BTS Services informatiques aux organisations- SISR

Session 2025

E6 – Support et mise à disposition de services informatiques

Coefficient 4

DESCRIPTION DE LA REALISATION PROFESSIONNELLE

NOM et prénom du candidat :

Nathan VANDENBOSSCHE

Contexte de la réalisation professionnelle

- **Layer Bureautique et Informatique** est une entreprise spécialisée dans la gestion d'infrastructures IT et la virtualisation, offrant des services essentiels pour répondre aux besoins de performance, sécurité et continuité des systèmes informatiques du client vdb-pro.
- La problématique principale réside dans le besoin pour les utilisateurs d'accéder à un environnement de travail distant, centralisé et sécurisé pour avoir accès au logiciel ERP Dolibarr, tout en assurant une gestion efficace des droits et des flux réseau.
- La solution choisie consiste à déployer d'un serveur RDS sous Windows Server 2022 intégré à l'Active Directory, avec gestion des accès via GPO et séparation des réseaux via VLAN.

Intitulé de la réalisation professionnelle

Déploiement d'une Solution de Bureau à Distance

Période de réalisation : 10/02/25- 12/02/25 **Lieu :** Auxerre

Modalité : ☒ Individuelle ☐ En équipe

Principale(s) activité(s) concernée(s) :

- METTRE A DISPOSITION DES UTILISATEURS UN SERVICE INFORMATIQUE
- ORGANISER SON DEVELOPPEMENT PROFESIONNEL
- GERER LE PATRIMOINE INFORMATIQUE

Conditions de réalisation

- **Ressources disponibles (Situation avant RP)**
  L'infrastructure de départ comprend un serveur ESXi opérationnel pour l'hébergement de machines virtuelles, ainsi qu'un contrôleur de domaine Active Directory déjà en place, incluant un service DNS fonctionnel. D'autres services réseau de base (DHCP, VLANs, pare-feu) sont également configurés pour permettre le bon déroulement de la réalisation.
- **Résultats attendus (Situation après RP)**
  Les utilisateurs doivent pouvoir se connecter à distance à un environnement de travail virtualisé via RDS, avec des droits restreints et sécurisés pour accéder à l'**ERP Dolibarr**. L'intégration est complète au domaine Active Directory. L'administration doit être centralisée, et les flux réseau correctement segmentés par VLAN.
- **Durée de réalisation**
  Cela à pris 3 jours, incluant installation, configuration, sécurisation et phase de test.

Modalités d'accès à cette réalisation professionnelle.

https://portfolio.vdb-pro.fr mdp : *Cyb3r-M@P89$*

Partie 1 – Procédure de mise en œuvre

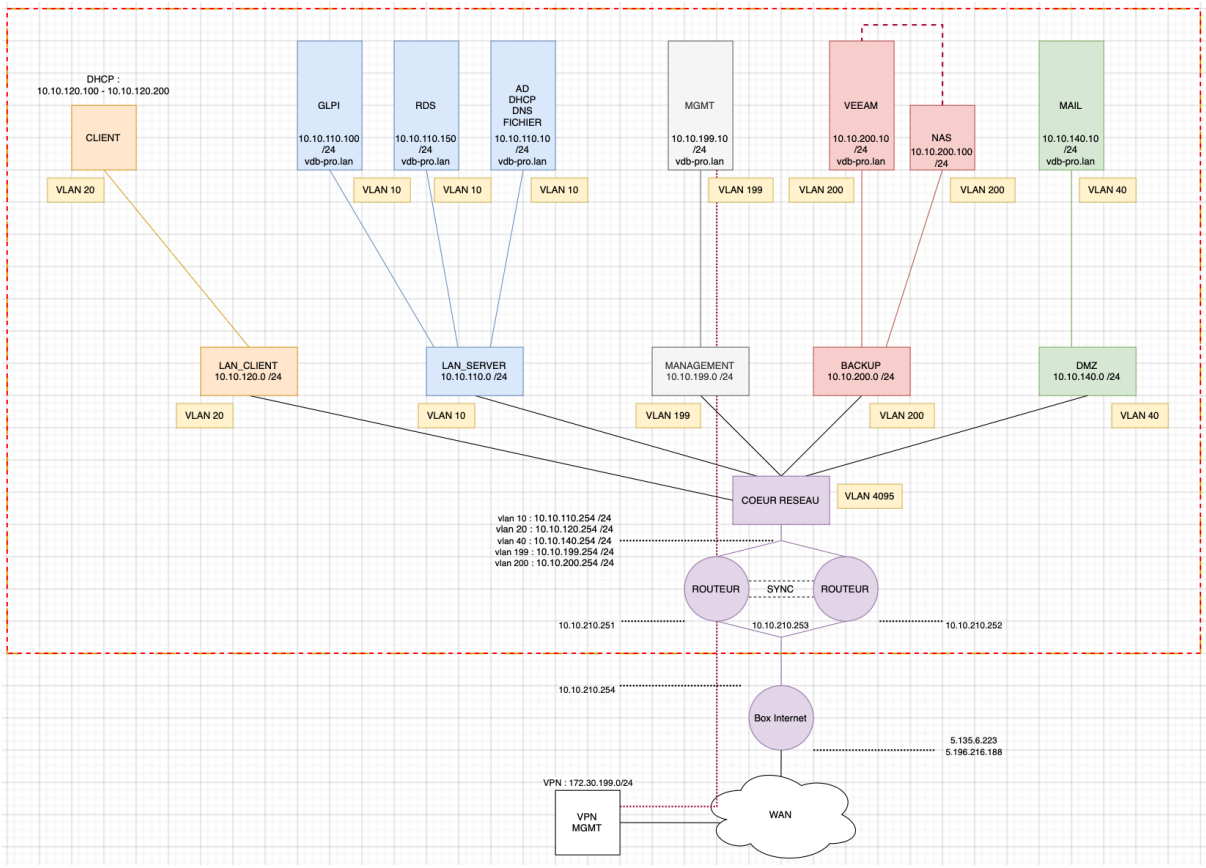
Dans le cadre de l'infrastructure informatique que j'ai mise en place pour l'entreprise, **vdb-pro,** j'ai conçu et déployé un réseau interne visant un environnement professionnel sécurisé et fonctionnel. Une composante essentielle de cette architecture repose sur la mise en place d'un service de bureau à distance, basé sur Microsoft Windows Server 2022 et utilisant le rôle Remote Desktop Services (RDS).

Cette solution permet aux utilisateurs d'accéder à un environnement de travail distant (session Windows virtuelle) depuis n'importe quel poste client autorisé, tout en assurant une sécurité, une centralisation et une gestion simplifiée.

La gestion des comptes utilisateurs et des droits d'accès à ce service sera assurée par l'Active Directory, préalablement mis en place dans le cadre d'une autre Réalisation Professionnelle. Cela garantit une centralisation de l'authentification et une meilleure gestion des ressources au sein de l'organisation.

Objectifs de la réalisation

L'objectif principal de cette réalisation au sein de mon entreprise *vdb-pro* était de déployer un **serveur Windows Server 2022** configuré avec le rôle **Remote Desktop Services (RDS)**, afin de fournir un environnement de travail distant, stable et sécurisé aux utilisateurs pour qu'ils accèdent au logiciel ERP Dolibarr. Ce serveur devait permettre aux collaborateurs d'accéder à une session de bureau virtuelle, sans avoir un accès physique direct aux machines hôtes. Pour garantir une **authentification centralisée** et une gestion efficace des droits d'accès, le serveur RDS a été intégré à une **infrastructure Active Directory** préexistante. Par ailleurs, une **segmentation réseau par VLAN** a été mise en place afin de séparer les flux entre les postes utilisateurs et les serveurs, renforçant ainsi la sécurité de l'architecture. L'ensemble de la solution repose sur une **gestion centralisée des comptes utilisateurs et des autorisations**, assurant une administration simplifiée et conforme aux bonnes pratiques en entreprise.

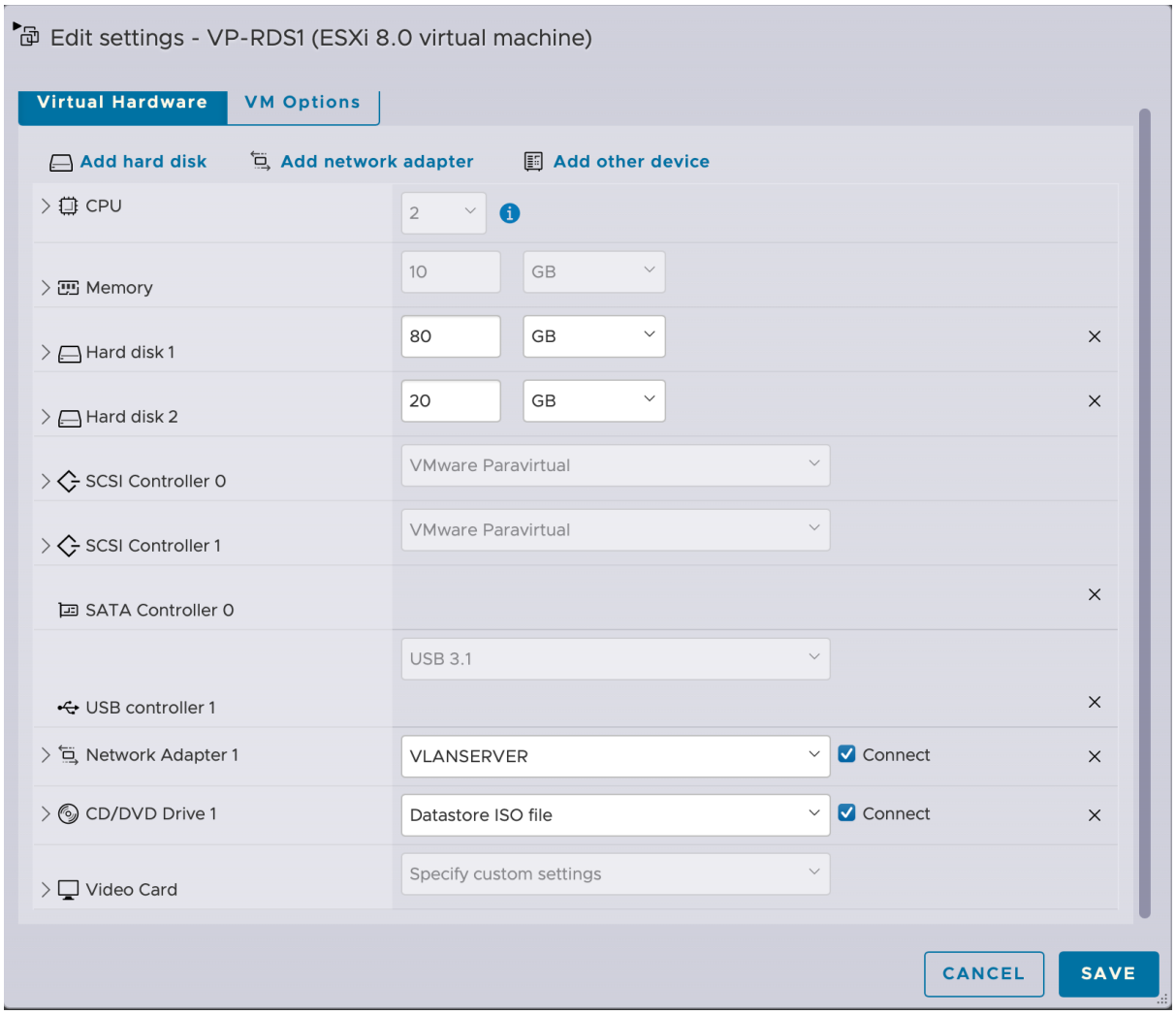


Infrastructure et environnement technique

L'infrastructure déployée au sein de *vdb-pro* repose sur un environnement **virtualisé sous VMware ESXi**, dans lequel a été installé un **serveur Windows Server 2022** dédié au rôle **Remote Desktop Services (RDS)**, avec un **déploiement de type Session-Based**. Ce serveur a été intégré à un **contrôleur de domaine Active Directory**, également sous Windows Server 2022, déjà mis en place dans le cadre d'une autre réalisation. Les **clients RDS** sont constitués de postes de travail sous **Windows 10 et 11**, tous intégrés au domaine, permettant une gestion centralisée des connexions. Sur le plan réseau, l'architecture est segmentée en deux VLANs distincts : le **VLAN 10 (LAN_SERVER)**, réservé aux serveurs, notamment le RDS, et le **VLAN 20 (LAN_CLIENTS)**, dédié aux utilisateurs finaux. Cette séparation permet un **meilleur contrôle des flux réseau et une sécurisation accrue** de l'environnement. Divers **outils d'administration** ont été utilisés pour cette réalisation, tels que les **stratégies de groupe (GPO)** pour restreindre l'environnement utilisateur sur les sessions distantes, le **gestionnaire de serveur RDS** pour le déploiement et la gestion des services, ainsi que le **pare-feu Windows**, configuré pour assurer un **filtrage strict entre les VLANs**.

Mise en place d'une machine virtuelle

J'ai procédé à la création d'une **machine virtuelle dédiée au rôle RDS** sur mon **hyperviseur VMware ESXi**. Cette machine a été configurée avec un **disque principal de 80 Go** destiné au système d'exploitation, ainsi qu'un **second disque de 20 Go** utilisé comme espace de **swap**, afin d'optimiser les performances de la machine en cas de surcharge mémoire. Pour assurer un **contrôle précis des disques virtuels** et améliorer les performances d'E/S, j'ai configuré deux **contrôleurs SCSI** en mode **VMware Paravirtual (PVSCSI)**, une option recommandée pour les environnements fortement sollicités en lecture/écriture. Côté réseau, la machine a été rattachée au **réseau LAN_SERVER (VLAN 10)** afin de garantir un cloisonnement logique avec les autres segments du réseau. Enfin, j'ai effectué une **réservation de 10 Go de mémoire vive (RAM)** exclusivement pour ce serveur, afin d'éviter toute contention de ressources avec d'autres machines virtuelles hébergées sur l'ESXi, et d'assurer une **stabilité optimale** pour les sessions distantes hébergées.



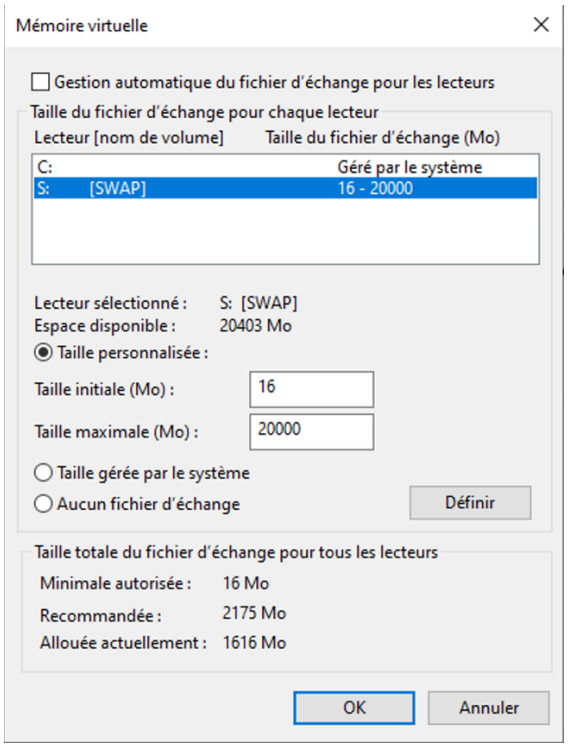
Installation de Windows Server 2022 et Intégration au Domain

J'ai commencé par procéder à l'installation du système d'exploitation Windows Server 2022. Avant son intégration au domaine, j'ai effectué une configuration initiale comprenant la définition du nom d'hôte en tant que VP-RDS1. Ce nom a été choisi dans une logique d'évolutivité, afin de prévoir la possibilité d'ajouter ultérieurement d'autres serveurs RDS (ex. VP-RDS2, VP-RDS3, etc.) pour constituer une ferme RDS complète en fonction des besoins futurs de mon entreprise vdb-pro.

La configuration réseau statique du serveur a été réalisée manuellement avec l'attribution d'une adresse IP fixe, la passerelle (Gateway) par défaut et les serveurs DNS, en cohérence avec le plan d'adressage défini pour le VLAN 10 (LAN_SERVER). Une fois cette configuration terminée, le serveur a été rejoint au domaine Active Directory "VDB-PRO", préalablement mis en place. J'ai ensuite vérifié la bonne remontée des enregistrements DNS dans le gestionnaire DNS du contrôleur de domaine, afin de m'assurer que le serveur VP-RDS1 pouvait être résolu correctement par les clients du réseau. Cette étape est essentielle pour garantir une intégration cohérente dans l'infrastructure existante.

Configuration du PageFile.sys sur un autre disque

Afin d'optimiser la gestion de la mémoire virtuelle du serveur, j'ai déplacé le fichier **pagefile.sys** (fichier d'échange) vers un **disque différent de celui contenant le système d'exploitation**. Cette configuration permet de **réduire la charge sur le disque principal**, d'**améliorer les performances en cas de surallocation de la mémoire RAM**, et de mieux répartir les ressources du système. Pour ce faire, je suis passé par les **paramètres système avancés** de Windows, dans l'onglet **"Performances" > "Paramètres" > "Avancé"**, puis j'ai défini manuellement l'emplacement et la taille du fichier d'échange sur le second disque.

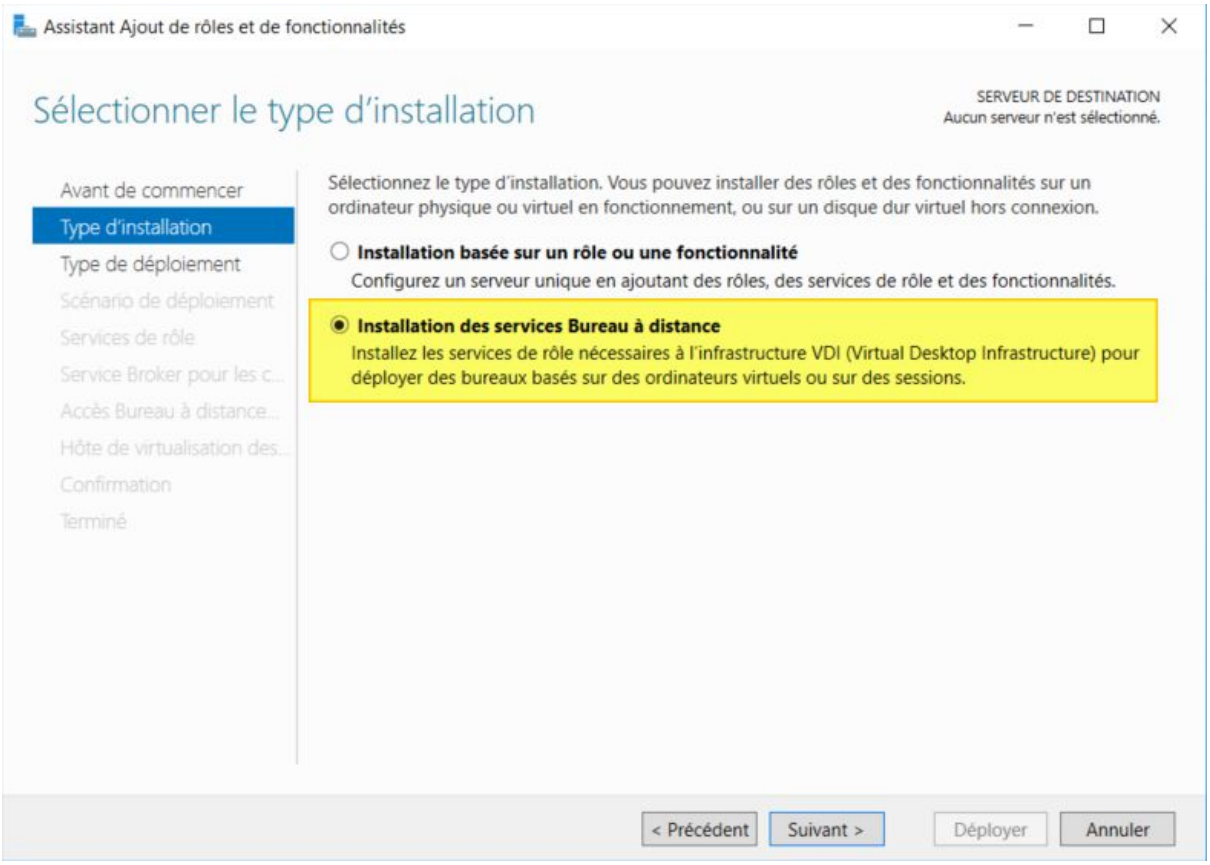


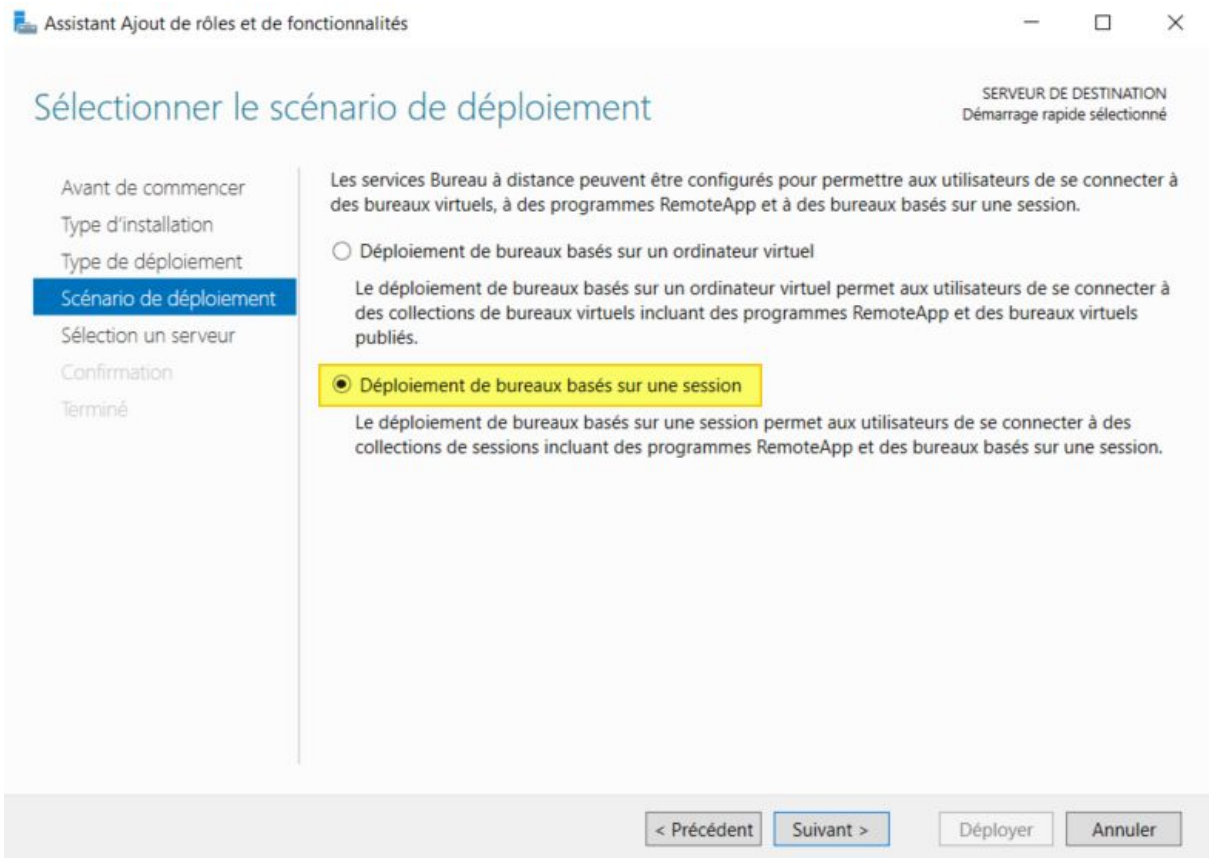
Installation des services Remote Desktop Services

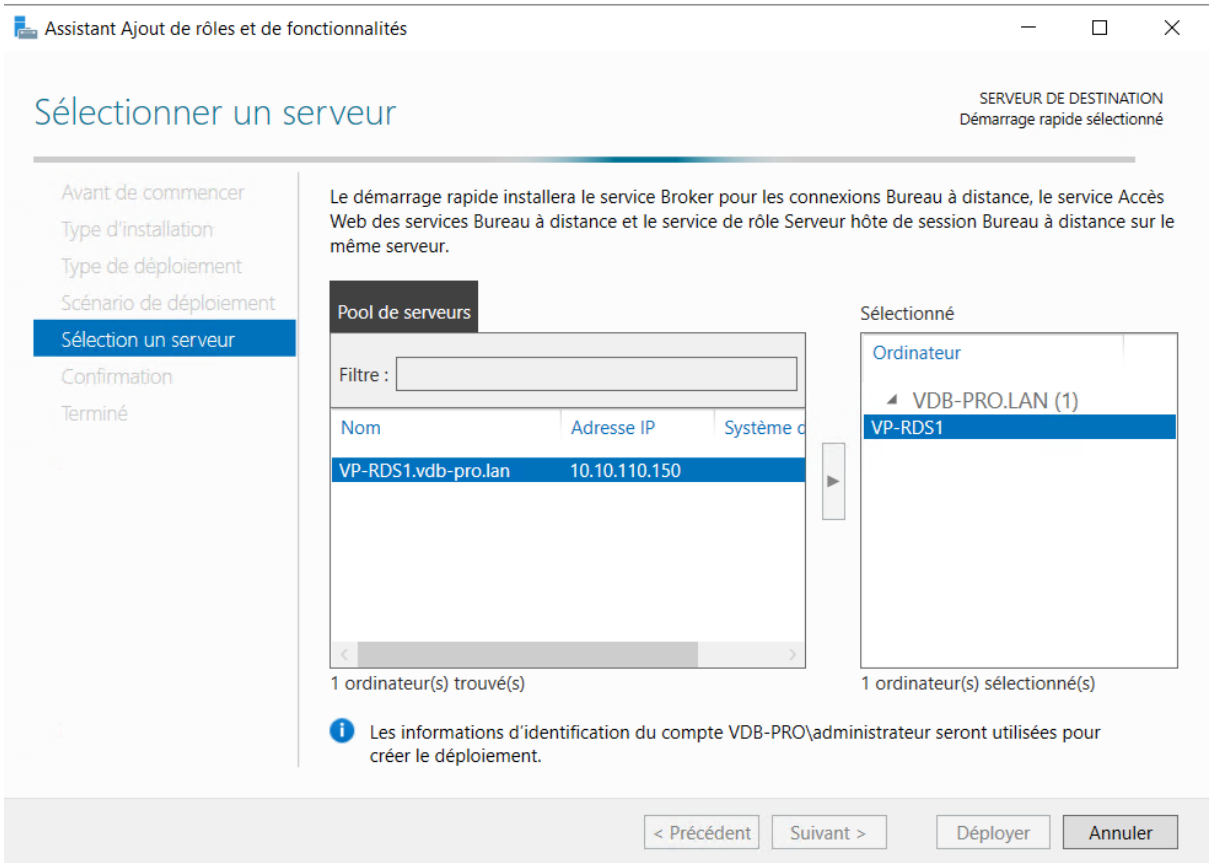
Par la suite, j'ai procédé à l'installation des services essentiels au bon fonctionnement de Remote Desktop Services (RDS) sur le serveur VP-RDS1. Pour cela, j'ai utilisé le Gestionnaire de serveur afin d'ajouter les rôles nécessaires à la mise en place d'un environnement RDS basé sur les sessions. Les services installés incluent notamment :

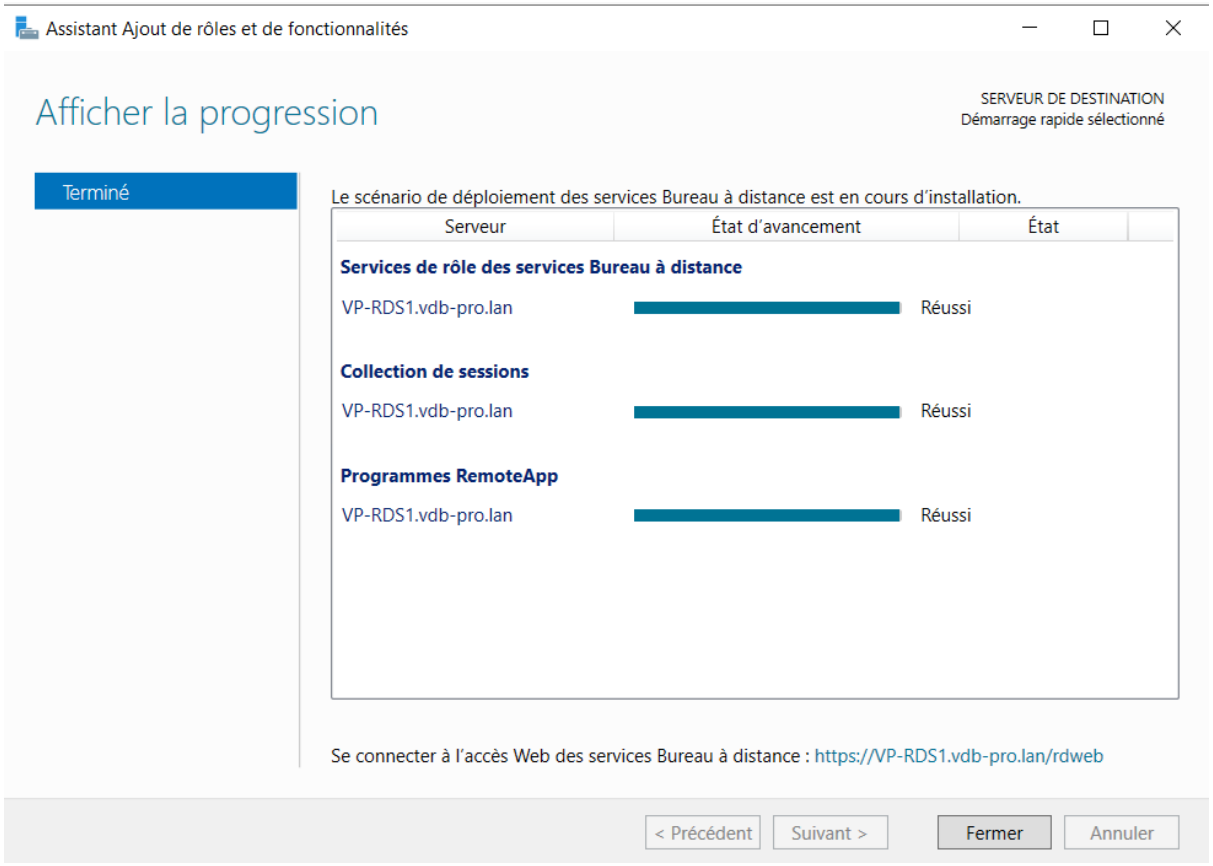
- Remote Desktop Session Host (RDSH) : service principal permettant d'héberger les sessions de bureau à distance auxquelles les utilisateurs se connectent. (Page 6-7)
- Remote Desktop Web Access (facultatif selon le besoin) : permet l'accès aux ressources via un navigateur Web sécurisé. (Page 6-7)
- Remote Desktop Licensing (prévu pour une mise en conformité future) : gestion des licences d'accès client (CAL) RDS. (Page 8-9)

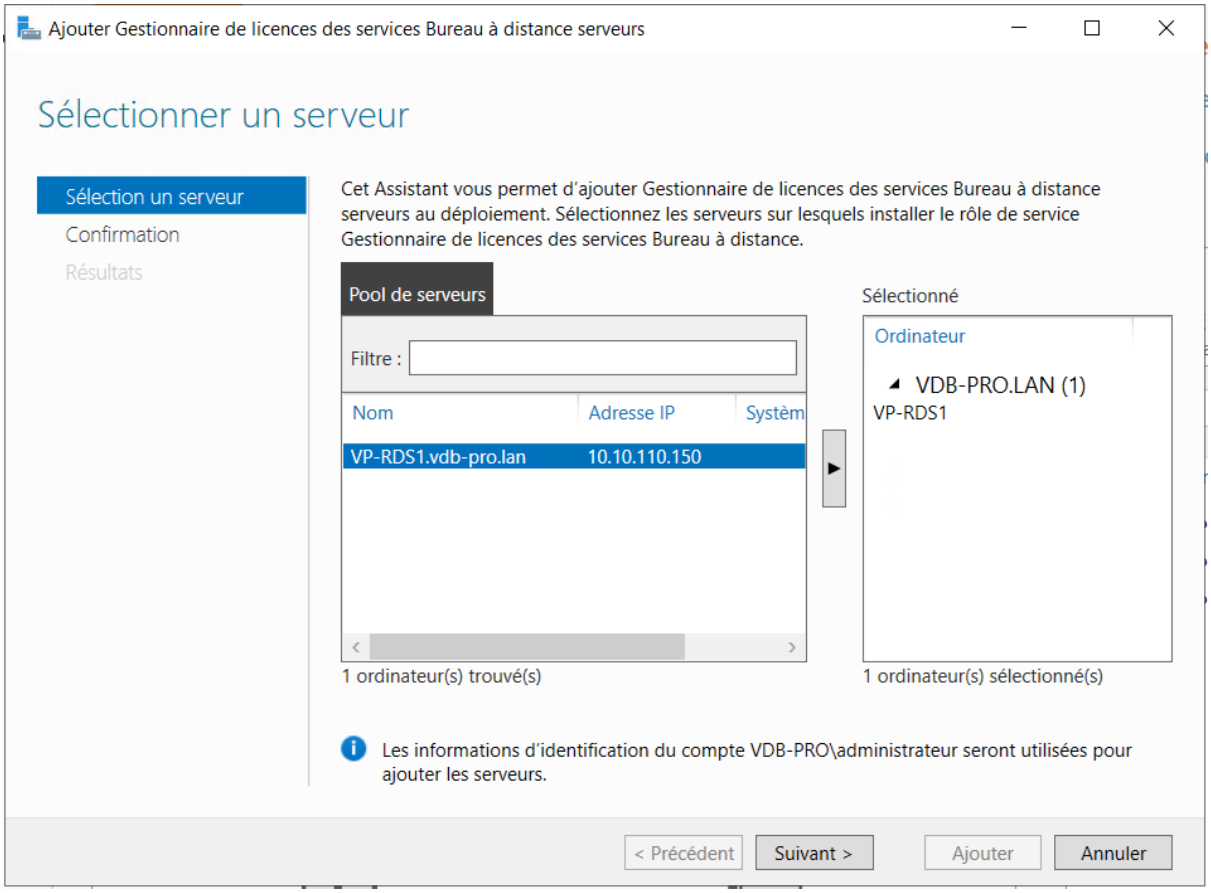
Chaque rôle a été installé de manière à respecter les bonnes pratiques de sécurité et à permettre une évolution progressive de l'infrastructure RDS. L'installation a été suivie d'un redémarrage du serveur et d'une vérification de l'état des services RDS via la console d'administration, afin de garantir que tous les composants soient opérationnels.

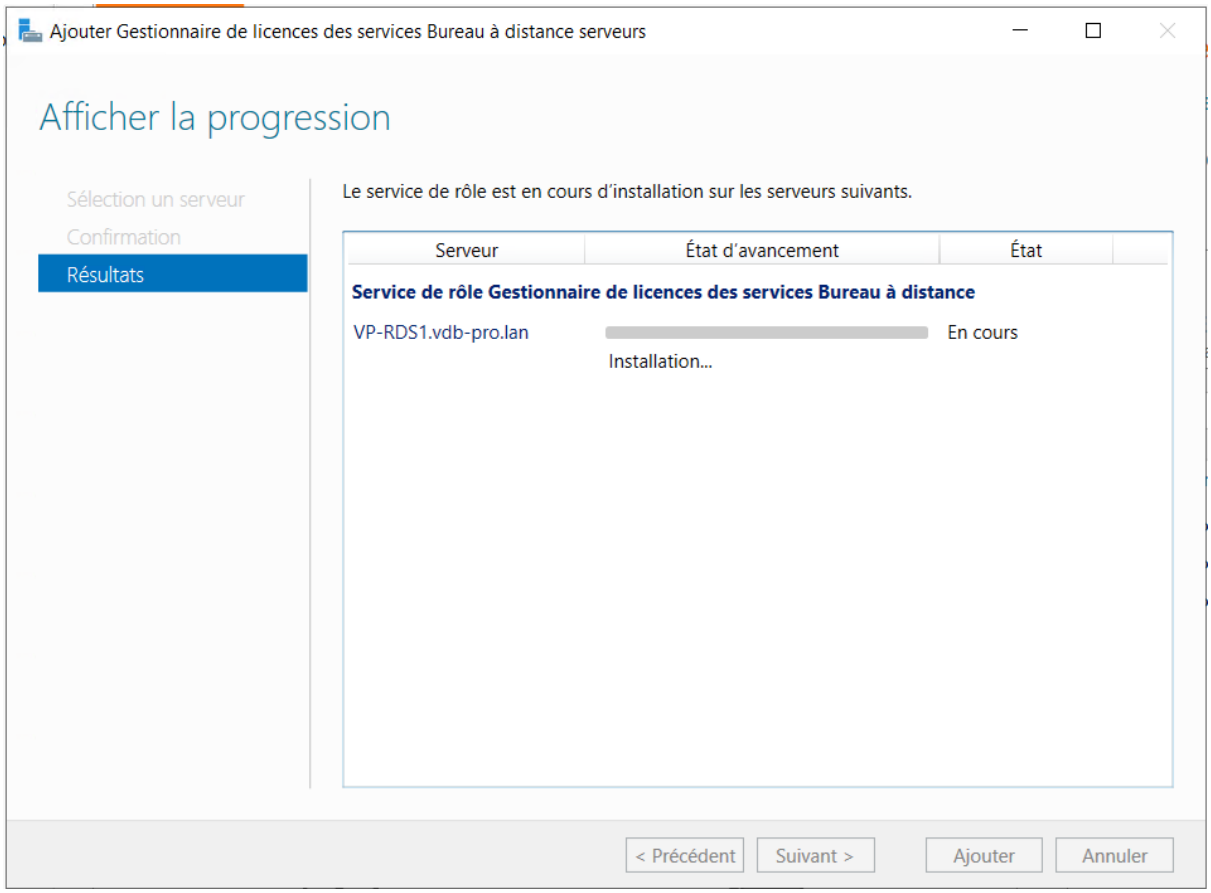


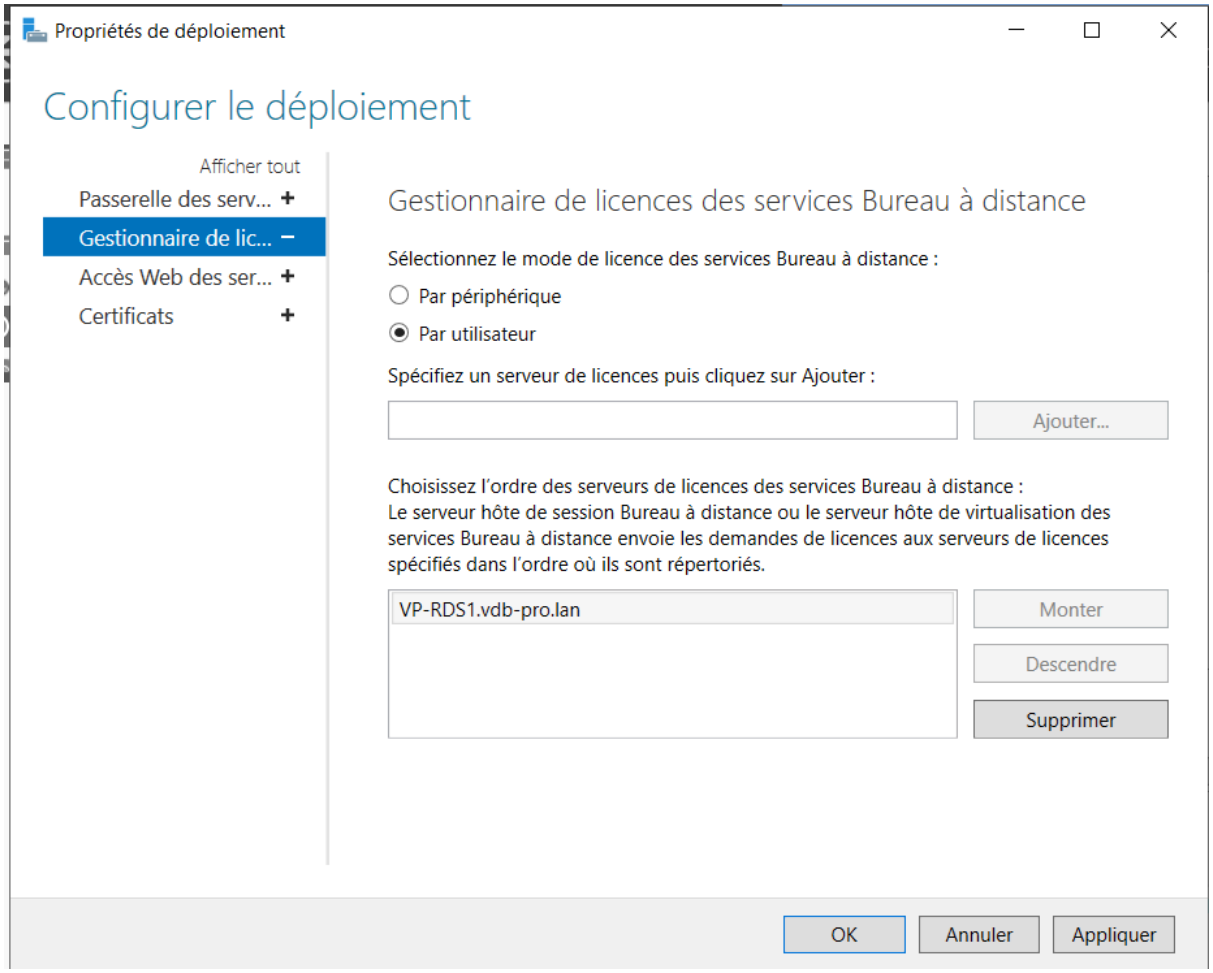

Assistant Ajout de rôles et de fonctionnalités
Sélectionner le scénario de déploiement
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Sélection un serveur
Confirmation
Terminé
Les services Bureau à distance peuvent être configurés pour permettre aux utilisateurs de se connecter à des bureaux virtuels, à des programmes RemoteApp et à des bureaux basés sur une session.
Déploiement de bureaux basés sur un ordinateur virtuel
Le déploiement de bureaux basés sur un ordinateur virtuel permet aux utilisateurs de se connecter à des collections de bureaux virtuels incluant des programmes RemoteApp et des bureaux virtuels publiés.
Déploiement de bureaux basés sur une session
Le déploiement de bureaux basés sur une session permet aux utilisateurs de se connecter à des collections de sessions incluant des programmes RemoteApp et des bureaux basés sur une session.
< Précédent
Suivant >
Déployer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Sélectionner un serveur
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Avant de commencer
Type d'installation
Type de déploiement
Scénario de déploiement
Sélection un serveur
Confirmation
Terminé
Le démarrage rapide installera le service Broker pour les connexions Bureau à distance, le service Accès Web des services Bureau à distance et le service de rôle Serveur hôte de session Bureau à distance sur le même serveur.
Pool de serveurs
Filtre :
Nom
Adresse IP
Système d
VP-RDS1.vdb-pro.lan
10.10.110.150
1 ordinateur(s) trouvé(s)
Sélectionné
Ordinateur
VDB-PRO.LAN (1)
VP-RDS1
1 ordinateur(s) sélectionné(s)
Les informations d'identification du compte VDB-PRO\administrateur seront utilisées pour créer le déploiement.
< Précédent
Suivant >
Déployer
Annuler


Assistant Ajout de rôles et de fonctionnalités
Afficher la progression
SERVEUR DE DESTINATION
Démarrage rapide sélectionné
Terminé
Le scénario de déploiement des services Bureau à distance est en cours d'installation.
Serveur
État d'avancement
État
Services de rôle des services Bureau à distance
VP-RDS1.vdb-pro.lan
Réussi
Collection de sessions
VP-RDS1.vdb-pro.lan
Réussi
Programmes RemoteApp
VP-RDS1.vdb-pro.lan
Réussi
Se connecter à l'accès Web des services Bureau à distance : https://VP-RDS1.vdb-pro.lan/rdweb
< Précédent
Suivant >
Fermer
Annuler

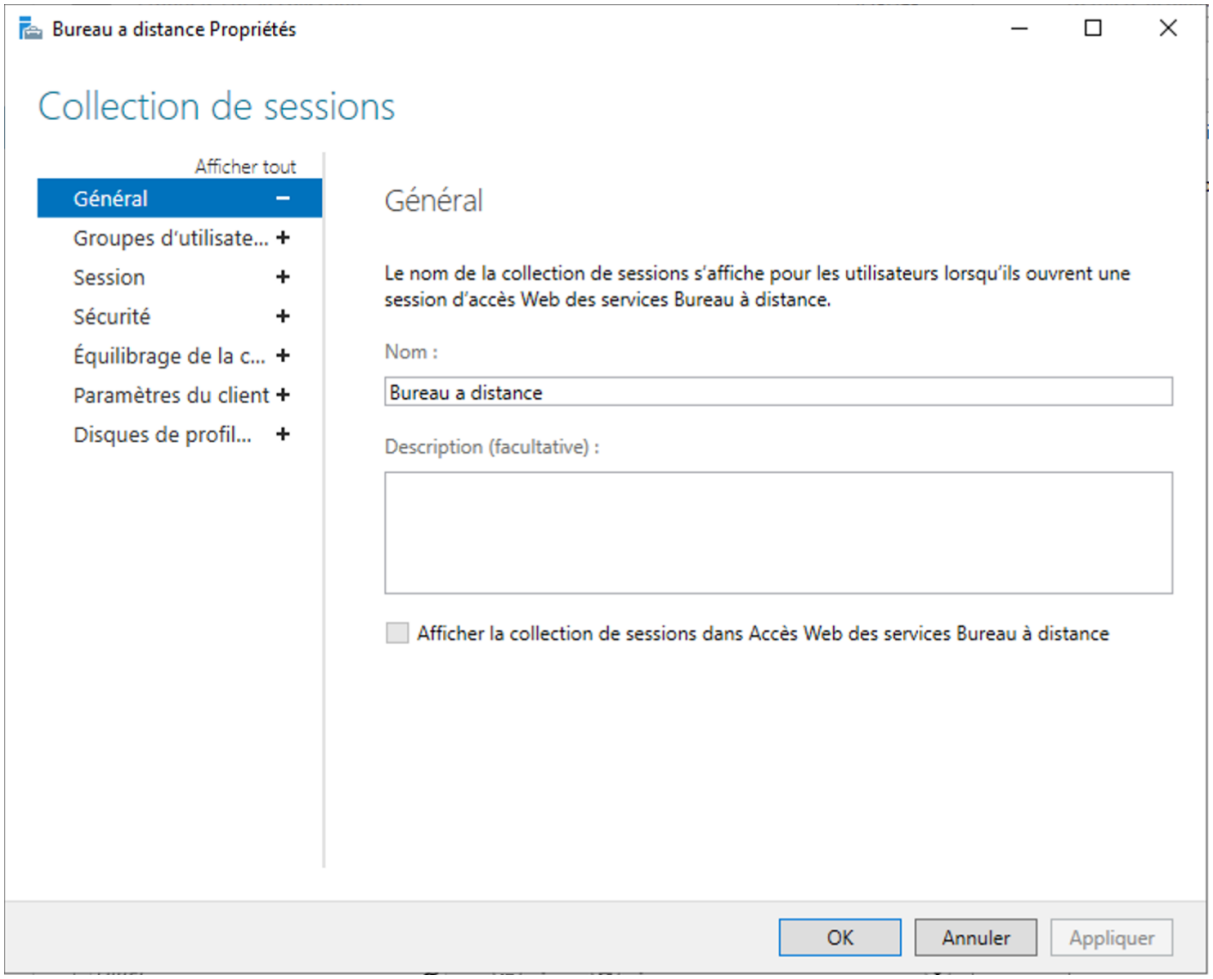

Ajouter Gestionnaire de licences des services Bureau à distance serveurs
Sélectionner un serveur
Sélection un serveur
Confirmation
Résultats
Cet Assistant vous permet d'ajouter Gestionnaire de licences des services Bureau à distance serveurs au déploiement. Sélectionnez les serveurs sur lesquels installer le rôle de service Gestionnaire de licences des services Bureau à distance.
Pool de serveurs
Filtre :
Nom
Adresse IP
Systèm
VP-RDS1.vdb-pro.lan
10.10.110.150
1 ordinateur(s) trouvé(s)
Sélectionné
Ordinateur
VDB-PRO.LAN (1)
VP-RDS1
1 ordinateur(s) sélectionné(s)
Les informations d'identification du compte VDB-PRO\administrateur seront utilisées pour ajouter les serveurs.
< Précédent
Suivant >
Ajouter
Annuler


Ajouter Gestionnaire de licences des services Bureau à distance serveurs
Afficher la progression
Sélection un serveur
Confirmation
Résultats
Le service de rôle est en cours d'installation sur les serveurs suivants.
Serveur
État d'avancement
État
Service de rôle Gestionnaire de licences des services Bureau à distance
VP-RDS1.vdb-pro.lan
En cours
Installation...
< Précédent
Suivant >
Ajouter
Annuler


Propriétés de déploiement
Configurer le déploiement
Afficher tout
Passerelle des serv...
Gestionnaire de lic...
Accès Web des ser...
Certificats
Gestionnaire de licences des services Bureau à distance
Sélectionnez le mode de licence des services Bureau à distance :
Par périphérique
Par utilisateur
Spécifiez un serveur de licences puis cliquez sur Ajouter :
Ajouter...
Choisissez l'ordre des serveurs de licences des services Bureau à distance :
Le serveur hôte de session Bureau à distance ou le serveur hôte de virtualisation des services Bureau à distance envoie les demandes de licences aux serveurs de licences spécifiés dans l'ordre où ils sont répertoriés.
VP-RDS1.vdb-pro.lan
Monter
Descendre
Supprimer
OK
Annuler
Appliquer

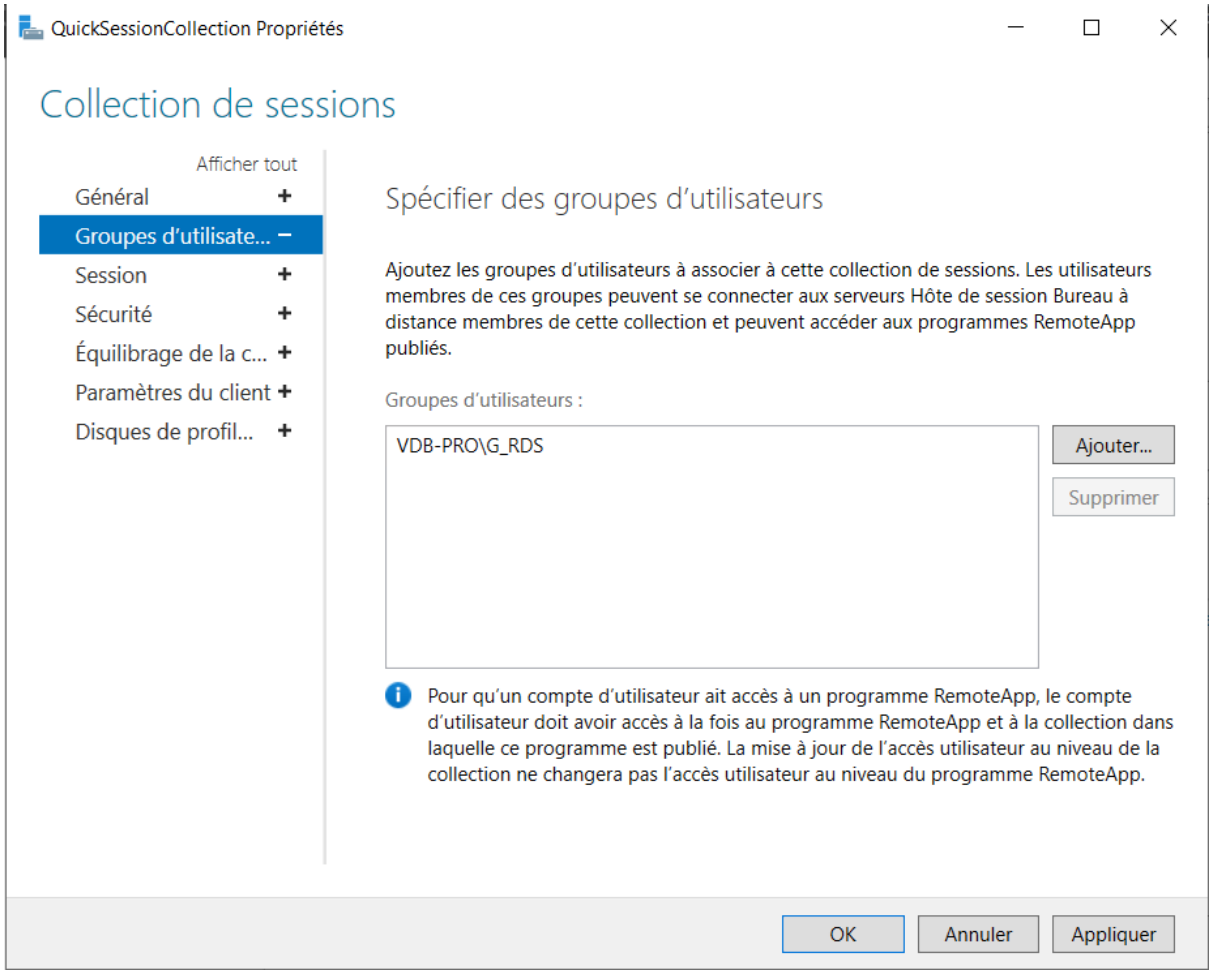
Configuration d'une collection de session

Une fois les rôles RDS installés, j'ai procédé à la création d'une collection de sessions, qui constitue l'élément central dans la gestion des connexions utilisateurs au sein d'un environnement Remote Desktop Services. La collection de sessions permet de définir les règles de fonctionnement des bureaux à distance : elle regroupe les utilisateurs autorisés, les ressources disponibles, et permet de gérer la façon dont les sessions sont ouvertes et administrées.

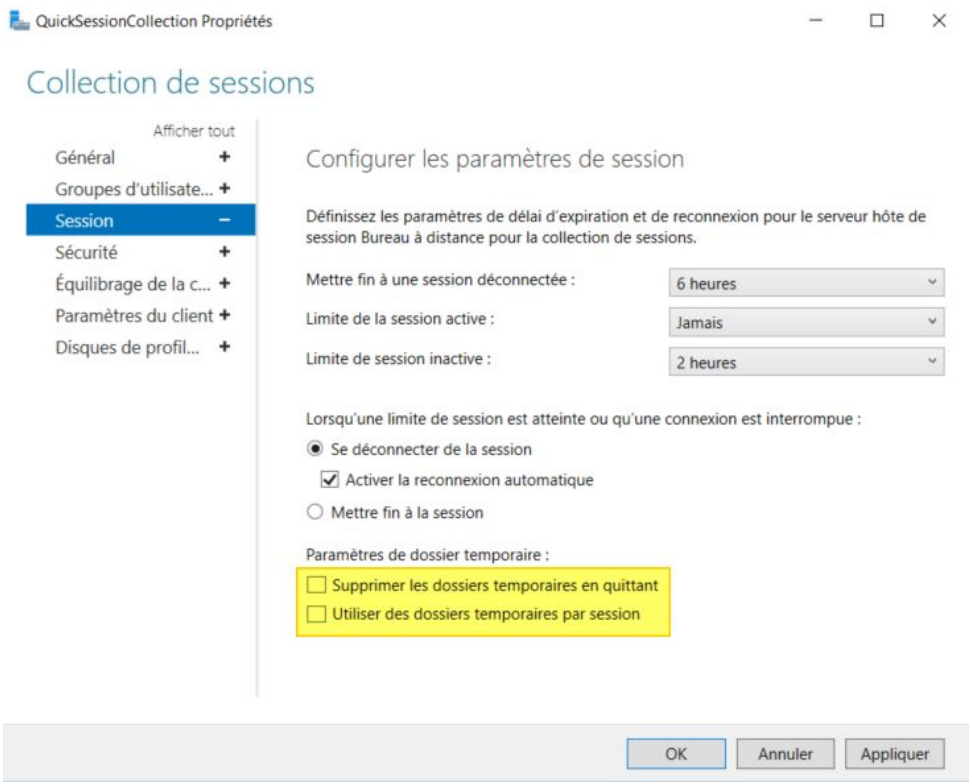


Au sein de cette collection, plusieurs paramètres peuvent être configurés afin de contrôler finement l'utilisation du service. Parmi ceux-ci, on peut notamment :

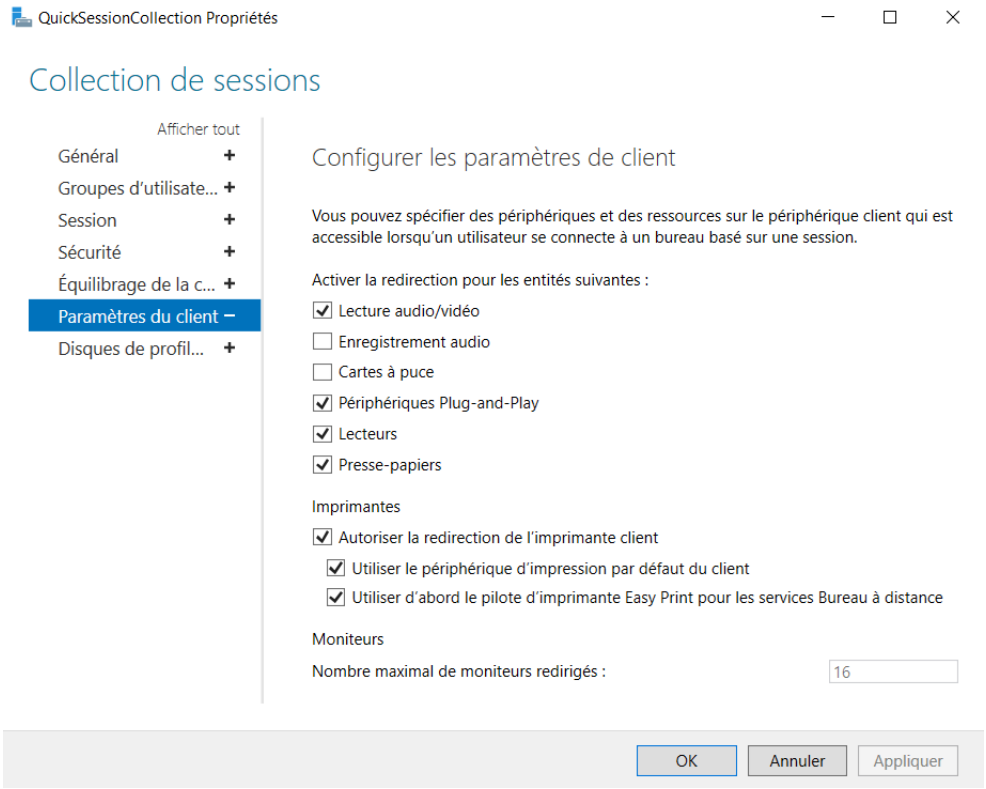
- Définir un dossier de profil utilisateur centralisé pour uniformiser l'environnement de travail,
- Déployer automatiquement des applications spécifiques via un environnement de type RemoteApp (si besoin).
- Restreindre l'accès à certains utilisateurs ou groupes Active Directory,



- Configurer des limites de temps d'inactivité ou de déconnexion automatique pour des raisons de sécurité,

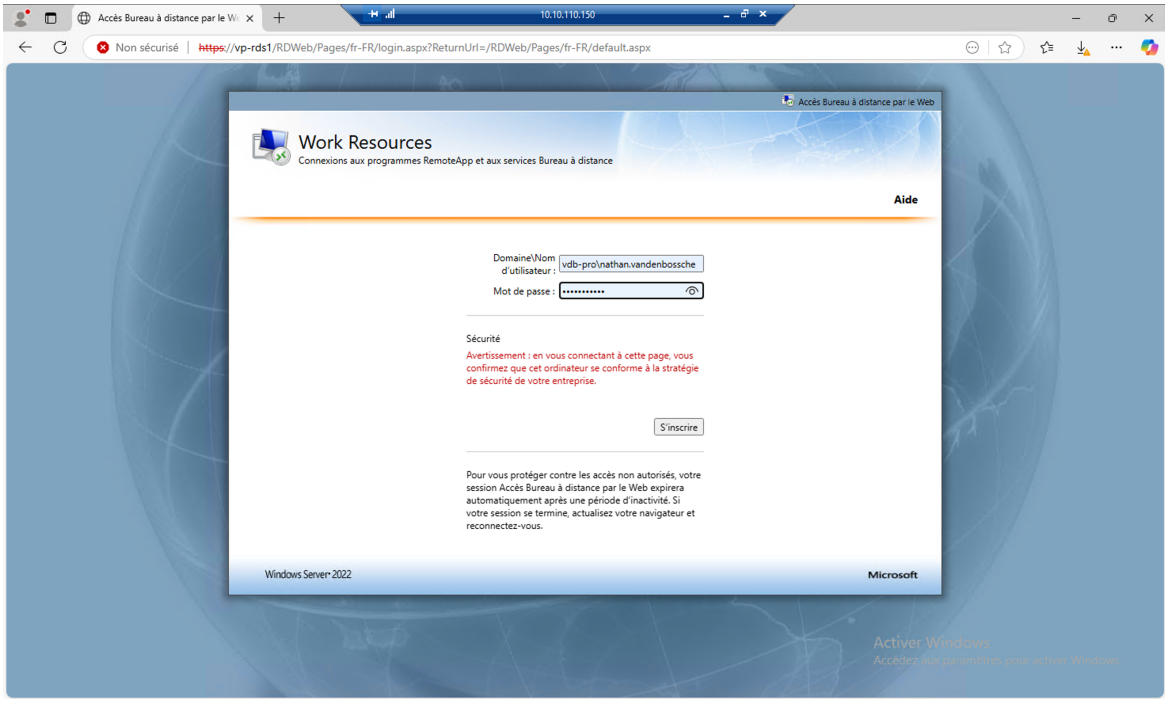


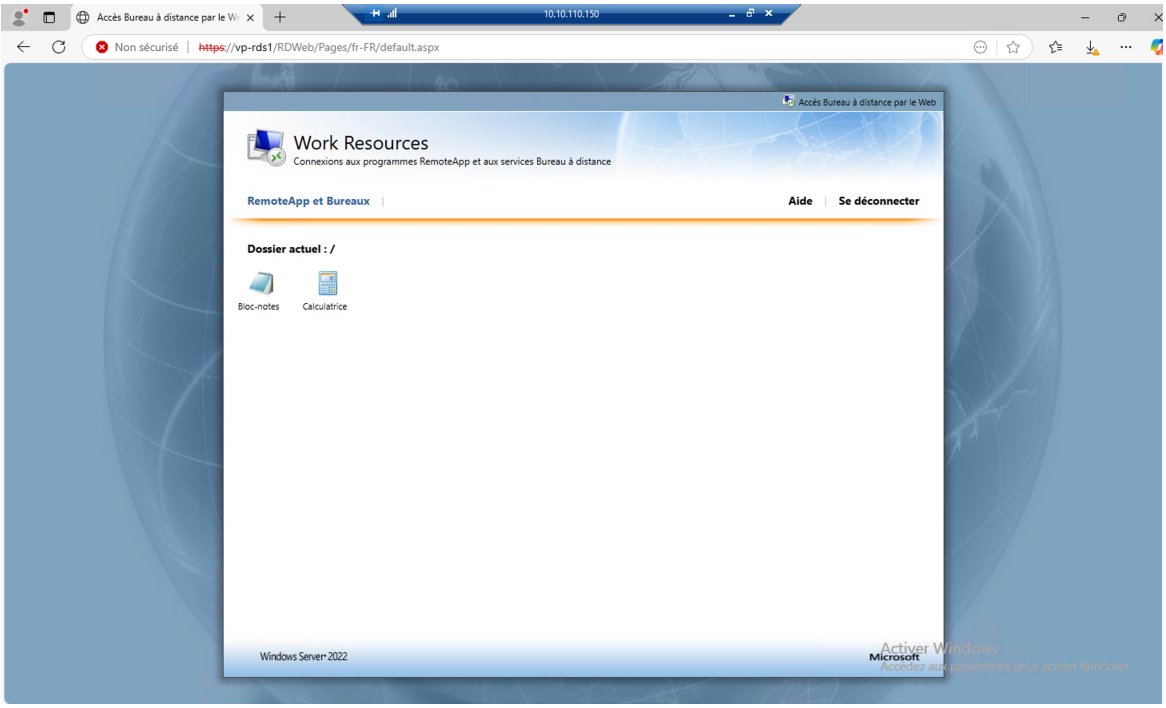
- Activer ou désactiver la redirection des périphériques (clés USB, imprimantes, presse-papiers),



Configuration du RemoteApp Web

J'ai également mis en place la fonctionnalité **RemoteApp via l'interface Web**, permettant aux utilisateurs autorisés de se connecter à un portail web RDS. Grâce à cette interface, ils peuvent lancer des applications spécifiques publiées sur le serveur, comme le Bloc-notes ou la Calculatrice, directement depuis leur poste local. Bien que l'application semble s'exécuter localement, elle est en réalité hébergée et traitée sur le serveur RDS. Cette solution permet une **expérience utilisateur fluide**, tout en **centralisant l'exécution des applications** et en **réduisant la charge sur les postes clients**.

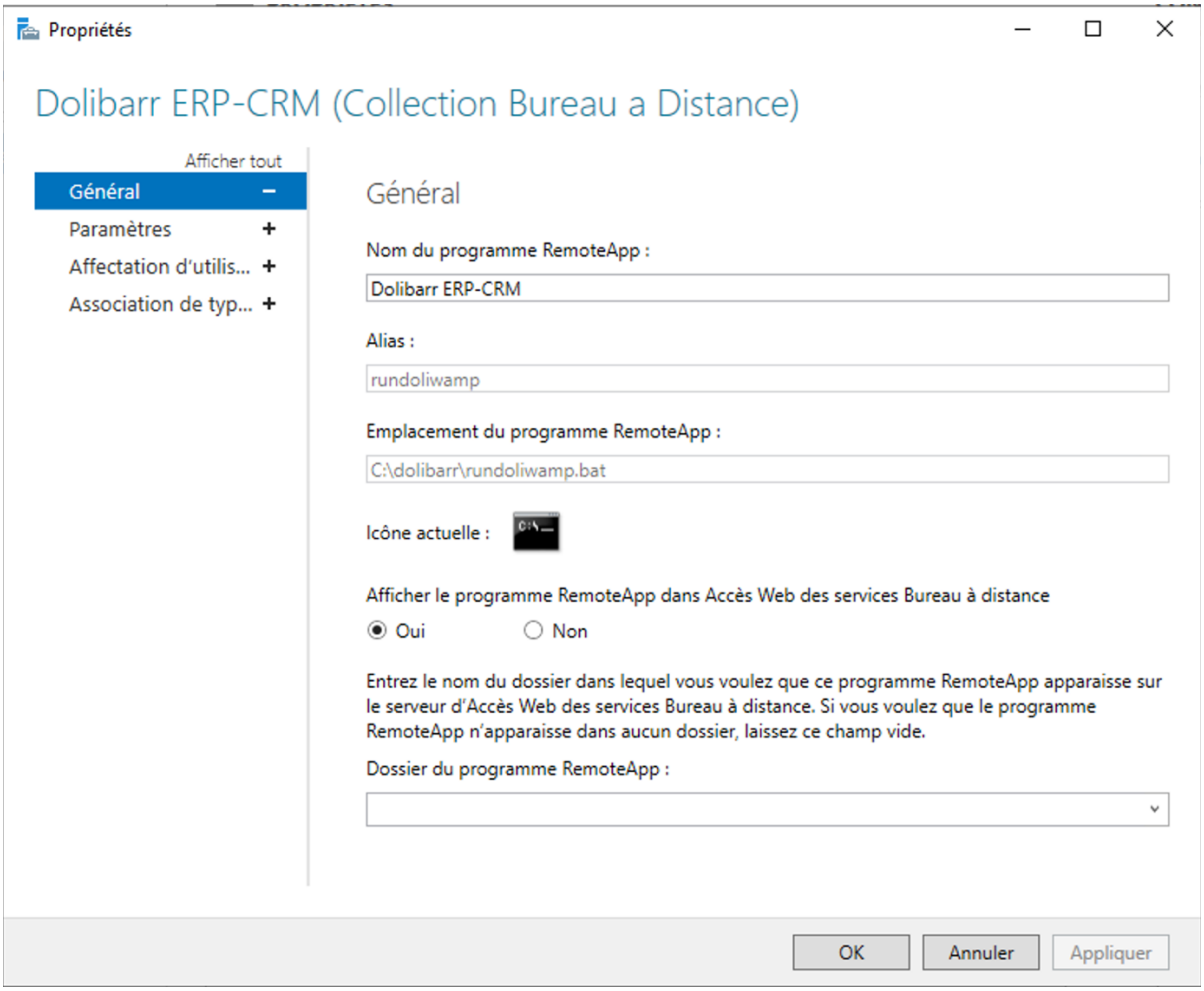




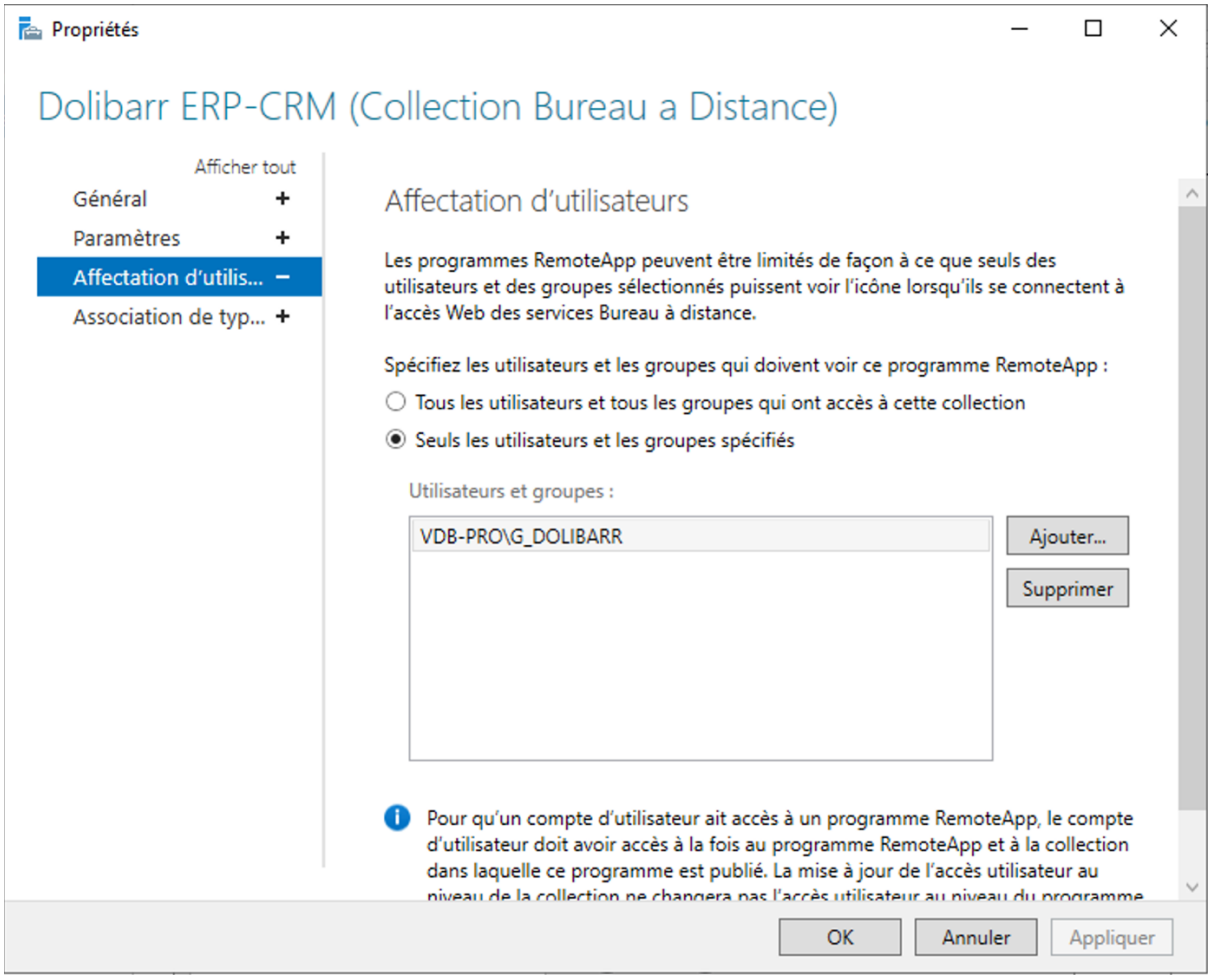
Ajout du logiciel ERP Dolibarr au RemoteApp Web

Pour ajouter le logiciel Dolibarr au portail RemoteApp, je me rends dans le **Gestionnaire de serveur RDS**, puis je clique sur **"Programmes RemoteApp"**, ensuite sur **"Tâches" > "Publier des programmes RemoteApp"**. Une fenêtre s'ouvre, affichant la liste des applications installées sur le serveur.

Je sélectionne **Dolibarr** parmi les programmes disponibles, puis je passe à l'étape suivante : **"Affectation des utilisateurs"**.



À ce niveau, je choisis de restreindre l'accès à l'application uniquement aux membres du **groupe de sécurité Active Directory** G_DOLIBARR, garantissant ainsi que seuls les utilisateurs autorisés puissent y accéder via RDWeb.



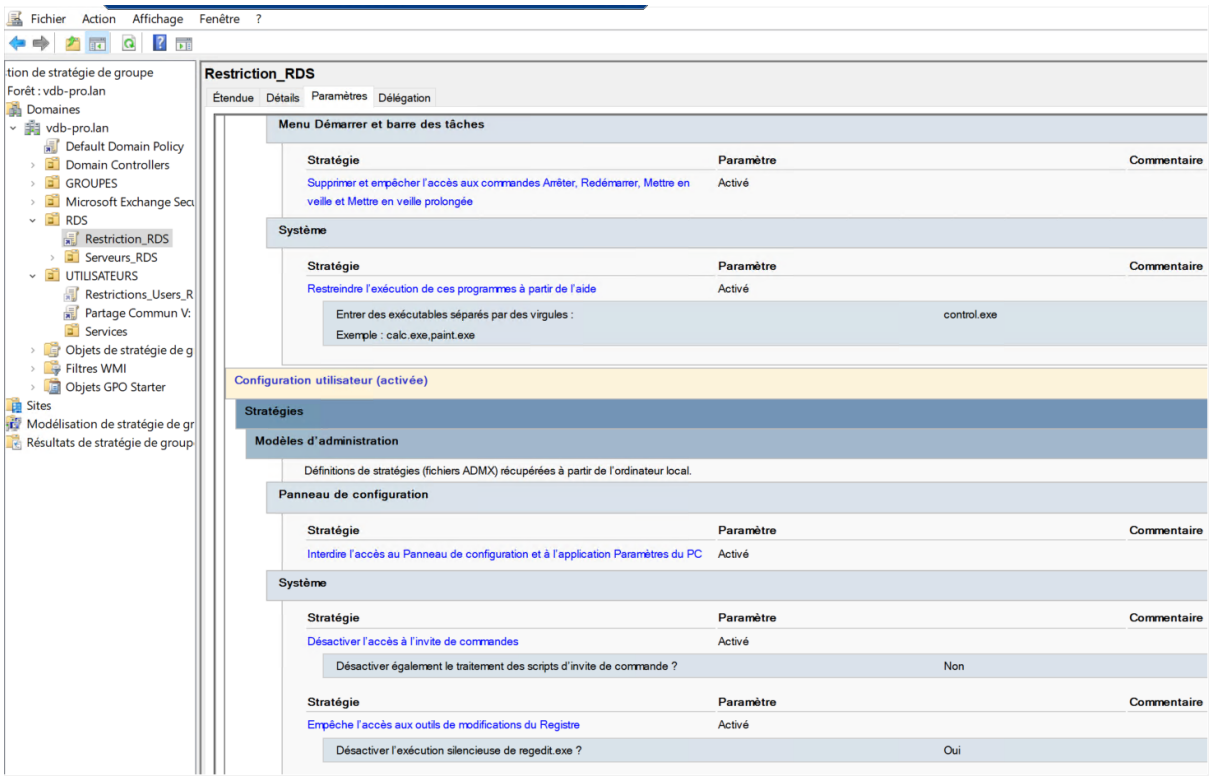
Configuration de GPO pour restreindre

Afin de renforcer la sécurité et de maîtriser l'environnement utilisateur sur les sessions distantes, j'ai mis en place un ensemble de restrictions à l'aide des stratégies de groupe (GPO). Ces GPO ont été appliquées spécifiquement aux utilisateurs de la collection RDS, via une unité d'organisation (OU) dédiée dans l'Active Directory.

Les restrictions mises en œuvre avaient pour objectif de limiter les fonctionnalités disponibles au sein de la session RDS, afin de garantir une utilisation conforme aux besoins de l'entreprise vdb-pro tout en réduisant les risques de mauvaise manipulation ou d'accès non autorisé à certaines fonctions du système.

Parmi les paramètres restreints via GPO, on peut citer :

- La désactivation de l'accès au panneau de configuration et aux paramètres système,
- La désactivation de l'accès au modificateur de registre,
- La désactivaiton de l'accès au terminal,
- La désactivation de l'installation de périphériques ou de logiciels,
- Le blocage de la commande Exécuter, de l'accès au gestionnaire des tâches et à certaines touches du clavier (Ctrl+Alt+Suppr, etc.),
- La redirection de certains dossiers vers des lecteurs réseau (ex : Bureau, Documents),



Cette configuration GPO contribue à créer un espace de travail distant stable, cohérent et sécurisé, adapté à une utilisation en entreprise. Elle permet également de réduire la charge de support technique en limitant les possibilités de modification du système par les utilisateurs.

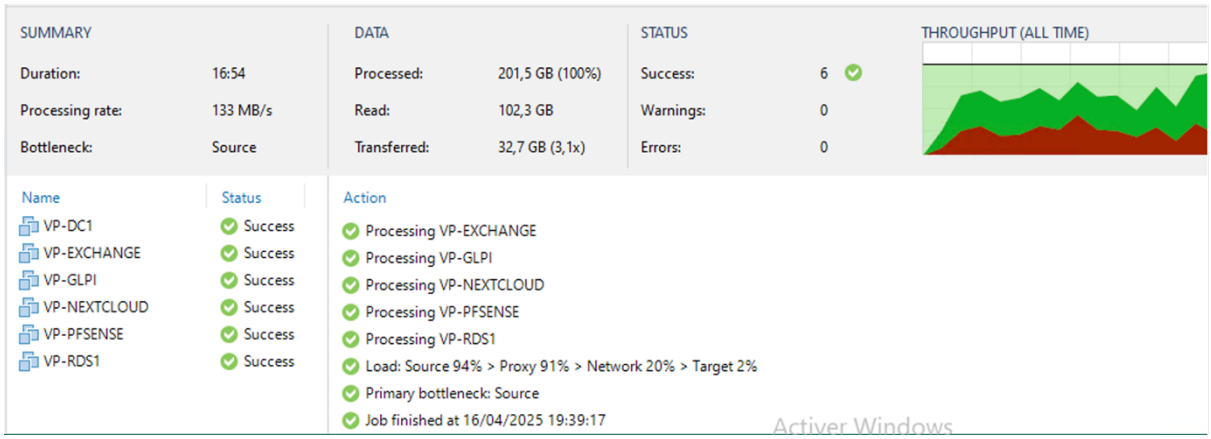
Gérer le patrimoine informatique

La mise en place de l'environnement RDS au sein de vdb-pro, une attention particulière a été portée à la gestion différenciée des droits d'accès entre les utilisateurs standards et les administrateurs système. Pour cela, j'ai configuré des stratégies de groupe (GPO) de manière ciblée, en appliquant des restrictions uniquement aux utilisateurs finaux, tout en laissant les administrateurs avec un accès complet à l'environnement distant.

Concrètement, les GPO restrictives (suppression du panneau de configuration, blocage de la commande Exécuter, désactivation du gestionnaire des tâches, etc.) sont liées à une unité d'organisation (OU) spécifique dans laquelle seuls les comptes utilisateurs standards sont placés. Les comptes d'administration, quant à eux, sont conservés en dehors de cette OU ou sont explicitement exclus de l'application des GPO via des filtres de sécurité et la fonctionnalité de filtrage par groupe de sécurité intégrée à Active Directory.

Cette approche permet de garantir une sécurité renforcée pour les utilisateurs, tout en maintenant la souplesse d'administration nécessaire pour les techniciens et les responsables informatiques, notamment lors des phases de maintenance, de supervision ou de dépannage sur les sessions RDS.

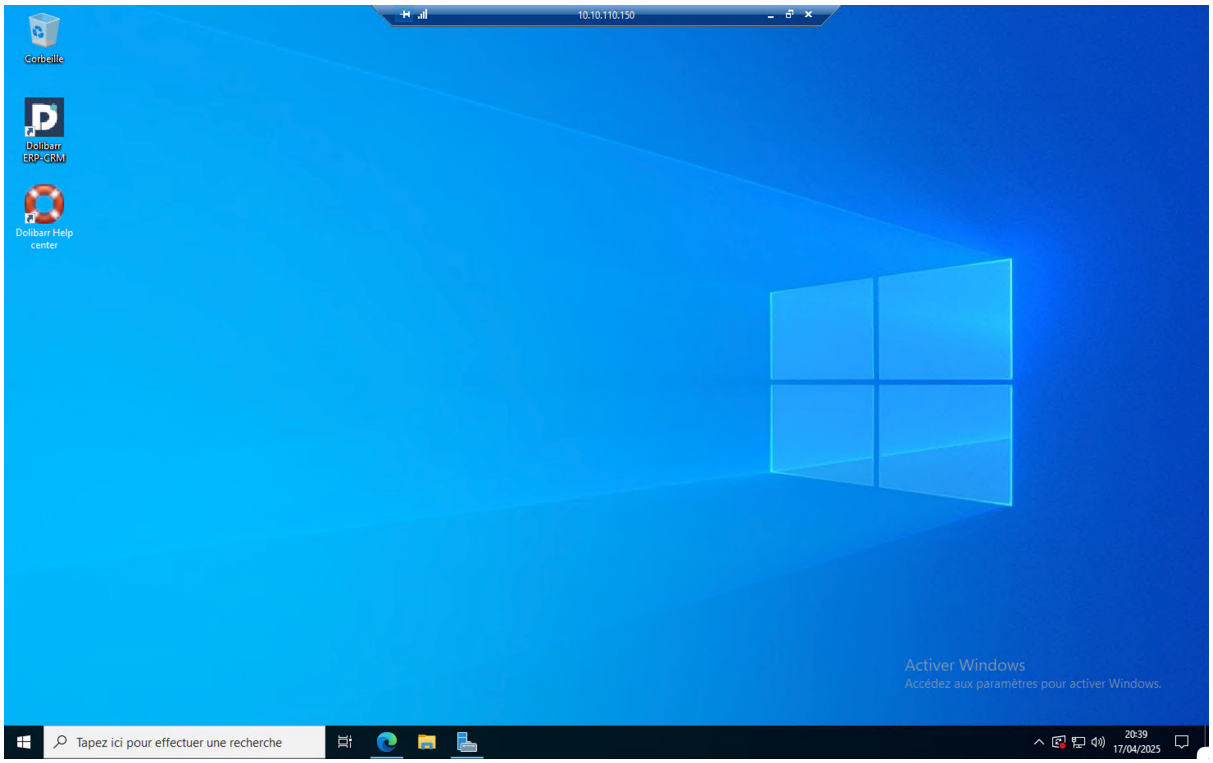
De plus, afin de garantir la pérennité des données et de pouvoir restaurer rapidement le service en cas d'incident, j'ai intégré le serveur RDS à un job de sauvegarde quotidien. Cette sauvegarde est planifiée via la solution de sauvegarde de l'entreprise VEEAM. Cette stratégie s'inscrit dans une politique de continuité de service et de gestion des risques liée à l'infrastructure.



Partie 2 – Validation

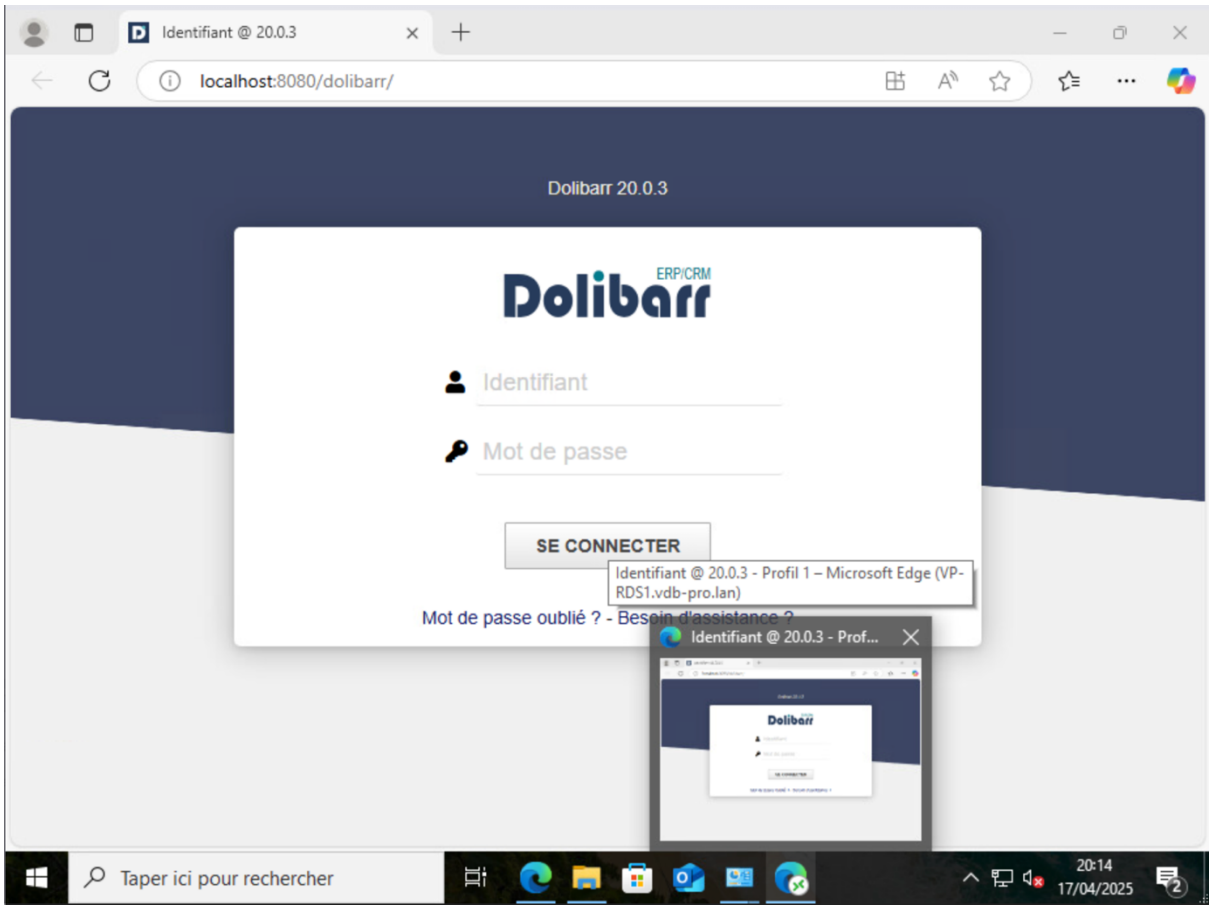
Pour valider le bon fonctionnement de l'installation et de la configuration du serveur RDS, j'ai réalisé une phase de tests fonctionnels à l'aide d'un compte utilisateur créé à mon nom dans l'Active Directory. Ce test a été réalisé depuis un poste client situé sur le VLAN 20 (LAN_CLIENTS), afin de simuler une connexion utilisateur réelle dans les conditions prévues par l'architecture réseau de l'entreprise vdb-pro.

Lors de la connexion à la session distante, j'ai pu vérifier que l'accès au bureau à distance était opérationnel, et que l'environnement chargé correspondait bien aux paramètres définis dans la collection de sessions RDS. J'ai également contrôlé que les stratégies de groupe (GPO) appliquées à l'unité d'organisation de l'utilisateur étaient bien effectives : restrictions d'accès, suppression de fonctionnalités système, redirections éventuelles, etc.

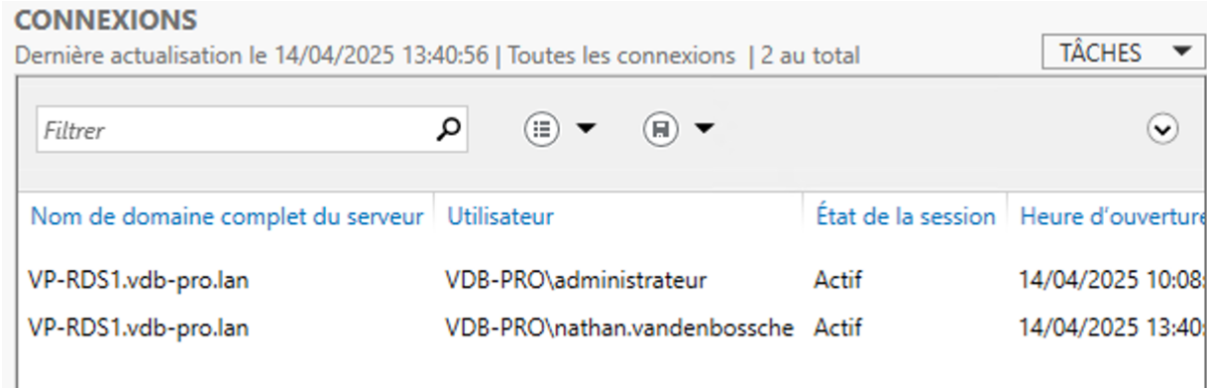


Le logiciel **Dolibarr ERP**, que j'ai installé sur le serveur, est également disponible via l'interface **RemoteApp Web**. Les utilisateurs autorisés peuvent ainsi **télécharger le fichier** .RDP **généré automatiquement**, puis l'exécuter depuis leur poste local. Une fois lancé, l'application **s'ouvre directement dans une session distante**, tout en donnant l'impression qu'elle est utilisée localement.

Dolibarr fonctionne en mode client/serveur, et l'ensemble des données saisies sont **synchronisées en temps réel avec la base de données hébergée sur le serveur RDS1**, garantissant **centralisation, sécurité et accessibilité** des informations métiers.



Enfin, depuis le serveur VP-RDS1, j'ai utilisé les outils d'administration RDS pour surveiller en temps réel la session de l'utilisateur connecté. Cela m'a permis de confirmer que l'utilisateur était bien enregistré comme actif sur le serveur, que sa session avait été correctement initiée, et qu'aucune erreur n'était présente dans les journaux d'événements liés à la connexion.



Ces vérifications m'ont permis de valider la conformité de la solution déployée, tant sur le plan fonctionnel que sur le plan de la sécurité et de la gestion centralisée.

Partie 3 – Veille Technologique

Dans le cadre de cette réalisation, j'ai également mené une veille technologique afin de m'informer sur les alternatives aux services Remote Desktop Services (RDS) de Microsoft, les évolutions possibles de l'infrastructure, ainsi que les bonnes pratiques en matière de sécurité informatique.

Organiser son développement professionnel

Environnement d'apprentissage personnel

Mon environnement d'apprentissage personnel est clairement défini : je travaille principalement sur une infrastructure virtualisée via VMware ESXi, ce qui me permet de simuler des environnements professionnels. Cela comprend des machines virtuelles Windows Server, des postes clients, des VLANs configurés, et des services comme Active Directory, DNS, RDS, etc. Cet environnement me permet de tester, apprendre de mes erreurs et développer mes compétences techniques en autonomie.

Mise en œuvre d'une veille technologique

Ma veille est régulière et structurée. Elle a pour objectif :

- de repérer les technologies émergentes dans les domaines des systèmes, réseaux et de la cybersécurité (par exemple : solutions cloud, alternatives à RDS comme Citrix, ou innovations en MFA),
- d'utiliser des moyens fiables et variés de recherche, tels que Feedly, les blogs officiels Microsoft, CERT-FR, ZDNet, GitHub ou encore des forums techniques spécialisés,
- et de renforcer mes compétences sur des sujets techniques spécifiques ou en lien avec la sécurité des systèmes d'information.

Alternatives à RDS

Parmi les solutions concurrentes à Microsoft RDS, Citrix Virtual Apps and Desktops se démarque comme une alternative robuste et performante. Elle propose des fonctionnalités avancées comme :

- Une meilleure gestion des ressources avec le protocole HDX, plus optimisé que RDP,
- Une expérience utilisateur plus fluide, notamment pour les applications graphiques ou en cas de faible bande passante,
- Des capacités d'intégration cloud plus poussées (Azure, AWS),
- Un niveau de granularité plus élevé dans la gestion des accès et des ressources.

Cependant, cette solution est plus complexe à déployer et nécessite une licence payante généralement plus onéreuse que celle de Microsoft RDS.

Améliorations possibles

À court ou moyen terme, plusieurs pistes d'évolution peuvent être envisagées pour faire monter en puissance l'infrastructure :

- Mise en place d'un serveur de licences RDS pour une gestion conforme des accès,
- Déploiement de RemoteApp, pour publier uniquement certaines applications sans donner accès au bureau complet,
- Implémentation d'un broker de connexion pour permettre la tolérance de panne et le rééquilibrage de charge en environnement multi-RDS,
- Intégration d'une solution de supervision (type Centreon ou Zabbix) pour surveiller les performances et les connexions.
- L'implémentation de solutions de double authentification (MFA) pour renforcer l'accès distant,

Veille sécurité

Du point de vue de la sécurité, la veille porte sur :

- Les vulnérabilités RDP recensées dans la base CVE (Common Vulnerabilities and Exposures),
- L'utilisation du chiffrement TLS et la désactivation des anciennes versions du protocole RDP (RDP 5.0 et antérieurs),
- La segmentation réseau renforcée et la journalisation des accès via un SIEM (Security Information and Event Management).