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

Diff ısion			
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		Validateur	
Nom	Date	Nom	Date
Dylan Chau	27/09/2023	DSI	27/09/2023
Date d'application : 27/09/2023			

Sommaire

Prérequis

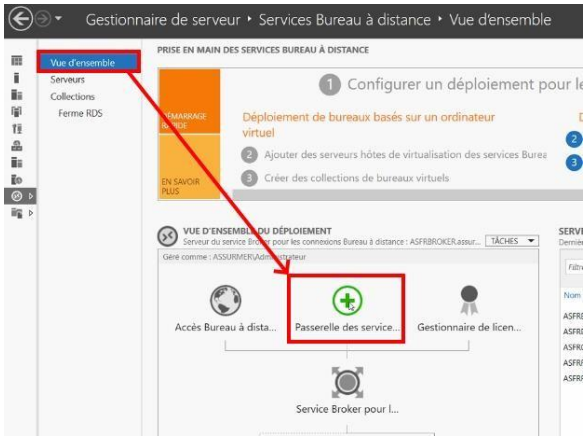
- 4 machines virtuelles Windows Server
- Un ISO Windows Server
- Un serveur Proxmox VE dans la DMZ
- Un NetGate PfSense

V. Installation de la passerelle des services Bureau à distance

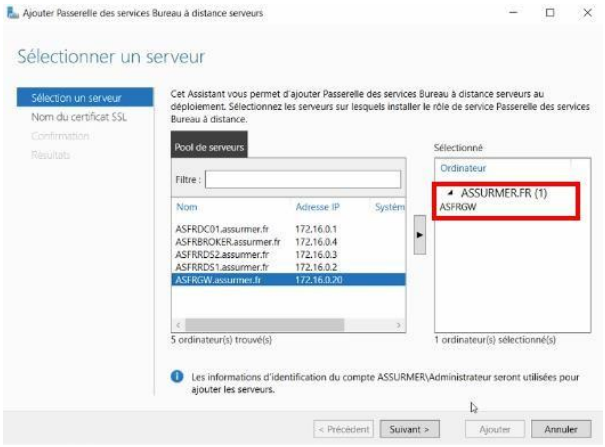
La passerelle de Bureau à distance offre la possibilité d'accéder à des ressources, tels que des serveurs ou des ordinateurs, depuis l'extérieur de l'entreprise via le port 443 (utilisé pour HTTPS). Cette connexion s'effectue sans nécessité d'établir un réseau privé virtuel (VPN) tout en mettant en place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

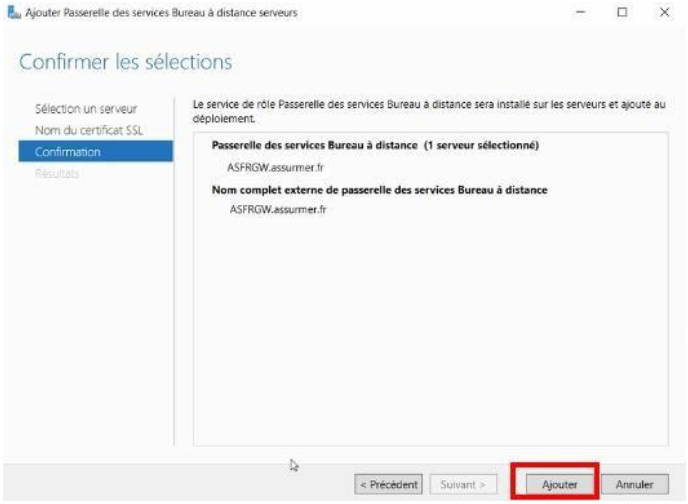


- Sélectionner le serveur ASFRGW qui sera le serveur de passerelle des services Bureau à distance du déploiement. Puis cliquer sur « Suivant ».

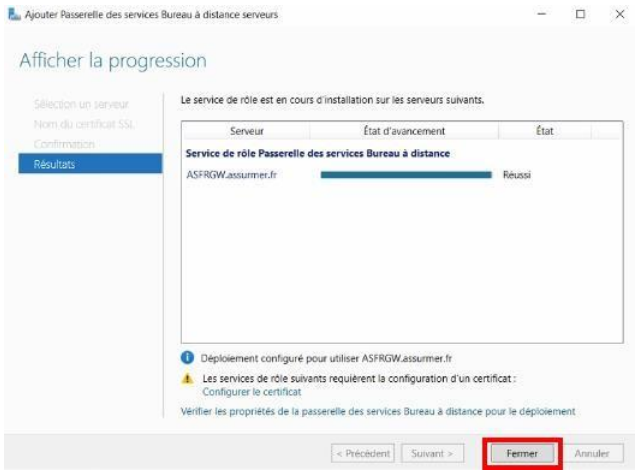


- Ajouter le nom du certificat SSL qui permettra le chiffrement entre les postes clients et la passerelle. Puis cliquer sur « Suivant ». Ce certificat sera importé sur les PC utilisateurs via une GPO.

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



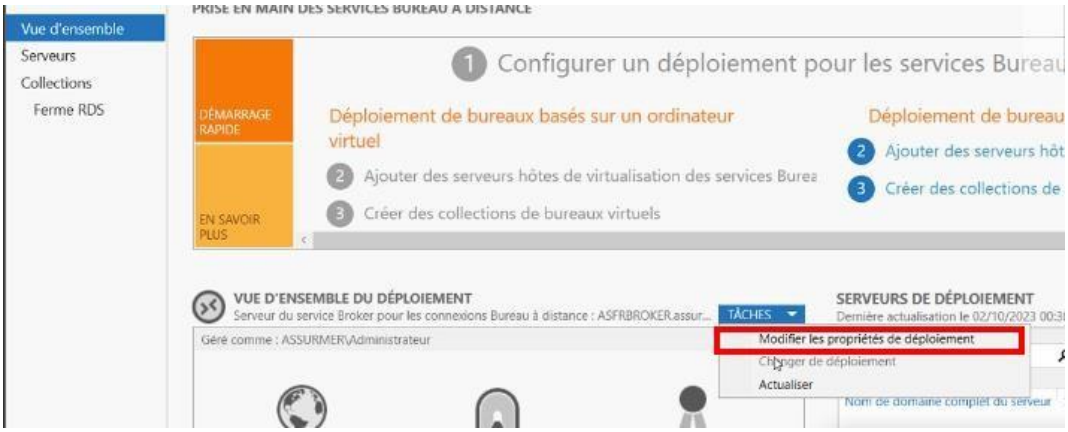
- Patienter puis cliquer sur « Fermer ».



2. Configuration du déploiement

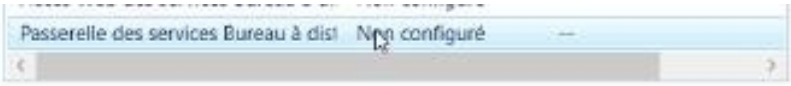
a) Ajout du certificat auto-signé

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

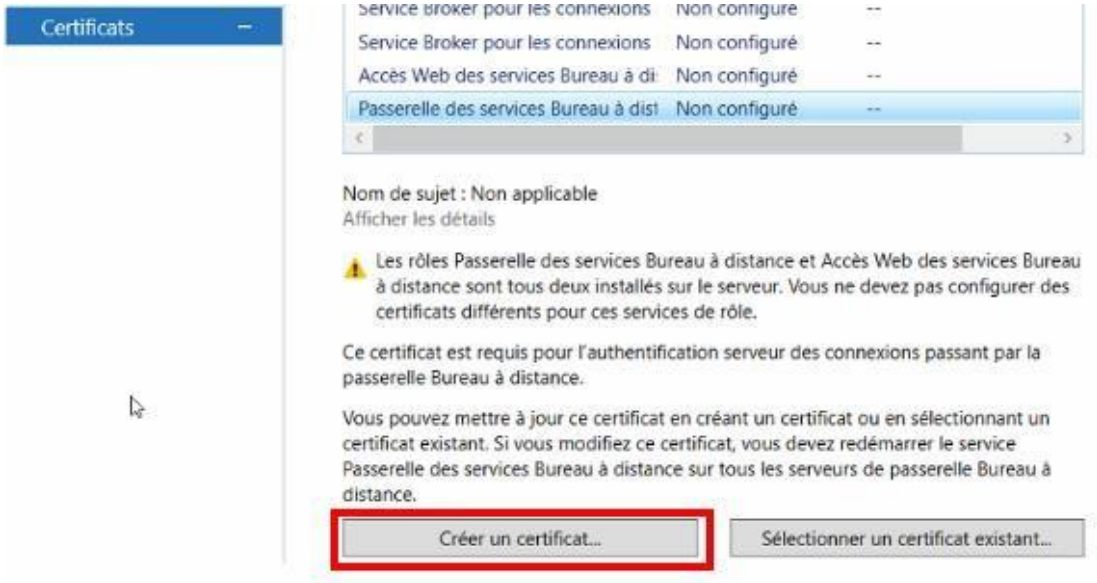


- Cliquer sur « Certificats ».

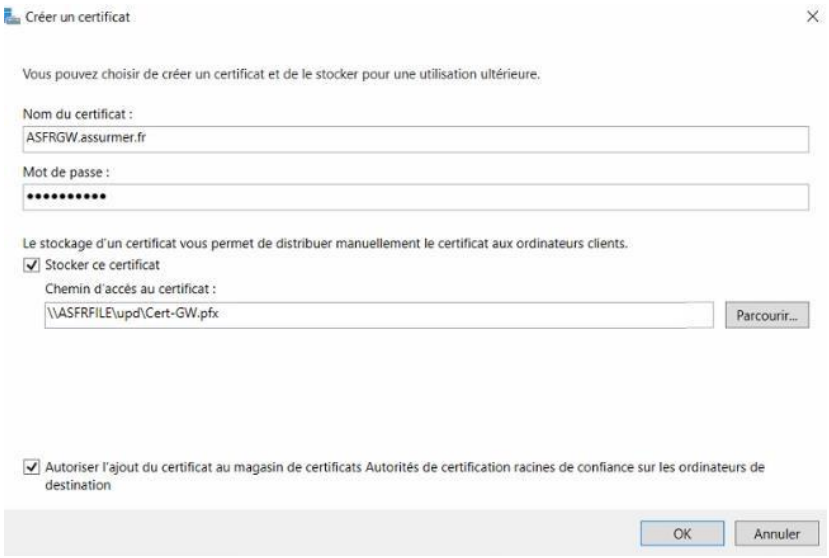
- Cliquer sur « Passerelle des services Bureau à distance ».



- Cliquer ensuite sur « Créer un certificat ».



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



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

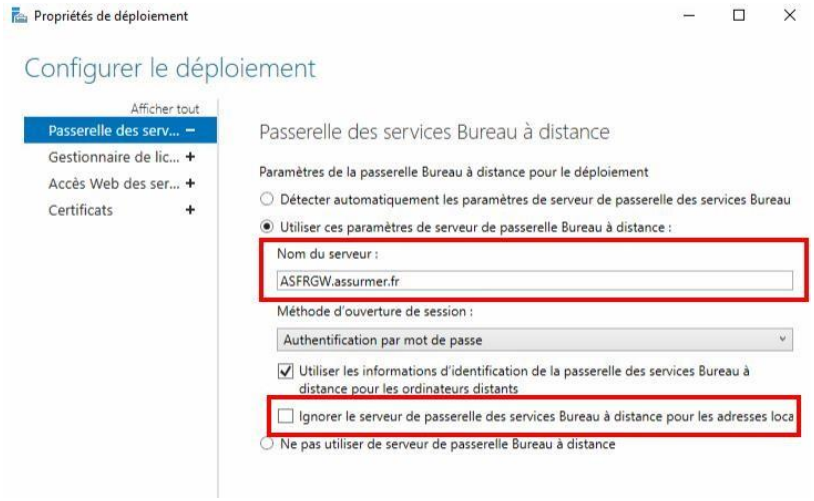
- Cliquer ensuite sur « Sélectionner un certificat existant ».

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

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

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 ».



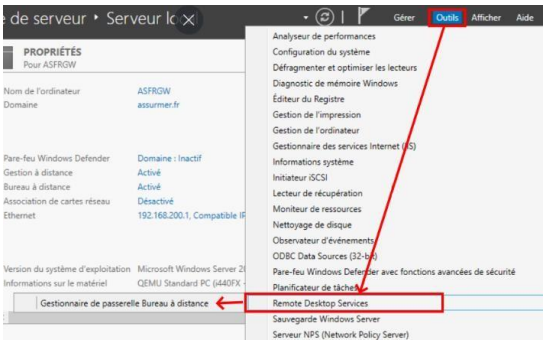
3. Configuration de la passerelle

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

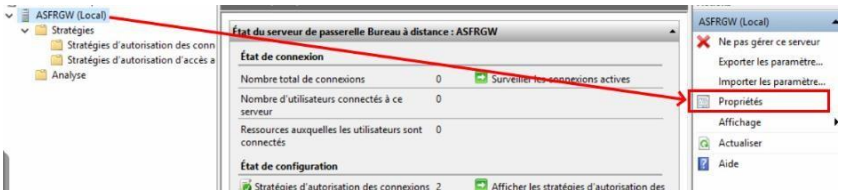
- Stratégies d'autorisation des connexions : elles définissent qui peut se connecter à la passerelle (utilisateurs et postes), quels périphériques sont redirigés et le délai d'expiration des sessions.
- Stratégies d'autorisation d'accès aux ressources : elles définissent qui peut se connecter à quoi.

a) Ajout du certificat

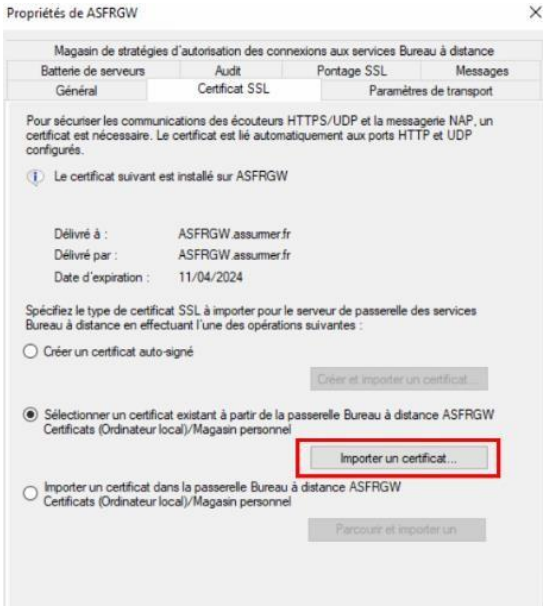
- Sur le serveur Proxmox, se connecter sur ASFRGW.
- Cliquer sur « Outils » puis « Remote Desktop Services » et accéder au gestionnaire.



- 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.

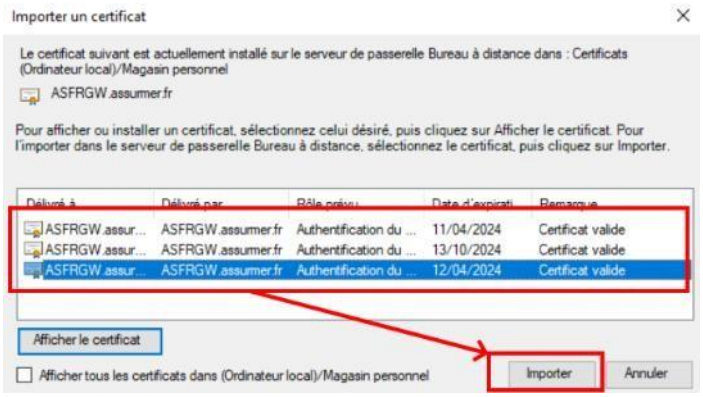


- Sur « Certificat SSL », cliquer sur « Importer un certificat ».


Propriétés de ASFRGW
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
Délivré à : ASFRGW.assurmer.fr
Délivré par : ASFRGW.assurmer.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.



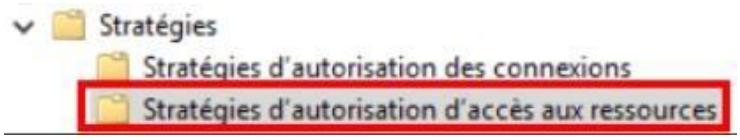
b) Présentation des stratégies par défaut

- 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 ».

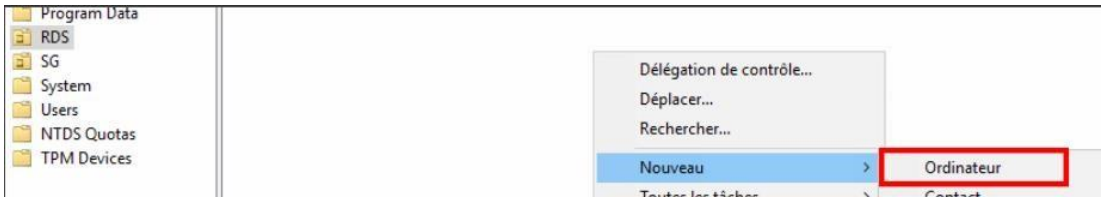


- Cliquer sur la stratégie « RDG_AllDomainComputers ».

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.

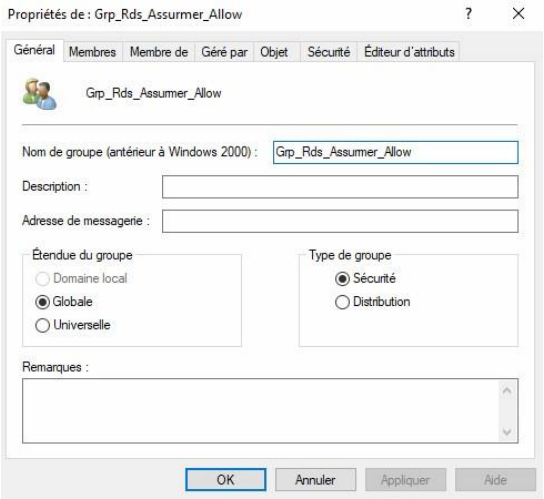


-

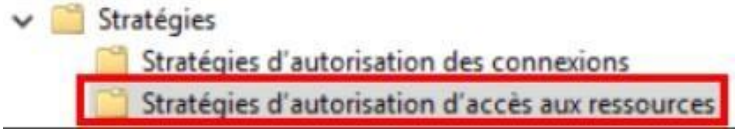
Entrer le nom « RDS » qui correspond à l'alias.

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

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



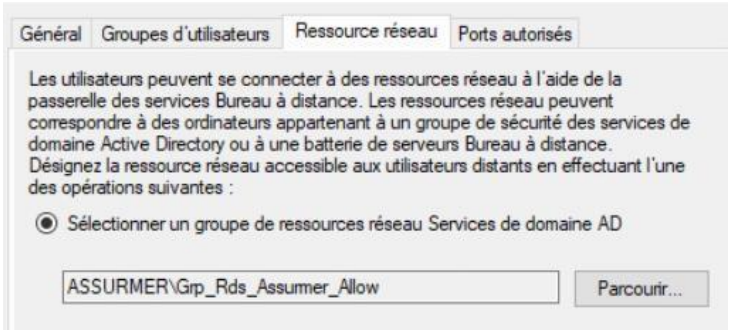
- Cliquer sur « Stratégies » puis « Stratégies d'autorisation d'accès aux ressources ».



-

Cliquer sur la stratégie « RDG_AllDomainComputers ».

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

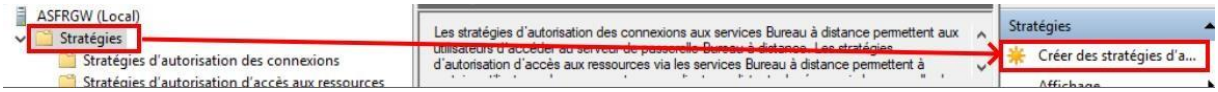


La stratégie permettra de limiter l'accès des utilisateurs uniquement aux ordinateurs de la ferme RDS. Il est aussi possible de créer des groupes gérés par la passerelle.

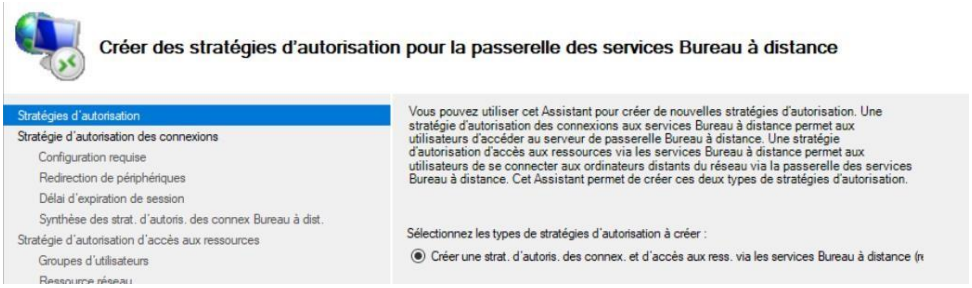
d) Création d'une stratégie pour les administrateurs

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

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

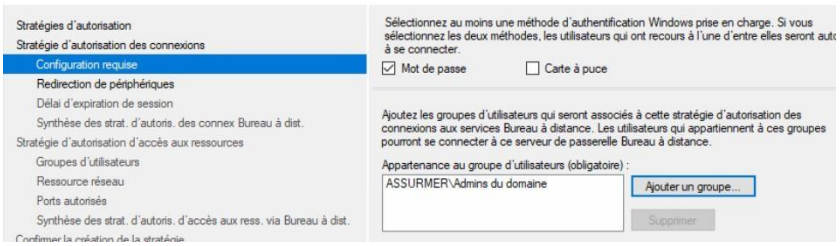


- Sélectionner la première option puis « Suivant ».



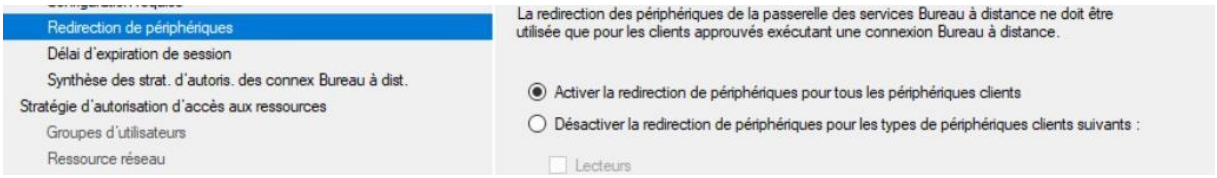
- Choisir un nom.

- Ajouter le groupe « Admins du domaine ».

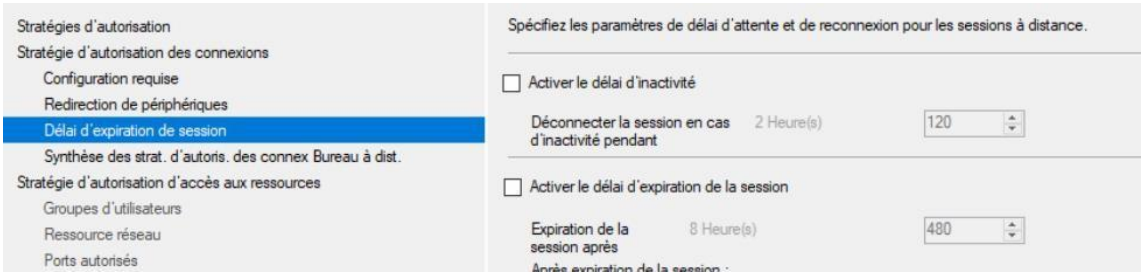


-

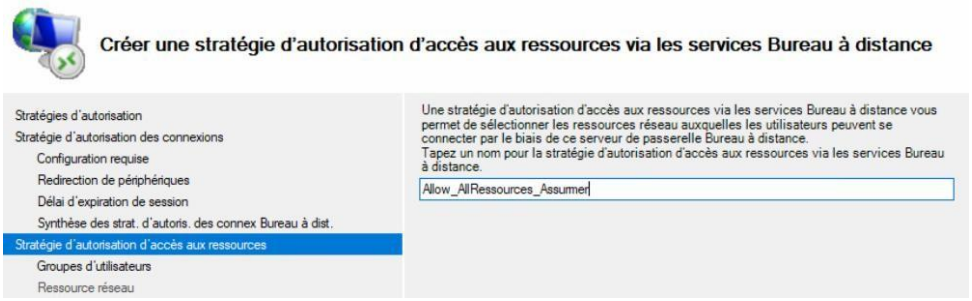
Laisser la redirection des périphériques par défaut.



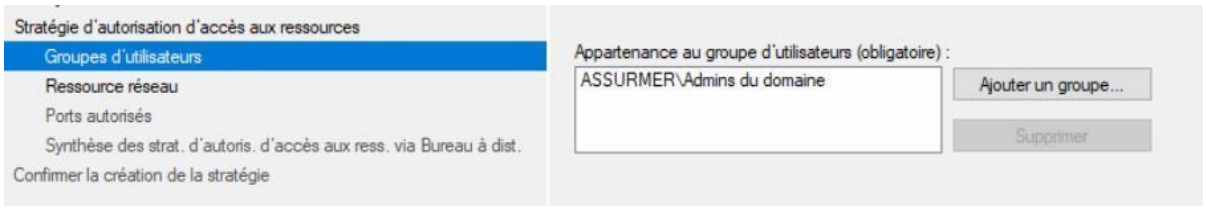
- Laisser le délai par défaut.



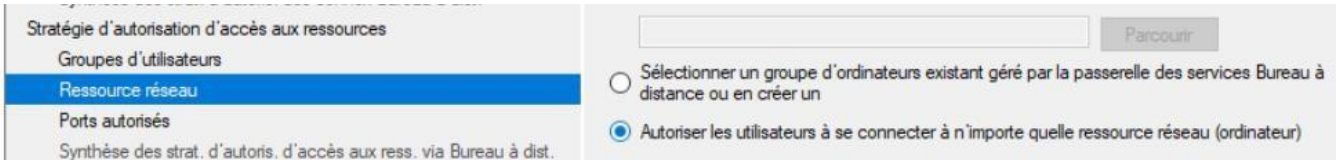
- Un résumé s'affiche. Cliquer sur « Suivant ». Nous allons maintenant passer à la création de la stratégie d'accès aux ressources.
- Ajouter un nom.



- Le groupe d'appartenance est déjà défini.

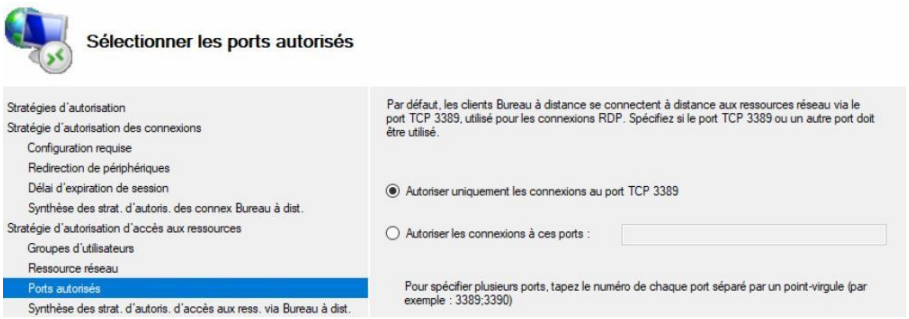


- Sur l'onglet « Ressource réseau », cocher « Autoriser les utilisateurs à se connecter à n'importe quelle ressource réseau ».



Laisser les ports par défaut.

-



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