AP 7 : MISE EN PLACE D'UNE SOLUTION D'APPLICATIONS DISTANTES	HUYNH Michael SAKO Bah FRANÇAIS Benjamin 2B-SISR

ASSURMER

Version	Auteur	Date	Nombre de pages	À l'attention de	Mode de diffusion	Validateur
1.0	HUYNH Michael	18/08/2024	11	Assurmer-IT	Document PDF	FRANÇAIS Benjamin

PRESENTATION DES PRINCIPALES FONCTIONNALITES DU SERVICE RDS

Table des matières

Introduction

Dans le cadre de notre projet, nous avons pour mission d'implémenter une solution de bureaux et applications distantes à l'aide du service RDS sous Windows Server 2022. Cette solution permettra aux utilisateurs, qu'ils soient en déplacement ou au bureau, d'accéder à leurs applications essentielles via des connexions sécurisées, répondant ainsi aux besoins croissants de mobilité et d'efficacité.

Notre projet vise à mettre en place une solution RDS en intégrant plusieurs fonctionnalités :

- **Le protocole RDP** (Remote Desktop Protocol) qui permet une communication fluide entre clients et serveurs grâce à une encapsulation sécurisée des données.
- **Les Hôtes de session Bureau à distance** (RDSH) qui gère l'accès multi-utilisateurs à des sessions de bureau sur un serveur centralisé.
- **L'accès Web au Bureau à distance** (RD Web Access) offre aux utilisateurs la flexibilité d'accès via un navigateur sécurisé, n'importe où et sur tout appareil.
- **Le Service Broker pour les connexions Bureau à distance** (RDCB) qui assure le routage des sessions et une répartition optimale des charges entre les serveurs.
- **La Passerelle des services Bureau à distance** (RD Gateway) qui fournit un tunnel sécurisé pour les connexions RDP via Internet sans nécessiter de VPN.
- **Le Gestionnaire des licences** qui garantit la conformité de notre solution avec les exigences de licences Microsoft pour les accès utilisateur et périphérique.

Nous ferons d'abord une configuration testée sous VM Workstation, assurant ainsi une maîtrise des étapes et des éventuels ajustements avant le déploiement sur les serveurs en production. Les rôles seront documentés avec une procédure d'installation détaillée pour chaque composant. Voici comment nous nous sommes organisés.

Planning

	Étude des fonctionnalités principales du service RDS	Installation et configuration sous VM Workstation	Installation et configuration sur serveurs	Tests d'intégration	Finalisation des livrables
Affecté à	Michael HUYNH	Benjamin FRANCAIS	BAH SAKO	Toute l'équipe	Toute l'équipe
Date de la finalisation	30/10/2024	30/10/2024	13/11/2024	13/11/2024	27/11/2024
Documents associés	PresentationRDS.docx	ProcédureInstallation.docx	ProcédureInstallation.docx	TestIntégration.docx	Procédure Utilisateurs.docx

1. Rôle et fonctionnement du protocole RDP (Remote Desktop Protocol)

Le protocole RDP (Remote Desktop Protocol) est la base des connexions à distance dans un environnement RDS. Concrètement, il permet de « projeter » l'interface d'un serveur RDSH sur le poste de l'utilisateur, en transmettant à distance les actions effectuées (mouvements de la souris, saisie au clavier) et en renvoyant l'affichage mis à jour de l'écran.

Sur le plan technique, RDP utilise principalement le port 3389 et suit un modèle client-serveur. L'utilisateur envoie ses actions au serveur via des paquets TCP ou UDP, et celui-ci renvoie en retour une image compressée et encodée de l'écran, ce qui optimise les performances. Le protocole est conçu en plusieurs couches : l'application gère l'interaction utilisateur, la couche transport assure la stabilité et la fiabilité des échanges, tandis que la couche présentation se charge de la compression et du codage graphique.

En matière de sécurité, on s'appuie sur TLS (également appelé SSL) pour chiffrer les données, empêchant ainsi les accès non autorisés. Des stratégies de groupe (GPO) peuvent également être mises en place pour restreindre l'accès et définir des règles spécifiques d'authentification et d'autorisation.

En pratique, le RDP est très utile pour les salariés qui doivent se connecter à leur environnement de travail depuis divers lieux (un autre bureau, leur domicile, etc.). Il leur garantit un accès fiable, sécurisé et performant à leurs ressources, même à distance.

2. Hôtes de session Bureau à distance (Remote Desktop Session Host - RDSH)

Le RDSH (Remote Desktop Session Host) est le serveur qui fournit aux utilisateurs un accès à des bureaux et à des applications centralisées. Chaque utilisateur possède sa propre session isolée, garantissant une exécution indépendante des applications et limitant les interférences entre les sessions. Cette approche favorise une centralisation plus efficace des ressources et des données.

Sur le plan technique, le RDSH alloue dynamiquement les ressources matérielles (processeur, mémoire vive, etc.) entre les différentes sessions en fonction des besoins réels. L'installation unique des applications sur le serveur permet de simplifier considérablement leur gestion et leurs mises à jour, évitant ainsi la multiplication des interventions sur les postes de travail individuels. Grâce au protocole RDP, les utilisateurs peuvent accéder à ces applications sans nécessiter de déploiements complexes sur leurs propres machines.

Le recours à un RDSH diminue les coûts matériels et de maintenance, tout en facilitant la gestion globale de l'infrastructure. Néanmoins, il est crucial de bien dimensionner le serveur afin de prévenir tout risque de saturation et de dégradation des performances en cas d'utilisation intensive. En résumé, un RDSH correctement configuré assure une utilisation optimale des ressources, une centralisation efficace et une expérience utilisateur stable.

3. Accès Web au Bureau à distance (Remote Desktop Web Access - RD Web Access)

RD Web Access offre un portail web sécurisé permettant aux utilisateurs d'accéder aux bureaux et aux applications hébergés, sans nécessiter l'installation préalable d'un client lourd. Cette solution est particulièrement adaptée à ceux qui doivent se connecter depuis une grande variété d'appareils (ordinateurs personnels, tablettes, etc.). Cependant, dans une perspective à plus long terme, il est recommandé de déployer également un VPN, afin de sécuriser la connexion au réseau de l'entreprise, quel que soit l'appareil utilisé.

Le portail RD Web Access est accessible via une simple connexion HTTPS, offrant aux utilisateurs une interface claire où ils peuvent sélectionner le bureau ou les applications nécessaires. Une fois l'authentification validée, une session RDP est lancée, soit par le client RDP natif du système, soit directement au sein du navigateur.

L'un des principaux avantages de RD Web Access réside dans la simplicité d'accès aux ressources, sans qu'une configuration complexe soit requise sur la machine de l'utilisateur. Le chiffrement via HTTPS garantit déjà un certain niveau de sécurité, et la mise en place ultérieure d'une authentification multi-facteurs (MFA) viendra renforcer davantage la protection des accès.

Néanmoins, la qualité de l'expérience utilisateur dépendra de la performance du navigateur et de la stabilité de la connexion réseau. RD Web Access convient donc particulièrement aux employés en mobilité ou en télétravail, ayant besoin d'un accès sécurisé sans lourdes contraintes d'installation. Malgré tout, il est important de noter que l'utilisation du client lourd, lorsque cela est possible, restera généralement plus optimale en termes de performances et de fonctionnalités.

4. Service Broker pour les connexions Bureau à distance (Remote Desktop Connection Broker - RDCB)

Le Service Broker est un composant essentiel de l'infrastructure RDS, chargé de gérer le routage des utilisateurs vers les serveurs RDSH. Il peut, en fonction de la situation, réorienter un utilisateur vers une session déjà ouverte, démarrer une nouvelle session ou mettre fin à une session inutilisée. Cette fonctionnalité permet d'assurer une continuité de session en cas de déconnexion et contribue à une meilleure stabilité du service en répartissant la charge sur l'ensemble des serveurs RDSH disponibles.

D'un point de vue opérationnel, le Service Broker évalue en continu l'état des serveurs RDS et répartit les connexions en fonction des ressources disponibles. Cet équilibrage de charge (load balancing) prévient les risques de surcharge sur un serveur donné et améliore ainsi les performances et la stabilité globales de l'environnement RDS.

Si le Service Broker offre une gestion de session grandement optimisée, notamment dans les environnements de grande envergure, sa mise en œuvre requiert une configuration réseau soignée. Il convient, en effet, d'éviter les points de contention qui pourraient augmenter la latence et de maintenir un niveau de sécurité élevé afin d'assurer une expérience utilisateur fluide et fiable.

5. Passerelle des services Bureau à distance (Remote Desktop Gateway - RD Gateway)

La RD Gateway joue un rôle d'intermédiaire entre l'internet public et le réseau interne de l'entreprise, offrant ainsi la possibilité d'accéder aux applications et aux bureaux distants via un tunnel sécurisé. Cette solution encapsule les connexions RDP dans un flux HTTPS sur le port 443, permettant de s'affranchir de l'utilisation d'un VPN pour accéder aux ressources internes.

Concrètement, lorsqu'un utilisateur tente de se connecter, la RD Gateway établit un tunnel HTTPS, chiffré par TLS/SSL, garantissant la confidentialité et l'intégrité des données échangées. Il est également possible d'intégrer une authentification multi-facteurs (MFA) afin de renforcer le niveau de sécurité des accès, réduisant ainsi le risque d'intrusion non autorisée.

Grâce à cette passerelle, les utilisateurs itinérants bénéficient d'un accès à distance flexible et sécurisé, depuis n'importe quel appareil connecté à Internet. Le chiffrement et l'authentification via la RD Gateway assurent une connexion fiable, sécurisée et adaptée aux besoins des environnements professionnels modernes.

6. Gestionnaire des licences RDS license (Remote Desktop Licensing)

Le Gestionnaire des licences pour RDS veille à ce que chaque utilisateur ou chaque périphérique accédant aux services à distance dispose d'une licence appropriée, assurant ainsi le respect des exigences de Microsoft. Deux types de licences principales sont disponibles (les CAL, ou Client Access Licenses) :

- **CAL par utilisateur** : Cette licence est attribuée directement à une personne. L'utilisateur ainsi licencié peut se connecter aux services RDS depuis plusieurs appareils, ce qui s'avère particulièrement pratique pour les collaborateurs nécessitant une grande flexibilité dans leurs méthodes de travail.

- **CAL par appareil** : Cette licence est liée à un poste de travail spécifique, permettant à n'importe quel utilisateur de cet équipement d'accéder aux services RDS. Ce modèle est idéal pour les environnements dans lesquels plusieurs employés partagent le même dispositif.

Le Gestionnaire des licences contrôle en continu la disponibilité des licences dès qu'une connexion est établie. Si une licence est libre, elle est automatiquement attribuée, et le Gestionnaire en assure le suivi précis. Cette supervision centralisée facilite la gestion et garantit une conformité permanente.

En veillant à ce que chaque connexion RDS soit couverte par une licence valide, le Gestionnaire des licences contribue à éviter les interruptions de service liées à un manque de licences, tout en assurant le respect des conditions légales imposées par Microsoft. Un suivi régulier des licences est néanmoins nécessaire, afin d'éviter toute non-conformité pouvant entraîner des pénalités. Il convient également d'intégrer le coût d'acquisition et de renouvellement des licences RDS dans la planification budgétaire de l'entreprise.

7. Webographie

- https://learn.microsoft.com/fr-fr/windows-server/remote/remote-desktop-services/rds-roles
- https://www.digicert.com/fr/what-is-ssl-tls-and-https
- https://www.eginnovations.com/supported-technologies/rdsh-server-desktop-monitoring#:~:text=RDSH%20stands%20for%20Remote%20Desktop,for%20remote%20access%20by%20users.
- https://v2cloud.com/tutorials/rd-web-access#:~:text=Remote%20Desktop%20Web%20Access%20(RD,(IIS)%20is%20also%20installed.
- https://std.rocks/fr/windows_rds_farm.html
- https://www.techtarget.com/searchvirtualdesktop/definition/remote-desktop-connection-broker#:~:text=A%20remote%20desktop%20connection%20broker%20is%20software%20that%20allows%20a,remote%20desktop%20host%20or%20server.
- https://www.ninjaone.com/blog/how-to-set-up-remote-desktop-gateway/#:~:text=RD%20Gateway%2C%20Microsoft%20Remote%20Desktop,network%20over%20a%20secure%20channel.
- https://www.appsanywhere.com/resource-centre/understanding-rds-licensing
- https://www.it-connect.fr/deploiement-rapide-dun-serveur-rds-avec-windows-server-2016/