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

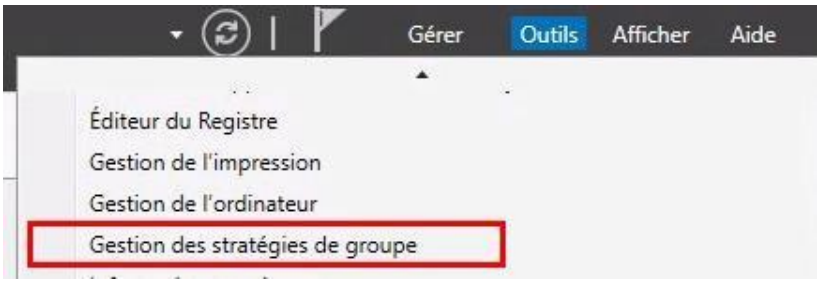
VII. Personnalisation de l'environnement RDS

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

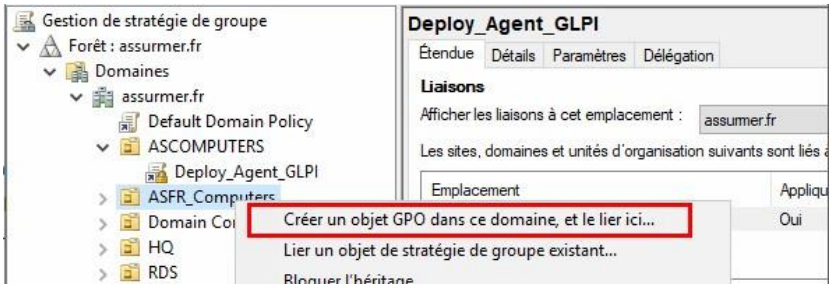
1. Authentification unique (SSO)

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

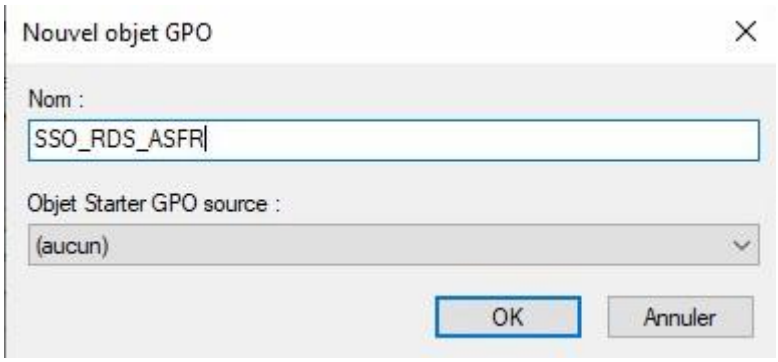
- Ouvrir la console « Gestion des stratégies de groupes ».



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

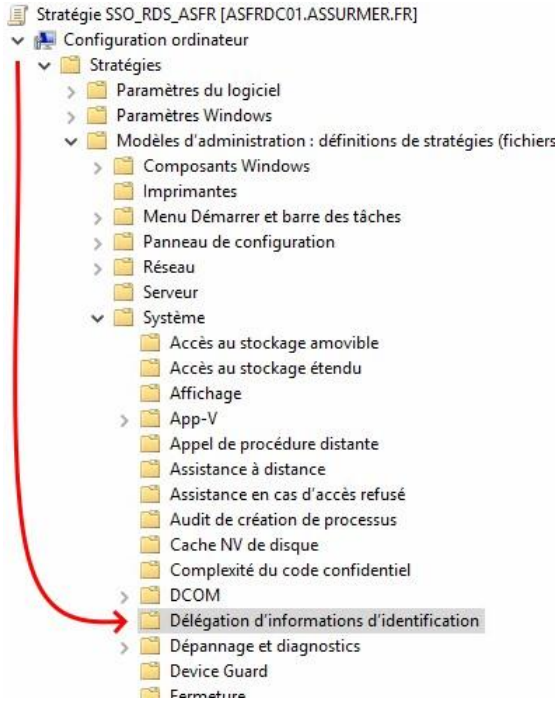


- Nommer la GPO et cliquer sur « OK ».

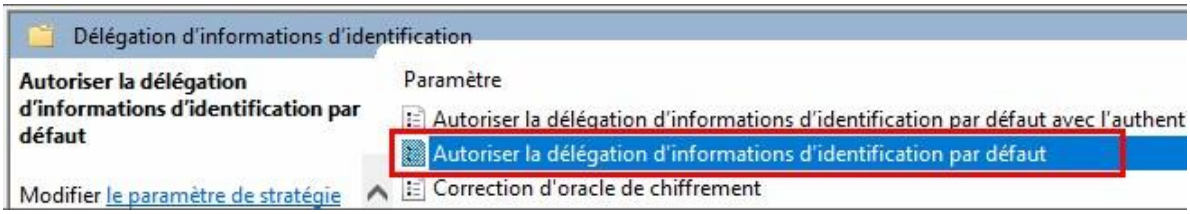


- Faire clic droit sur la GPO puis la modifier.

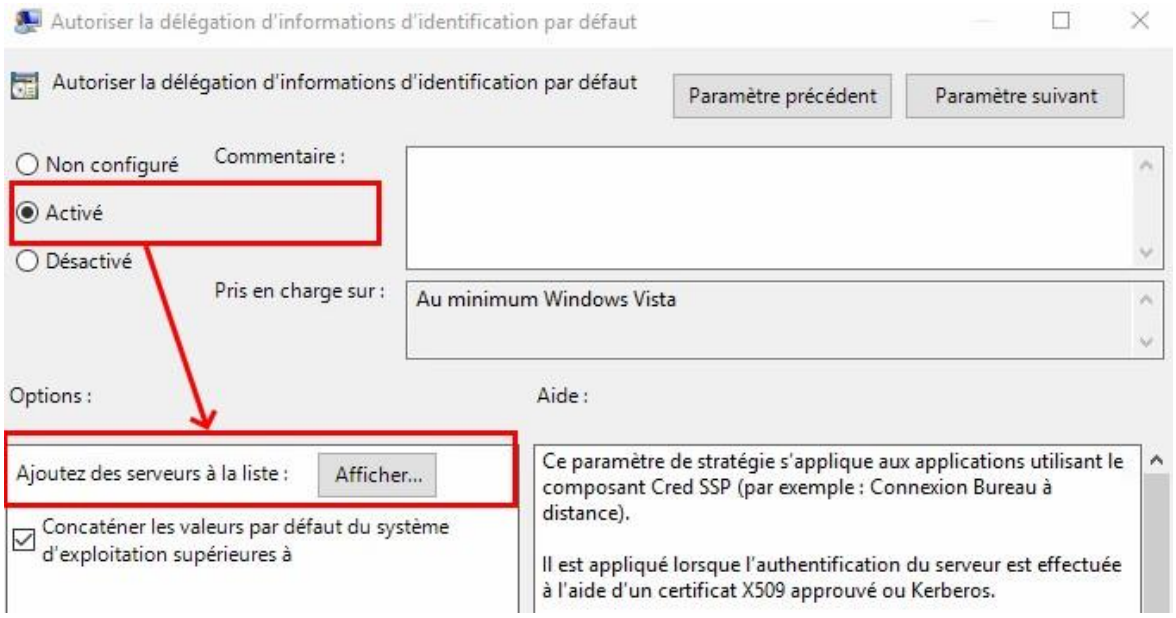
- Se rendre à l'emplacement suivant : Configuration ordinateur / Stratégies / Modèles d'administrations / Système / Délégation d'informations d'identification.



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

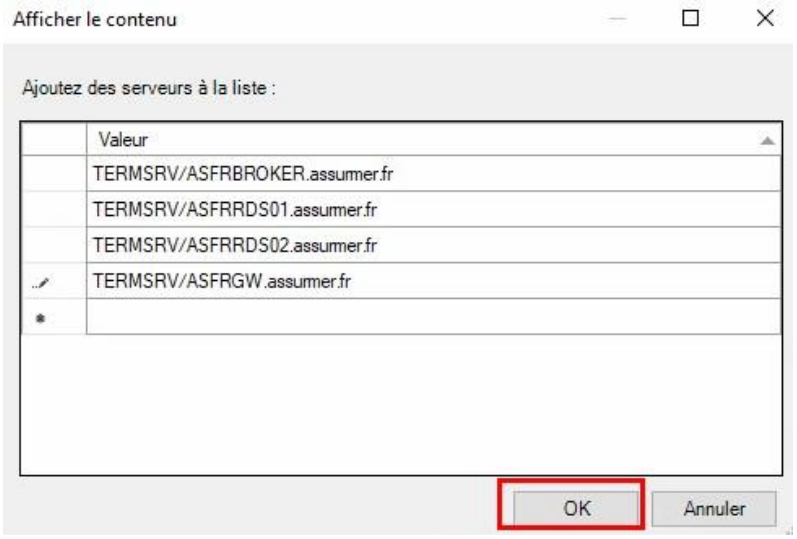


- Cliquer sur la coche « Activé » puis sur « Afficher ».

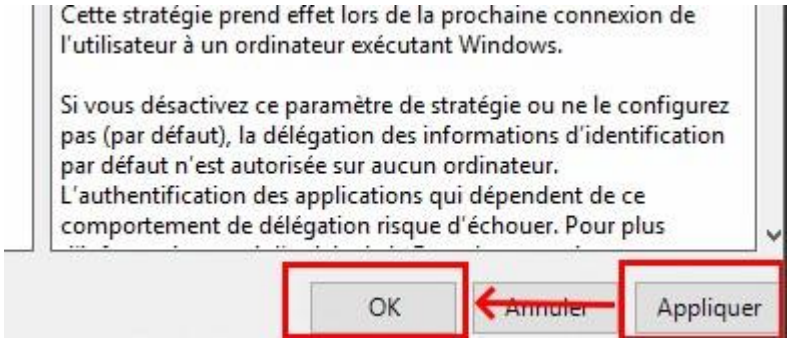


- Ajouter les serveurs sur lesquels il faut activer le SSO. Puis cliquer sur « OK ».

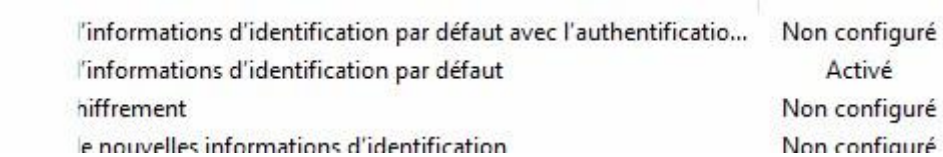
- TERMSRV//server.assurmer.fr



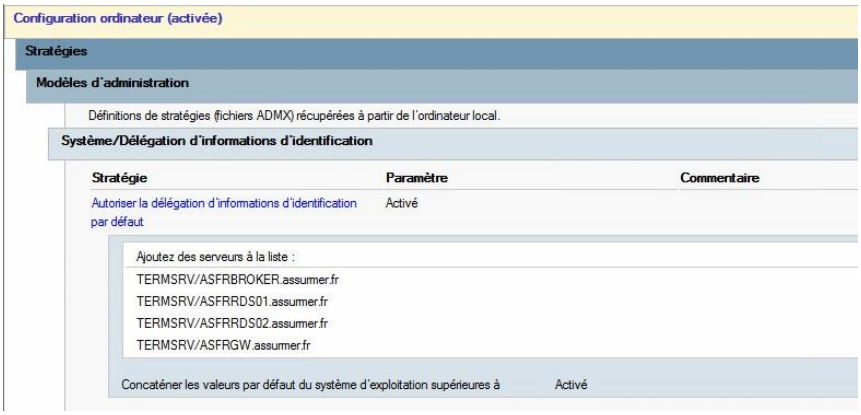
- Cliquer sur « Appliquer » puis « OK ».



- Le paramètre est activé.



Résumé de la stratégie :



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

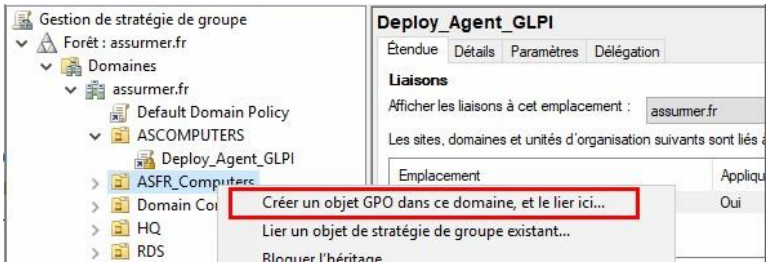
2. Raccourcis WEB et RDP

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.

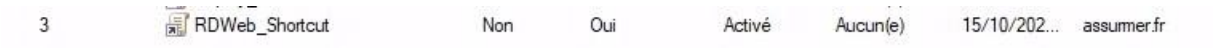
a) Configuration du raccourci

- 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 ».

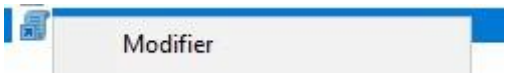


- Nommer la GPO et cliquer sur « OK ».

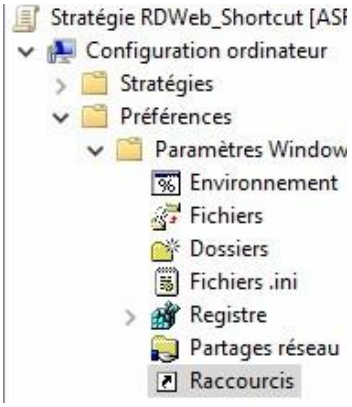


- Lier la GPO à l'OU HQ des comptes utilisateurs également.

- Faire clic droit sur la GPO puis la modifier.

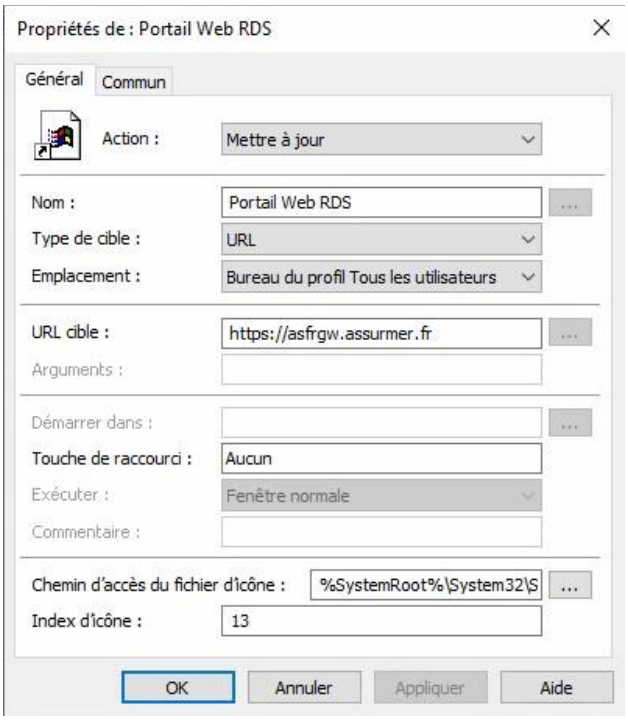


- Se rendre à l'emplacement suivant : Configuration ordinateur / Préférences / Paramètres Windows / Raccourcis.



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

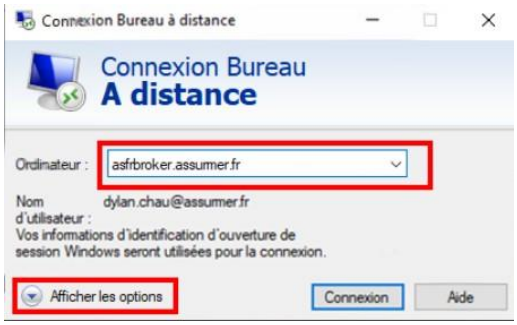
- Renseigner les informations du raccourci, cliquer sur « Appliquer » puis « OK ».



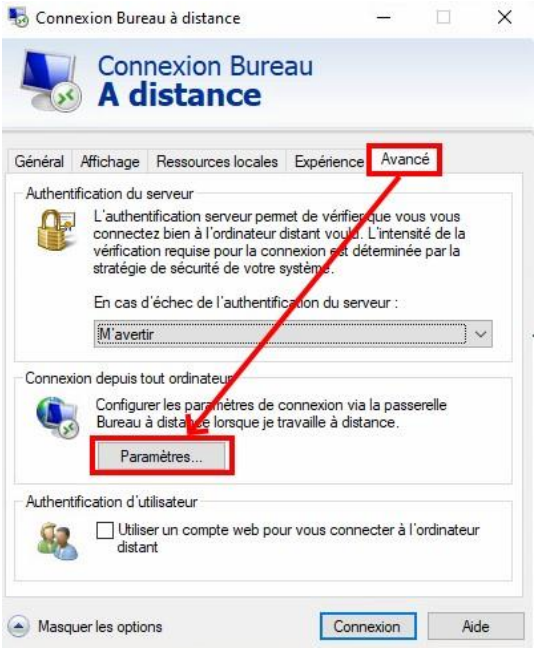
Nous allons également créer un raccourci rdp pour le Broker (qui redistribuera les sessions vers les serveurs RDS) qui fonctionnera en parallèle avec la GPO SSO.

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

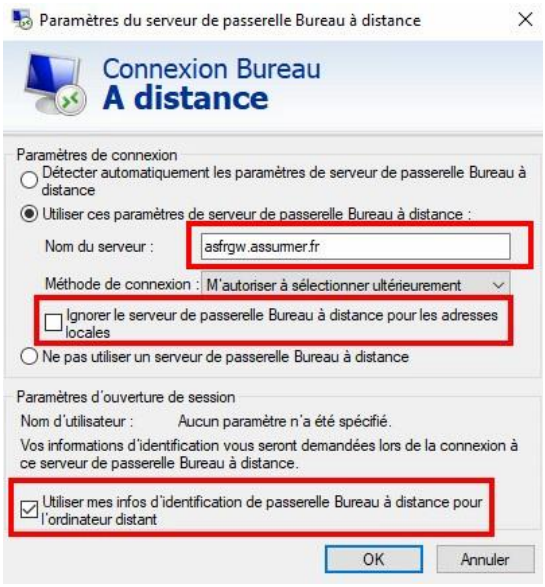
- Lancer le client sur le Filer, entrer l'alias broker et cliquer sur « Options ».



- Cliquer sur « Avancé » puis « Paramètres ».

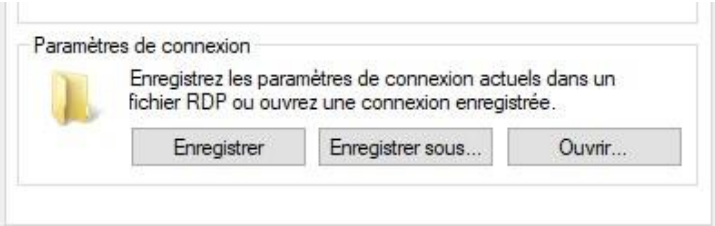


- Ajouter le serveur de passerelle Bureau à distance, décocher la case « Ignorer pour les adresses locales » et cocher la dernière case.



Cliquer sur « OK ».

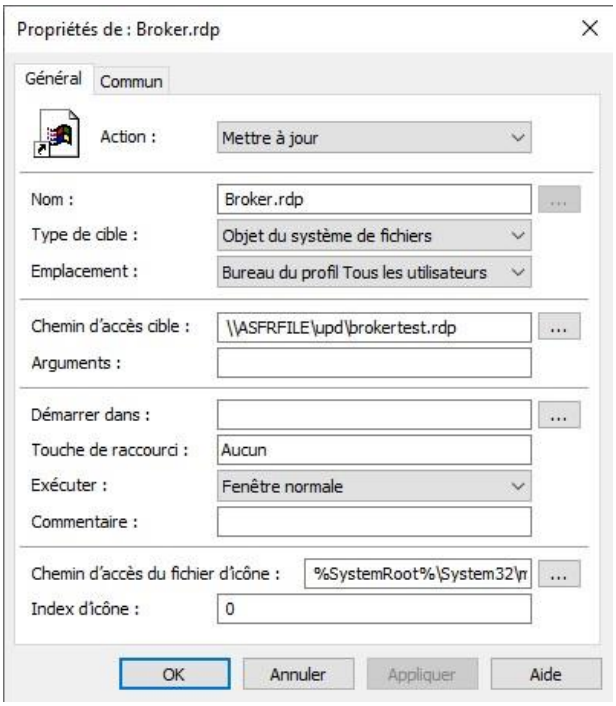
- Dans « Général », cliquer sur « Enregistrer sous » et placer le sur le serveur de fichiers.



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

- Rajouter les lignes :
    - **use redirection server name:i:1** au lieu de **use redirection server name:i:0** ○ 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.

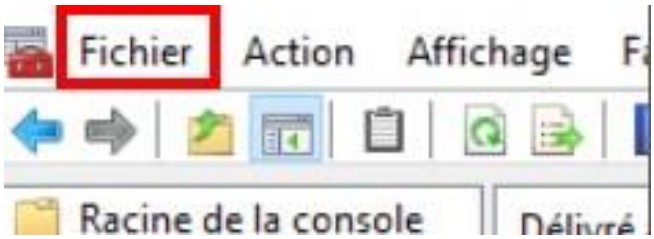
-

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).

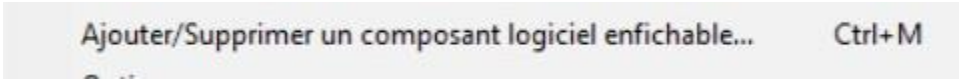
Nous allons donc exporter le certificat ne contenant que la clé publique.

a) Exportation du certificat

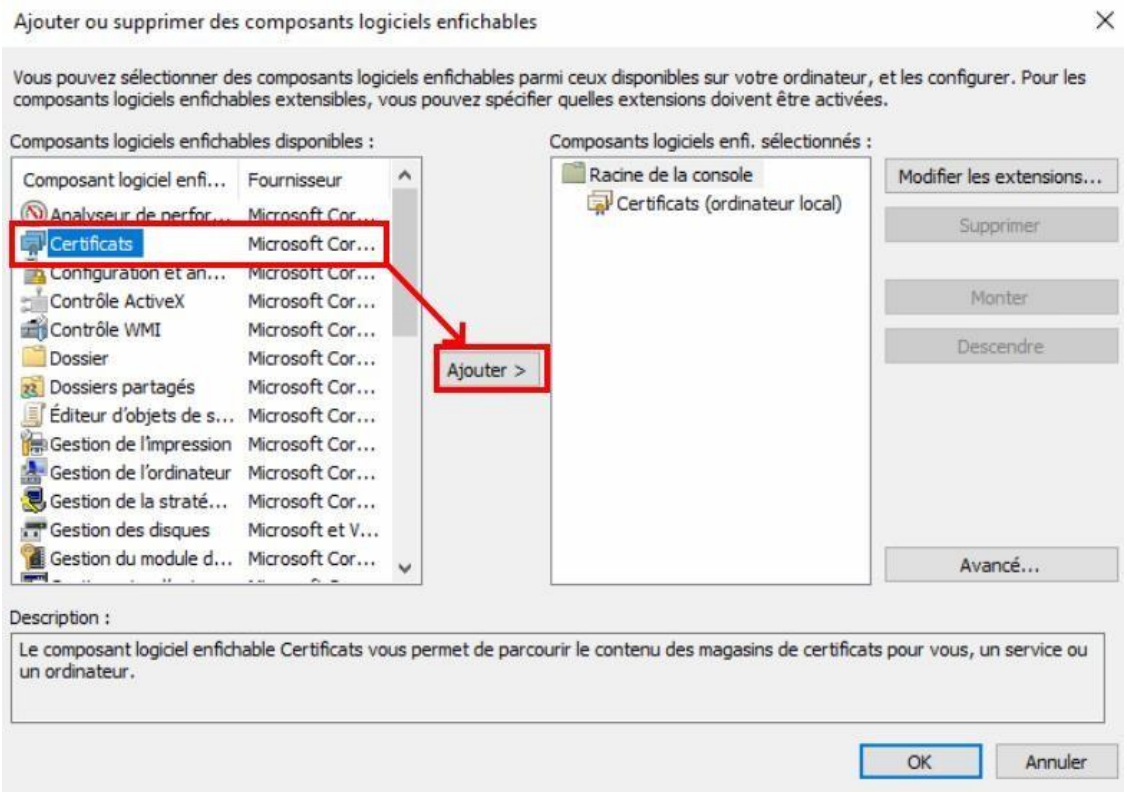
- Sur les serveurs contenant les certificats .pfx, ouvrir la console MMC de gestion de certificat sur l'ordinateur local et aller sur le magasin où est stocké le certificat. - Cliquer sur « Fichier ».



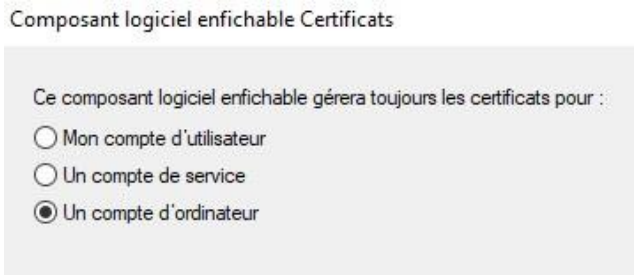
- Cliquer sur « Ajouter/Supprimer un composant logiciel enfichable… »



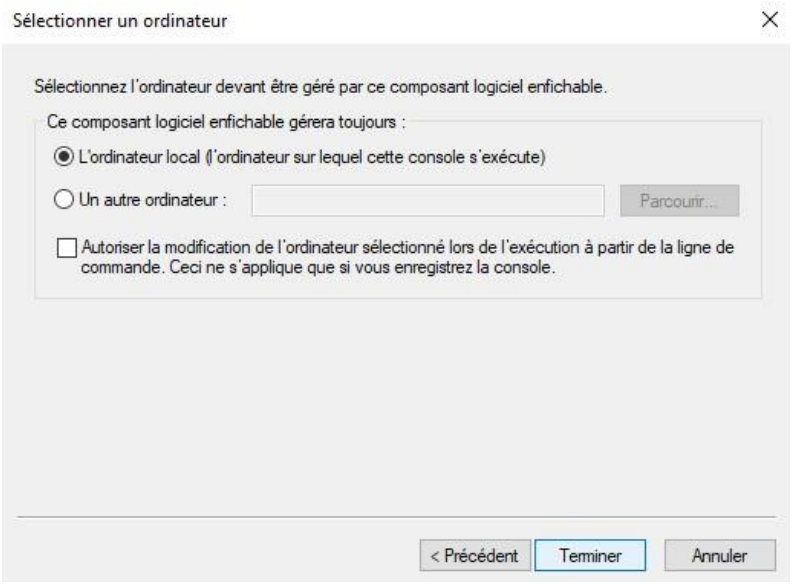
- Choisir Certificats puis l'ajouter.



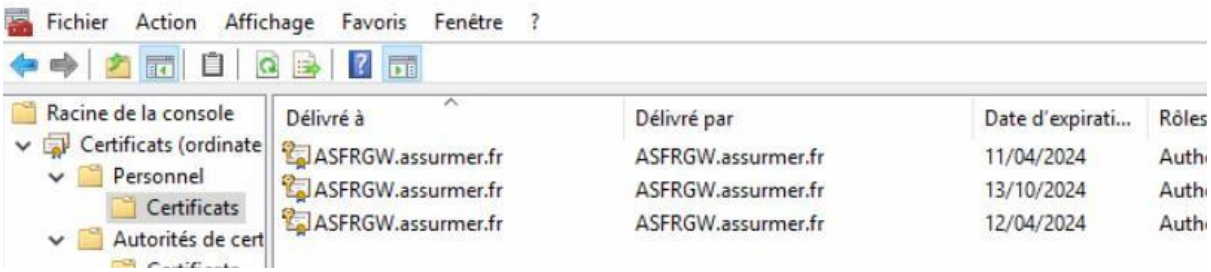
Choisir « Un compte d'ordinateur ».



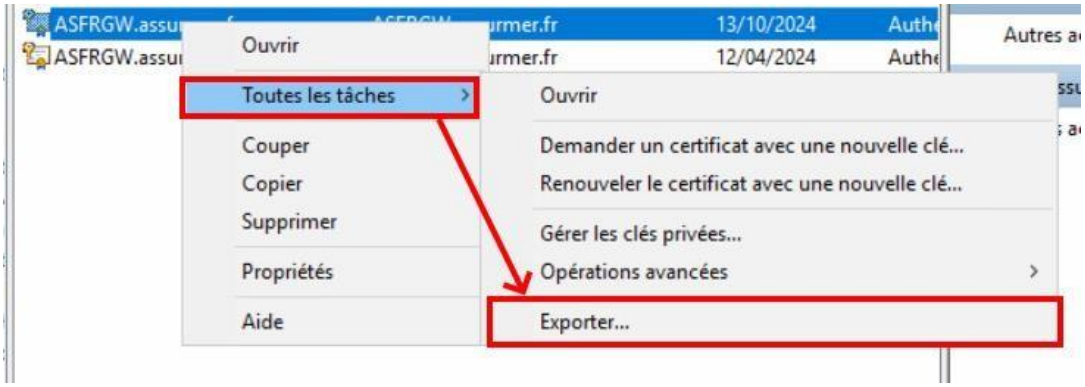
- Sélectionner « l'ordinateur local » puis cliquer sur « Terminer ».



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

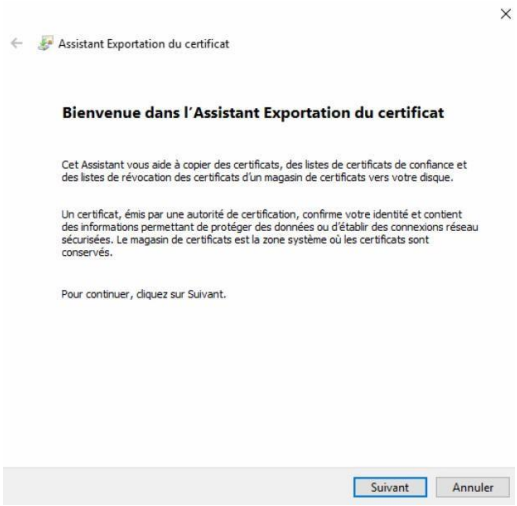


- Faire clic droit sur le certificat, puis aller sur « Toutes les tâches » et « Exporter ».



-

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

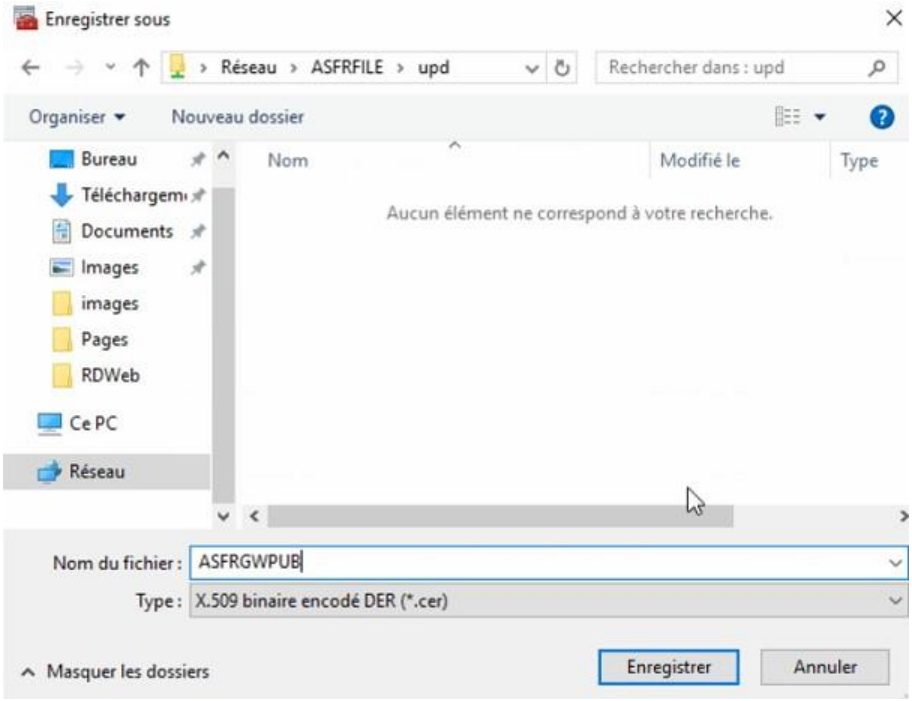


- Laisser « Non ne pas exporter la clé privée » (le certificat ne contiendra que la clé publique).

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

-

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



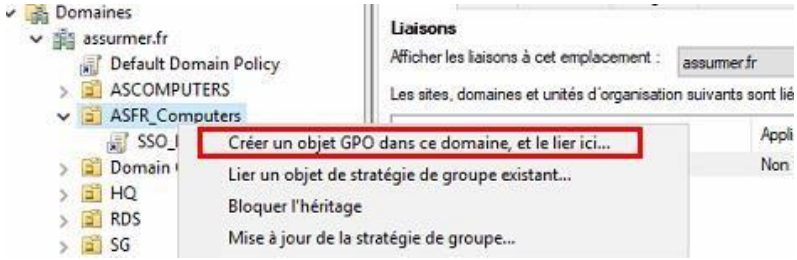
- Cliquer sur « Terminer ».
- Réitérer l'opération pour le certificat du Broker.
- Nos certificats avec clé publique sont bien créés sur ASFRFILE.

b)

Création de la GPO

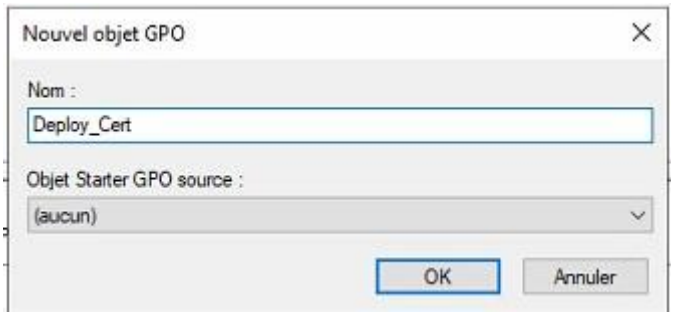
- Se rendre sur la console de Gestion des stratégies de groupe.

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



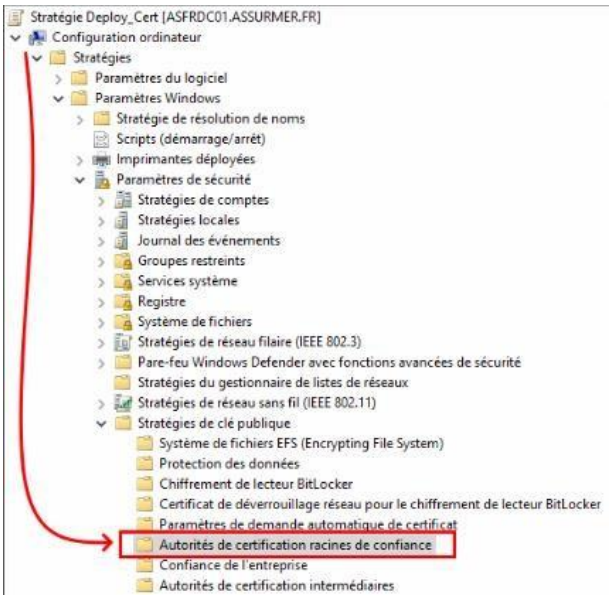
-

Nommer la stratégie.



- Faire clic droit sur la stratégie puis « Modifier ».

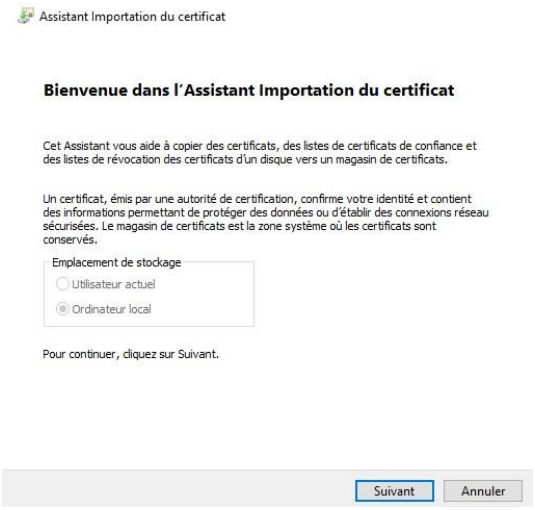
- Aller au paramètre de « Autorités de certification racines de confiance » qui se trouve dans : Configuration ordinateur / Stratégies / Paramètres Windows / Paramètres de sécurité / Stratégie de clé publique.



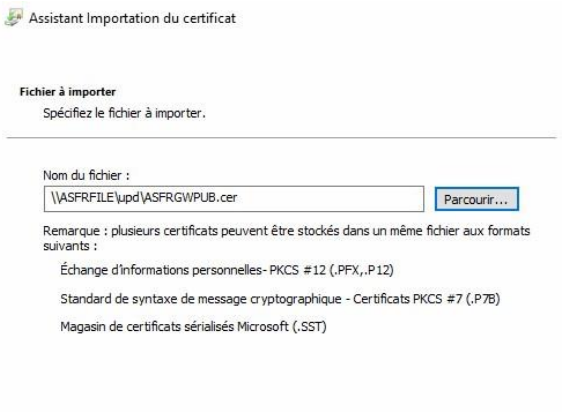
- Faire clic droit et cliquer sur « Importer ».

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

-

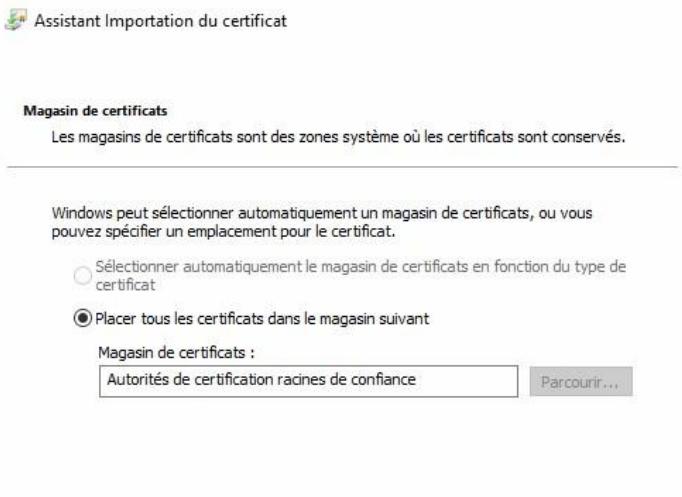


- Cliquer sur « Parcourir » et ajouter le certificat.



- Cliquer sur « Suivant ».

- Laisser le magasin et cliquer sur « Suivant ».



Cliquer sur « Terminer ».

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

Paramètres de la stratégie :

4. Page Web personnalisée Assurmer

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

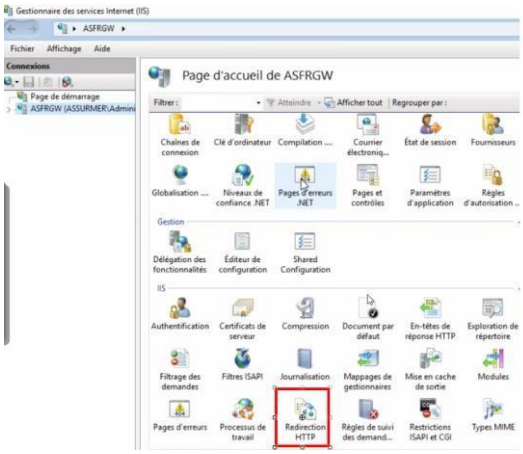
a) Changement du texte « Work Resources »

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

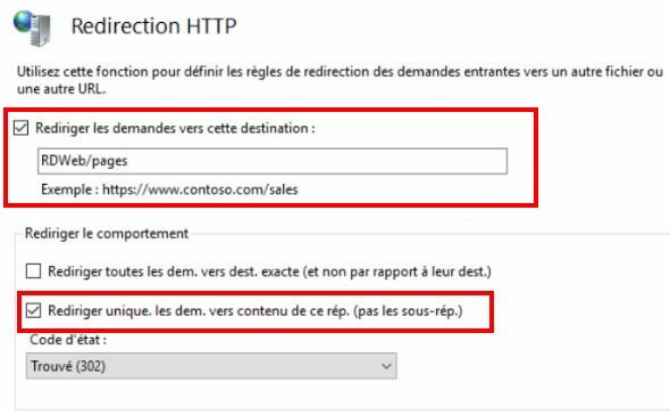
```
PS C:\Users\Administrateur.ASSURMER> Set-RDWorkspace -Name "Assurmer RD Workspace"
```

b) Ajout d'une redirection automatique vers RDWeb

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



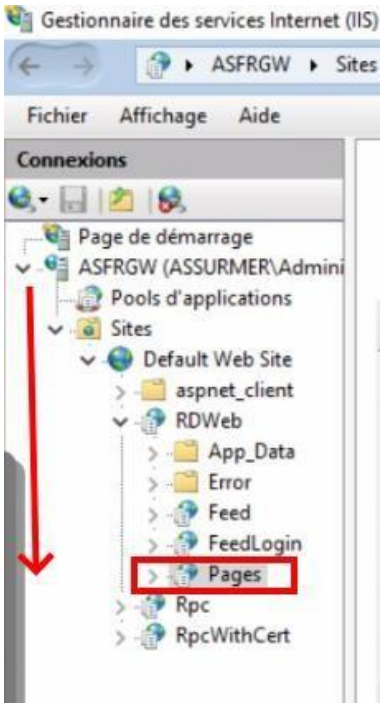
- Ajouter la redirection et cocher la case « Rediriger unique. les dem. vers contenu de ce rép. ».



- Cliquer sur « Appliquer ».

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

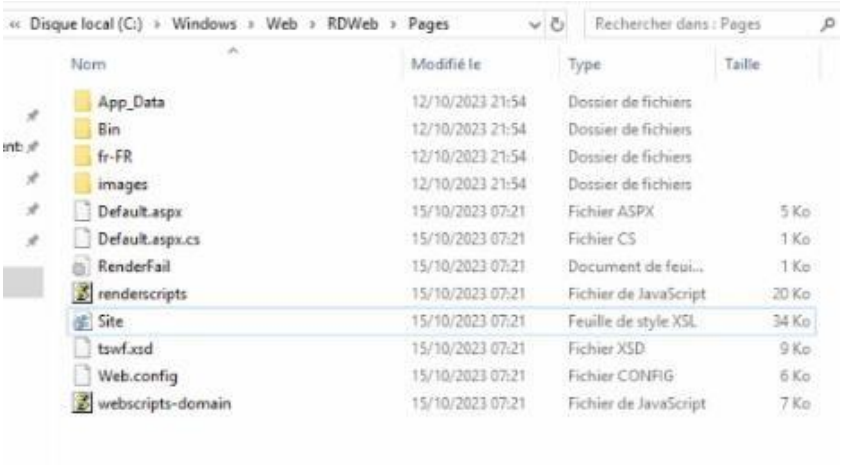
- Sur le gestionnaire des services Internet (IIS), dérouler le menu dans ASFRGW\Sites\Default Web Site\RDWeb\Pages



- Changer la valeur de PasswordChangeEnabled en « true ».

d) Modification des fichiers de la page

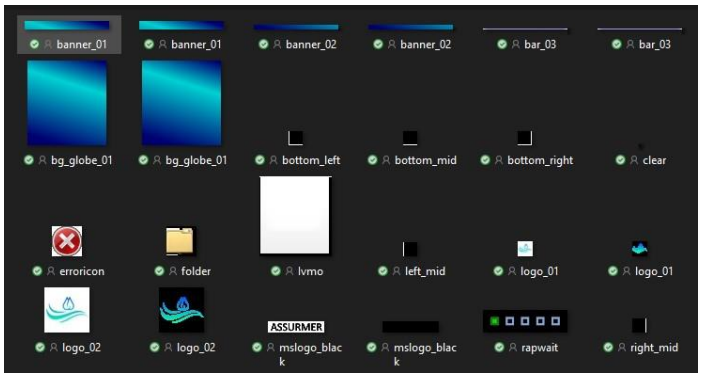
Sur le serveur ASFRGW directement, modifier les fichiers dans les chemins suivants à l'aide de Notepad++ ou du Bloc-notes :



- \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.xsl 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\RDWAStrings.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 :