

Compte rendu d'Installation d'un « Windows 2012R2 PKI »

Table des matières

Objectif(s) :.....	2
Légende :.....	2
Configuration principale :	3
Installation :.....	9
Configuration de l'installation :.....	14
Certificat racine :	21
Exporter le certificat racine :	26
Interface Web Certsrv :	29
Création d'un modèle de certificat :	29
Création d'un certificat SSL :	35
Configuration serveur IIS :	40
Navigation sur l'interface web :	42
Connexion certifié en TSE :	44

Objectif(s) :

Dans ce tutoriel, nous allons créer une autorité de certification racine d'entreprise (liée à l'Active Directory) et nous modifierons les stratégies de groupe pour que les clients de l'Active Directory reçoivent automatiquement le certificat de notre autorité de certification racine.

Ainsi, notre autorité sera reconnue par les ordinateurs clients et aucun avertissement ne s'affichera concernant nos certificats SSL.

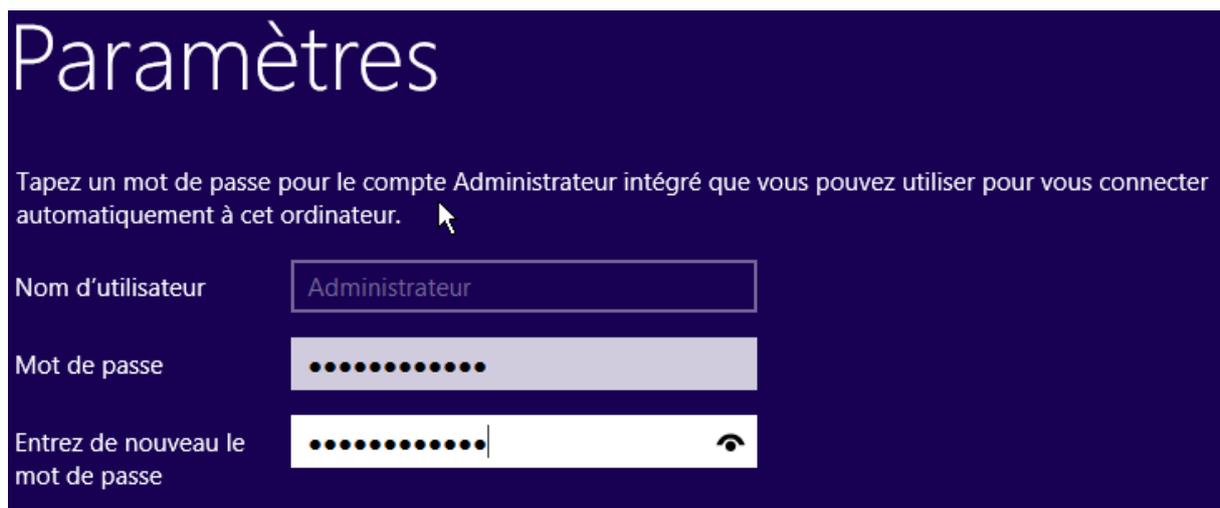
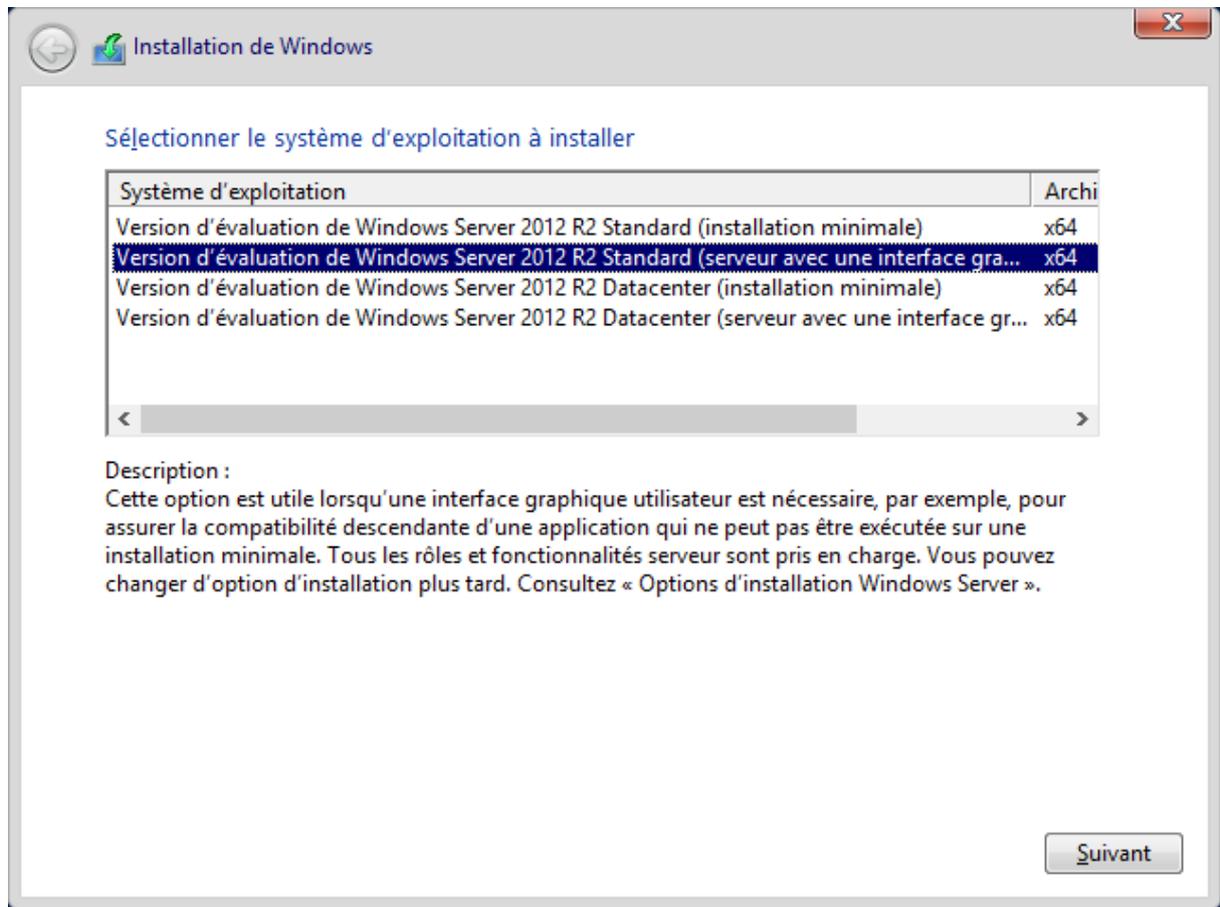
Légende :

- Les commandes ou les chemins (absolue/relatif) sont en gras, souligné et en italique ex :
 - *Apt-get update*
- Des captures d'écrans ont été prises afin de faciliter la compréhension du lecteur.

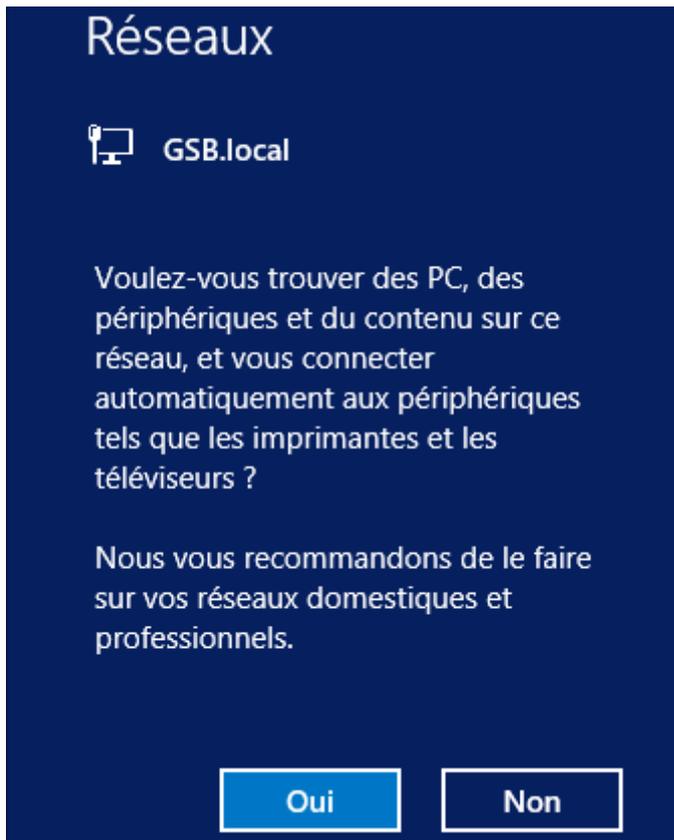
Machine	Os	Distribution	Version	C/S	IP
POSTE21	Windows R2	Windows	2012	S	192.168.1.143 W2012R2PKI

Configuration principale :

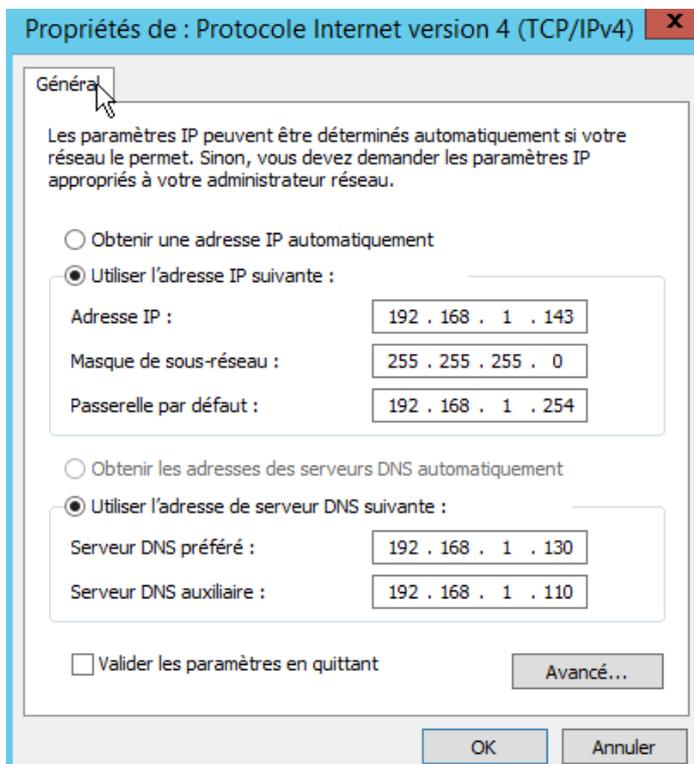
Installation du Système d'exploitation :



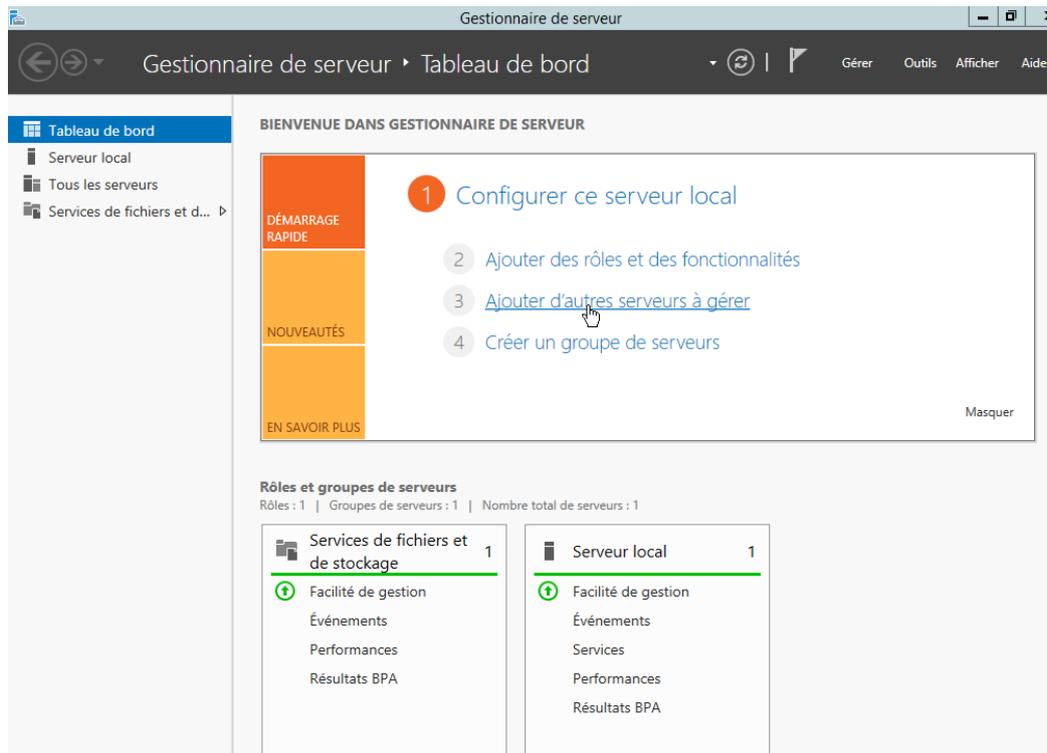
Password1234



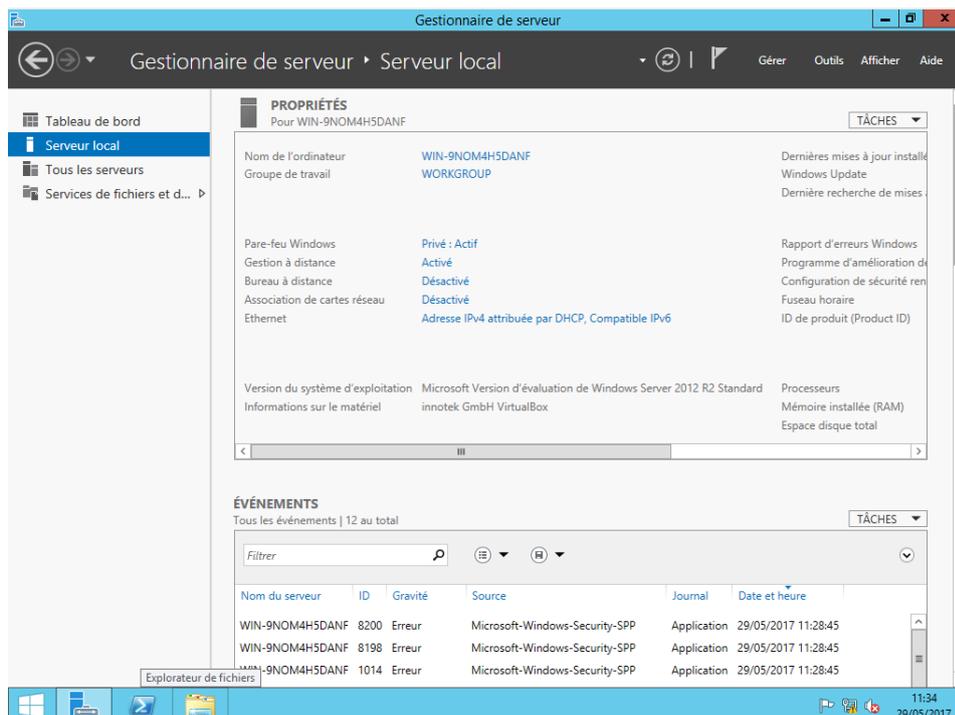
Nous allons ajouter le DNS de notre serveur LEBANNU 1 afin que notre serveur W2012R2PKI soit sur le domaine : GSB.local



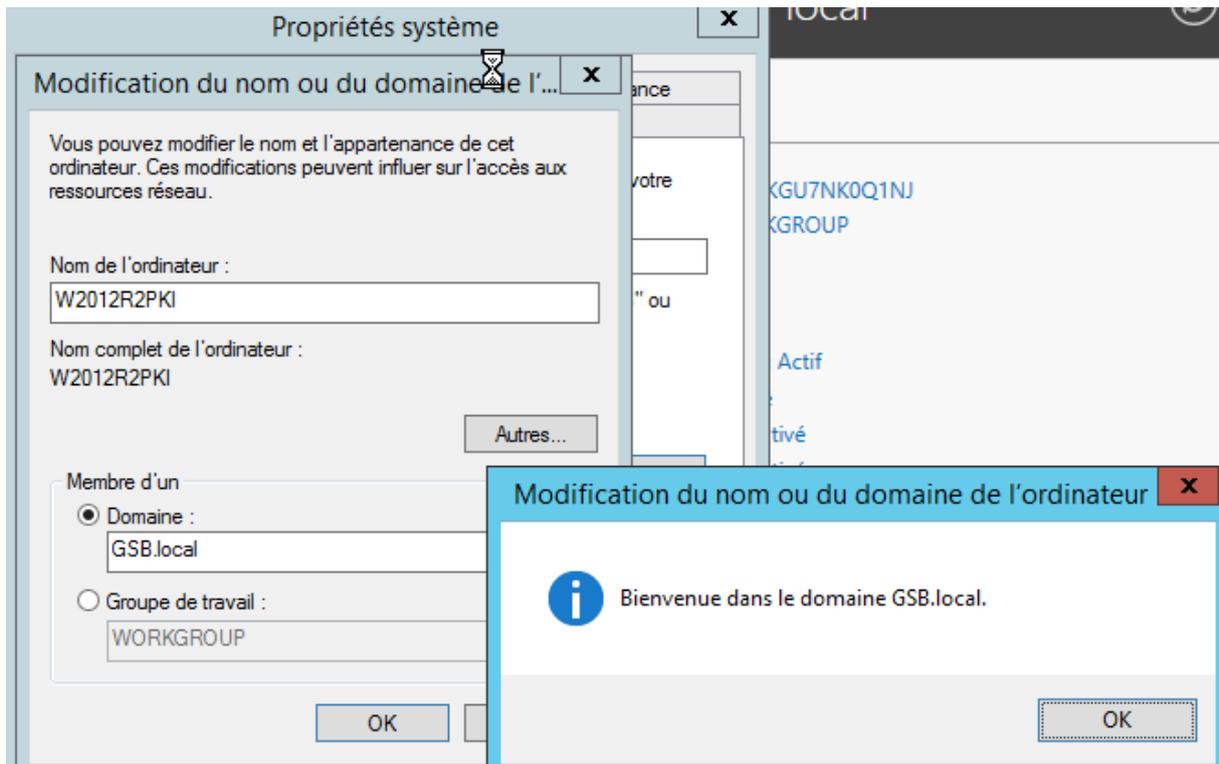
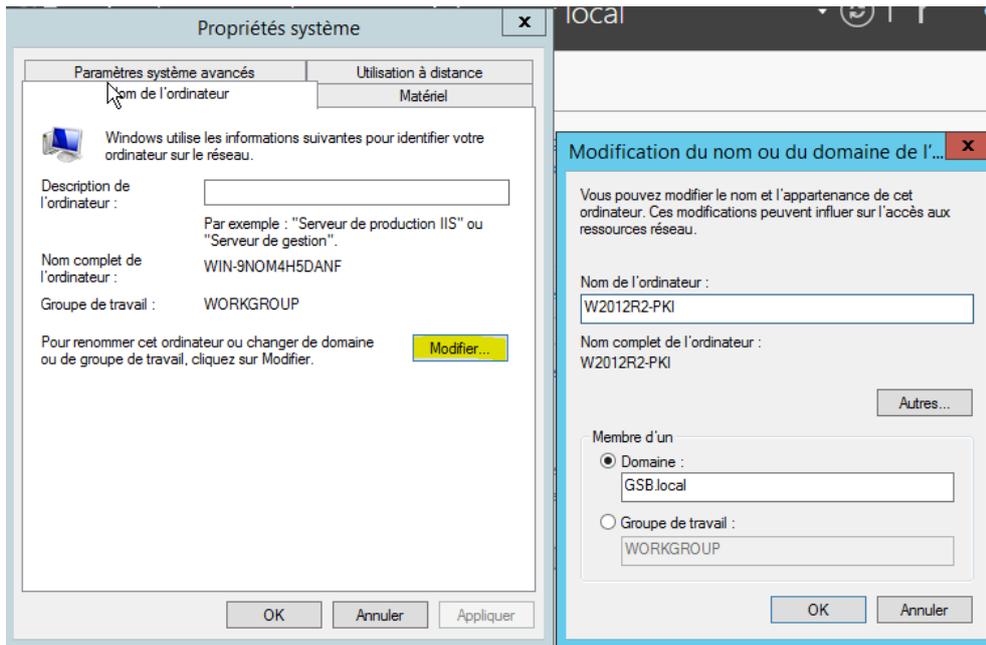
Voici le gestionnaire de serveur :



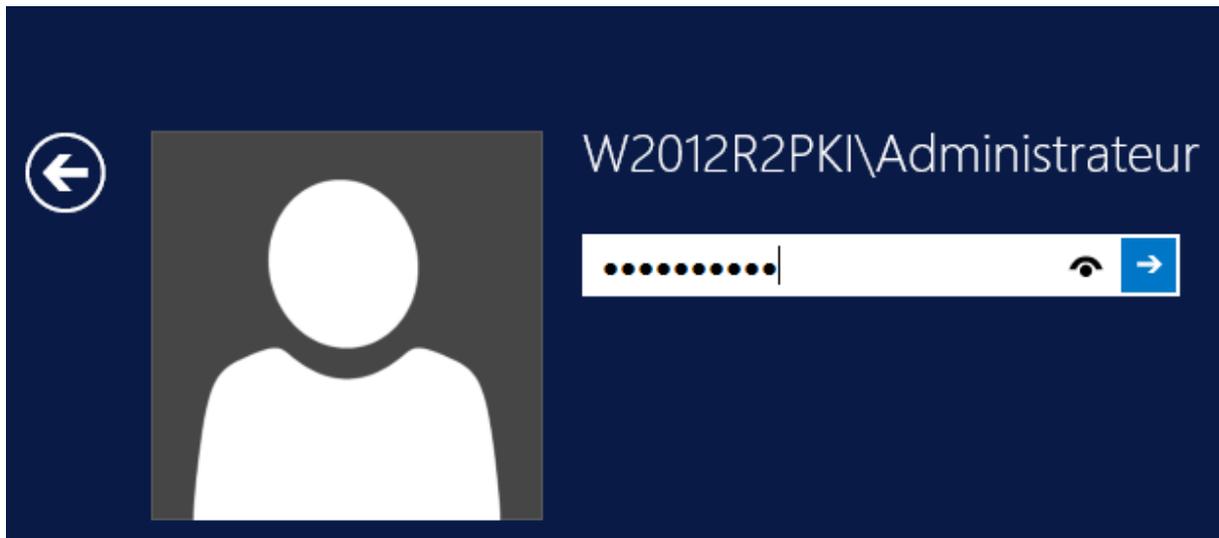
On va se diriger vers le serveur local afin de le configurer :



On va modifier le nom de la machine et inscrire la machine dans le domaine GSB.local :

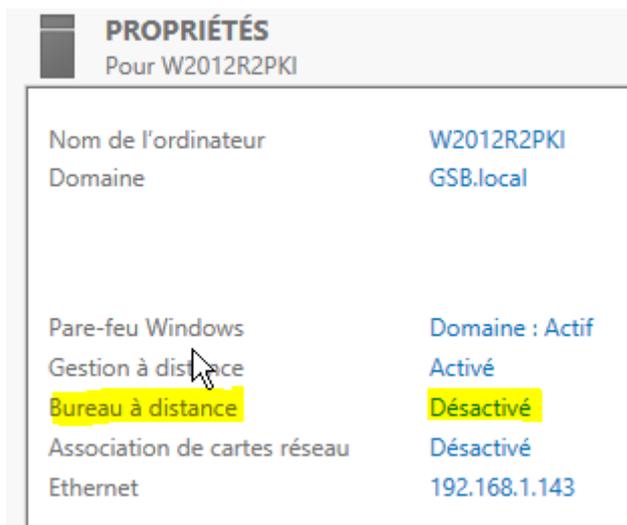


On va ensuite devoir redémarrer le PC afin de pouvoir mettre en place nos modifications.



Password1234

On va ensuite activer le bureau a distance afin d'avoir plus d'aisance :



Il suffit simplement de cliquer sur Désactivé en face de Bureau à distance, puis cliquer sur Autoriser comme ci-dessous.

Bureau à distance

Choisissez une option, puis spécifiez qui peut se connecter.

Ne pas autoriser les connexions à distance à cet ordinateur

Autoriser les connexions à distance à cet ordinateur

N'autoriser que la connexion des ordinateurs exécutant le Bureau à distance avec authentification NLA (recommandé)

[Comment choisir ?](#)

Propriétés du windows server 2012 :

PROPRIÉTÉS	
Pour W2012R2PKI	
Nom de l'ordinateur	W2012R2PKI
Domaine	GSB.local
Pare-feu Windows	Domaine : Actif
Gestion à distance	Activé
Bureau à distance	Activé
Association de cartes réseau	Désactivé
Ethernet	192.168.1.143

Installation :

On va maintenant ajouter le Rôle « Service de certificats Active Directory » Pour cela on va se connecter au serveur en Administrateur du domaine : GSB\Administrateur // Password123

Dans le gestionnaire de serveur, Ajouter des rôles et des fonctionnalités

BIENVENUE DANS GESTIONNAIRE DE SERVEUR

DÉMARRAGE RAPIDE

NOUVEAUTÉS

EN SAVOIR PLUS

- 1 Configurer ce serveur local
- 2 Ajouter des rôles et des fonctionnalités
- 3 Ajouter d'autres serveurs à gérer
- 4 Créer un groupe de serveurs

Cliquez sur suivant :

Assistant Ajout de rôles et de fonctionnalités

Avant de commencer

SERVEUR DE DESTINATION
W2012R2PKI.GSB.local

Avant de commencer

Type d'installation

Sélection du serveur

Rôles de serveurs

Fonctionnalités

Confirmation

Résultats

Cet Assistant permet d'installer des rôles, des services de rôle ou des fonctionnalités. Vous devez déterminer les rôles, services de rôle ou fonctionnalités à installer en fonction des besoins informatiques de votre organisation, tels que le partage de documents ou l'hébergement d'un site Web.

Pour supprimer des rôles, des services de rôle ou des fonctionnalités :
[Démarrer l'Assistant Suppression de rôles et de fonctionnalités](#)

Avant de continuer, vérifiez que les travaux suivants ont été effectués :

- Le compte d'administrateur possède un mot de passe fort
- Les paramètres réseau, comme les adresses IP statiques, sont configurés
- Les dernières mises à jour de sécurité de Windows Update sont installées

Si vous devez vérifier que l'une des conditions préalables ci-dessus a été satisfaite, fermez l'Assistant, exécutez les étapes, puis relancez l'Assistant.

Cliquez sur Suivant pour continuer.

Ignorer cette page par défaut

< Précédent Suivant > Installer Annuler

Cliquez de nouveau sur suivant :

Sélectionner le type d'installation

SERVEUR DE DESTINATION
W2012R2PKI.GSB.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le type d'installation. Vous pouvez installer des rôles et des fonctionnalités sur un ordinateur physique ou virtuel en fonctionnement, ou sur un disque dur virtuel hors connexion.

- Installation basée sur un rôle ou une fonctionnalité**
Configurez un serveur unique en ajoutant des rôles, des services de rôle et des fonctionnalités.
- Installation des services Bureau à distance**
Installez les services de rôle nécessaires à l'infrastructure VDI (Virtual Desktop Infrastructure) pour déployer des bureaux basés sur des ordinateurs virtuels ou sur des sessions.

< Précédent Suivant > Installer Annuler

Cliquez encore sur suivant :

Assistant Ajout de rôles et de fonctionnalités

Sélectionner le serveur de destination

SERVEUR DE DESTINATION
W2012R2PKI.GSB.local

Avant de commencer
Type d'installation
Sélection du serveur
Rôles de serveurs
Fonctionnalités
Confirmation
Résultats

Sélectionnez le serveur ou le disque dur virtuel sur lequel installer des rôles et des fonctionnalités.

- Sélectionner un serveur du pool de serveurs
- Sélectionner un disque dur virtuel

Pool de serveurs

Filtre :

Nom	Adresse IP	Système d'exploitation
W2012R2PKI.GSB.local	192.168.1.143	Microsoft Version d'évaluation de Windows Server 2012

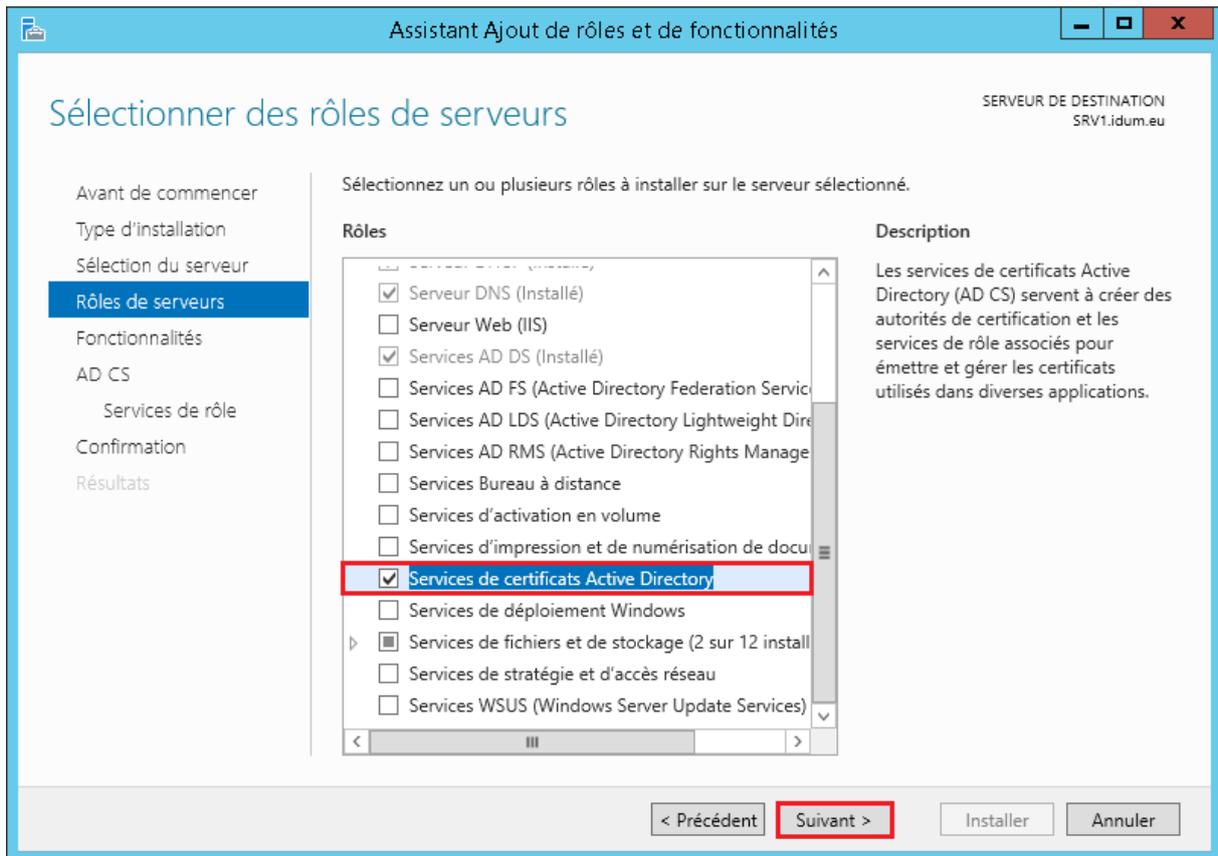
< ||| >

1 ordinateur(s) trouvé(s)

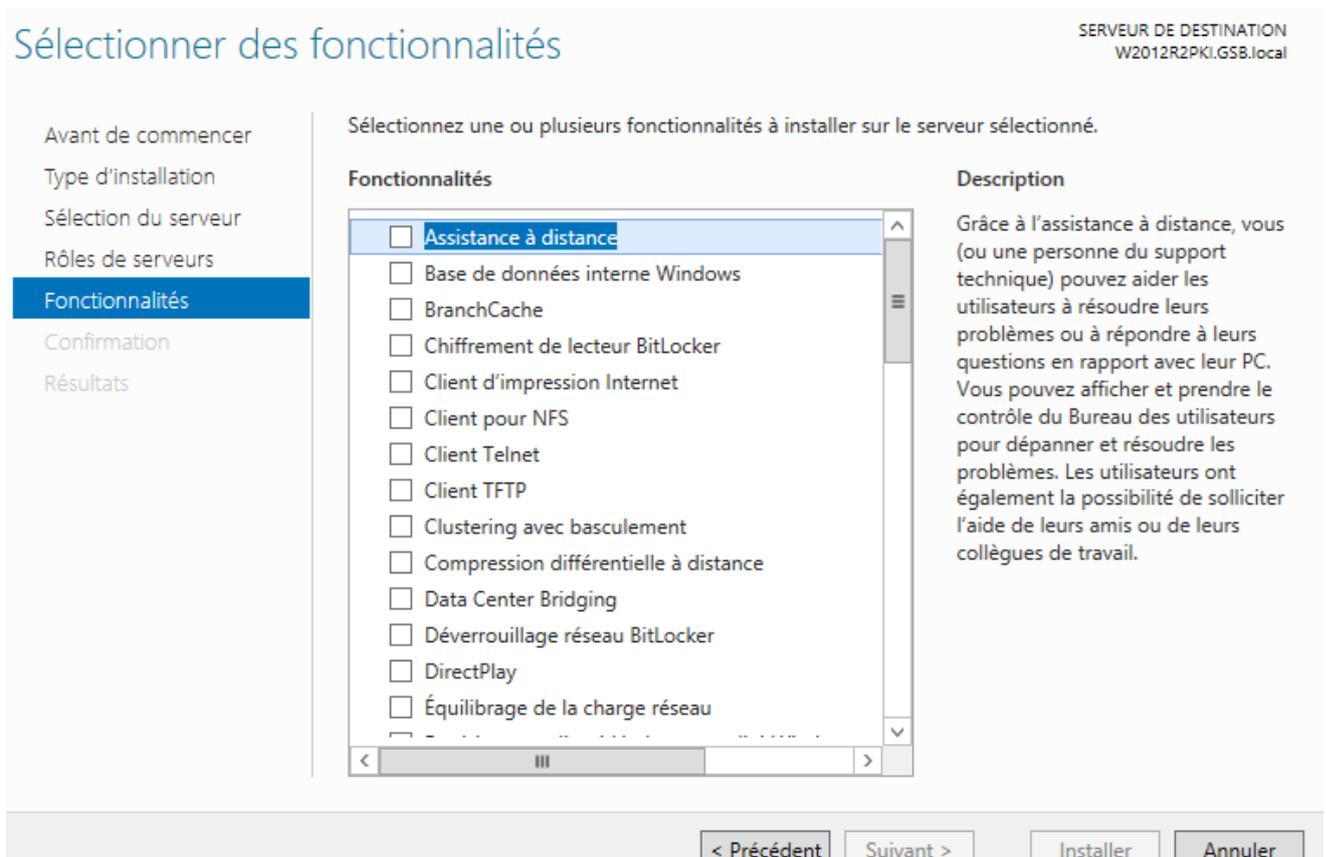
Cette page présente les serveurs qui exécutent Windows Server 2012 et qui ont été ajoutés à l'aide de la commande Ajouter des serveurs dans le Gestionnaire de serveur. Les serveurs hors ligne et les serveurs nouvellement ajoutés dont la collection de données est toujours incomplète ne sont pas répertoriés.

< Précédent Suivant > Installer Annuler

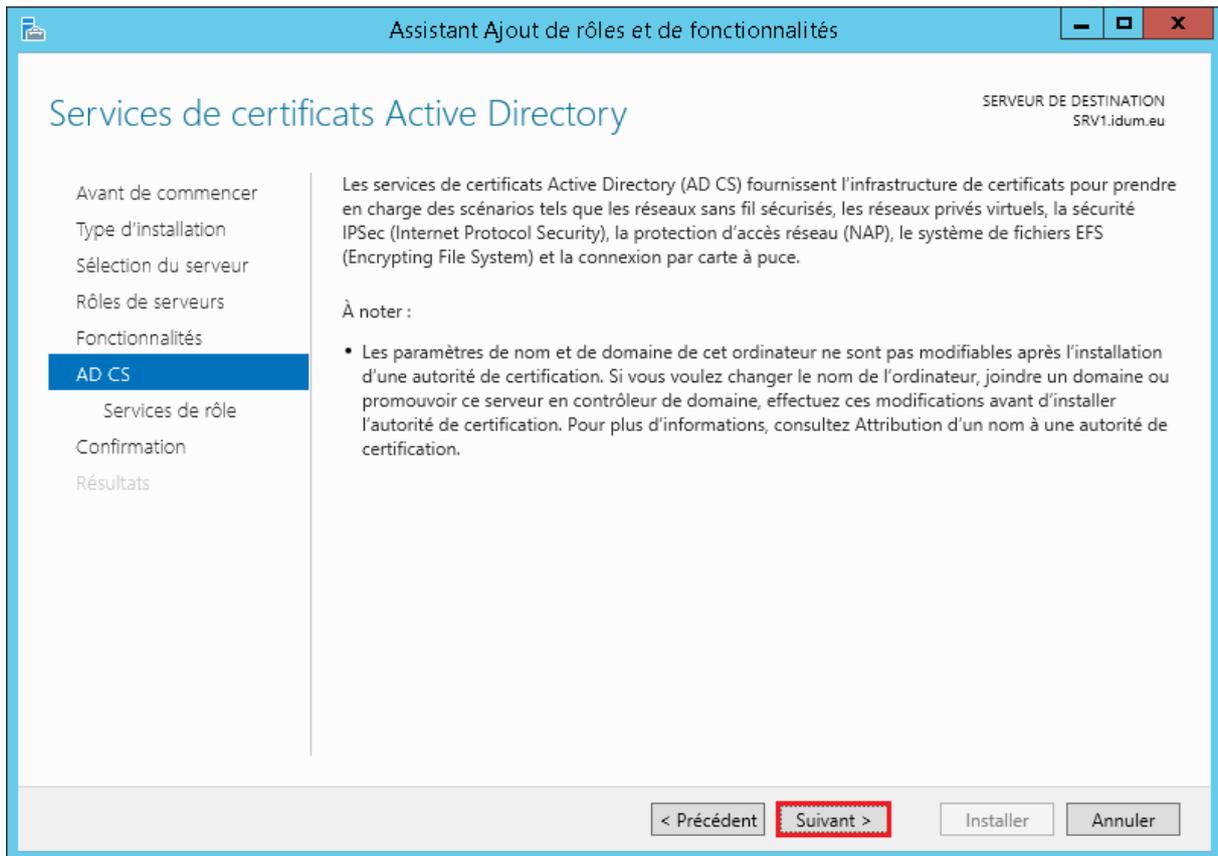
Cochez Service de certificats Active Directory, puis suivant :



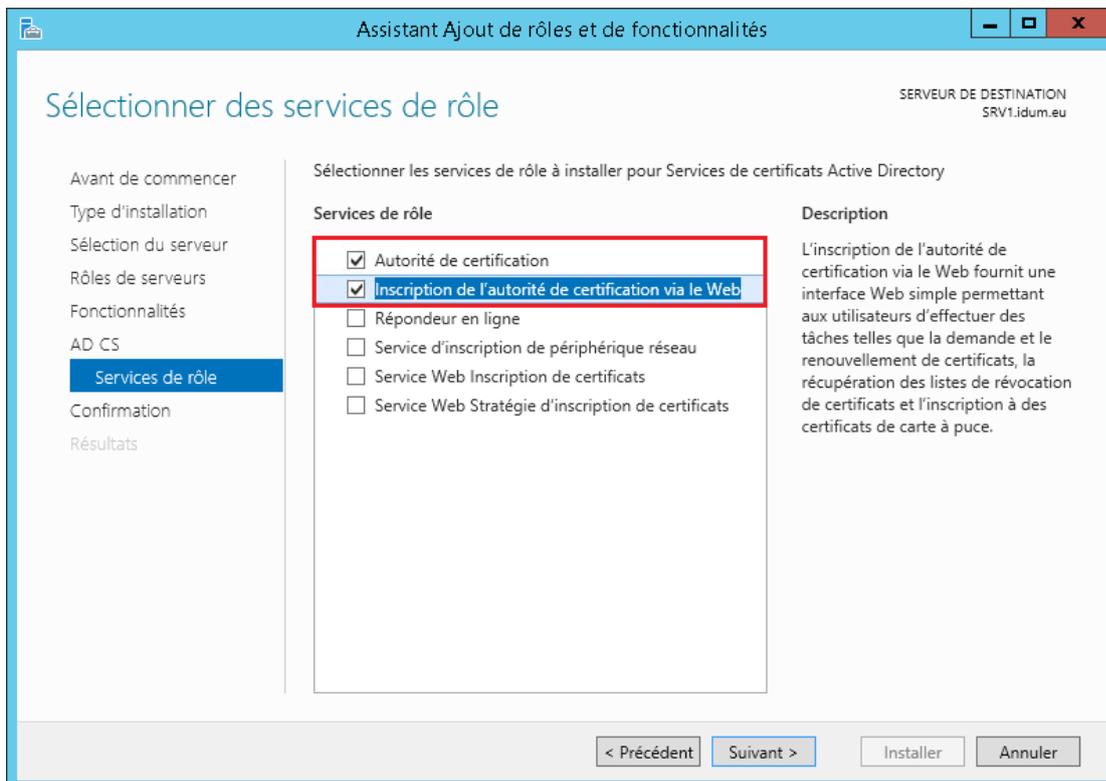
puis suivant :



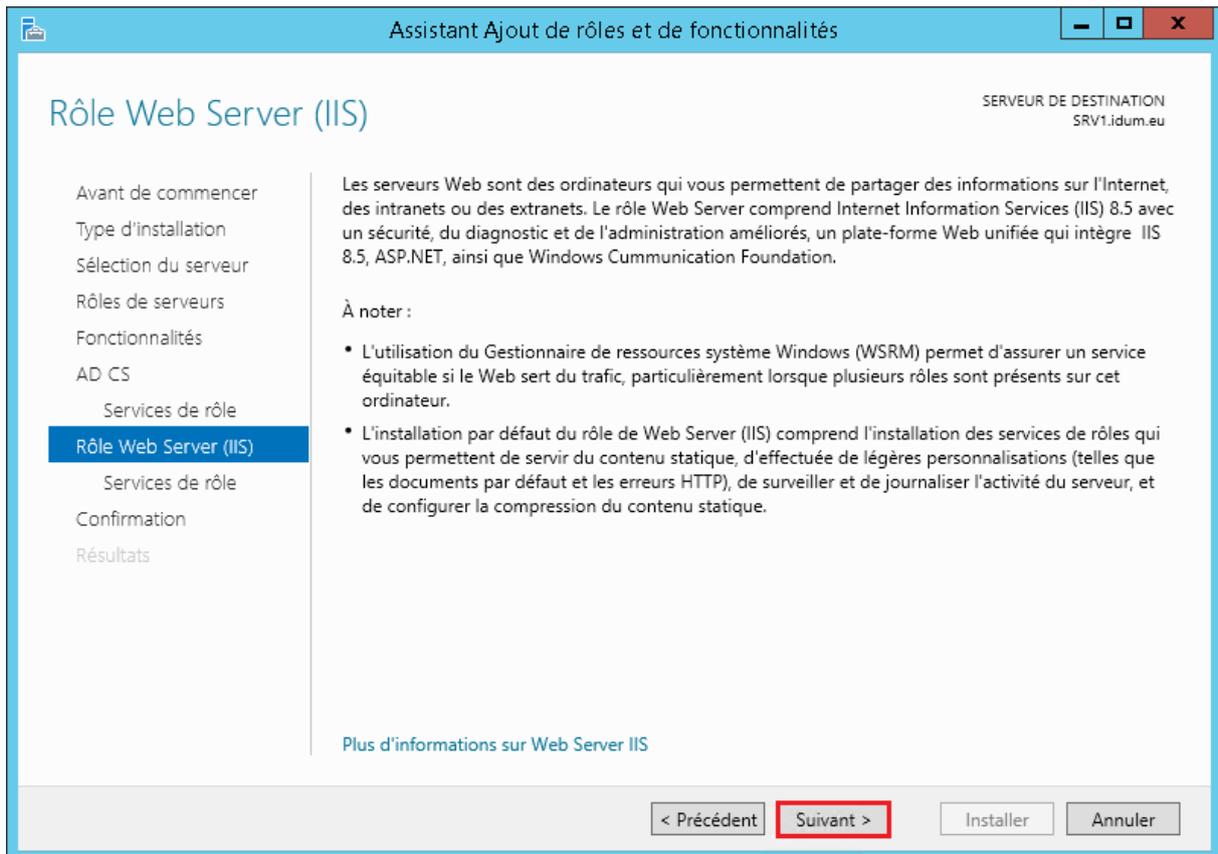
Puis suivant :



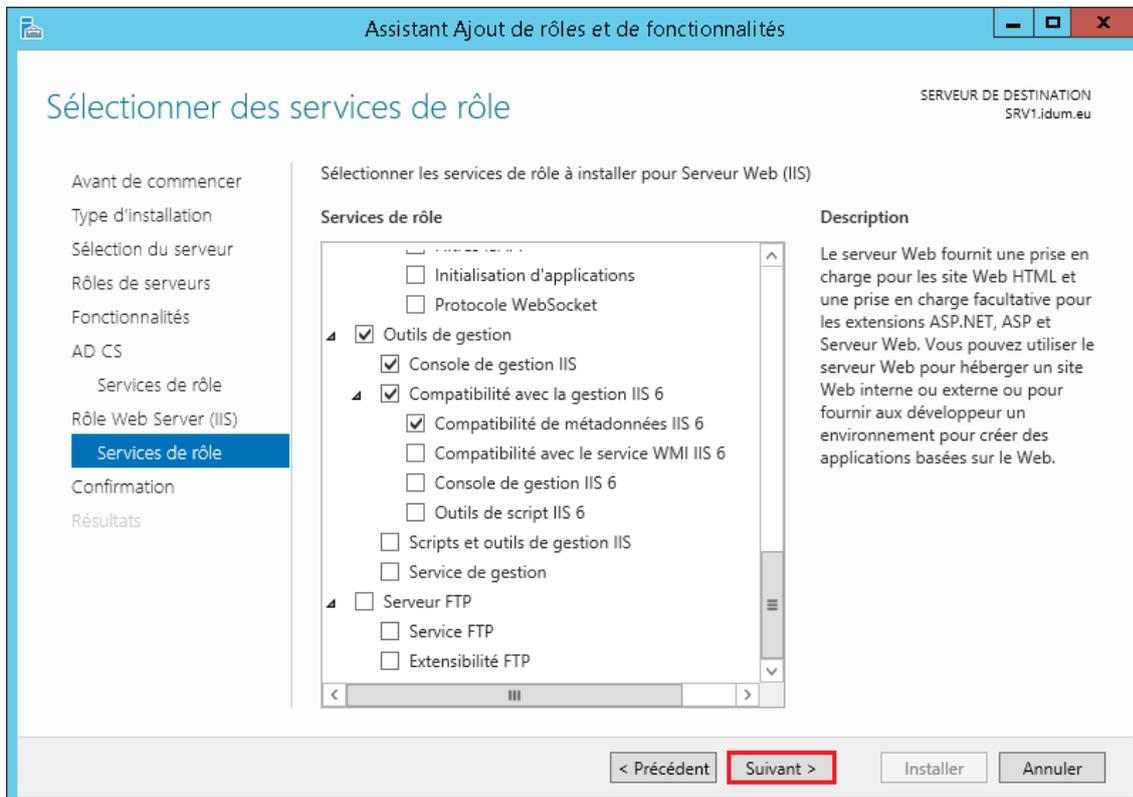
Cochez les options « Autorité de certification » et « Inscription de l'autorité de certification via le Web »



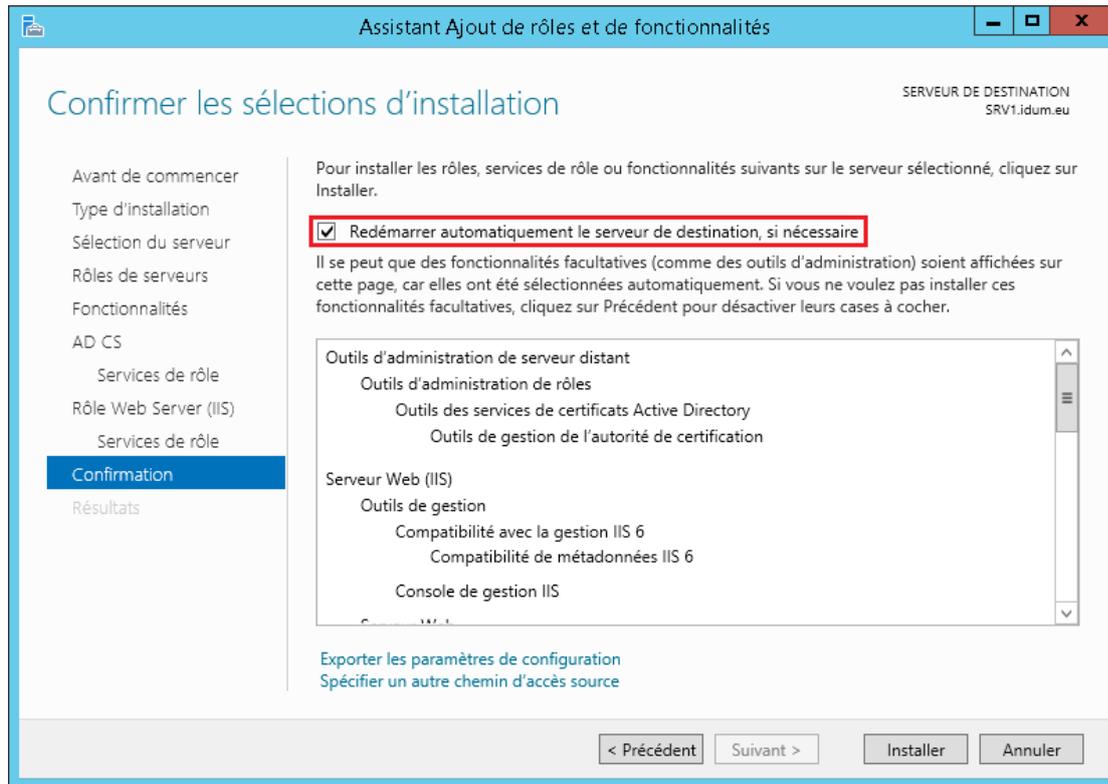
Puis suivant :



Cliquez sur suivant :

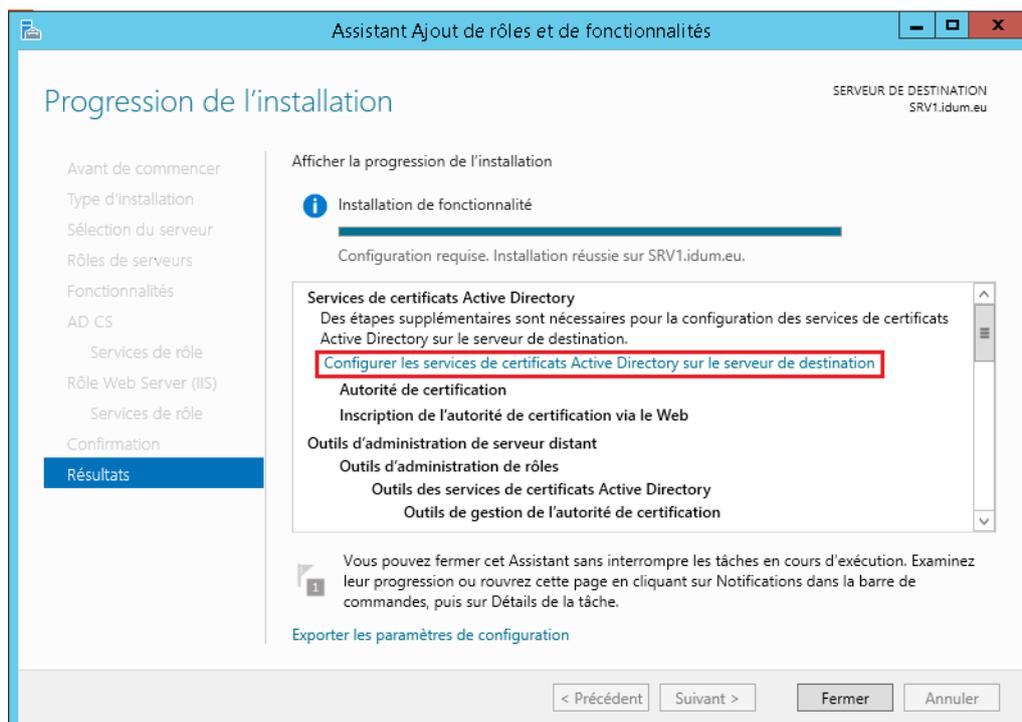


Cochez l'option « Redémarrer automatiquement le serveur de destination, si nécessaire », puis installer :

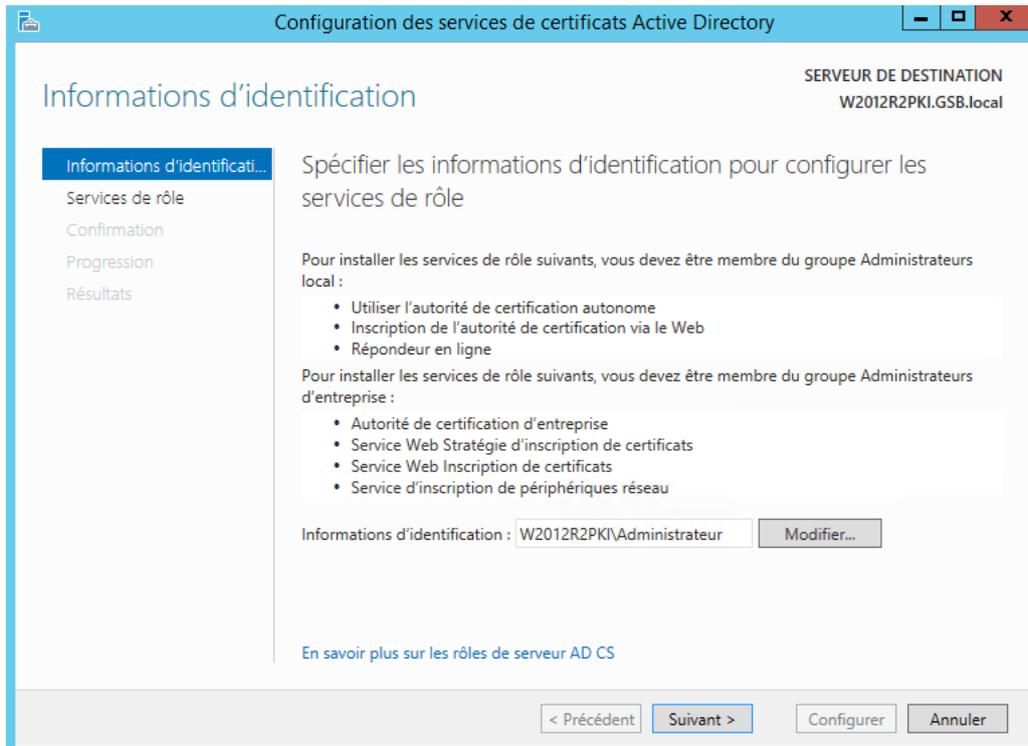


Configuration de l'installation :

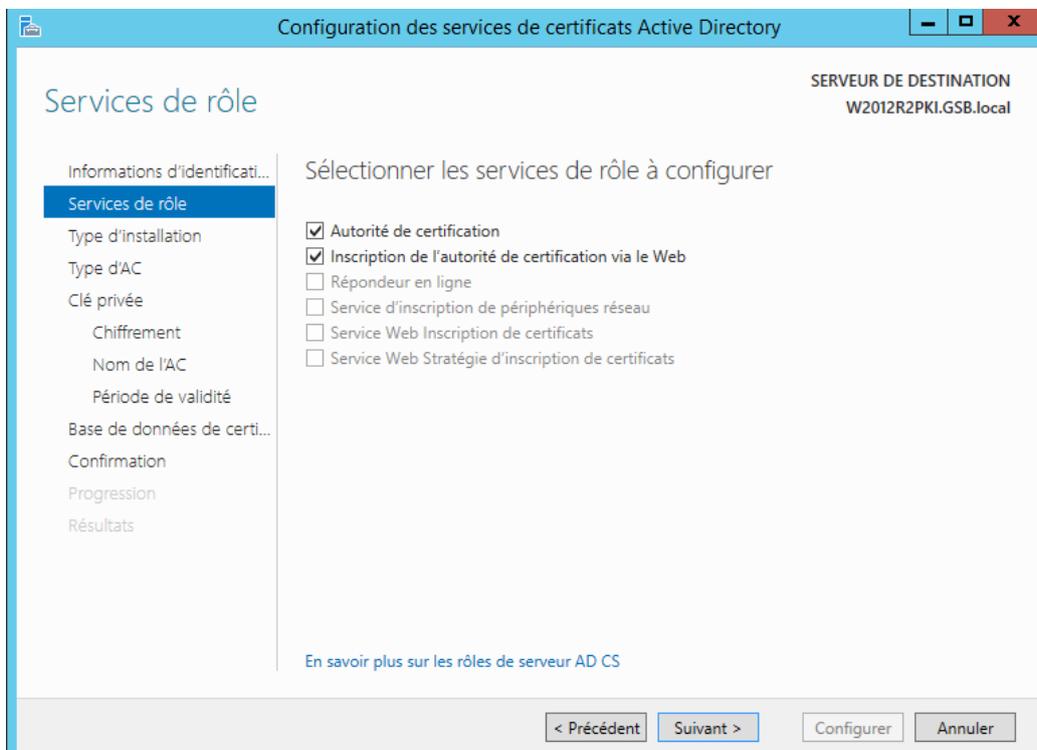
Cliquez sur le lien « Configurer les services de certificats Active Directory sur le serveur de destination »



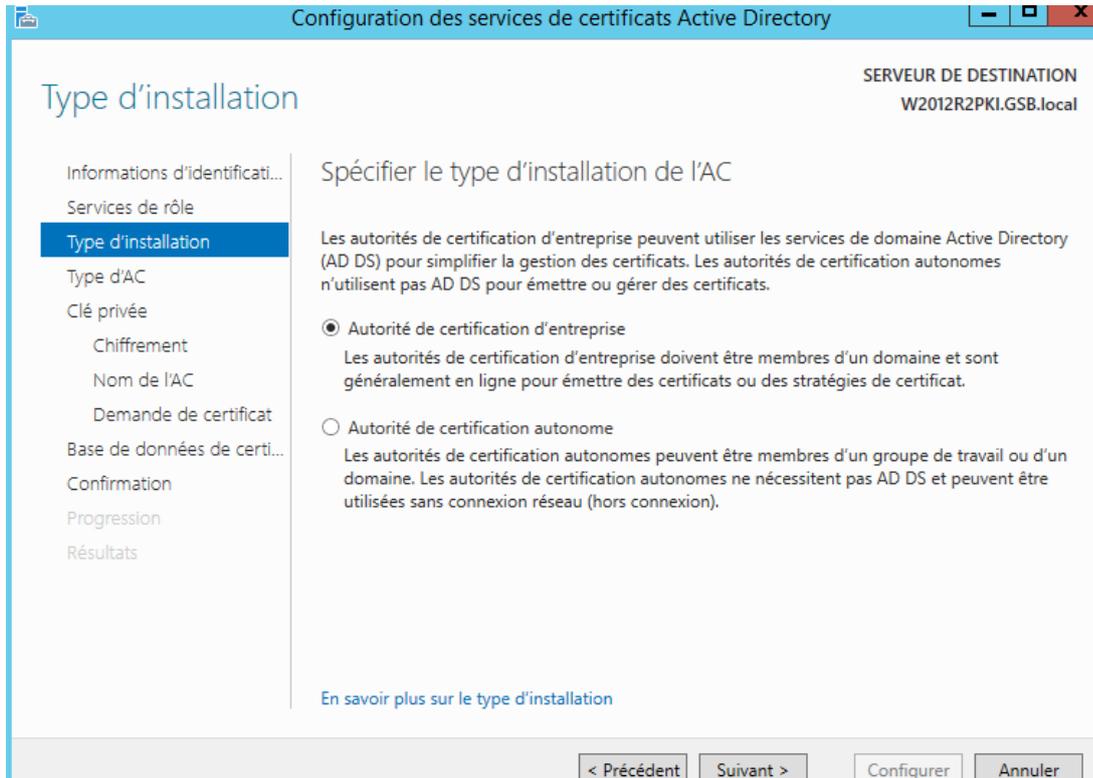
L'assistant de configuration vous demande ensuite de définir un compte avec les droits demandés pour continuer la configuration. Cliquez sur suivant :



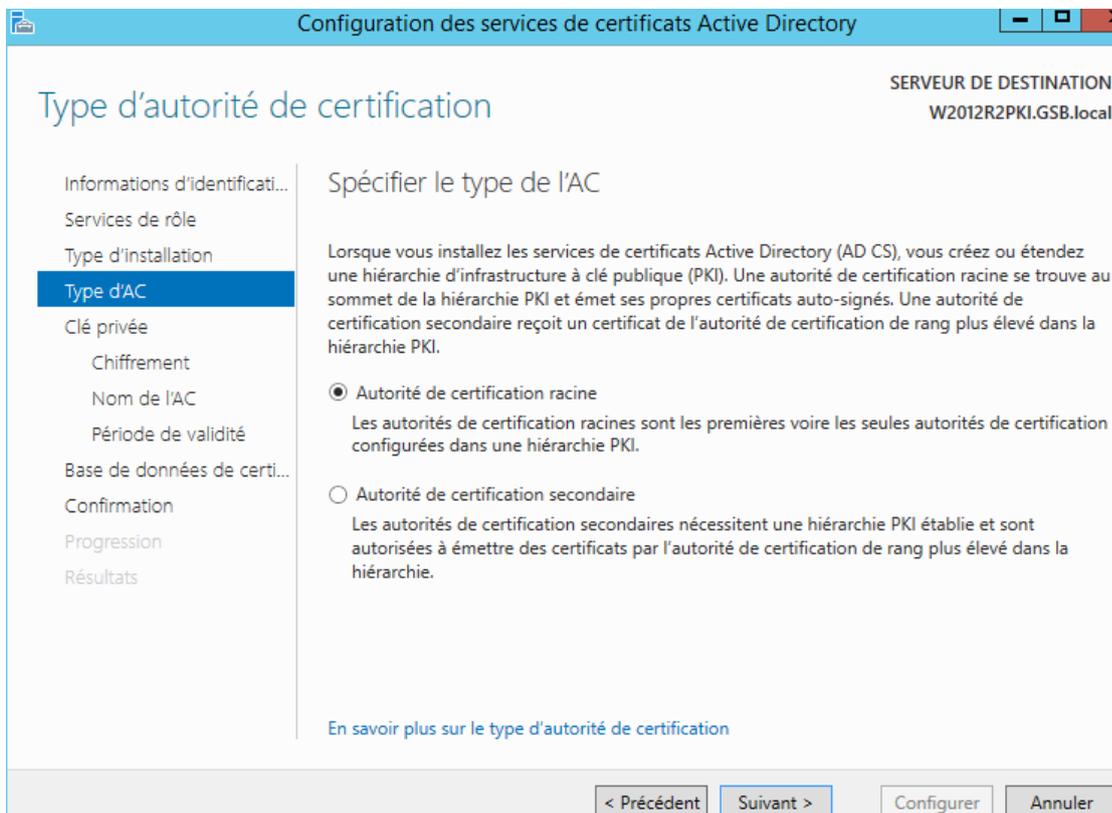
Cochez les deux options « Autorité de certification » et « Inscription de l'autorité de certification via le web » Ensuite cliquez sur Suivant :



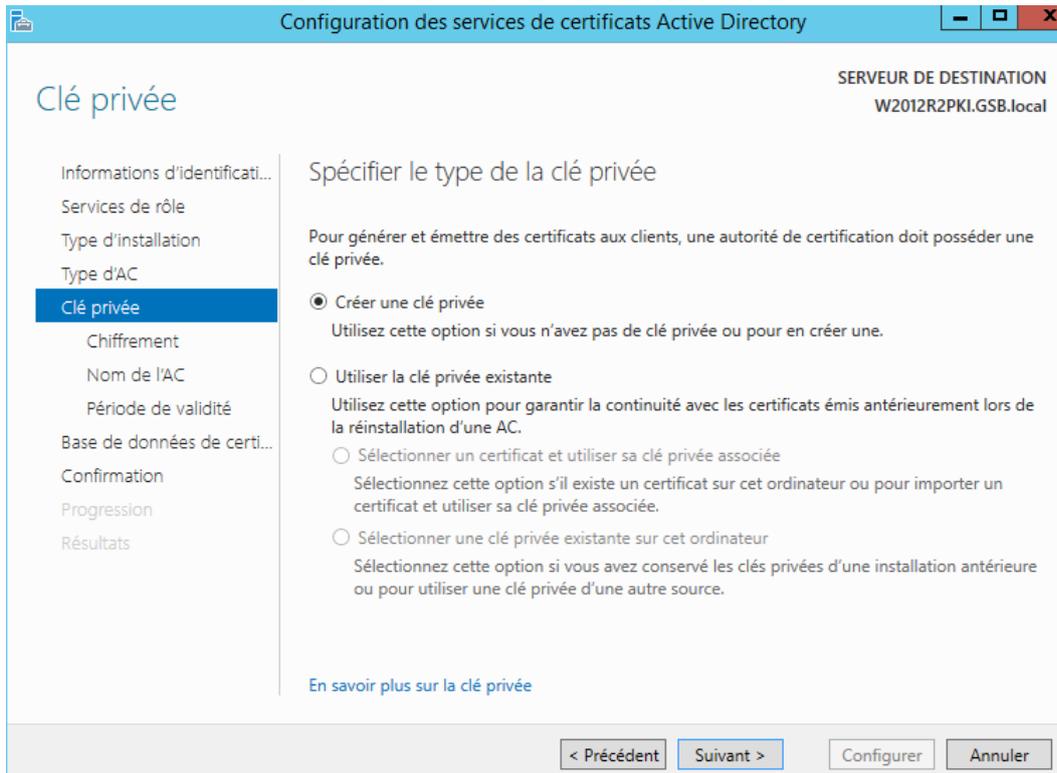
Sélectionnez « Autorité de certification d'entreprise ». Pour info cette option est grisée si votre serveur n'est pas dans un domaine. Ensuite cliquez sur « Suivant ».



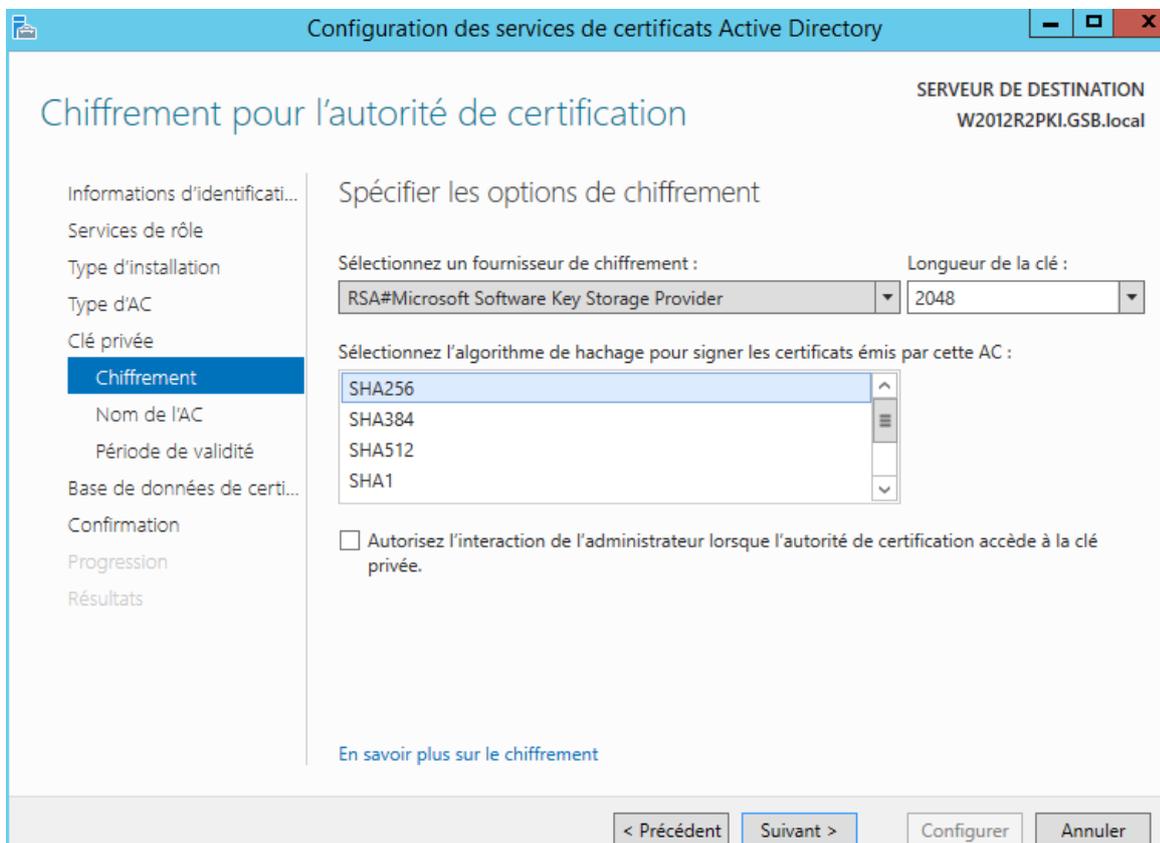
Sélectionnez « Autorité de certification racine », car nous n'avons pas de certificat signé par une autre autorité de certification supérieur et d'un organisme de certification. Ensuite cliquez sur « Suivant ».



Sélectionnez « Créer une clé privée », car nous ne disposons pas de clé existante. Ensuite cliquez sur « Suivant ».



Sélectionnez « SHA256 » et cliquez sur « Suivant » :



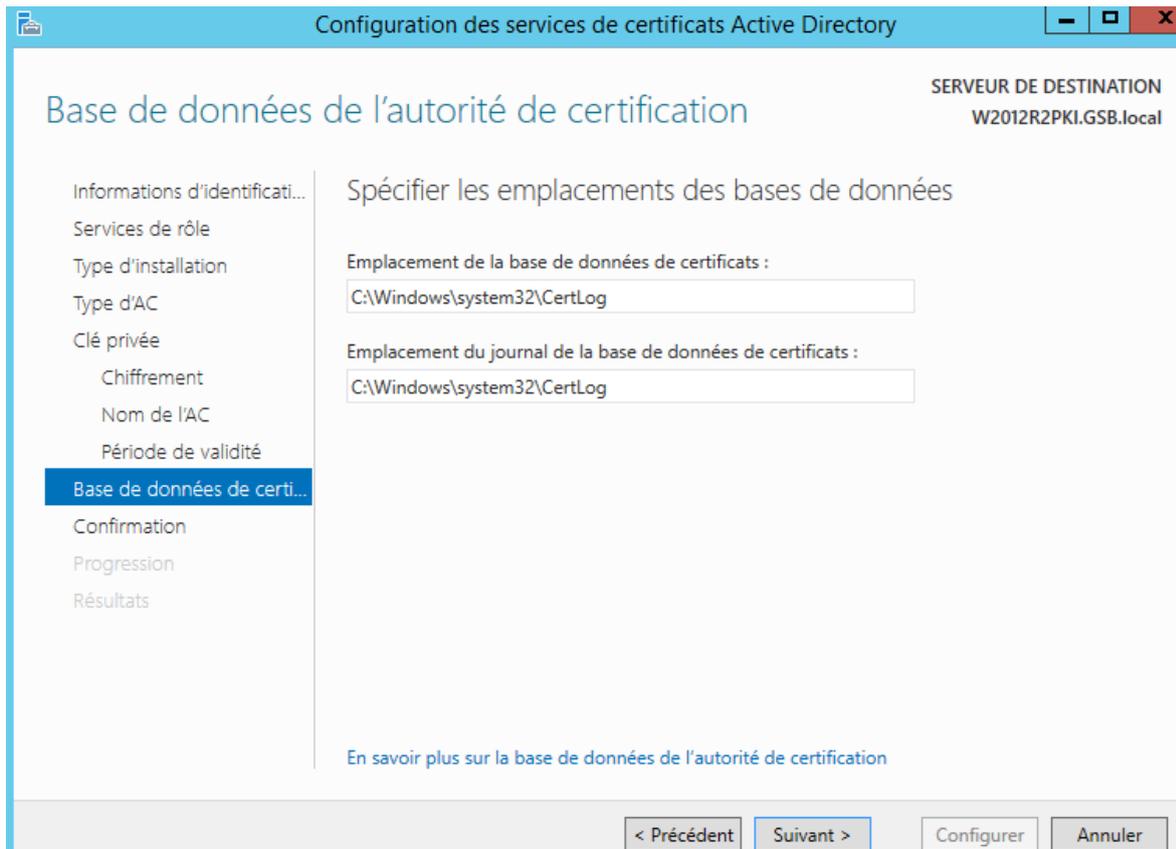
Suivant :

The screenshot shows the 'Configuration des services de certificats Active Directory' wizard. The title bar indicates the server is 'SERVEUR DE DESTINATION W2012R2PKI.GSB.local'. The main heading is 'Nom de l'autorité de certification'. A left-hand navigation pane lists steps: Informations d'identificati..., Services de rôle, Type d'installation, Type d'AC, Clé privée, Chiffrement, **Nom de l'AC**, Période de validité, Base de données de certi..., Confirmation, Progression, and Résultats. The main area is titled 'Spécifier le nom de l'AC' and contains the following text: 'Tapez un nom commun pour identifier cette autorité de certification. Ce nom est ajouté à tous les certificats émis par l'autorité de certification. Les valeurs des suffixes du nom unique sont générées automatiquement, mais elles sont modifiables.' Below this are three input fields: 'Nom commun de cette AC : GSB-W2012R2PKI-CA', 'Suffixe du nom unique : DC=GSB,DC=local', and 'Aperçu du nom unique : CN=GSB-W2012R2PKI-CA,DC=GSB,DC=local'. A link 'En savoir plus sur le nom de l'autorité de certification' is at the bottom. The bottom navigation bar includes '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

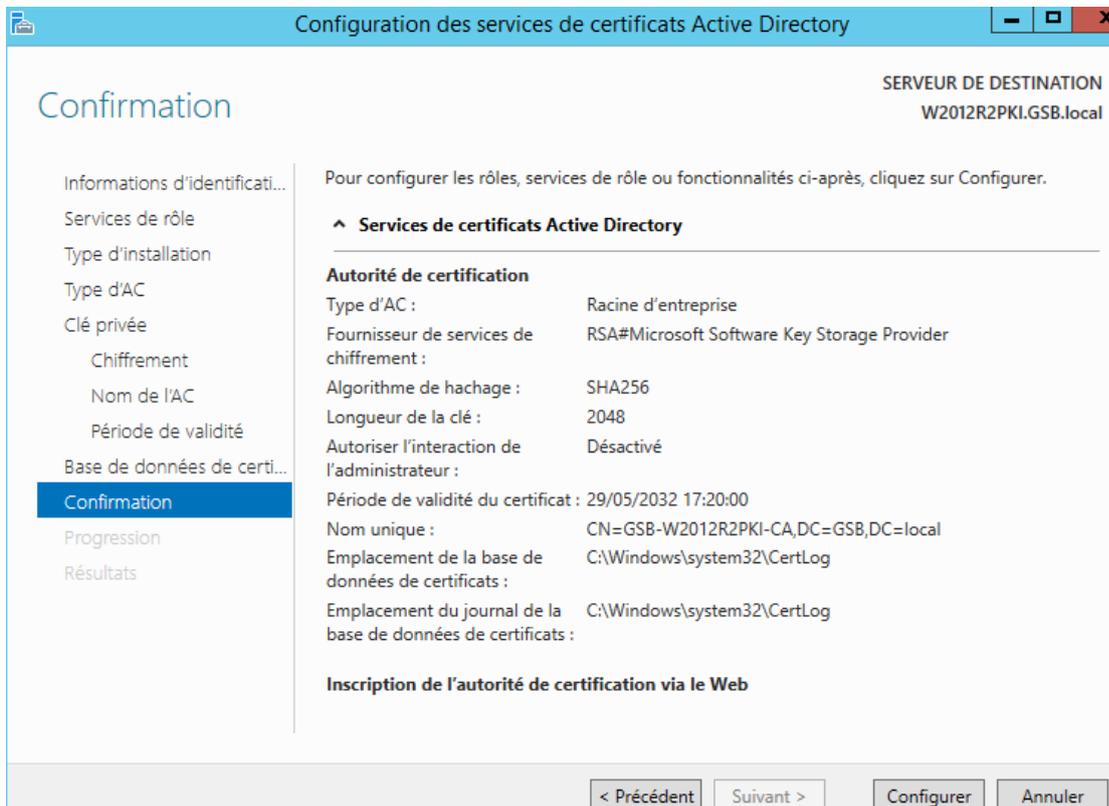
On va ensuite définir une durée de validité du certificat de l'autorité :

The screenshot shows the 'Configuration des services de certificats Active Directory' wizard. The title bar indicates the server is 'SERVEUR DE DESTINATION W2012R2PKI.GSB.local'. The main heading is 'Période de validité'. The left-hand navigation pane lists steps: Informations d'identificati..., Services de rôle, Type d'installation, Type d'AC, Clé privée, Chiffrement, Nom de l'AC, **Période de validité**, Base de données de certi..., Confirmation, Progression, and Résultats. The main area is titled 'Spécifier la période de validité' and contains the following text: 'Sélectionnez la période de validité du certificat généré pour cette autorité de certification :'. Below this is a dropdown menu with '15' in the input field and 'Années' in the dropdown. The text 'Date d'expiration de l'AC : 29/05/2032 17:20:00' is displayed. Below that, it says: 'La période de validité configurée pour ce certificat d'autorité de certification doit dépasser la période de validité pour les certificats qu'elle émettra.' A link 'En savoir plus sur la période de validité' is at the bottom. The bottom navigation bar includes '< Précédent', 'Suivant >', 'Configurer', and 'Annuler'.

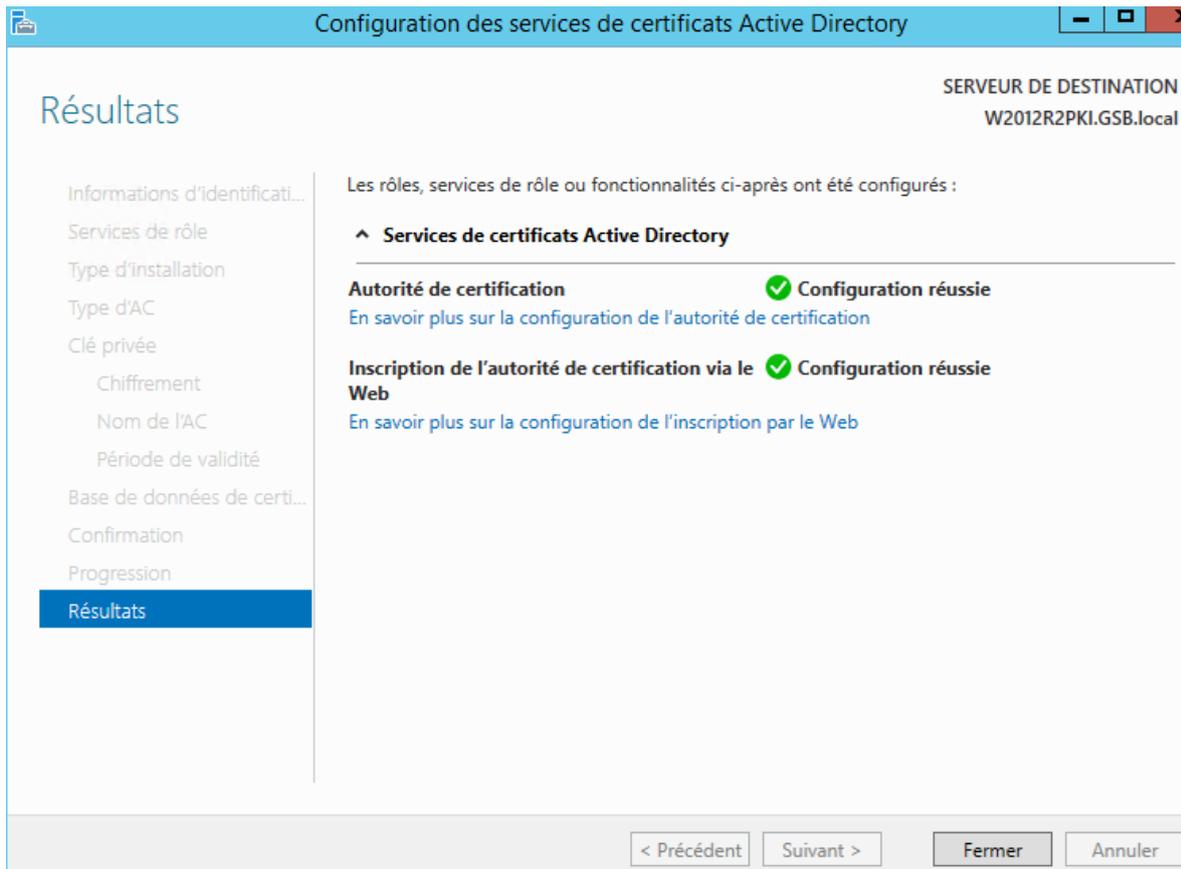
Cliquez ensuite sur « Suivant » :



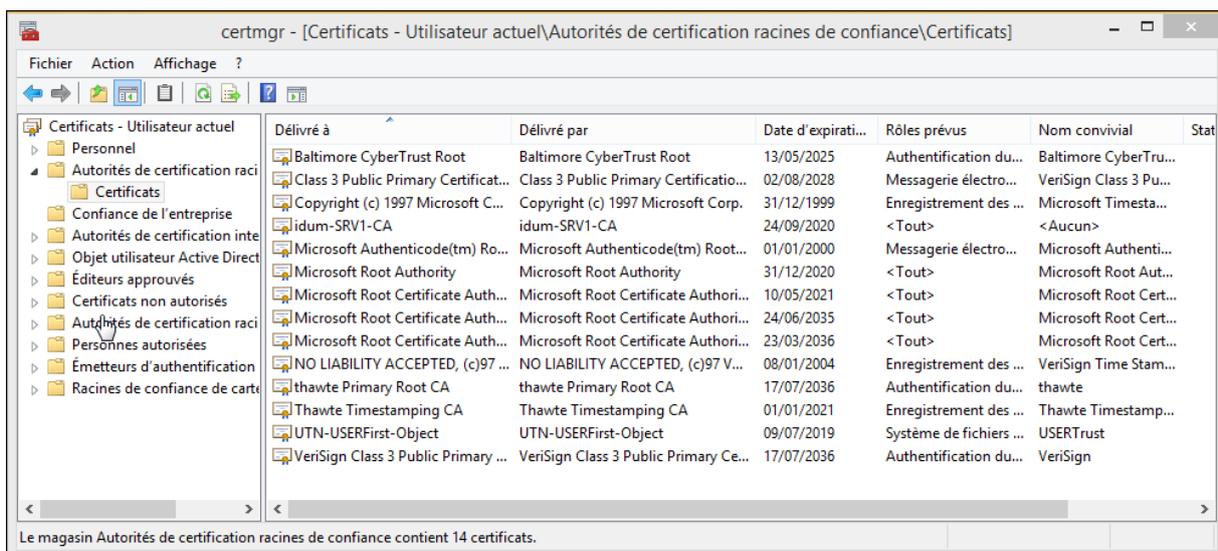
Cliquez sur « Configurer » si les paramètres affichés sont corrects :



Une fois la configuration terminée, cliquez sur « Fermer » :



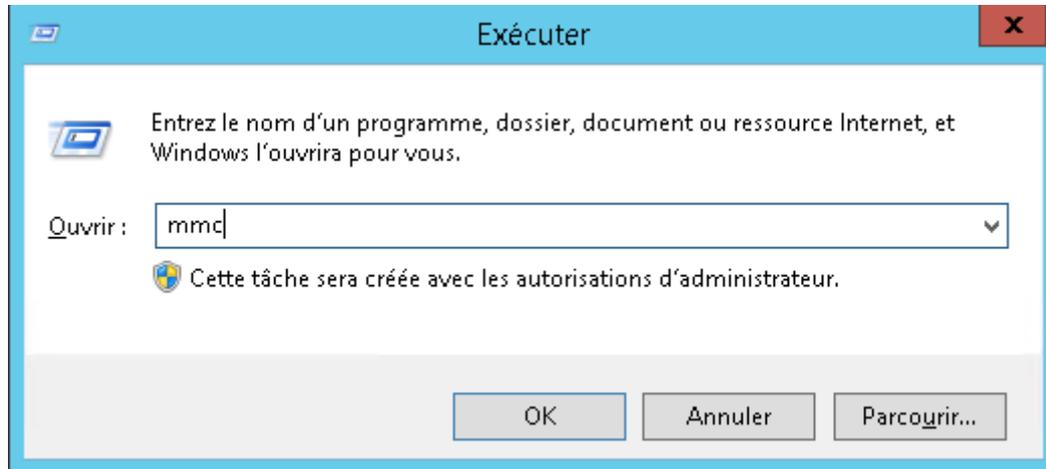
Lors de l'installation de l'autorité de certification dans un domaine, le certificat de l'autorité de certification créée est automatiquement déployé sur les machines du domaine dans le « magasin autorité racine de confiance ».



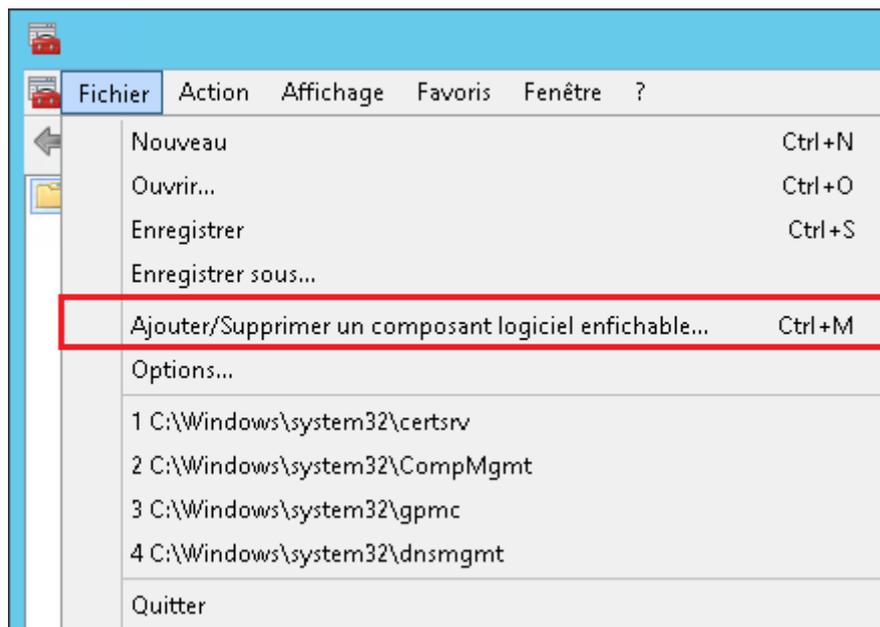
Certificat racine :

Pour voir le certificat racine suivez les instructions suivantes :

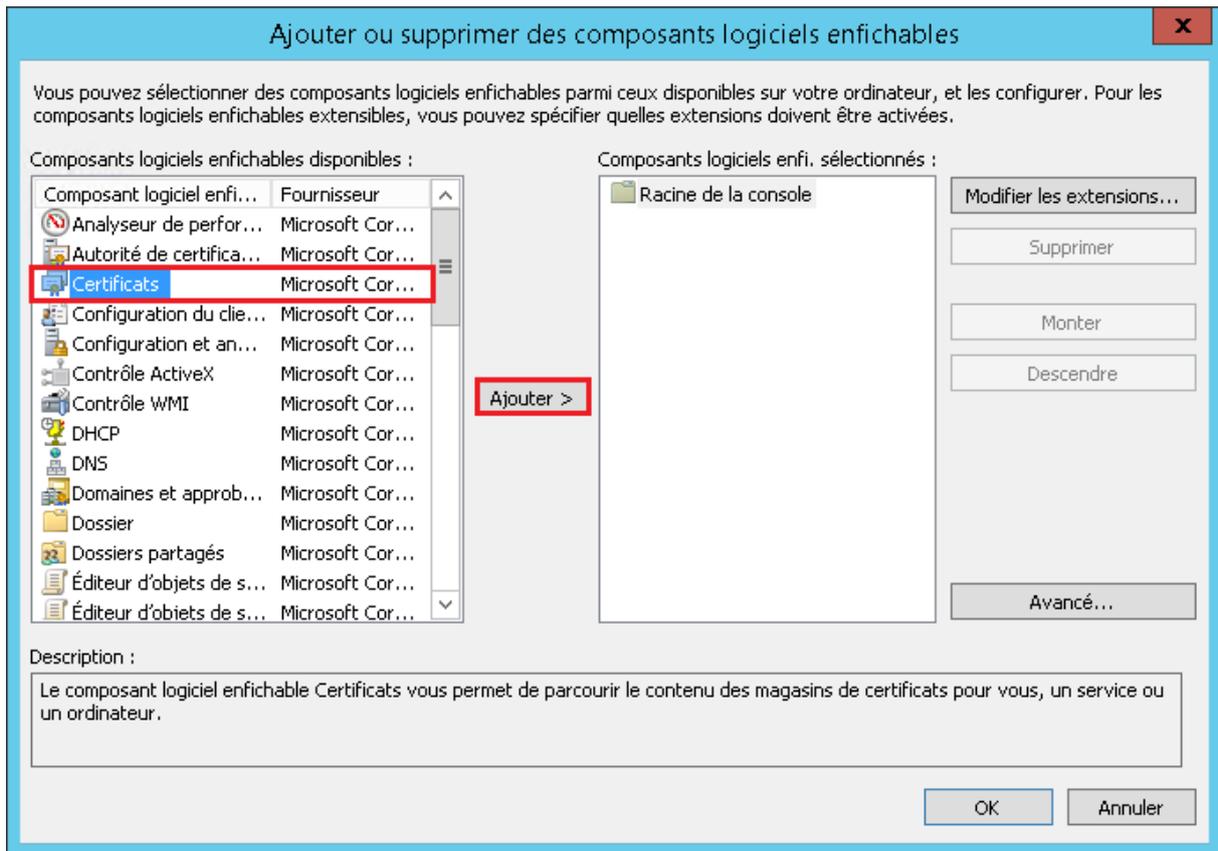
Appuyez sur les touches WIN + R, afin d'ouvrir la fenêtre « Exécuter » puis tapez « MMC ».



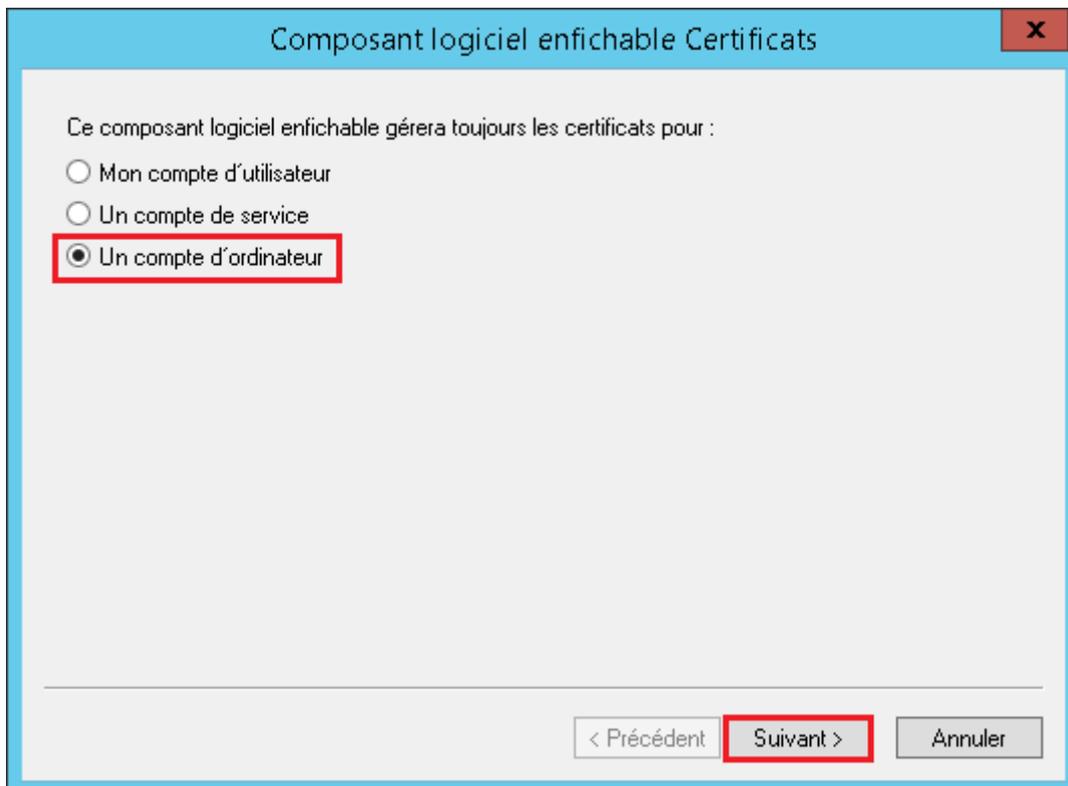
On va ensuite aller dans « Fichier », puis « Ajouter/supprimer un composant logiciel enfichable »



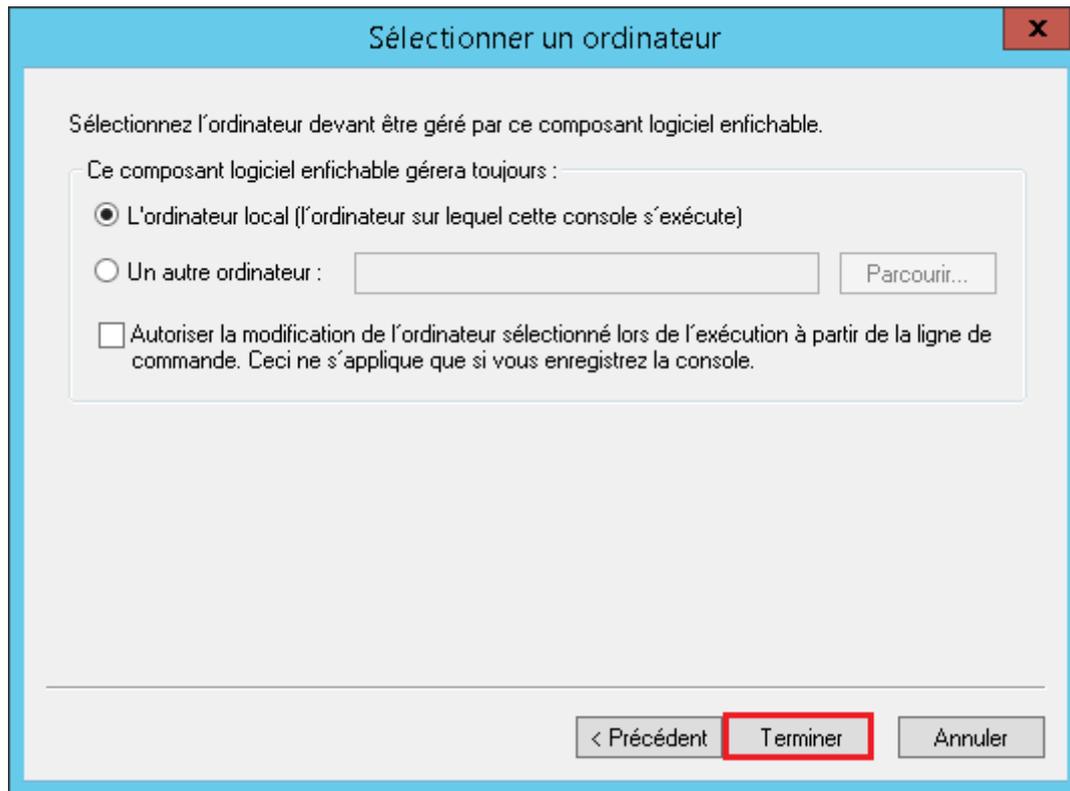
On va ensuite cliquer sur « Certificats » puis l' « ajouter ».



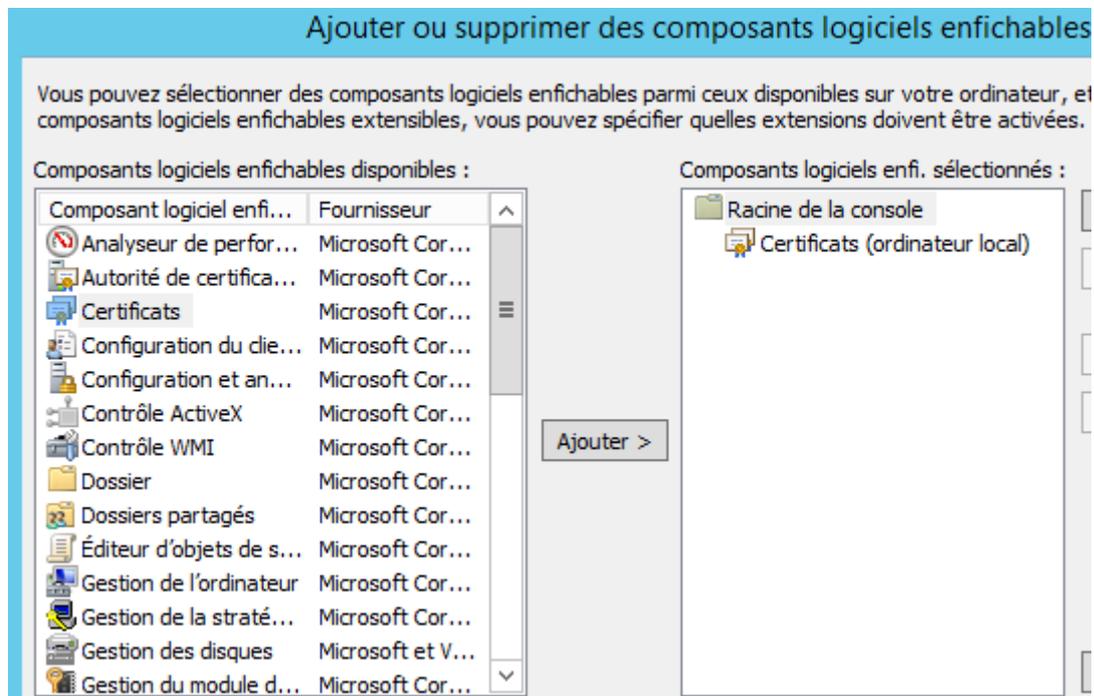
Sélectionnez « Un compte d'ordinateur »



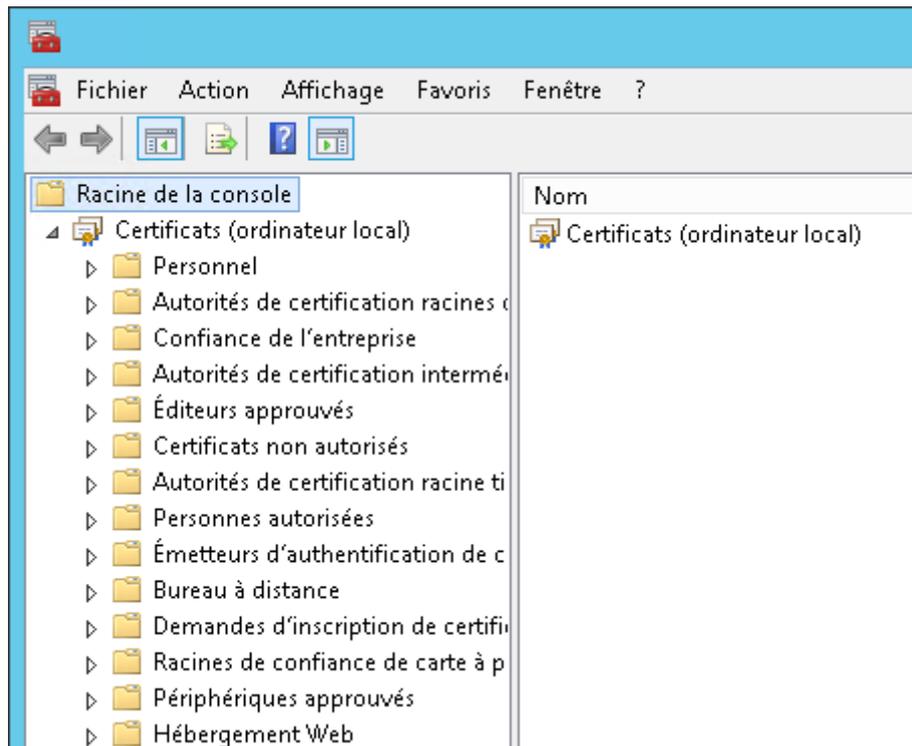
Sélectionnez « L'ordinateur local », puis cliquez sur « Terminer »



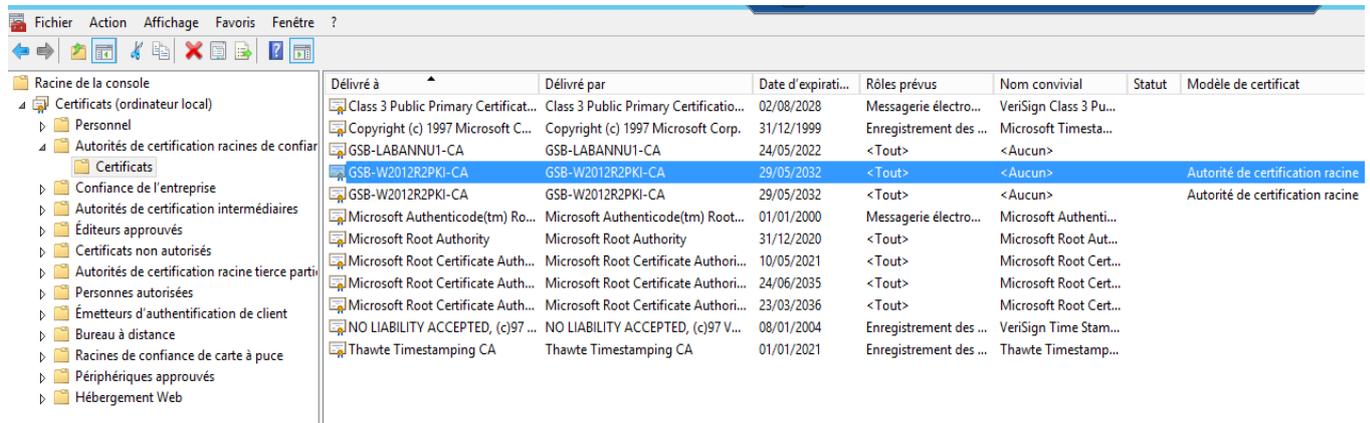
On va maintenant Développez l'arborescence de « Certificats »



On va ensuite Développez l'arborescence de « certificats » :

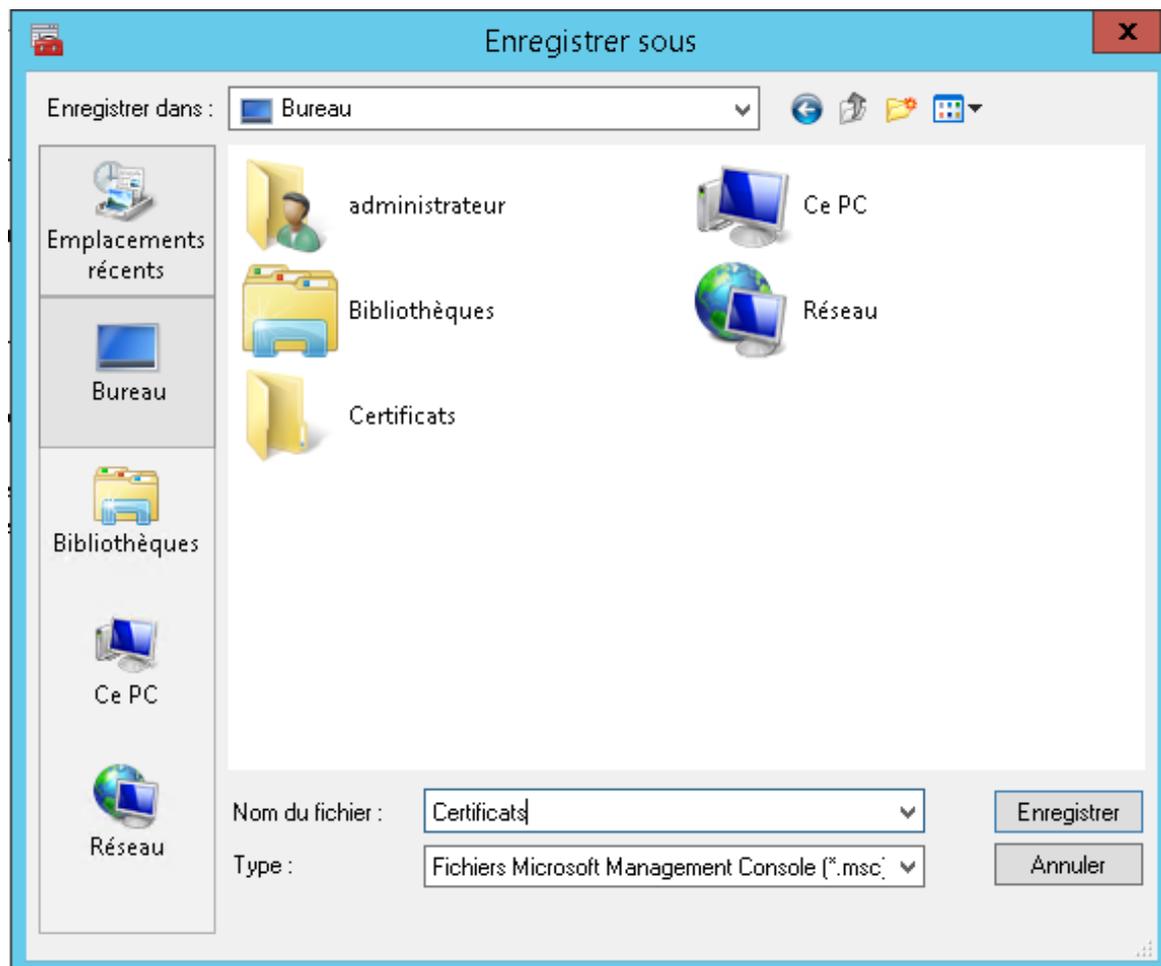
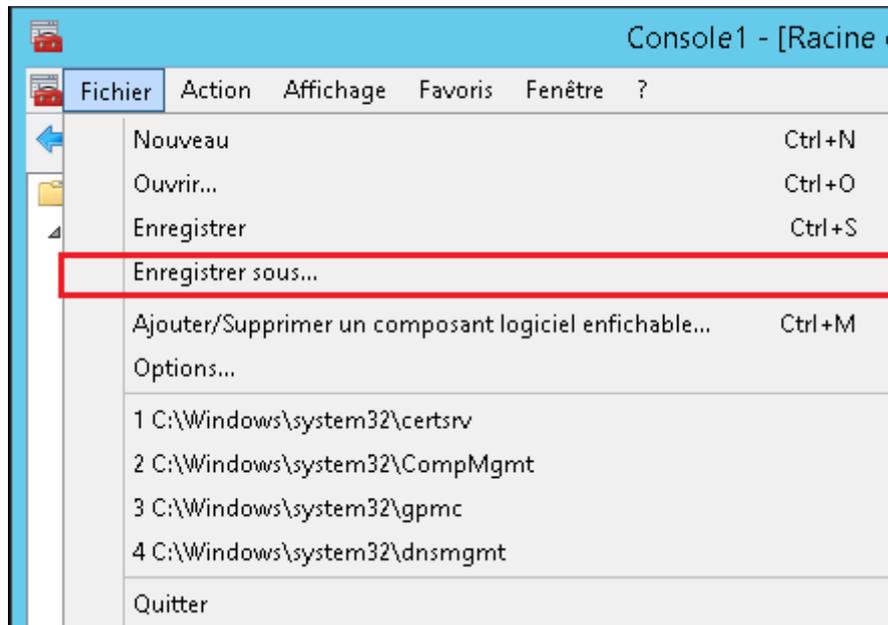


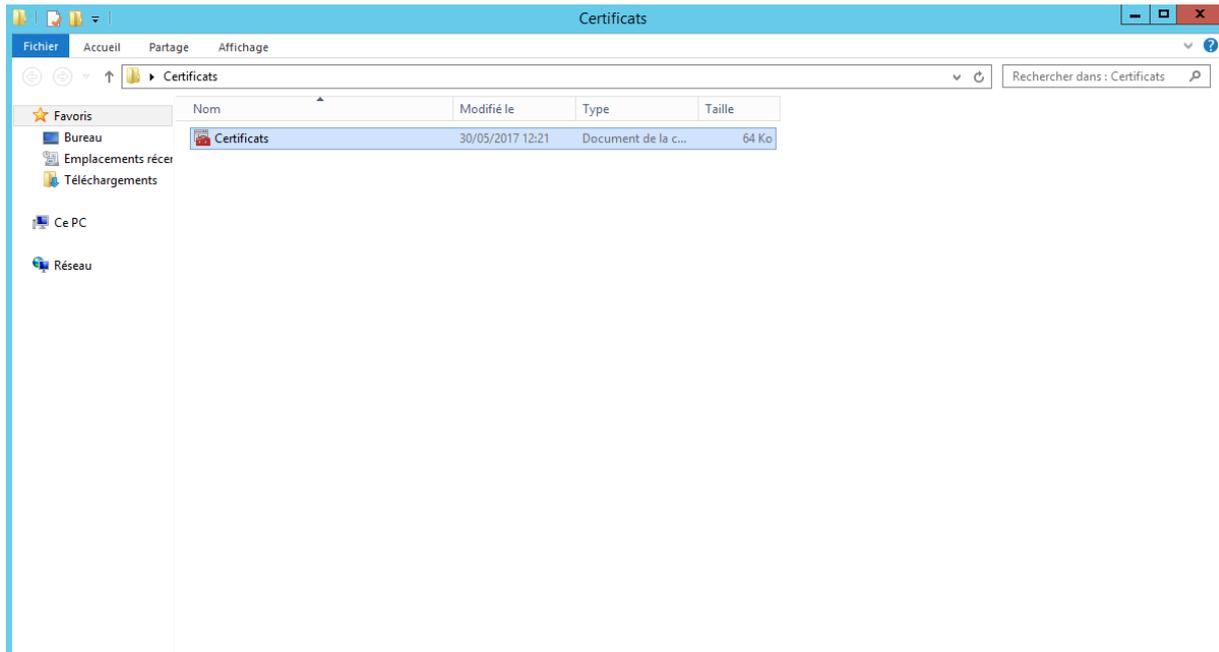
Développez l'arborescence de « Autorités de certification racines de confiance », puis « Certificats ».



On voit ici nos deux certificats racine de GSB-W2012R2-PKI-CA

Pour pouvoir revenir rapidement à cette console, vous pouvez créer un raccourcis sur le bureau en cliquant sur « Fichier », puis « Enregistrer sous ».





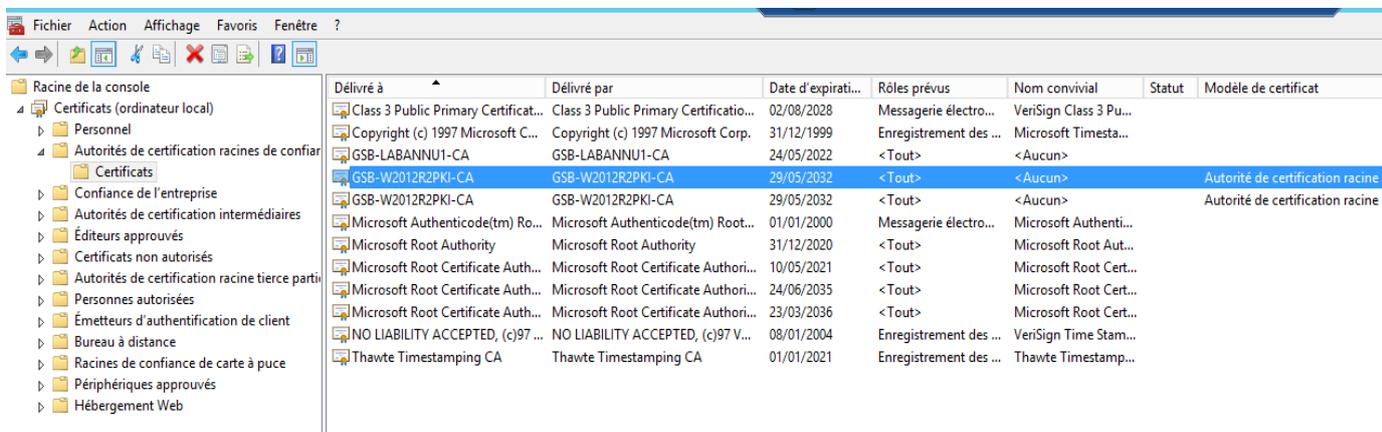
Exporter le certificat racine :

Comme expliqué dans l'introduction, un ordinateur souhaitant vérifier une clé publique ou certificat doit comparer la signature de l'autorité de certification présente dans la clé publique ou certificat, avec le certificat de l'autorité racine.

Notre certificat étant généré par une autorité de certification autonome, nous devons partager le certificat racine avec toutes les machines du domaine. Ainsi chaque ordinateur devra avoir le certificat racine dans le conteneur « Autorité de certification racines de confiance »

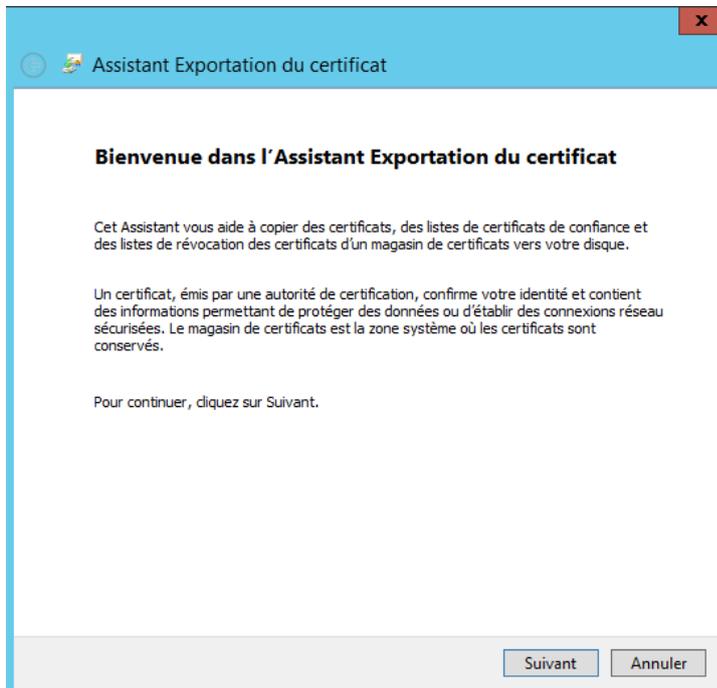
Pour pouvoir partager le certificat racine, il faut commencer par l'exporter

Pour cela on va ouvrir la console MMC pour accéder aux certificats comme indique dans le chapitre précédent :

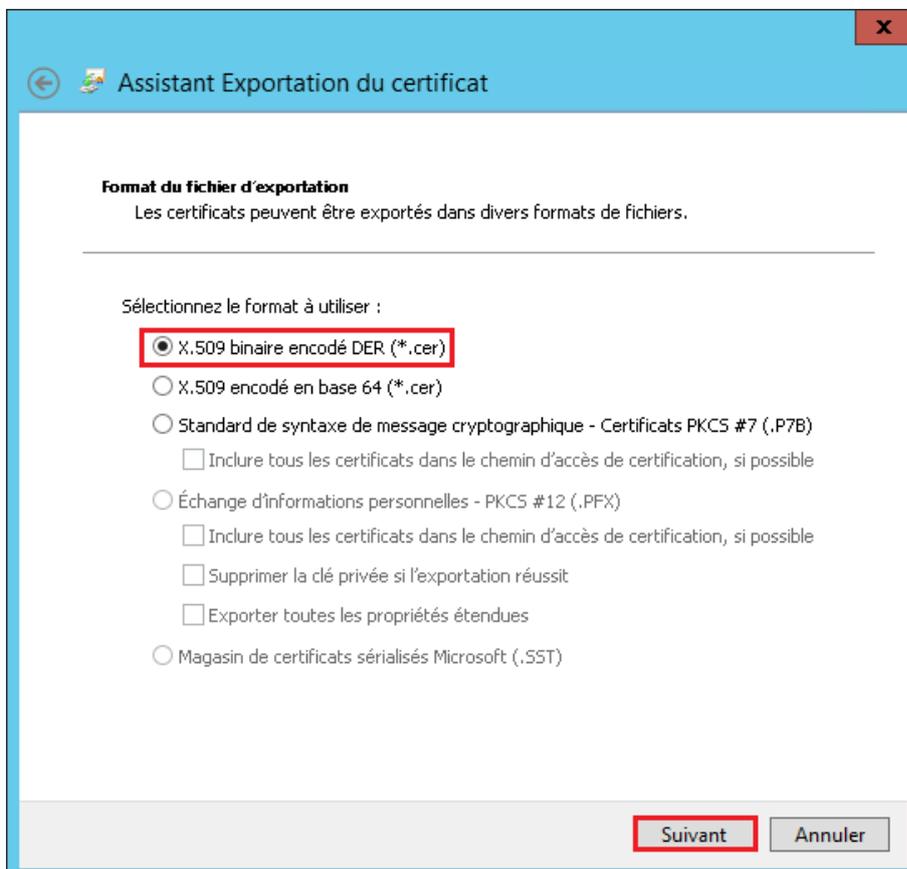


On va sélectionner le premier certificat racine. Puis faire un clic droit, « Toute les taches » et enfin cliquez sur « Exporter ».

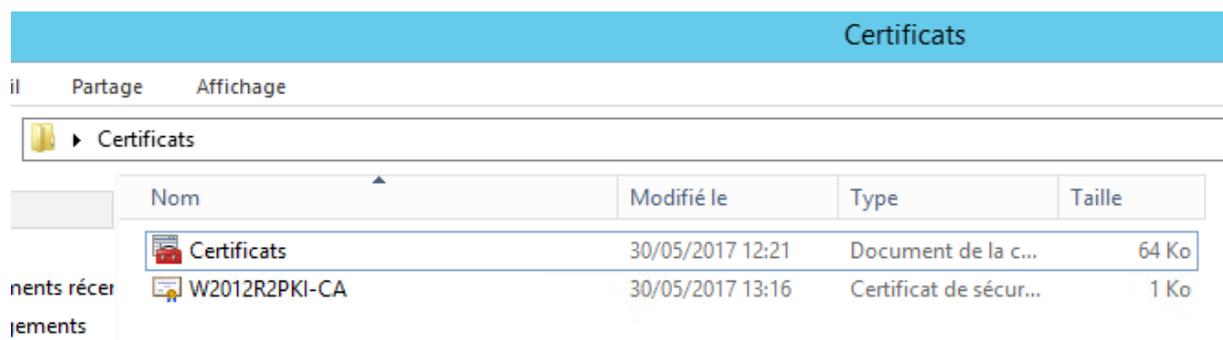
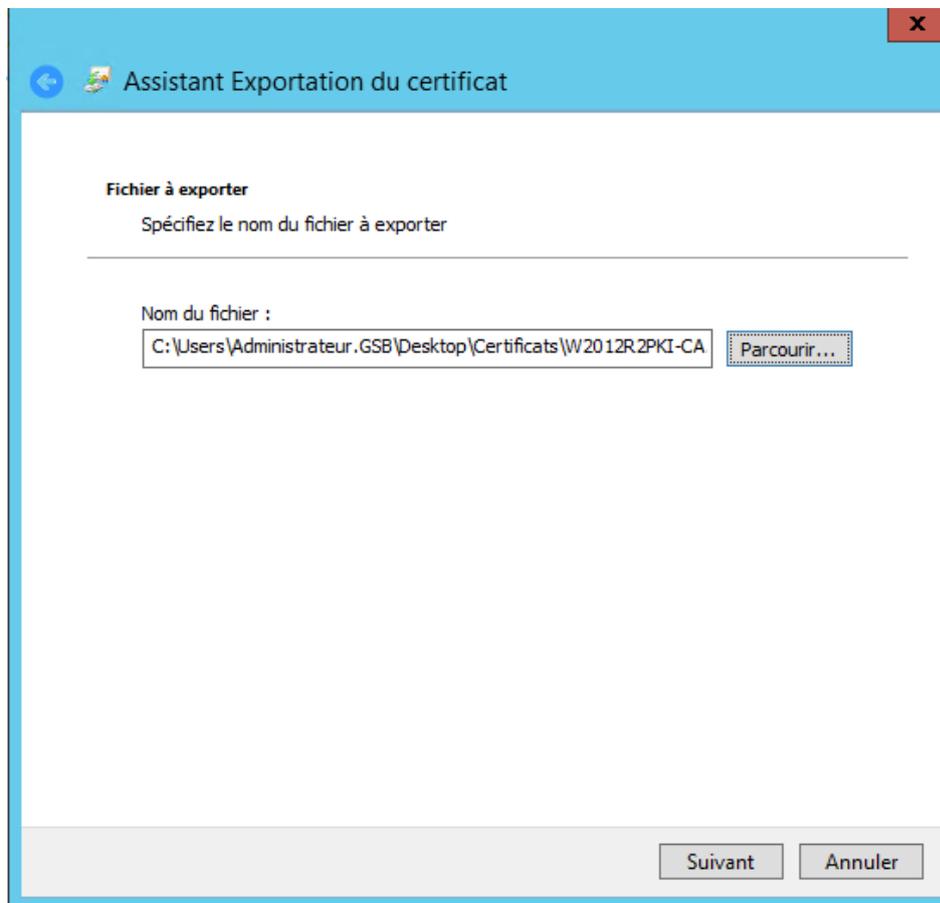
L'assistant d'exportation se lance. Cliquez sur « suivant » :



Choisissez « X.509 binaire encodé DER ». Cliquez sur « suivant »



Il suffit ensuite de définir le chemin pour enregistrer le certificat. On va enregistrer temporairement le certificat sur le bureau du serveur dans le dossier certificats. Puis appuyez sur « Terminer ».



Interface Web Certsrv :

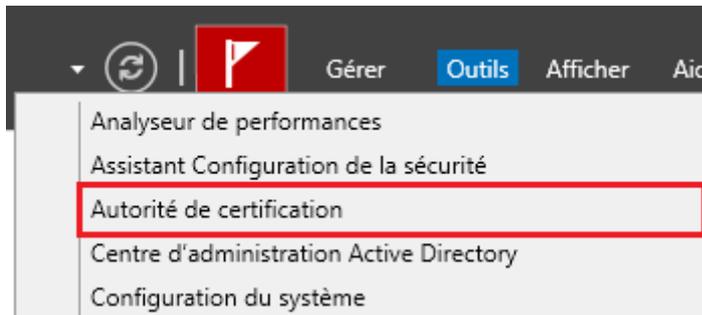
Nous allons maintenant configurer l'interface web de l'autorité de certification pour que celle-ci utilise un certificat délivré par l'autorité de certification. Les ordinateurs du domaine verront alors un site sécurisé.

On va tout d'abord commencer par la création d'un modèle de certificat.

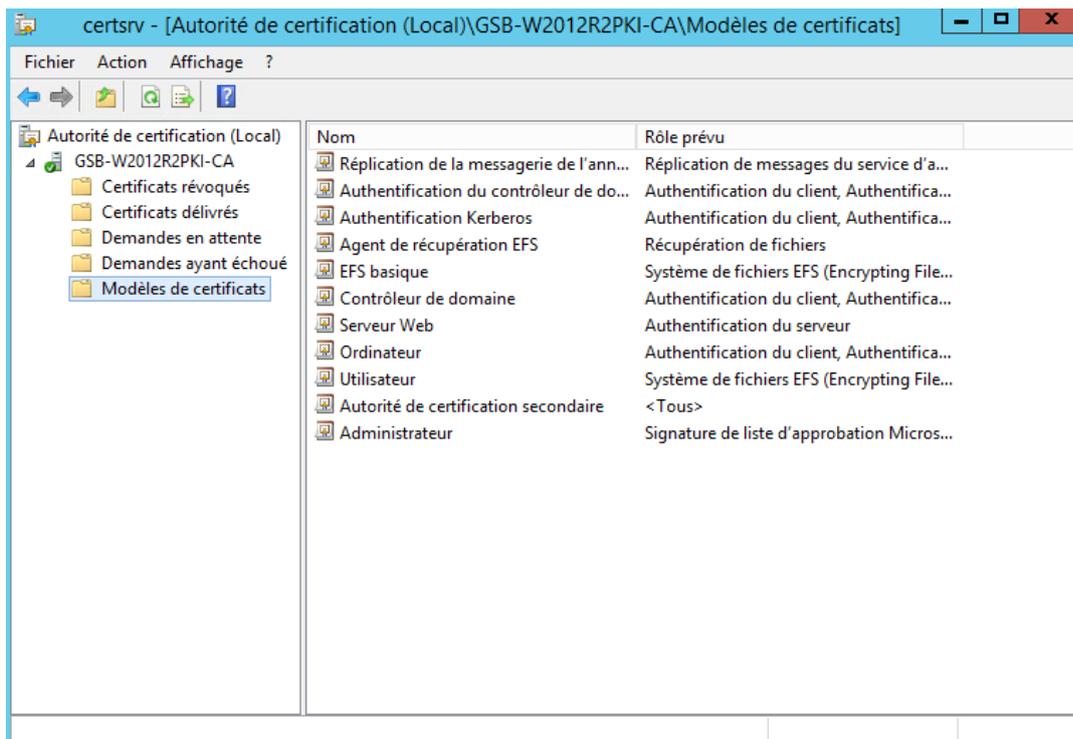
Création d'un modèle de certificat :

Tout d'abord un modèle de certificat que l'on peut appeler aussi « Template » de certificat permet de définir des paramètres comme la durée de validité, le domaine, les droits, etc. Ces paramètres seront appliqués à chaque certificat généré à partir du modèle.

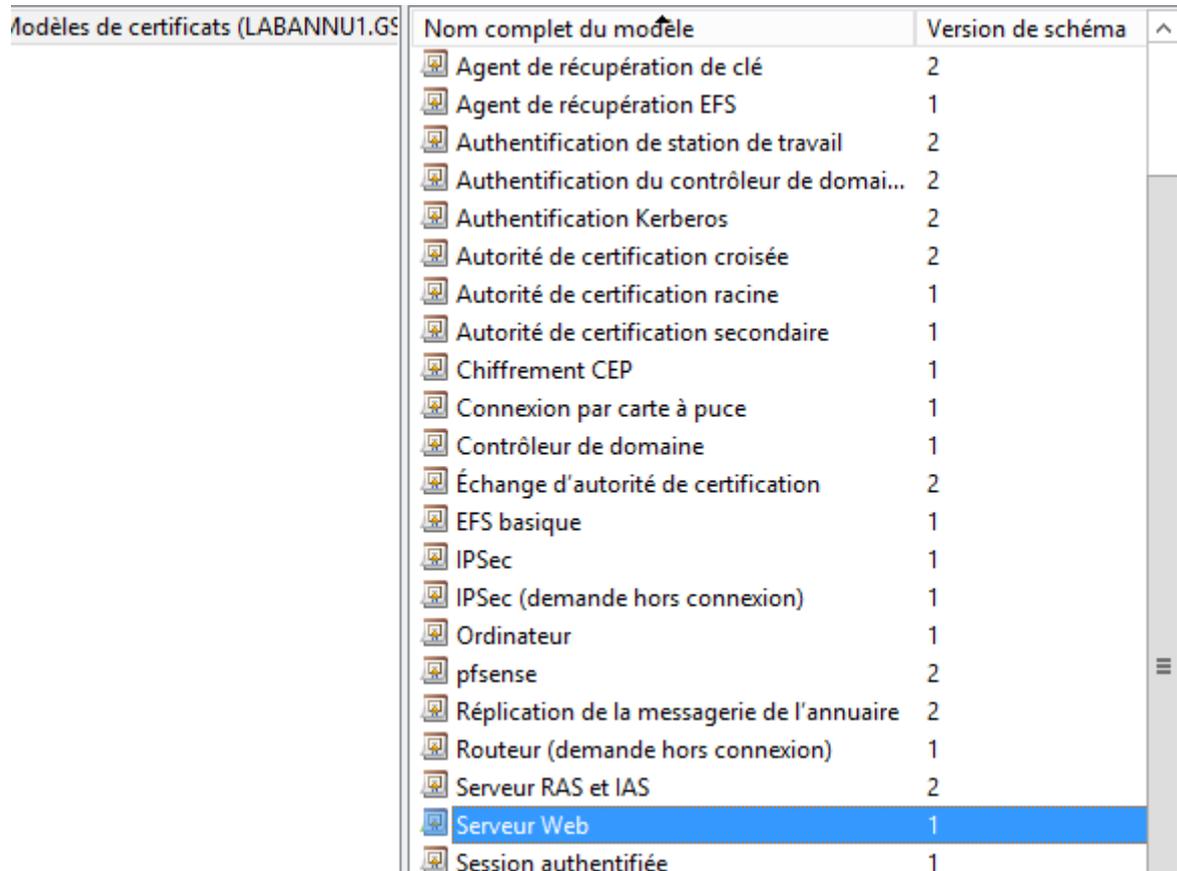
On va ouvrir le « Gestionnaire de serveur », puis dans le menu en haut à droite, cliquez sur « Outils » puis « Autorité de certification ».



On va ensuite aller dans « Modèles de certificats »



On va ensuite faire un clic droit sur le répertoire « Modèle de certificats », puis cliquer sur « Gérer », dans la nouvelle fenêtre qui s'ouvre à vous, trouvez le modèle « Serveur Web ». Faites un clic droit, puis cliquez sur « Dupliquer le modèle ».



Nom complet du modèle	Version de schéma
Agent de récupération de clé	2
Agent de récupération EFS	1
Authentification de station de travail	2
Authentification du contrôleur de domai...	2
Authentification Kerberos	2
Autorité de certification croisée	2
Autorité de certification racine	1
Autorité de certification secondaire	1
Chiffrement CEP	1
Connexion par carte à puce	1
Contrôleur de domaine	1
Échange d'autorité de certification	2
EFS basique	1
IPSec	1
IPSec (demande hors connexion)	1
Ordinateur	1
pfsense	2
Réplication de la messagerie de l'annuaire	2
Routeur (demande hors connexion)	1
Serveur RAS et IAS	2
Serveur Web	1
Session authentifiée	1

Notre autorité de certification sera pour notre Windows serveur 2012 R2 PKI. Nous allons permettre de résoudre le fait qu'un client qui se connecte en bureau à distance n'est pas de message d'avertissement. Nous allons donc mettre le destinataire du certificat :

Les options de modèle disponibles reposent sur les versions de système d'exploitation les plus anciennes définies dans Paramètres de compatibilité.

Afficher les modifications résultantes

Paramètres de compatibilité

Autorité de certification
Windows Server 2012 R2

Destinataire du certificat
Windows 7 / Server 2008 R2

Il se peut que ces paramètres n'empêchent pas les systèmes d'exploitation plus anciens d'utiliser ce modèle.

Puis dans l'onglet « Général », saisissez le nom du modèle. Puis définissez la « période de validité » ainsi que la « Période de renouvellement ». N'oubliez pas, la « Période de validité » doit être inférieure à la Période de validité du certificat de l'autorité de certification qu'on a défini juste avant (15 ans).

Attestation de clé		Nom du sujet		Serveur	
Conditions d'émission	Modèles obsolètes	Extensions	Sécurité		
Compatibilité	Général	Traitement de la demande		Chiffrement	

Nom complet du modèle :

Nom du modèle :

Période de validité : années

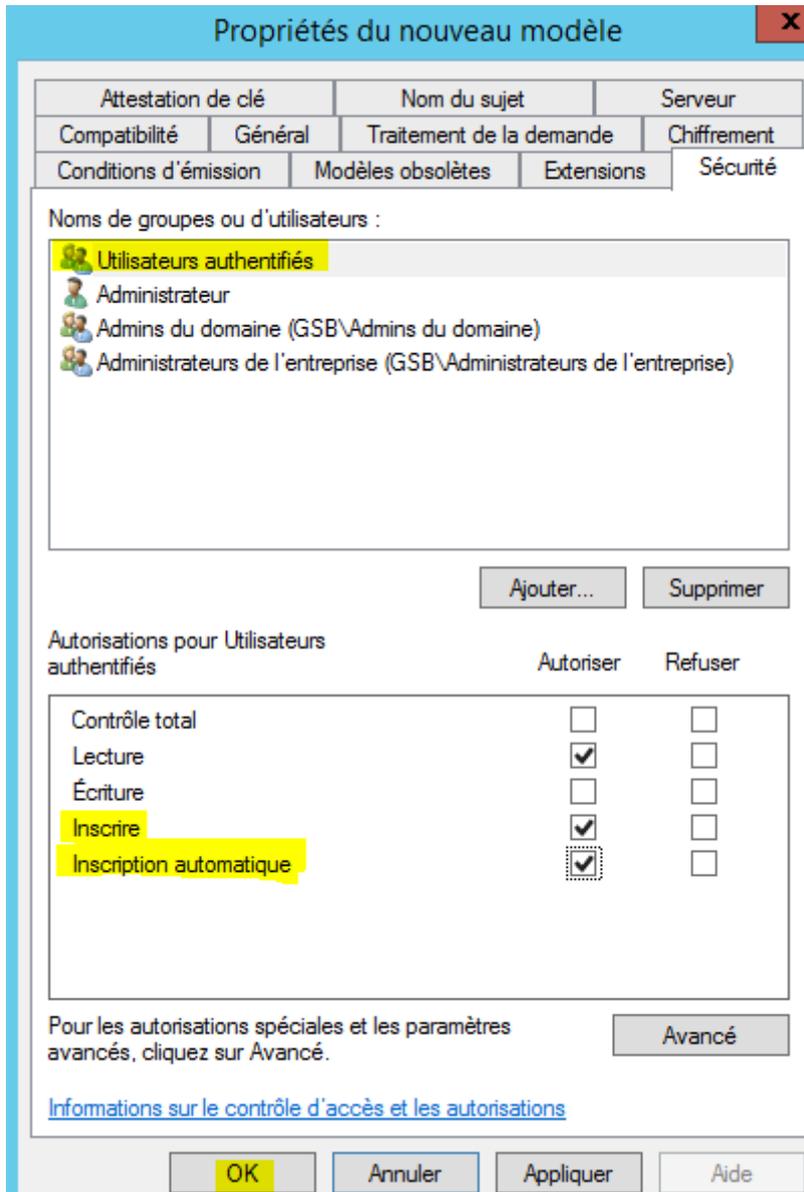
Période de renouvellement : semaines

Publier le certificat dans Active Directory

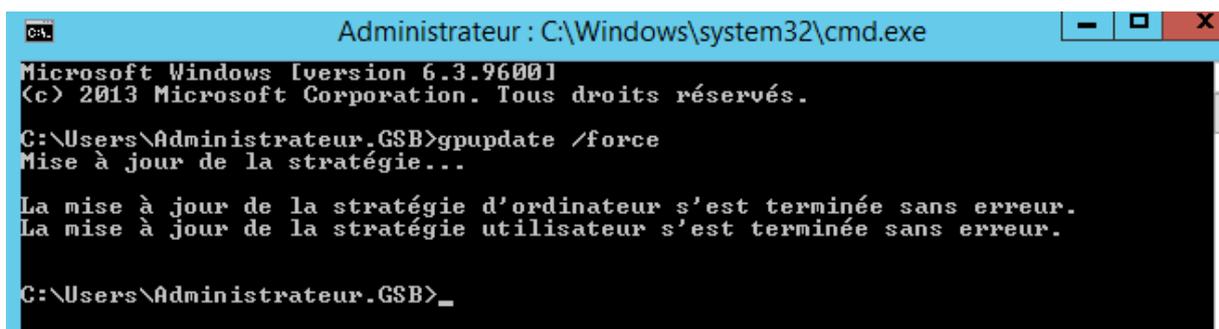
Ne pas utiliser la réinscription automatique si un certificat dupliqué existe dans Active Directory

OK Annuler Appliquer Aide

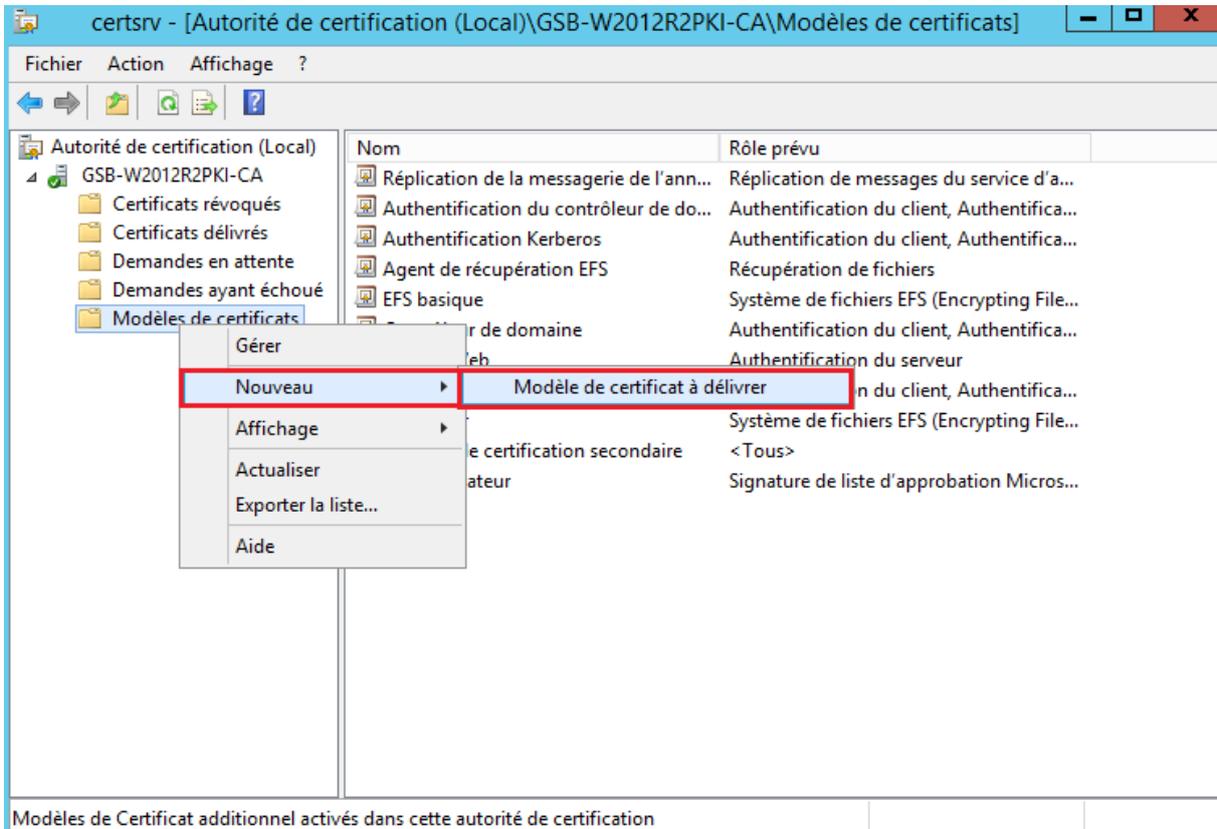
Dans l'onglet « Sécurité », pour le groupe d'utilisateur « utilisateurs authentifiés » cochez les deux options suivantes : « Inscrire » et « Inscription automatique ». Pour terminer, cliquez sur « Appliquer » puis « OK ».



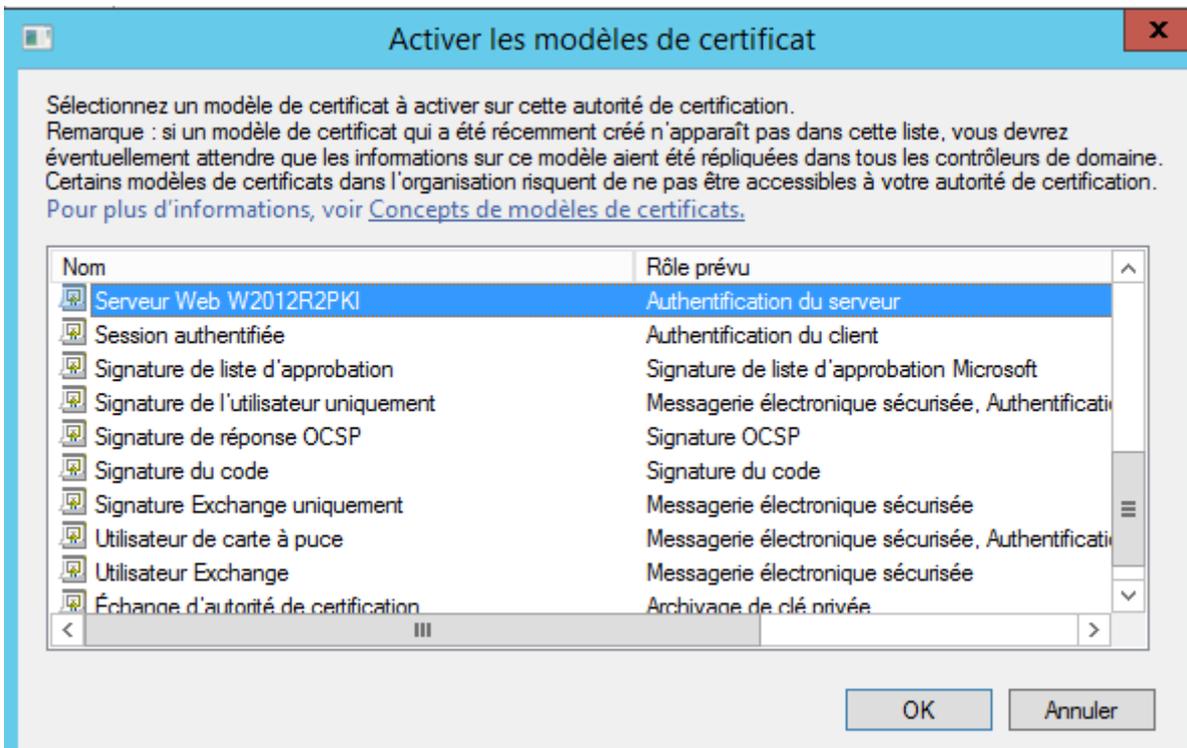
Pour que le nouveau modèle soit correctement pris en compte, il est conseillé de faire une mise à jour des GPO. Il faut donc ouvrir l'invite de commande (CMD), puis taper la commande « gpupdate /force ».



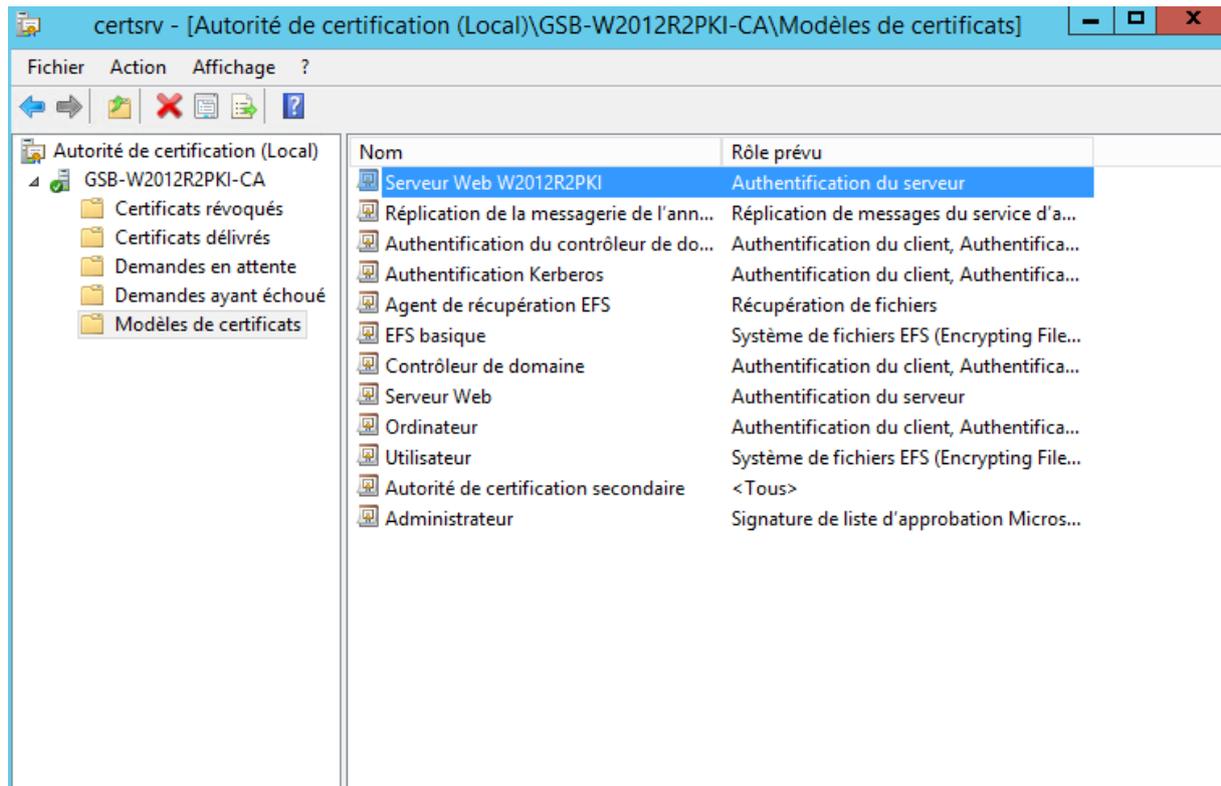
On va ensuite retourner sur la fenêtre « CERTSRV », puis faites de nouveau un clic droit sur le répertoire « Modèles de certificats ». Cliquez sur « Nouveau » et enfin sur « Modèle de certificat à délivrer »



On va ensuite recherchez le modèle qu'on vient de créer (serveur web W2012R2PKI)



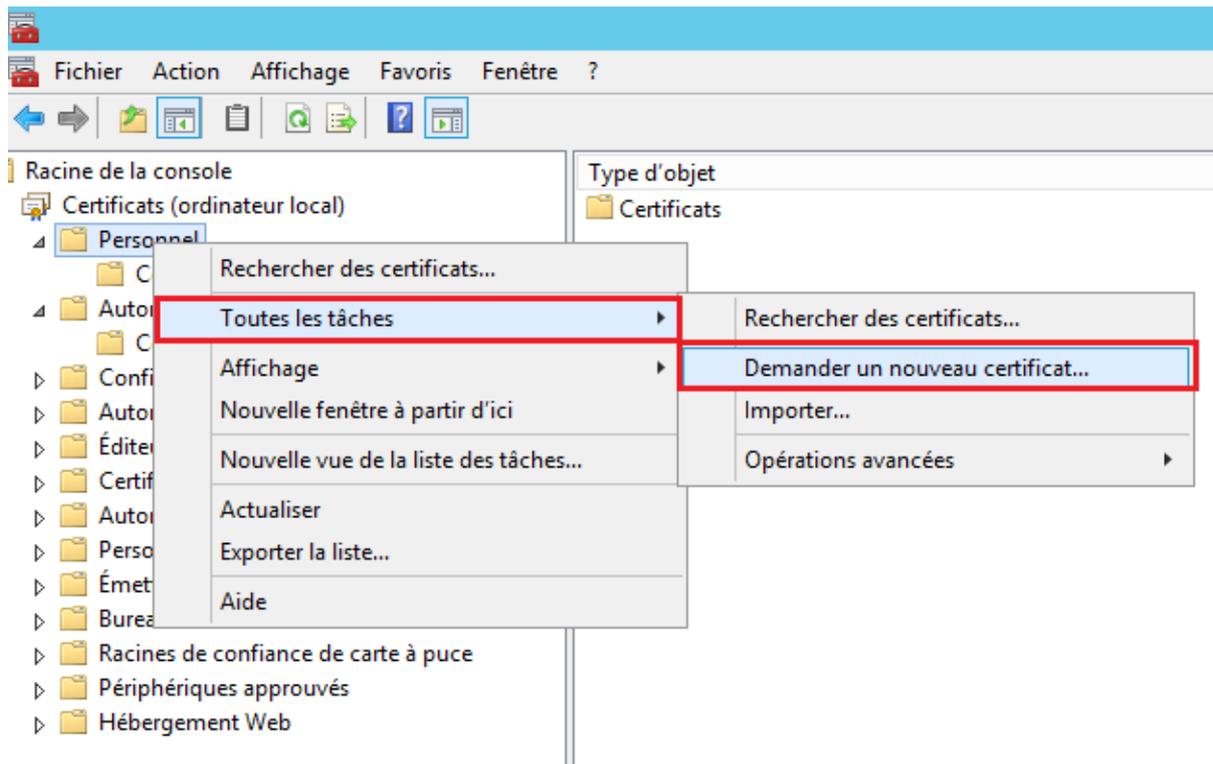
On voit que le nouveau modèle de certificat à délivrer s'affiche maintenant dans la liste :



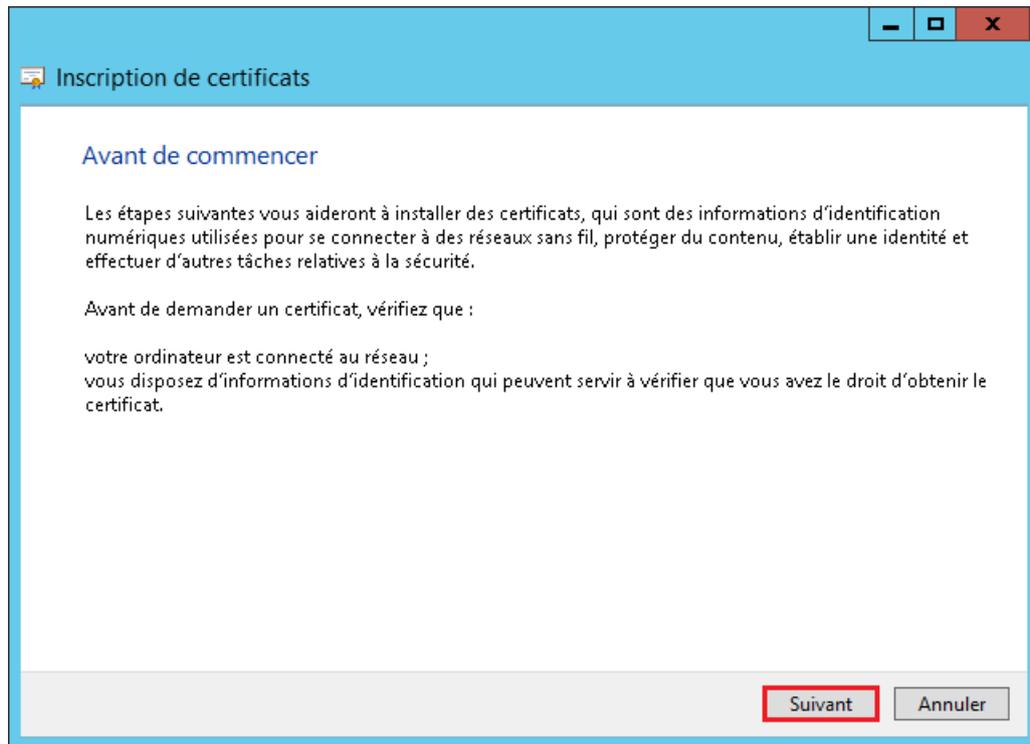
Création d'un certificat SSL :

Nous voulons maintenant générer un nouveau certificat SSL :

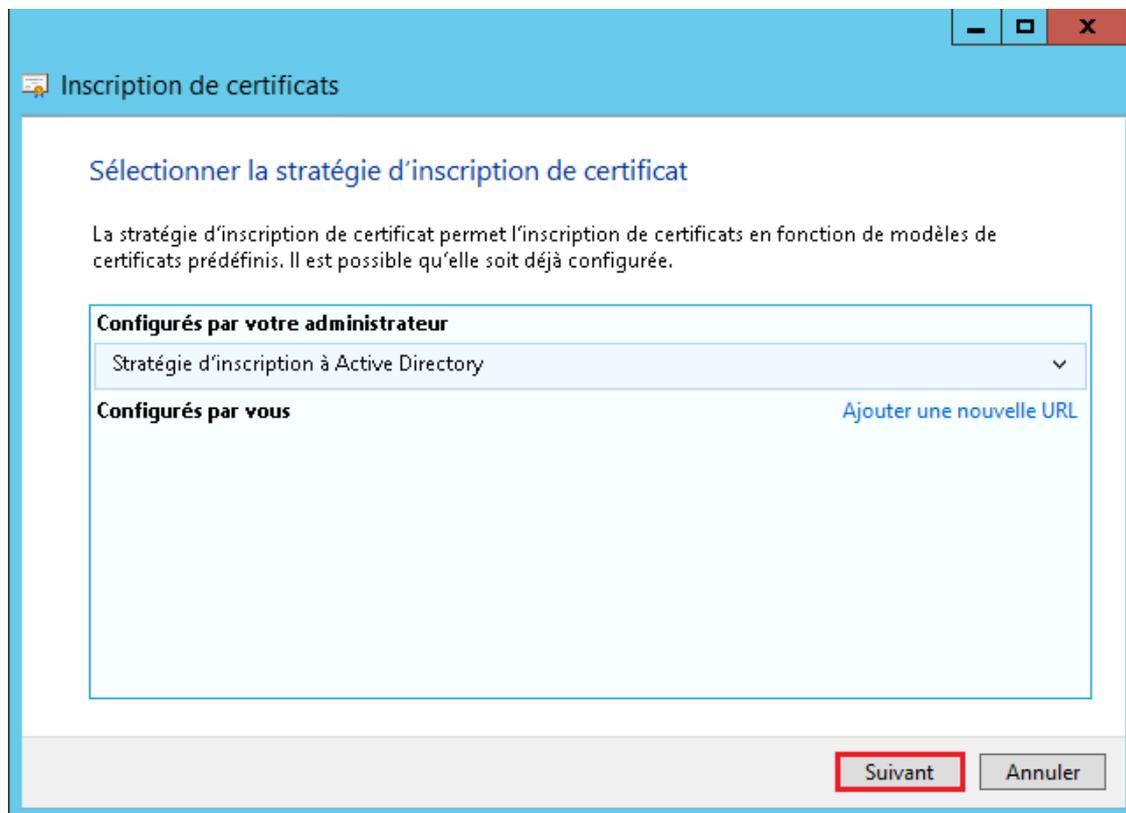
Ouvrez la console MMC avec le composant logiciel enfichable « Certificats ». Développez l'arborescence, faites un clic droit sur le répertoire « Personnel », puis cliquez sur « Toutes les tâches » et enfin « Demander un nouveau certificat ».



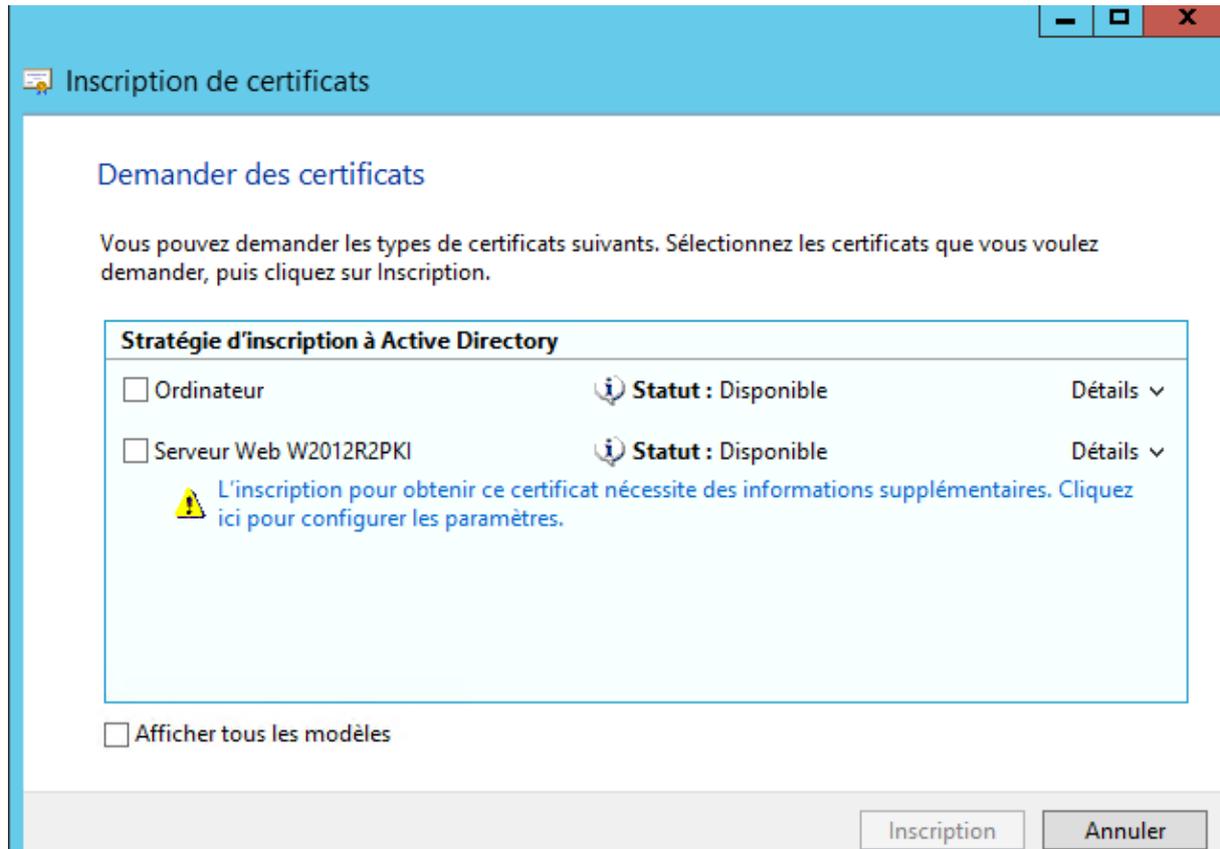
Une fenêtre s'ouvre, il suffit simplement de faire suivant :



Cliquez de nouveau sur suivant :



Sélectionnez le modèle précédemment créé, puis cliquez sur le lien en dessous « L'inscription pour obtenir ce certificat nécessite des informations supplémentaires ».



Dans le premier onglet, définissez le nom du domaine pour le champ « Nom commun ».

Nom du sujet :

Type :		
Nom commun	Ajouter >	
Valeur :	< Supprimer	
W2012R2PKI.GSB.local		
Autre nom :		

Cliquez ensuite sur « Ajouter »

The screenshot shows the 'Objet' (Subject) tab of a certificate properties dialog. The 'Type' dropdown is set to 'Nom commun'. The 'Valeur' (Value) field is empty. The 'Ajouter >' button is active, and the 'CN=W2012R2PKI.GSB.local' entry is visible in the list on the right. The 'Supprimer <' button is disabled.

Objet Général Extensions Clé privée Autorité de certification Signature

Le sujet d'un certificat est l'utilisateur ou l'ordinateur vers lequel le certificat est émis. Vous pouvez entrer des informations sur les types de noms de sujet et d'autres noms qui peuvent être utilisés dans un certificat.

Sujet du certificat
L'utilisateur ou l'ordinateur qui reçoit le certificat

Nom du sujet :

Type :
Nom commun

Valeur :
[Empty text box]

Ajouter >

< Supprimer

CN=W2012R2PKI.GSB.local

Vous pouvez définir ensuite un « Nom convivial » Dans l'onglet Général. Cliquez pour terminer sur « Ok ».

The screenshot shows the 'Général' (General) tab of a certificate properties dialog. The 'Nom convivial' (Friendly name) field contains 'CERT_W2012R2PKI.GSB.local'. The 'Description' field is empty.

Propriétés du certificat

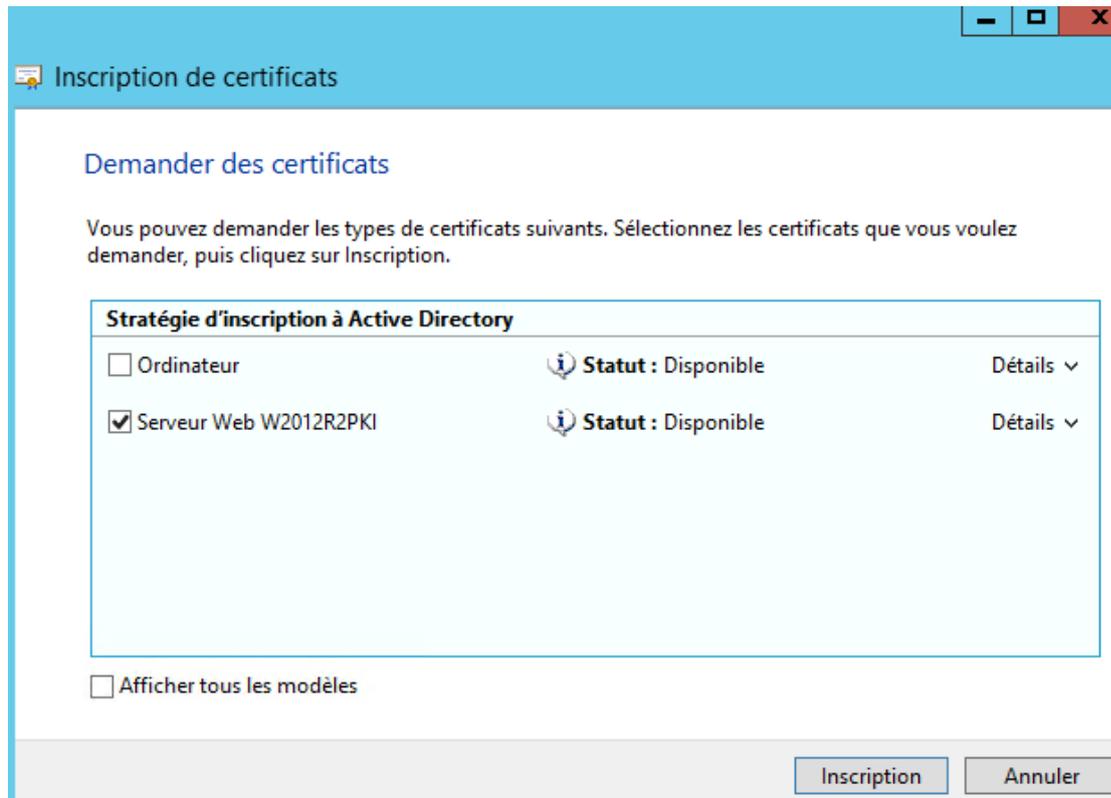
Objet Général Extensions Clé privée Autorité de certification Signature

Un nom convivial et une description facilitent l'identification et l'utilisation d'un certificat.

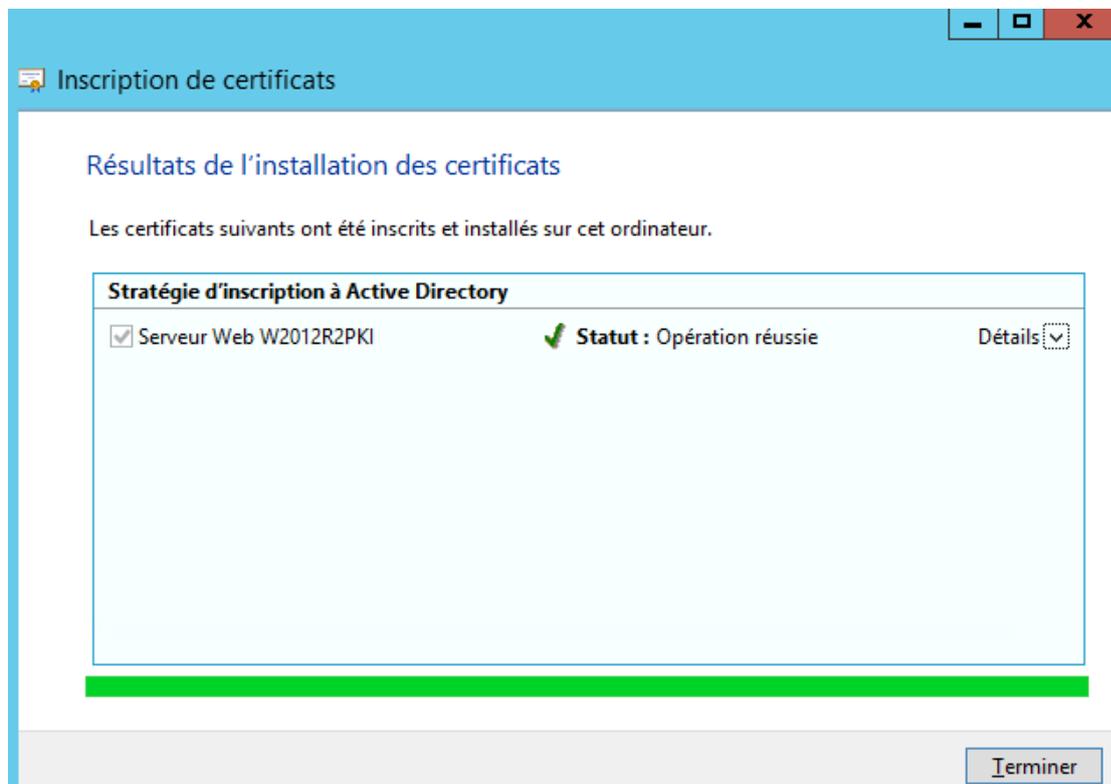
Nom convivial :
CERT_W2012R2PKI.GSB.local

Description :
[Empty text box]

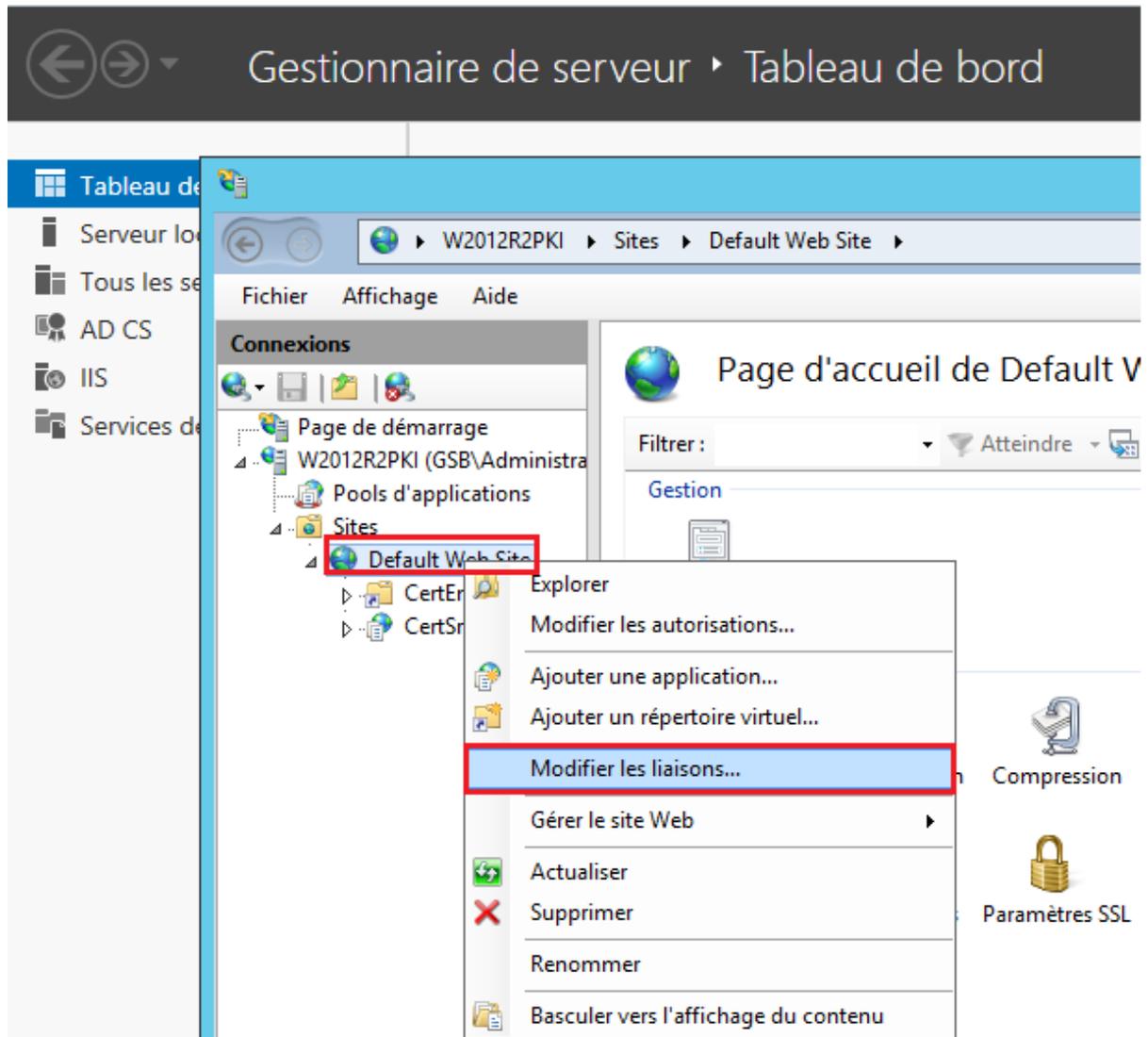
Cliquez ensuite sur « Inscription ».



Cliquez sur « Terminer »



Configuration serveur IIS :



Modifier la liaison de site

Type : Adresse IP : Port :

Nom de l'hôte :

Exiger l'indication de nom du serveur

Certificat SSL :

Liaisons de sites

Type	Nom de l'hôte	Port	Adresse IP	Informations sur...
https		443	*	

Navigation sur l'interface web :

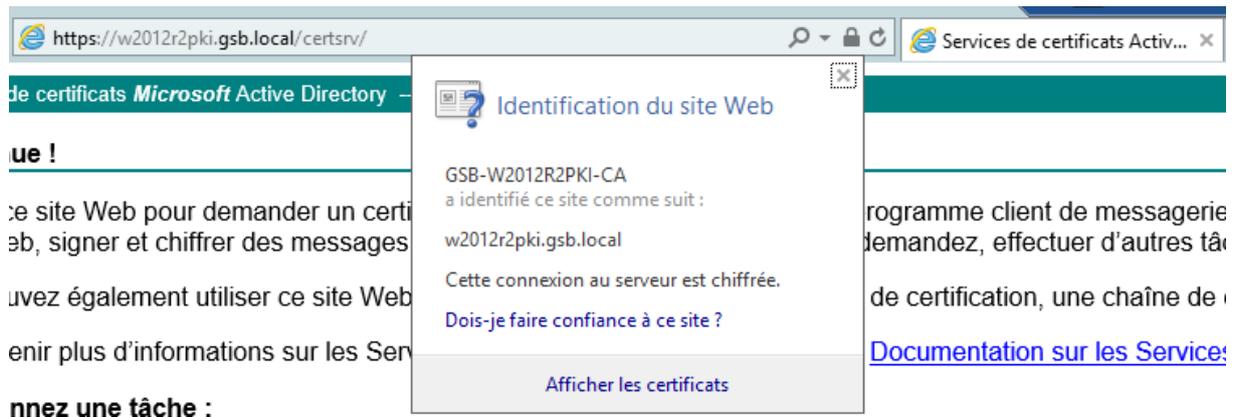
L'interface web permet de :

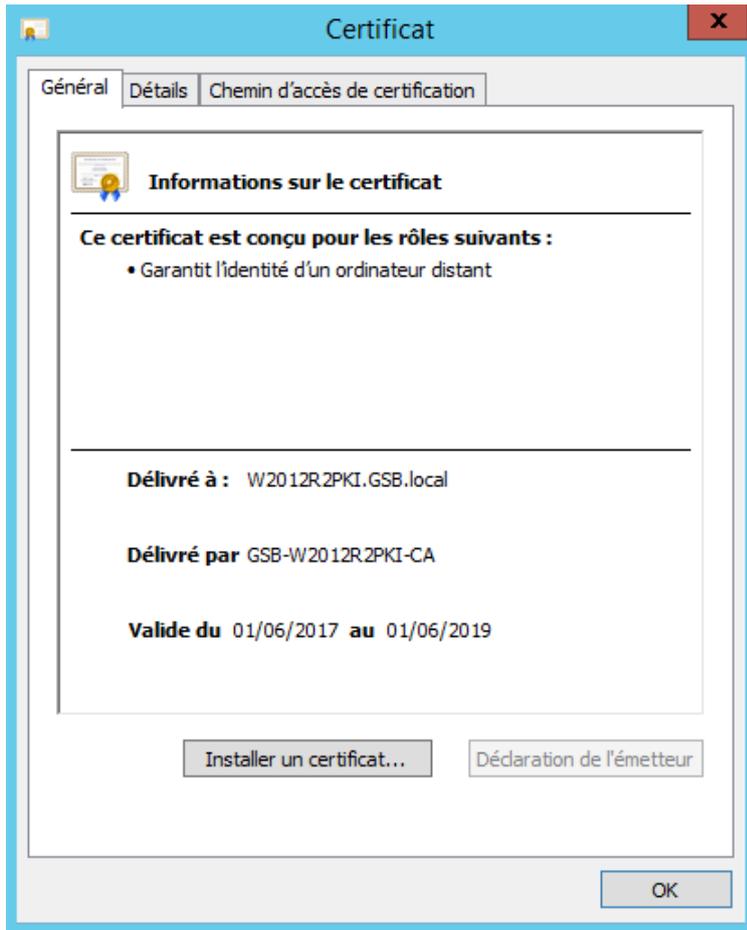
- Demander un certificat : En copiant une requête de certificat à faire signer par l'autorité de certification
- Afficher le statut d'une requête de certificat : Ne concerne que l'autorité autonome (donc cela ne nous concerne pas)
- Télécharger un certificat d'autorité de certification ... : Vous permet de télécharger le certificat de votre autorité, la chaîne de certificat d'autorités (si vous avez créé une autorité secondaire au lieu d'une autorité racine) et les listes de révocation (celle de base + les listes delta).

Accès à l'interface et vérification HTTPS :

On va ouvrir notre navigateur web et tapez dans la barre d'adresse :

https://W2012R2PKI.GSB.local/certsrv/





A partir de ce point mon autorité de certificat permet à chaque machine sur le domaine, pour n'importe quel utilisateur d'aller sur mon interface web avec une connexion certifiée.

Voici donc la première expression de besoin qui est réalisée :

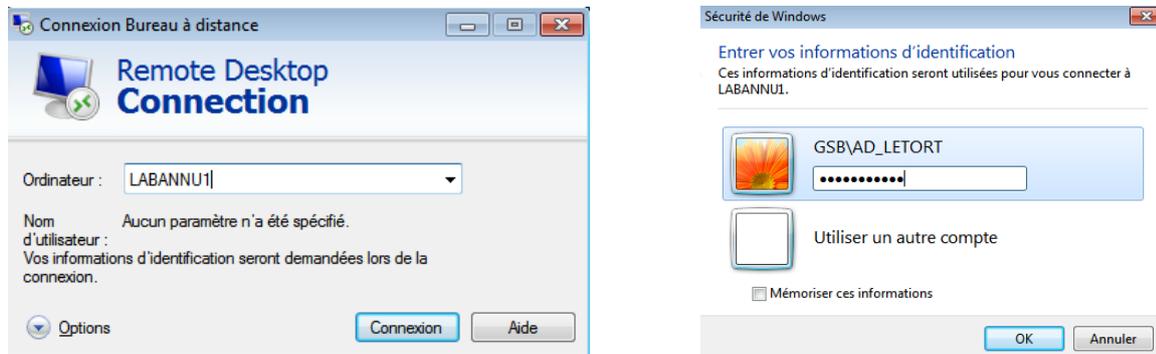
- ✓ Connexion certifiée à l'interface web du serveur IIS

Nous allons donc nous attaquer maintenant à la connexion certifiée sur un client en connexion à distance (connexion TSE)

Connexion certifié en TSE :

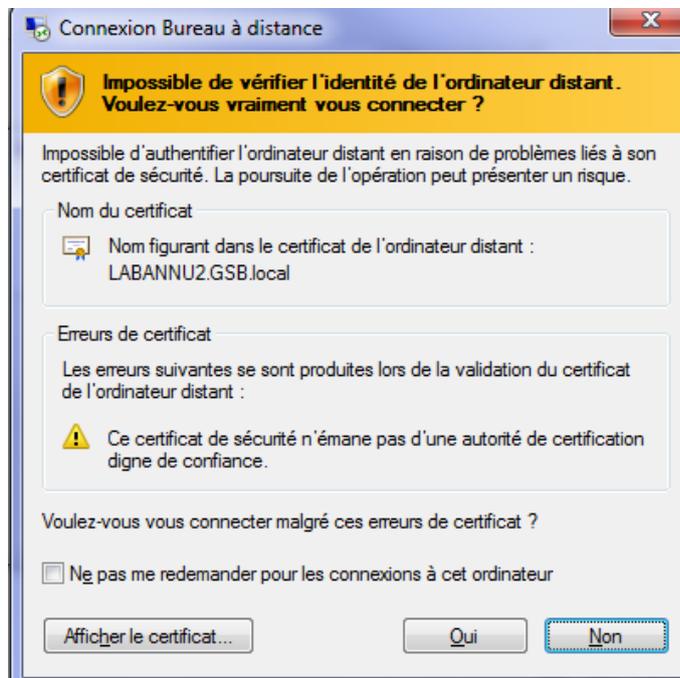
Faisons d'abord le test sans la configuration pour voir ce qu'on ne devrait pas obtenir !

Nous allons créer une VM W7 se nommant « W7TEST_OUT_TSE », puis nous allons nous connecter à un contrôleur du domaine (LABANNU1 // LABANNU2 ou sur serveur 2IS) avec un identifiant Admin du domaine car pour se connecter à un contrôleur de domaine il faut être admin du domaine.



AD_LETORT est un utilisateur promu au rang d'admin du domaine par mes soins afin de pouvoir tester mes différents tests à effectuer pour valider mes situations professionnels.

ID : AD_LETORT // MDP : Password123

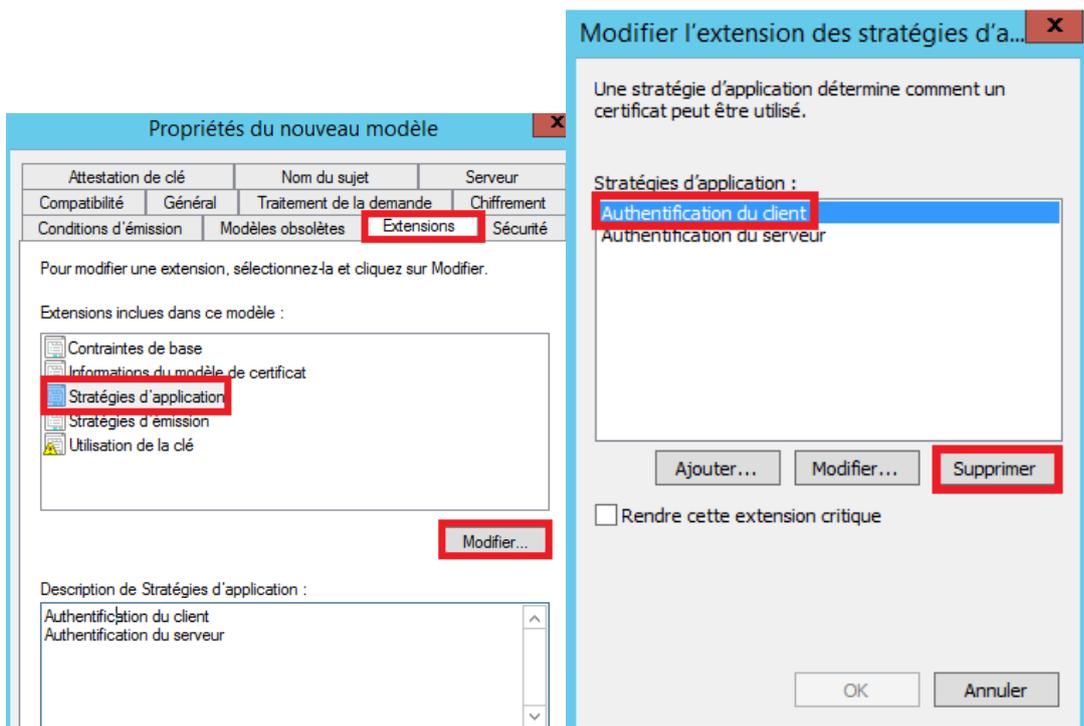
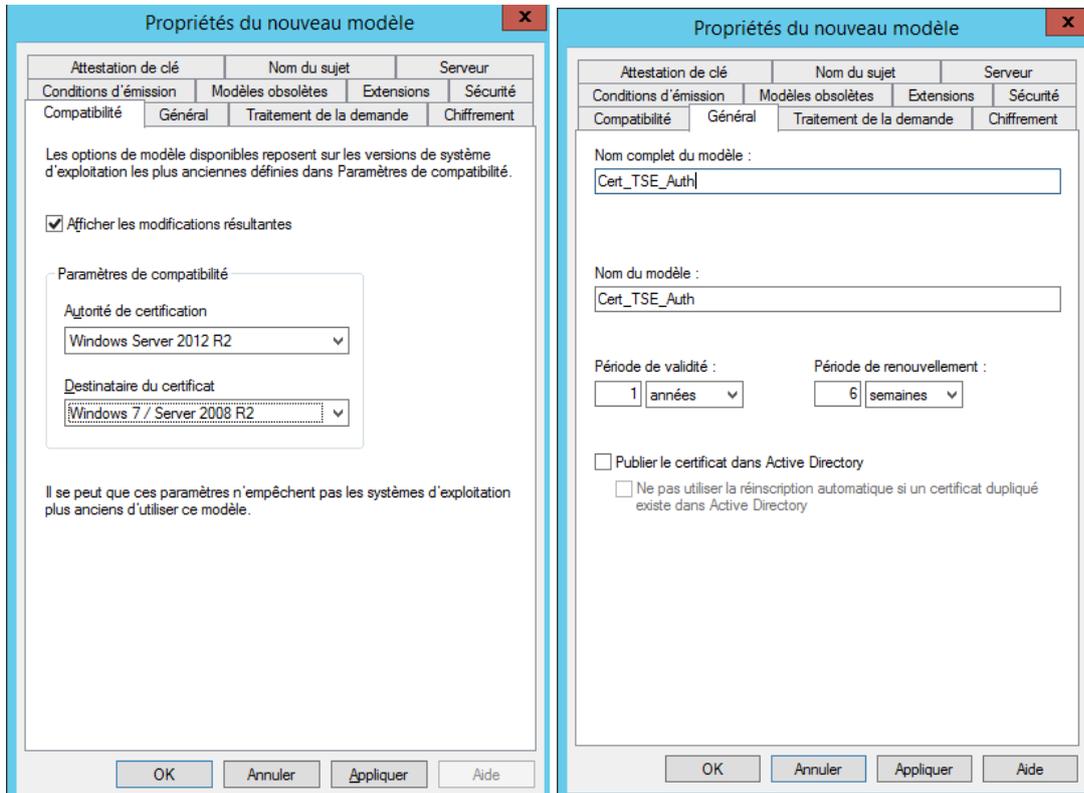


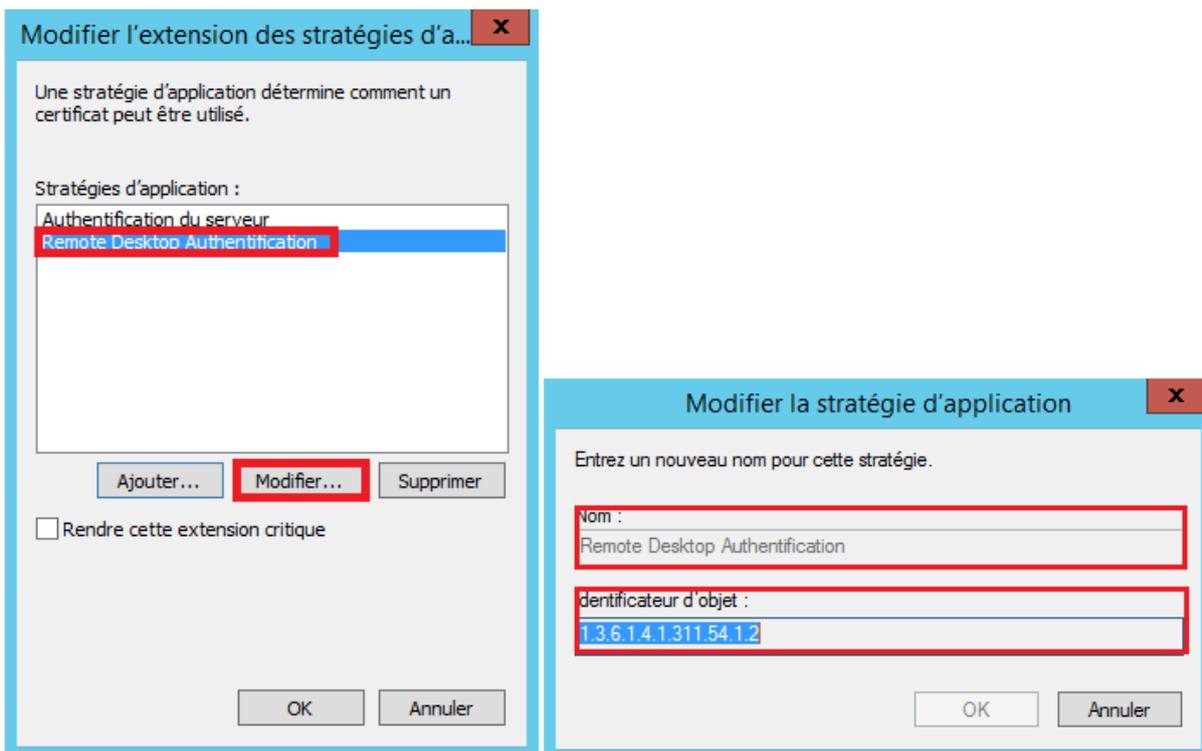
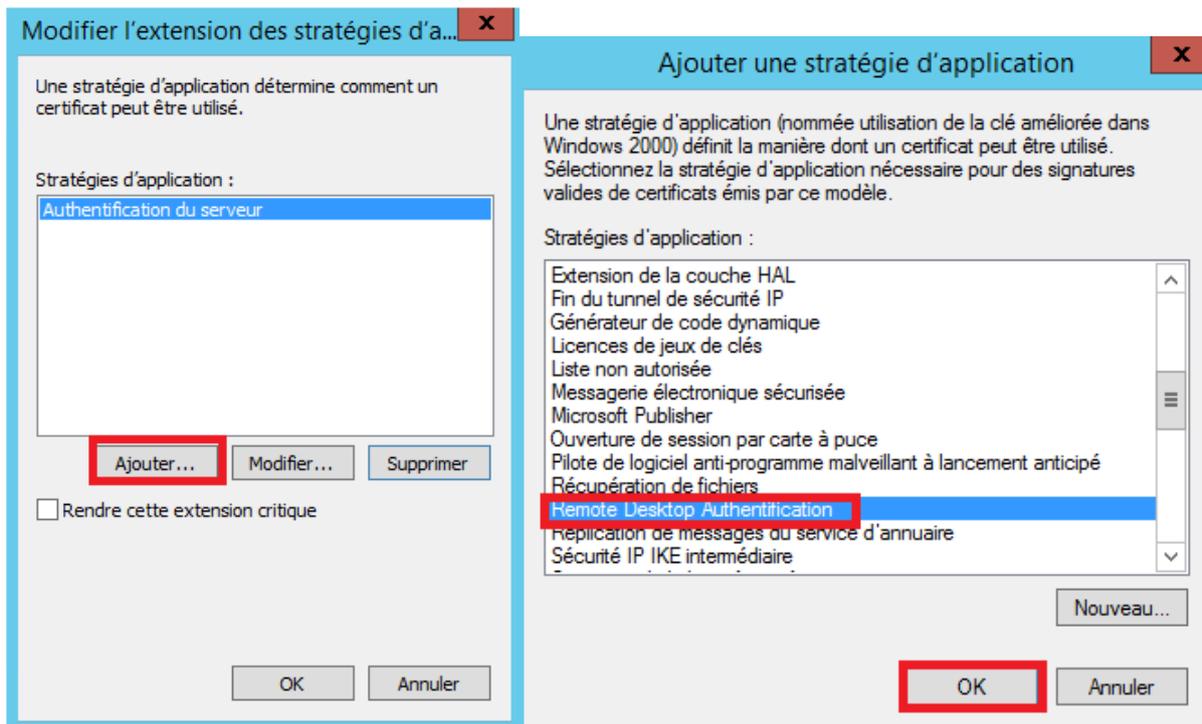
Une fois cette partie finit nous allons pouvoir nous connecter directement avec une connexion certifiée.

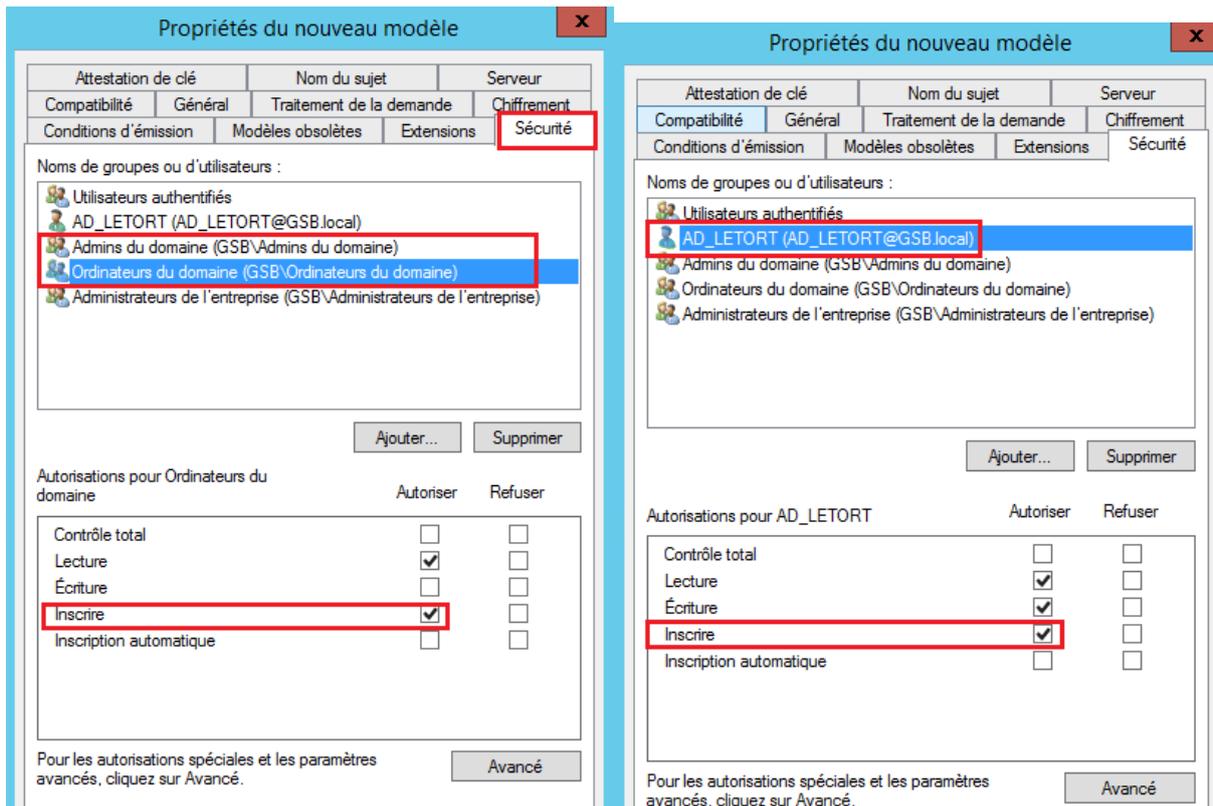
Nous allons aller sur l'AD puis dans « Autorité de certification ». Nous allons ensuite faire un clic droit sur modèles de certificats puis gérer :

On arrive dans la console des modèles de certificat, on va faire un clic droit sur le modèle Ordinateur et faire « Dupliquer le modèle » :

Voici les modifications à faire :

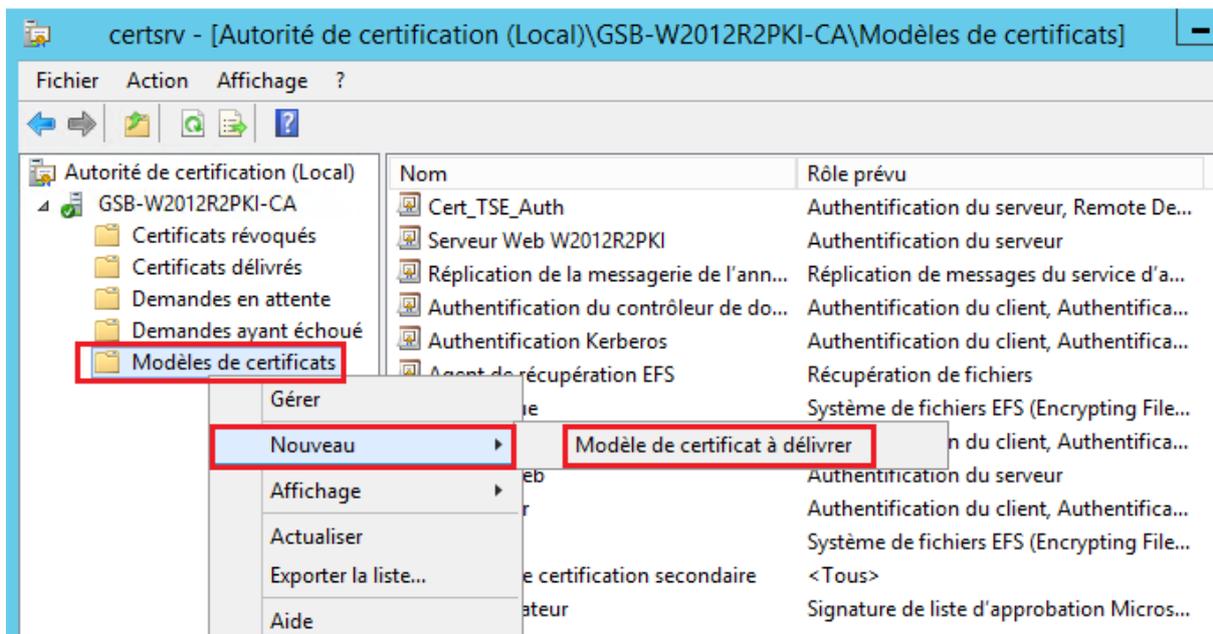






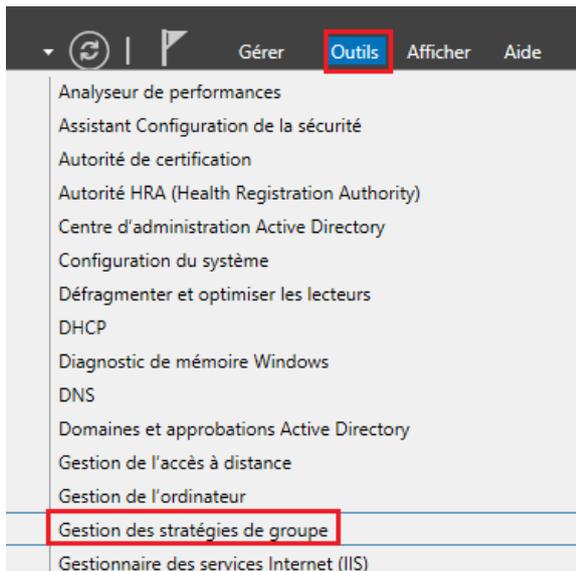
Une fois toutes ces modifications faites, nous allons pouvoir faire ok !

Nous allons ensuite aller dans les modèles de Certificats :

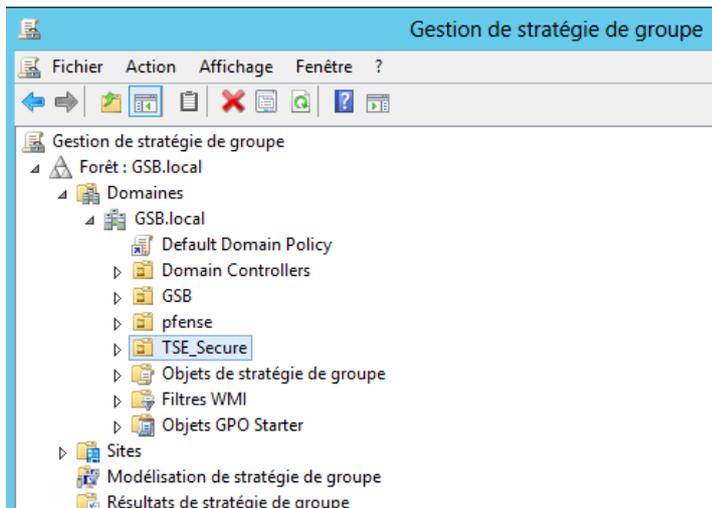


On va ensuite trouver notre modèle est cliquer dessus, et faire ok

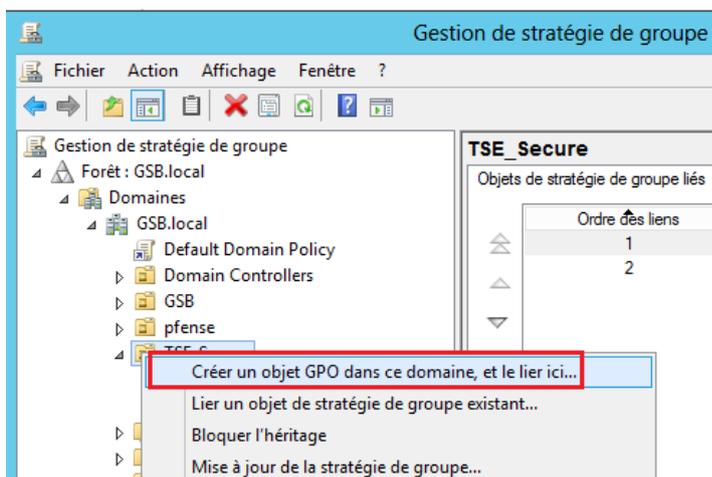
Nous allons ensuite créer la GPO qui correspond à notre modèle :



On va ensuite créer une UO correspondant à notre certification, on va l'appeler « TSE_Secure » :



On va pouvoir ensuite créer une GPO pour cela on va directement faire un clic droit sur TSE_Secure et faire

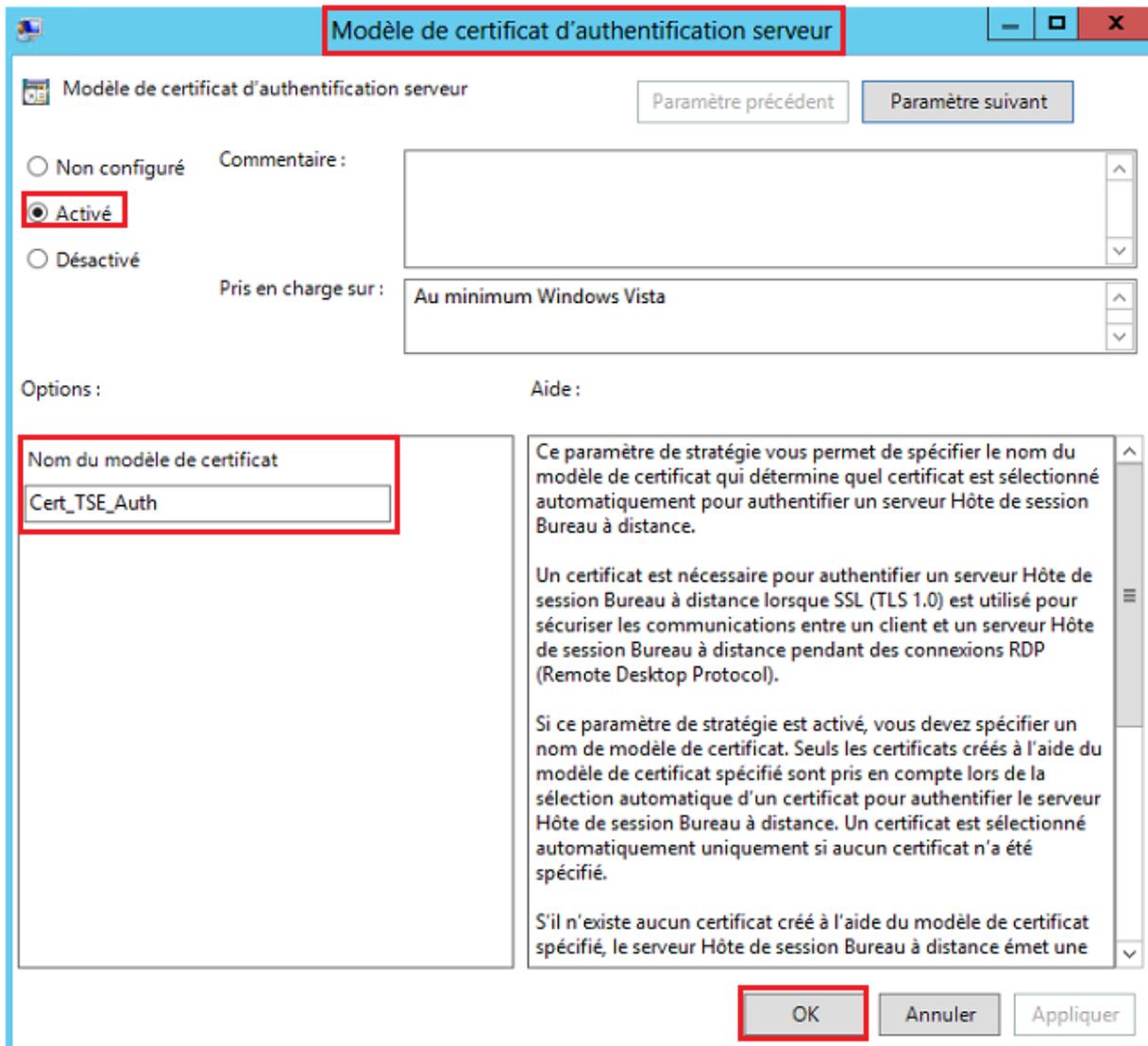




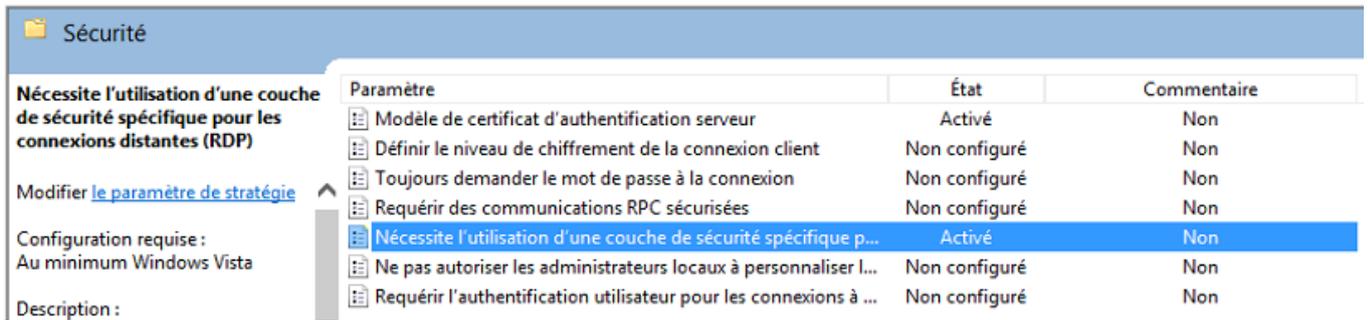
Une fois créée elle apparaît dans les Objets de stratégie de groupe liés, nous allons simplement faire un clic droit dessus et faire gérer :

Puis « Configuration d'ordinateur », puis « modèles d'administration ... », puis « Composants Windows », puis « Service Bureau à distance », puis « Hôte de la session Bureau à distance », puis « Sécurité », et enfin « Modèle de certificat d'authentification serveur ».

On arrive donc sur cette page, il suffira ensuite d'activer le modèle et de choisir le modèle que nous avons créé précédemment !!

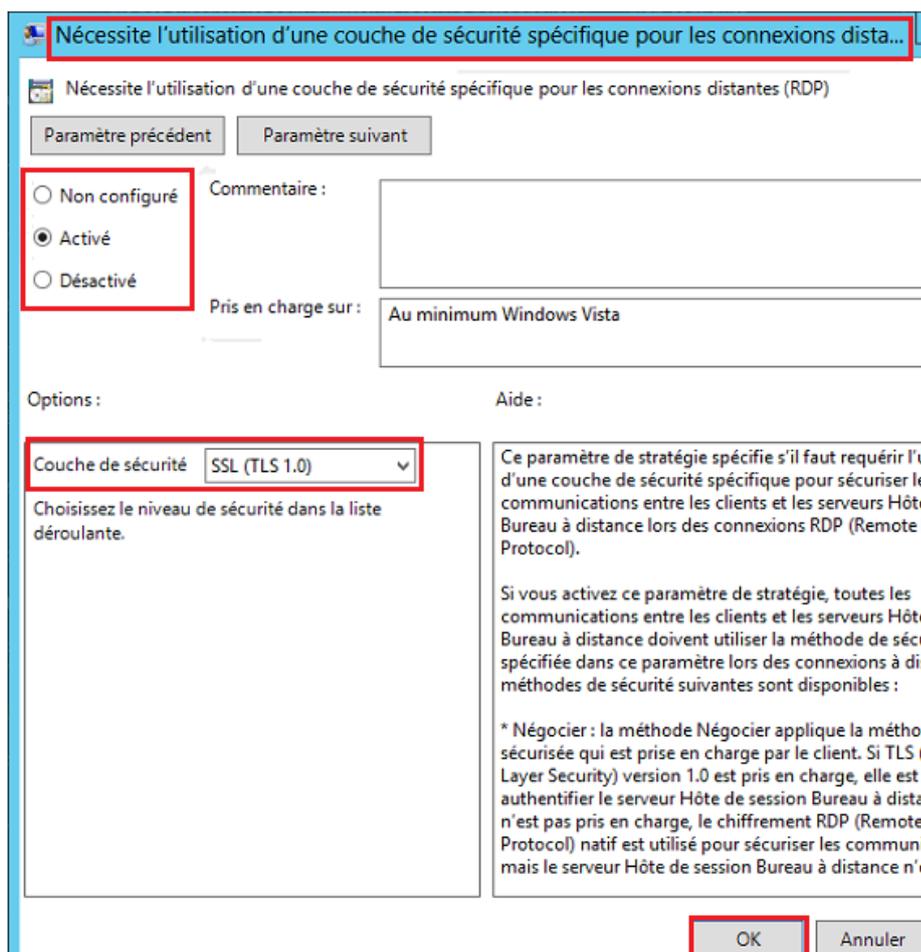


Ensuite sur la même page, on va aller sur « Nécessite l'utilisation d'une couche de sécurité » :



Paramètre	État	Commentaire
Modèle de certificat d'authentification serveur	Activé	Non
Définir le niveau de chiffrement de la connexion client	Non configuré	Non
Toujours demander le mot de passe à la connexion	Non configuré	Non
Requérir des communications RPC sécurisées	Non configuré	Non
Nécessite l'utilisation d'une couche de sécurité spécifique p...	Activé	Non
Ne pas autoriser les administrateurs locaux à personnaliser l...	Non configuré	Non
Requérir l'authentification utilisateur pour les connexions à ...	Non configuré	Non

Nous allons donc l'activer et mettre en couche de sécurité SSL (TLS 1.0), puis faire ok.



Nécessite l'utilisation d'une couche de sécurité spécifique pour les connexions distantes

Paramètre précédent Paramètre suivant

Non configuré Commentaire :
 Activé
 Désactivé

Pris en charge sur : Au minimum Windows Vista

Options : Aide :

Couche de sécurité : **SSL (TLS 1.0)**

Choisissez le niveau de sécurité dans la liste déroulante.

Ce paramètre de stratégie spécifie s'il faut requérir l'utilisation d'une couche de sécurité spécifique pour sécuriser les communications entre les clients et les serveurs Hôte Bureau à distance lors des connexions RDP (Remote Desktop Protocol).

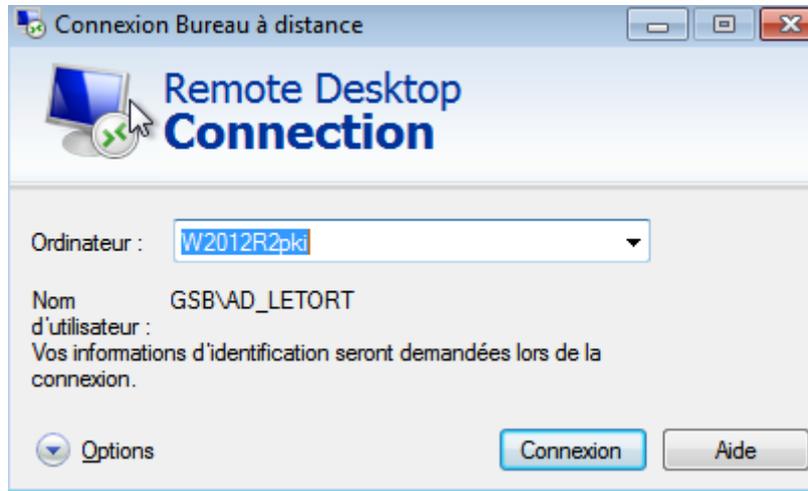
Si vous activez ce paramètre de stratégie, toutes les communications entre les clients et les serveurs Hôte Bureau à distance doivent utiliser la méthode de sécurité spécifiée dans ce paramètre lors des connexions à distance. Les méthodes de sécurité suivantes sont disponibles :

* Négocier : la méthode Négocier applique la méthode sécurisée qui est prise en charge par le client. Si TLS (Transport Layer Security) version 1.0 est prise en charge, elle est utilisée pour authentifier le serveur Hôte de session Bureau à distance. Si TLS n'est pas pris en charge, le chiffrement RDP (Remote Desktop Protocol) natif est utilisé pour sécuriser les communications, mais le serveur Hôte de session Bureau à distance n'est pas sécurisé.

OK Annuler

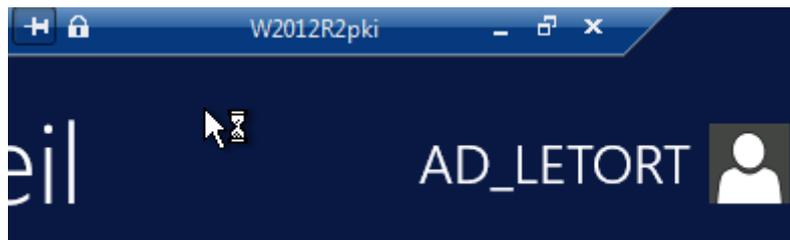
Tout est maintenant configuré pour la GPO.

Nous allons pouvoir maintenant faire les tests et regarder si les certificats sont délivrés, nous allons prendre notre VM de test qui se nomme « W7Test_Situation » et qui se situe dans l'UO sur l'AD ou nous avons appliqué la GPO :



AD_LETORT // Password123

Et nous nous connectons bien sur notre serveur d'autorité de certification :



Les deux expressions de besoins sont maintenant remplies !

- ✓ Connexion certifiée à l'interface web du serveur IIS
- ✓ Connexion certifiée à distance à partir d'un client client sur un contrôleur de domaine ou un Serveur d'autorité de certification