

ASSURMER

Installation et configuration du service RDS

PROCEDURE

Date de création : 27/09/2023

Version : 5.0

Pour validation : DSI

A destination : DSI

Mode de diffusion : Intranet

Nombre de pages : 58

Auteur : Dylan CHAU

Métadonnées

Diffusion			
Périmètre de diffusion	Contrôlé	Interne	Libre

Historique des évolutions		
Auteur	Version	Objet de la version et liste des modifications
Dylan Chau	1.0	Initialisation du document
Dylan Chau	5.0	Mise à jour

Validation			
Rédacteur		Valideur	
Nom	Date	Nom	Date
Dylan Chau	27/09/2023	DSI	27/09/2023
Date d'application : 27/09/2023			

Sommaire

Métadonnées	2
Prérequis	5
I. Préparation de l'environnement	Erreur ! Signet non défini.
1. Préparation d'une machine	Erreur ! Signet non défini.
2. Création d'une unité d'organisation pour les serveurs hôtes de session de bureau à distance	Erreur ! Signet non défini.

3. Création du dossier pour les disques de profils utilisateurs – UPD (User Profile Disks).....	Erreur ! Signet non défini.
4. Création d'un pointeur DNS.....	Erreur ! Signet non défini.
5. Ajout des serveurs dans la console du gestionnaire du serveur.....	Erreur ! Signet non défini.
6. Création d'un groupe de serveurs.....	Erreur ! Signet non défini.
II. Installation des rôles sur les différents serveurs.....	Erreur ! Signet non défini.
III. Création d'une collection de sessions.....	Erreur ! Signet non défini.
IV. Publication des RemoteApp pour les utilisateurs.....	Erreur ! Signet non défini.
a. Distribution des RemoteApp par métier.....	Erreur ! Signet non défini.
V. Installation de la passerelle des services Bureau à distance.....	6
1. Ajout du serveur.....	6
2. Configuration du déploiement.....	7
a) Ajout du certificat auto-signé.....	7
b) Configuration de la « passerelle des services Bureau à distance ».....	9
3. Configuration de la passerelle.....	10
a) Ajout du certificat.....	10
b) Présentation des stratégies par défaut.....	12
c) Configuration de la stratégie.....	12
d) Création d'une stratégie pour les administrateurs.....	14
VI. Gestionnaire de licences des services Bureau à distance.....	Erreur ! Signet non défini.
1. Ajout du serveur.....	Erreur ! Signet non défini.
2. Configuration du déploiement.....	Erreur ! Signet non défini.
3. Ajout des licences.....	Erreur ! Signet non défini.
VII. Personnalisation de l'environnement RDS.....	Erreur ! Signet non défini.
1. Authentification unique (SSO).....	Erreur ! Signet non défini.
2. Raccourcis WEB et RDP.....	Erreur ! Signet non défini.
a) Configuration du raccourci.....	Erreur ! Signet non défini.
b) Configuration du fichier rdp pour les sessions distantes (Raccourci GPO).....	Erreur ! Signet non défini.
3. GPO pour les certificats Broker et Passerelle.....	Erreur ! Signet non défini.
a) Exportation du certificat.....	Erreur ! Signet non défini.
b) Création de la GPO.....	Erreur ! Signet non défini.
4. Page Web personnalisée Assurmer.....	Erreur ! Signet non défini.
a) Changement du texte « Work Resources ».....	Erreur ! Signet non défini.

- b) Ajout d'une redirection automatique vers RDWeb..... **Erreur ! Signet non défini.**
 - c) Ajout de la réinitialisation de mot de passe depuis le portail..... **Erreur ! Signet non défini.**
 - d) Modification des fichiers de la page **Erreur ! Signet non défini.**
- VIII. Axes d'améliorations **Erreur ! Signet non défini.**

Prérequis

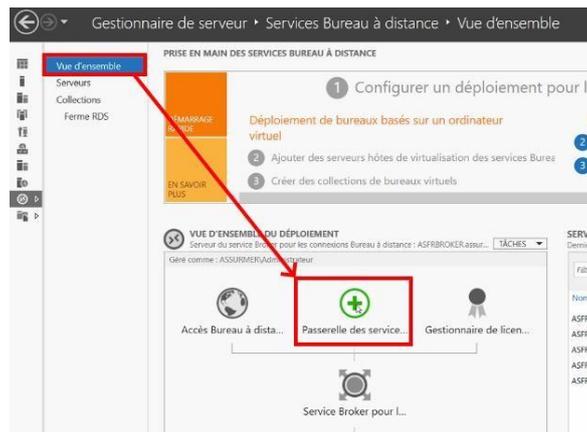
- 4 machines virtuelles Windows Server
- Un ISO Windows Server
- Un serveur Proxmox VE dans la DMZ
- Un NetGate PfSense

V. Installation de la passerelle des services Bureau à distance

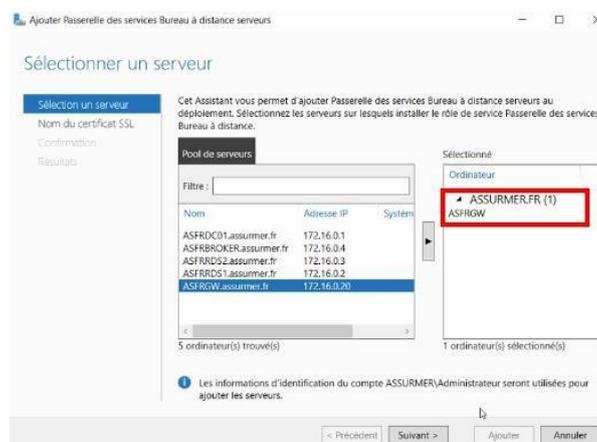
La passerelle de Bureau à distance offre la possibilité d'accéder à des ressources, tels que des serveurs ou des ordinateurs, depuis l'extérieur de l'entreprise via le port 443 (utilisé pour HTTPS). Cette connexion s'effectue sans nécessité d'établir un réseau privé virtuel (VPN) tout en mettant en place des mesures de sécurité spécifiques pour garantir la protection des données et des systèmes.

1. Ajout du serveur

- Dans « Vue d'ensemble », cliquer sur l'icône verte « Passerelle des service... ».



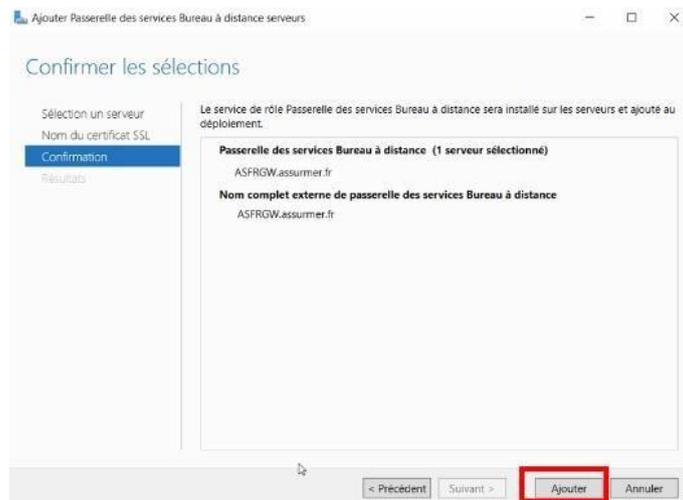
- Sélectionner le serveur ASFRGW qui sera le serveur de passerelle des services Bureau à distance du déploiement. Puis cliquer sur « Suivant ».



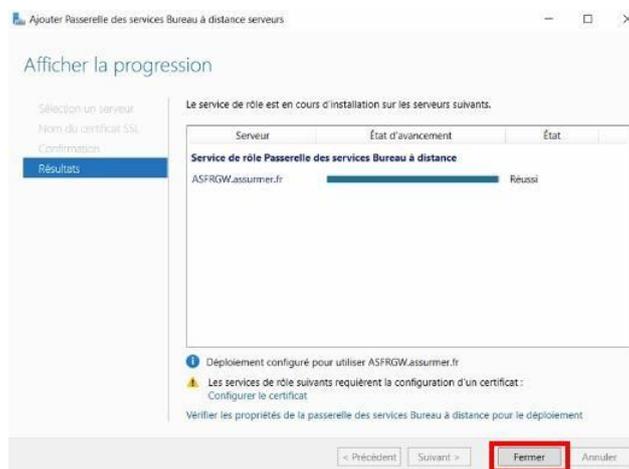
- Ajouter le nom du certificat SSL qui permettra le chiffrement entre les postes clients et la passerelle. Puis cliquer sur « Suivant ». Ce certificat sera importé sur les PC utilisateurs via une GPO.



- Cliquer sur « Ajouter » pour lancer l'installation.



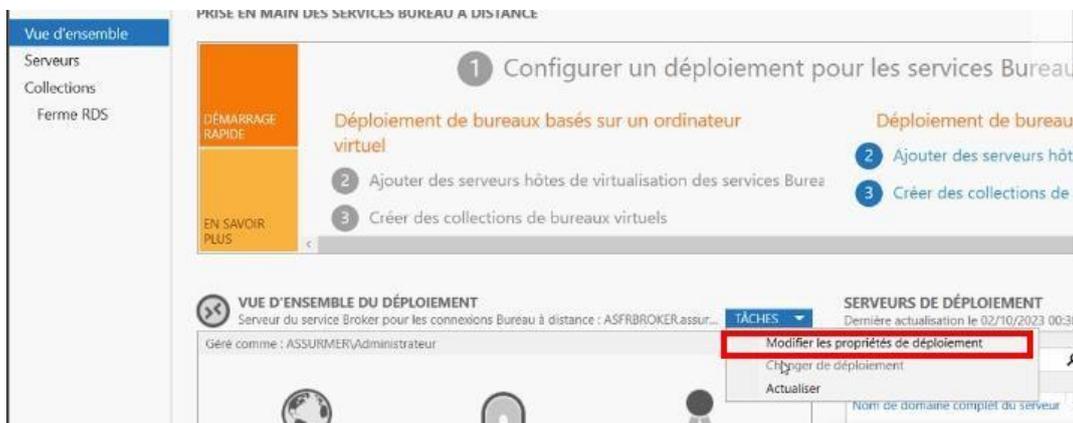
- Patienter puis cliquer sur « Fermer ».



2. Configuration du déploiement

a) Ajout du certificat auto-signé

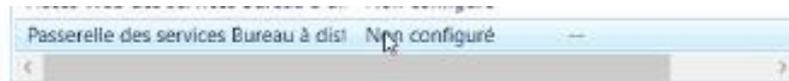
- Dans « Vue d'ensemble », puis « Vue d'ensemble du déploiement », cliquer sur « Tâches » puis « Modifier les propriétés de déploiement ».



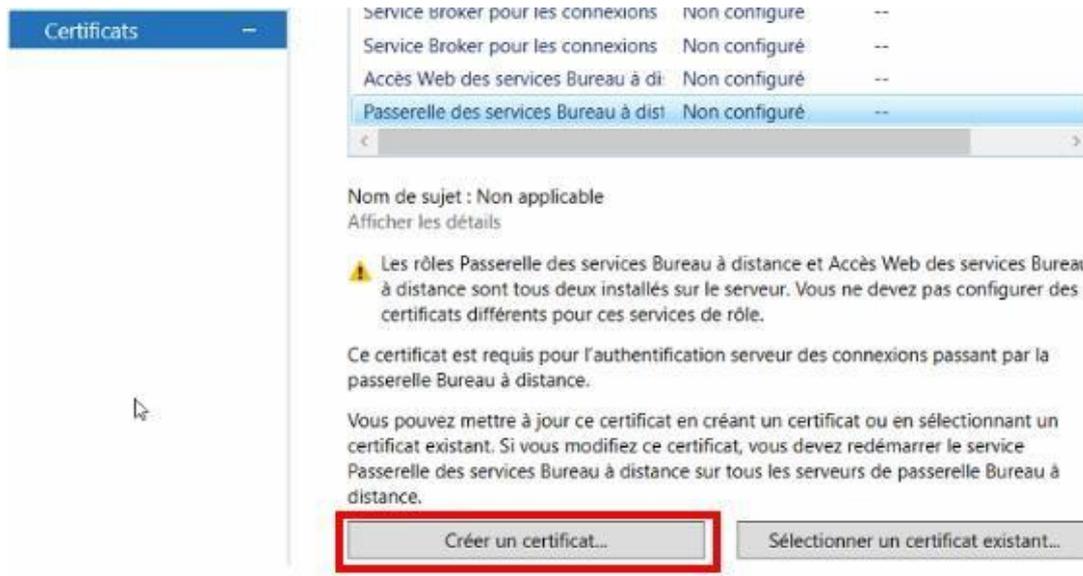
- Cliquer sur « Certificats ».



- Cliquer sur « Passerelle des services Bureau à distance ».

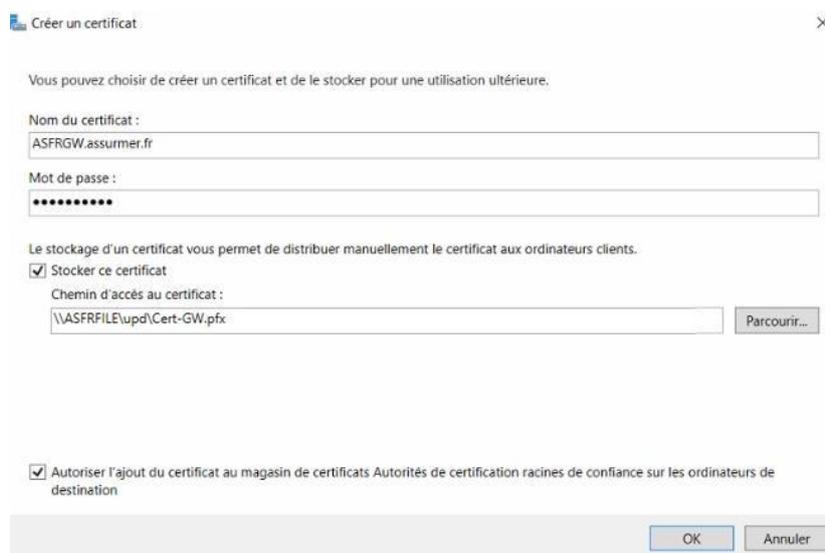


- Cliquer ensuite sur « Créer un certificat ».



- Ajouter au certificat :

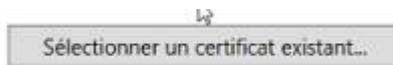
- o Un nom
- o Un mot de passe
- o L'emplacement de stockage qui sera sur ASFRFILE
- o Cocher la case pour l'ajouter sur les ordinateurs de destination.



- Cliquer sur « OK ».
- Cliquer sur « Accès Web des services Bureau à distance ».

Accès Web des services Bureau à di: Non configuré --

- Cliquer ensuite sur « Sélectionner un certificat existant ».



- Ajouter le chemin du certificat précédemment créé, son mot de passe et cocher la case pour l'ajout sur l'ordinateur de destination.

Choisir un autre certificat

Chemin d'accès au certificat :

Mot de passe :

Autoriser l'ajout du certificat au magasin de certificats Autorités de certification racines de confiance sur les ordinateurs de destination

- Répéter l'opération pour créer un second certificat sur ASFRFILE pour les services BROKER et l'ajouter sur les services Broker pour les connexions.

Le niveau de certification actuel du déploiement est **Non approuvé**
Qu'est-ce qu'un niveau de certification ?

Service de rôle	Niveau	État	État
Service Broker pour les connexions	Non approuvé	OK	
Service Broker pour les connexions	Non approuvé	OK	
Accès Web des services Bureau à di	Non approuvé	OK	
Passerelle des services Bureau à dist	Non approuvé	OK	

b) Configuration de la « passerelle des services Bureau à distance »

- Sur l'onglet « Passerelle des services Bureau à distance », ajouter le nom du serveur en dessous de « Utiliser ces paramètres de serveur de passerelle Bureau à distance » et décocher la case « Ignorer le serveur pour les adresses locales ».

Propriétés de déploiement

Configurer le déploiement

Afficher tout

- Passerelle des serv... -
- Gestionnaire de lic... +
- Accès Web des ser... +
- Certificats +

Passerelle des services Bureau à distance

Paramètres de la passerelle Bureau à distance pour le déploiement

Détecter automatiquement les paramètres de serveur de passerelle des services Bureau

Utiliser ces paramètres de serveur de passerelle Bureau à distance :

Nom du serveur :

Méthode d'ouverture de session :

Utiliser les informations d'identification de la passerelle des services Bureau à distance pour les ordinateurs distants

Ignorer le serveur de passerelle des services Bureau à distance pour les adresses locales

Ne pas utiliser de serveur de passerelle Bureau à distance

3. Configuration de la passerelle

Pour fonctionner la passerelle de bureau à distance utilise 2 types de stratégies :

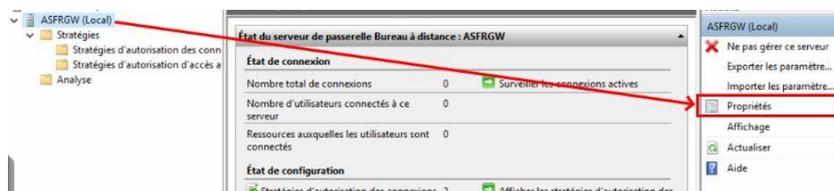
- Stratégies d'autorisation des connexions : elles définissent qui peut se connecter à la passerelle (utilisateurs et postes), quels périphériques sont redirigés et le délai d'expiration des sessions.
- Stratégies d'autorisation d'accès aux ressources : elles définissent qui peut se connecter à quoi.

a) Ajout du certificat

- Sur le serveur Proxmox, se connecter sur ASFRGW.
- Cliquer sur « Outils » puis « Remote Desktop Services » et accéder au gestionnaire.



- Lors de l'installation du rôle, l'assistant crée automatiquement 2 stratégies rendant la passerelle utilisable. Nous allons ici créer des stratégies supplémentaires. - Cliquer sur « Propriétés » à droite.



- Sur « Certificat SSL », cliquer sur « Importer un certificat ».

Magasin de stratégies d'autorisation des connexions aux services Bureau à distance			
Batterie de serveurs	Audit	Pontage SSL	Messages
Général	Certificat SSL	Paramètres de transport	

Pour sécuriser les communications des écouteurs HTTPS/UDP et la messagerie NAP, un certificat est nécessaire. Le certificat est lié automatiquement aux ports HTTP et UDP configurés.

 Le certificat suivant est installé sur ASFRGW

Déjà à : ASFRGW.assumer.fr
Déjà par : ASFRGW.assumer.fr
Date d'expiration : 11/04/2024

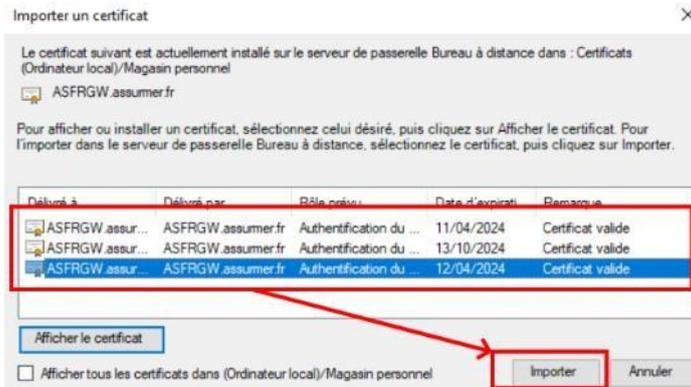
Spécifiez le type de certificat SSL à importer pour le serveur de passerelle des services Bureau à distance en effectuant l'une des opérations suivantes :

Créer un certificat auto-signé Créer et importer un certificat...

Sélectionner un certificat existant à partir de la passerelle Bureau à distance ASFRGW Certificats (Ordinateur local)/Magasin personnel Importer un certificat...

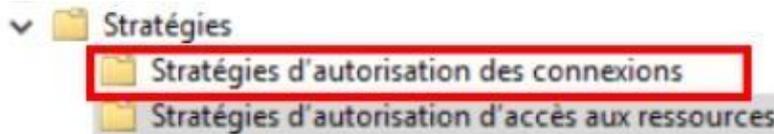
Importer un certificat dans la passerelle Bureau à distance ASFRGW Certificats (Ordinateur local)/Magasin personnel Parcourir et importer un...

Sélectionner les certificats, puis les importer un par un.



b) Présentation des stratégies par défaut

- Cliquer sur « Stratégies » puis « Stratégies d'autorisation des connexions ».

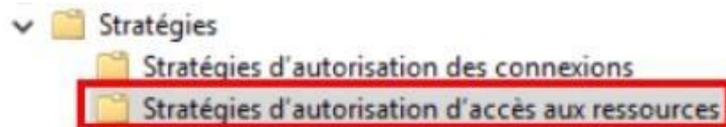


- Cliquer sur la stratégie « RDG_CAP_AllUsers ».



Il est possible d'activer cette stratégie, de choisir les groupes autorisés et la méthode d'authentification, la redirection des périphériques et les délais d'expiration. Nous allons laisser les paramètres par défaut qui correspondent aux besoins de l'entreprise.

- Cliquer sur « Stratégies » puis « Stratégies d'autorisation d'accès aux ressources ».



- Cliquer sur la stratégie « RDG_AllDomainComputers ».



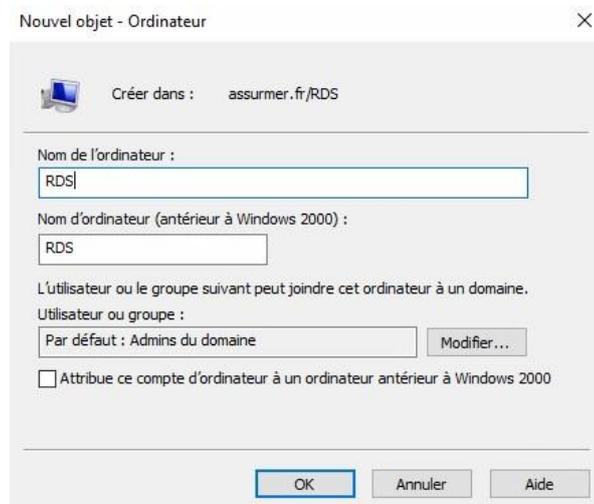
Il est possible d'activer cette stratégie, de choisir les groupes autorisés, les ressources réseaux autorisées (qui seront les éléments de la ferme RDS) et les ports autorisés.

c) Configuration de la stratégie

- L'utilisation d'un alias DNS (qui a été créé au début de la procédure) pour les serveurs hôtes empêche la connexion à la ferme RDS du fait que l'ordinateur RDS (objet AD) n'existe pas.
- Sur l'OU RDS dans ASFRDC01, créer un nouvel ordinateur.



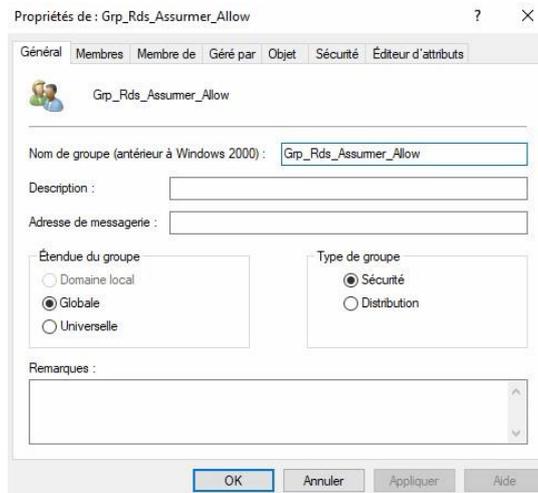
Entrer le nom « RDS » qui correspond à l'alias.



- L'ordinateur appartient donc au groupe « Ordinateurs du domaine » et il fonctionne avec la règle RDS par défaut.

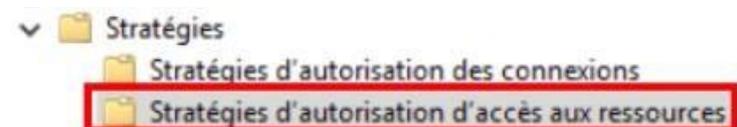
Ordinateurs du domaine assumer.fr/Users

- Créer un groupe de sécurité « Grp_Rds_Assumer_Allow » et ajouter les ordinateurs de la ferme RDS dedans.

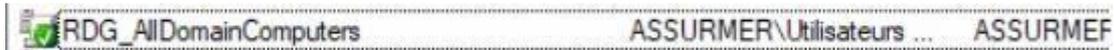


Nom	Dossier Services de domaine Active Directory
ASFRBROKER	assumer.fr/ASCOMPUTERS
ASFRRDS01	assumer.fr/RDS
ASFRRDS02	assumer.fr/RDS
RDS	assumer.fr/RDS

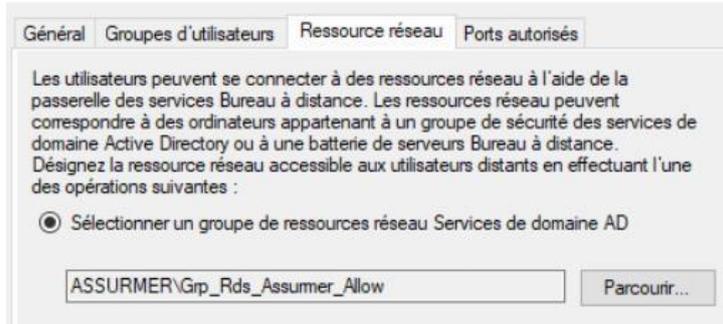
- Cliquer sur « Stratégies » puis « Stratégies d'autorisation d'accès aux ressources ».



Cliquer sur la stratégie « RDG_AllDomainComputers ».



Dans « Ressources réseau », sélectionner le groupe de sécurité.

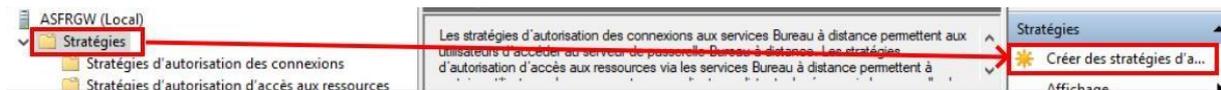


La stratégie permettra de limiter l'accès des utilisateurs uniquement aux ordinateurs de la ferme RDS. Il est aussi possible de créer des groupes gérés par la passerelle.

d) Création d'une stratégie pour les administrateurs

La stratégie permettra aux administrateurs d'accéder à toutes les ressources.

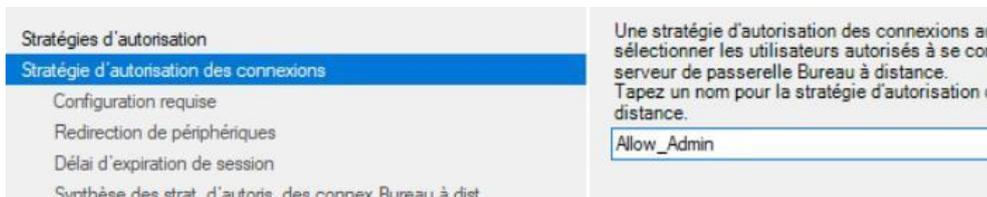
Sur le dossier « Stratégies », cliquer sur « Créer des stratégies d'autorisation ».



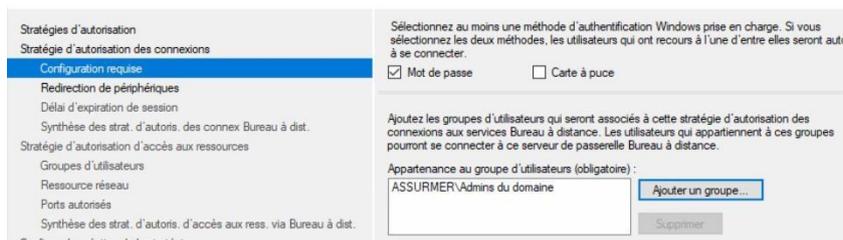
Sélectionner la première option puis « Suivant ».



Choisir un nom.



Ajouter le groupe « Admins du domaine ».



Laisser la redirection des périphériques par défaut.

Laisser le délai par défaut.

Un résumé s'affiche. Cliquer sur « Suivant ». Nous allons maintenant passer à la création de la stratégie d'accès aux ressources.

Ajouter un nom.



Créer une stratégie d'autorisation d'accès aux ressources via les services Bureau à distance

Le groupe d'appartenance est déjà défini.

Sur l'onglet « Ressource réseau », cocher « Autoriser les utilisateurs à se connecter à n'importe quelle ressource réseau ».

Laisser les ports par défaut.



Sélectionner les ports autorisés

<p>Stratégies d'autorisation</p> <p>Stratégie d'autorisation des connexions</p> <p>Configuration requise</p> <p>Redirection de périphériques</p> <p>Délai d'expiration de session</p> <p>Synthèse des strat. d'autoris. des connex Bureau à dist.</p> <p>Stratégie d'autorisation d'accès aux ressources</p> <p>Groupes d'utilisateurs</p> <p>Ressource réseau</p> <p>Ports autorisés</p> <p>Synthèse des strat. d'autoris. d'accès aux ress. via Bureau à dist.</p>	<p>Par défaut, les clients Bureau à distance se connectent à distance aux ressources réseau via le port TCP 3389, utilisé pour les connexions RDP. Spécifiez si le port TCP 3389 ou un autre port doit être utilisé.</p> <p><input checked="" type="radio"/> Autoriser uniquement les connexions au port TCP 3389</p> <p><input type="radio"/> Autoriser les connexions à ces ports : <input type="text"/></p> <p>Pour spécifier plusieurs ports, tapez le numéro de chaque port séparé par un point-virgule (par exemple : 3389;3390)</p>
---	--

- Un résumé s'affiche, cliquer sur « Terminer » puis « Fermer ». - La configuration de la passerelle est terminée.

