Windows 2016 – Works-Folder

Windows 2016 – Works folder – dossiers de travail windows 10

Michel Cabaré – Ver 1.1 – décembre 2016-

http://WWW.CABARE.NET ©

Windows 2016 - Works Folder

Michel Cabaré – Ver 1.1 – Décembre 2016

www.cabare.net ©

TABLE DES MATIERES

WORKS FOLDER

Works Folder – Dossier de travail

Les **Works Folder** ou « Dossier de travail » font partie des nouveautés de Windows serveur 2012 R2 et Windows 8.1. Il s'agit d'un dossier de synchronisation entre différents périphérique appartenant au même utilisateur.

Il s'agit d'utiliser un nouveau protocole de synchronisation pour les données sur un serveur **on-premise** (et non **SaaS**)

Les **Works Folders** sont une nouvelle fonctionnalité apparues pour le **rôle de Services de fichiers et de stockage**

L'objectif c'est de faire en sorte que l'on partage sur plusieurs appareils différents une même base qui est en fait centralisée sur un serveur interne de l'entreprise. Lorsque l'on modifie un fichier sur un appareil donné, (stocké dans un dossier nommé **Work Folders**), il y a mise à jour des tous les autres endroits de stockages appartenant à cet utilisateur, qu'il s'agisse du serveur central, (mais à la limite c'est le seul qu'il n'utilise pas directement…) , mais aussi de tous les autres périphériques utilisés.

En d'autres termes, lorsqu'un utilisateur crée ou modifie un fichier dans son **Work Folders**, depuis n'importe lequel de ses PC ou tablettes, il y a :

- d'abord une réplication automatique via **Secure Sockets Layer (SSL)** sur le serveur d'entreprise
- puis une réplication sur tous les autres périphériques configurés, dans leurs dossiers respectifs **Work Folders**

Version configuration minimale

Coté Serveur:	Windows 2016 ou 2012R2, dédié car va héberger un IIS
	Un espace dossier de stockage NTFS
Coté Client:	Windows 10 - Windows 8.1

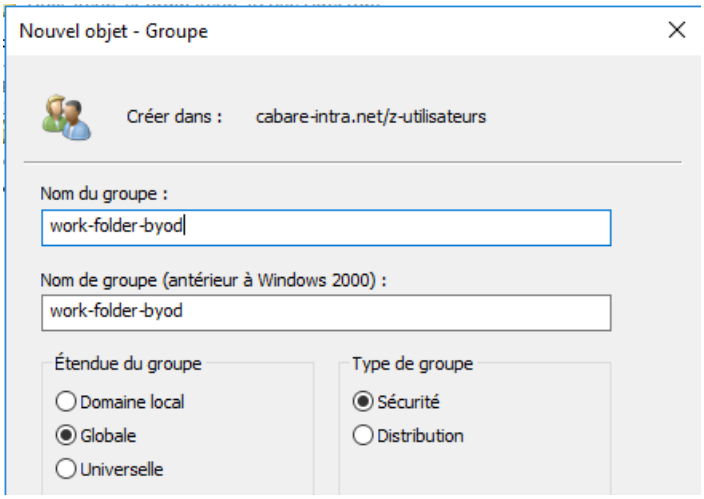
N.B: Si l'ouverture avec SSH est requise, alors la gestion des certificats sera obligatoire

Groupe de sécurité utilisateur Work Folder

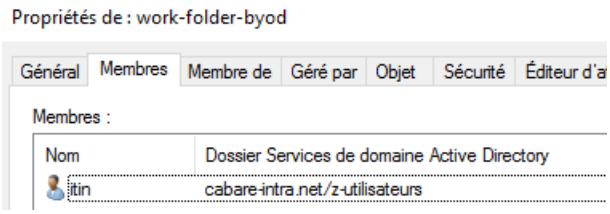
Pour que l'on s'y retrouve, il serait bien de se créer un groupe de sécurité spécifique à l'utilisation de cette fonctionnalité.

En effet les partages vont être gérés avec de la sécurité **NTFS**, et donc il peut être plus simple de créer un **groupe**, auquel on donnera les droits au dossier **work folder** stocké sur le serveur interne.

Dans l'AD on va se créer donc un nouveau **Groupe** de **Sécurité Globale** dans l'exemple nommé ***work-folder-byod***



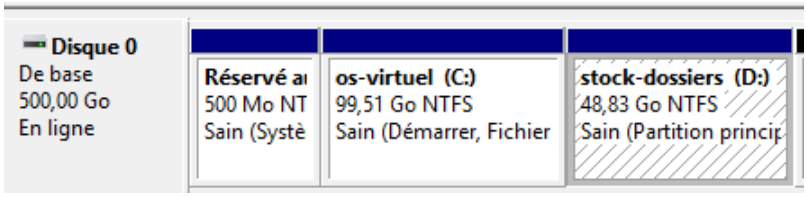
avec au moins un futur utilisateur itinérant… dans l'exemple ***itin***



Dossier NTFS sur volume dédié

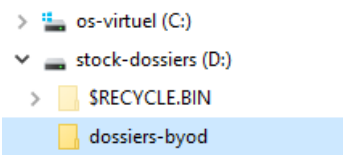
Il faut préparer l'emplacement de nos dossiers de stockage dans un espace **NTFS**, dédié

par exemple ici un Volume ***d:***



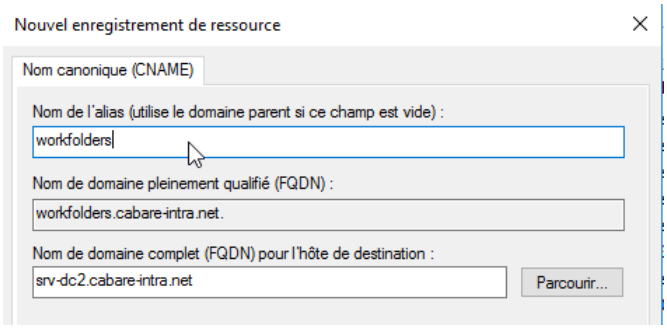
avec

avec le dossier ***dossiers-byod***



Alias Cname DNS (option)

Ce n'est pas obligatoire, mais si on veut ensuite utiliser des **GPO** et s'affranchir des contraintes de re-nomage – modifications, on peut créer dans le **DNS** un **alias** pour le nom du serveur hébergeant les services **Work Folder**



Si le serveur hébergeant les fonctionnalités **Work Folder** est nommé par exemple ***srv-dc2.cabare-intra.net***,

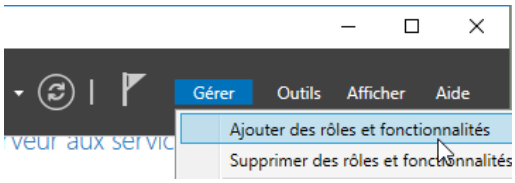
on peut faire un alias du genre ***workfolder***!

Nom	Type	Données	Horodateur
workfolders	Alias (CNAME)	srv-dc2.cabare-intra.net.	statique

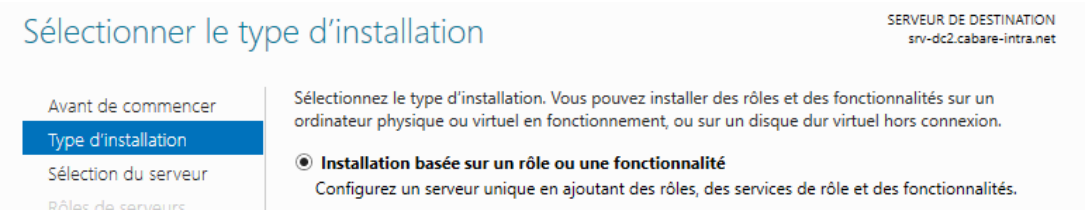
WORKS FOLDER – SERVEUR

Ajout du Rôle Dossier de travail

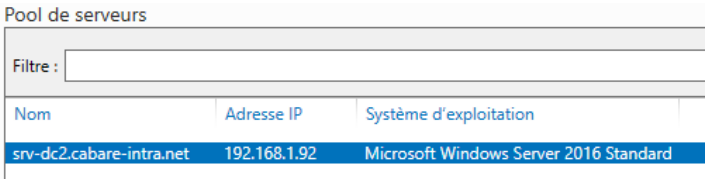
On a dans l'exemple un serveur ***srv-dc2*** sur lequel on souhaite installer cette fonctionnalité. Dans le **gestionnaire de serveur** on demande Gérer, **Ajouter des Rôles et des Fonctionnalités**



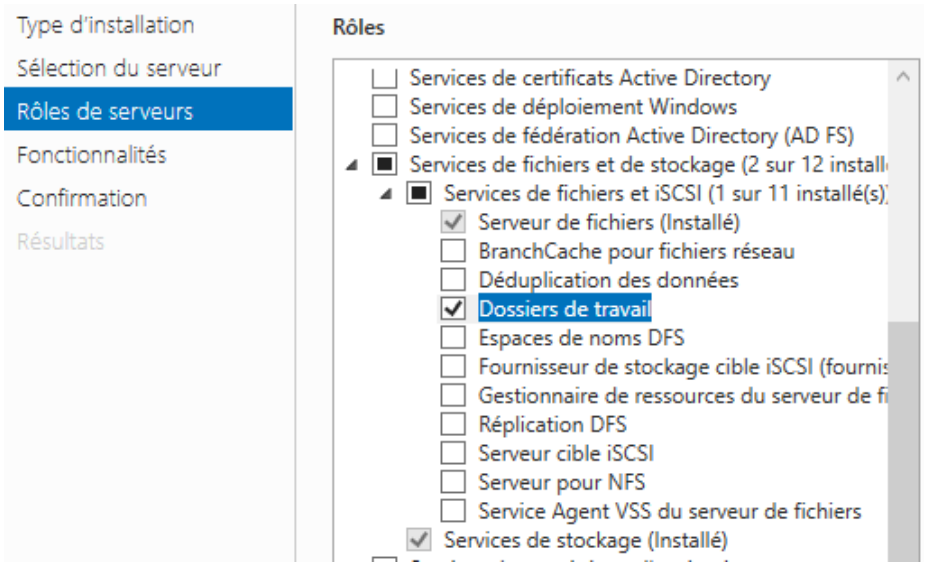
On indique que l'on veut un rôle …



On indique notre serveur

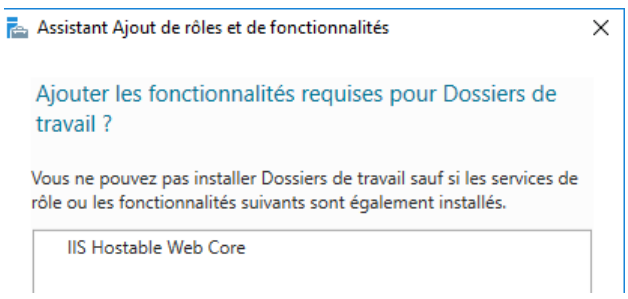


Et on coche dans **Services de fichiers et de stockage** que **Dossier de travail**

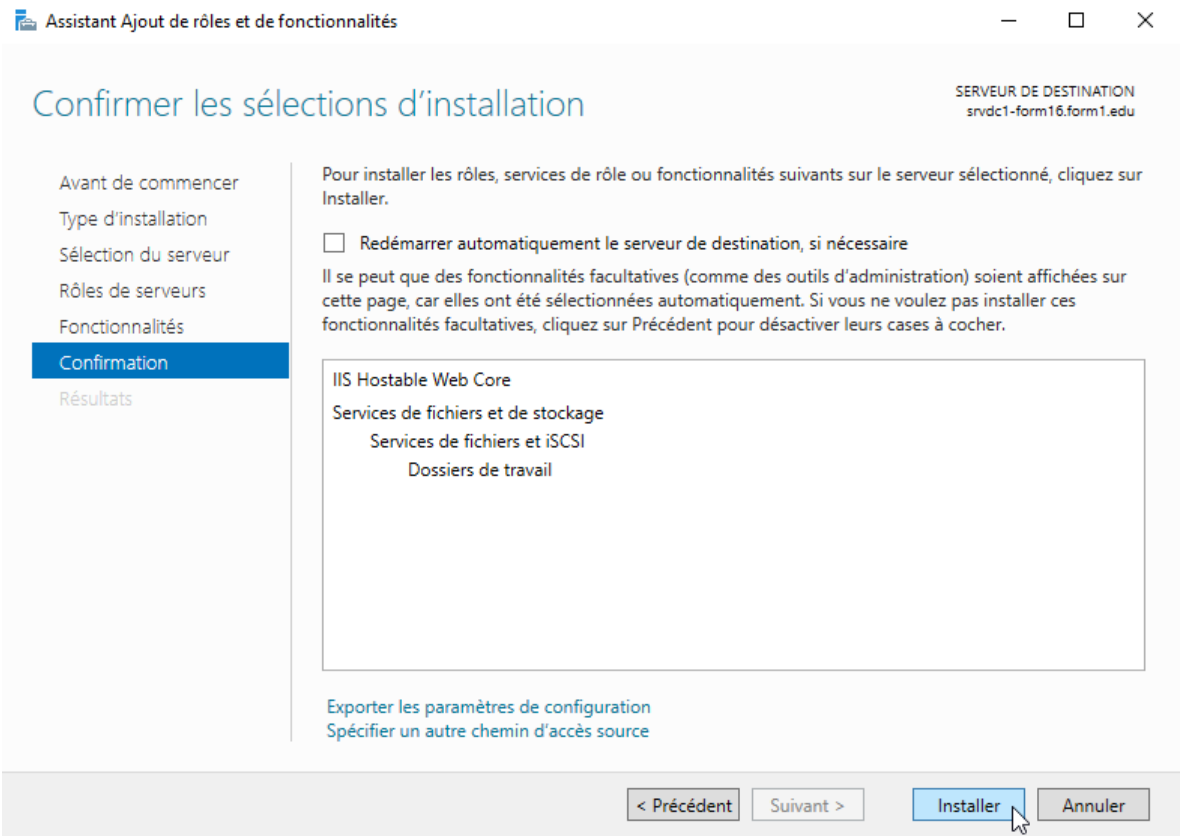


Et les fonctionnalitées automatiquements associées, c'est-à-dire

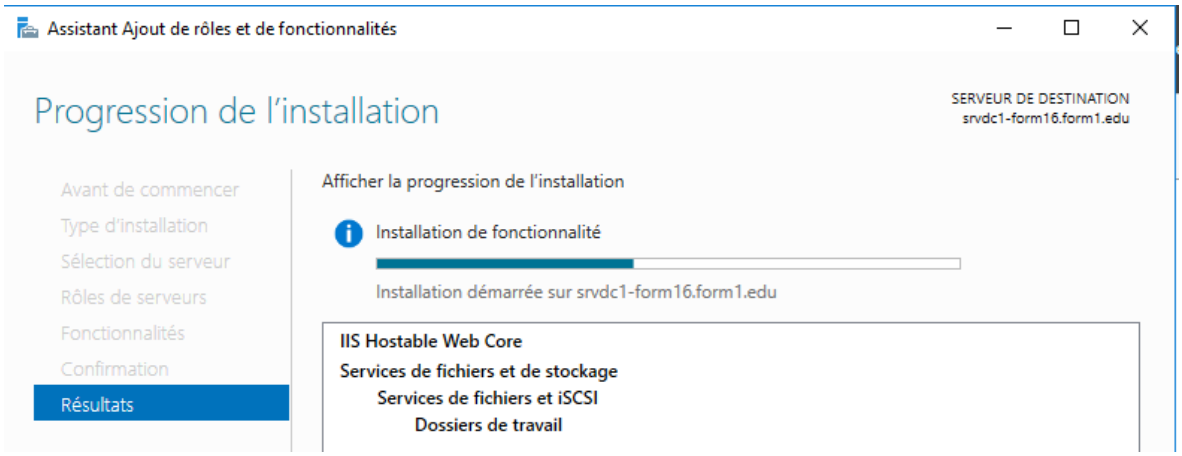
IIS Hostable Web Core



On confirme en demandant **Installer**

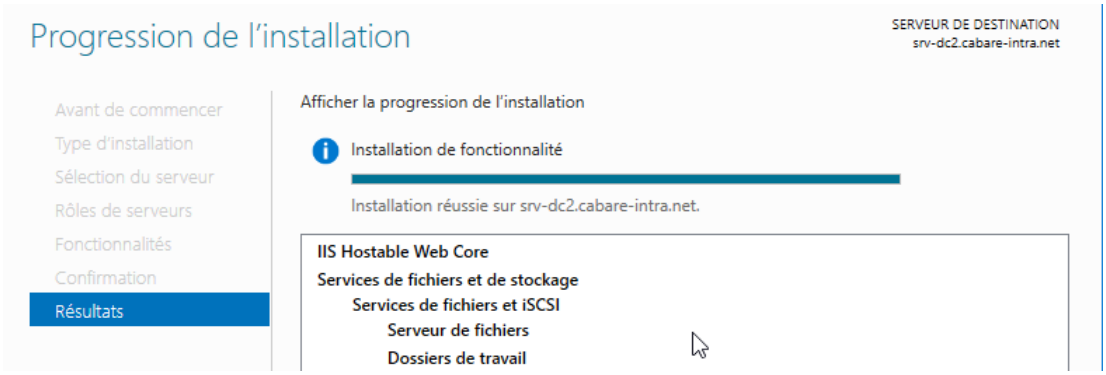


Cela peut prendre quelques minutes

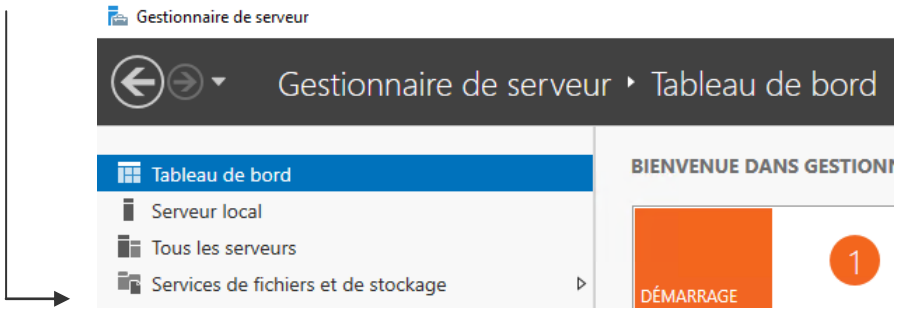


Paramétrage du Rôle Dossier de travail

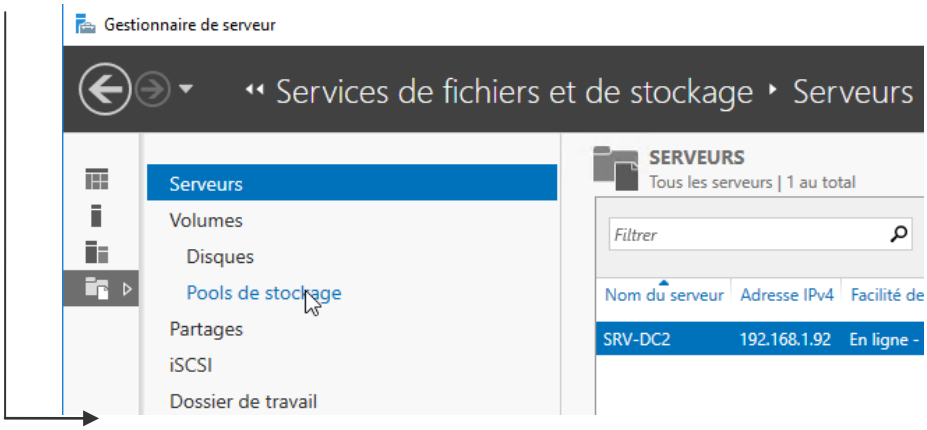
Maintenant que le rôle est installé il faut le configurer.



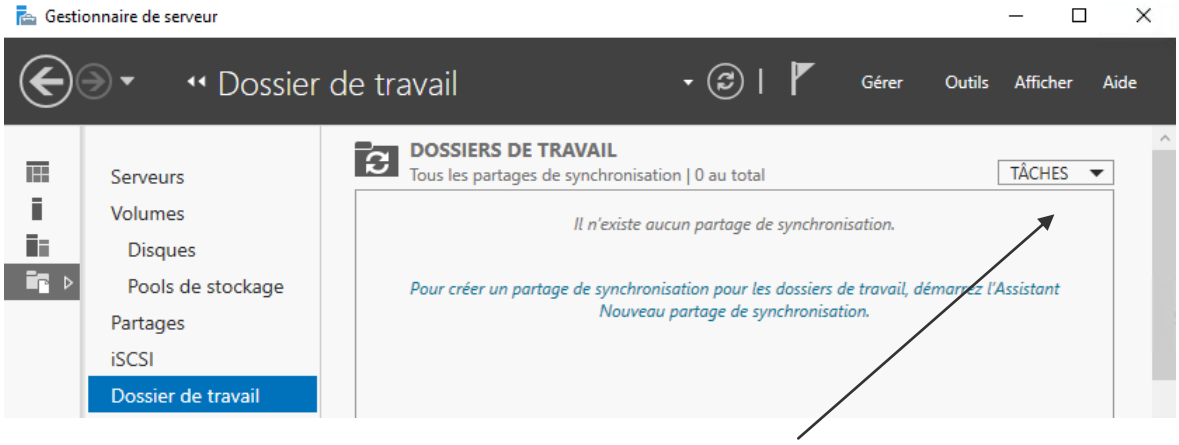
Dans le **gestionnaire de serveur**, on demande **Services de fichiers et de stockage**,



Dans lequel on va demander **Dossier de travail**



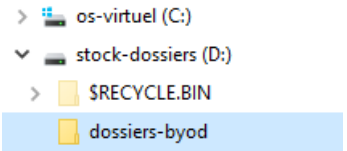
Où l'on voit qu'il n'y a aucun **dossier de travail** installé



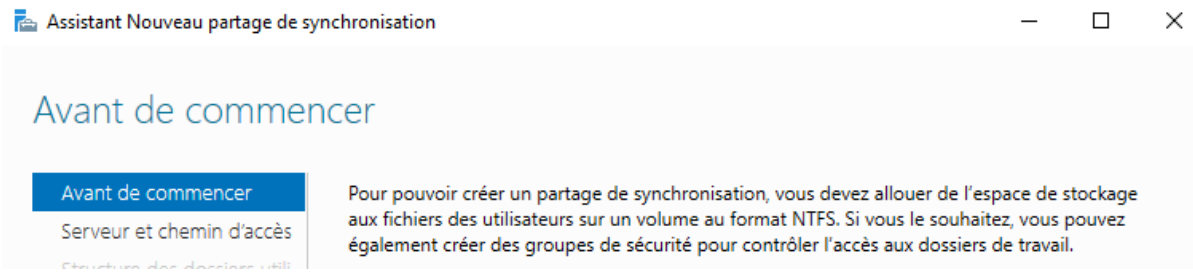
On demande alors via **Tâches** d' ajouter un **Nouveau partage de synchronisation**

cela déclanche un assistant

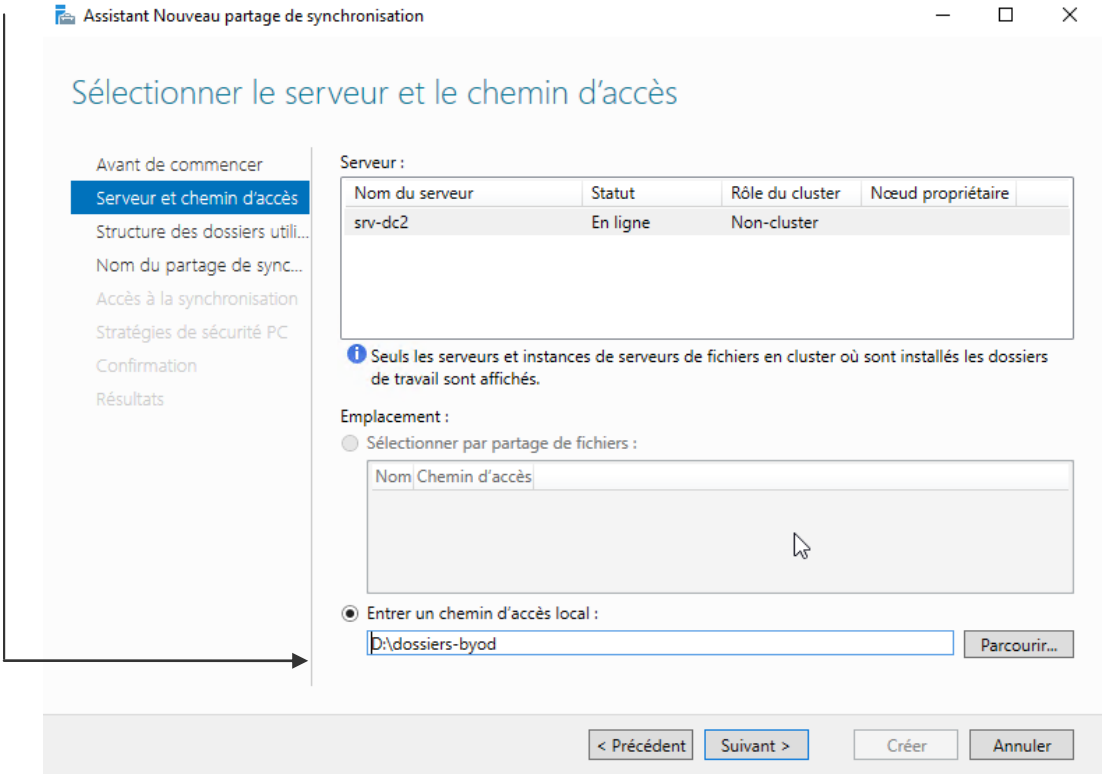
N.B : On a déjà préparé l'emplacement de nos dossiers de stockage dans un espace **NTFS dédié**, par exemple ici un Volume ***d:*** avec le dossier ***dossiers-byod***



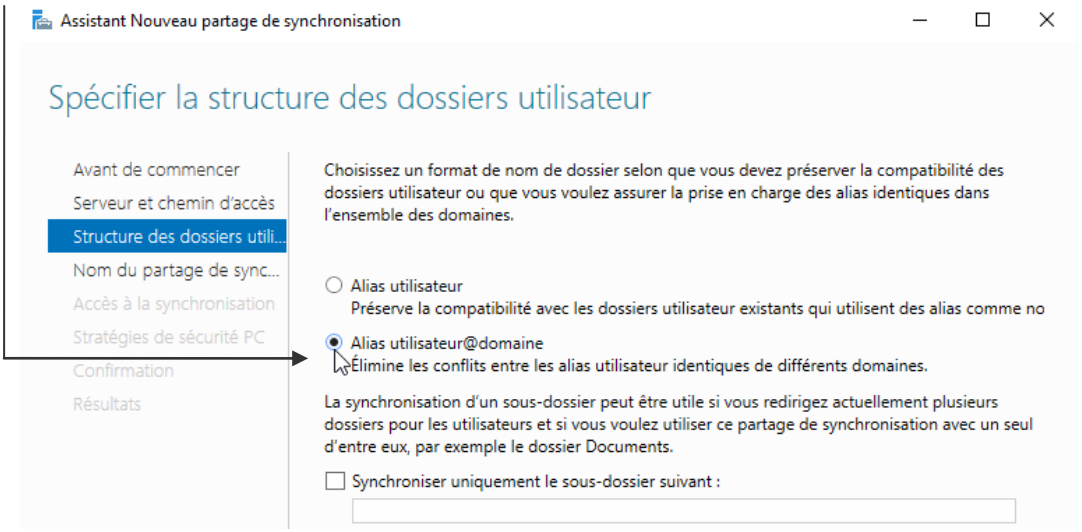
L'assistant se déroule :



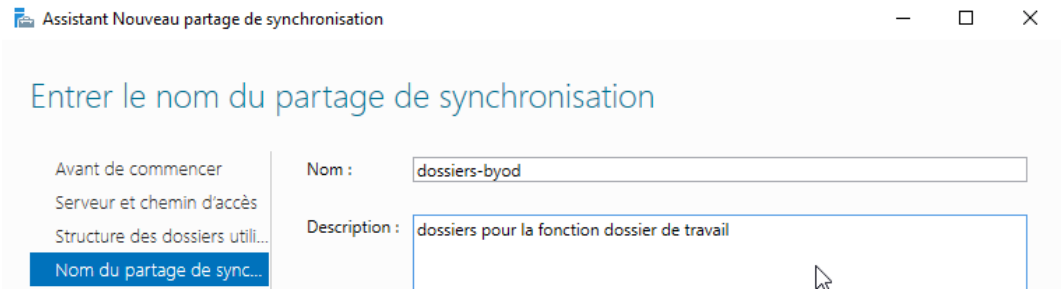
On choisit le serveur, et le chemin local de stockage de nos futurs **dossiers de travail**



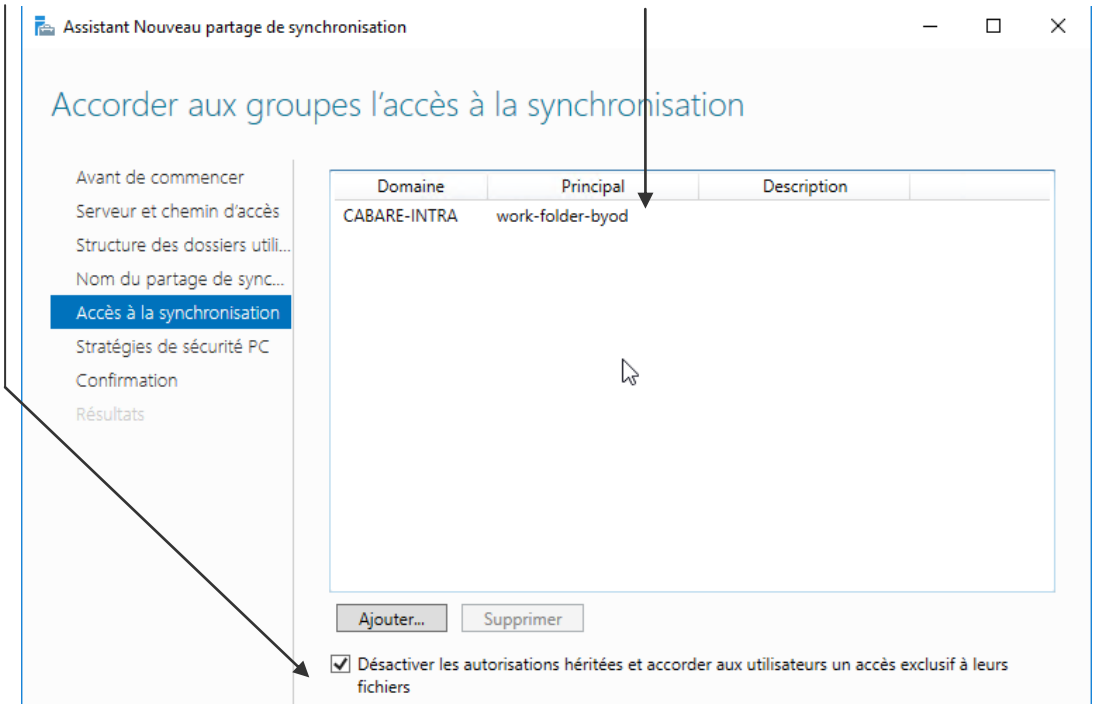
On choisit plutôt une appellation complète de type **utilisateur@domaine**



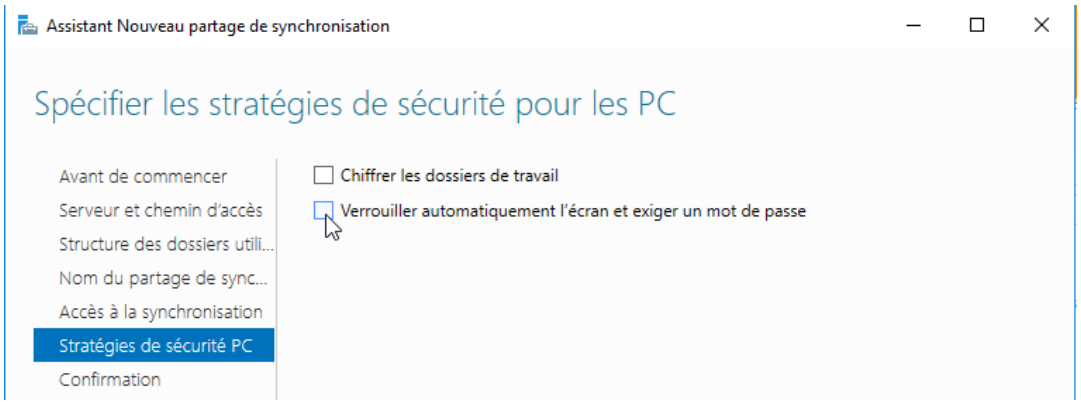
On donne un nom de partage



On affecte le groupe de sécurité crée auparavant, et on coche ou non **Désactiver les autorisations héritées** (si l'on souhaite que l'administrateur puisse accéder à ces dossiers on décoche)



Politique de sécurité sur le partage (du client):

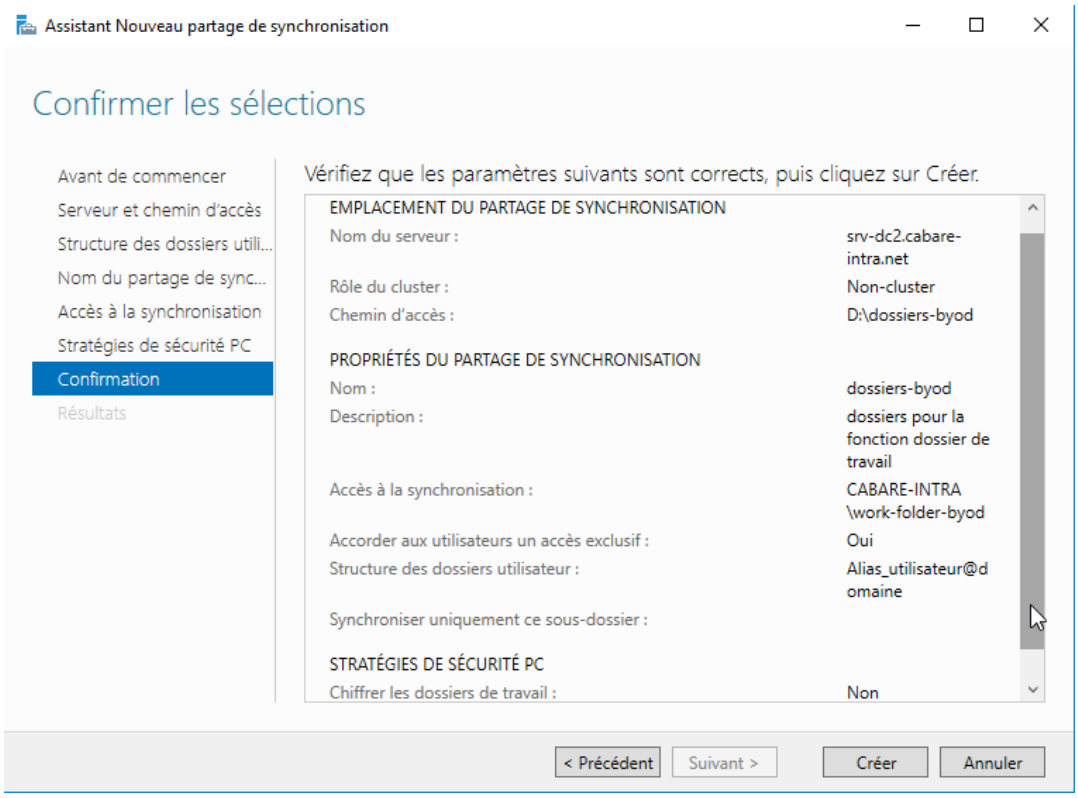


Dans l'état actuel de la technologie, on n'impose rien !

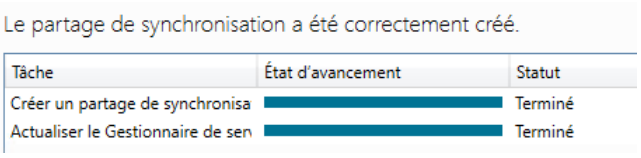
le **chiffrement EFS** des fichiers synchronisés sur le poste client

le verrouillage de l'écran et un mot de passe obligatoire

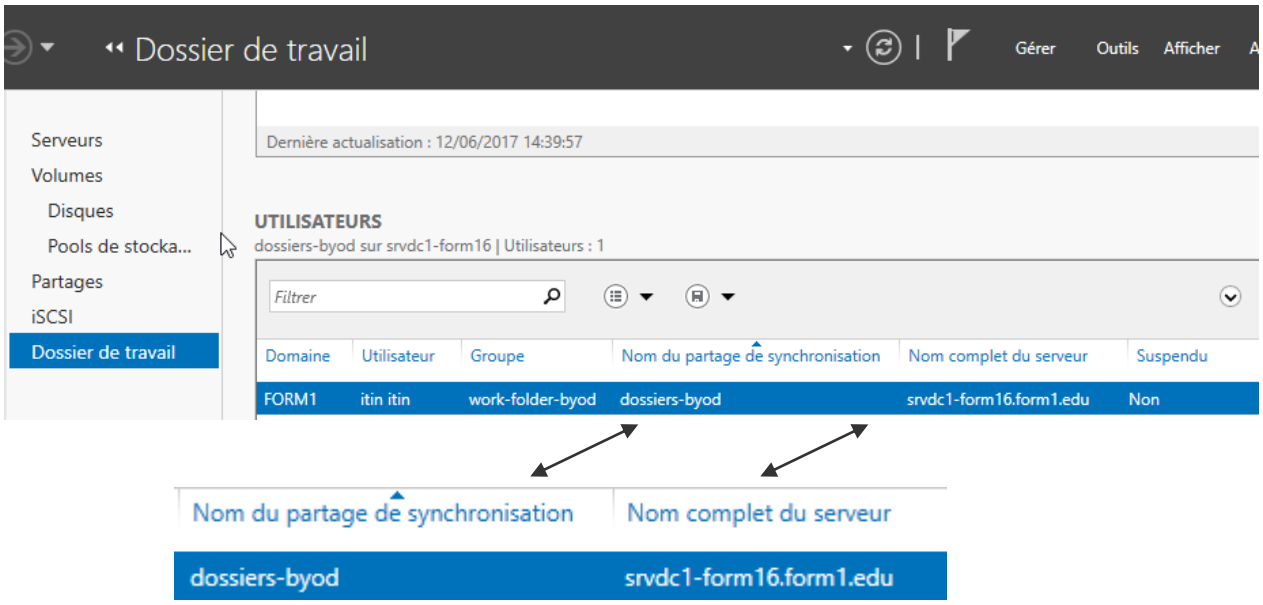
on confirme



Et on obtient

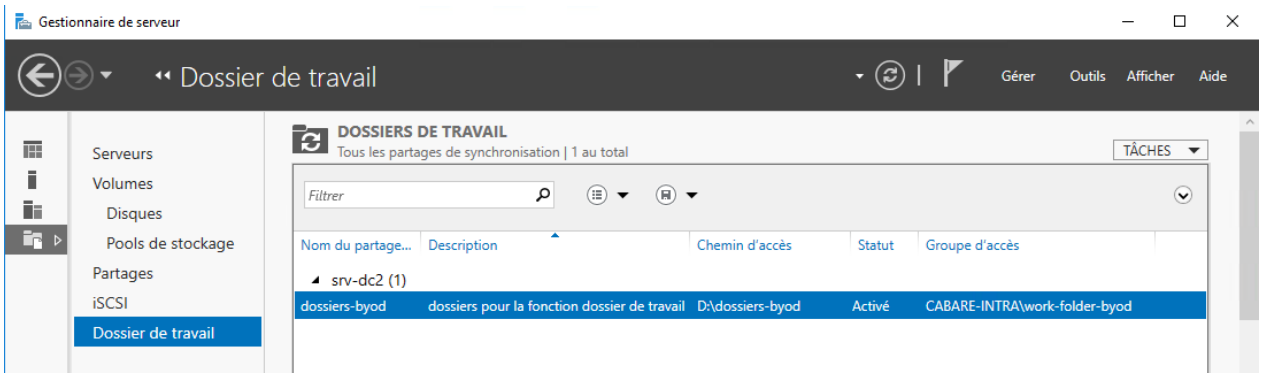


Actuellement donc on se retrouve donc avec un accès ouvert à la syncrhonisation des work folder via l'URL Domaine\nom de partage que l'on retrouve dans **Dossiers de travail** – **Utilisateurs** :

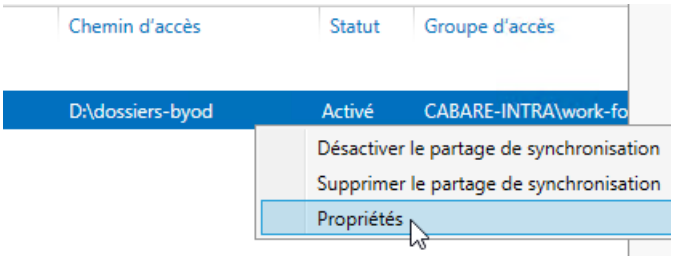


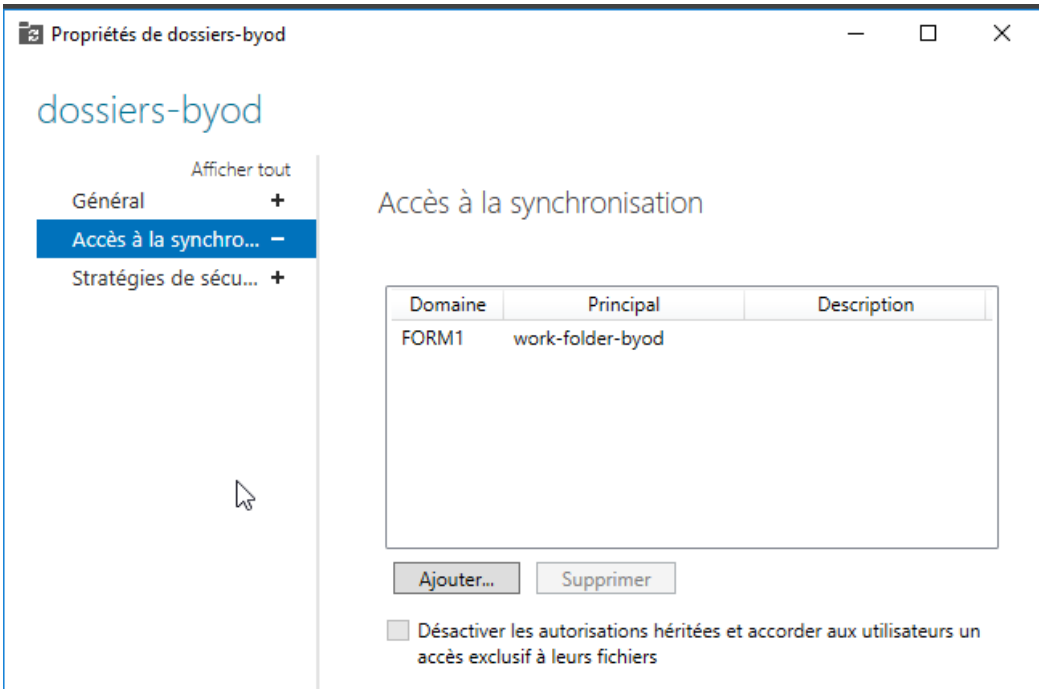
Interface de gestion Dossier de travail

Depuis le gestionnaire de serveur,



Sur lequel on peut demander **Propriétés** par exemple pour remodifier notamment les autorisations d'accès (accès synchronisation)

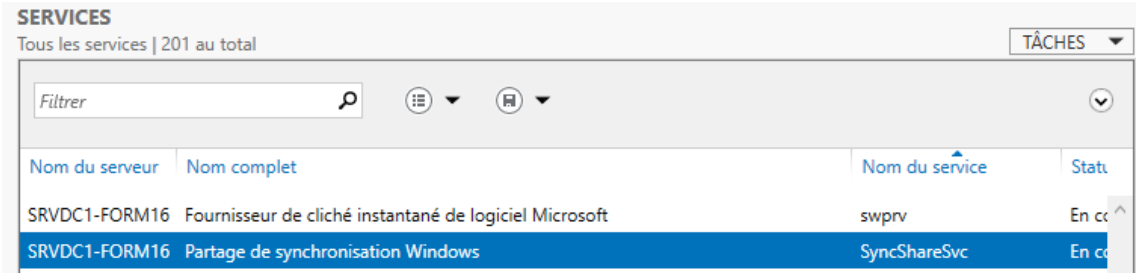




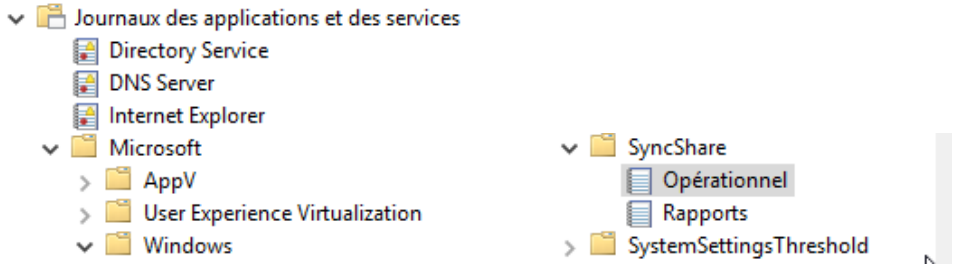
Plus bas on peut voir aussi

Service SyncShareSvc - Supervision journaux

Le service se nomme **SyncShareSvc**



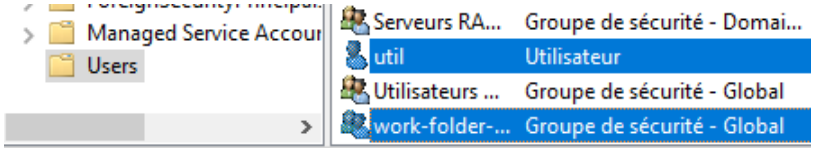
Dans **l'observateur d'évènement** on pourra lire le journal **SyncShare**



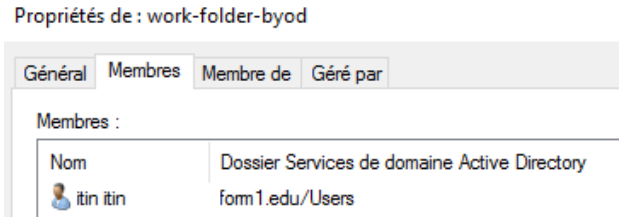
WORKS FOLDER – CLIENT

Utilisateur Itin membre du groupe Workfolder

L'idée c'est qu'un utilisateur itinérant, nommé ***itin*** mdp ***Domaine2016*** puisse utiliser les workfolder..Il faut donc vérifier que l'on ait bien un compte ***itin***



Membre du groupe de sécurité global ***Work-folder-byod***… :



Paramétrage client en http (sans https)

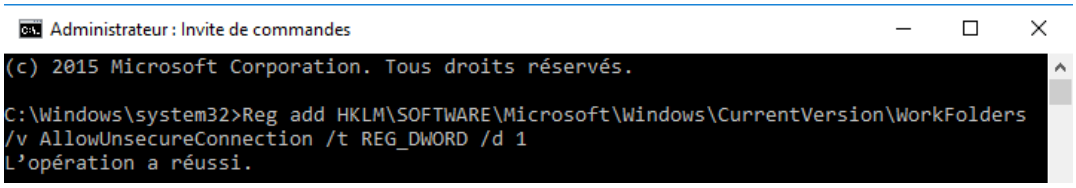
La configuration du client peut se faire soit :

- manuellement, via le **panneau de configuration**,
- soit par **GPO**.

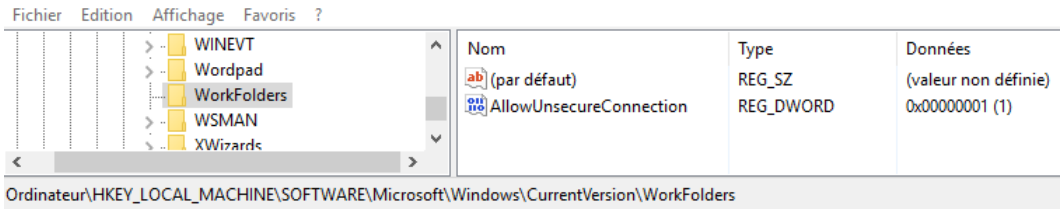
Par défaut la connexion va chercher à se connecter en **https (SSL)**. Avant de configurer des **certificats** on va autoriser la connexion en **http**. Pour cela il faut ajouter dans la base de registre du client : la clé **WorkFolders** valeur **REG_DWORD 1** dans **HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion**

Soit avec donc une commande (en administrateur) du genre

Reg add HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\WorkFolders /v AllowUnsecureConnection /t REG_DWORD /d 1

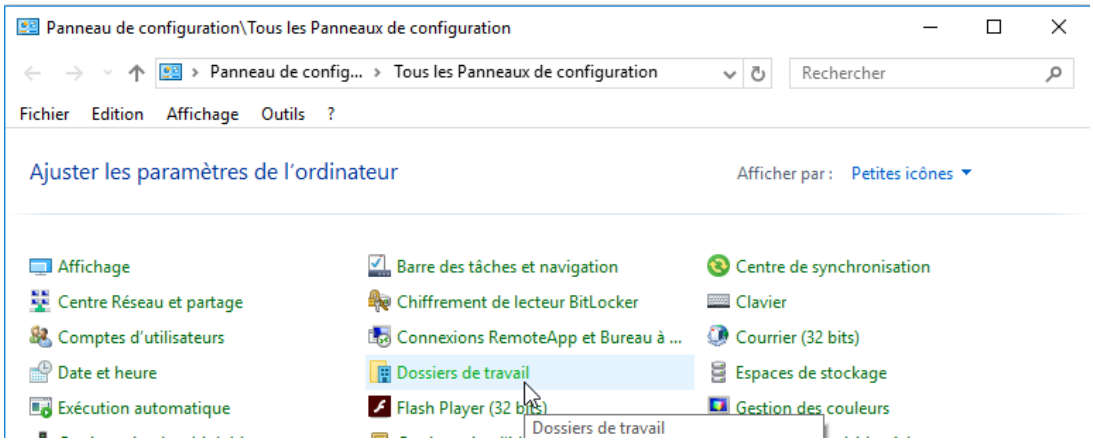


Que l'on peut vérifier via **regedit**

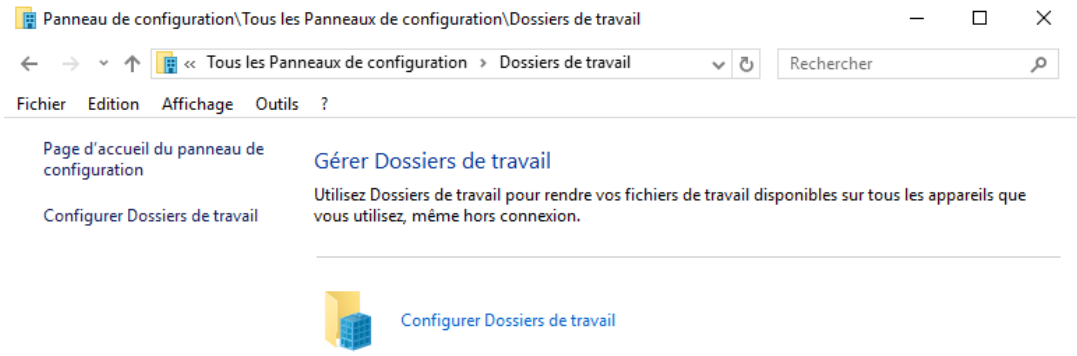


Client Via le panneau de configuration

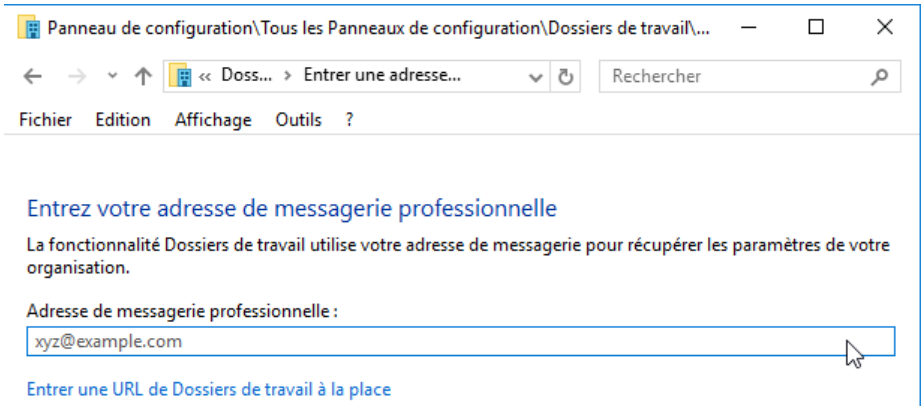
Dans le **panneau de configuration**, on deamnde **Dossiers de Travail**



On peut commencer via **Configurer Dossier de travail**



Dans la boite de dialogue suivante

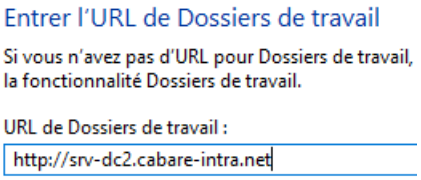


Cette adresse email est en fait juste utilisée pour trouver le serveur de synchronisation. Par exemple si l'on entre **user@bidon.local** c'est L'URL : **https://workfolders.bidon.local** qui sera utilisée

N.B: Si cette URL auto ne répond pas, l'assistant redemandera une URL

N.B: pour utiliser http à la place de https il faudra nous rentrer une URL

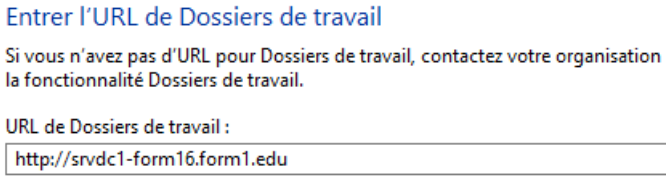
On peut dans l'exemple entrer: **http://srv-dc2.cabare-intra.net**



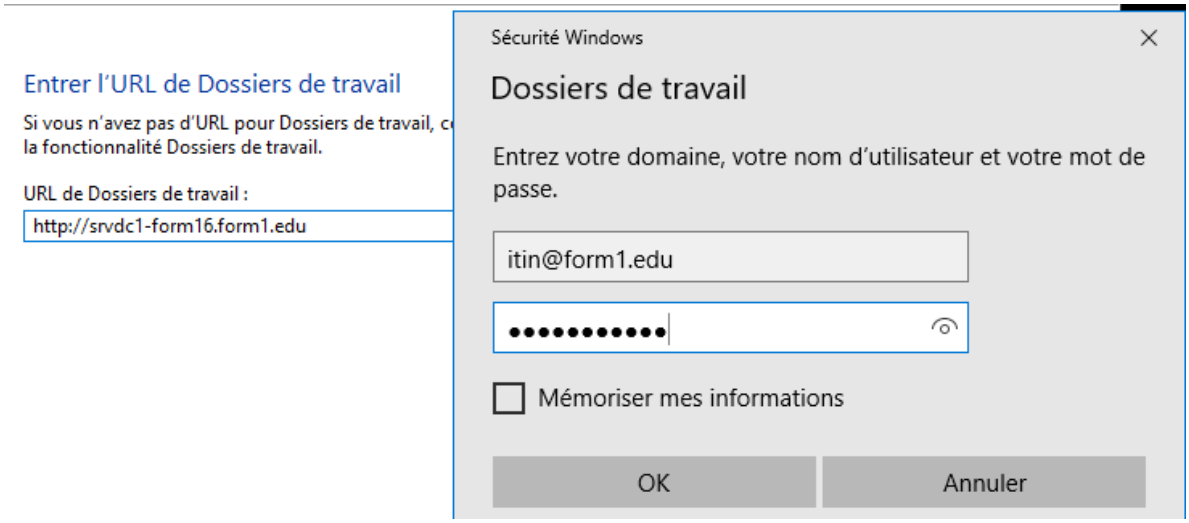
N.B: Si on a créé le CNAME pour workfolders dans le DNS, on peut utiliser ce nom et donc entrer comme URL: **http://workfolders.cabare-intra.net**.

Si on avait cela : ***srvdc1-form16.form1.edu***

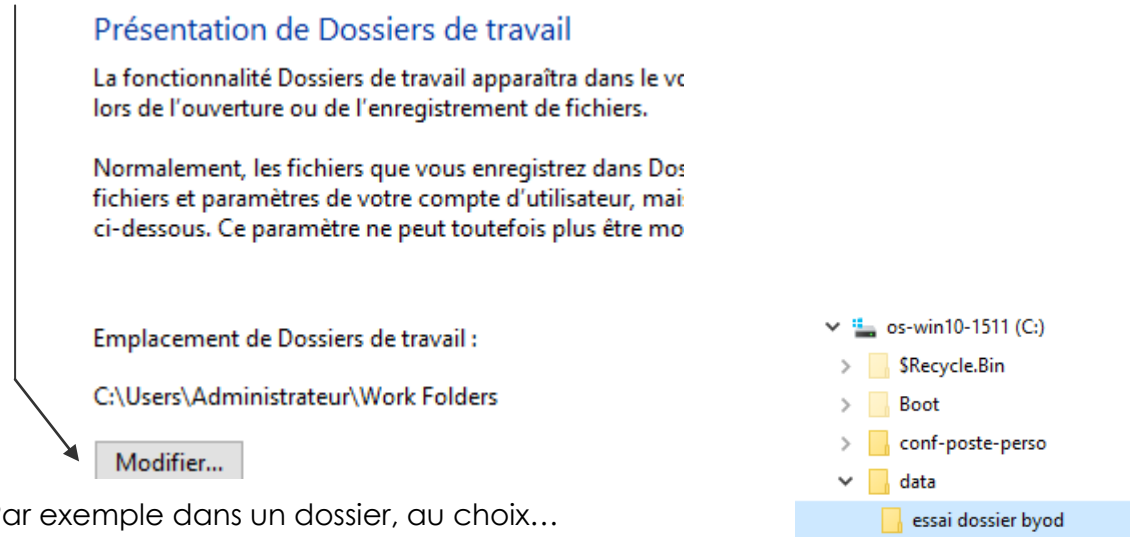
alors on peut rentrer ***http:srvdc1-form16.form1.edu***



Forcement il y a une demande d'authentification (il faut rentrer l'identifiant de notre utilisateur itinérant..)

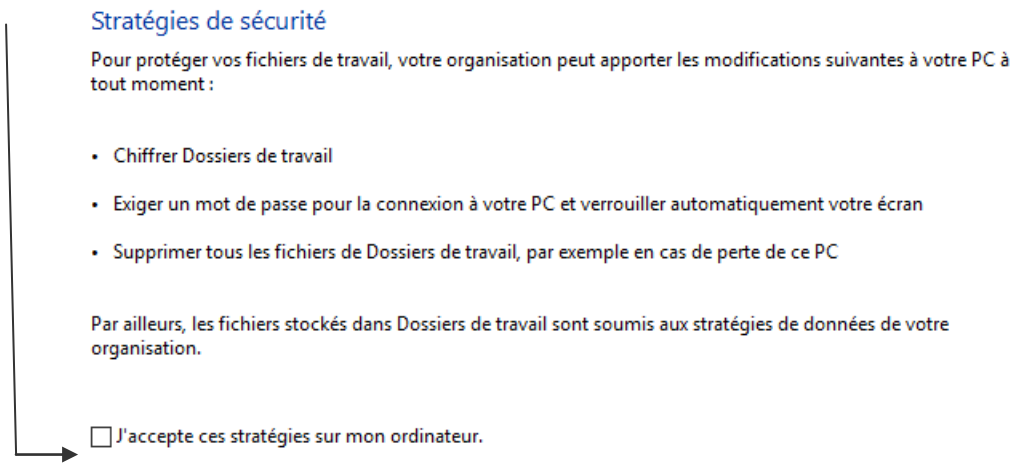


On choisit ensuite où l'on veut poser sur notre machine le dossier de travail… par défaut le dossier de travail est posé dans le profil utilisateur qui s'est authentifié, mais on peut le mettre ou l'on veut via **Modifier…**

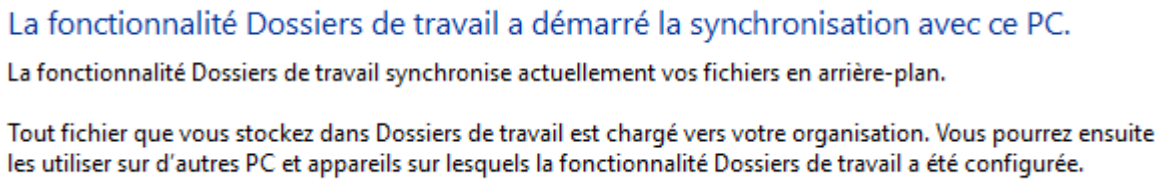


Par exemple dans un dossier, au choix…

Il faut accepter obligatoire les **GPO de sécurité**



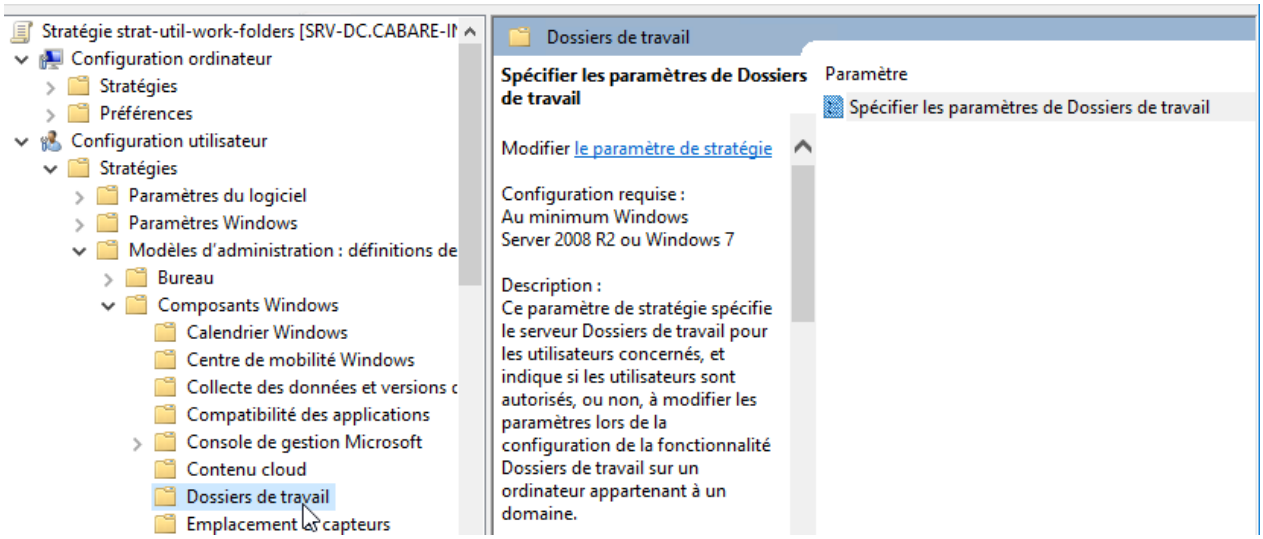
Et voilà !



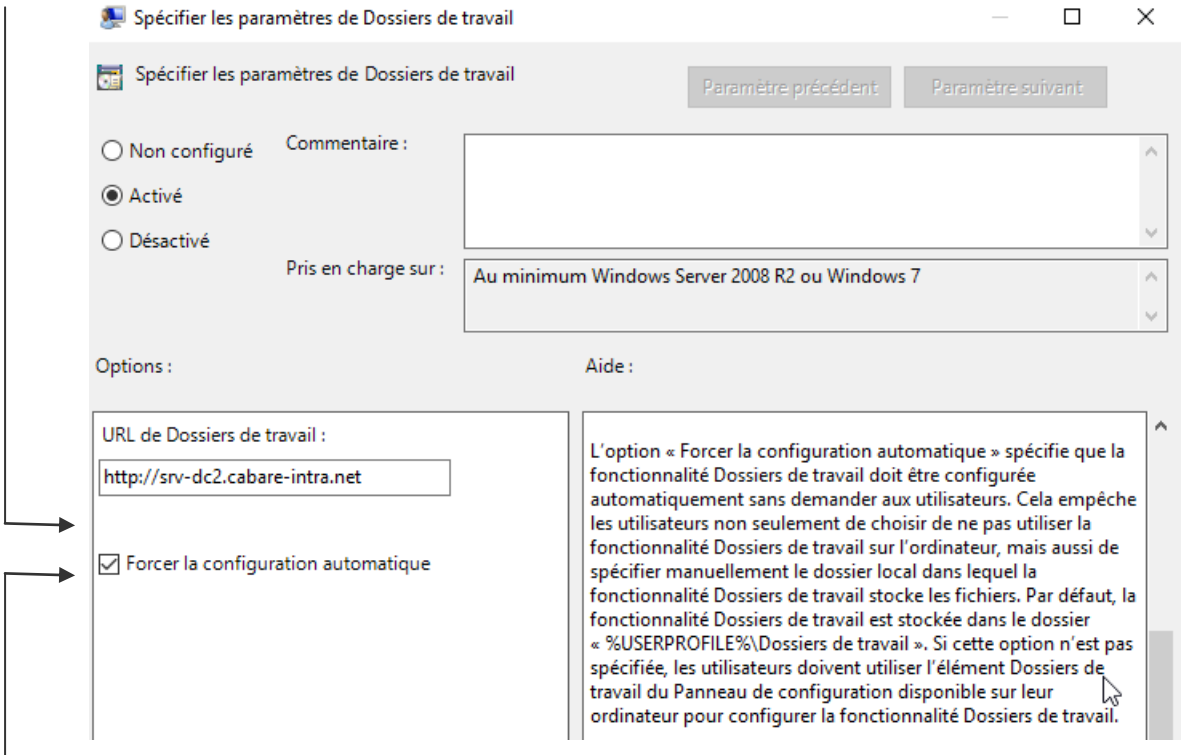
Client Via GPO

Il parait plus "sain de créer une **GPO** que l'on appliquera aux postes sur lesquels on veut mettre en place les **works folders**…

On se crée une nouvelle **GPO** utilisateur, par exemple ***strat-util-work-folders***



Dans laquelle assez simplement on indique l'Url du serveur stockant les Dossiers de travail, dans l'exemple **http://srv-dc2.cabare-intra.net**



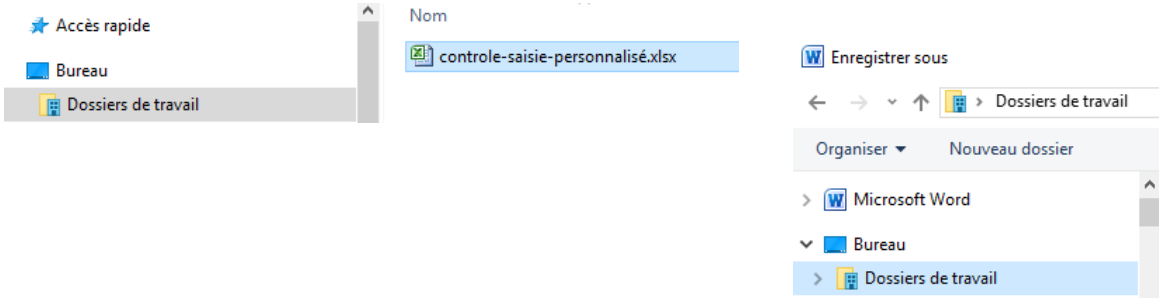
Il est de bon ton de ne pas laisser le choix à l'utilisateur

Du coup, le dossier de travail apparaît directement dans le **Profil utilisateur**

Test - utilisation

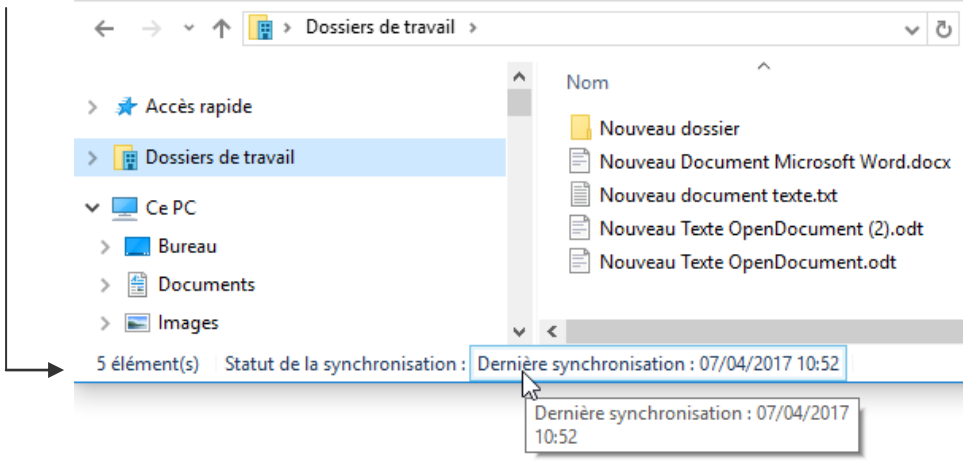
Depuis un client paramétré, l'utilisateur ***itin@cabare-intra.net*** travaille simplement avec ce nouveau dossier **Dossiers de travail** qui apparaît dans l'interface du gestionnaire de fichier, Ou applicative

Soit là où l'on l'a paramétré (dans le cas d'une installation du client manuelle), soit directement sous le Bureau (si utilisation d'une **GPO** : mieux !)

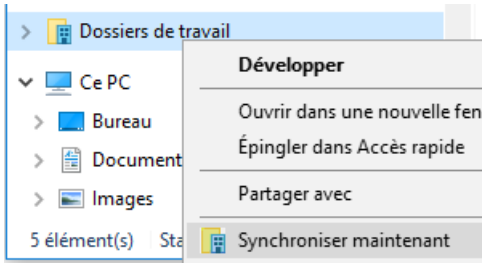


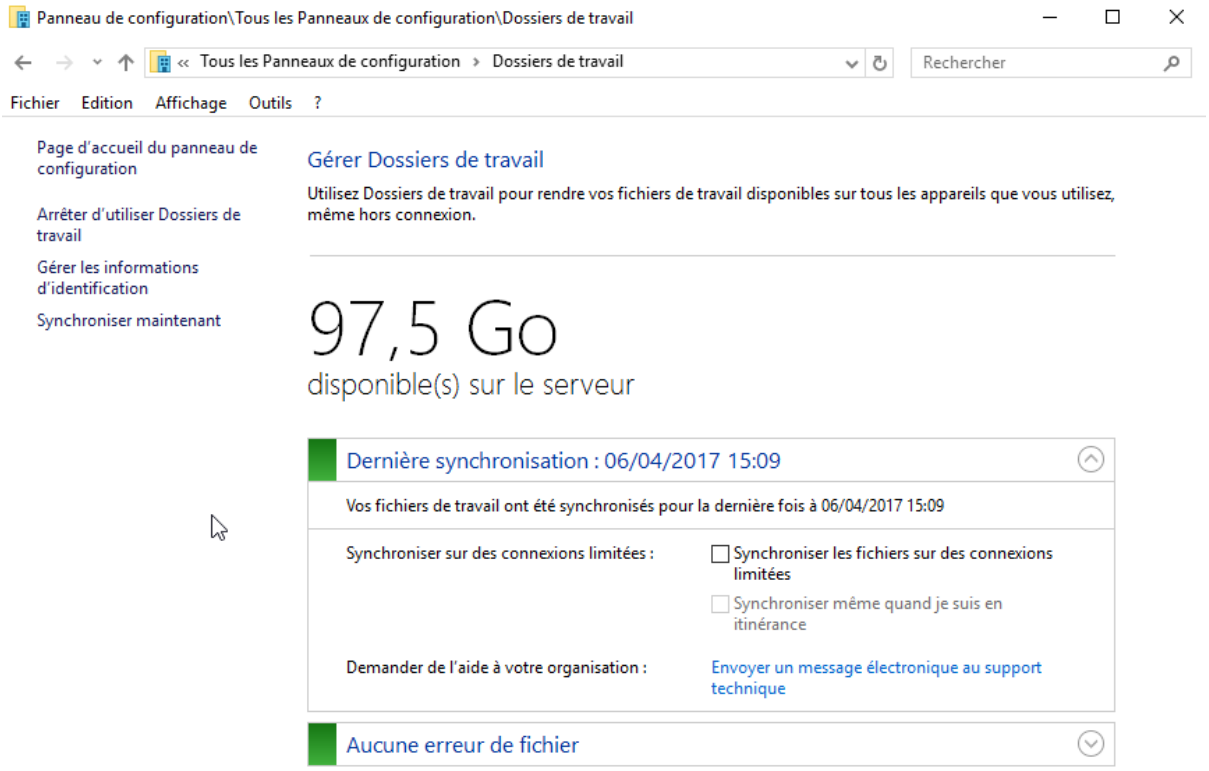
Tout ce qui s'y trouve est transmis sur le serveur

Vérification Possible depuis le **panneau de configuration / dossier de travail** du client ou en cliquant sur le bas de la barre des tâches, lorsque l'on est dans le dossier de travail

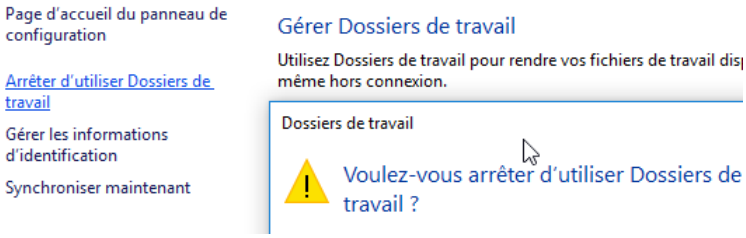


L'utilisateur peut aussi demander rapidement (clic droit) **Synchroniser maintenant**





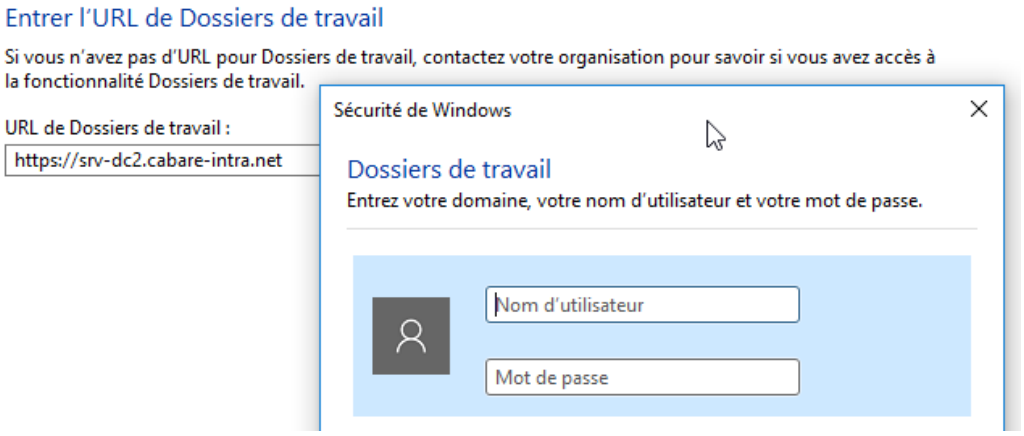
Notamment avec une possibilité d'arrêt (si pas de GPO)



lorsque l'on coupe la stratégie créant un work folder pour un utilsateur, celui-ci va se retrouver avec un dossier de travail "normal"

Souplesse d'utilisation "à la volée"

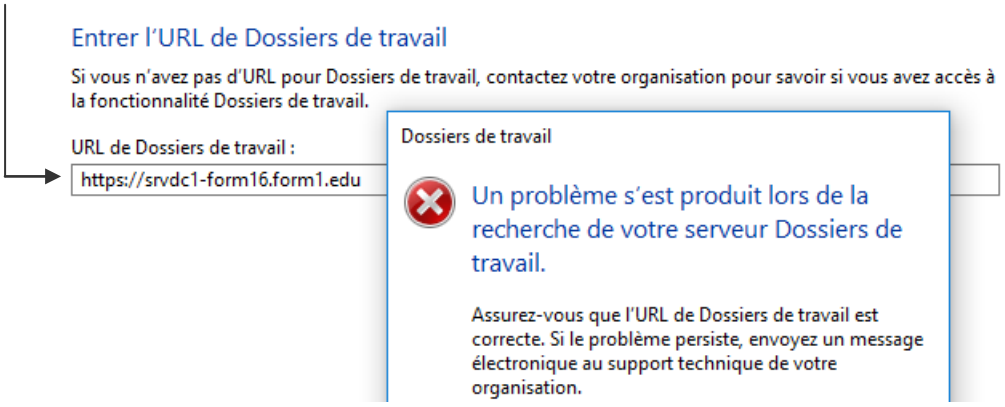
A tout moment, sur une **machine en domaine**, (ou en **workgroup** si on a importé le **certificat de racine de confiance du domaine**) on peut dans le **panneau de configuration** demander de mettre en place les **dossiers de travail**, et éventuellement les démonter après usage…



SSL et certificats

Pour utiliser **SSL**, il faut un **certificat SSL** pour notre serveur gérant les dossiers de travail **srv-dc2.cabare-intra.net** ou **workfolders.cabare-intra.net.**

En effet le protocole **https** a besoin d'un certificat authentifiant le serveur d'où proviennent les communications en **https-443**. Si on tente une connexion **https** sans certificat on a une erreur bloquante :

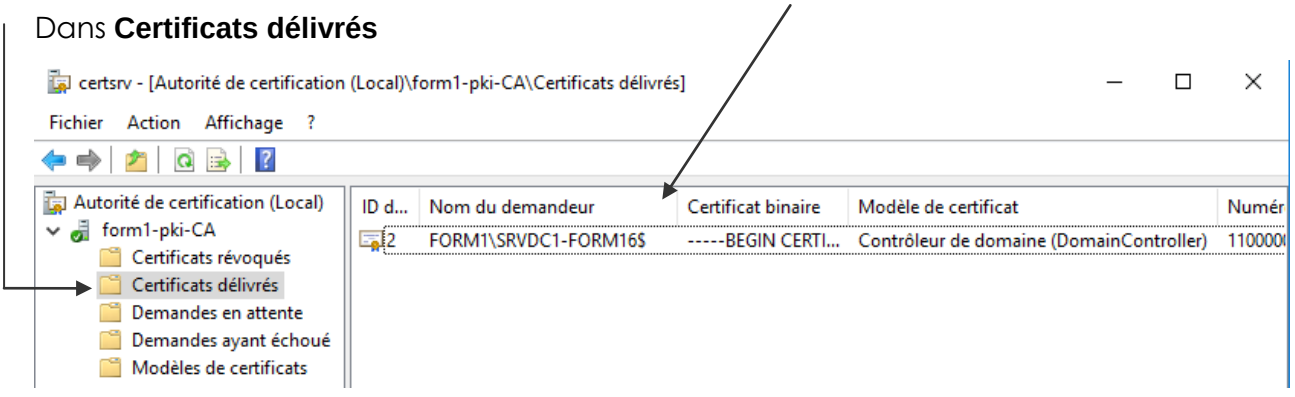


- Certificat de Domaine + machine de Domaine, tout est Ok.
- Certificat de Domaine + machine hors Domaine alors il faudra **importer le certificat de l'autorité de certification** dans le magasin des **autorités racines de confiance** des machines hors domaine. en effet, celles-ci ne font pas confiance par défaut à la CA du domaine. (évidemment les membres du domaine eux font confiance automatiquement).
- **N.B**: Ce point peut justifier l'achat d'un **certificat SSL** auprès d'une **autorité de certification publique** déjà reconnue par tous les types de clients.

Quel certificat pour quel serveur

Actuellement, aucun certificat spécifique n'a été demandé, par conséquent dans la liste des certificats attribués, le seul certificat qui peut apparaitre sera celui octroyé par défaut au **Contrôleur de Domaine**

Dans **Certificats délivrés**



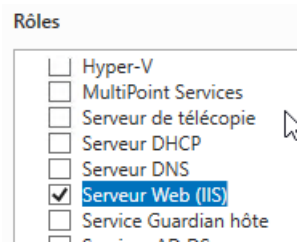
Installation console de gestion IIS

Il va falloir que l'on soit capable de faire une demande de **certificat** pour notre serveur hébergeant les **Works Folders**

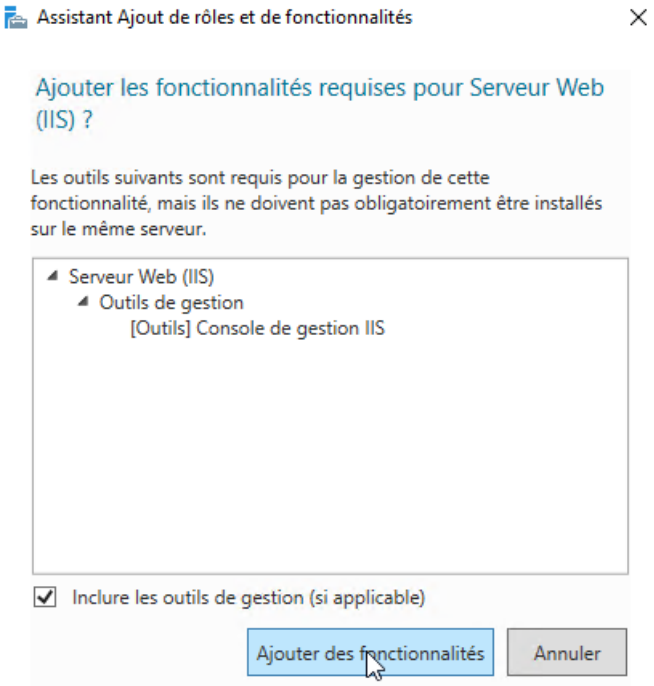
Cela pourra se faire de manière interactive via la **console de gestion IIS**, qu'il va falloir installer

N.B : ne jamais installer en production un **IIS** sur un **contrôleur de domaine**

Cela suppose d'ajouter le rôle se serveur Web IIS



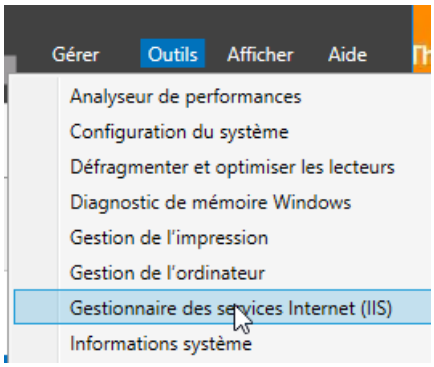
et ses outils de gestion



N.B: On pourra constater que le site web par défaut est arrêté. C'est normal, car le service de synchronisation de fichiers n'utilise pas un site IIS mais le service **IIS Hostable Web Core (HWC).**

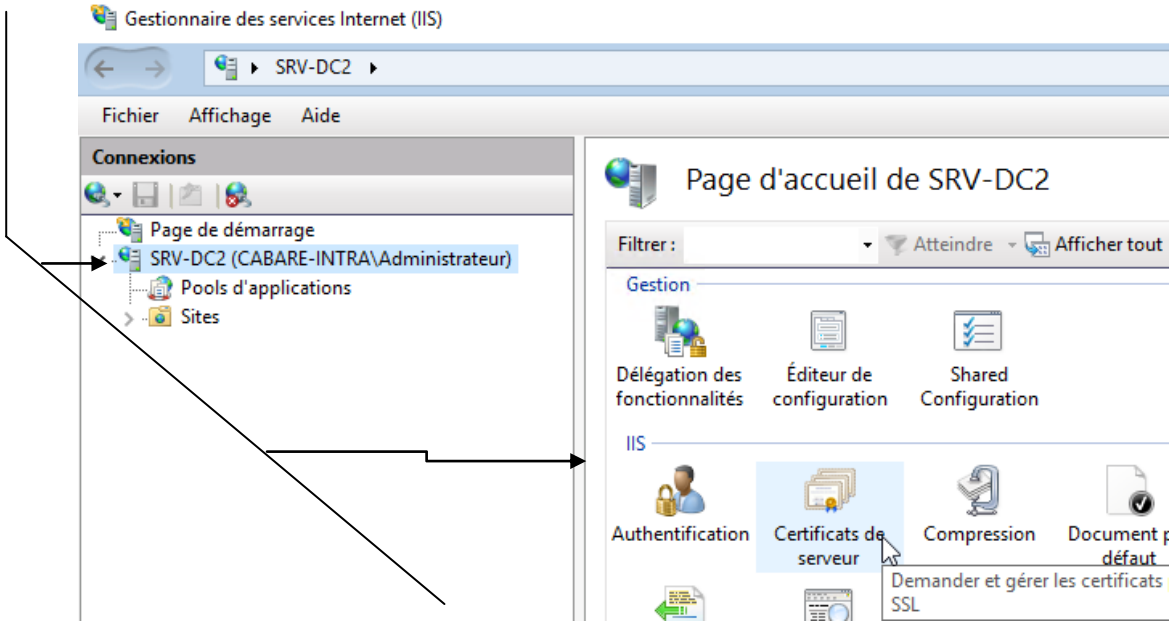
Création du certificat de domaine du serveur

Via la console **Gestionnaire de service Internet (IIS)**



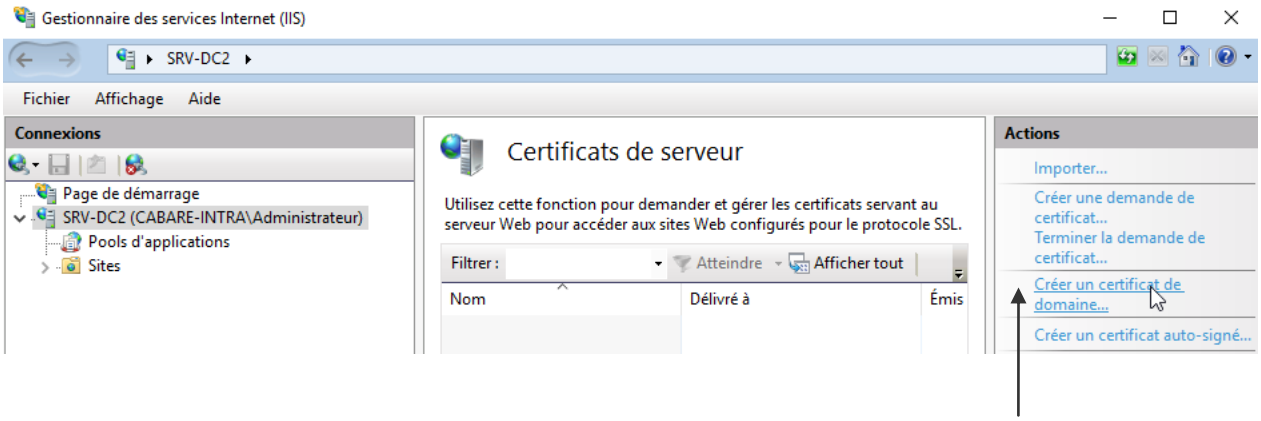
Dans la console, on se place sur notre serveur …

(ici SRV-DC2) , puis dans la section **IIS** on clic sur **Certificats de serveur**



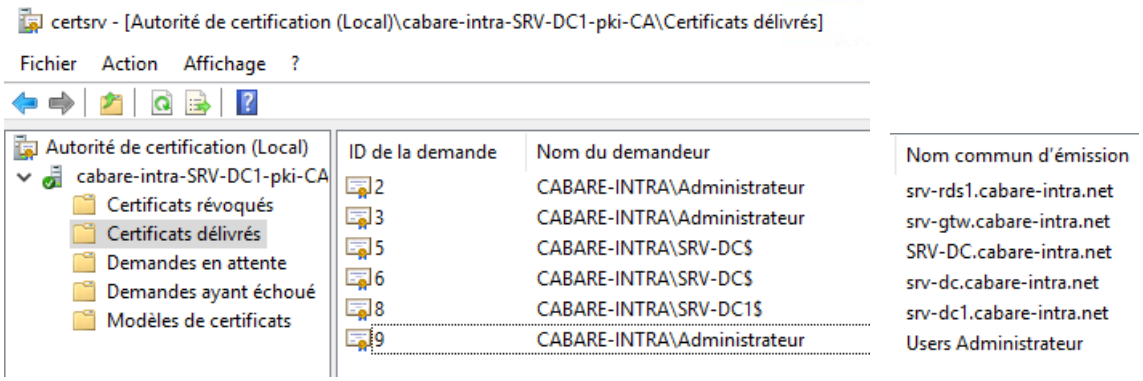
un **certificat auto-signé** du serveur peut apparaître, mais souvent aucun certificat n'existe sur une machine fraichement installée

N.B : il peut y avoir d'autres certificats de type autre que serveur Web

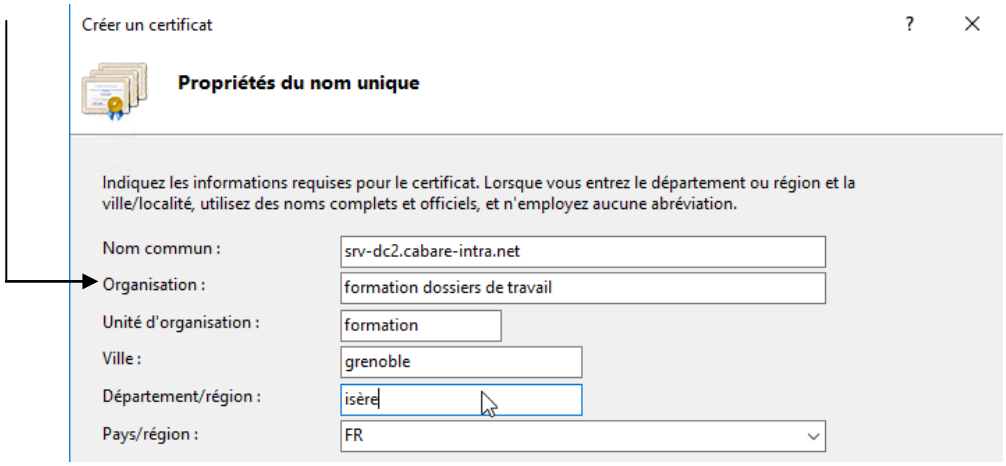


Pour avoir un **certificat de domaine** (la **racine PKI** étant déjà créé), il faut demander **Créer un certificat de domaine… (**et surtout pas **auto-signé)**

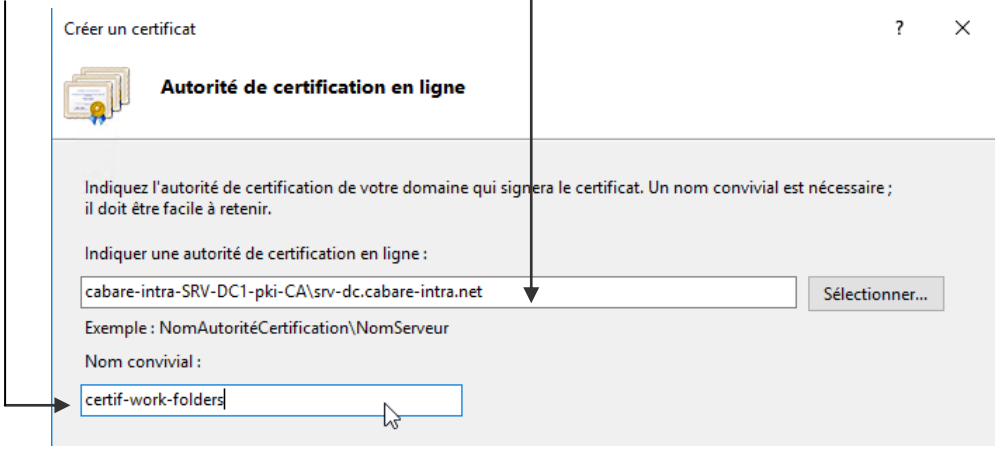
N.B: on peut voir coté **autorité de certification** (là où notre **pki** est installée)que pour l'instant notre serveur ***srv-dc2*** n'a pas de certificat



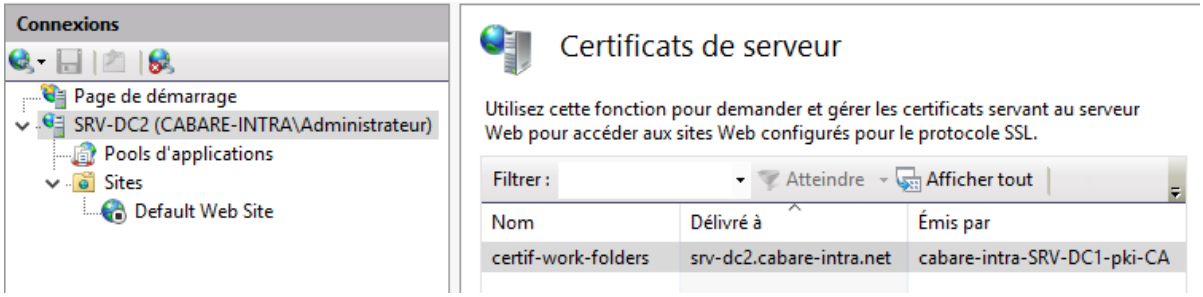
Cela déclenche un assistant, dont seule la première ligne **Nom commun** avec le **FQDN du serveur à certifier** est importante



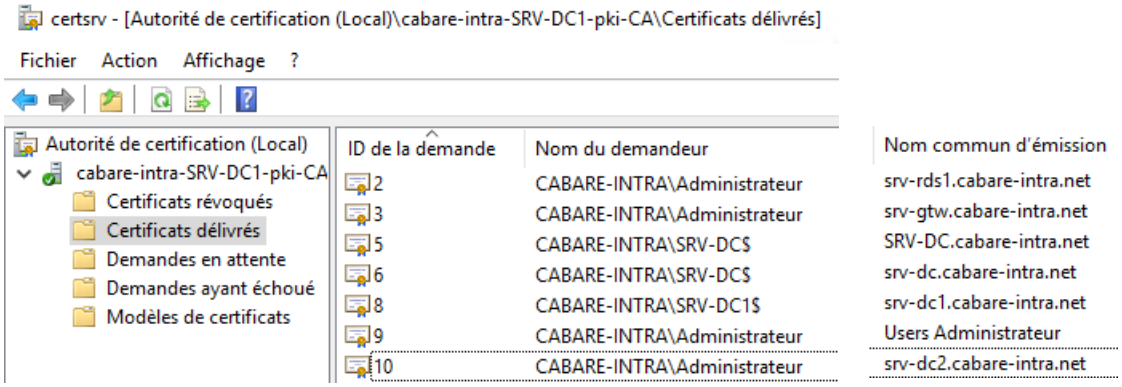
On va chercher notre **autorité racine PKI** de domaine et on peut donner un nom logique à ce certificat…



Et on obtient

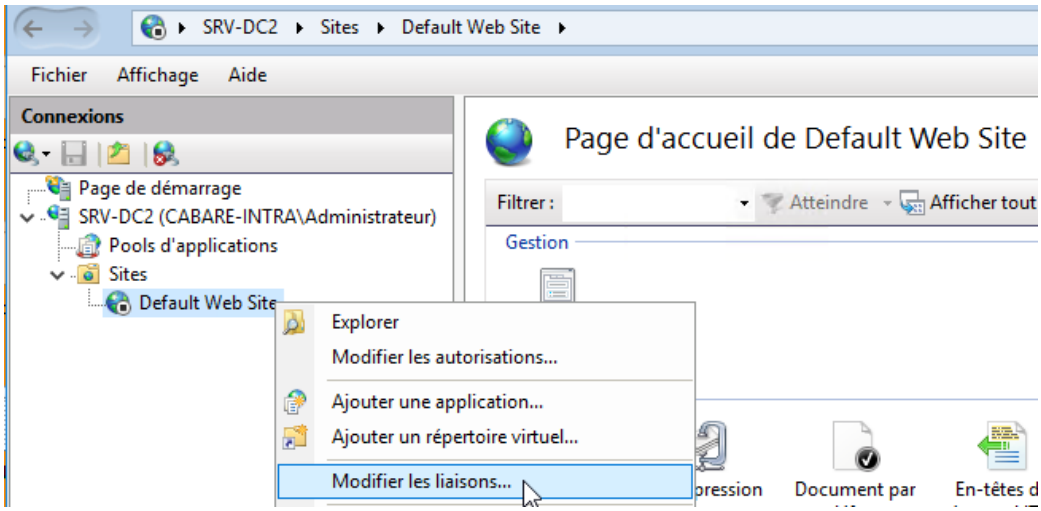


N.B: on peut voir coté **autorité de certification** (là où notre **pki** est installée) que maintenant notre serveur ***srv-dc2*** possède bien un certificat

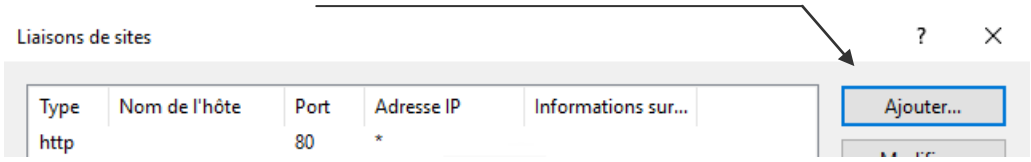


Ajout du protocole https avec le certificat

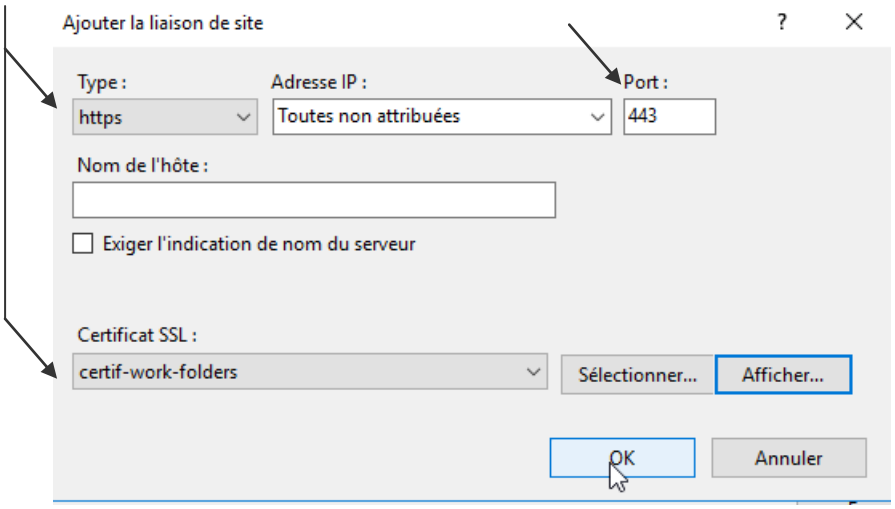
Toujours via la console **Gestionnaire de service Internet (IIS)** on demande dans les **Sites**, sur le Site Web par défaut **Default Web Site** et clic droit **Modifier les liaisons...**



On demande **Ajouter…**

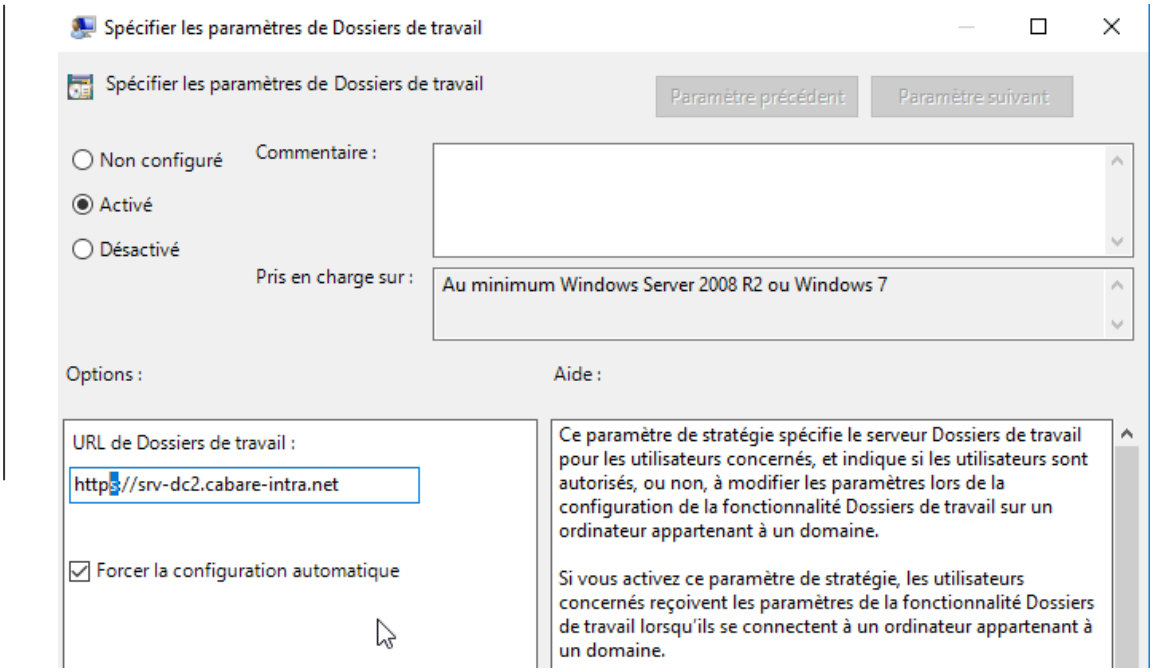


https, port **443** avec notre **certificat** nouvellement crée !

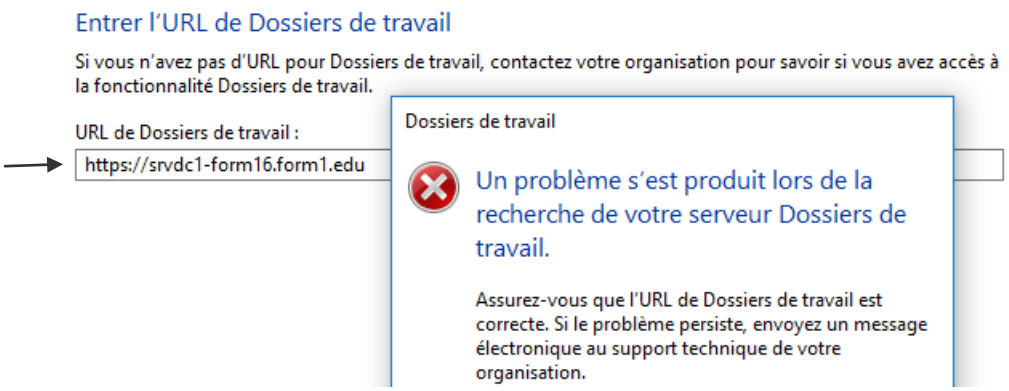


GPO avec nouvelle adresse en https

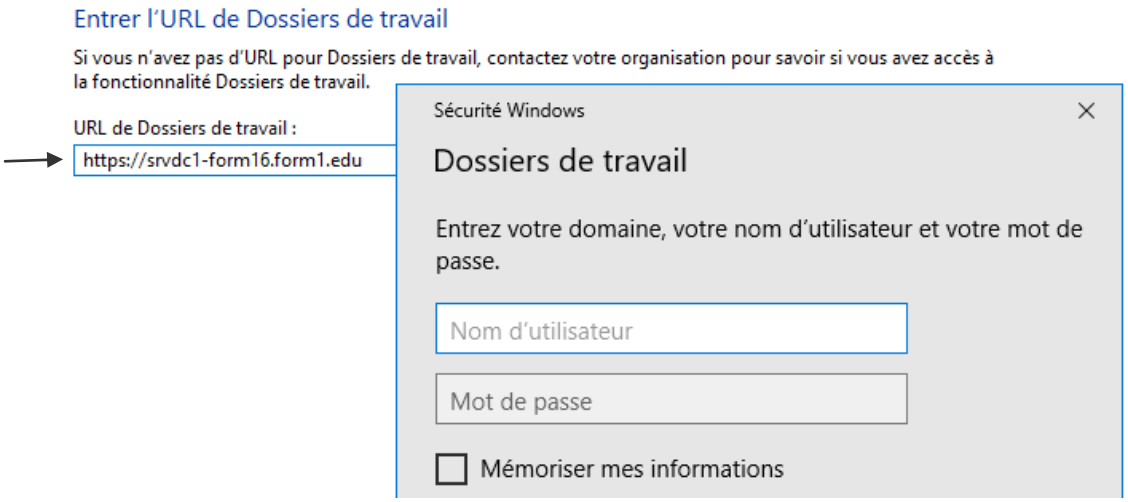
Modification de la **GPO** avec une adresse en **https** comme par exemple **https://srv-sdc2.cabare-intra.net**



Et donc désormais, là ou on avait



On devrait maintenant « passer » et avoir le demande d'authentification



MACHINE HORS DOMAINE

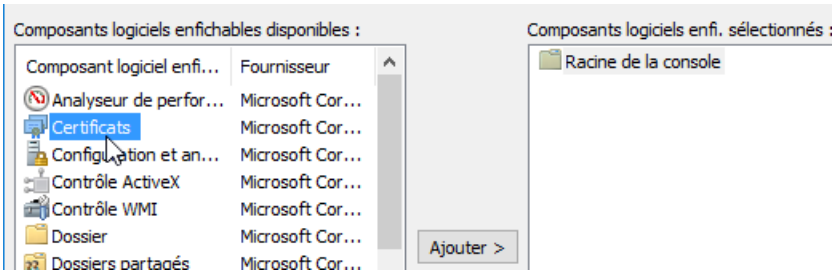
PB validité de certificat "hors domaine"

Il parait évidemment impossible de pouvoir utiliser une **GPO utilisateur** de **domaine.** De plus comment faire pour que, que lorsque l'on voudra saisir l'URL de destination, de la forme ***https://srv-dc2.cabare-intra.net*** on puisse valider le **SSL**… avec un « certificat de domaine »…

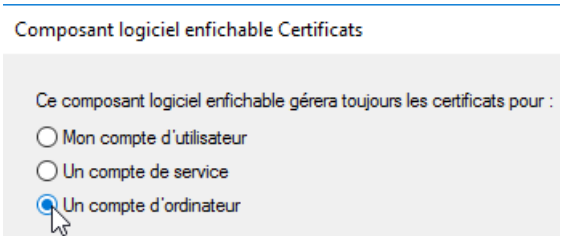
Situation dans un domaine

Une machine de domaine possède comme **Autorité de certification de racine de confiance**, La **PKI** de son domaine

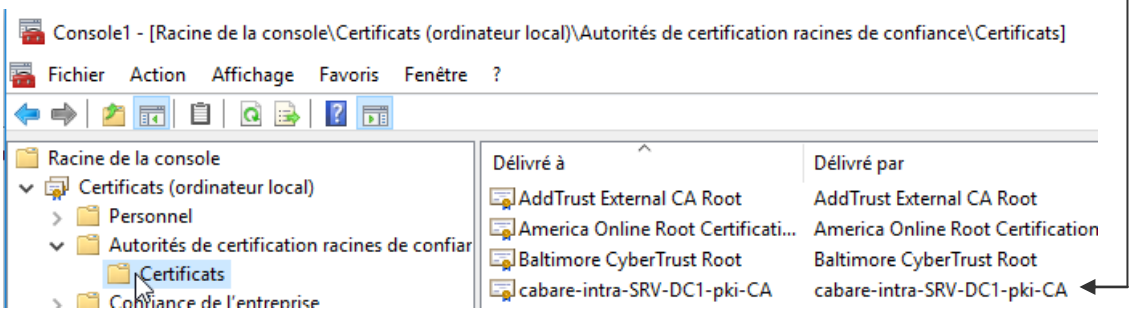
On peut le voir dans le **gestionnaire de certificats**, (utilisateur) ou mieux via une **console mmc** dans laquelle on ajouterais le **composant logiciel enfichable certificat – ordinateur**



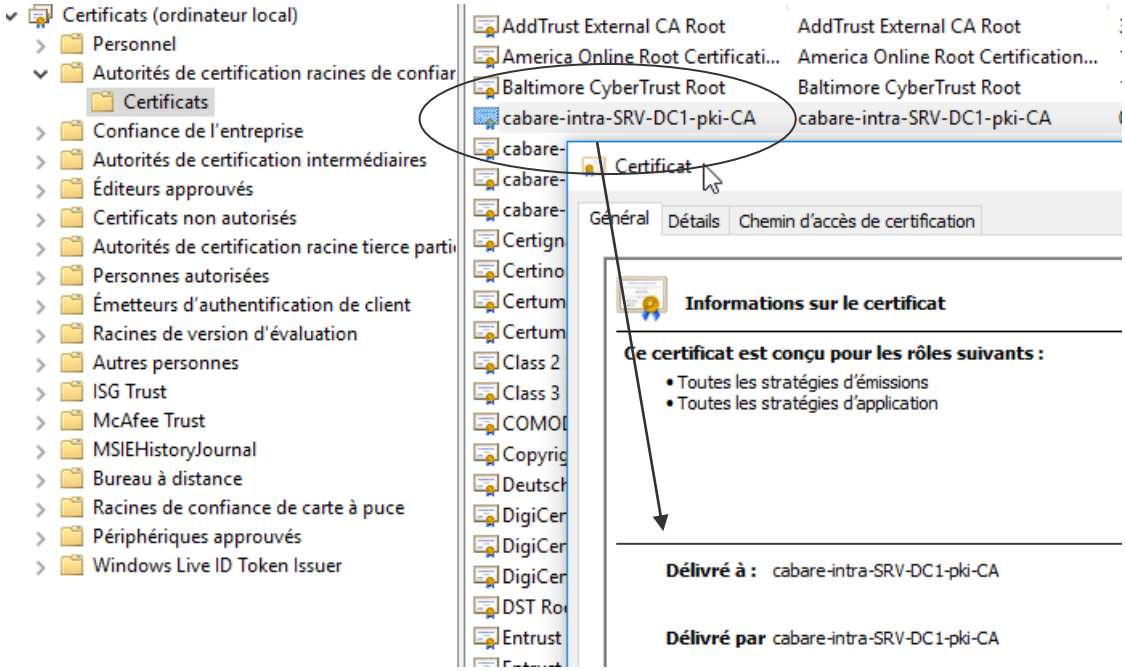
Avec par exemple



Pour avoir du coup tous les certificats de domaine

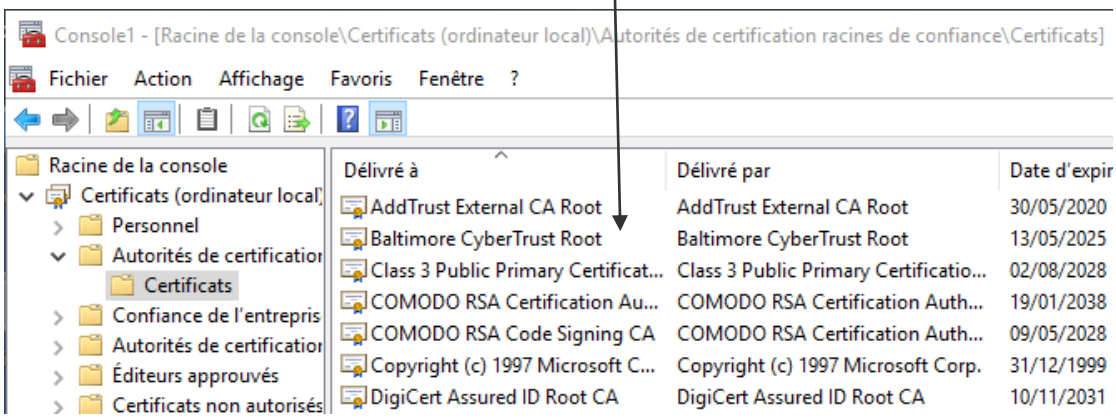


Du coup les certificats "de domaine" sont valables, car ils font référence à une **PKI** connue et accessible

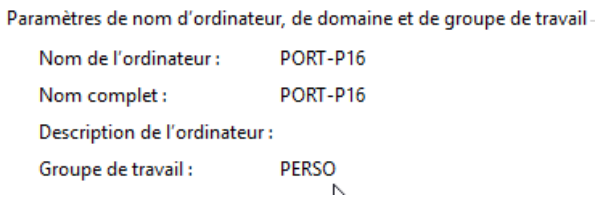


Situation en Workgroup

Par défaut, une machine en **workgroup**, ne connait évidemment pas la **PKI** de domaine…

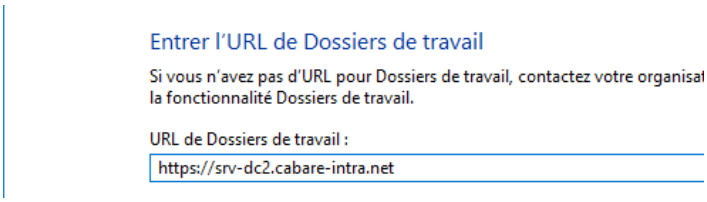


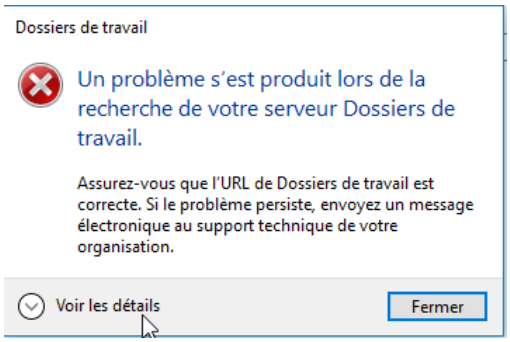
sur une machine en workgroup par exemple ici ***PERSO***



si on veut configurer les **dossier de travail**, on passe manuellement par le **panneau de configuration / Configurer dossier de travail**

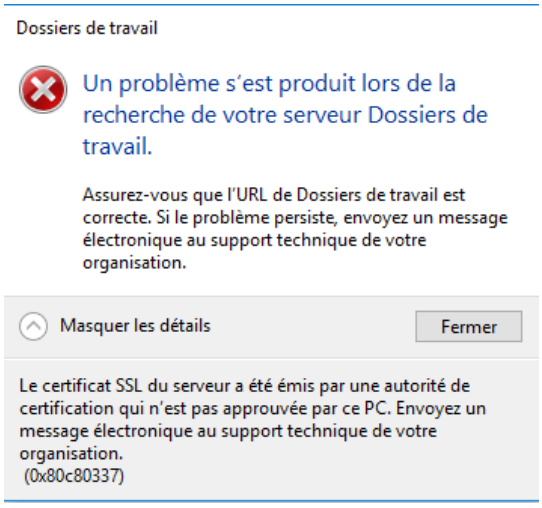
sauf que au moment ou on tape l'URL du serveur





on a un message d'erreur normal !

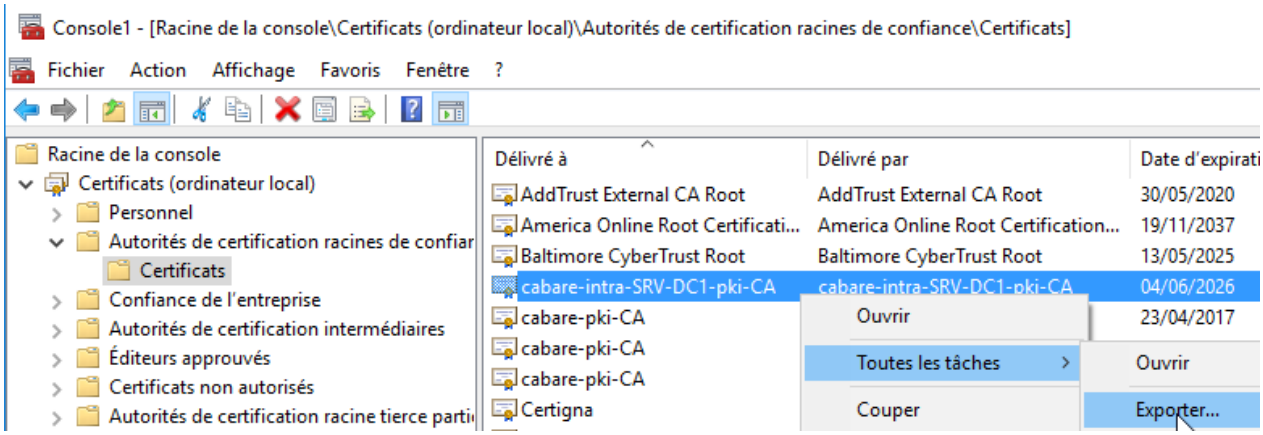
et si on demande le détail il nous donne même la bonne réponse **Problème SSL ! l'autorité de certification n'est pas approuvée par ce PC**:



Export de certificat:

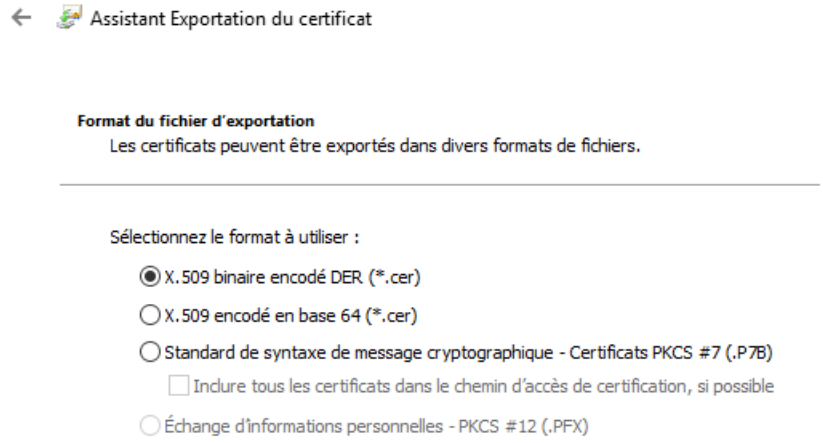
Depuis une machine du domaine, on va d'**exporter le certificat de l'autorité de certification** qui se trouve dans le magasin des **autorités racines de confiance**

pour exporter le certificat obtenu du domaine, on se place dessus, puis on demande **Toutes les taches/ Exporter…**

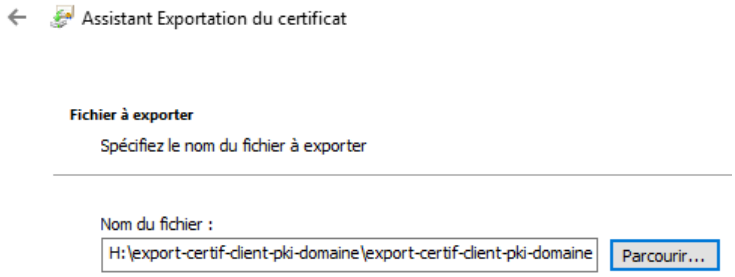


Un assistant se declanche

On garde le format par défaut

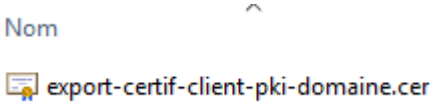


Et on le stocke ou l'on veut



Il n'y a plus qu'à confirmer

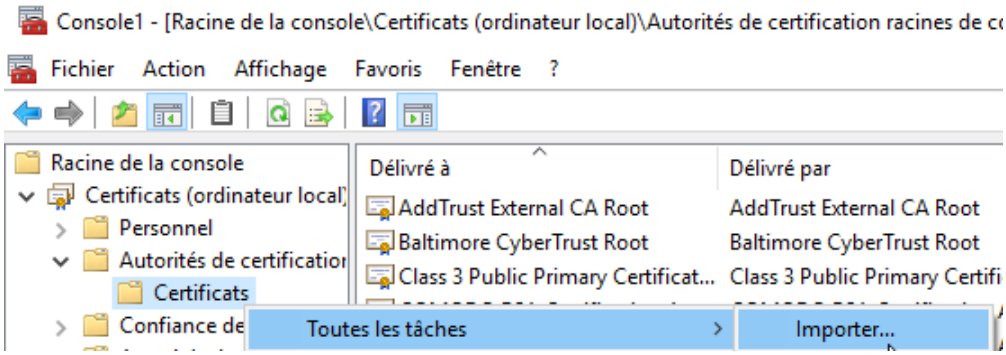
Pour obtenir le fichier contenant la **cle publique du certificat**



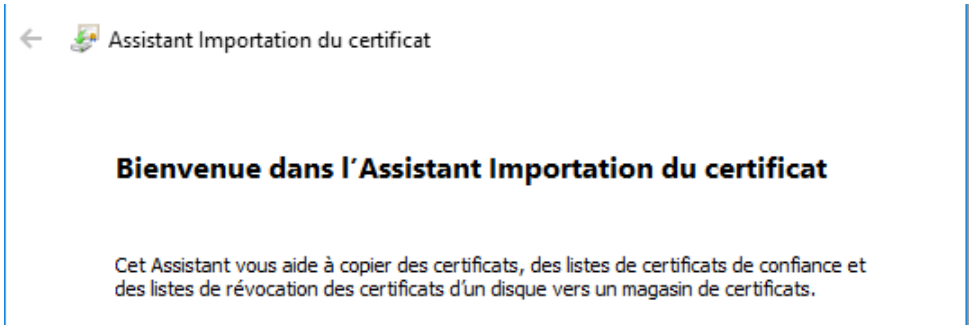
Import de certificat sur une machine en workgroup:

Sur notre machine en workgroup, on va donc décider d'**importer le certificat de l'autorité de certification** dans le magasin des **autorités racines de confiance**

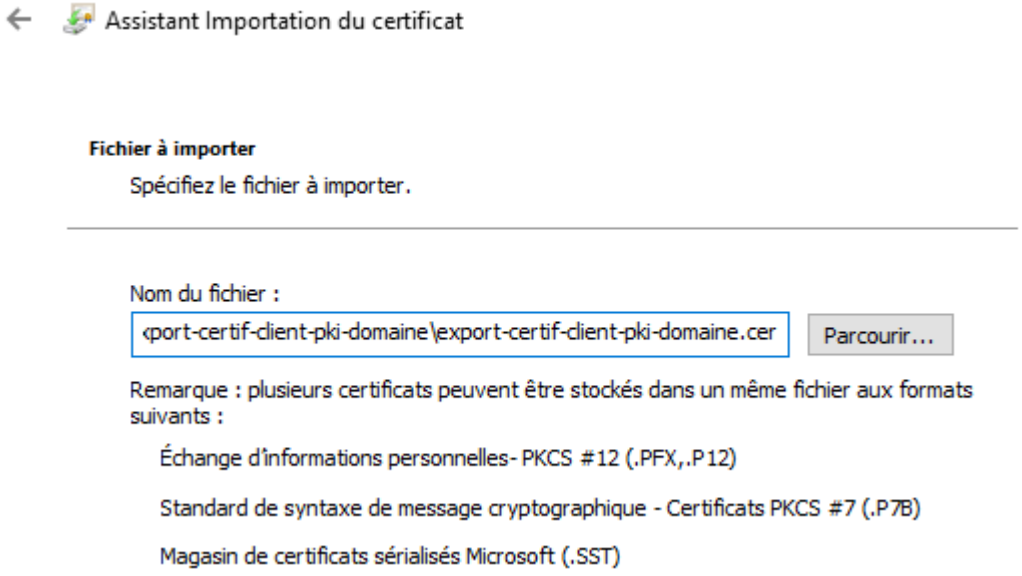
On se place sur **Certificats**, **Autorités de Certification/ Certificats** et on demande **Toutes les tâches / importer**



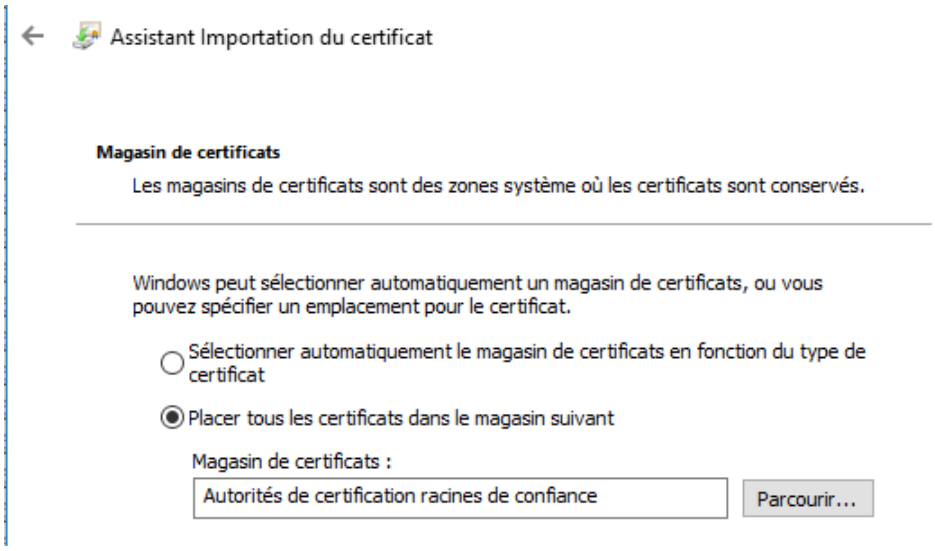
Un assistant se déclenche…



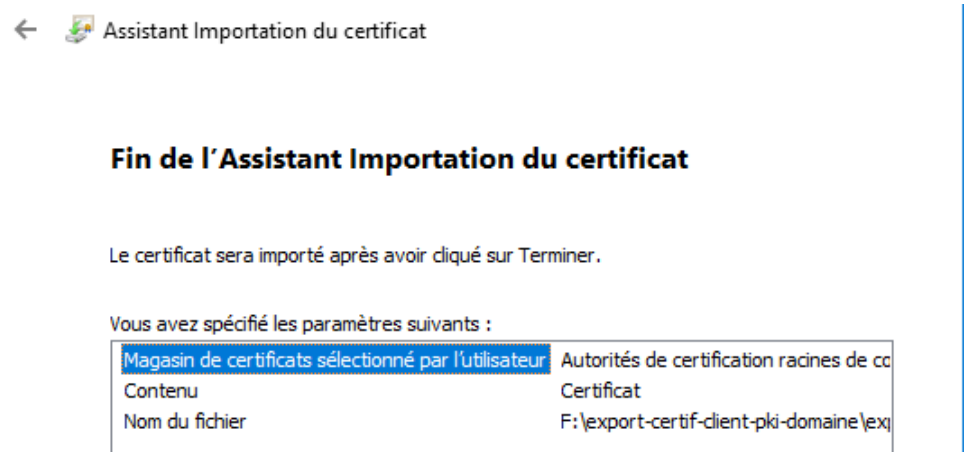
On va chercher le certificat préalablement exporté



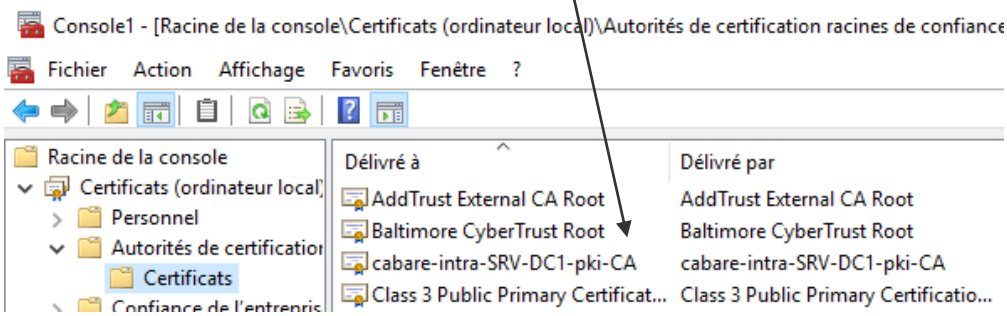
On demande de la restaurer



On confirme



Et on obtient



CERTIFICAT ET PKI

Types de Certificats et PKI

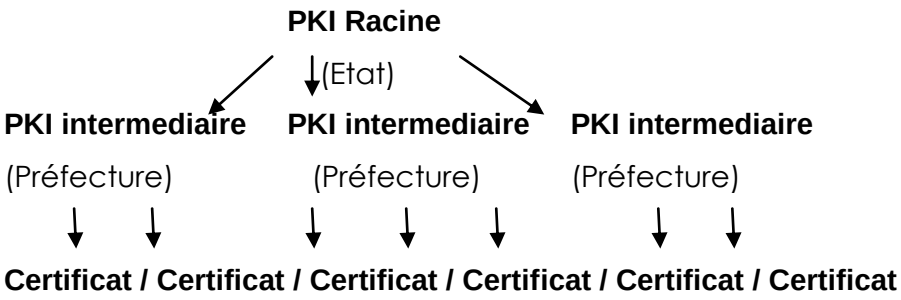
Le Certificat sert à être sûr que la machine que l'on utilise soit la bonne. Il existe 3 types de certificats SSL selon leur origine d'émission :

- **Autosigné - (interne)**: la machine génère son propre certificat, qui n'est valable que sur... cette machine !
  (à éviter !)
- **PKI-de-domaine (interne)**: le certificat est valable sur tout le domaine (il suffit d'être sur une machine membre du domaine pour en bénéficier)
  (pour les tests, formations, c'est ok)
- **PKI-internet (publique)**: le certificat est valable dans le monde entier. On peut en trouver des gratuits mais en général le service est payant(*)
  (obligatoire en production)
  (*) **STARTSSL** propose des certificats gratuits fonctionnant sur 90 % des browser, **RAPIDSSL** propose des certificats connus par quasiment 100% des navigateurs pour environ 40€/an... ensuite il y a **Verisign.**. etc...

Les **PKI** = **PUBLIC KEY INFRASTRUCTURE** contiennent les clés publiques et privées permettant la reconnaissance et le cryptage= ETAT

Les **PKI** sont elles-mêmes émises, renouvelées et éventuellement révoquées, elles sont construites selon une structure pyramidale. Une **PKI** est une identité qui effectue 3 opérations, elle émet, révoque et renouvelle des **certificats**.

Le **Certificat** = Pièce d'identité. On peut comparer les certificats à des pièces d'identités, permettant de reconnaître des machines dans un domaine. La signature de la carte d'identité prouve que le document de l'état est officiel, la signature du certificat par la PKI fait de même



(Carte nationale identité / Carte nationale identité / Carte nationale identité)

1 pièce d'identité à 3 éléments : Nom – prénom
Durée de Validité
Signature de l'Autorité = Etat / Préfecture

1 certificat à 3 éléments : Nom de poste/serveur en FQDN
Durée Validité Horodatage
Origine de l'autorité de Certification = PKI

Création PKI de domaine:

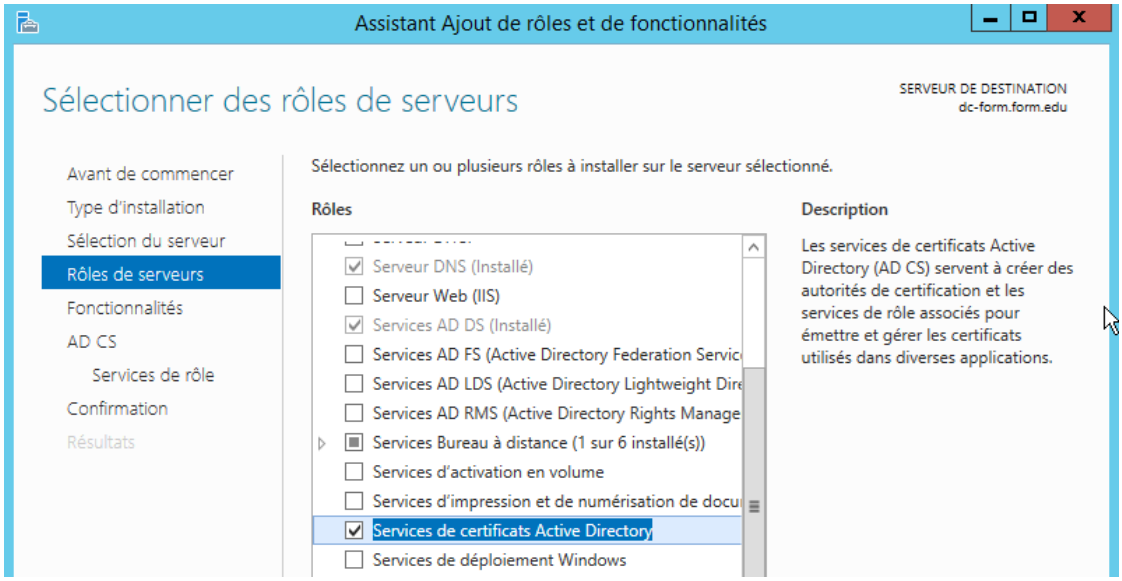
Si cela n'est pas fait, on crée une **PKI de Domaine**, qui a vocation à être connue dans toute l'**AD**.

La **PKI** se pose sur un serveur unique (pas de redondance possible) que l'on doit par conséquent sauvegarder. Il faut absolument ne pas la perdre !

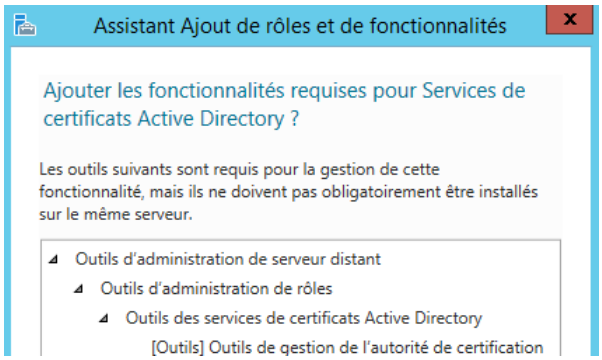
On peut la stocker sur le **DC** qui intègre les **5 rôles**, et un **CG**. Lorsque l'on sauvera le **System State**, ou l'**AD**, elle fera partie de la sauvegarde…

Ajout rôle Service de certificats AD

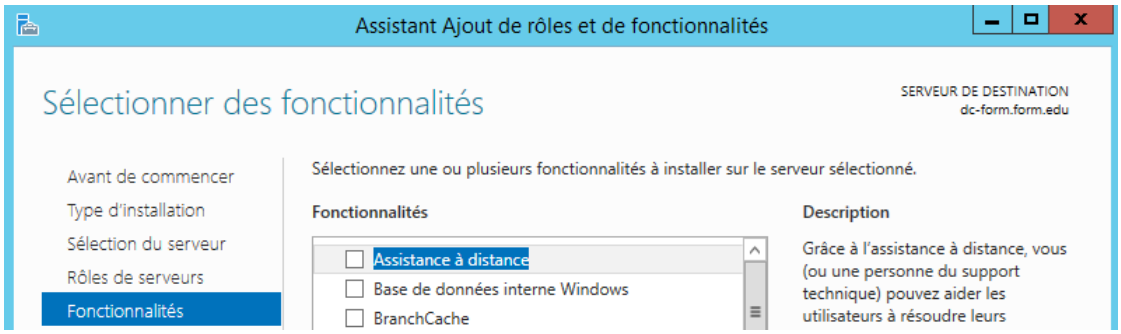
Le rôle peut se poser sur un **DC** ou un serveur spécifique (…). C'est le rôle nommé **Services de certificats Active Directory**



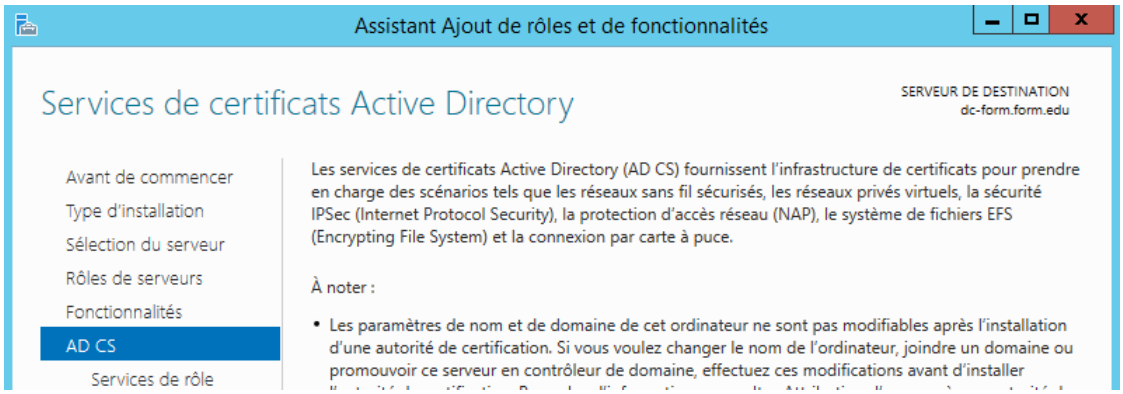
Et toutes les fonctions associées



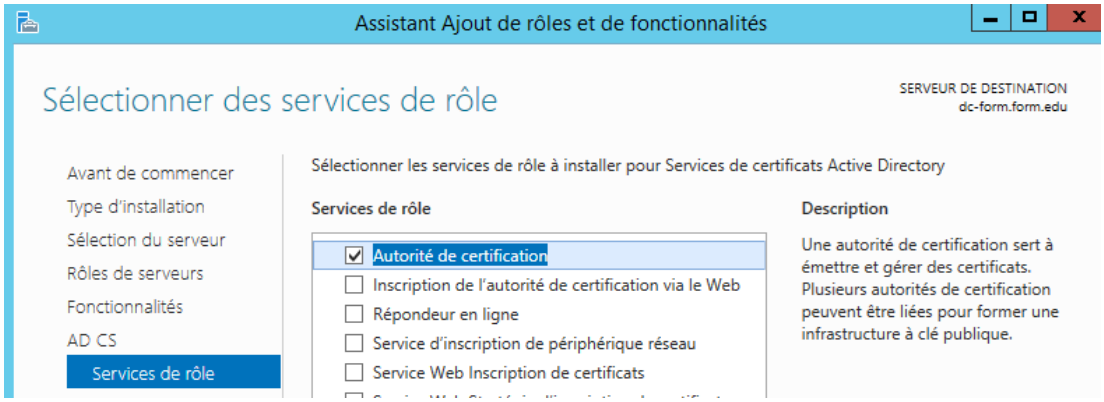
On ne modifie rien d'autres



On est informé que les noms poste et de domaine devront être immuables…



Dans les **Services de Rôle** on demande uniquement **Autorité de certification**

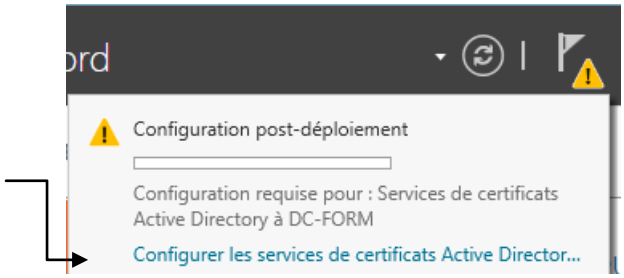


On confirme

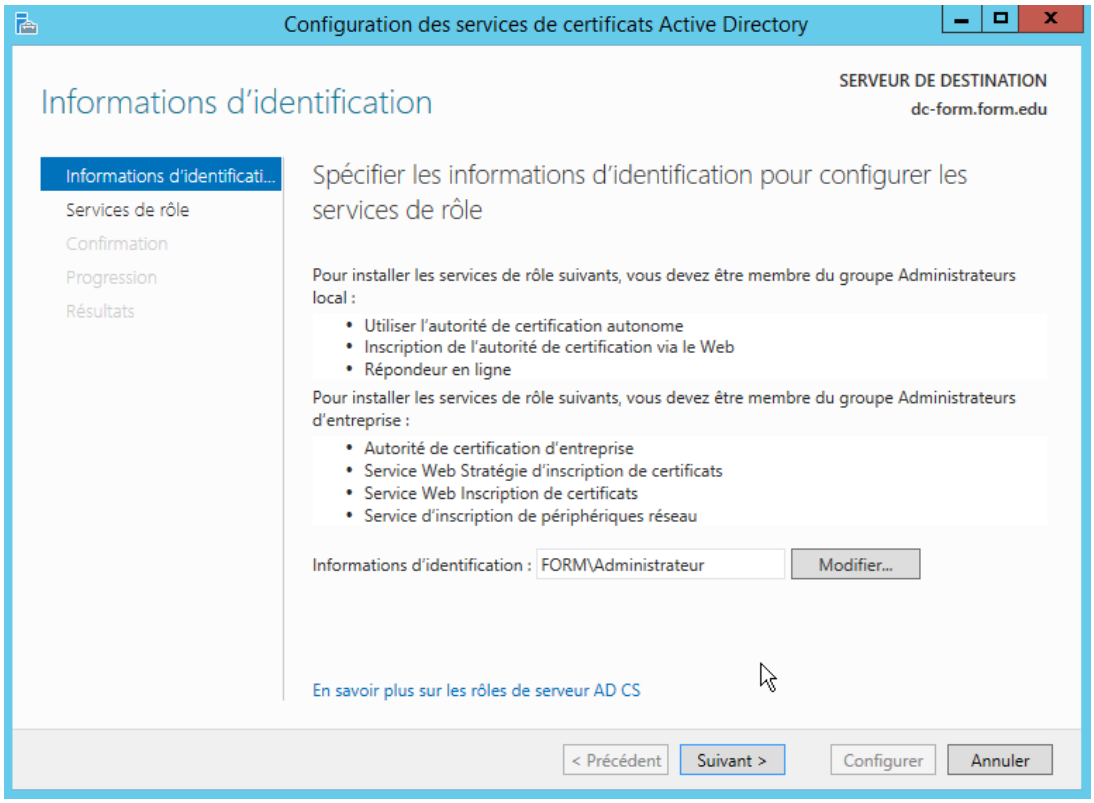
Et cela s'installe

Paramétrage du rôle Service de certificats AD

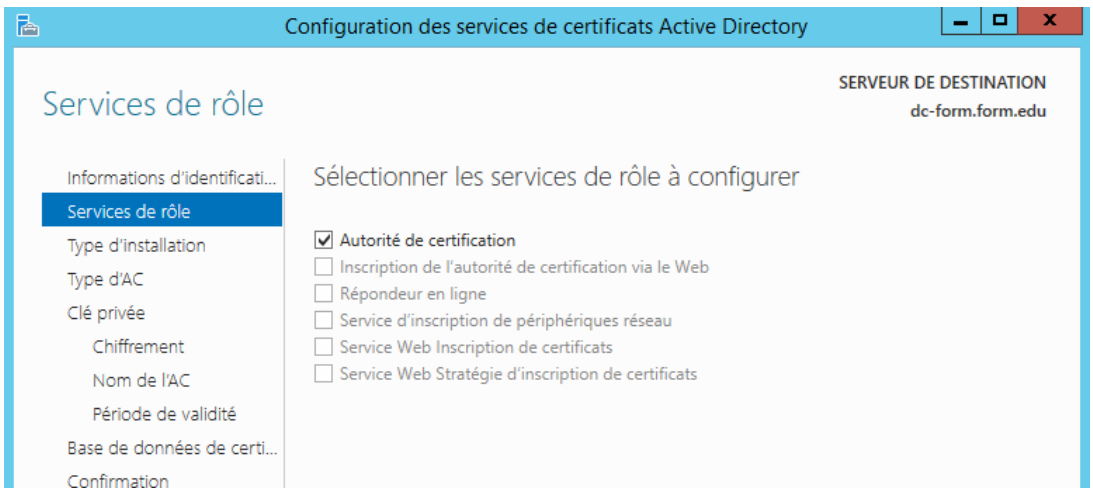
Le **Gestionnaire de Serveur** nous indique qu'il reste à effectuer la **configuration des services de certificat Active directory**



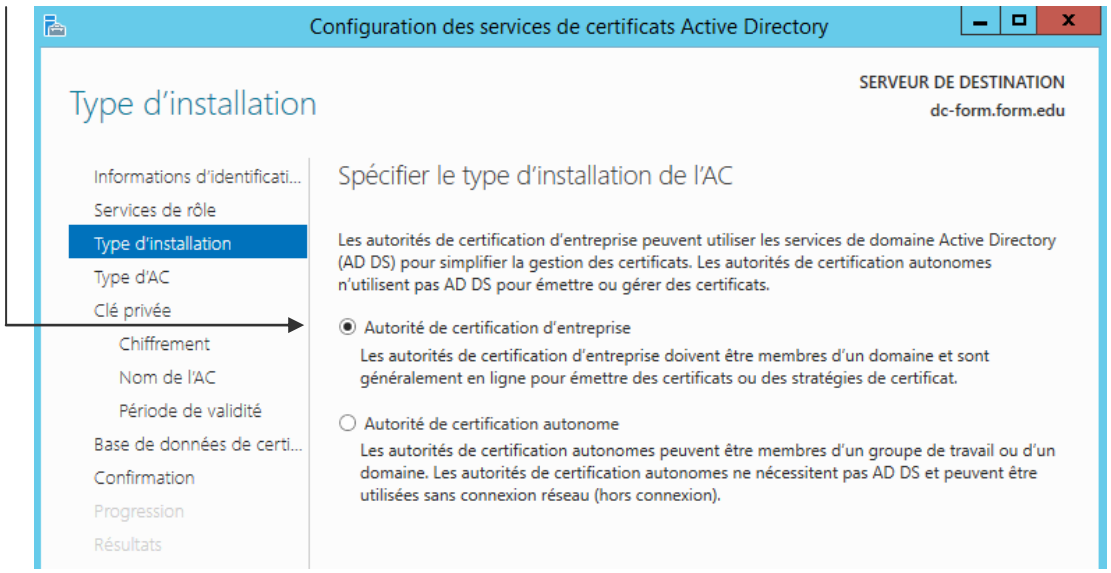
Cela déclenche un assistant (évidemment il faut être loggué en Administrateur de domaine)



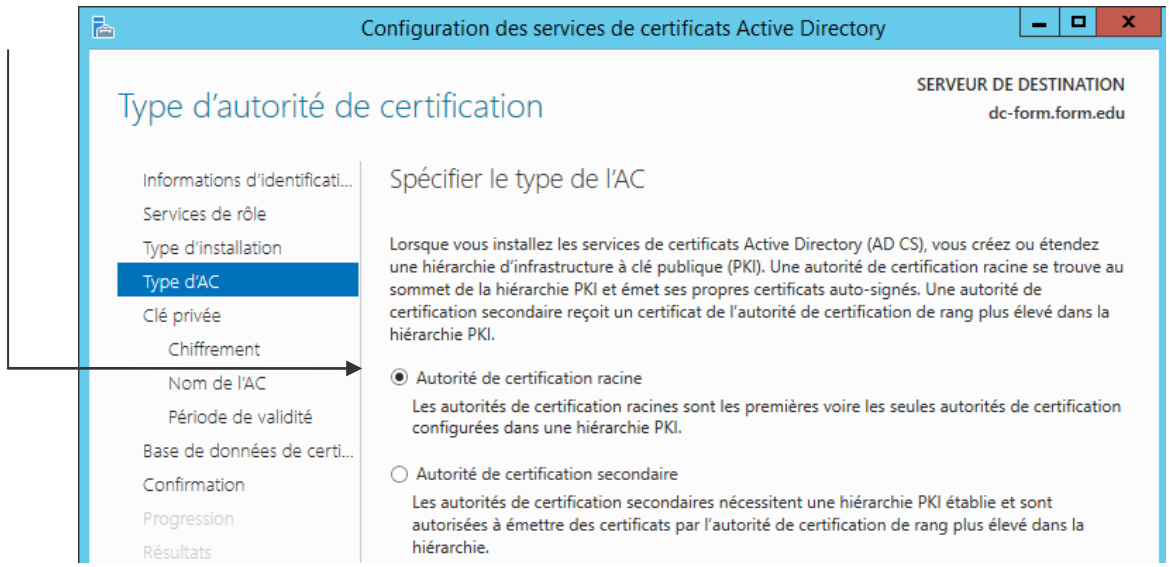
Qui va configurer notre rôle **Autorité de certification** (il faut cocher)



De type **entreprise** (avec publication dans l'**AD**) la portée sera la **forêt**

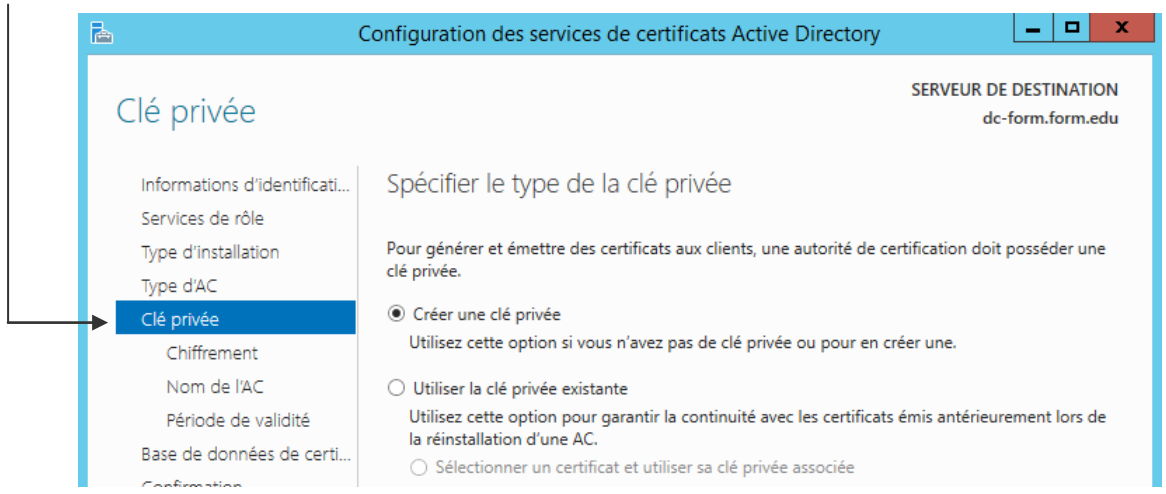


On créé une **PKI RACINE** , (=équivalent ETAT) Dans certains cas on peut déclarer être une autorité de certification secondaire (=équivalent PREFECTURE)

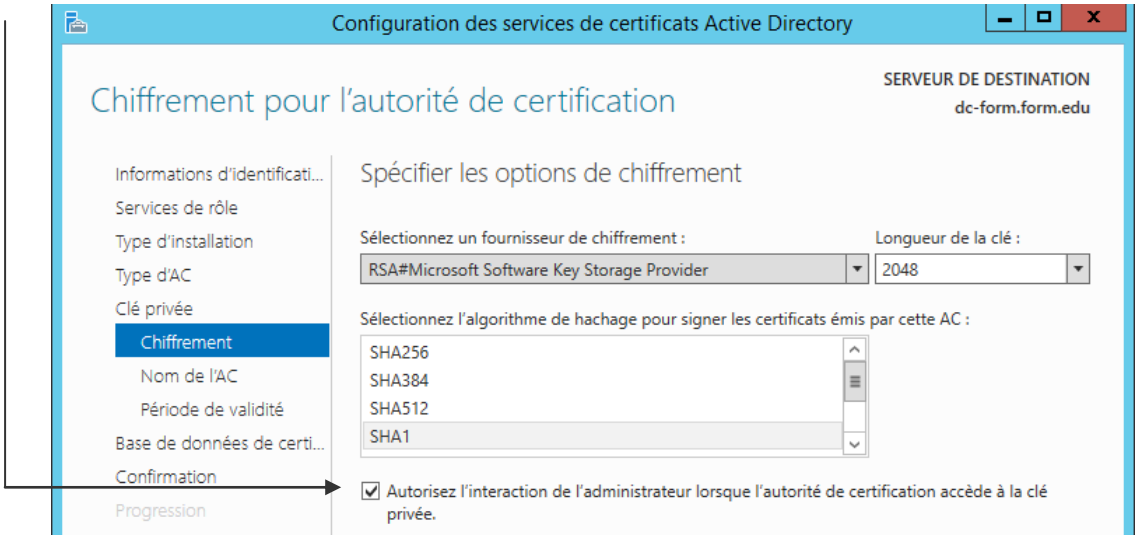


On demande de créer une nouvelle **clé privée**… sauf dans le cas d'une réinstallation, car alors on utiliserait une clé déjà existante…

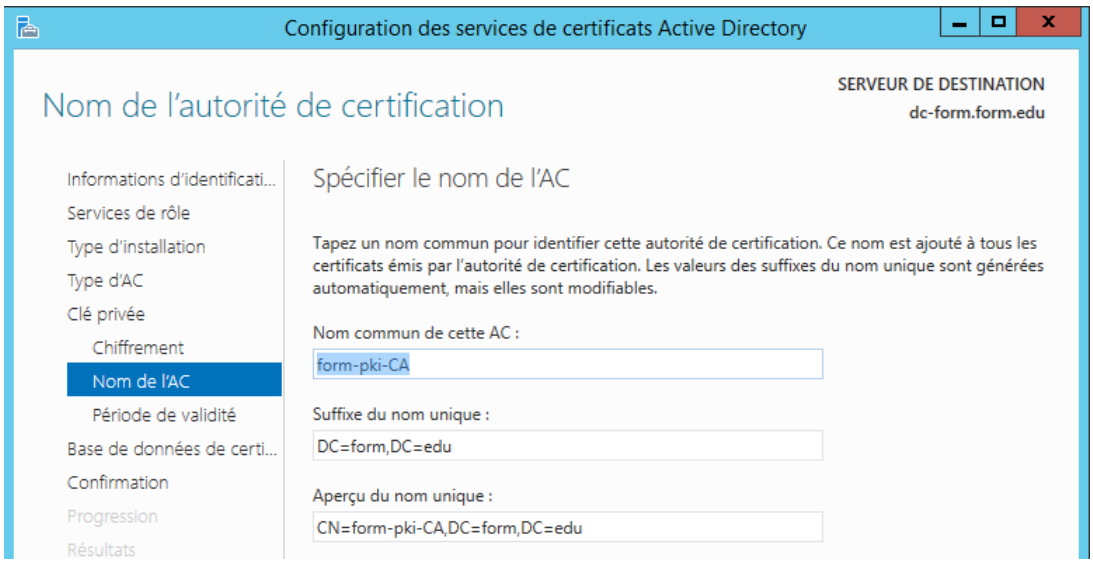
N.B: Si lors d'une réinstallation on génère par erreur une nouvelle clé, il faudra refaire tous les certificats…



On garde le chiffrement proposé **RSA - 2048 - SHA1 et** on autorise l'administrateur à gérer la clé privée



Le nom proposé par défaut peut être et devrait être modifié, par exemple de ***form-DC-FORM-CA*** en ***form-pki-CA*** ***(***pour ***Certification Autorité pki*** du domaine ***FORM)***

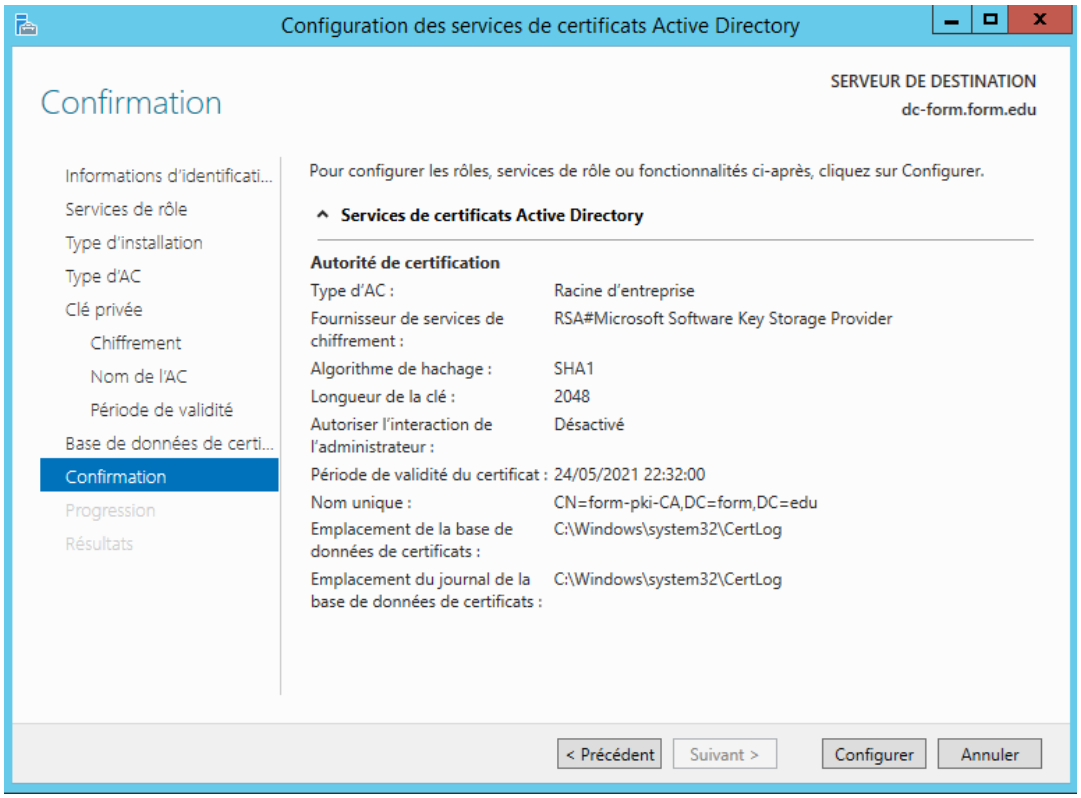


Cela deviendra le **nom de l'Autorité de Certification** qui apparaîtra dans la console **Services de Certificats Active Directory**

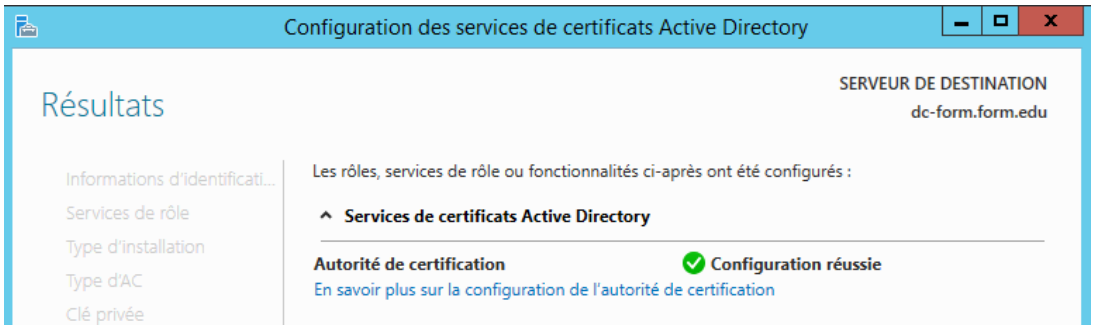
On indique une durée de validité (on met la durée que l'on veut)

On garde les emplacements de stockage par défaut

Un résumé est affiché, on demande **Configurer**



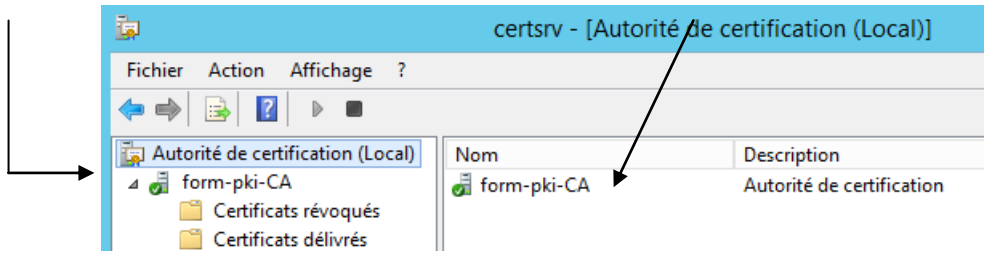
Et on a une confirmation



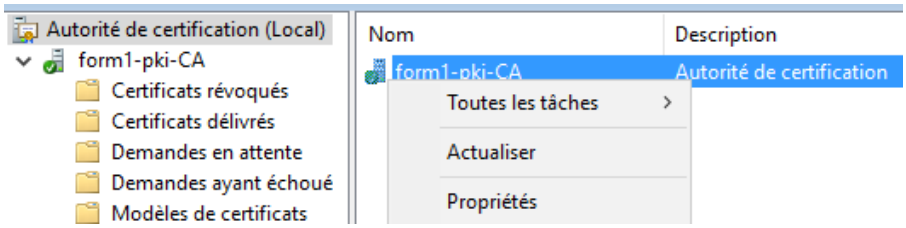
Visualisation PKI

Désormais une MMC nouvelle est disponible dans les Outils du **gestionnaire de serveur**…nommée **Autorité de certification !**

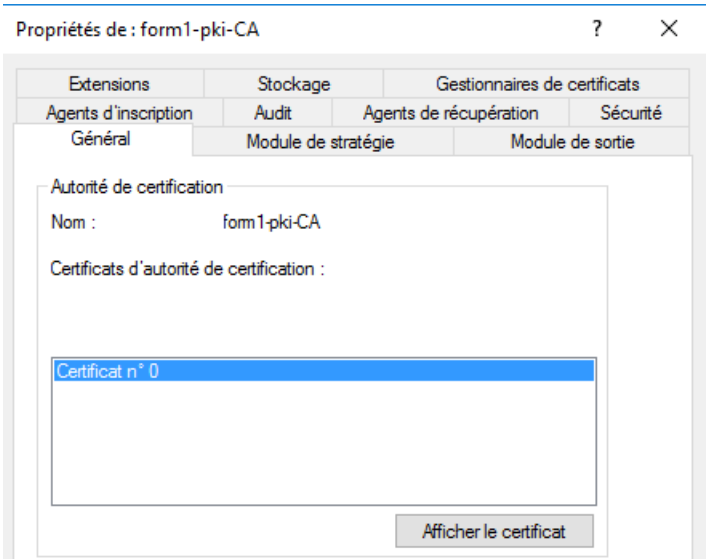
Sur le Serveur ou on a installé l'autorité **nom de l'Autorité**



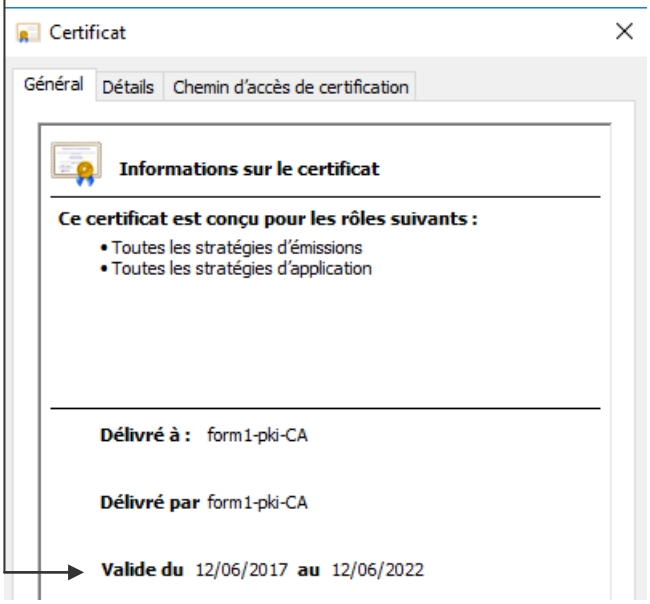
On se place sur la **Pki** et on demande **Propriétés**



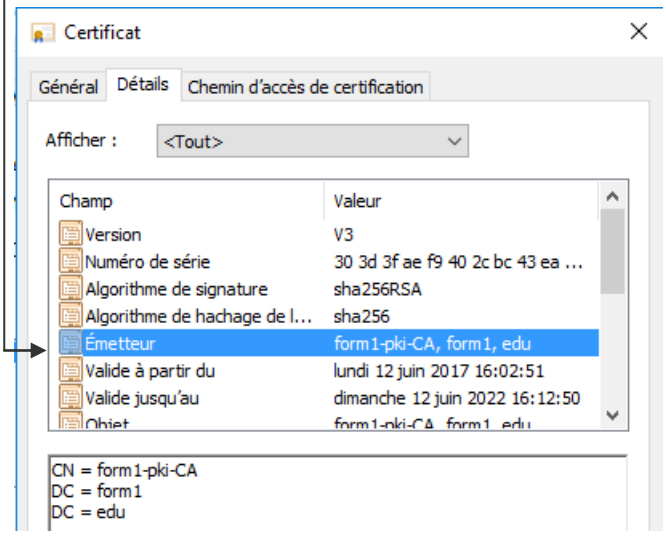
Il ne reste plus qu'à afficher le certificat



Onglet **Général**



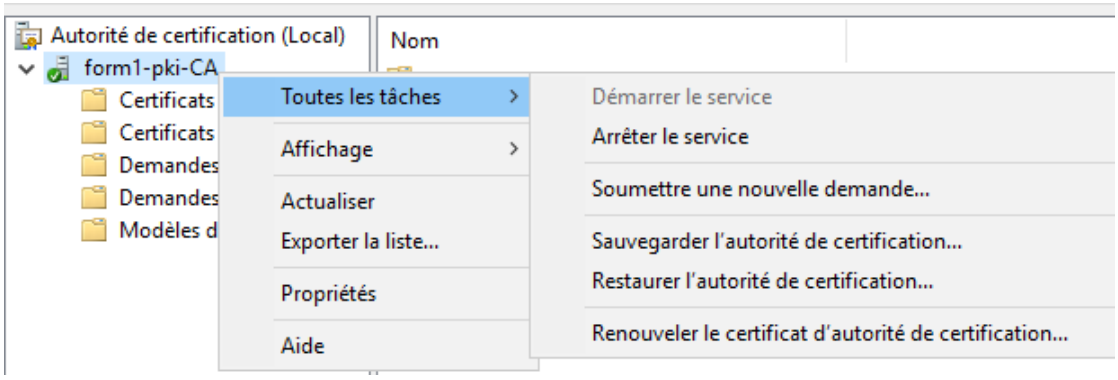
Onglet **Détails**



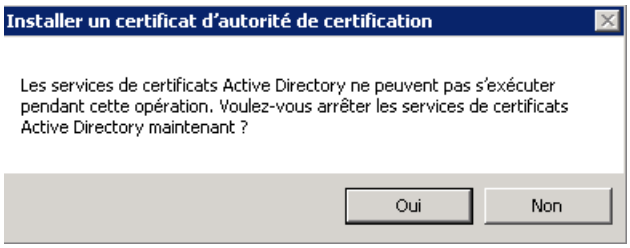
Renouvellement PKI de domaine:

forcément cette **PKi** va arriver à échéance un jour

il suffira alors de demander **Toutes les tâches / Renouveler le Certificat d'autorité de certification**



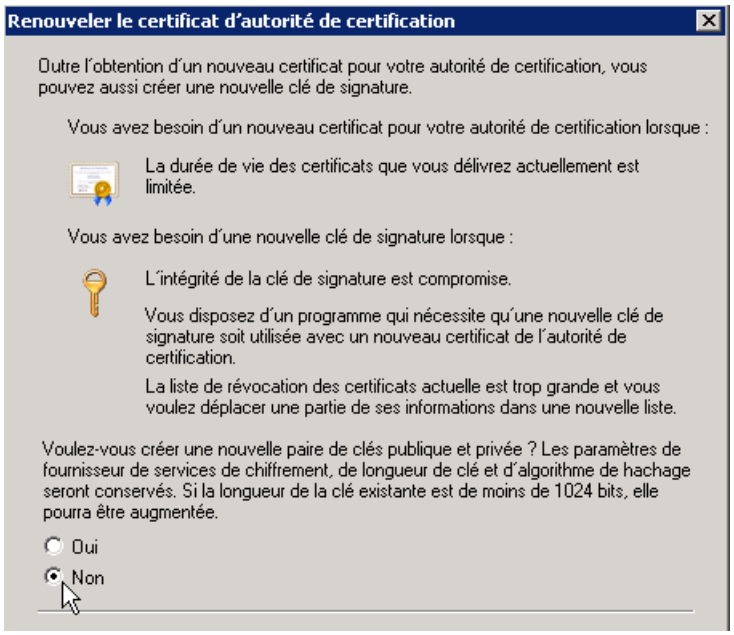
un message apparaît pour stopper le service



il ne faut pas renouveler les clés...

NON

car si on renouvelle les clés, il faudra refaire tous les certificats !



et on obtient le renouvellement pour 5 ans…