I. Introduction et Présentation des principales fonctionnalités du service RDS

Dans le cadre de l'épreuve E4 du BTS SIO 2025, le projet consiste à mettre en place une solution d'applications distantes pour l'entreprise Assurmer. Cette solution permettra aux utilisateurs de se connecter à distance aux outils et applications nécessaires à l'exercice de leur activité, tout en garantissant une sécurité optimale des accès.

La mise en œuvre repose sur l'utilisation de Remote Desktop Services (RDS), une technologie de Microsoft qui offre des fonctionnalités avancées pour le déploiement et la gestion des services bureautiques et métiers à distance. Ce projet s'inscrit dans un contexte où le télétravail et les déplacements professionnels nécessitent des solutions robustes pour maintenir la continuité des activités tout en répondant aux exigences de sécurité.

1. **Protocole RDP (Remote Desktop Protocol)**

Rôle : Le protocole RDP est le cœur du fonctionnement des services RDS. Il est conçu pour permettre une communication entre le client (l'utilisateur) et le serveur (hébergeant les applications ou bureaux à distance). RDP offre une interface graphique permettant aux utilisateurs d'accéder à un environnement distant comme s'ils étaient connectés directement à la machine.

- Déployer des sessions distantes sur votre serveur en mettant à disposition un bureau pour chaque utilisateur
- Déployer des applications en mode Remote App pour permettre l'accès distant sans passer par un bureau distant
- Déployer des sessions distantes directement au travers d'un ordinateur virtuel attribué à chaque utilisateur (virtualisation de postes de travail)

2. **Sécurité et Avantages**

- Le Protocole RDP permet de chiffrer les données échangées pour garantir leur confidentialité.
- La configuration de certificats SSL/TLS sur la passerelle RD Gateway pour sécuriser les connexions externes.

Avantages :

- Gestion centralisée des licences.
- Permet un suivi précis de l'utilisation des licences pour garantir la conformité.

Gestion stricte des droits d’accès

Ne donner accès qu'aux utilisateurs ayant besoin des services RDS.

Restreindre les permissions d'accès aux applications ou fichiers selon les rôles.

Utiliser Active Directory pour centraliser la gestion des droits d'accès.

Configurer des groupes de sécurité spécifiques pour limiter les connexions aux hôtes RDS.

Surveillance et audit

Activer les journaux d'événements Windows pour surveiller les connexions RDP :

- Tentatives de connexion échouées.
- Activités suspectes, telles que des connexions depuis des adresses IP inhabituelles.

Protection contre les attaques externes

- Modifier le port RDP par défaut (3389) pour réduire les risques d’attaques automatisées. Exemple : définir un port personnalisé.
- Mettre en œuvre un **pare-feu** pour limiter l’accès au port RDP uniquement aux adresses IP approuvées.
- Utiliser **RD Gateway** pour fournir un accès sécurisé via HTTPS (port 443) au lieu d’exposer directement les serveurs RDS à Internet.

Cela permet de filtrer les connexions et d’ajouter une couche de protection supplémentaire

Mise à jour et gestion des vulnérabilités

- Maintenir à jour les systèmes d'exploitation et les services RDS pour corriger les failles de sécurité connues.
- Mettre à jour régulièrement les certificats SSL/TLS pour éviter les problèmes d’expiration.