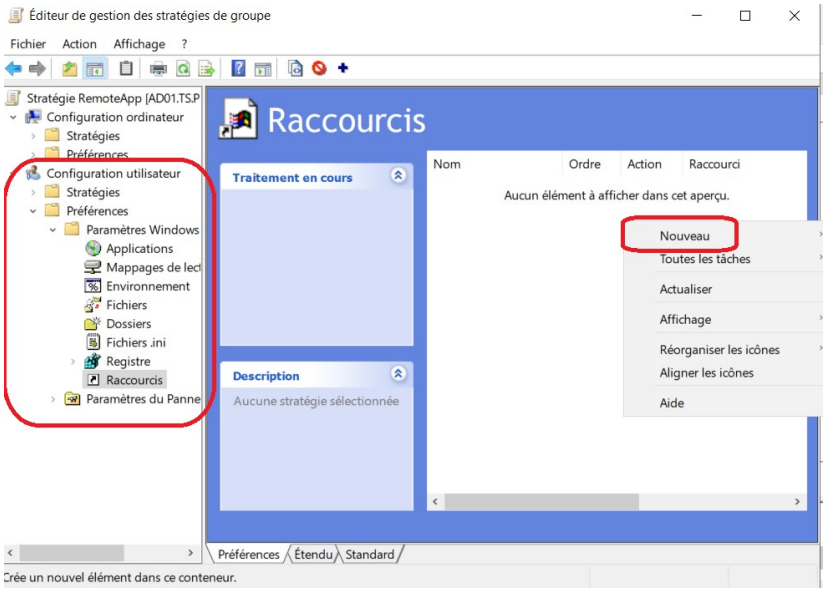
\\AD01\sysvol\TS.priv\Policies

Dans ce répertoire, nous créons un dossier APP et y déposons le fichier .rdp correspondant à l'application, ici la calculatrice.

Nous allons maintenant créer une stratégie de groupe (GPO) pour distribuer ce raccourci sur les postes des utilisateurs. Pour cela, nous ouvrons le Gestionnaire de serveur, puis nous accédons à Outils > Gestion des stratégies de groupe. Dans la section Objets de stratégie de groupe, nous créons une nouvelle GPO nommée RemoteAPP, puis nous faisons un clic droit dessus pour la modifier.

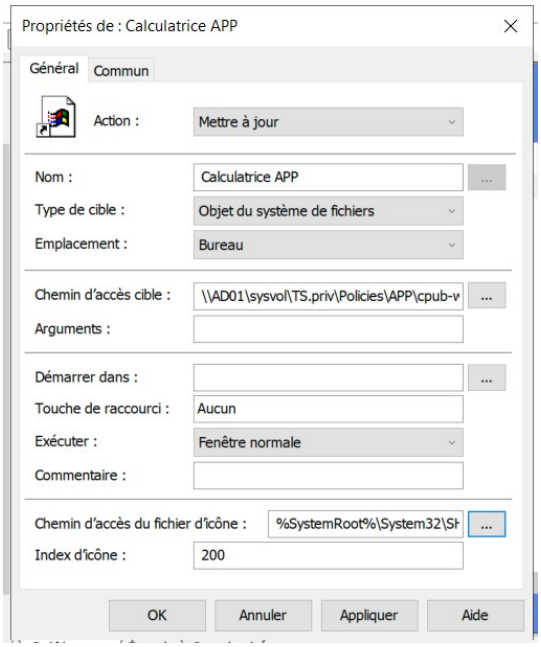


Dans l'éditeur de stratégie de groupe, nous naviguons vers Configuration utilisateur > Préférences > Paramètres Windows > Raccourcis. Nous faisons un clic droit dans l’espace vide et sélectionnons Nouveau > Raccourci.



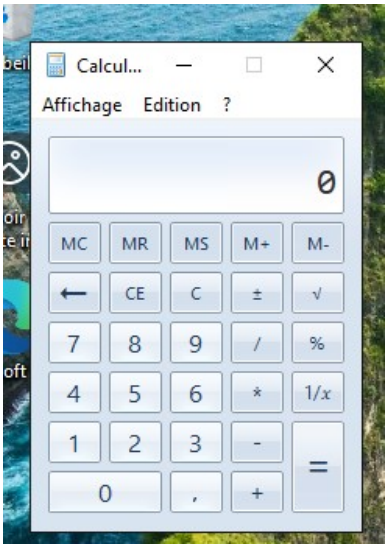
Une fenêtre s'ouvre où nous renseignons les paramètres suivants :

- Nom : Nom de l’application (exemple : Calculatrice APP).
- Emplacement : Sélectionner Bureau pour que l'icône apparaisse sur le bureau des utilisateurs.
- Chemin d’accès cible : Indiquer le chemin du fichier .rdp stocké dans le SYSVOL.
- Icône : Modifier si nécessaire pour correspondre à l’application.



Ensuite, nous devons affecter et filtrer la GPO. Pour cela, nous la rattachons à l'OU contenant les utilisateurs. Dans l'onglet Filtrage de sécurité, nous retirons "Utilisateurs authentifiés" et ajoutons uniquement le groupe Collaborateurs, ce qui garantit que seuls les utilisateurs de ce groupe auront le raccourci.

Enfin, nous testons l'application de la GPO en exécutant gpupdate /force sur un poste client qui se trouve dans le domaine. Vérifions maintenant que le raccourci apparaît bien sur le bureau des utilisateurs et qu'il permet de lancer l'application correctement via RemoteApp. Ainsi, nous avons automatisé et sécurisé la mise à disposition des applications à distance pour les collaborateurs.



Conclusion

L'implémentation d'un serveur RDS avec RemoteApp et GPO permet un déploiement centralisé et sécurisé des applications métier. L'intégration avec Active Directory et le pare-feu DynFi assure un contrôle précis des accès et garantit une continuité de service optimale.

Ce projet reproduit une infrastructure que j'ai eu l'occasion de mettre en œuvre en entreprise dans le cadre de ma formation. Il s'inscrit dans la continuité du Projet 1, démontrant comment ajouter une couche supplémentaire de services distants sur une base réseau sécurisée et redondante. Cette approche contribue à rationaliser la gestion informatique, tout en réduisant les coûts de maintenance et en améliorant la flexibilité des utilisateurs dans leur environnement de travail.