



ETUDE CONCERNANT LES FONCTIONNALITEES DU SERVICE RDS

Aymeric P, Abdou A, Elijah B

Étude des fonctionnalités principales des Remote Desktop Services (RDS)

Rôle Web pour l'accès distant

Le rôle RD Web Access permet aux utilisateurs de se connecter à des applications ou bureaux publiés via un portail web. Ce portail est hébergé sur un serveur configuré avec IIS (Internet Information Services).

Principales fonctionnalités :

- Portail Web sécurisé : Les utilisateurs accèdent au portail via une URL spécifique en HTTPS.
- Publication des ressources : Les administrateurs peuvent rendre disponibles des applications (RemoteApps) ou des bureaux complets.
- Accessibilité universelle : Le portail est accessible depuis n'importe quel navigateur.

Configuration requise :

- Un serveur avec IIS configuré.
- Installation du rôle "Accès Web aux services Bureau à distance".
- Certificat SSL pour sécuriser les connexions HTTPS.

Service Broker pour les connexions Bureau à distance

Le rôle RD Connection Broker est un composant central dans les RDS, permettant de gérer les connexions utilisateur.

Principales fonctionnalités :

- Gestion des sessions : Les utilisateurs reprennent leur session active même s'ils se reconnectent depuis un autre appareil.
- Équilibrage de charge : Le Broker répartit les connexions entre plusieurs serveurs RDS.
- Haute disponibilité : Peut être configuré en cluster pour éviter les interruptions.

Configuration requise :

- Une base de données SQL (facultative) pour la haute disponibilité.
 - Un certificat SSL pour sécuriser les communications.
-

Passerelle d'authentification (RD Gateway)

Le rôle RD Gateway permet d'établir des connexions sécurisées entre des utilisateurs distants et les ressources internes de l'entreprise.

Principales fonctionnalités :

- Connexion via HTTPS : Utilise le port 443 pour éviter les restrictions réseau.
- Authentification sécurisée : Prend en charge les protocoles RADIUS et les certificats d'authentification.
- Protection réseau : Fournit un contrôle des connexions basé sur des stratégies utilisateur.

Configuration requise :

- Un serveur avec le rôle RD Gateway installé.
 - Certificat SSL valide pour le rôle Gateway.
 - Configuration des stratégies de connexion et d'autorisation (CAP/RAP).
-

Hôtes de session Bureau à distance

Les RD Session Hosts sont les serveurs qui hébergent les sessions utilisateur ou les applications RemoteApp.

Principales fonctionnalités :

- Hébergement des sessions utilisateur : Permet à plusieurs utilisateurs de se connecter simultanément.
- Exécution des applications : Les applications publiées sont exécutées sur le serveur, et non sur l'appareil utilisateur.
- Gestion des ressources : Paramètres avancés pour limiter la consommation CPU, RAM et disque.

Configuration requise :

- Systèmes Windows Server 2019 ou 2022.
 - Paramètres GPO pour gérer la redirection de ressources (imprimantes, presse-papiers, etc.).
-

Gestionnaire de licences

Le RD Licensing Manager gère les licences utilisateur ou périphérique nécessaires pour se connecter aux services RDS.

Principales fonctionnalités :

- Types de licences :
 - Par utilisateur : une licence par utilisateur unique.
 - Par périphérique : une licence par appareil utilisé.
- Gestion centralisée : Permet de gérer toutes les licences depuis une console unique.
- Activation des licences : Nécessite l'activation du serveur de licences via Internet ou téléphone.

Configuration requise :

- Installation du rôle "Gestionnaire de licences des services Bureau à distance".
 - Acquisition des licences CAL (Client Access License).
-

Synthèse :

Les Remote Desktop Services (RDS) offrent une solution complète pour le déploiement d'applications et de bureaux accessibles à distance. Chaque rôle joue un rôle critique dans le fonctionnement global :

- RD Web Access : interface utilisateur.
- RD Connection Broker : gestion des sessions.
- RD Gateway : sécurisation des connexions.
- RD Session Host : exécution des sessions.
- RD Licensing Manager : gestion des licences.