Prérequis

L'objectif de cette documentation étant de tester la mise en place d'une telle infrastructure, nous ne nous attarderons pas sur la mise en place du contrôleur de domaine, ou du serveur DNS. Voici la pré-configuration que vous devez avoir mise en place avant l'installation des rôles RDS.

1. Configuration du DNS

La première configuration à appliquer se fait au niveau du DNS, sur **DC1**. La zone de recherche directe doit être configurée ainsi :

Nom	Type	Données
_msdcs		
_sites		
_tcp		
_udp		
DomainDnsZones		
ForestDnsZones		
(identique au dossier parent)	Hôte (A)	172.16.0.1
DC1	Hôte (A)	172.16.0.1
RDS-BROKER	Hôte (A)	172.16.0.10
RDS-01	Hôte (A)	172.16.0.11
ferme1	Hôte (A)	172.16.0.11
RDS-02	Hôte (A)	172.16.0.12
ferme1	Hôte (A)	172.16.0.12
RDS-GATE	Hôte (A)	172.32.0.1
RDS-WEB	Hôte (A)	172.32.0.2
(identique au dossier parent)	Serveur de noms (NS)	dc1.gsb.com.
(identique au dossier parent)	Source de nom (SOA)	[82], dc1.gsb.com., hostm...

N'oubliez pas de créer les pointeurs PTR associés en conséquence, dans la zone de recherche inversée. Vous pouvez voir que les noms **ferme1** pointent vers deux adresses IPv4 : celle de **RDS-01**, et celle de **RDS-02**. C'est normal ; il s'agit d'un tourniquet DNS (ou Round-Robin). C'est notamment ce qui permettra au Broker, de manière transparente, de rediriger les requêtes clientes vers les serveurs de la ferme, lorsqu'il effectueront une requête vers **ferme1**.

2. Création des comptes utilisateurs

La dernière étape de cette phase de pré-configuration consiste à créer les comptes utilisateurs et leurs garantir certains droits pour faciliter nos tests. Pour cela, dans l'AD, créez un groupe de sécurité appelé **Utilisateurs_RDS,** et un autre appelé **Utilisateurs_Winrar**. Ensuite, créez un compte utilisateur « **John Doe** » (login : jdoe@gsb.com) et ajoutez-le dans les groupes suivants : **Administrateurs**, **Administrateurs du domaine**, **Utilisateurs_RDS** et **Utilisateurs_Winrar**.

Vous devriez être prêt à la mise en place de l'infrastructure.

Mise en place de l'infrastructure

I. Mise en place du routeur pfSense

Dans cette première partie, nous verrons très rapidement comment configurer le routeur/pare-feu pfSense et ses interfaces.

Dans le menu de pfSense, on peut remarquer que chaque interface a un nom qui lui est propre (em0, em1 et em2). Entrez 1 pour configurer les interfaces telles que :

- **em0**, correspondant au réseau interne **lan**, soit la passerelle du LAN (**172.16.0.254/24**).
- **em1** correspondant au réseau **dmz**, soit la passerelle de la DMZ (**172.32.0.254/24).**
- **em2** correspondant au réseau **WAN**, soit la passerelle du WAN (**192.168.1.254/24).**

Vous pouvez ensuite adresser chaque interface en entrant 2. Vous devriez avoir la configuration suivante :

```
*** Welcome to pfSense 2.4.4-RELEASE-p3 (amd64) on pfSense ***

 WAN (wan)       -> em2        -> v4: 192.168.1.254/24
 LAN (lan)       -> em0        -> v4: 172.16.0.254/24
 OPT1 (opt1)     -> em1        -> v4: 172.32.0.254/24
```

Vous pouvez ensuite accéder au configurateur Web via le navigateur de n'importe quel poste du LAN, en entrant l'adresse ip de la passerelle LAN dans la barre de recherche. Il ne vous reste plus qu'à créer les règles suivantes :

Interface WAN						
Protocol	**Source**	**Port**	**Destination**	**Port**	**Action**	**Commentaire**
TCP	*	443	172.32.0.0/24	443	Allow	Accès Web
TCP	*	80	172.32.0.0/24	80	Allow	Accès Web

Interface LAN						
Protocol	**Source**	**Port**	**Destination**	**Port**	**Action**	**Commentaire**
UDP	172.32.0.1/24	88	172.16.0.0/24	88	Allow	Authentification Kerberos
TCP	172.32.0.1/24	135	172.16.0.0/24	135	Allow	Remote Procedure Call
TCP/UDP	172.32.0.1/24	389	172.16.0.0/24	389	Allow	Port LDAP
TCP	172.32.0.1/24	3389	172.16.0.10/24	3389	Allow	RDP

Les règles sont à définir en profondeur dans un environnement de production ; ici nous sommes trop permissifs sur l'interface LAN, mais c'est le strict minimum pour assurer le fonctionnement des services.

La règle suivante peut-être ajoutée sur l'interface LAN, sauf si le groupe souhaite déposer un nom de domaine public. Il faudra alors définir une stratégie obligeant les clients à effectuer leurs requêtes DNS vers les serveurs DNS du groupe :

UDP	*****	**53**	**172.16.0.1/24**	**53**	**Allow**	**Requêtes DNS**

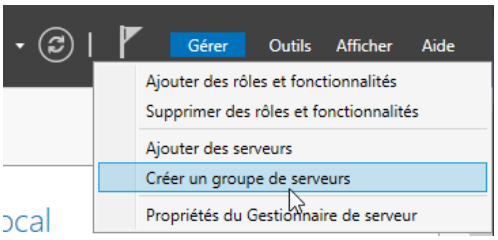
II. Création de la ferme

Dans cette seconde partie, nous verrons comment créer une ferme d'hôtes de session RDS, à l'aide du Broker de session RDS. C'est ce dernier qui va permettre une haute disponibilité des applications mises à disposition. En effet, le rôle du service Broker est d'assurer une tolérance de panne, en permettant un basculement vers un des serveurs de la ferme si un autre tombe en panne (« failover »). De plus, le service Broker effectue une répartition des charges entre les différents hôtes de la ferme (« load balancing »).

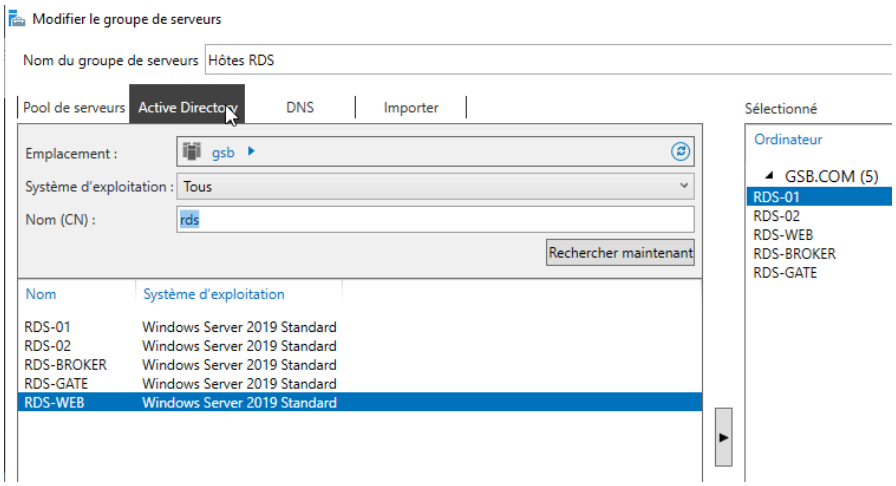
A ce stade : vous devez avoir configuré correctement votre routeur, ainsi que votre DNS et vos comptes AD comme vu en phase de préparation. Vos machines virtuelles doivent ainsi pouvoir communiquer entre elles, et être intégrées au domaine.

1. Création du groupe de serveurs RDS

Ici, nous allons voir comment réunir les serveurs RDS dans un « **pool** » de serveur (fonctionnalité disponible depuis Windows Server 2012, permettant de créer des groupes de serveurs afin de faciliter leur surveillance & administration. A ne pas confondre avec une ferme, puisque qu'un pool ne permet pas de répartition de charge ou de basculement). Nous pourrons ensuite déployer les services nécessaires sur les serveurs du pool plus facilement.



Allumez tous les serveurs. Connectez-vous sur **RDS-BROKER** en tant qu'administrateur local, et rendez-vous dans le gestionnaire de serveurs. Dans le gestionnaire de serveurs, cliquez sur **Gérer > Créer un groupe de serveurs.**



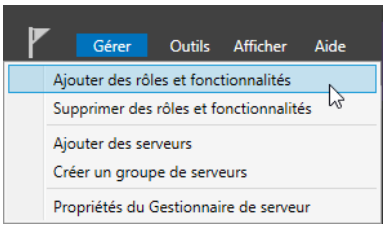
Saisissez un nom (par exemple **Hôtes RDS**). Dans l'onglet Active Directory, recherchez **RDS-01** et ajoutez-le au pool en cliquant sur la flèche. De même pour **RDS-02**, **RDS-BROKER, RDS-GATE** et **RDS-WEB**.

Faites **OK**.

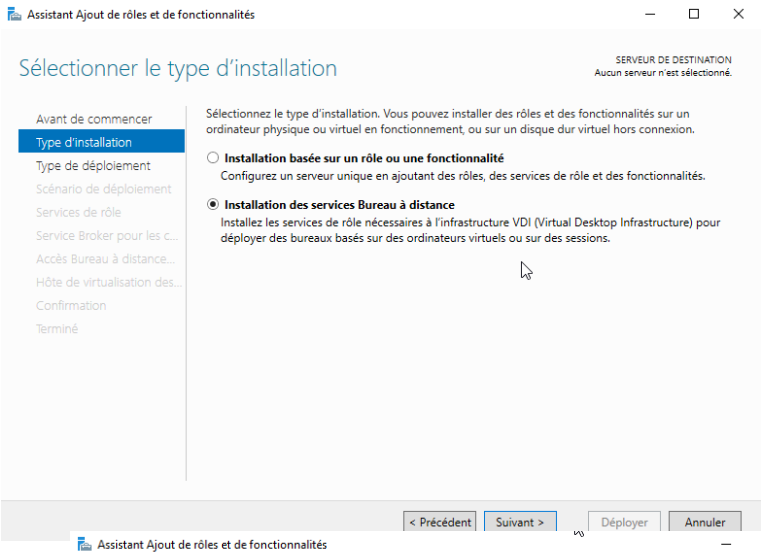
Votre groupe étant créé, vous pouvez désormais déployer les services Bureau à distance sur ses serveurs.

2. Installation des services Bureau à distance

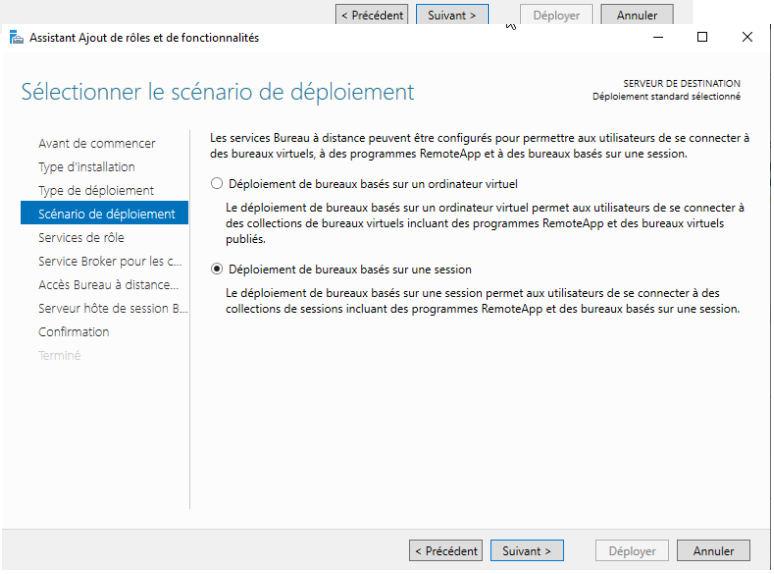
Sur **RDS-BROKER**, rendez-vous dans le gestionnaire de serveurs.



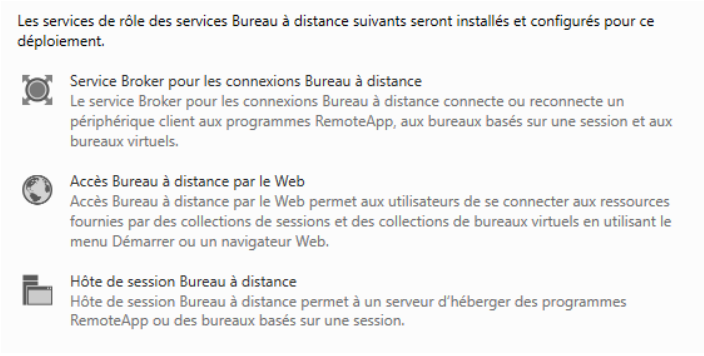
Cliquez sur **Gérer > Ajouter des rôles et fonctionnalités.**



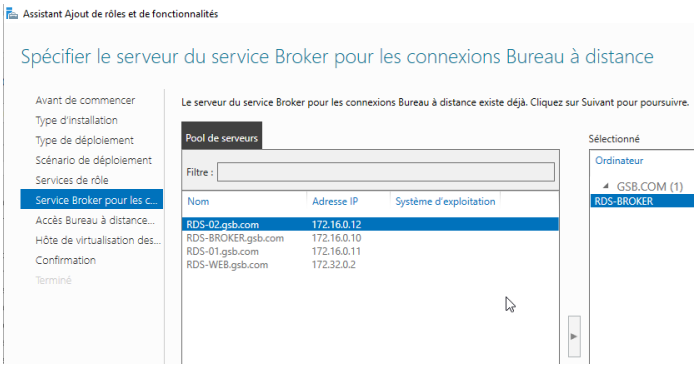
Cochez **Installation des services Bureau à distance.** Faites **Suivant,** puis cochez **Déploiement standard,** puis **Suivant.**



Cochez **Déploiement de bureaux basés sur une session**. Faites **Suivant.**

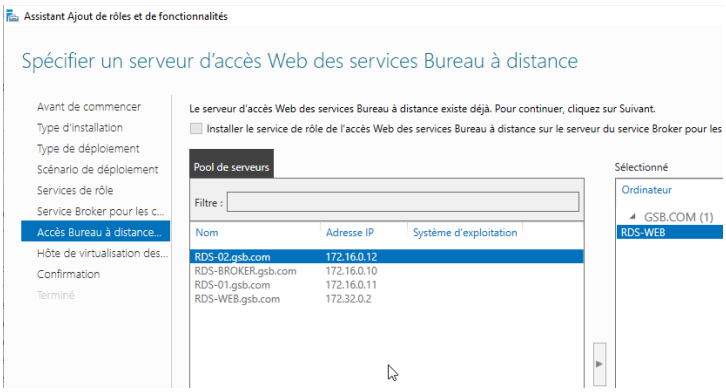


Cette page nous indique que les services Broker (que nous n'utiliserons pas sur ces serveurs), Accès par le Web et Hôte de session seront installés par défaut. Faites **Suivant**.



Ici, il faut spécifier quel serveur jouera le rôle du Broker de session RDS. Ajoutez donc **RDS-BROKER** aux serveurs sélectionnés, en le sélectionnant et en cliquant sur la flèche. Nous le configurerons dans la partie IV.

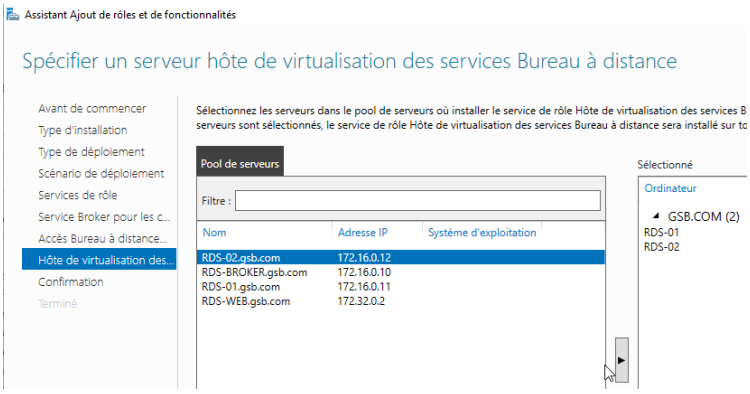
Faites **Suivant**.



Ici, il faut spécifier quel serveur hébergera le portail Web des services Remote Desktop.

Ajoutez **RDS-WEB** aux serveurs sélectionnés, en le sélectionnant et en cliquant sur la flèche.

Faites **Suivant**.



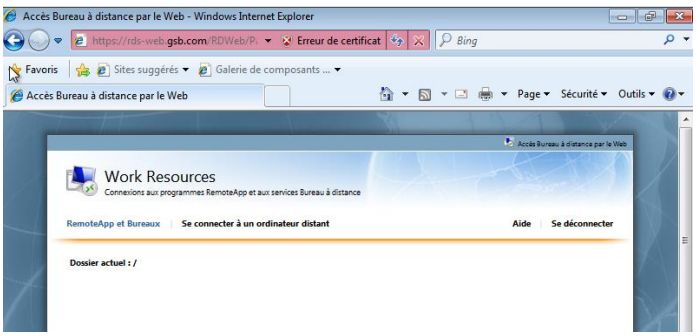
Ici, il faut spécifier quels serveurs seront hôtes de session Remote Desktop.

Ajoutez donc **RDS-01** et **RDS-02** aux serveurs sélectionnés, en les sélectionnant et en cliquant sur la flèche.

Faites **Suivant**.

La dernière page résume les déploiements sur les différents serveurs. **Cochez Redémarrer automatiquement le serveur de destination si nécessaire** et cliquez sur **Déployer**.

Attendez la fin du déploiement. Une fois qu'il s'est terminé succès, vous devriez pouvoir, sans configuration additionnelle, accéder au portail Web depuis le poste client. Sur **TEST-PC**, ouvrez un navigateur et accédez à l'adresse **https://rds-web.gsb.com/rdweb**. Vous aurez une erreur de certificat ; passez outre cette erreur et connectez-vous au portail via le compte **GSB\j.doe**.



La connexion s'établit. L'onglet **RemoteApp et Bureaux** ne devrait pas avoir de contenu ; dans l'onglet **Se connecter à un ordinateur distant**, vous devriez pouvoir vous connecter à **RDS-01** ou **RDS-02**. (si vous n'atteignez pas le portail, vérifiez l'URL, votre configuration réseau, vos enregistrements DNS et vérifiez que vous avez les protocoles TLS et SSL activés dans les paramètres d'Internet Explorer).

La connexion en Remote Desktop sur **RDS-01** s'établit.

Pour tester la ferme, mettez alternativement une des VMs hôtes de session en pause et connectez-vous à **ferme1**. Ouvrez un invité de commande et saisissez la commande **Hostname** pour vérifier que votre session s'est ouverte sur l'hôte toujours disponible.

Vous pouvez éteindre la VM **RDS-GATE**, nous la configurerons plus tard.

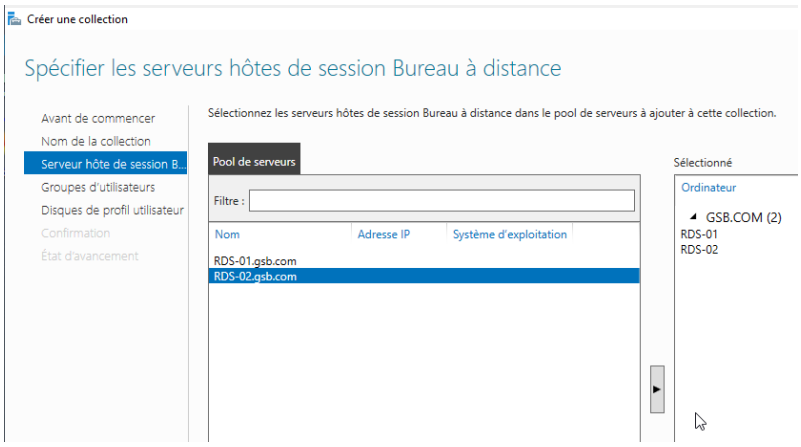
III. Mise à disposition d'applications distantes par portail Web

Dans cette partie, nous allons voir comment mettre à disposition des applications distantes via le portail Web mis en place. Il s'agit principalement de créer des collections, une fonctionnalité permettant de gérer les déploiements via RemoteApp, et leurs comptes/groupes administrateurs associés.

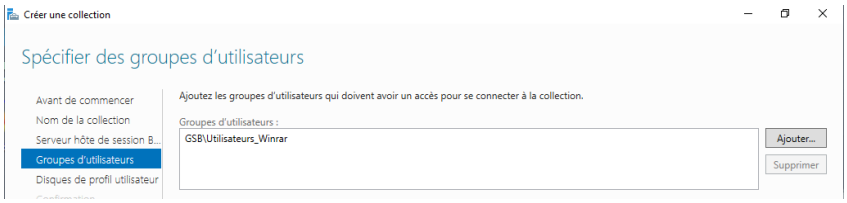
<u>A ce stade :</u> Vos deux hôtes de sessions devraient être accessibles via le portail Web, depuis le poste client.

1. Création d'une collection d'applications RemoteApp

Sur **RDS-BROKER**, dans le gestionnaire de serveur, onglet **Services Bureau à distance > Vue d'ensemble**, cliquez sur **Créer une collection de sessions**.



Nommez votre collection (ici **CollectionTest**), puis choisissez vos serveurs hôtes de session. Il est nécessaire que les serveurs hôtes de session possèdent les mêmes collections. Dans le cas où une collection est absente sur l'un des serveurs, en cas de panne de l'autre, le broker redirigera les requêtes clientes vers celui où la collection est absente. Les applications qu'elle propose seront donc inaccessibles.



Ici, supprimez le groupe par défaut qui est **Utilisateurs du domaine**, et ajoutez le groupe **Utilisateurs_Winrar**.

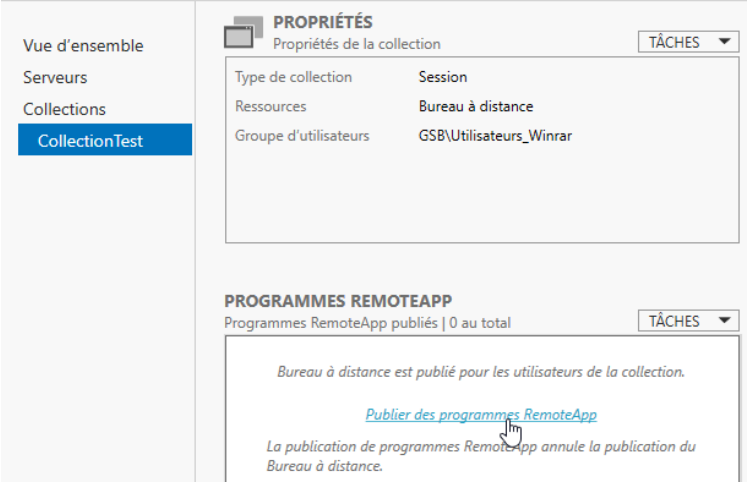
La page suivante vous propose de spécifier les disques de profil utilisateurs, c'est-à-dire des chemins d'accès vers des emplacements où seront stockées les données et paramètres de chaque utilisateur interagissant avec les applications de la collection. Cet emplacement peut être un dossier partagé sur un serveur de stockage, par exemple. Nous n'utiliserons pas cette fonctionnalité dans notre démonstration. Faites **Suivant**, puis **Créer**.

Attendez la fin de la création de la collection. Une fois fait, nous allons pouvoir commencer à distribuer l'application **Winrar**.

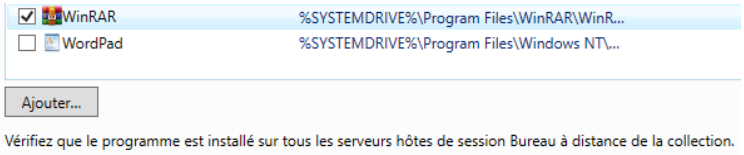
2. Publication de programmes RemoteApp

Tout d'abord, installez **Winrar** sur les hôtes de session RDS. Même chose qu'avec les collections : si Winrar est manquant sur l'un des hôtes, il sera inutilisable si l'autre hôte tombe en panne. Veilliez donc bien à installer l'application que vous souhaitez déployer sur tous vous hôtes de session.

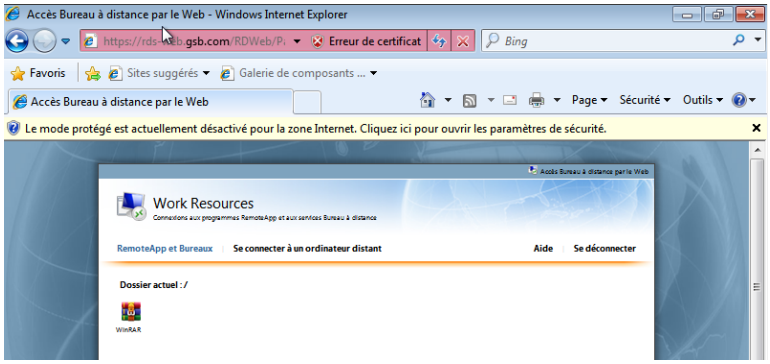
Retournez ensuite dans le gestionnaire de serveur sur **RDS-01**.



Dans **CollectionTest**, que nous venons de créer, cliquez sur **Publier des programmes RemoteApp**.



Sélectionnez l'application **Winrar**. Faites **Suivant** puis **Publier**.



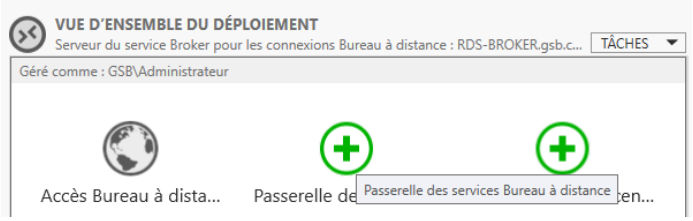
A présent, vous pouvez retourner sur **TEST-PC** et vous connecter au portail Web, et vérifier la présence de l'application **Winrar**. Lorsque vous l'exécutez, un avertissement apparaît ; confirmez.

Winrar se lance sur l'un des hôtes RDS, et son affichage est déporté vers le poste client.

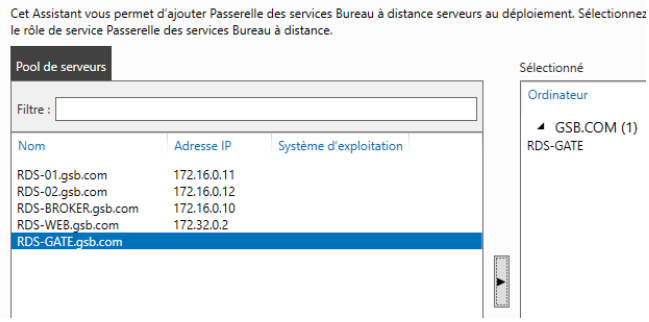
IV. Mise en place de la passerelle

Dans cette troisième partie, nous verrons comment mettre en place une Passerelle des services RDS. Le rôle d'une telle passerelle (ou « gateway ») est de sécuriser l'accès aux applications distantes mises à disposition. La gateway permet d'encapsuler le trafic Remote Desktop Protocole dans le protocole HTTPS, de manière transparente pour l'utilisateur. Ainsi, les échanges sont chiffrés asymétriquement via le protocole HTTPS ; de plus, ce protocole étant généralement autorisé par les pares-feux, cela permet le passage des flux RDP vers l'extérieur d'un réseau privé. C'est donc ce qui permettra aux utilisateurs d'accéder à leurs applications distantes, depuis Internet par exemple. C'est pourquoi la passerelle RDS est à mettre en place dans une DMZ.

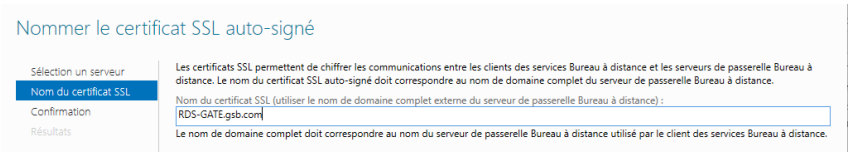
1. Installation



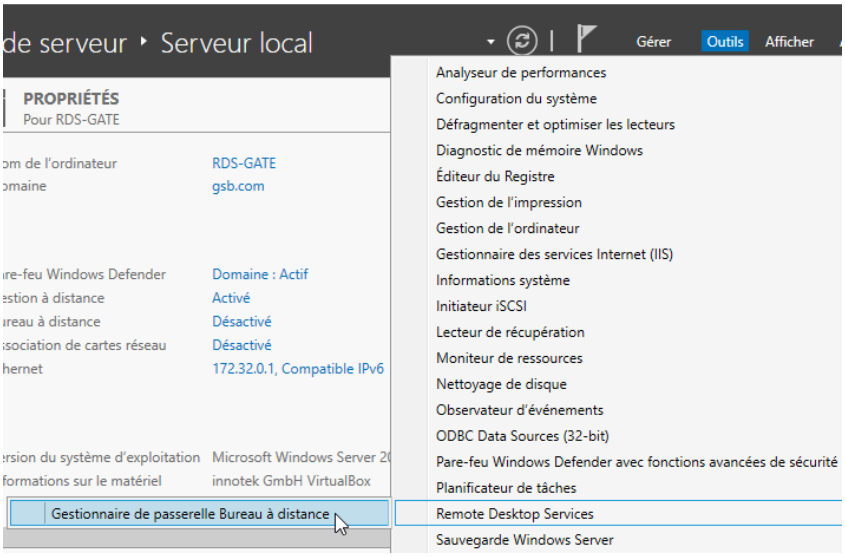
Allez sur **RDS-BROKER**, dans le gestionnaire de serveur, onglet **Services Bureau à distance > Vue d'ensemble**. Dans le champ **Vue d'ensemble du déploiement**, cliquez sur **Passerelle des services Bureau à distance**.



Ajoutez **RDS-GATE** aux serveurs sélectionnés.

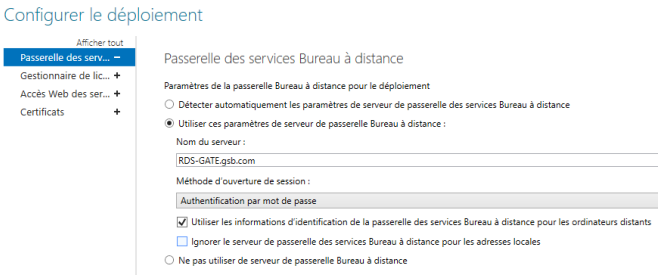


Entrez un nom pour le certificat autosigné SSL en précisant le domaine (**RDS-GATE.gsb.com**). Faites **Suivant** et attendez la fin du déploiement du service.



Rendez-vous ensuite sur **RDS-GATE**, et dans le gestionnaire de serveurs, allez dans **Outils > Remote Desktop Services > Gestionnaire de passerelle Bureau à distance**.

<u>Optionnel :</u> nous allons ici décocher une option, ce qui forcera les clients présents sur le réseau LAN à passer par la passerelle lors du lancement d'une application distante. Sur **RDS-BROKER**, dans le gestionnaire de serveur, onglet **Services Bureau à distance > Vue d'ensemble**, cliquez sur **Tâches > Modifier les propriétés de déploiement**.



Dans l'onglet Passerelle des services RDS, décochez **Ignorer le serveur de passerelle des services Bureau à distance pour les adresses locales**.

Avant de tester si la passerelle fonctionne correctement et avancer dans la documentation, vous devrez importer le certificat SSL créé lors de l'installation dans les certificats d'autorité racine sur TEST-PC. Pour plus de détails sur comment déployer un certificat, passez directement à la partie V avant de continuer.

2. Stratégies

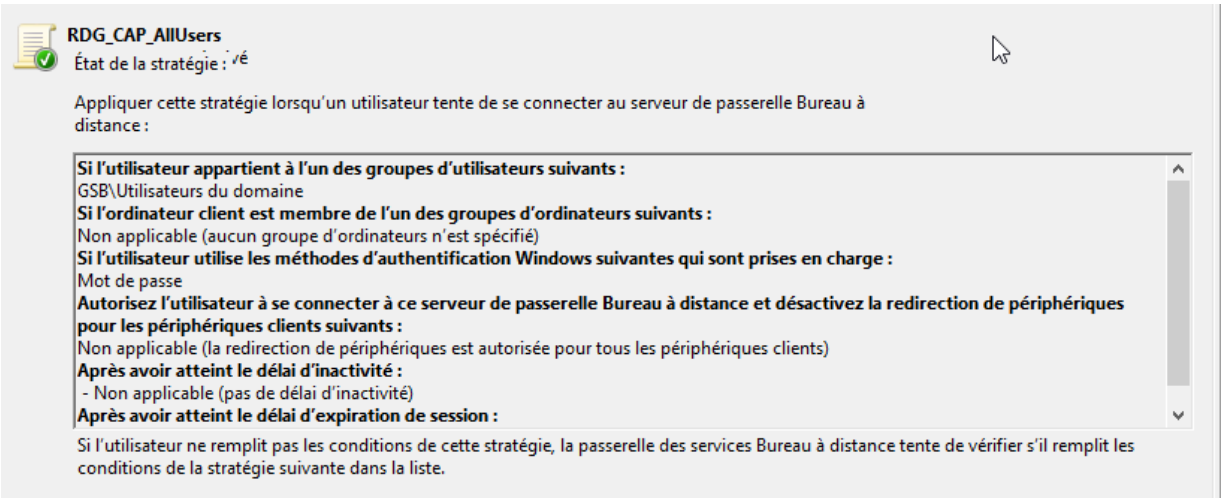
Les stratégies d'autorisation sont des paramètres à définir sur la passerelle. Elles permettent le filtrage des connexions à celle-ci, ainsi que des connexions aux ressources RDS de l'entreprise.

Sur **RDS-GATE**, rendez-vous dans le gestionnaire de serveurs, puis cliquez sur **Outils > Remote Desktop Services > Gestionnaire de passerelle des services Bureau à distance**.

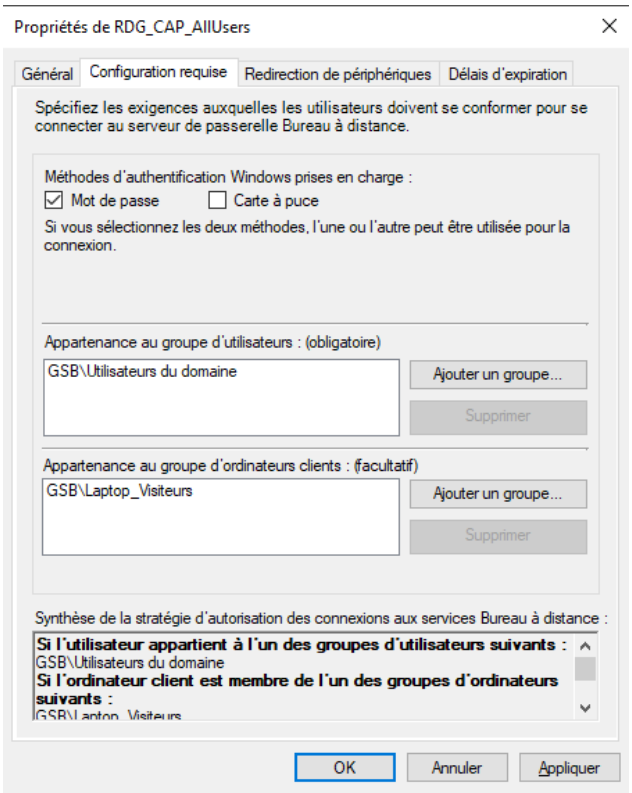
Vous verrez qu'il existe déjà des stratégies par défaut des deux types. Ces stratégies sont trop permissives. Nous allons donc définir nos propres stratégies, afin d'autoriser les utilisateurs du domaine ainsi que les utilisateurs du groupe **Utilisateurs_RDS** à se connecter à la passerelle, ainsi qu'aux serveurs RDS.

Stratégies d'autorisation des connexions

Cliquez sur Stratégies d'autorisation des connexions. Il existera la stratégie par défaut **RDG_CAP_AllUsers**. Cliquez dessus et lisez son résumé :

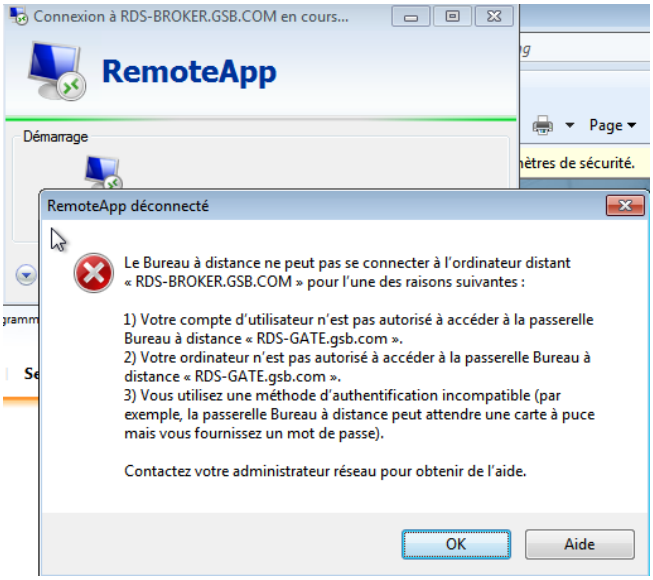


Le deuxième paramètre n'est pas précisé, ce qui signifie que n'importe quel ordinateur est autorisé à accéder à la passerelle. Ce point est important dans notre contexte, puisque les postes nomades mis à disposition aux visiteurs médicaux doivent être ajoutés au domaine. Nous pouvons donc limiter l'accès à la passerelle à ces postes-là. Cela évitera les connexions depuis un poste inconnu. Sur **DC1**, créez un groupe d'ordinateurs (par exemple **Laptop_visiteurs**) mais n'y ajoutez pas encore **TEST-PC**.



De retour sur **RDS-GATE**, faites clic-droit **> Propriétés** sur la stratégie **RDG_CAP_AllUsers** et allez dans l'onglet **Configuration requise**. Ajoutez le groupe AD précédemment créé.

Appliquez.

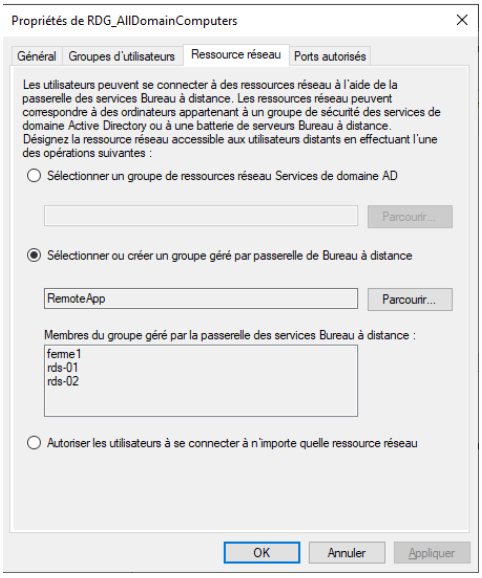


Sur votre poste de test, ouvrez l'application **Winrar** à partir du portail Web. A l'authentification, vous aurez cette erreur. C'est notre stratégie d'autorisation de connexion à la passerelle qui nous empêche d'accéder à l'application.

Ajoutez votre poste de test au groupe AD **Laptop_visiteurs** et votre connexion refonctionnera. Vous pouvez également explorer les autres options proposées, comme les périphériques clients pris en charge lors de la connexion RDS, ou le délai d'inactivité avant déconnexion des services.

Stratégies d'autorisation d'accès aux ressources

Dans les stratégies d'autorisation d'accès aux ressources, deux stratégies existent par défaut. La première autorise les utilisateurs du domaine à accéder à tous les postes du domaine en RDS. La seconde autorise également la connexion en RDS au Broker de session. Il faut donc modifier ces stratégies. Pour la première, remplacez **Utilisateurs du domaine** par **Utilisateurs_RDS**.



Ensuite, dans l'onglet **Ressource réseau,** cochez **Sélectionner ou créer un groupé géré par la passerelle de Bureau à distance.** Créez un groupe (par ex : **RemoteApp**) et ajoutez-y bien **ferme1**, **RDS-01** et **RDS-02**.

Faites **OK**.

Pour ce qui est de la seconde stratégie par défaut, vous pouvez vous contenter de remplacer Utilisateurs du domaine par un groupe AD spécialement définit pour accéder à RDS-Broker en RDS (ici, **RDS_Admins**).

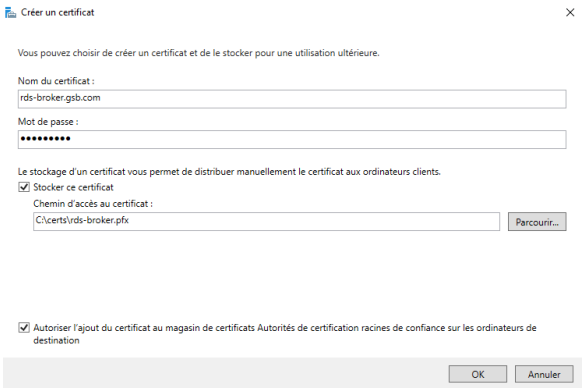
Vous avez mis en place des stratégies restreignant l'accès aux serveurs RDS. Dans un environnement de production, ces stratégies sont à définir plus en profondeur si besoin.

V. Déploiement de certificats autosignés

Dans cette partie, nous verrons comment créer/exporter des certificats autosignés pour chacun de nos serveurs. Cela permettra aux clients d'assurer la bonne connexion aux serveurs du groupe GSB, et ainsi éviter la falsification de ses services. Il s'agit donc d'une mesure de sécurité, mais les certificats sont également utiles pour fluidifier l'accès à ces services (éviter les messages d'avertissements).

1. Création des certificats

Sur **RDS-BROKER**, dans le gestionnaire de serveur, onglet **Services Bureau à distance > Vue d'ensemble**, cliquez sur **Tâches > Modifier les propriétés de déploiement**. Dans l'onglet **Certificats**, pour chaque serveur, faites **Créer un certificat**. (Vous pouvez aussi importer le certificat SSL créé précédemment à l'installation de la passerelle).

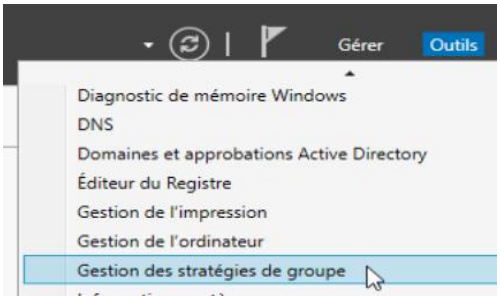


Nommez le certificat avec le FQDN du serveur, renseignez un mot de passe administrateur, cochez **Stocker ce certificat** et définissez un chemin d'accès où le stocker. Cochez la dernière case.

Faites **OK**.

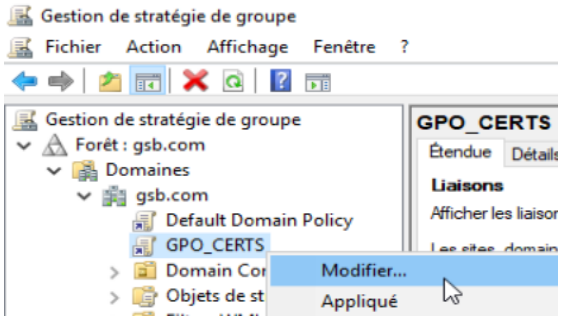
2. Déploiement des certificats par stratégie de groupe

Pour déployer ces certificats sur nos postes clients, nous utiliserons les stratégies de groupe (ou GPO). Ces dernières sont des paramètres à définir sur le contrôleur de domaine, qui s'appliqueront à des groupes de postes ou d'utilisateurs définis. Elles permettent également la distribution de scripts d'ouverture de session, ou de certificats. Dans un environnement de production, la méthode de distribution des certificats reste à définir ; en effet les GPO ont comme limite leur portée, c'est-à-dire qu'elles ne peuvent s'appliquer à un poste qui ne communique pas avec le contrôleur de domaine.

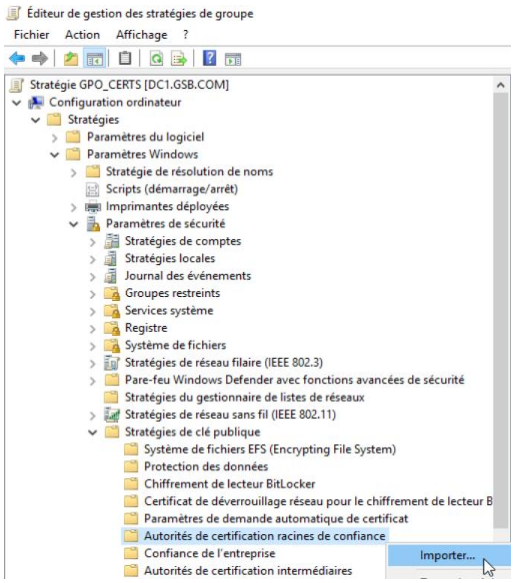


Sur **DC1**, ouvrez le gestionnaire de serveur et cliquez sur **Outils > Gestion des stratégies de groupe**.

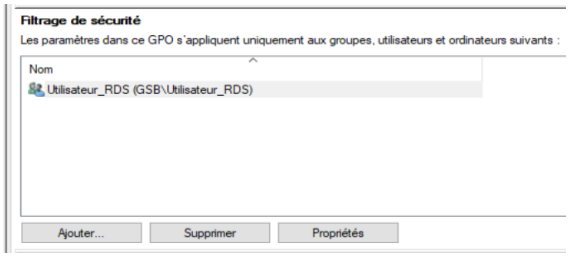
Développez **Forêt : gsb.com > Domaines** et faites clic-droit sur **gsb.com > Créer un objet GPO dans ce domaine, et le lier ici**. Nommez votre GPO (ici **GPO_CERTS**).



Faites clic-droit sur **GPO_CERTS > Modifier**.

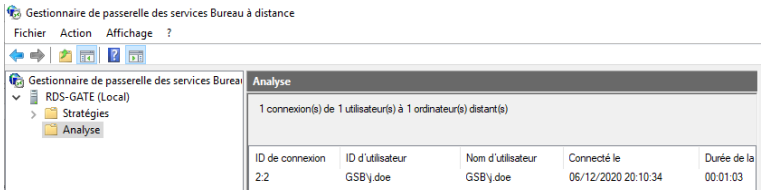


Développez **Configuration Ordinateur > Paramètres Windows > Paramètres de sécurité > Stratégies de clé publique** et faites clic-droit sur **Autorités de certification racines de confiance > Importer.** Dans la fenêtre qui s'ouvre, faites **Suivant**, renseignez le répertoire partagé où se situent les certificats, puis faites **Suivant** et **Terminer**. Répétez pour tous les certificats à importer.



De retour dans le gestionnaire de stratégie de groupe, dans l'onglet **Etendue** de **GPO_CERTS**, champ **Filtrage de sécurité**, ajoutez le groupe **Utilisateurs_RDS**. Ainsi, cette GPO sera appliquée uniquement aux membres de ce groupe.

Une fois fait, sur le poste client, ouvrez un invité de commande en administrateur et entrez la commande **gpupdate /force.** Redémarrez le poste. Vous retrouverez vos certificats dans les autorités de certifications racines de confiance, dans une console MMC.



Désormais, si vous accédez à l'application **Winrar** depuis le portail Web, votre compte apparaîtra dans le champ **Analyse** du gestionnaire de passerelle des services RDS, sur **RDS-GATE**.