



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 | Erreur ! Signet non défini. |
| 1. Ajout du serveur | Erreur ! Signet non défini. |
| 2. Configuration du déploiement | Erreur ! Signet non défini. |
| a) Ajout du certificat auto-signé..... | Erreur ! Signet non défini. |
| b) Configuration de la « passerelle des services Bureau à distance » | Erreur ! Signet non défini. |
| 3. Configuration de la passerelle | Erreur ! Signet non défini. |
| a) Ajout du certificat..... | Erreur ! Signet non défini. |
| b) Présentation des stratégies par défaut..... | Erreur ! Signet non défini. |
| c) Configuration de la stratégie | Erreur ! Signet non défini. |
| d) Création d'une stratégie pour les administrateurs | Erreur ! Signet non défini. |
| 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 | 6 |
| 1. Authentification unique (SSO) | 6 |
| 2. Raccourcis WEB et RDP | 9 |
| a) Configuration du raccourci | 9 |
| b) Configuration du fichier rdp pour les sessions distantes (Raccourci GPO) | 10 |
| 3. GPO pour les certificats Broker et Passerelle | 12 |
| a) Exportation du certificat | 13 |
| b) Création de la GPO | 16 |
| 4. Page Web personnalisée Assurmer | 20 |
| a) Changement du texte « Work Resources » | 20 |

| | |
|---|------------------------------------|
| b) Ajout d'une redirection automatique vers RDWeb | 20 |
| c) Ajout de la réinitialisation de mot de passe depuis le portail | 21 |
| d) Modification des fichiers de la page | 21 |
| 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

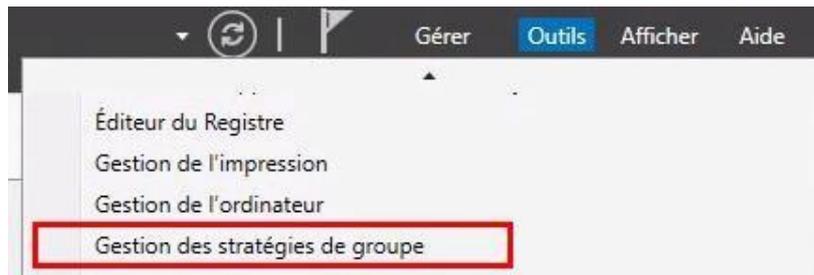
VII. Personnalisation de l'environnement RDS

Dans le but d'optimiser l'ergonomie de l'environnement RDS, nous entreprendrons les étapes suivantes pour une meilleure expérience des collaborateurs d'Assumer :

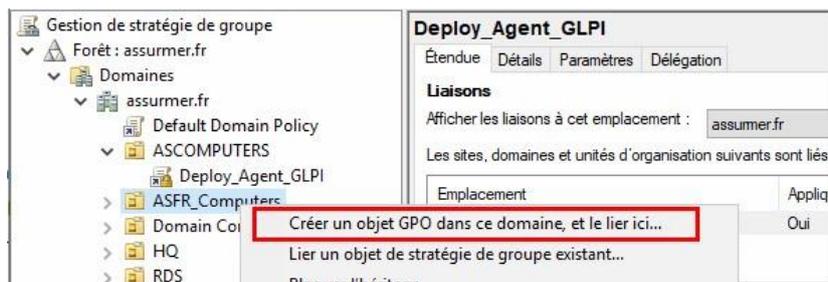
1. Authentification unique (SSO)

Il a été décidé de mettre en place une solution d'authentification unique pour simplifier la connexion des collaborateurs.

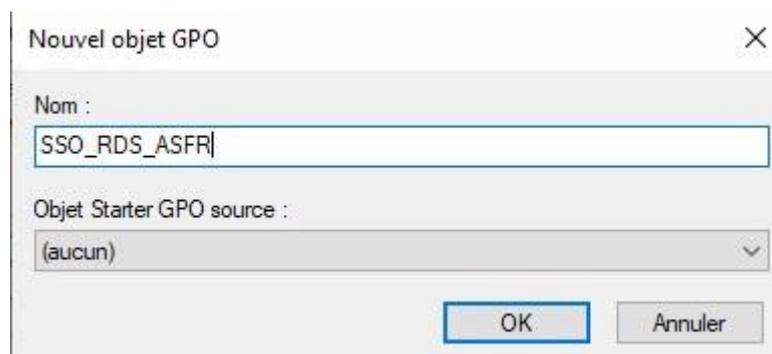
- Ouvrir la console « Gestion des stratégies de groupes ».



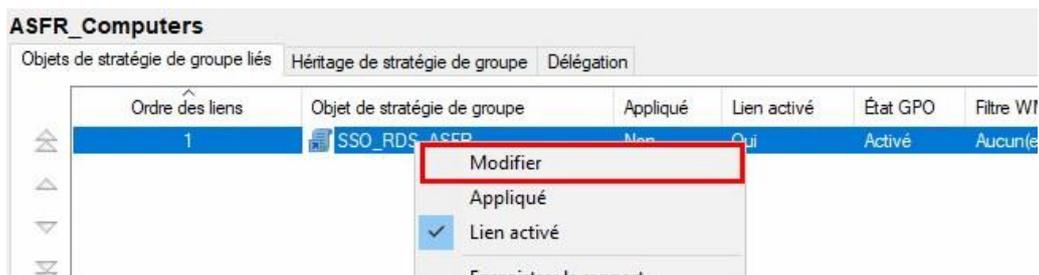
- Sur l'OU contenant les ordinateurs des collaborateurs, faire clic droit puis « Créer un objet GPO dans ce domaine, et le lier ici ».



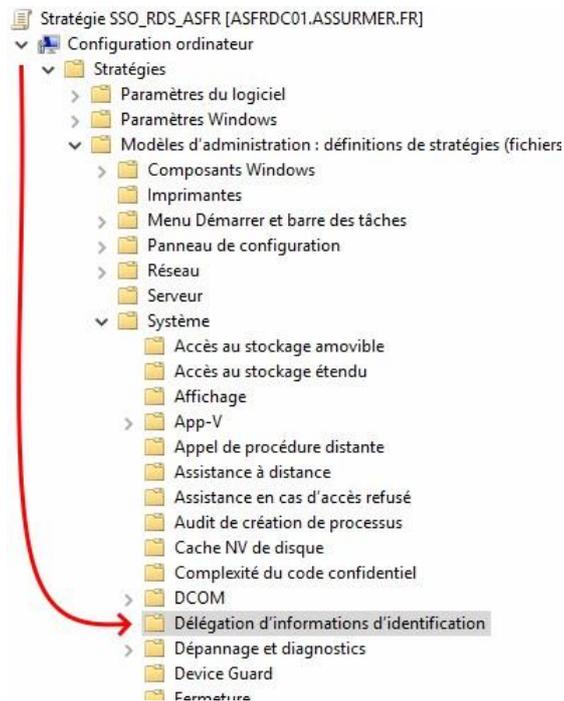
- Nommer la GPO et cliquer sur « OK ».



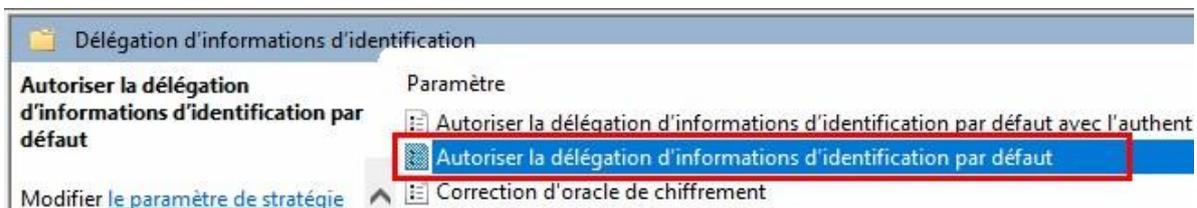
- Faire clic droit sur la GPO puis la modifier.



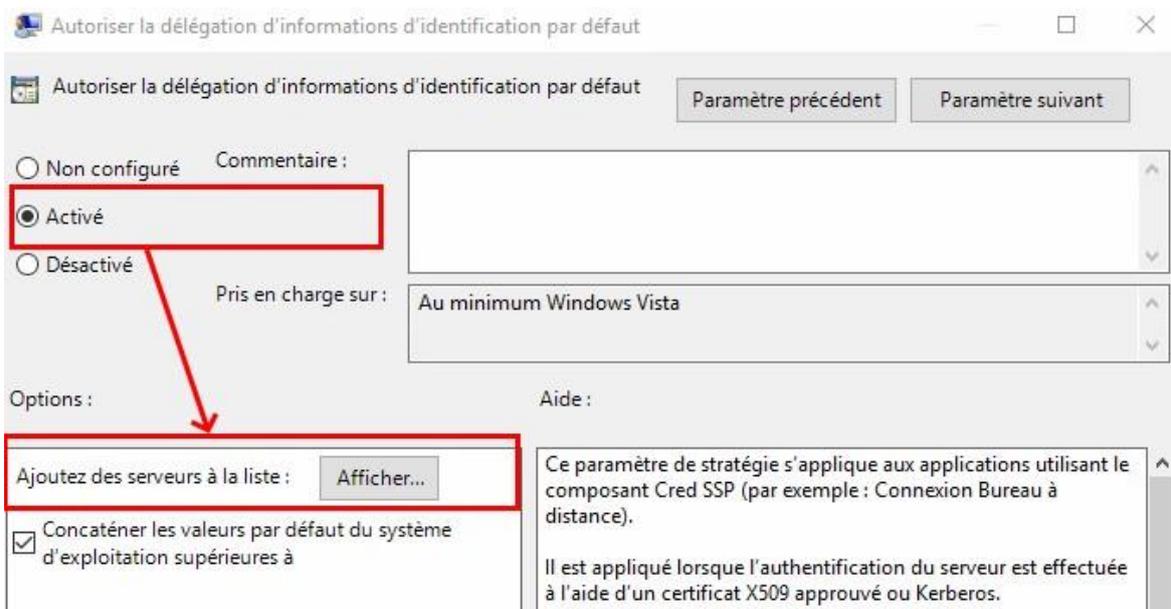
- Se rendre à l'emplacement suivant : Configuration ordinateur / Stratégies / Modèles d'administrations / Système / Délégation d'informations d'identification.



- Double cliquer sur « Autoriser la délégation d'information d'identification par défaut » pour ouvrir les paramètres.

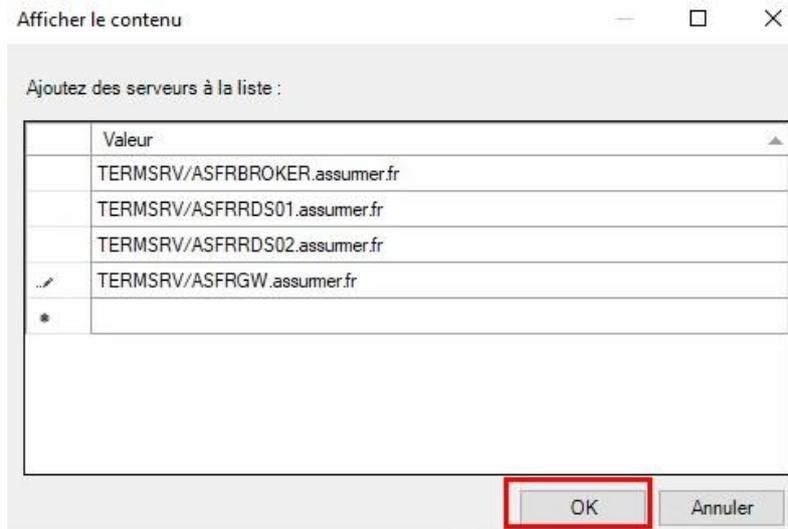


- Cliquer sur la coche « Activé » puis sur « Afficher ».

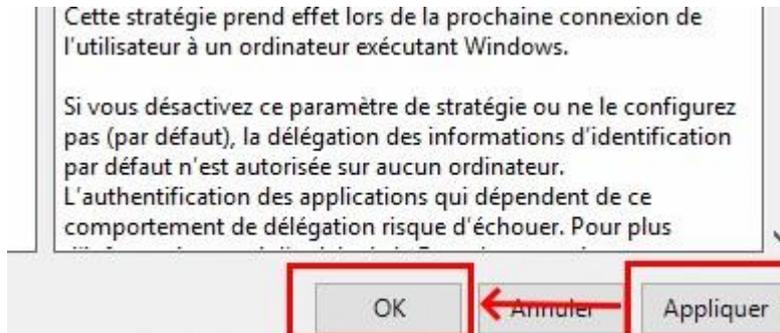


- Ajouter les serveurs sur lesquels il faut activer le SSO. Puis cliquer sur « OK ».

- o TERMSRV//server.assumer.fr



- Cliquer sur « Appliquer » puis « OK ».



- Le paramètre est activé.

| | |
|--|---------------|
| l'informations d'identification par défaut avec l'authentificatio... | Non configuré |
| l'informations d'identification par défaut | Activé |
| niffrement | Non configuré |
| le nouvelles informations d'identification | Non configuré |

Résumé de la stratégie :



- Sur le poste client, faire « Windows + R » puis la commande « gpupdate /force ».

2. Raccourcis WEB et RDP

Un raccourci Web sera présent directement sur les postes utilisateurs pour accéder aux RemoteApp ainsi que le raccourci rdp pour se connecter à la collection directement et ouvrir une session distante.

a) Configuration du raccourci

- Ouvrir la console « Gestion des stratégies de groupes ».



- Sur l'OU contenant les ordinateurs des collaborateurs, faire clic droit puis « Créer un objet GPO dans ce domaine, et le lier ici ».



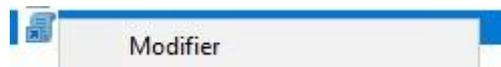
- Nommer la GPO et cliquer sur « OK ».

| | | | | | | | |
|---|----------------|-----|-----|--------|----------|--------------|------------|
| 3 | RDWeb_Shortcut | Non | Oui | Activé | Aucun(e) | 15/10/202... | assumer.fr |
|---|----------------|-----|-----|--------|----------|--------------|------------|

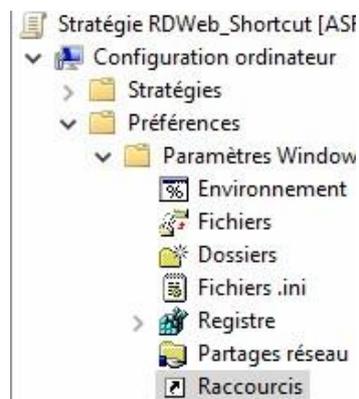
- Lier la GPO à l'OU HQ des comptes utilisateurs également.



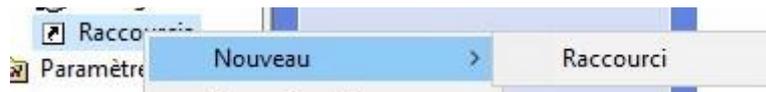
- Faire clic droit sur la GPO puis la modifier.



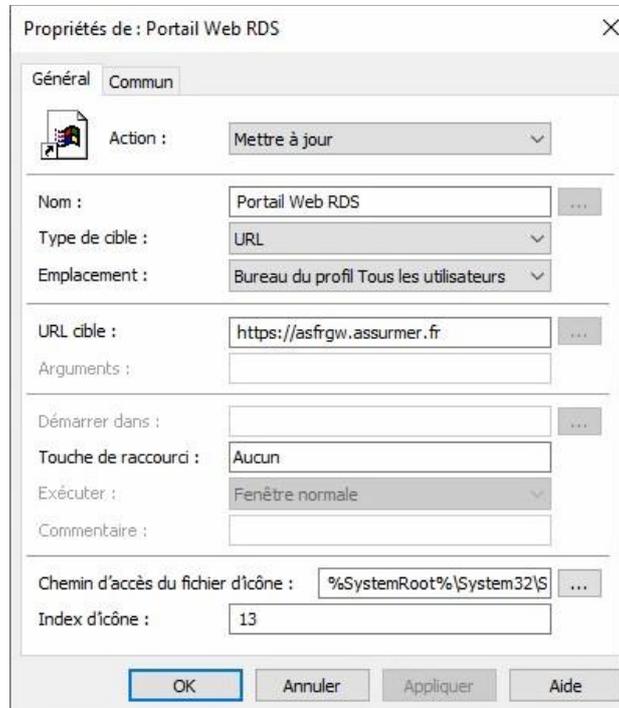
- Se rendre à l'emplacement suivant : Configuration ordinateur / Préférences / Paramètres Windows / Raccourcis.



- Faire clic droit, « Nouveau » puis « Raccourci ».



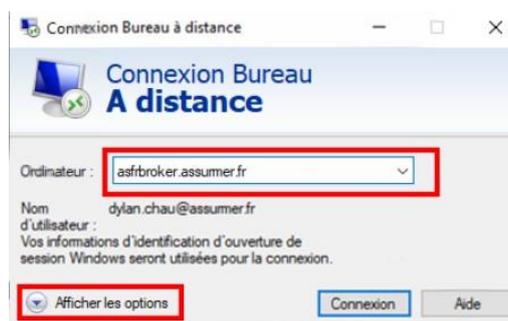
- Renseigner les informations du raccourci, cliquer sur « Appliquer » puis « OK ».



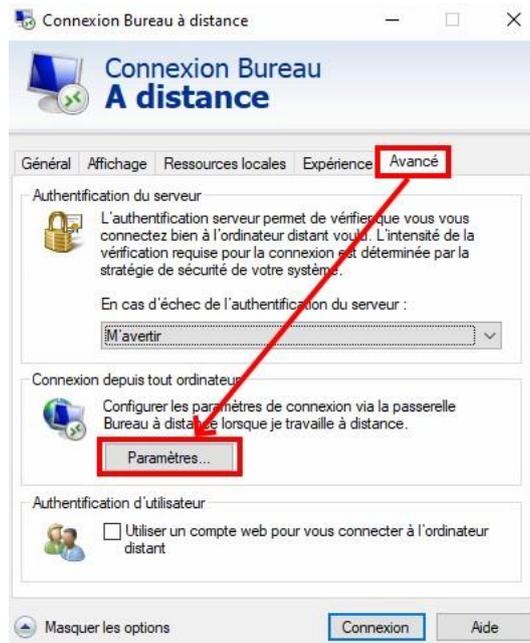
Nous allons également créer un raccourci rdp pour le Broker (qui redistribuera les sessions vers les serveurs RDS) qui fonctionnera en parallèle avec la GPO SSO.

b) Configuration du fichier rdp pour les sessions distantes (Raccourci GPO)

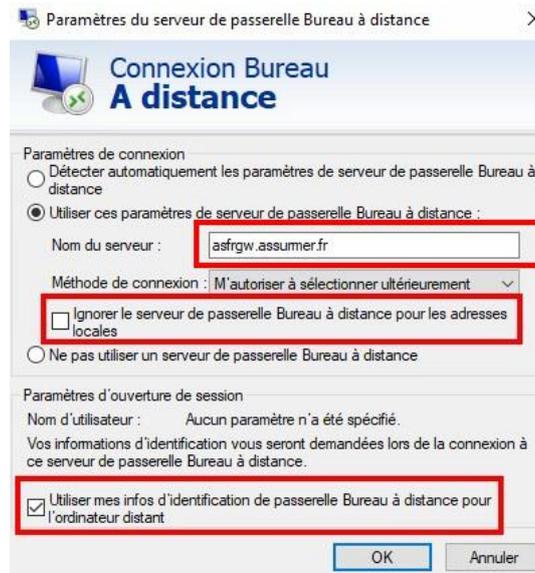
- Lancer le client sur le Filer, entrer l'alias broker et cliquer sur « Options ».



- Cliquer sur « Avancé » puis « Paramètres ».

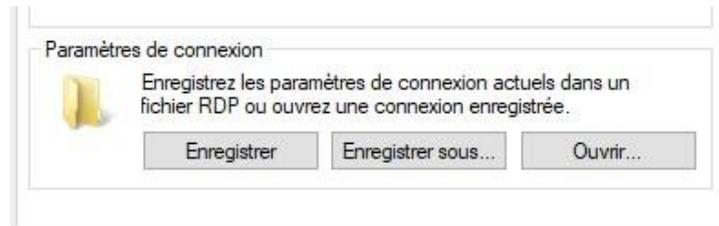


- Ajouter le serveur de passerelle Bureau à distance, décocher la case « Ignorer pour les adresses locales » et cocher la dernière case.



Cliquer sur « OK ».

- Dans « Général », cliquer sur « Enregistrer sous » et placer le sur le serveur de fichiers.

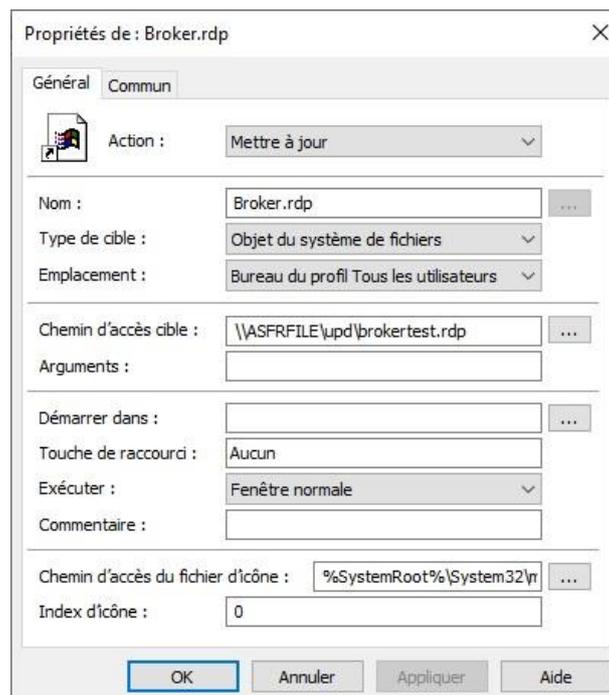


- Sur le serveur de fichiers, éditer le fichier avec le bloc-notes.



- Rajouter les lignes :
 - o **use redirection server name:i:1** au lieu de **use redirection server name:i:0**
 - o **loadbalanceinfo:s:tsv://MS Terminal Services Plugin.1.Ferme_RDS** (en mettant bien les _ pour le nom de la ferme).
- Sauvegarder. Le fichier est prêt à être déployé par GPO.

Sur ASFRDC01, ajouter ce raccourci :



- Les raccourcis devraient apparaître après un redémarrage ou gpupdate /force.

3. GPO pour les certificats Broker et Passerelle

L'objectif de cette GPO est d'assurer des communications sécurisées et fiables entre les ordinateurs clients de notre réseau et notre serveur en utilisant le protocole TLS/SSL.

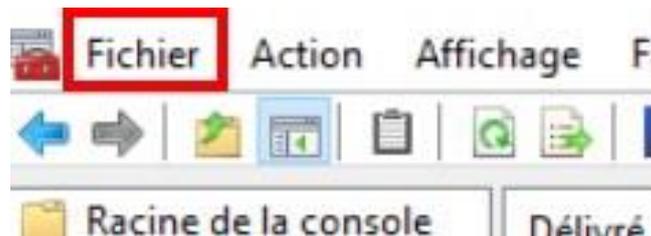
Celle-ci distribuera un certificat contenant la clé publique .cer à tous les clients, ce qui leur permettra de chiffrer les données échangées.

Sur le serveur, nous conservons un fichier .pfx contenant à la fois la clé publique (pour chiffrer) et la clé privée (importante pour déchiffrer les données).

Nous allons donc exporter le certificat ne contenant que la clé publique.

a) Exportation du certificat

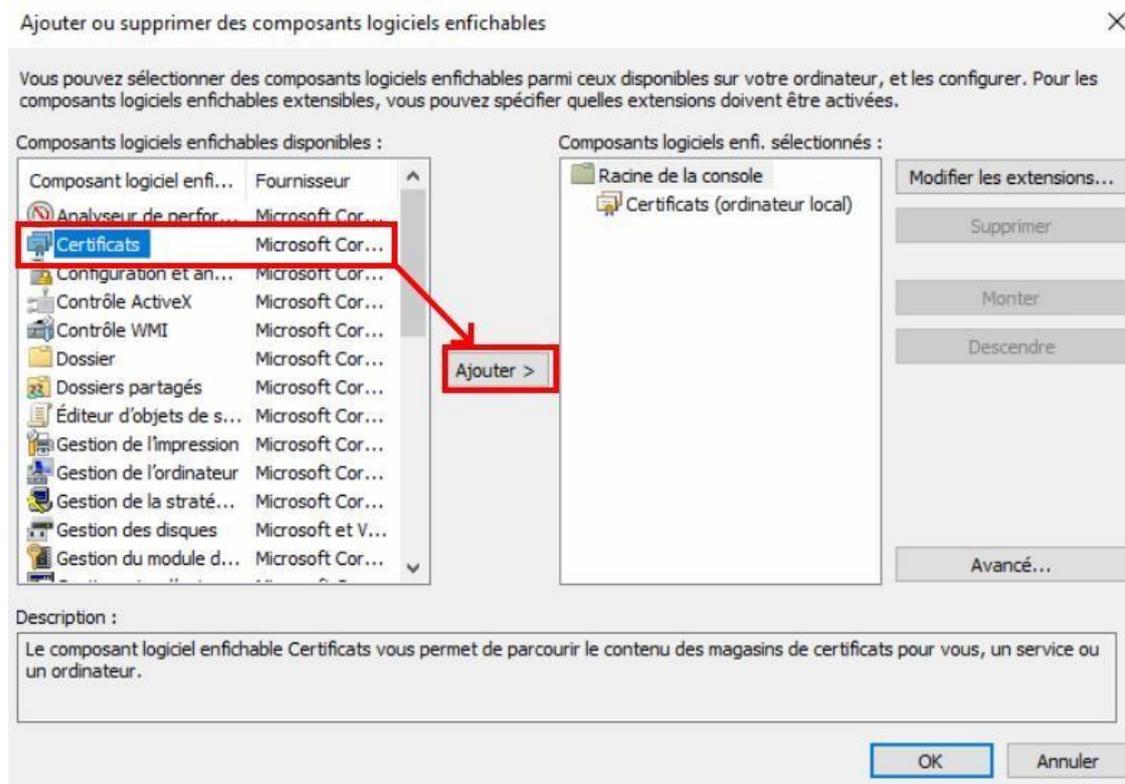
- Sur les serveurs contenant les certificats .pfx, ouvrir la console MMC de gestion de certificat sur l'ordinateur local et aller sur le magasin où est stocké le certificat. - Cliquer sur « Fichier ».



- Cliquer sur « Ajouter/Supprimer un composant logiciel enfichable... »

Ajouter/Supprimer un composant logiciel enfichable... Ctrl+M

- Choisir Certificats puis l'ajouter.



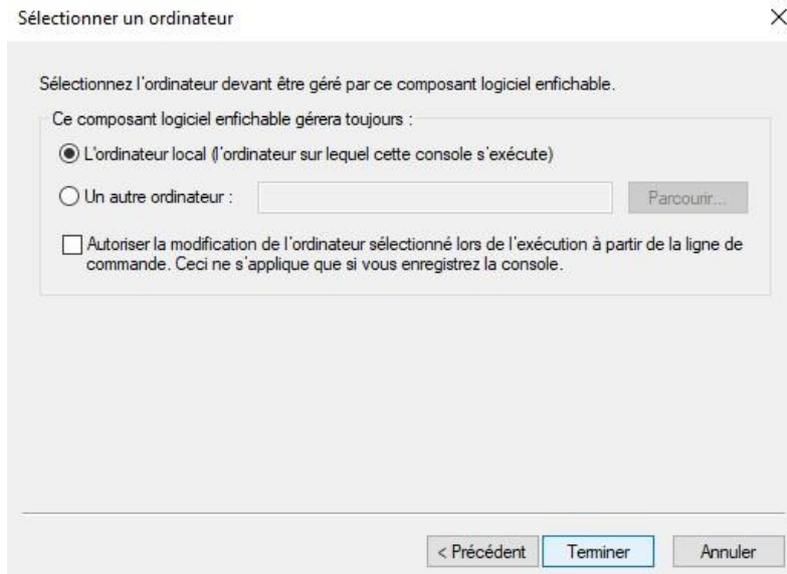
Choisir « Un compte d'ordinateur ».

Composant logiciel enfichable Certificats

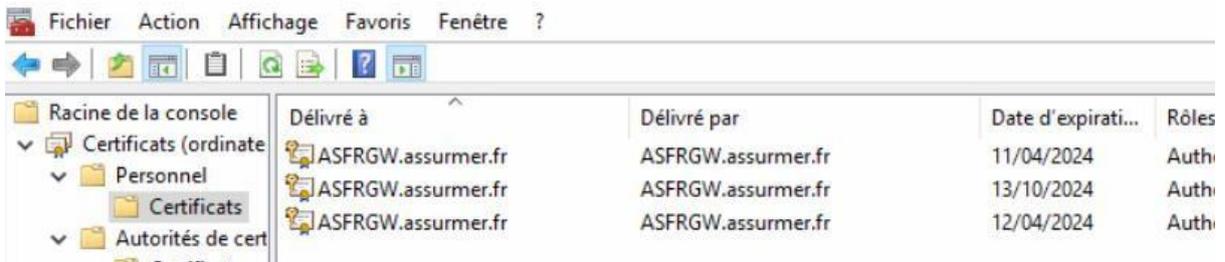
Ce composant logiciel enfichable gèrera toujours les certificats pour :

- Mon compte d'utilisateur
- Un compte de service
- Un compte d'ordinateur

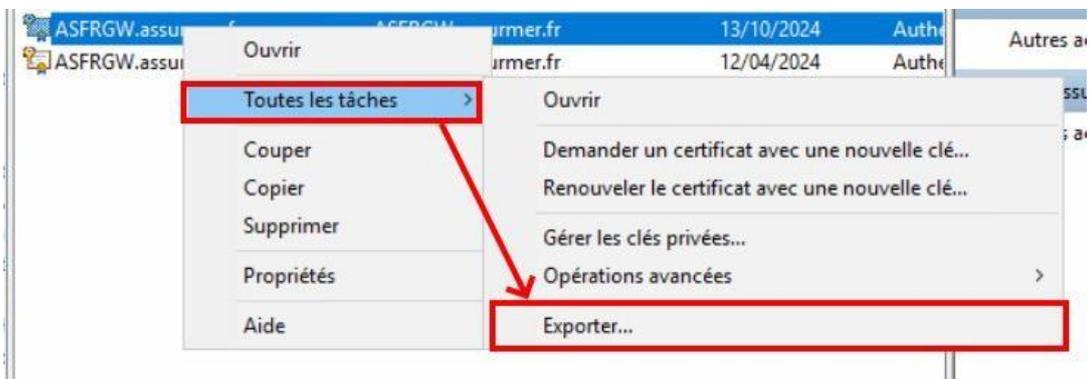
- Sélectionner « l'ordinateur local » puis cliquer sur « Terminer ».



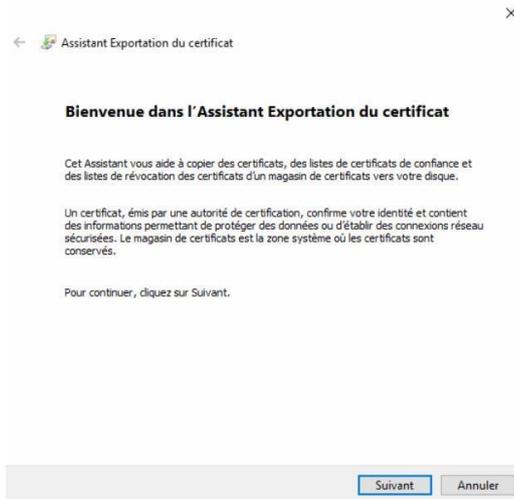
- Les certificats pfx précédemment importés sont présents dans Personnel/Certificats.



- Faire clic droit sur le certificat, puis aller sur « Toutes les tâches » et « Exporter ».



L'assistant d'exportation s'ouvre, cliquer sur « Suivant ».



- Laisser « Non ne pas exporter la clé privée » (le certificat ne contiendra que la clé publique).

Exporter la clé privée

Vous pouvez choisir d'exporter la clé privée avec le certificat.

Les clés privées sont protégées par mot de passe. Si vous voulez exporter la clé privée avec le certificat, vous devez taper un mot de passe dans une prochaine page.

Voulez-vous exporter la clé privée avec le certificat ?

- Oui, exporter la clé privée
- Non, ne pas exporter la clé privée

Remarque : la clé privée associée est marquée comme ne pouvant pas être exportée. Seul le certificat peut être exporté.

- Choisir l'option « X.509 binaire encodé DER » qui est une méthode d'encodage.

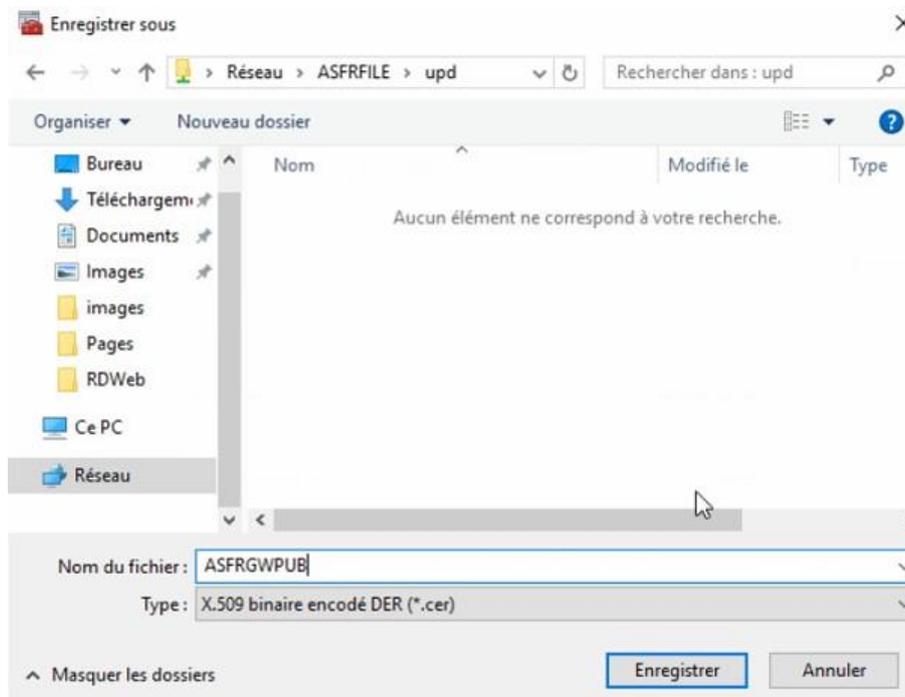
Format du fichier d'exportation

Les certificats peuvent être exportés dans divers formats de fichiers.

Sélectionnez le format à utiliser :

- X.509 binaire encodé DER (*.cer)
- X.509 encodé en base 64 (*.cer)
- Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)
- Inclure tous les certificats dans le chemin d'accès de certification, si possible
- Échange d'informations personnelles - PKCS #12 (.PFX)
- Inclure tous les certificats dans le chemin d'accès de certification, si possible
- Supprimer la clé privée si l'exportation réussit
- Exporter toutes les propriétés étendues
- Activer la confidentialité de certificat
- Magasin de certificats sérialisés Microsoft (.SST)

Parcourir les dossiers, ajouter un nom et exporter le certificat dans ASFRFILE. Cliquer sur « Suivant ».



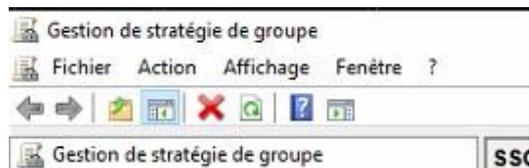
- Cliquer sur « Terminer ».
- Répéter l'opération pour le certificat du Broker.
- Nos certificats avec clé publique sont bien créés sur ASFRFILE.

| | | | |
|---------------|------------------|------------------------|------|
| ASFRBROKERPUB | 15/10/2023 17:01 | Certificat de sécur... | 1 Ko |
| ASFRGWPUB | 15/10/2023 16:59 | Certificat de sécur... | 1 Ko |

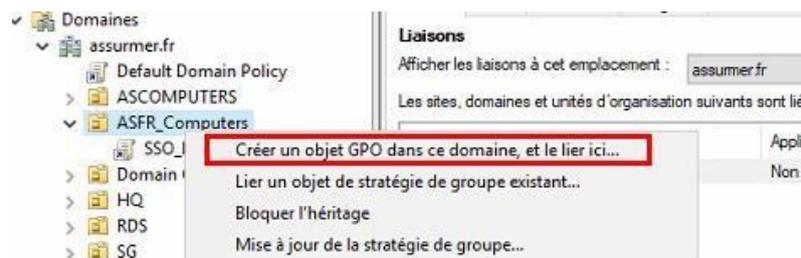
b)

Création de la GPO

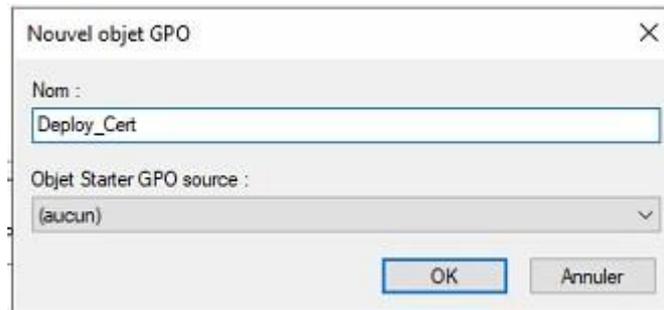
- Se rendre sur la console de Gestion des stratégies de groupe.



- Faire un clic droit sur OU ASFR_Computers puis cliquer sur « Créer un objet GPO dans ce domaine, et le lier ici ... ».



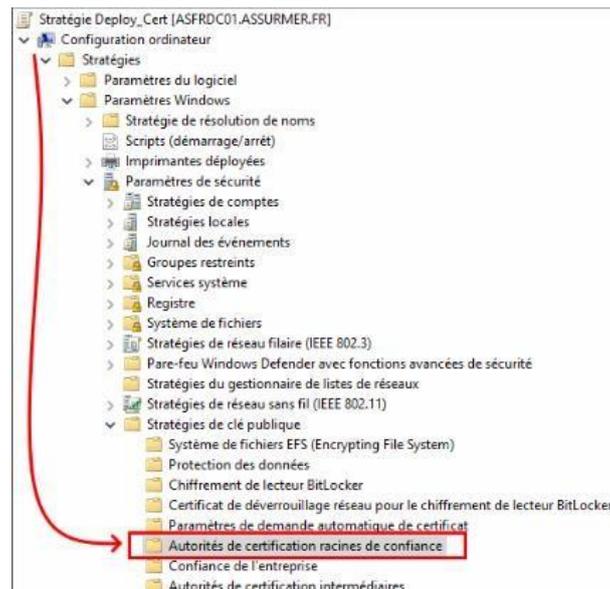
Nommer la stratégie.



Faire clic droit sur la stratégie puis « Modifier ».



Aller au paramètre de « Autorités de certification racines de confiance » qui se trouve dans : Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégie de clé publique.



Faire clic droit et cliquer sur « Importer ».



L'assistant va se lancer, cliquer sur « Suivant ».

Assistant Importation du certificat

Bienvenue dans l'Assistant Importation du certificat

Cet Assistant vous aide à copier des certificats, des listes de certificats de confiance et des listes de révocation des certificats d'un disque vers un magasin de certificats.

Un certificat, émis par une autorité de certification, confirme votre identité et contient des informations permettant de protéger des données ou d'établir des connexions réseau sécurisées. Le magasin de certificats est la zone système où les certificats sont conservés.

Emplacement de stockage

Utilisateur actuel

Ordinateur local

Pour continuer, cliquez sur Suivant.

Suivant

Annuler

- Cliquer sur « Parcourir » et ajouter le certificat.

Assistant Importation du certificat

Fichier à importer

Spécifiez le fichier à importer.

Nom du fichier :

\\ASFRFILE\upd\ASFRGW\Pub.cer

Parcourir...

Remarque : plusieurs certificats peuvent être stockés dans un même fichier aux formats suivants :

Échange d'Informations personnelles- PKCS #12 (.PFX,.P12)

Standard de syntaxe de message cryptographique - Certificats PKCS #7 (.P7B)

Magasin de certificats sérialisés Microsoft (.SST)

- Cliquer sur « Suivant ».

Suivant

Annuler

- Laisser le magasin et cliquer sur « Suivant ».

Assistant Importation du certificat

Magasin de certificats

Les magasins de certificats sont des zones système où les certificats sont conservés.

Windows peut sélectionner automatiquement un magasin de certificats, ou vous pouvez spécifier un emplacement pour le certificat.

Sélectionner automatiquement le magasin de certificats en fonction du type de certificat

Placer tous les certificats dans le magasin suivant

Magasin de certificats :

Autorités de certification racines de confiance

Parcourir...

Cliquer sur « Terminer ».

-
- L'importation a réussi, cliquer sur « OK ».
- Nos 2 certificats sont importés.

| Délivré à | Délivré par |
|---|-----------------------|
|  ASFRBROKER.assumer.fr | ASFRBROKER.assumer.fr |
|  ASFRGW.assumer.fr | ASFRGW.assumer.fr |

Paramètres de la stratégie :

| Configuration ordinateur (activée) | | | |
|--|-----------------------|---------------------|--|
| Stratégies | | | |
| Paramètres Windows | | | |
| Paramètres de sécurité | | | |
| Stratégies de clé publique/Autorités de certification de racine de confiance | | | |
| Certificats | | | |
| Émise à | Délivré par | Date d'expiration | Rôles prévus |
| ASFRBROKER.assumer.fr | ASFRBROKER.assumer.fr | 13/10/2024 19:12:13 | Authentification du client, Authentification du serveur |
| ASFRGW.assumer.fr | ASFRGW.assumer.fr | 13/10/2024 18:11:56 | Authentification du client, Authentification du serveur |
| Pour obtenir plus d'informations sur les paramètres, exécutez l'Éditeur d'objet de stratégie de groupe locale. | | | |

4. Page Web personnalisée Assumer

Nous avons modifié le portail Web pour le rendre propre à Assumer.

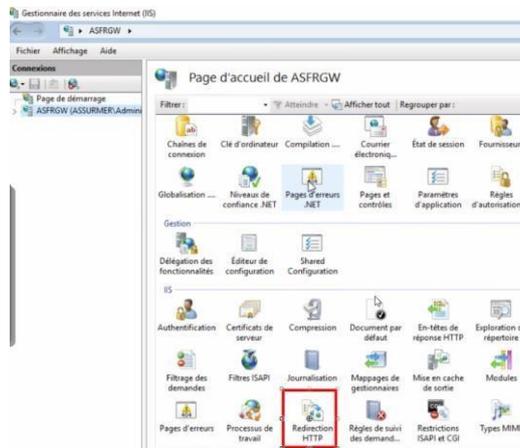
a) Changement du texte « Work Resources »

- Dans le serveur ASFRBROKER, lancer powershell.exe en Administrateur
- Rentrer la commande suivante :

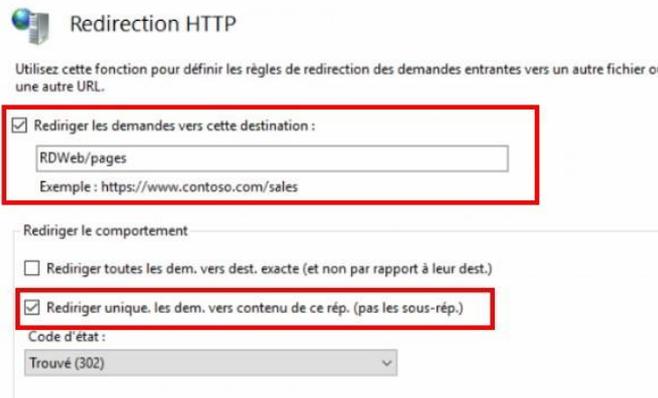
```
PS C:\Users\Administrateur.ASSURMER> Set-RDWorkspace -Name "Assumer RD Workspace"
```

b) Ajout d'une redirection automatique vers RDWeb

- Sur le gestionnaire des services Internet (IIS), cliquer sur « Redirection HTTP ».



- Ajouter la redirection et cocher la case « Rediriger unique. les dem. vers contenu de ce rép. ».

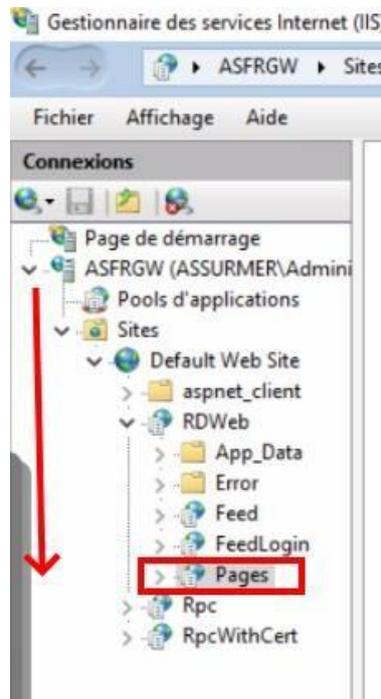


- Cliquer sur « Appliquer ».



c) Ajout de la réinitialisation de mot de passe depuis le portail

- Sur le gestionnaire des services Internet (IIS), dérouler le menu dans ASFRGW\Sites\Default Web Site\RDWeb\Pages

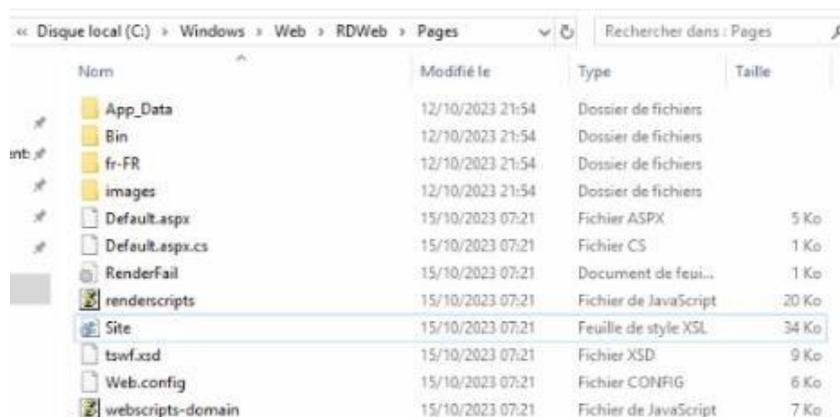


- Changer la valeur de PasswordChangeEnabled en « true ».



d) Modification des fichiers de la page

Sur le serveur ASFRGW directement, modifier les fichiers dans les chemins suivants à l'aide de Notepad++ ou du Bloc-notes :

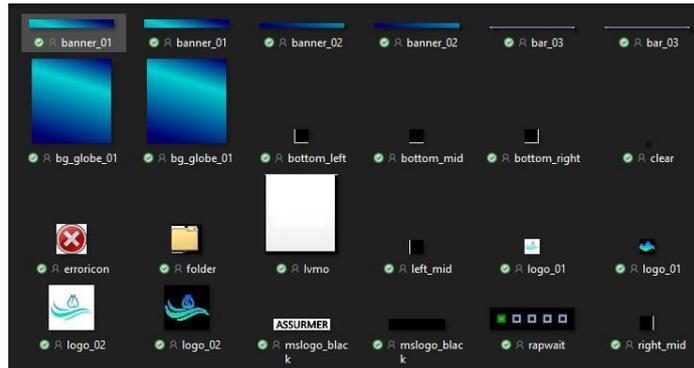


| Nom | Modifié le | Type | Taille |
|-------------------|------------------|-----------------------|--------|
| App_Data | 12/10/2023 21:54 | Dossier de fichiers | |
| Bin | 12/10/2023 21:54 | Dossier de fichiers | |
| fr-FR | 12/10/2023 21:54 | Dossier de fichiers | |
| images | 12/10/2023 21:54 | Dossier de fichiers | |
| Default.aspx | 15/10/2023 07:21 | Fichier ASPX | 5 Ko |
| Default.aspx.cs | 15/10/2023 07:21 | Fichier CS | 1 Ko |
| RenderFail | 15/10/2023 07:21 | Document de feui... | 1 Ko |
| renderscripts | 15/10/2023 07:21 | Fichier de JavaScript | 20 Ko |
| Site | 15/10/2023 07:21 | Feuille de style XSL | 34 Ko |
| tswf.xsd | 15/10/2023 07:21 | Fichier XSD | 9 Ko |
| Web.config | 15/10/2023 07:21 | Fichier CONFIG | 6 Ko |
| webscripts-domain | 15/10/2023 07:21 | Fichier de JavaScript | 7 Ko |

- \Web\RDWeb\Pages\fr-FR\rap-help.htm pour la page d'aide locale (Nous l'avons désactivé).
- \Web\RDWeb\Pages\login.aspx pour modifier le texte sur la protection contre les accès non autorisés.

Pour vous protéger contre les accès non autorisés, votre session Accès Bureau à distance par le Web expirera automatiquement après une période d'inactivité. Si votre session se termine, actualisez votre navigateur et reconnectez-vous. En cas de problème, veuillez contacter support@assurmer.fr

- \Web\RDWeb\pages\site.xml pour retirer certains éléments de la page.
- \Web\RDWeb\Pages\images\ pour les images qui composent le site. Nous avons modifié certaines des images pour les adapter à Assurmer.



- \Web\RDWeb\Pages\fr-FR\RDWASStrings.xml pour modifier certains textes sur la page de connexion.

- Après les modifications, redémarrer la page via cmd avec ISSRESET /restart :

```
C:\Users\Administrateur.ASSURMER>IISRESET /restart  
Tentative d'arrêt en cours...  
Les services Internet ont été arrêtés avec succès  
Tentative de démarrage en cours...  
Les services Internet ont été redémarrés avec succès
```

Les modifications nous permettent ainsi d'obtenir le portail suivant :

