http://WWW.CABARE.NET ©

RDS 2012 R2 - Web Access RDWA - Gateway RDG -

sys 32 – Cours & TP -

RDS 2012 - Client Léger - Bureau à Distance

Michel Cabaré – Ver 1.3 – mai 2016-

RDS 2012 accès externe

Cours – Travaux pratiques

Michel Cabaré – Ver 1.3 – Mai 2016

www.cabare.net ©

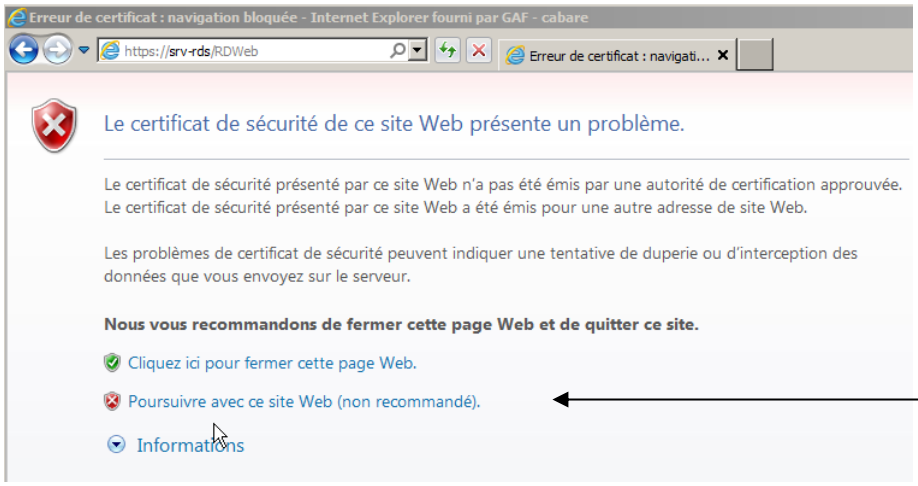
TABLE DES MATIÈRES

PKI ET CERTIFICAT

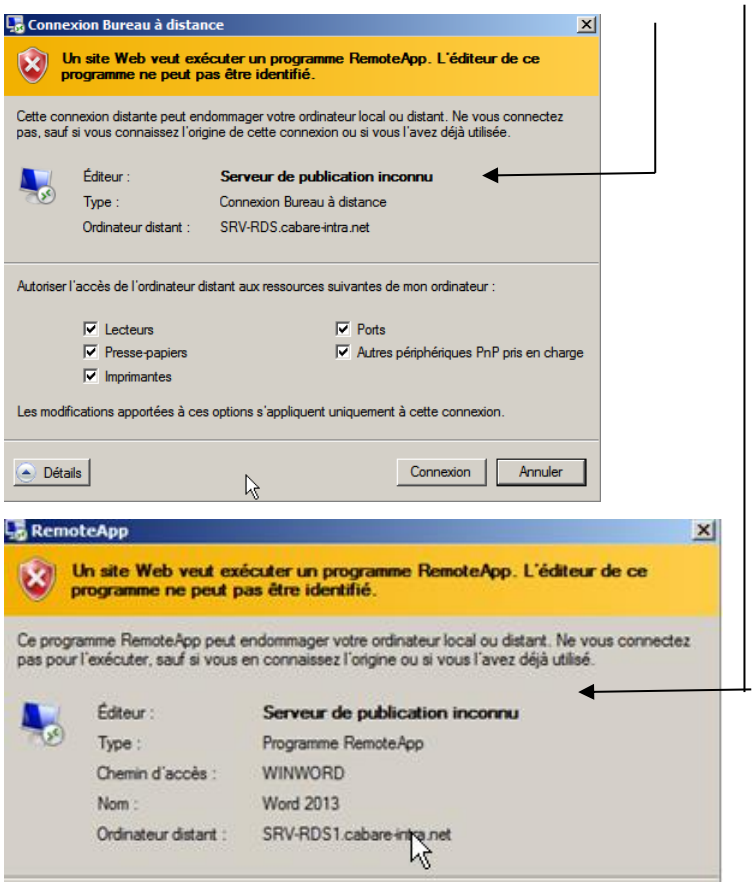
Besoin de certificats :

Il nous faut des certificats pour les applications qui sont mises à disposition sur notre serveur RDS, pour éviter le message de non confiance au lancement …

Que ce soit pour authentifier la connexion au portail web en **HTTPS**…



ou simplement pour authentifier le serveur hôte du **Bureau à Distance (ici une Application Word)**



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 qu'ils soient émis par

- **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)

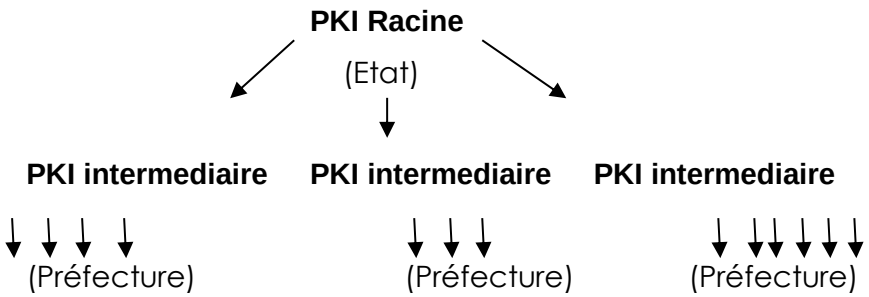
  (*) **STARTSSL** propose des certificats gratuits fonctionnant sur 90 % des browser, **RAPIDSSL** propose des certificats connus par quasiment 100% des navigateurs pour environ 40€/an... ensuite il y a **Verisign.**. etc...

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



Certificat / Certificat / Certificat / Certificat / Certificat / Certificat / Certificat

(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
Validité Horodatage
Origine de l'autorité de Certification = PKI

Déroulement gestion des certificats:

On va opérer le déroulement suivant:

1. On monte une **PKI de domaine** (formation) sur le **DC**
2. puis il faudra certifier/signer le serveur **WEB IIS** pour valider **HTTPS**... c'est à dire faire une demande de certificat pour le serveur WEB, et l'appliquer
3. puis il faudra certifier/signer le **Serveur RDS** c'est à dire faire une demande de certificat pour le **Serveur RDS**, et l'appliquer
   Si on monte un 2° **Serveur RDS**, une **Gateway** ou un **Session Brooker** il faut faire un demande de certificat pour chacun et les appliquer
4. puis il faudra valider/signer aussi chaque application publiée.

   N.B: Si on monte les certificats avant d'installer les applications, elles seront automatiquement signées. Sinon il faut les re-signer.

Création PKI de domaine:

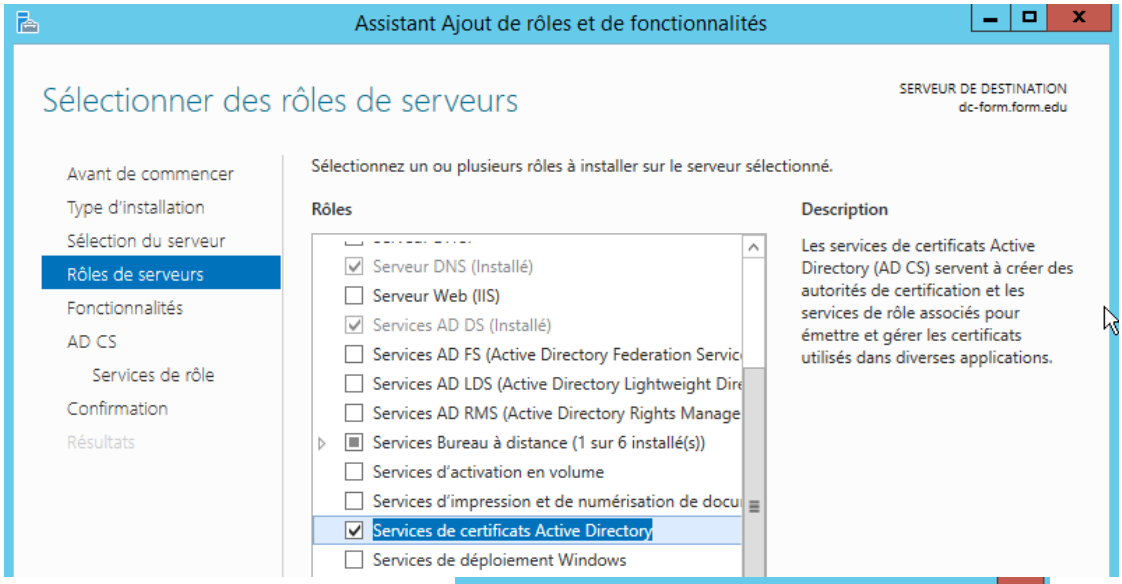
Si cela n'est pas fait, on crée une **PKI de Domaine**, connue dans toute l'**AD**.

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 !

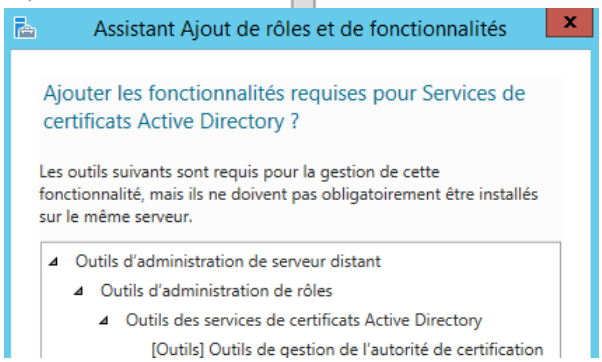
On peut la stocker sur le **DC** qui intègre les **5 rôles**, et un **CG**. Lorsque l'on sauvera le **System State**, ou l'**AD**, elle fera partie de la sauvegarde…

Ajout rôle Service de certificats AD

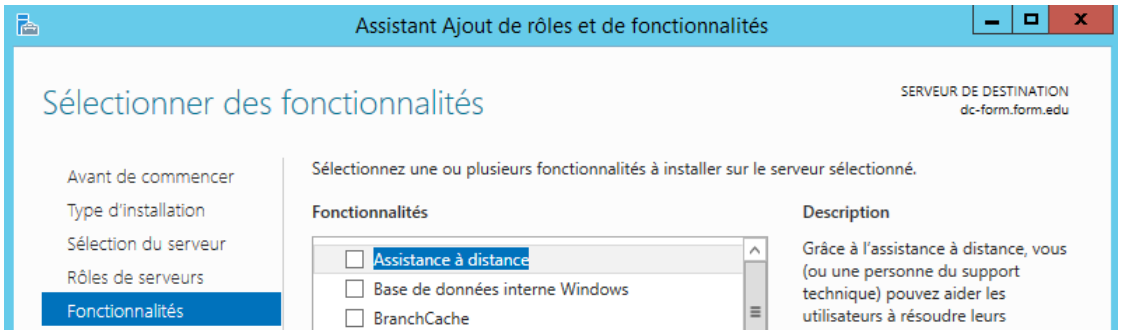
Le rôle peut se poser sur un **DC** ou un serveur spécifique (…) mais jamais sur le Serveur **RDS**. C'est le rôle nommé **Services de certificats Active Directory**



Et toutes les fonctions associées

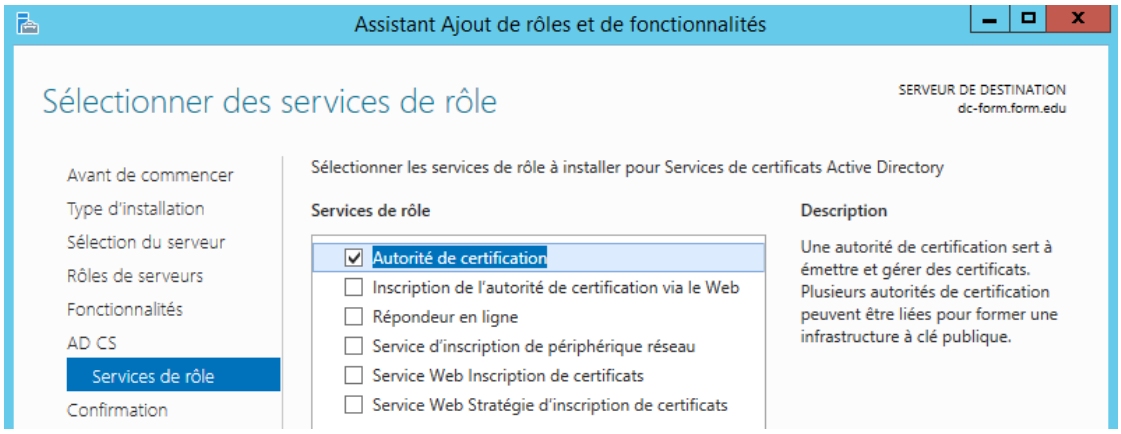


On ne modifie rien d'autres

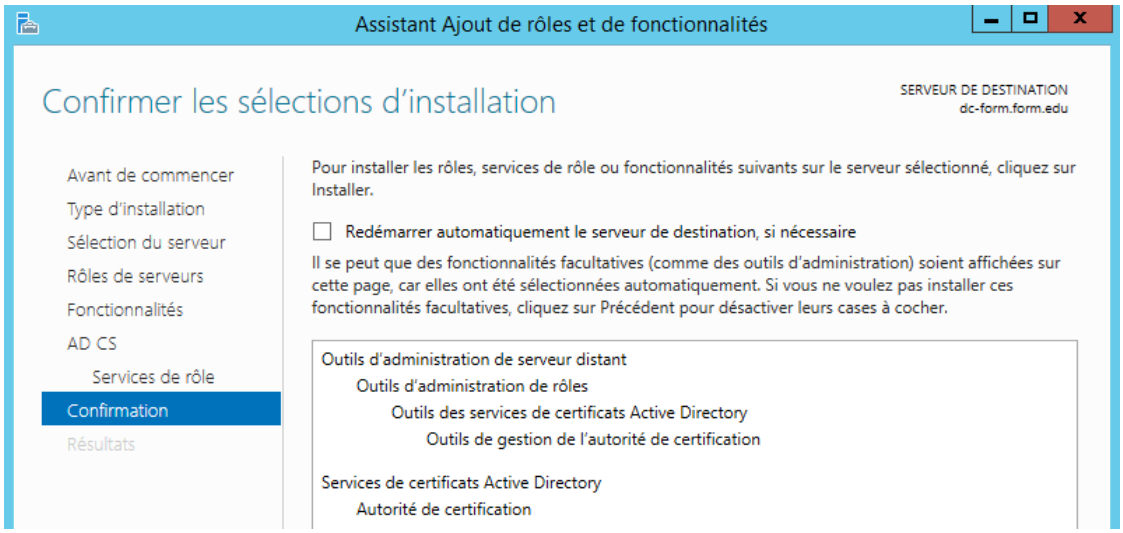


On est informé que les noms de poste et de domaine seront immuables…

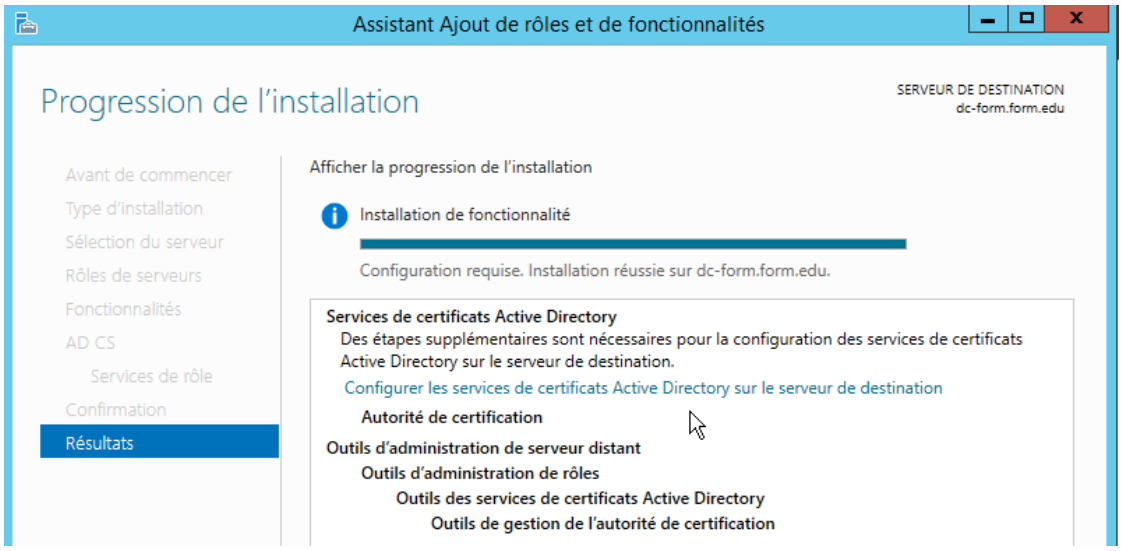
On demande uniquement **Autorité de certification**



On confirme

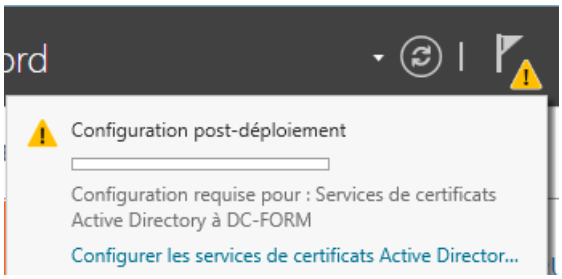


Et cela s'installe

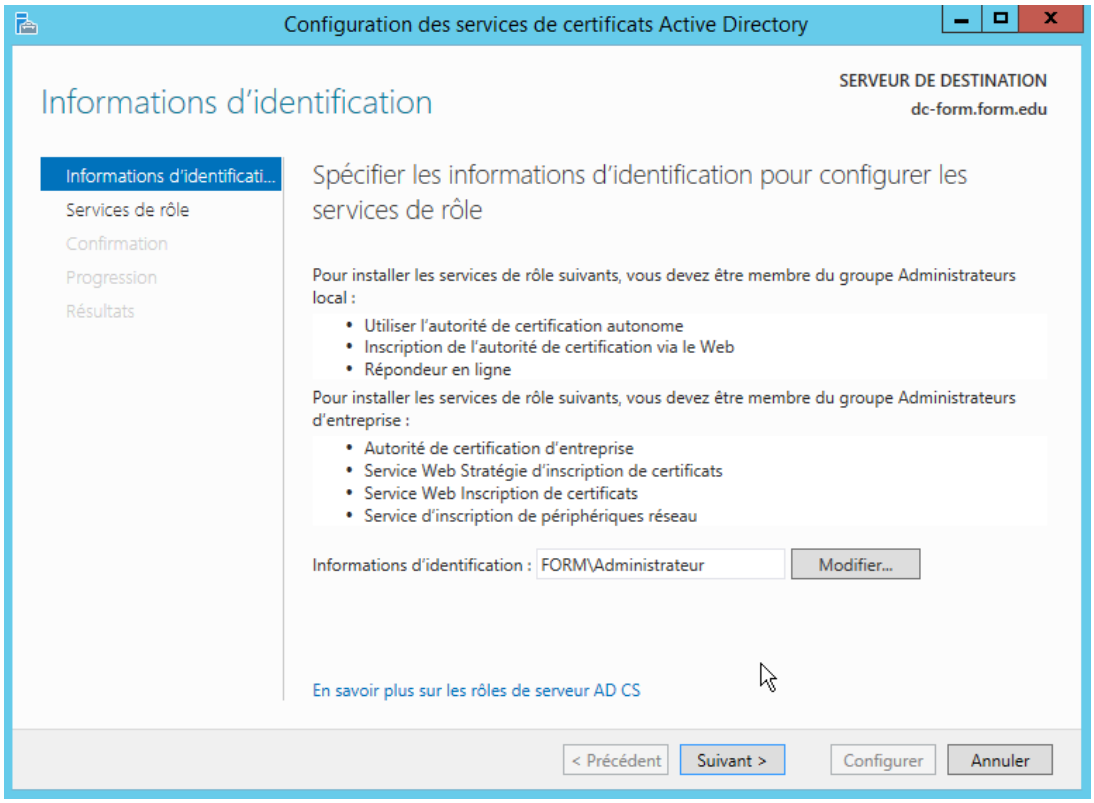


Paramétrage du rôle Service de certificats AD

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



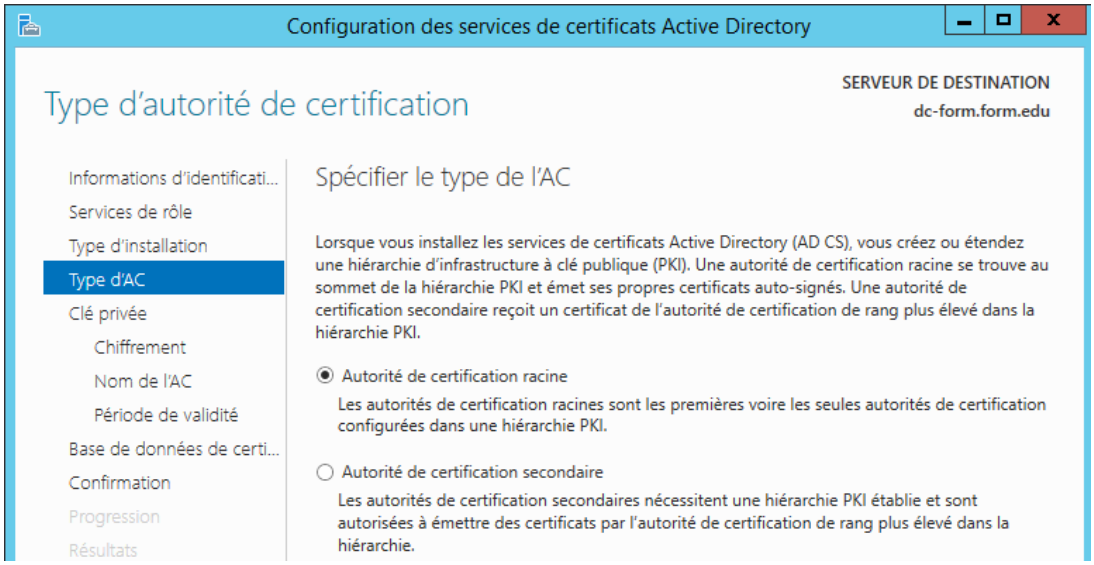
Cela déclenche un assistant



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

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

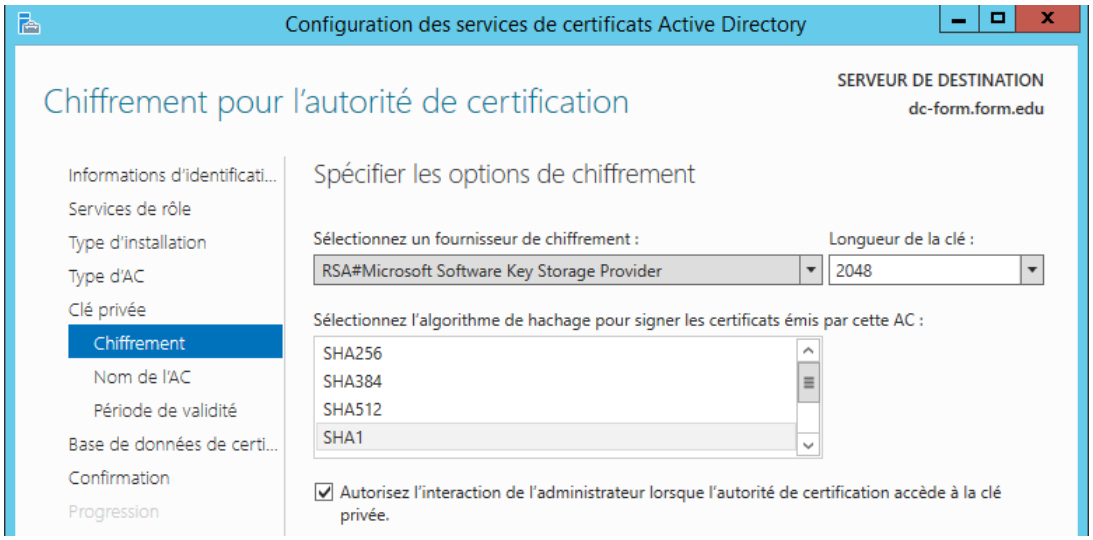
On créé une **PKI RACINE** , (=équivalent ETAT) Dans certains cas on peut déclarer être une autorité de certification secondaire (=équivalent PREFECTURE)



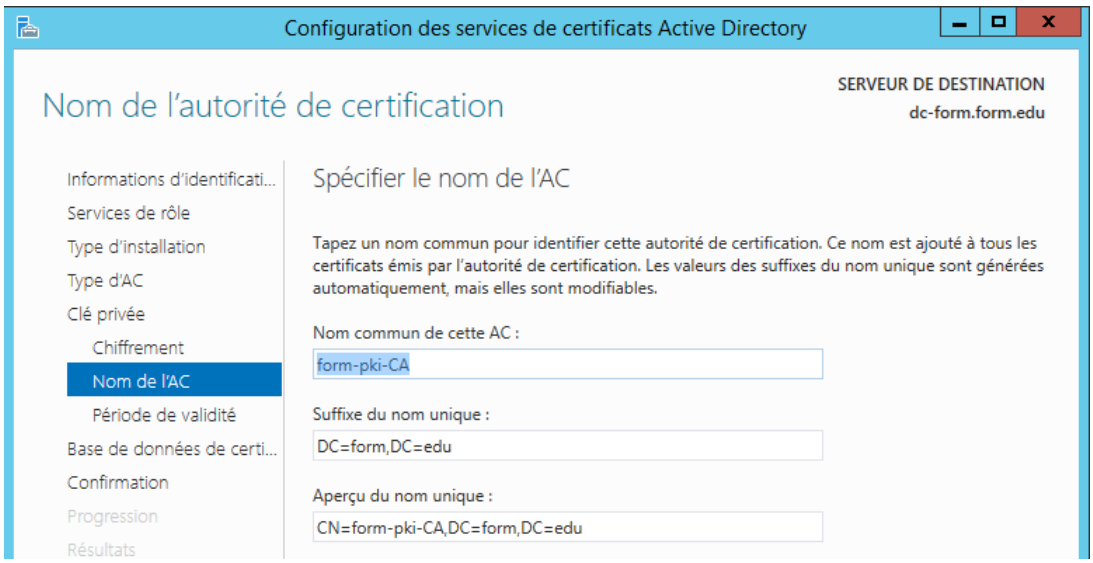
On demande de créer obligatoirement une nouvelle **clé privée**… sauf dans le cas d'une réinstallation, car alors on utiliserait une clé déjà existante...

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



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

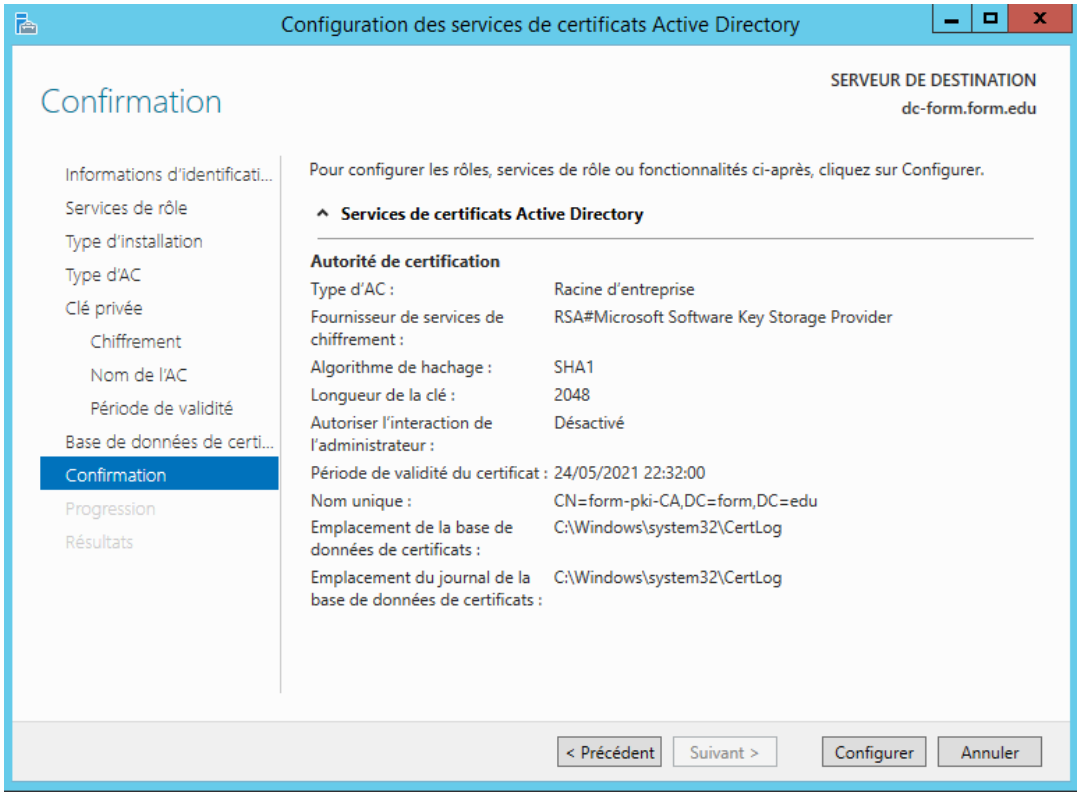


Cela devient le **nom de l'Autorité de Certification** qui apparaîtra dans la console **Services de Certificats Active Directory**

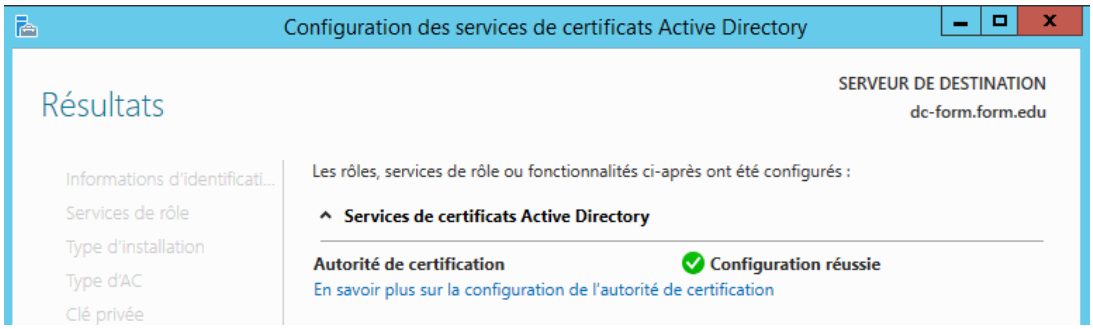
On indique une durée de validité (on met la durée que l'on veut)

On garde les emplacements de stockage par défaut

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

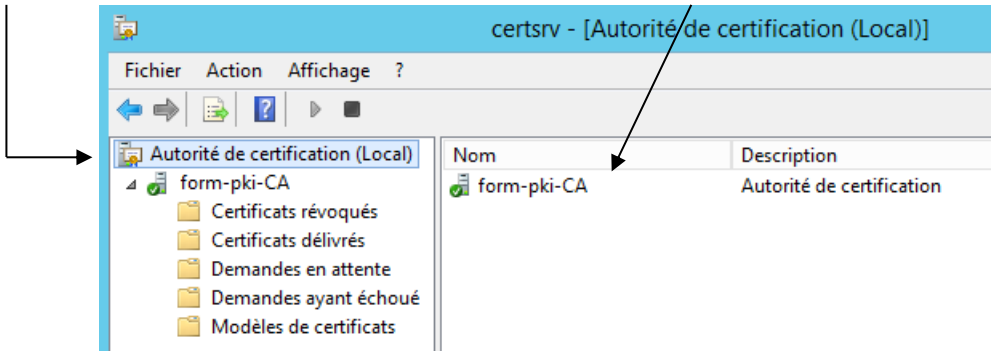


Et on a une confirmation



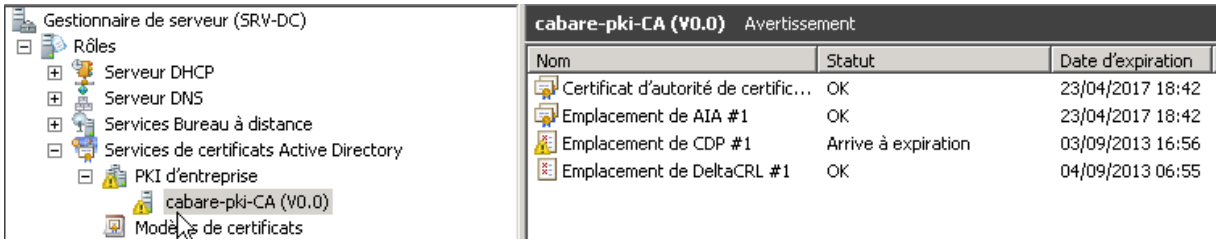
Désormais une MMC nouvelle est disponible dans les Outils du **gestionnaire de serveur**…nommée **Autorité de certification**

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

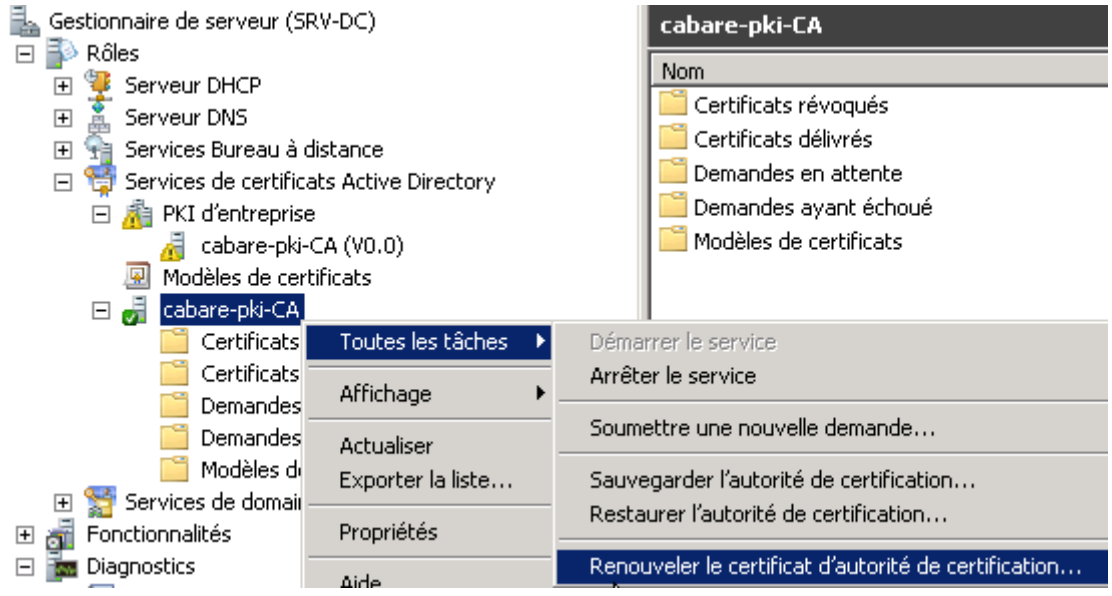


Renouvellement PKI de domaine:

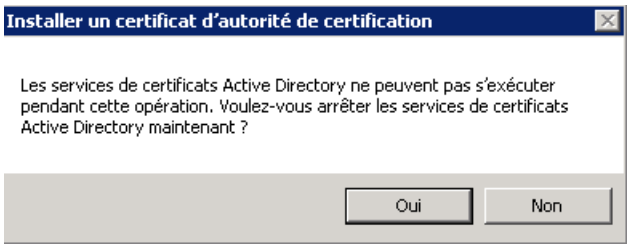
forcément cette **PKi** va arriver à échéance un jour



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



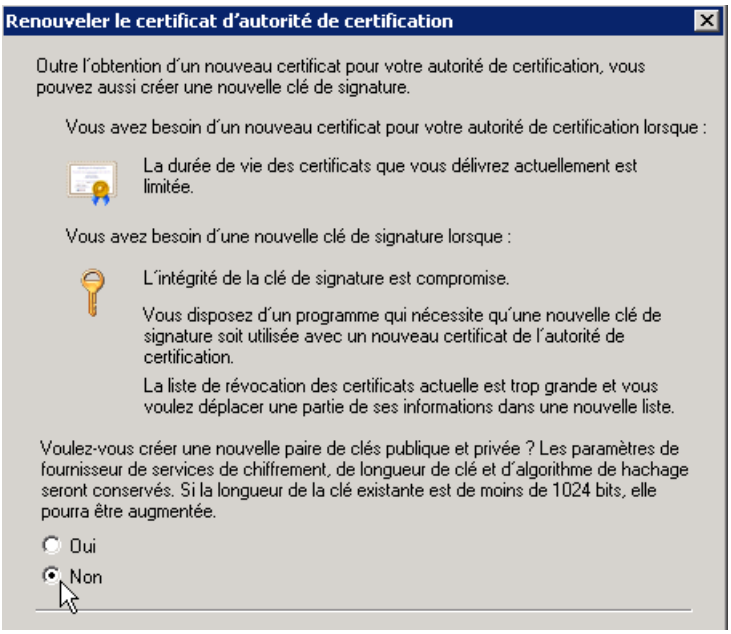
un message apparaît



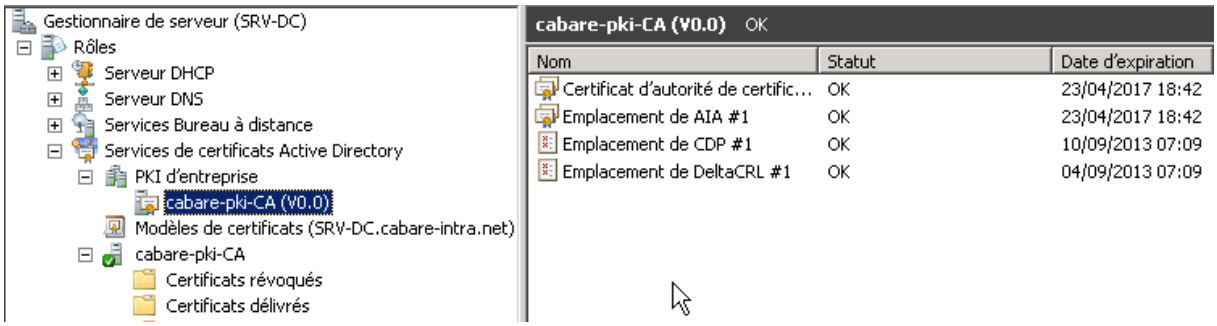
il ne faut pas renouveler les clés...

NON,

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



et on obtient le renouvellement



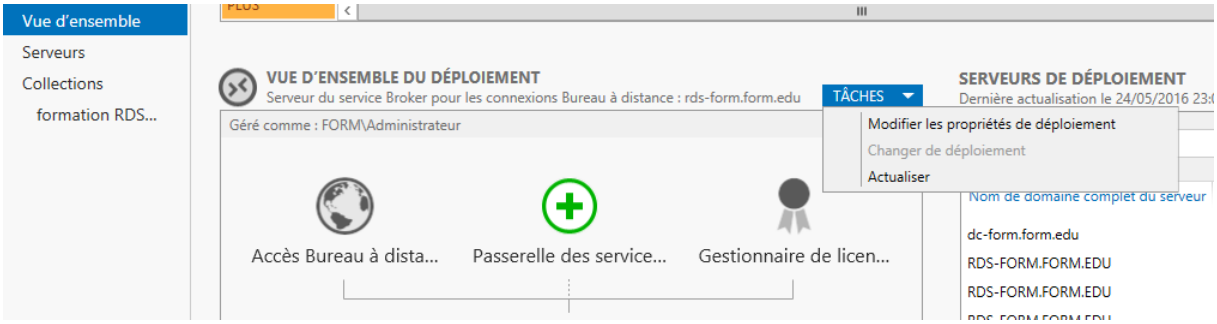
Voici quelques certificats types

Certificats délivrés

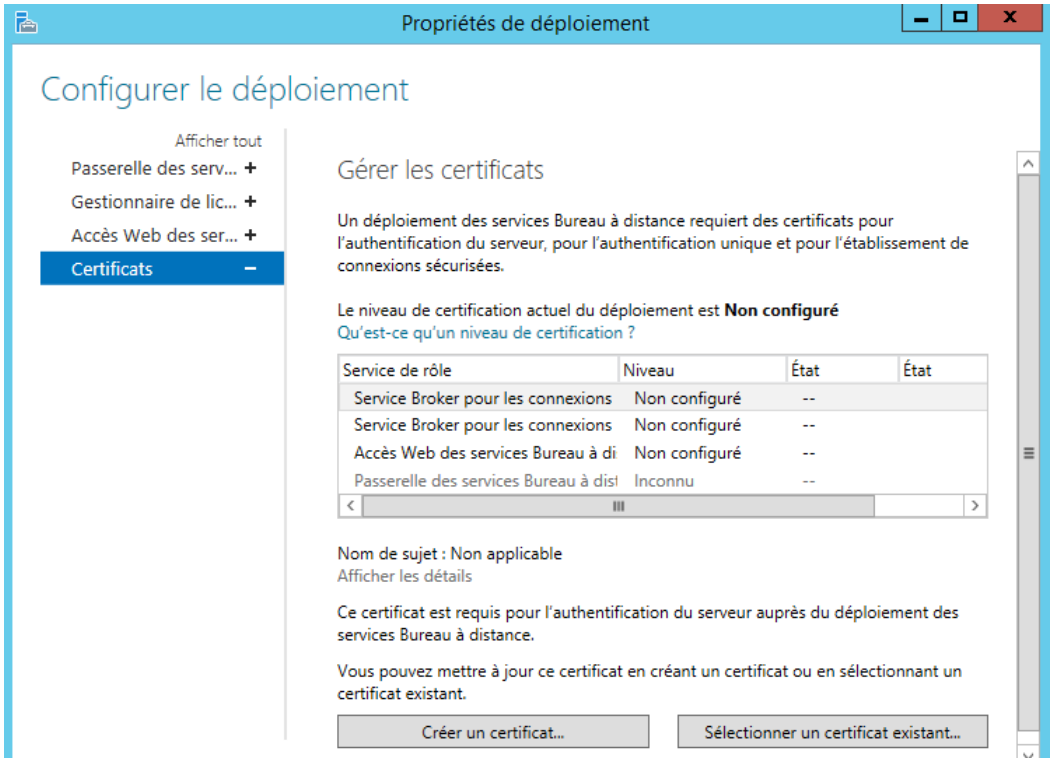
ID de la demande	Nom du demandeur	Certificat binaire	Modèle de certificat	Numéro de série	Date d'effet du certificat
2	CABARE-INTRA\SR...	-----BEGIN CERT...	Échange d'autorité de certification (CAExchange)	3b9294be00000...	23/04/2012 18:33
3	CABARE-INTRA\SR...	-----BEGIN CERT...	Contrôleur de domaine (DomainController)	3ba1161f00000...	23/04/2012 18:49
4	CABARE-INTRA\Ad...	-----BEGIN CERT...	Serveur Web (WebServer)	3bb41d2700000...	23/04/2012 19:10
5	CABARE-INTRA\SR...	-----BEGIN CERT...	Contrôleur de domaine (DomainController)	3c1604d000000...	23/04/2012 20:57
6	CABARE-INTRA\Ad...	-----BEGIN CERT...	Serveur Web (WebServer)	3e2cfbcd00000...	24/04/2012 06:41
7	CABARE-INTRA\SR...	-----BEGIN CERT...	Contrôleur de domaine (DomainController)	14b9e92b00000...	17/10/2012 09:09
8	CABARE-INTRA\SR...	-----BEGIN CERT...	Contrôleur de domaine (DomainController)	18ed905700000...	13/03/2013 00:14
9	CABARE-INTRA\SR...	-----BEGIN CERT...	Échange d'autorité de certification (CAExchange)	361ef22600000...	02/09/2013 18:35
11	CABARE-INTRA\Ad...	-----BEGIN CERT...	Serveur Web (WebServer)	362f566000010...	02/09/2013 19:07
12	CABARE-INTRA\SR...	-----BEGIN CERT...	Contrôleur de domaine (DomainController)	3d82dc3a00010...	05/09/2013 13:28

Déploiement - Quels Certificats pour Quels Serveurs:

On se met sur la **Vue d'ensemble** des **Services Bureau à distance**, et on demande dans les **tâches** de **Modifier les propriétés du déploiement**



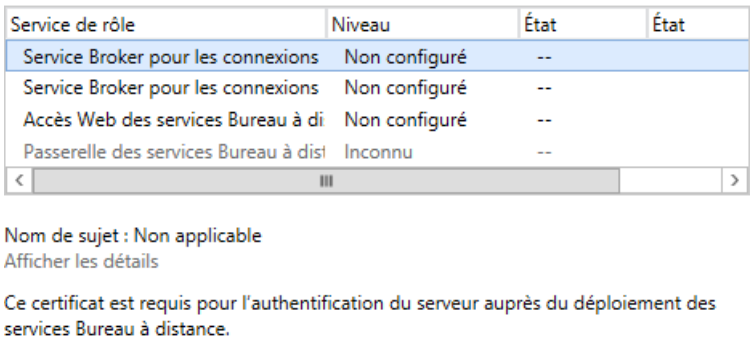
Et on se place sur **Certificats**



On l'a déjà dit, Pour chaque serveur physique / rôle logique, il faut faire une demande de **Certificat** pour attester que cette machine est bien celle qui porte ce nom là... (ne jamais renommer un Serveur, sans refaire le Certificat)

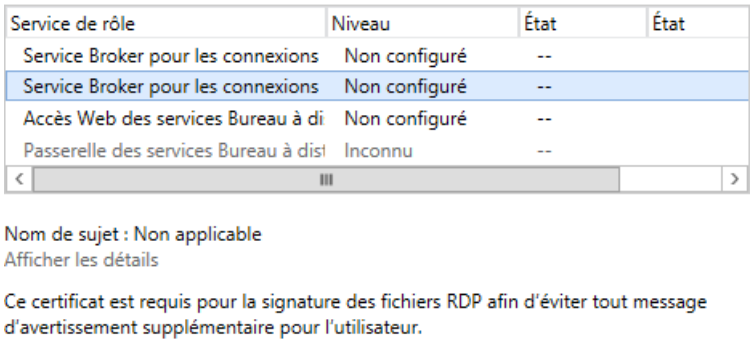
3 machines – rôles doivent être certifiés au minimum (4 si l'on a une passerelle)

- Sur le Serveur qui héberge le Rôle Hôte **RDSH**, il va falloir effectuer une demande de certificat avec le nom **FDQN** du serveur, puis l'appliquer au Serveur **(rôle Broker pour l'authentification SSo)**

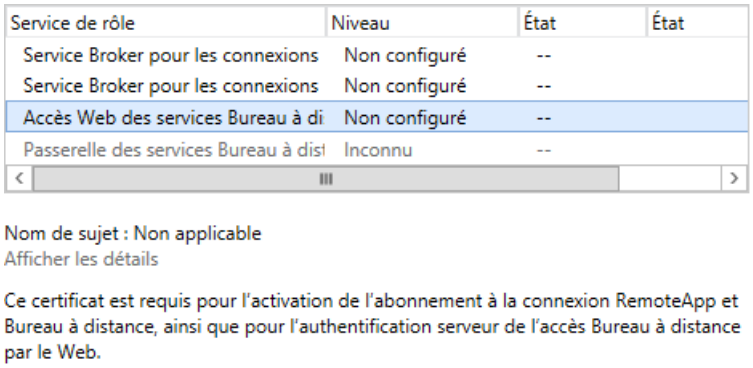


- Sur le Serveur qui héberge le Rôle Hôte **RDSH**, il va falloir effectuer une demande de certificat avec le nom **FDQN** du serveur, puis l'appliquer au Serveur **(Rôle RDSH pour authentification application RemoteApp)**

  N.B : Si un certificat existe déjà pour cette machine, il suffit de l'appliquer sans redemander la création.



- Sur le Serveur qui héberge le Rôle Serveur **RDWA**, il va falloir effectuer une demande de certificat avec le nom **FDQN** du serveur, puis l'appliquer au serveur **(Rôle RDWA pour https)**.

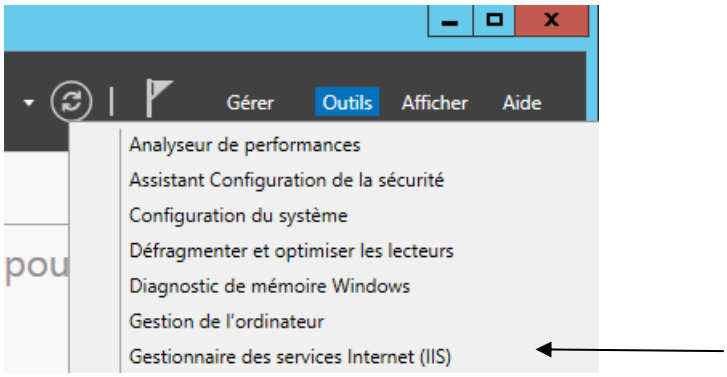


- Dans le cas d'une configuration avec une passerelle, il faudra également effectuer une demande de certificat avec le nom **FDQN** du serveur, puis l'appliquer sur la **Gateway**

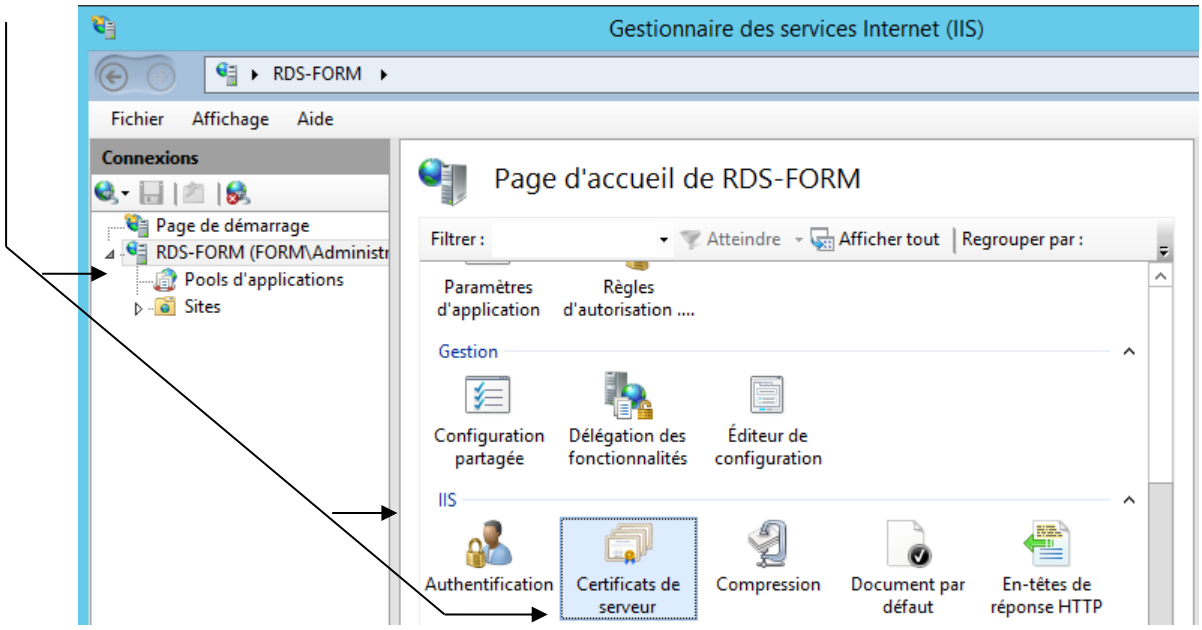
Demande de création de Certificat de Domaine – via IIS:

Il faut donc d'abord se créer un **certificat de domaine**. Cela peut se faire pour notre Serveur **RDSH / RDWA** par la console **Gestionnaire IIS**

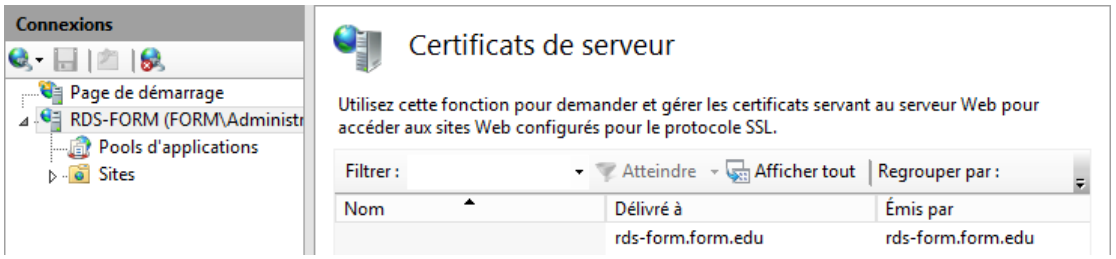
Dans le gestionnaire de Serveur on demande **gestionnaire des services internet (IIS)**



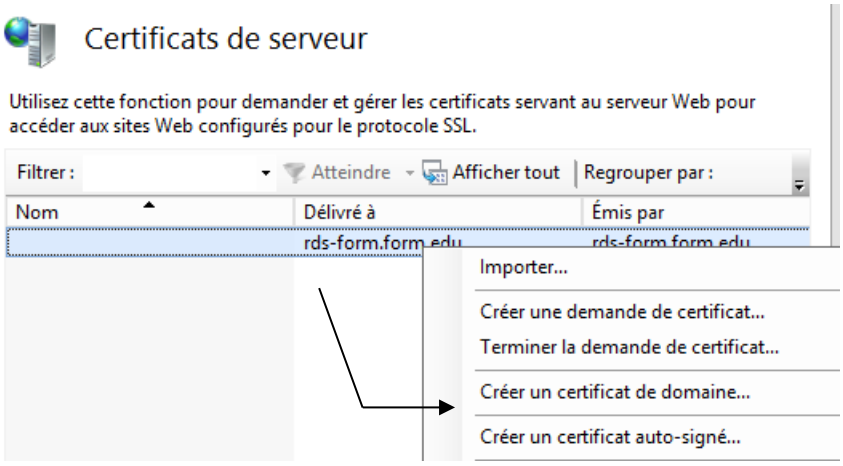
Dans la console, on se place sur notre serveur, puis dans la section **IIS** on clic sur **Certificats de serveur**



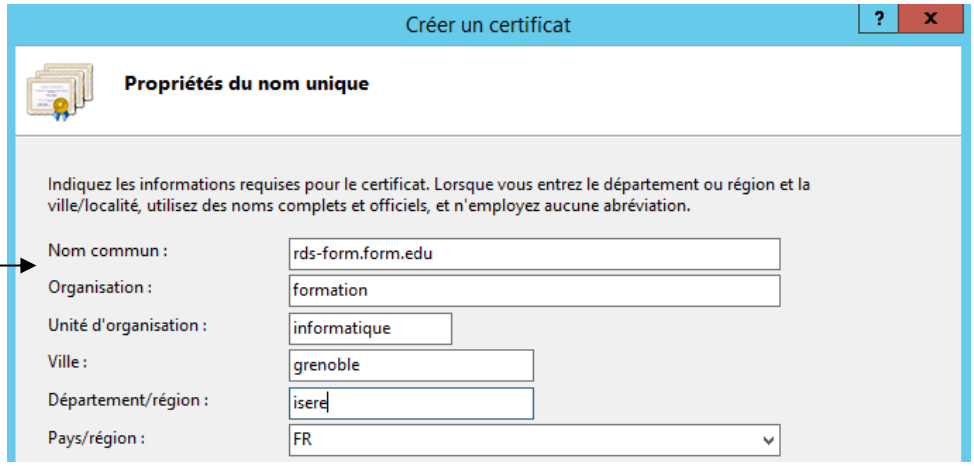
le **certificat auto-signé** du serveur apparaît



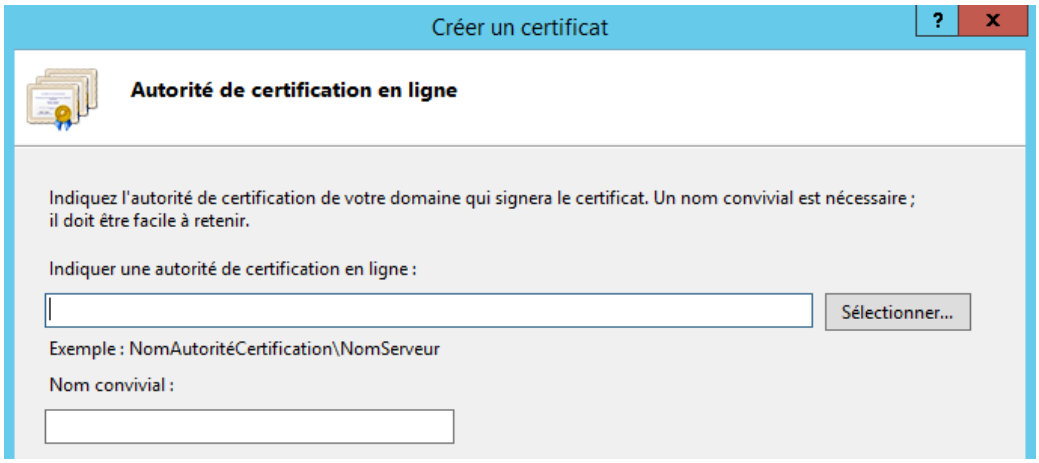
Pour avoir un **certificat de domaine** (la **racine PKI** étant déjà créé), il faut demander clic-droit **Créer un certificat de domaine…**



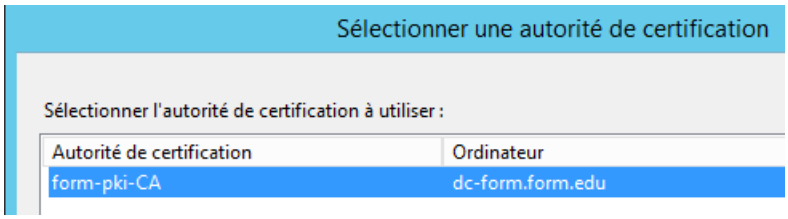
Seule la première ligne **Nom commun** avec le **FQDN** est importante



Ensuite il faut aller chercher notre **autorité racine PKI** par **Sélectionner**



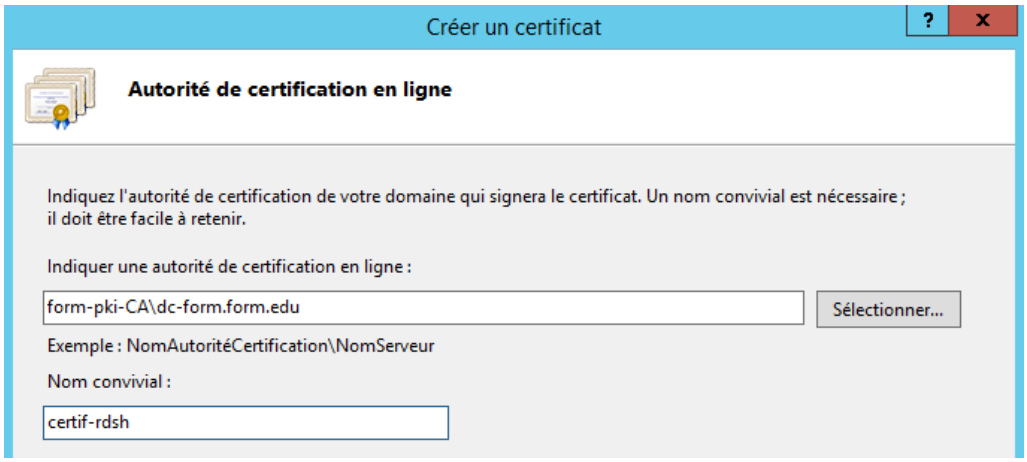
Et choisir notre **PKI**



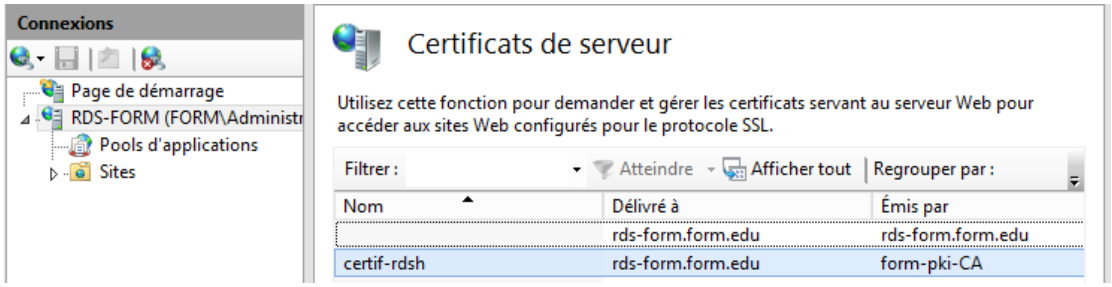
N.B: Dans **Sélectionner…** cela peut mettre du temps à apparaître, et on peut faire un **gpupdate /force** pour accéllerer un peu

```
C:\Users\Administrateur.CABARE-INTRA>gpupdate /force
Mise à jour de la stratégie...

La mise à jour de la stratégie utilisateur s'est terminée sans erreur.
La mise à jour de la stratégie d'ordinateur s'est terminée sans erreur.
```

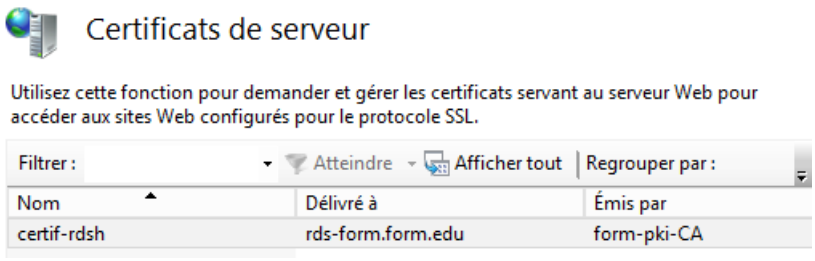
Et on donne un nom pratique à retenir, par exemple ***certif-rdsh***



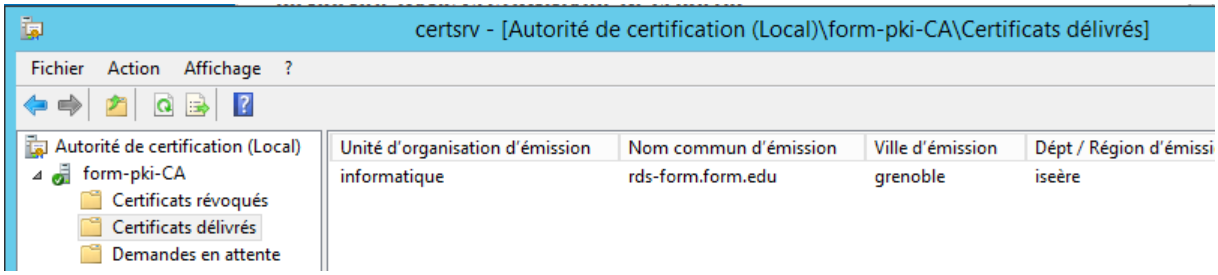
Et on notre certificat de domaine se crée, ici **certif-rdsh**



N.B : par mesure de sécurité, et pour éviter toute confusion, on peut supprimer le certificat auto signé et ne garder que celui de domaine !



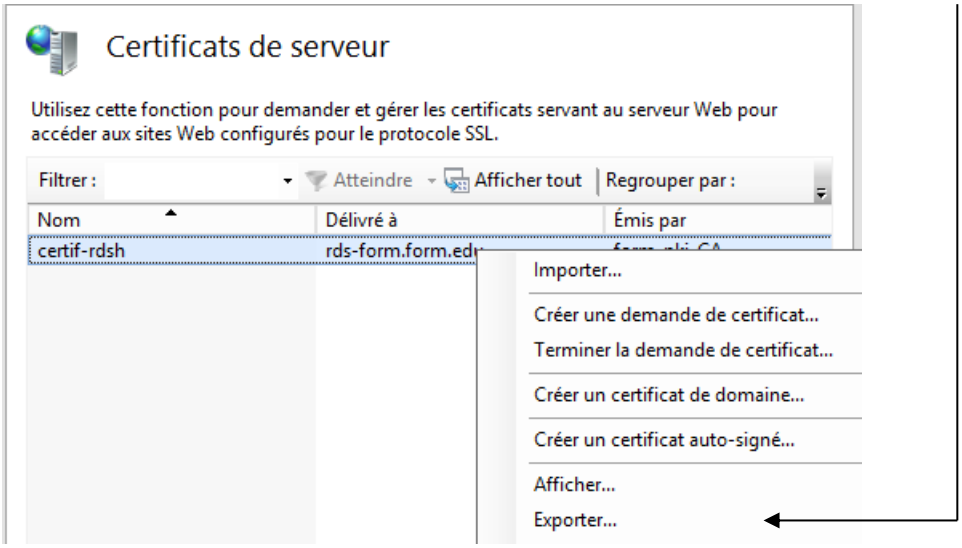
A titre d'information notre certificat est présent sur le serveur ou est installé **l'Autorité de certification**, dans les **certificats délivrés**



Il correspond à un certificat garantissant un ordinateur, délivré par notre **pki**..

Export de certificat:

Toujours depuis la console IIS on va exporter ce certificat clic droit **Exporter…**



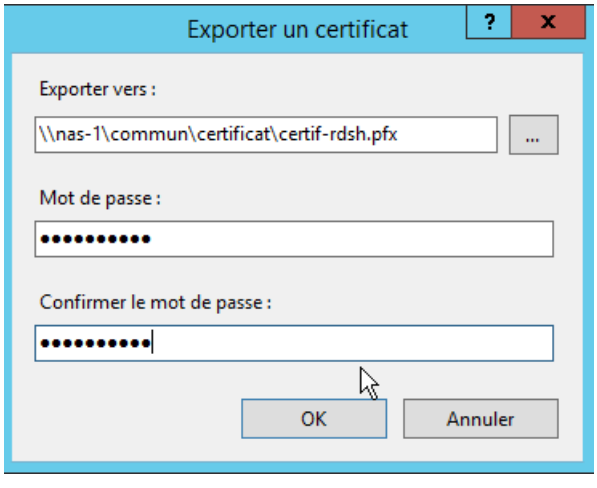
En le plaçant à un endroit accessible,

par exemple un emplacement

\\nas-1\commun\xxxx.**pfx**

Et 1 mot de passe identique pour tous les certificats, du genre

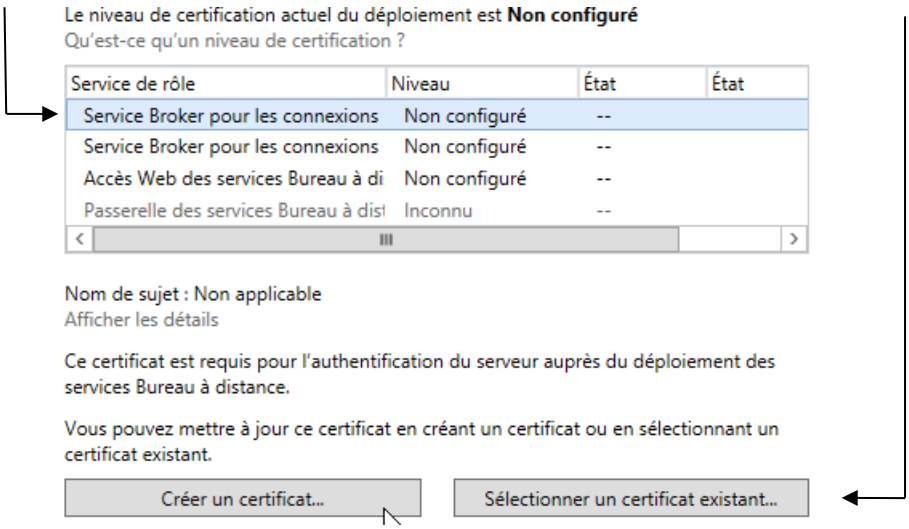
certifxxxx



Application / import de Certificat:

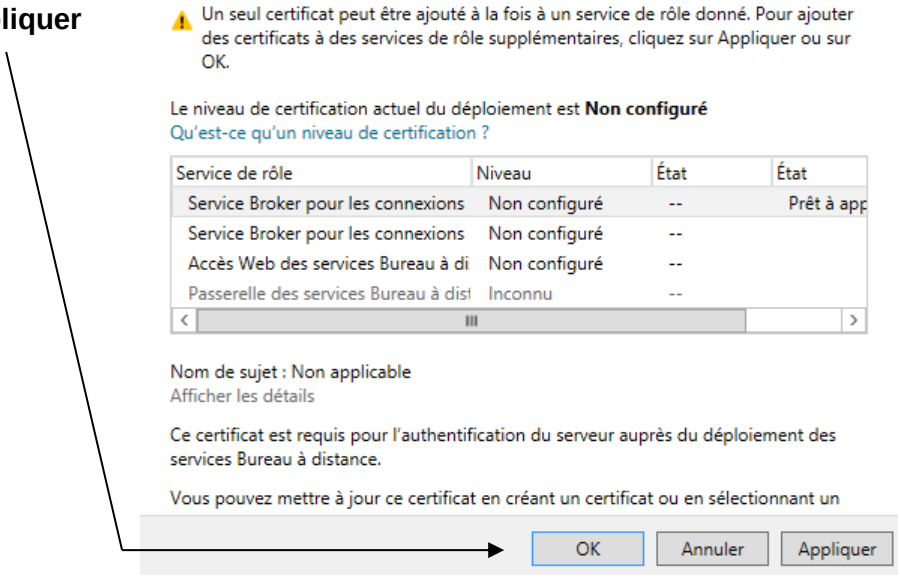
Dans la console **Configurer le Déploiement – Certificats** on n'utilise surtout pas **Créer un certificat** (qui crée des certificats auto signé) car on va aller chercher les certificats de domaine que l'on a préalablement crée via **IIS.**

On se place sur le premier Rôle et via **Sélectionner un certificat existant**



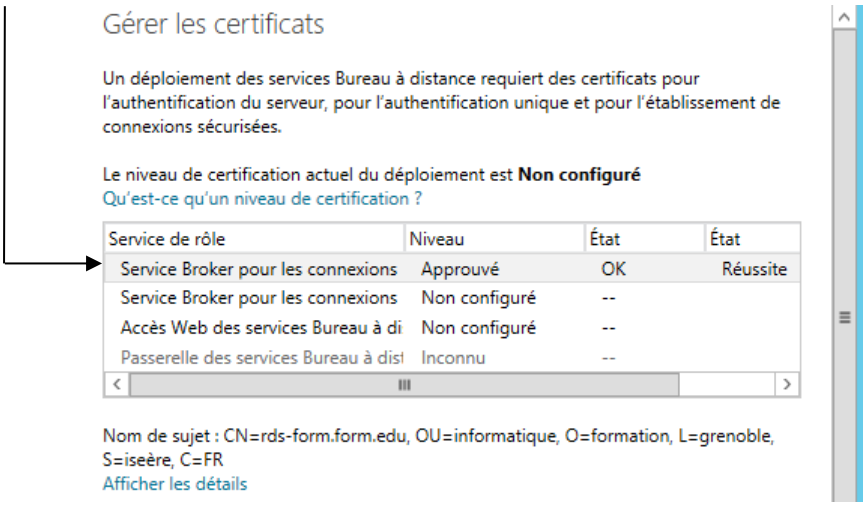
On va chercher notre certificat précédemment exporté

Et on demande **Appliquer**

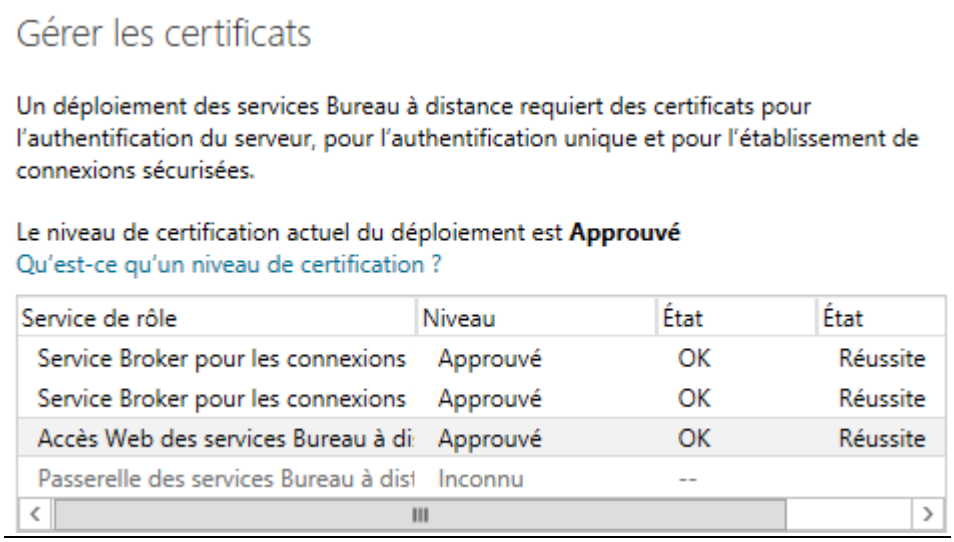


pour obtenir

Niveau **Approuvé** (certificat de domaine) Etat **OK**

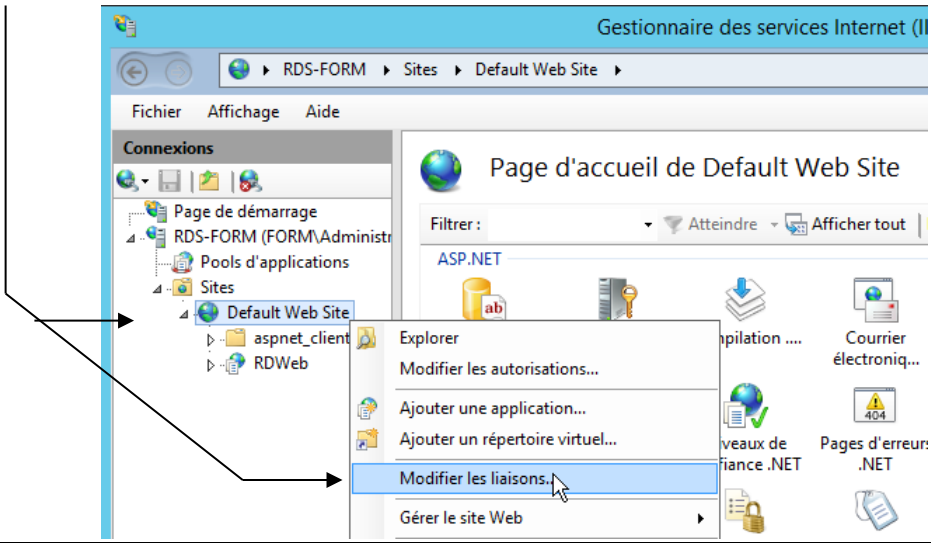


Comme les 3 rôles sont sur le même serveur, on refait la manip 2 fois de manière à avoir au final les 3 certificats (pour le même serveur physique)

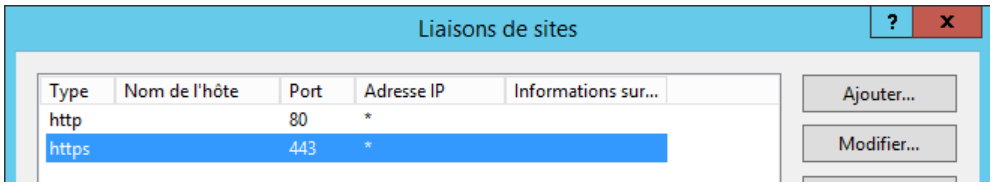


Application du Certificat sur IIS pour SSL (vérification) :

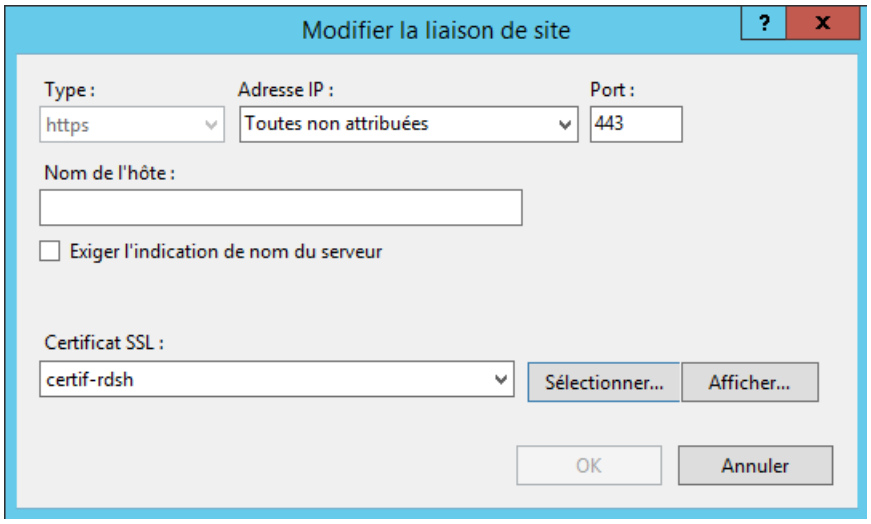
Dans le **Gestionnaire IIS** on demande dans les **Sites**, sur le Site Web par défaut **Default Web Site** et clic droit **Modifier les liaisons...**



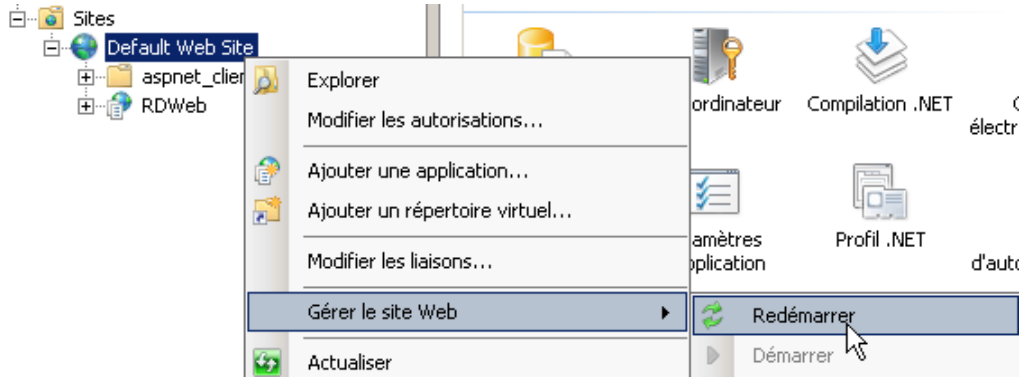
Et la on sélectionne ensuite la liaison **https 443** , et en demandant **Modifier…**



Si besoin on indique le nom "pratique"du certificat de domaine



Si on effectue un changement, bien penser à **Redémarrer** le serveur



VERIFICATION DES CERTIFICAT

Connexion HTTPS au portail RDWeb –FQDN et domaine:

Le problème était ce message sur (par exemple) l'URL **https://rds-form/RDWeb**

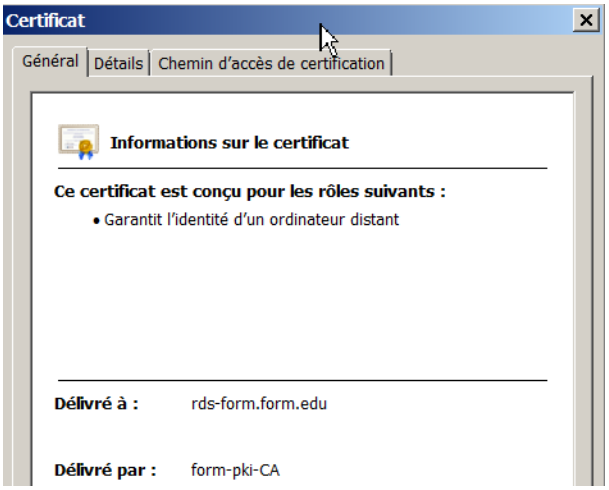
On indique simplement que on n'a pas certifié le bon site …

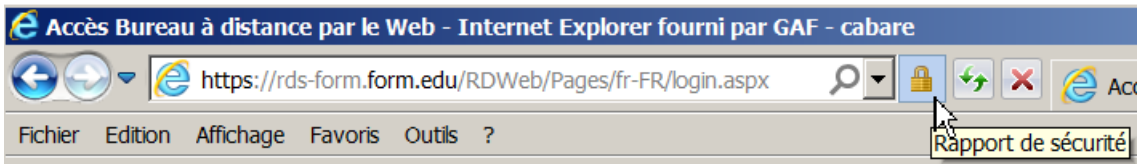
Il faut une adresse FQDN…

Lorsque l'on a certifié le serveur IIS, on a indiqué la machine **rds-form.form.edu** avec son **FQDN**,

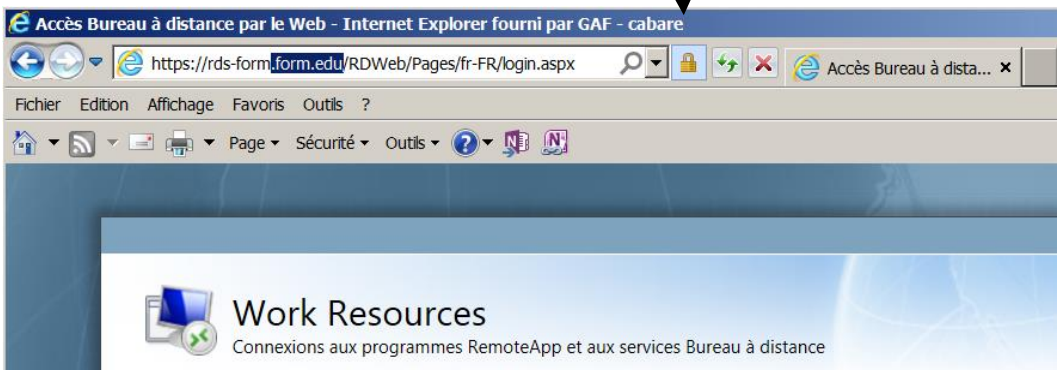
donc Par conséquent il faut désormais accéder au portail depuis une machine du domaine avec l'adresse suivante :

https://rds-form.form.edu/RDWeb



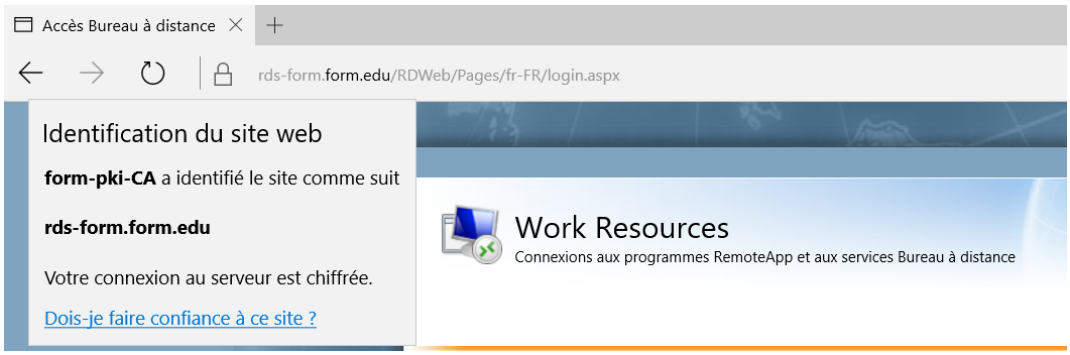


Et on accède au portail sans erreurs…



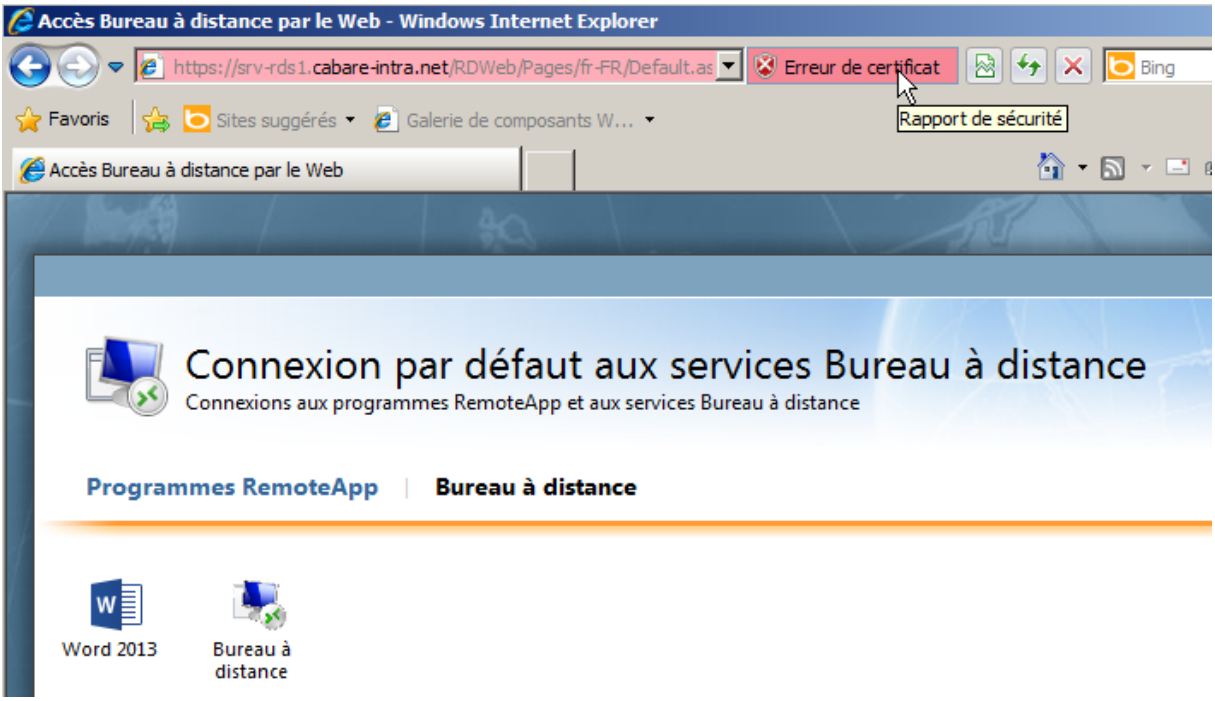
L'effacement du cache du navigateur, et autre effets de bords peuvent rendre ce test un peu... "laborieux"

N.B : Sous **EDGE** on ne peut pas avoir d'informations sur le certificat…

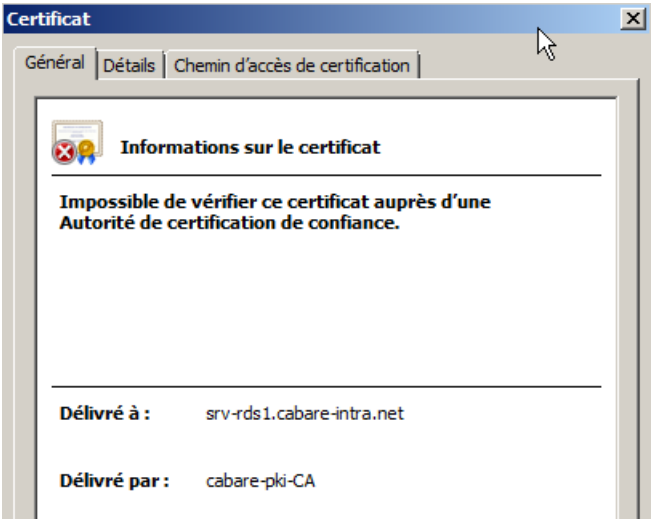


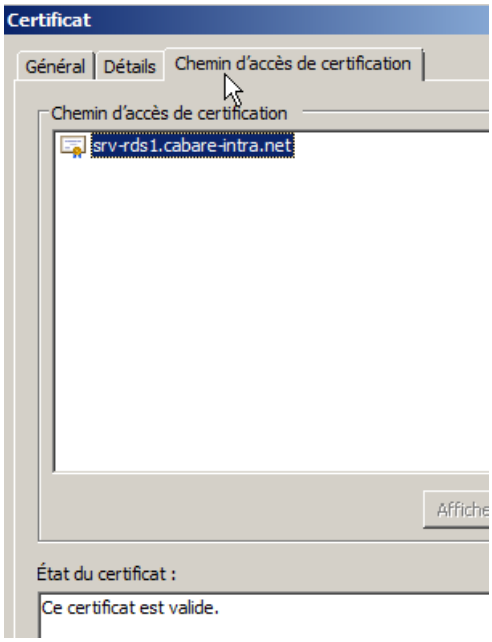
Connexion HTTPS depuis une machine hors domaine:

Si on se trouve sur une machine hors domaine, la portée de notre certificat est non valable. par conséquent on aura une **Erreur de certificat**



Si on demande d'afficher le certificat on voit bien que le Certificat est valide… simplement on ne peut pas y accéder car on ne fait pas partie du domaine





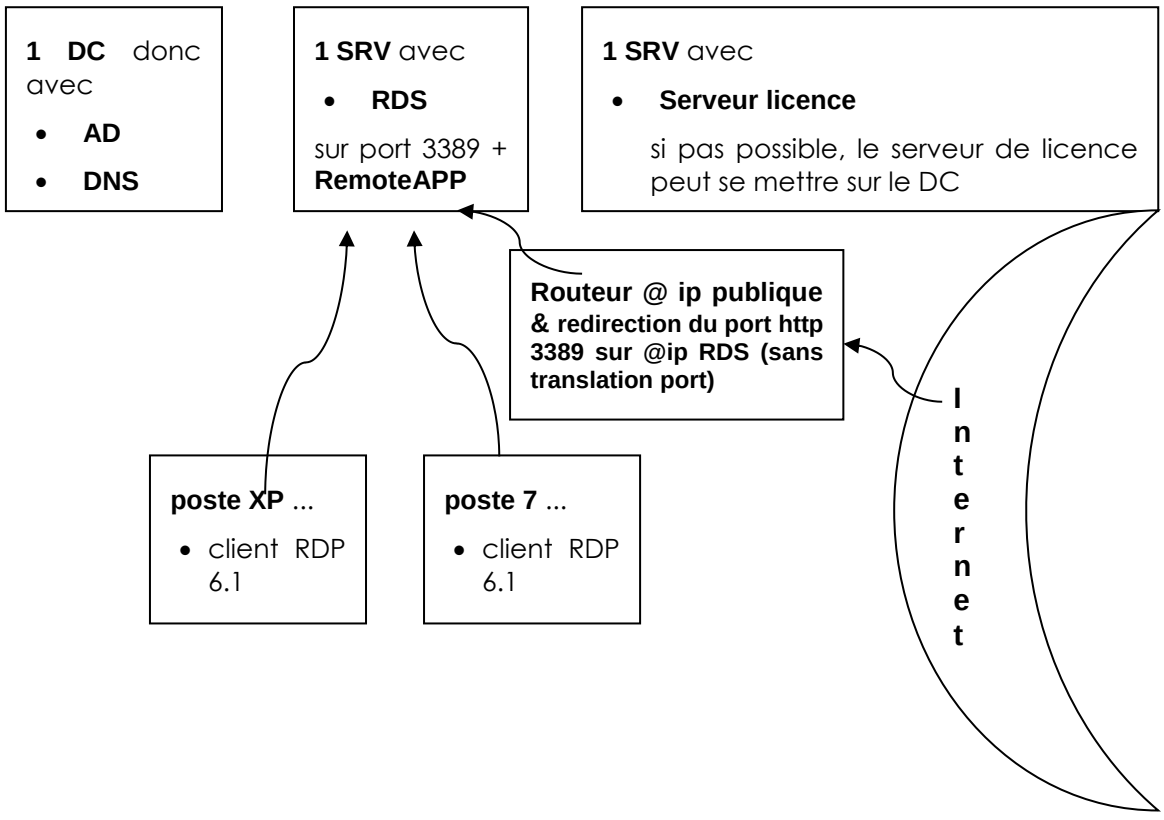
Accès externe RDP sans passerelle port 3389

Ce mode ne fonctionne que pour donner un accès depuis l'extérieur à notre Serveur **RDS**... il rend donc accessible un serveur **RDS** à travers **HTTPS** et non plus à travers son port dédié 3386, donc sans tunnel VPN... "avant" il fallait

1. monter un **VPN**
2. chercher le serveur TSE via une @ip privée en interne (Or on ne peut pas toujours faire un **VPN**, cela peut bloquer par exemple en wifi publique, si les pare-feu n'ouvrent pas les bons ports...)

On pouvait aussi rediriger directement le port **RDP 3389** (ou autre) vers notre serveur **RDS**... mais cela posait 2 soucis

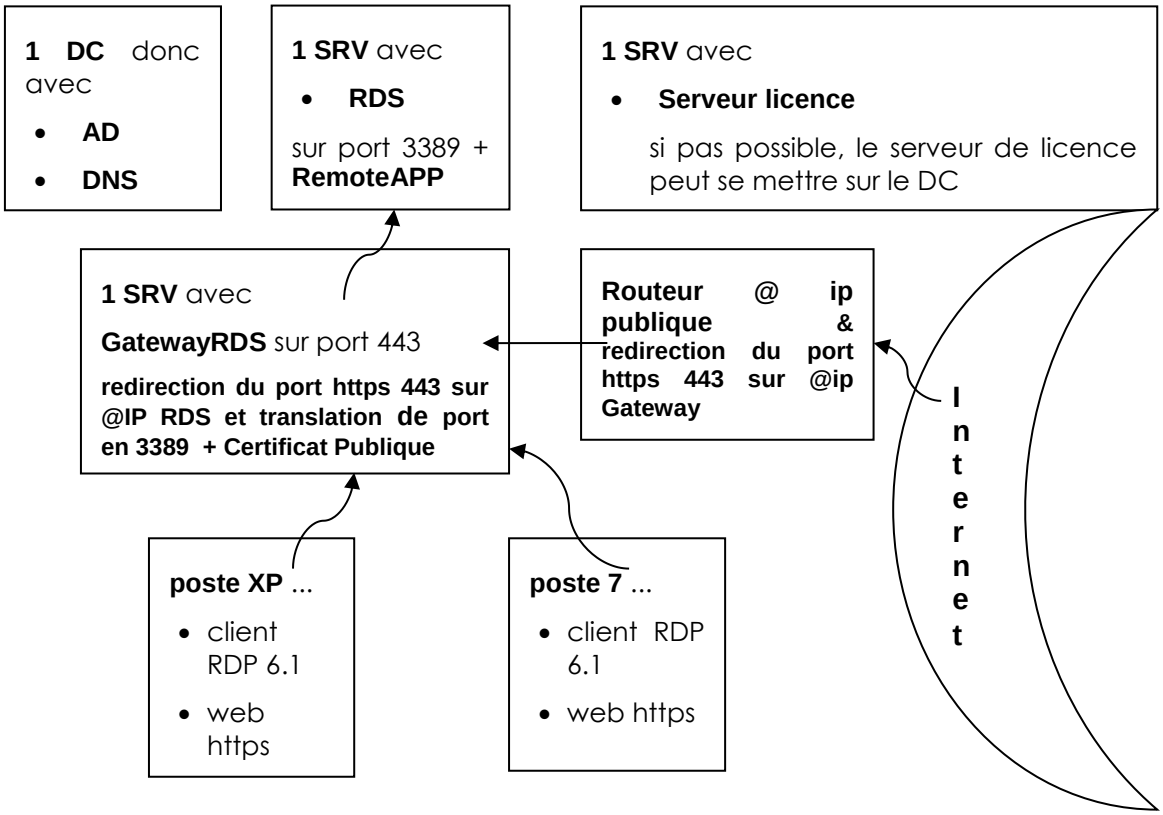
1. notre serveur **RDS** est directement exposé
2. le port **RDP 3389** n'est pas forcément ouvert partout... (Or on ne peut pas toujours faire transiter tous les ports cela peut bloquer par exemple en wifi publique



Accès externe avec passerelle https 443

Avec 2012 on utilisera **https**, cela marchera tout le temps car on fait du RDP encapsulé dans du HTTPS, et le **HTTPS** est un standard en général "ouvert" partout.

l'intérêt encore une fois c'est que l'utilisateur se servira de son **client RDP** normal... ou plutôt de son navigateur standard via https.



les clients "internes" du LAN peuvent accéder aussi par la passerelle...

N.B: comme on va rediriger sur notre **Gateway RDS** tous les accès **https**, , cela voudra dire que si on veut d'autres services **https** il faudra d'autres adresses IP Publiques ! ainsi par exemple

accès RDWeb	1 @ IP publique
accès RDWeb + Webmail OWA/Exchange	2 @ ip publiques
accès RDWeb + site web en https	2 @ ip publiques
accès RDWeb + Webmail + site web en https	3 @ ip publiques

N.B: Certificat et nom de domaine

L'utilisation d'un certificat auto signé ou même de domaine est insuffisant ici. Seul un **certificat public** donc à partir d'une **PKI publique** peut fonctionner avec une passerelle **RDS**. Si ce n'est pas possible il faudra ajouter le certificat manuellement sur la passerelle et tous les clients qui y accèdent ...

Le nom de domaine posé en intra sur la LAN doit être identique à celui du domaine déclaré pour le certificat public. Autrement dit le **nom de domaine** associé à l'adresse IP publique permettant d'arriver sur la passerelle depuis internet doit être le même que le **nom de domaine** LAN de l'Active Directory.

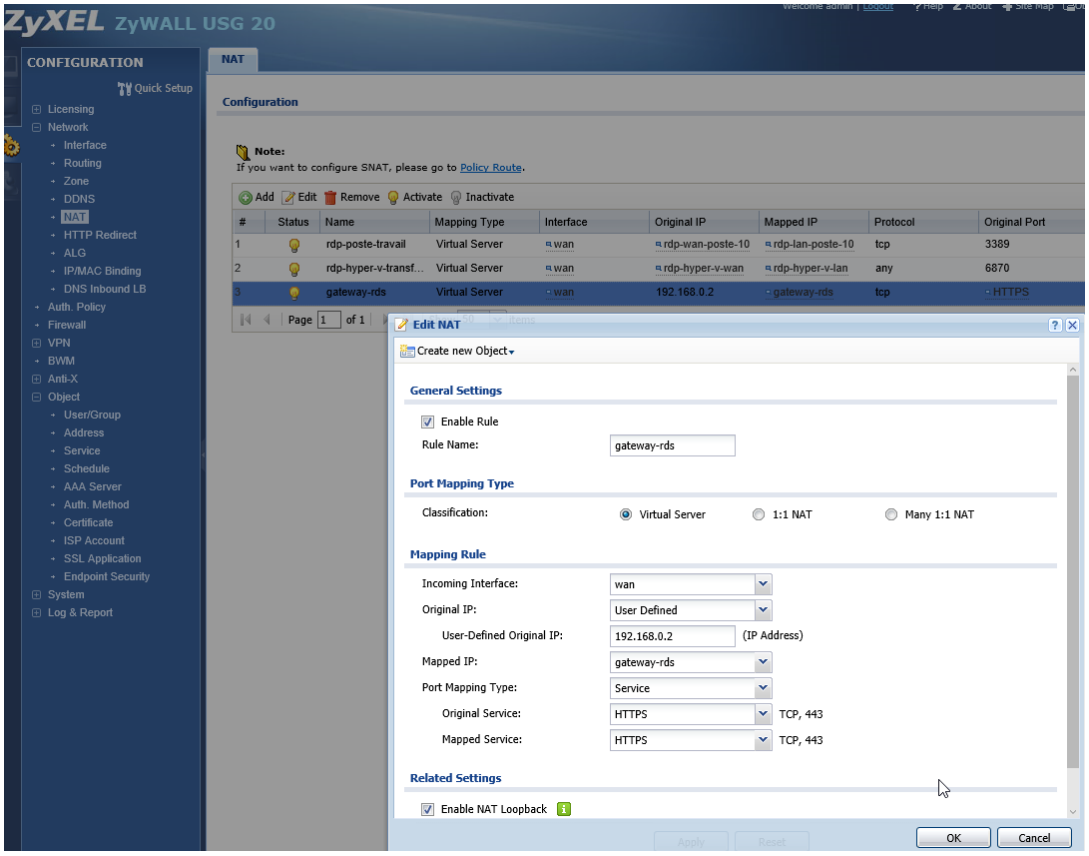
Redirection https et @ip gateway

Le poste hébergeant la fonctionnalité **RDG-Gateway** devrait être une machine dédié, car dessus on installe un IIS, et l'accès Web est redirigé par définition dessus. Cela semble donc dangereux de mettre la Gateway sur un DC.

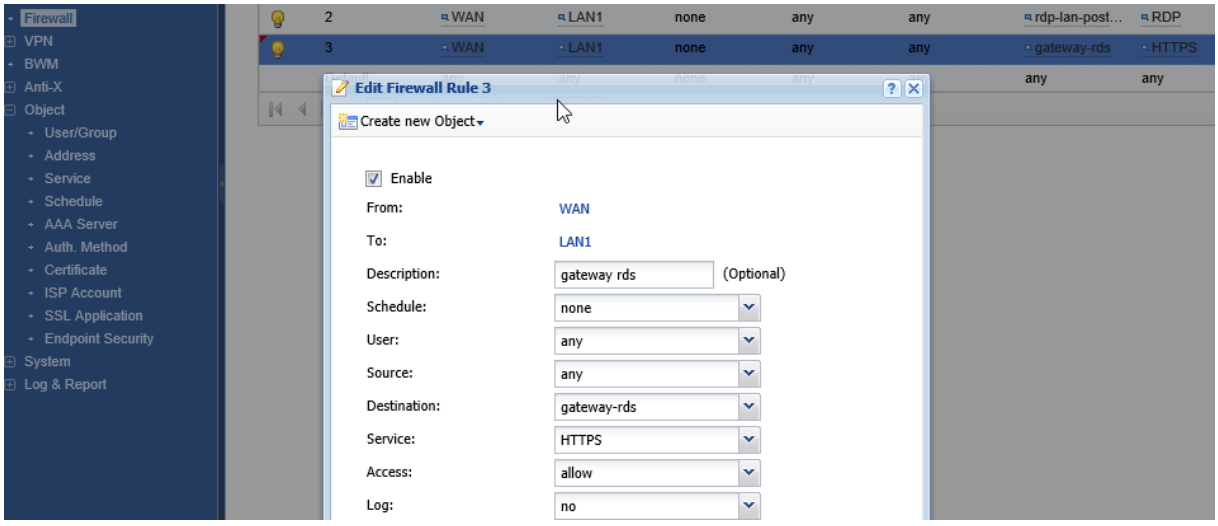
En production à exclure catégoriquement ! (même si c'est possible fonctionnellement pour un test ou une formation).

il faut sur le routeur rediriger les futures arrivées en https sur notre **gateway**

faire une règle de **NAT Network Adress Translation**



En général associée à une règle de Firewall



on pourra vérifier sur des sites comme

que le nom de domaine soit bien connu des DNS

```
traceroute to www.cabare-intra.net (193.251.23.12), 20 hops max, 40 byte packets
 1  208.64.252.229.uscolo.com (208.64.252.229)  0.329 ms  0.356 ms  0.424 ms
 2  208.64.248.17.uscolo.com (208.64.248.17)  0.792 ms  0.853 ms  0.905 ms
 3  69.31.114.17 (69.31.114.17)  0.693 ms  0.681 ms  0.663 ms
```

et que les ports soient bien ouverts et accessibles

Scanning ports on cabare-intra.net

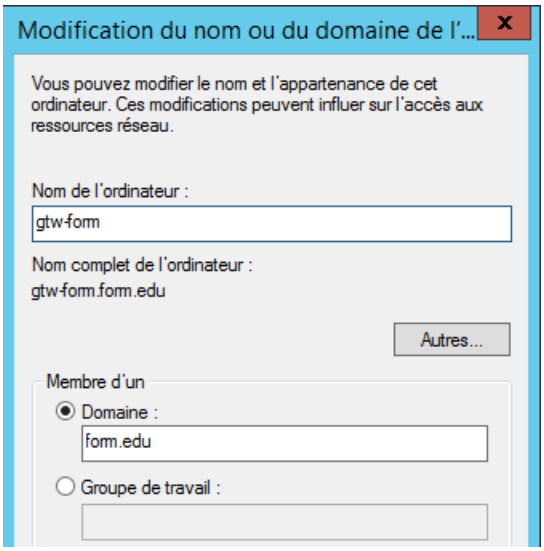
```
cabare-intra.net isn't responding on port 21 (ftp).
cabare-intra.net isn't responding on port 23 (telnet).
cabare-intra.net isn't responding on port 25 (smtp).
cabare-intra.net is responding on port 80 (http).

cabare-intra.net isn't responding on port 139 (netbios-ssn).
cabare-intra.net is responding on port 443 (https).

cabare-intra.net is responding on port 3389 (ms-wbt-server).

cabare-intra.net isn't responding on port 5900 ().
cabare-intra.net isn't responding on port 8080 (webcache).
```

Installation serveur Gateway

On l'a déjà dit, on peut en cas de "pénurie " de serveurs, installer la **Passerelle RDS** sur le serveur **Brooker**, (de la même manière que l'on peut installer un **serveur de licence** sur un **DC**)

Mais le mieux étant d'avoir une passerelle dédiée, on crée donc un poste spécifique nommé par exemple ***gtw-form*** avec un Windows 2012R2

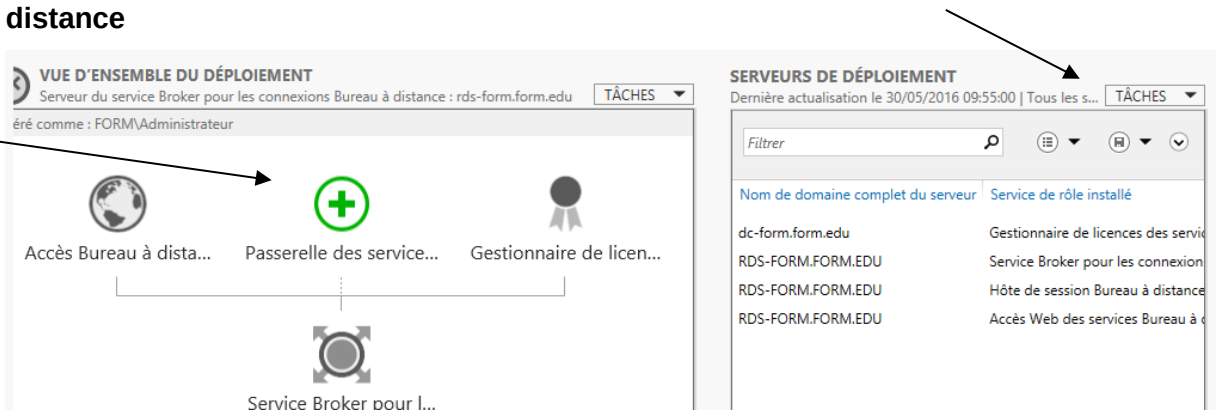
et on l'intègre au domaine...



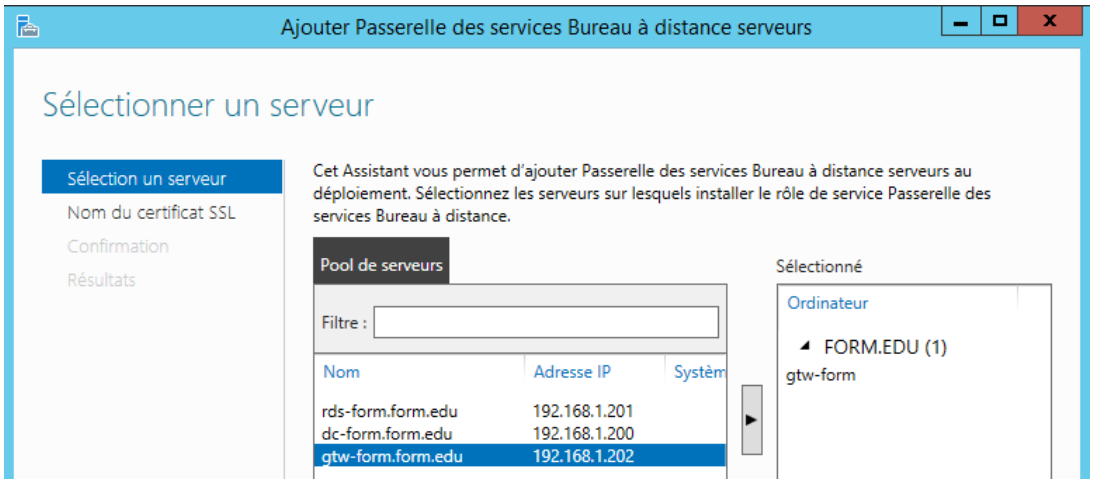
On se place sur le **gestionnaire de Serveur** du serveur sur lequel on a accès à la vision d'ensemble de notre déploiement RDS, (cela peut être notre serveur rds-form) puis

soit via **Passerelle des Services** (qui apparait comme non configurée)

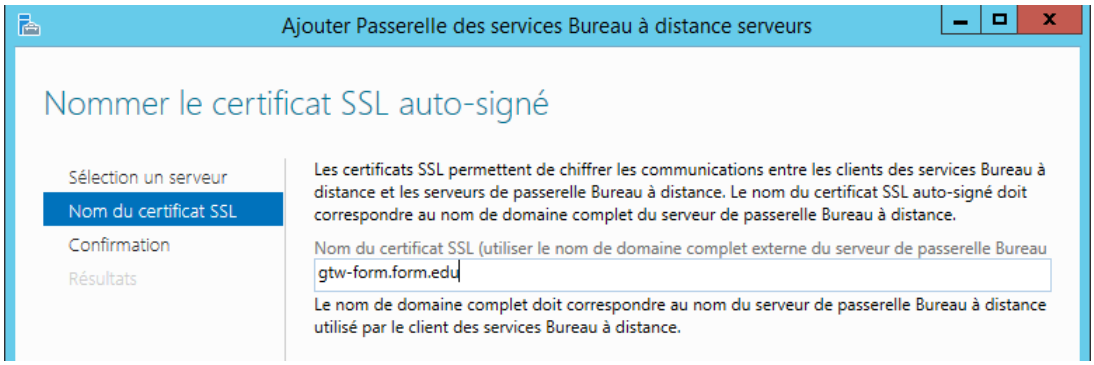
soit via les **Tâches** des **Serveurs de déploiement**, dans lesquelles on demandera alors **Ajouter des serveurs de passerelle des services Bureau à distance**



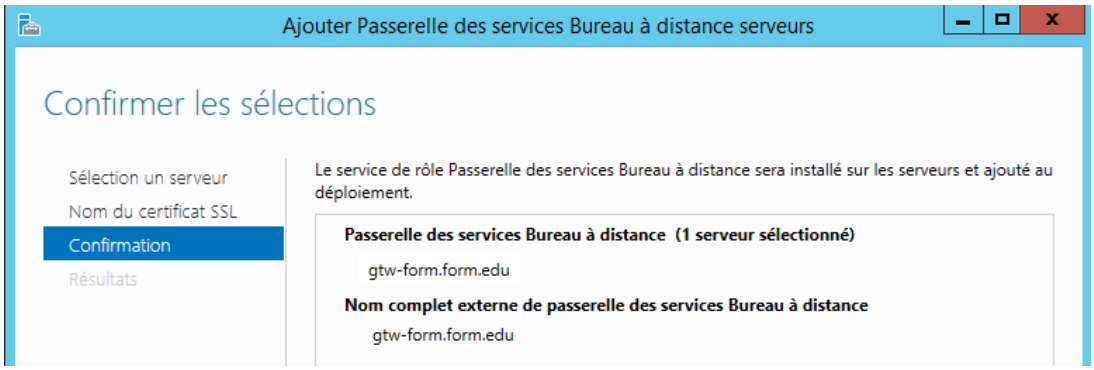
on ajoute notre serveur ***gtw-form***



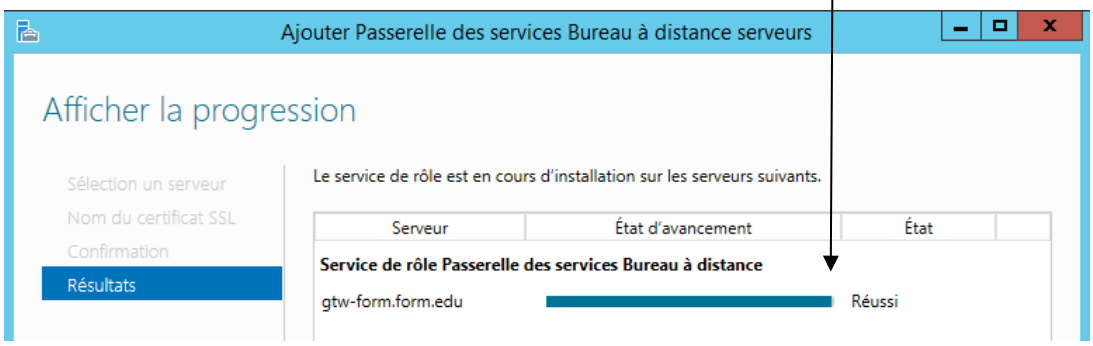
Un **certificat** auto signé est obligatoire, il doit porter le nom de la machine qui héberge les services Passerelle (et s'il s'agit, d'une ferme, le nom de la ferme), dans l'exemple ***gtw-from.form.edu***



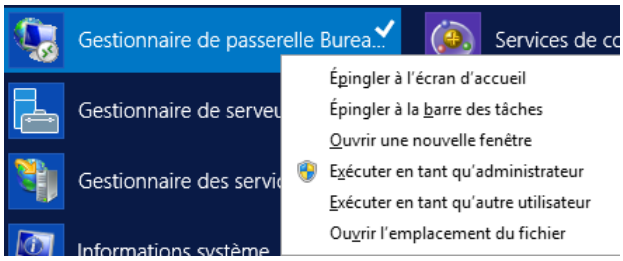
On confirme en demandant **Ajouter**



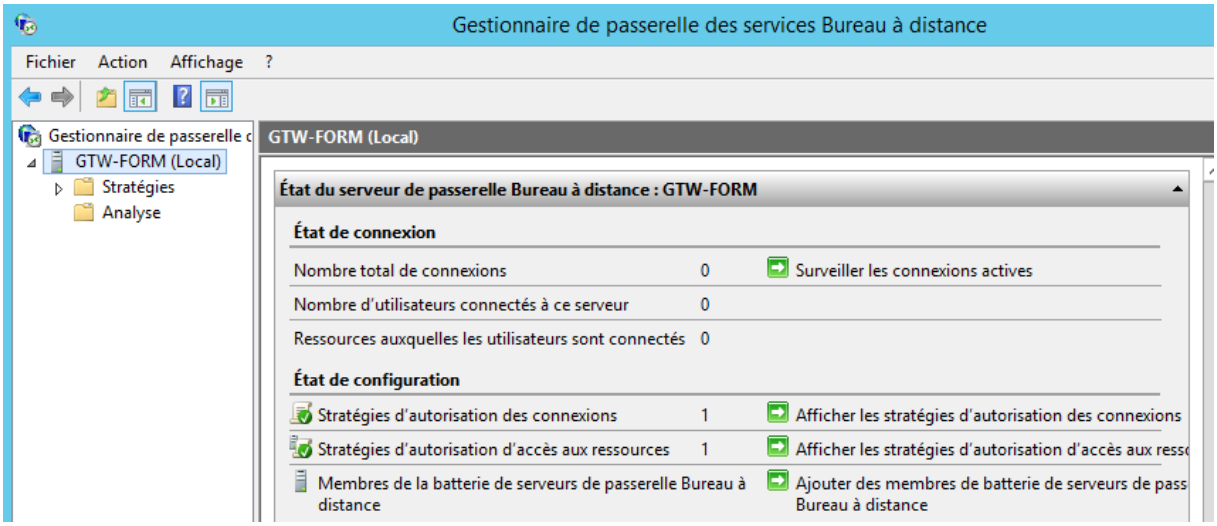
Et c'est terminé



Une nouvelle console d'administration doit apparaître sur notre serveur de passerelle ***gtw-form*** ,



accessible via **Gestionnaire de la Passerelle des Service Bureau à distance** donnant



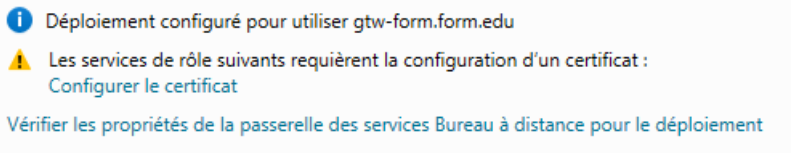
Cette installation aura pour effet d'installer sur notre poste ***gtw-form***

- un **serveur IIS**,
- un **Proxy RPC** qui convertira le flux **https/443** en **RDP/3389**
- un **NPS Network Policy Server** : qui permettra de définir des stratégies d'accès, c'est à dire permettra de spécifier qui peut "passer"...
  Le **NPS** transmettra ensuite au **NAP NAP Network Acces protocol** le résultat de sa décision. La **Gateway RDS** va donc permettre des filtrages à l'aide de **NPS**, il va falloir donc lister les Serveurs **RDS** à utiliser (on peut en effet décider de ne pas offrir sur le web tous les serveurs RDS dont on dispose...). Cela se fera sur la Gateway par la configuration de 2 GPO :
  - une **GPO RDS** dite **CAP Connexion Access policy** permettant de définir qui peut se connecter à la passerelle RDS (et cet accès est indépendant de qui peut accéder aux services des Bureaux à distance)
  - une **GPO RDS** dite **RAP Remote Access policy** permettant de définir quels sont les ordinateurs internes au LAN auxquels l'utilisateur peut avoir accès "via" la passerelle... (et ceci est indépendant de qui peut accéder à la passerelle)

N.B : il ne pas installer la passerelle via **Ajout de rôle**, sinon les deux stratégies précédentes ne seront pas créées par défaut.

Il reste donc fondamentalement

- A paramétrer les **2 GPO** d'accès **CAP** et **RAP**
- A gérer les **certificats**



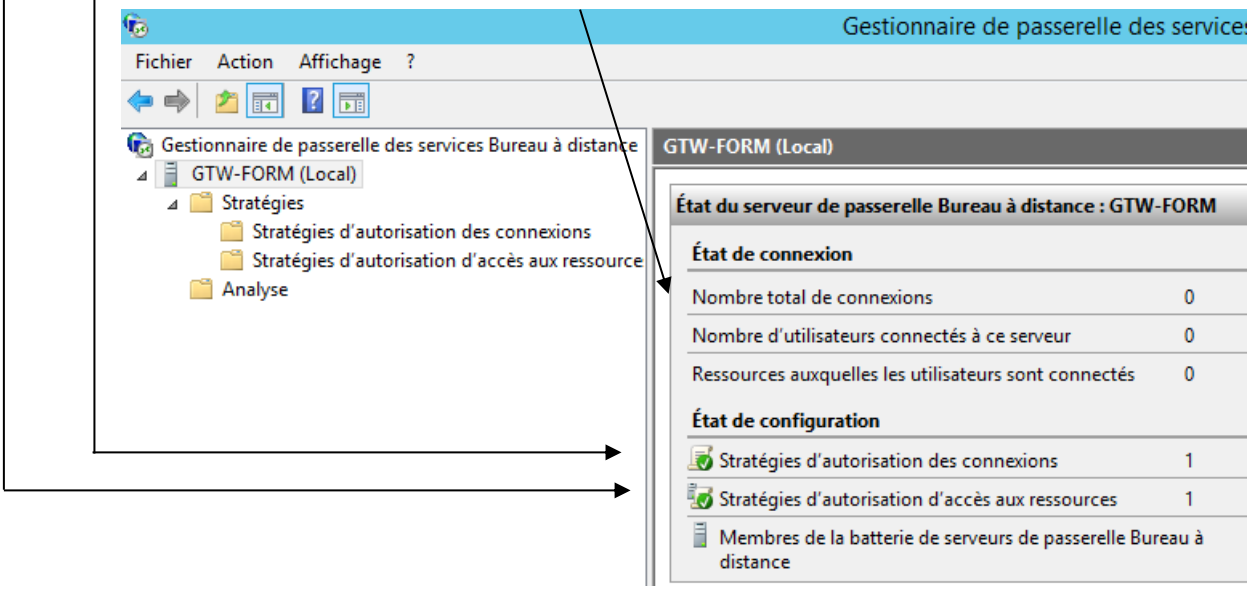
Gestionnaire de passerelle configuration post déploiement

Cette console affiche de manière synthétique,

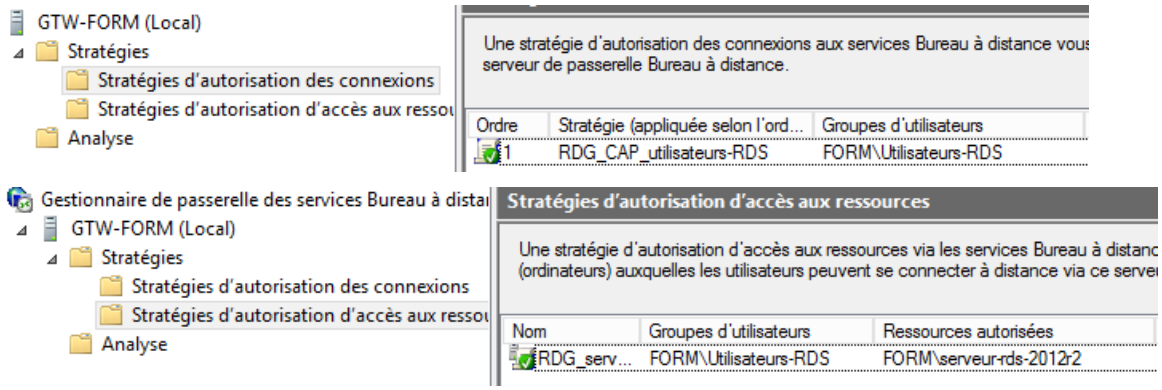
la **GPO** dite **RAP Remote Access policy** pour les serveurs RDS accessibles

La **GPO** dite **CAP Connexion Access policy** pour les accès utilisateurs

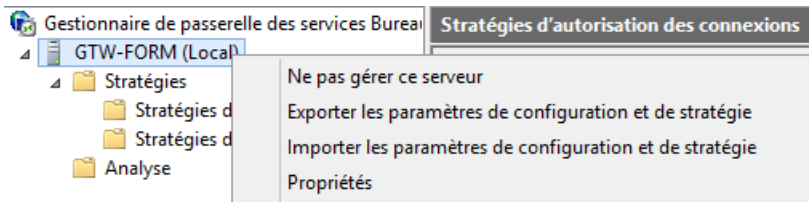
Ainsi que le nombre de flux passant par la passerelle



Lorsque l'on se place sur un nœud, on accède aux stratégies prédéfinies,



soit **aux propriétés** du serveur passerelle

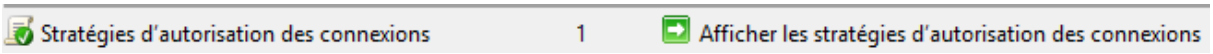


donnant

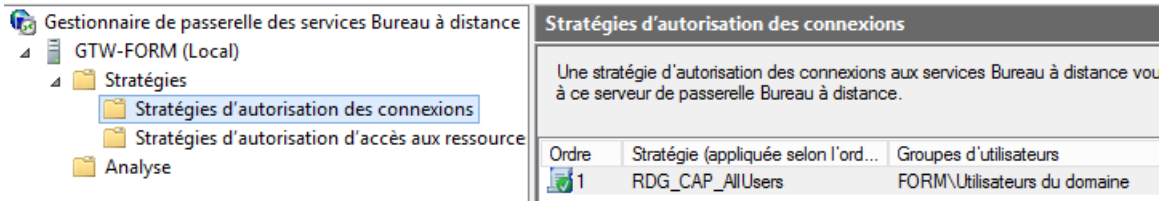
1 Paramétrage de la GPO CAP (utilisateurs)

Pour la 1° stratégie **CAP Connexion Access policy** permettant de définir qui peut se connecter à la **passerelle RDS** (cet accès est indépendant de qui peut accéder aux **services des Bureaux à distance**) il y a 2 points à traiter

- Qui (utilisateurs ou groupes)
- Comment on s'authentifie (mot de passe / carte à puce)



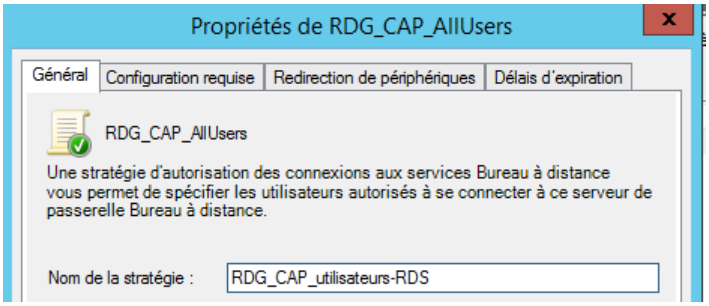
ou



Par défaut tous les utilisateurs peuvent utiliser l'accès distant sur notre Gateway…

on va faire en sorte que seul le groupe des ***Utilisateurs RDS*** puissent y accéder

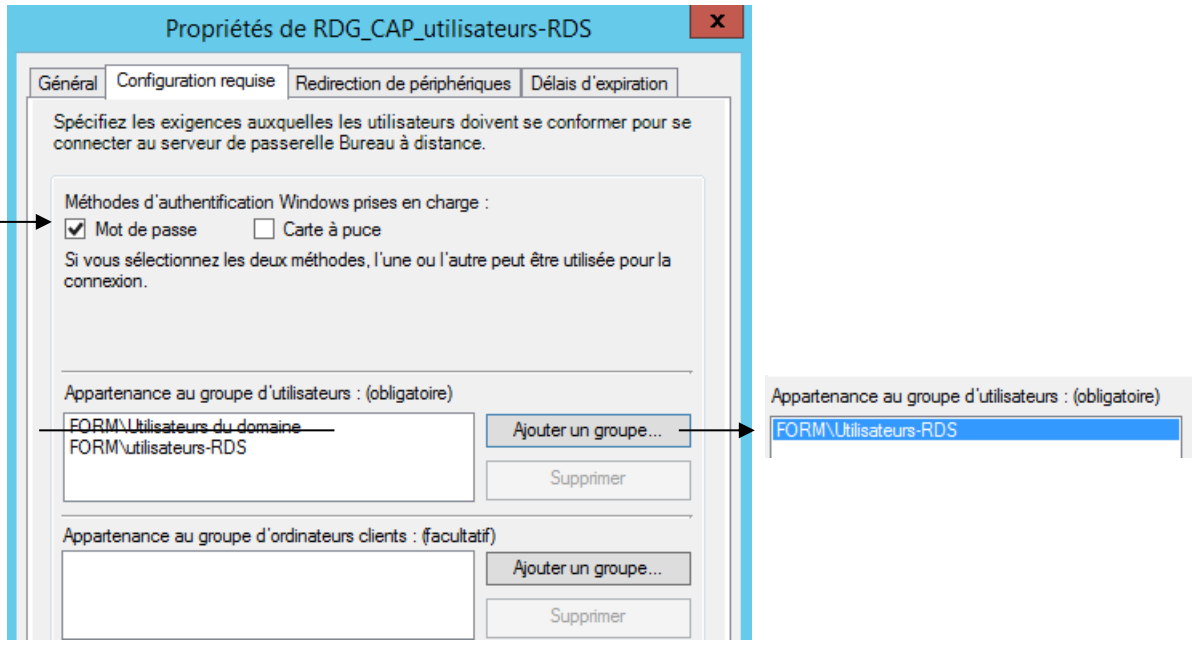
N.B: si on veut autoriser les Admins à utiliser les services de passerelle il faut ajouter le groupe Admin de domaine ici



On peut renommer cette GPO… pour que cela soit plus parlant

Mais surtout il faut indiquer que l'on s'authentifie par **mot de passe**,

Donc au final seul notre groupe d'utilisateurs à distance, plutôt que tous les utilisateurs du domaine, devrait accéder a notre passerelle avec une authentification par mot de passe

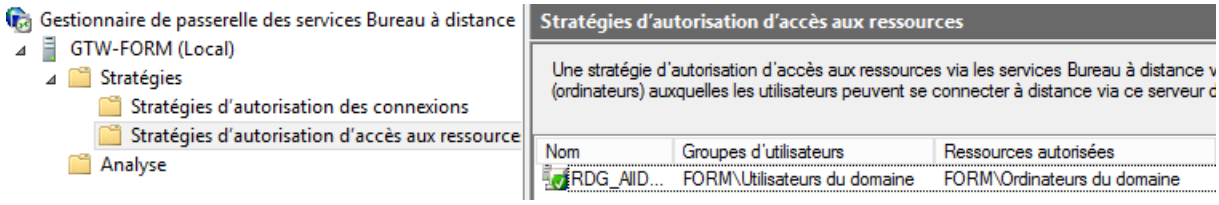


2 Paramétrage de la GPO RAP (machines ressources)

Pour la 2° stratégie **RAP Remote Access policy** permettant de définir quels sont les ordinateurs internes au LAN auxquels l'utilisateur peut avoir accès "via" la passerelle... (Indépendamment de qui peut accéder à la passerelle) il y a 1 point à traiter

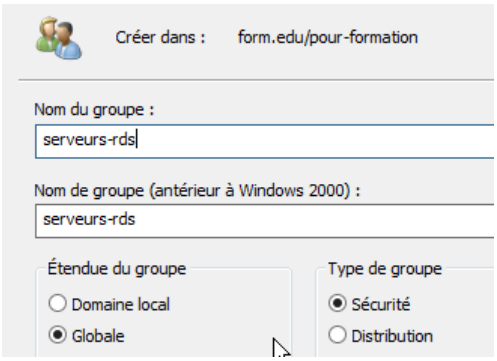
- vers quels serveurs RDS (groupe de machines accessibles)

Ou

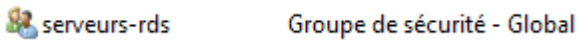


par défaut tous les utilisateurs peuvent utiliser toutes les machines

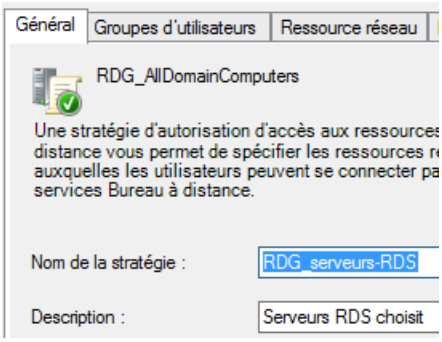
On va faire en sorte que seul le groupe des Utilisateurs RDS puissent utiliser le groupe des serveurs RDS et on peut éventuellement la renommer



N.B : Dans notre **AD** il est bon de se créer un **groupe global de domaine** d'ordinateur correspondant aux serveurs RDS (présents, ou à venir...) par exemple ***serveurs-rds***

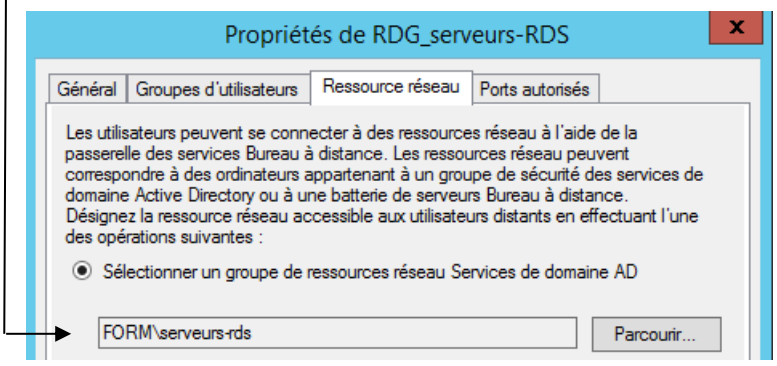


On peut renommer cette GPO... pour que cela soit plus parlant



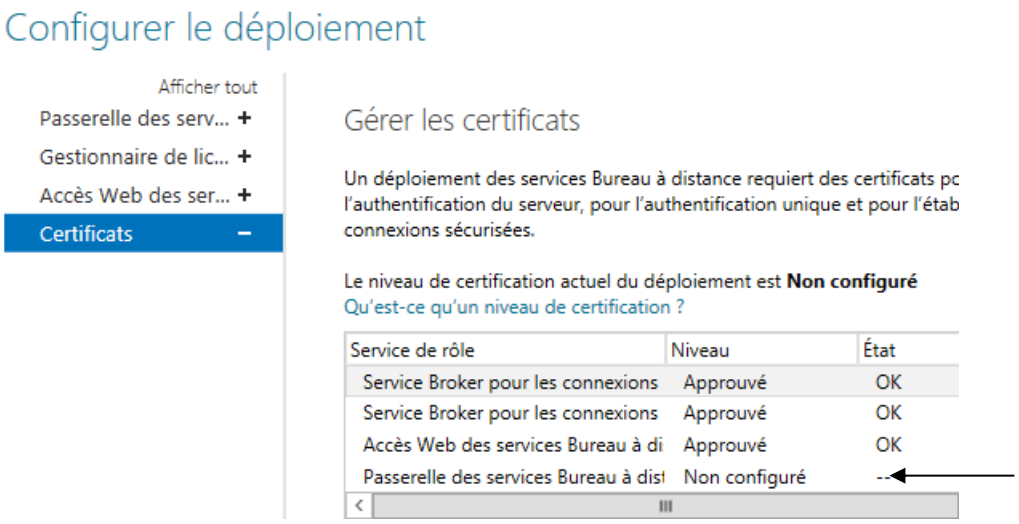
Puis préciser que seuls les ***utilisateurs-RDS*** (et les admins de domaine si on le souhaite)

peuvent utiliser les ***serveurs-RDS***



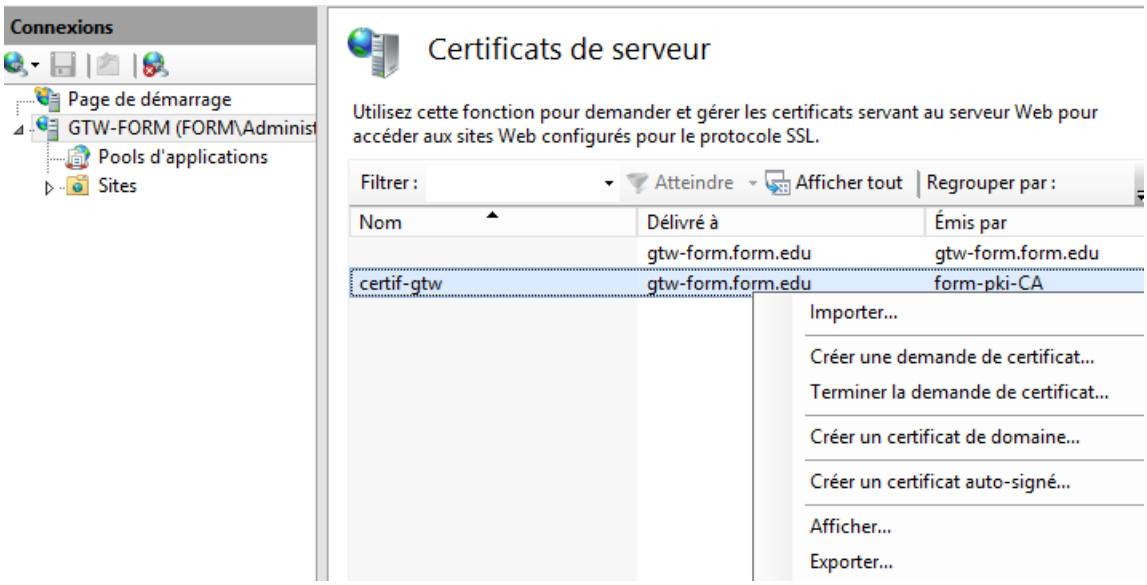
3 Gestion de Certificat

Dans la vue d'ensemble de notre déploiement, on peut demander via les tâches de Configurer le déploiement, et visualiser l'état des certificats



N.B: on fera faire ultérieurement une **PKI externe publique**, puis on l'importera le certificat et on l'ajoutera à notre serveur **Gateway RDS**...

On rejoue la même séquence que pour le certificat crée sur notre serveur **RDSH** à savoir depuis la console **gestionnaire IIS** on demande de **créer un certificat de domaine**, au nom simple de ***certif-gtw*** par exemple, puis on demandera de l'**Exporter**



En le plaçant à un endroit accessible,

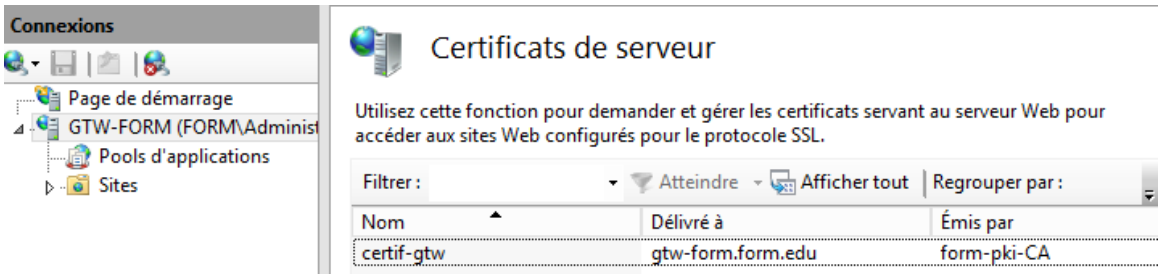
par exemple un emplacement

\\nas-1\commun\xxxx.**pfx**

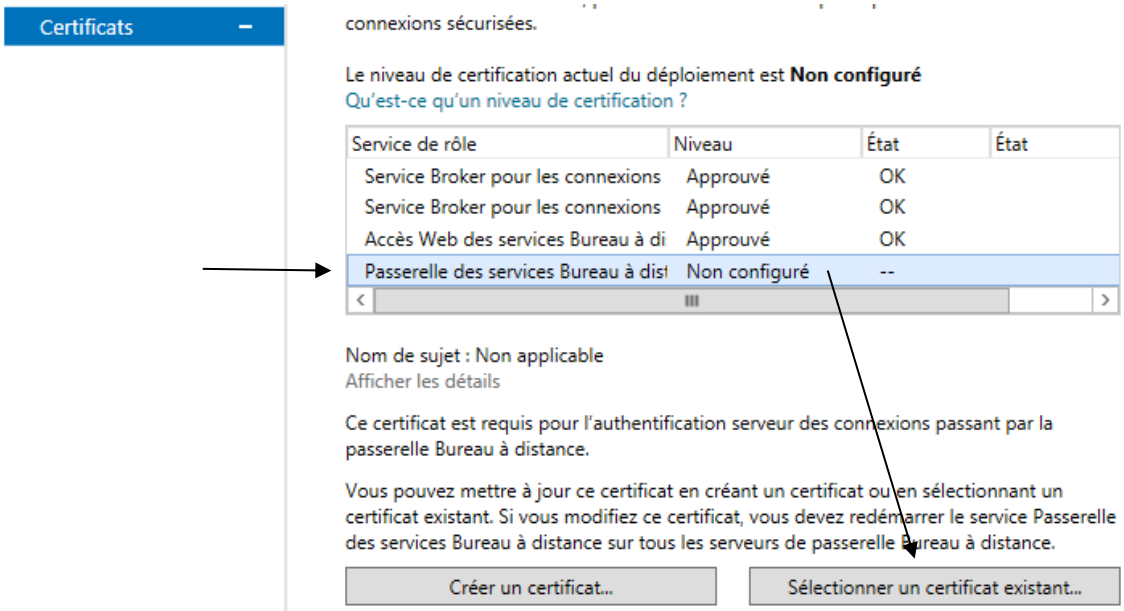
Et 1 mot de passe identique pour tous les certificats, du genre

certifxxxx

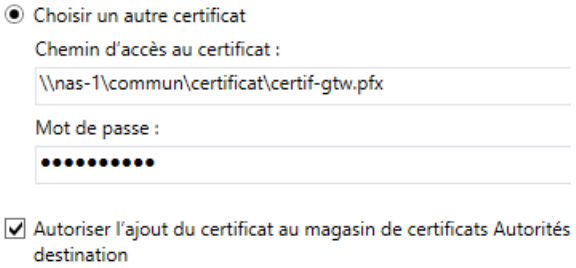
Pour faire propre, on fait le ménage, en supprimant le **certificat auto-signé** et en le remplaçant par le **certificat de domaine**



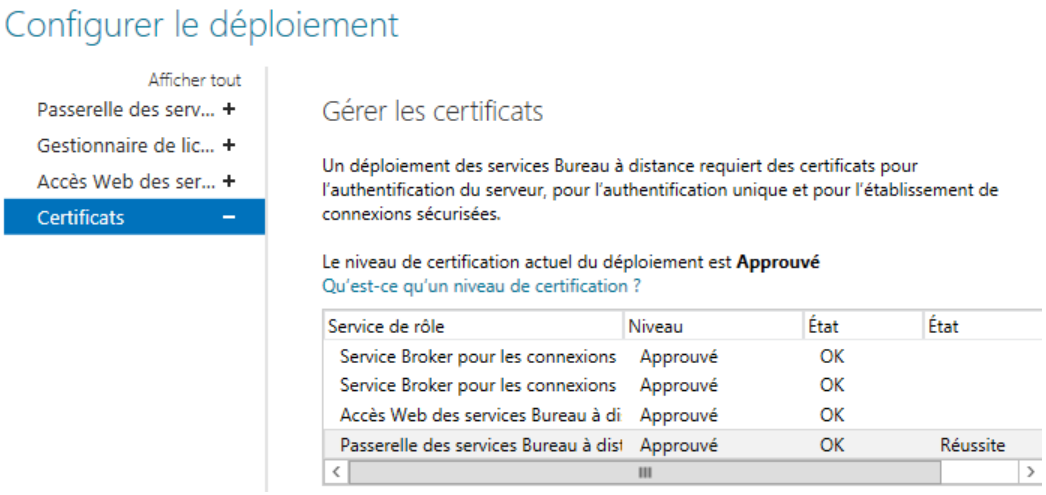
On va pouvoir ensuite renseigner dans notre configuration RDS que la Gateway dispose désormais d'un certificat de domaine



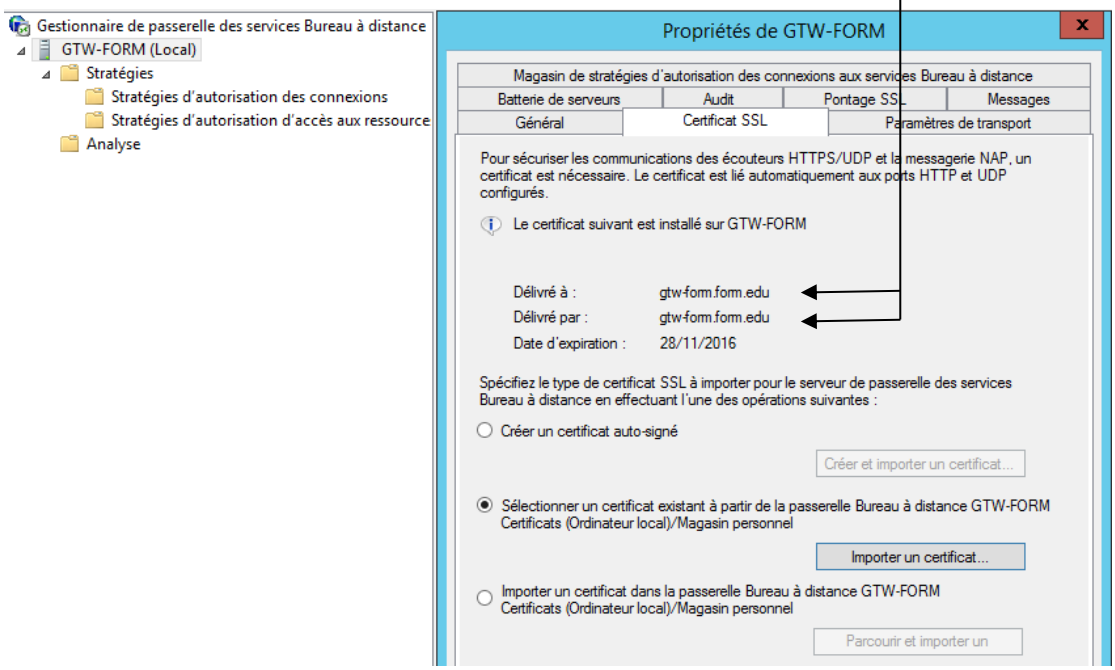
On demande **de sélectionner un certificat existant** et



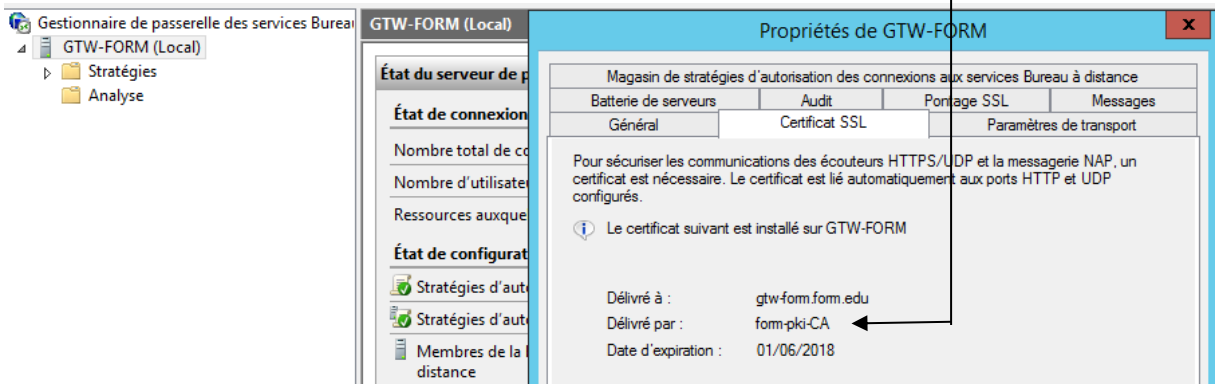
Et on obtient



Par défaut on disposait d'un **certificat auto signé**

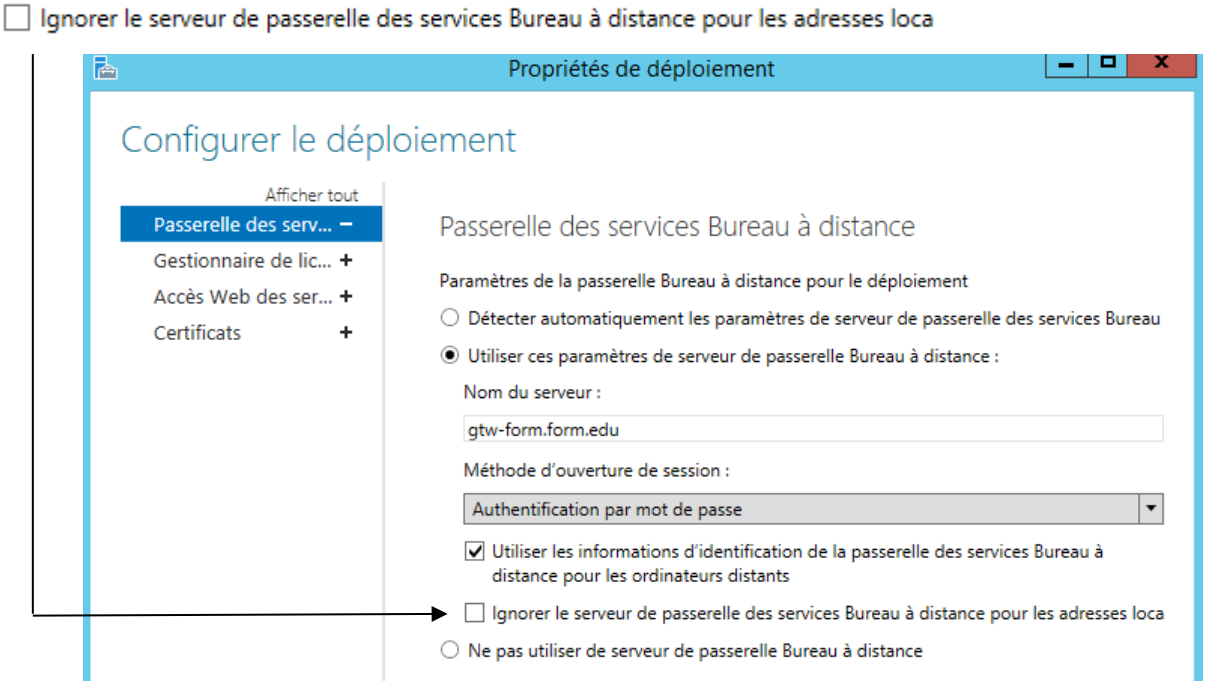


Maintenant on a un **certificat de domaine**



Paramétrage client RDP / Options déploiement

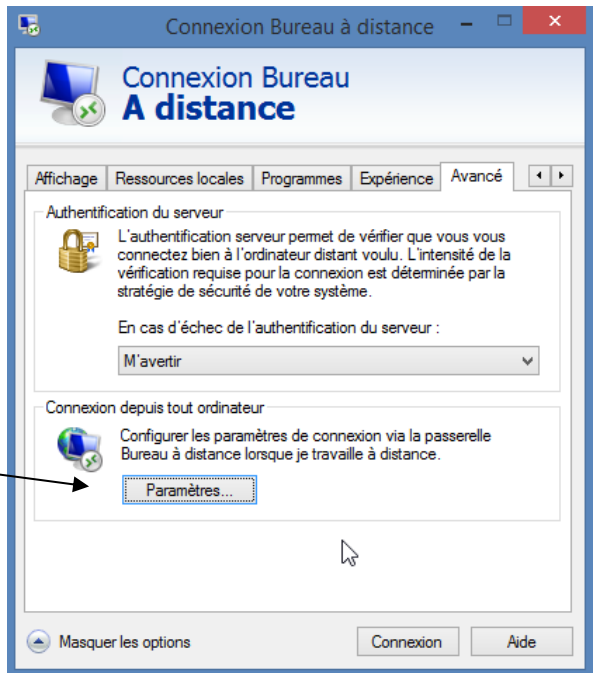
Si on veut tester la connexion aux services via la passerelle en interne, il faut déjà dans les **Propriétés de déploiement** demander de ne pas ignorer le service de passerelle, il faut donc décocher la case **Ignorer le serveur de passerelle Bureau à distance pour les adresses locales** (coché par défaut)



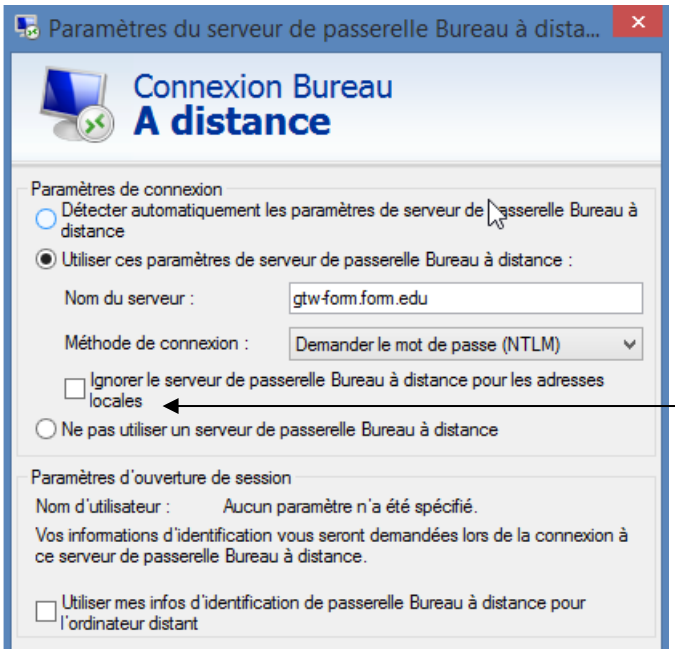
Puis il faut effectuer un paramétrage du client **RDP**

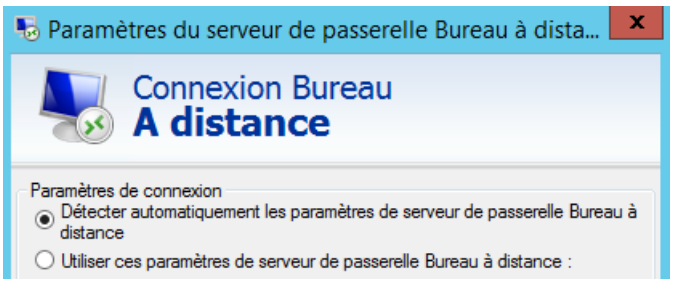
Donc depuis le client RDP dans **Afficher les Options**

Puis onglet **Avancé / connexion depuis tout ordinateur / Paramètres**



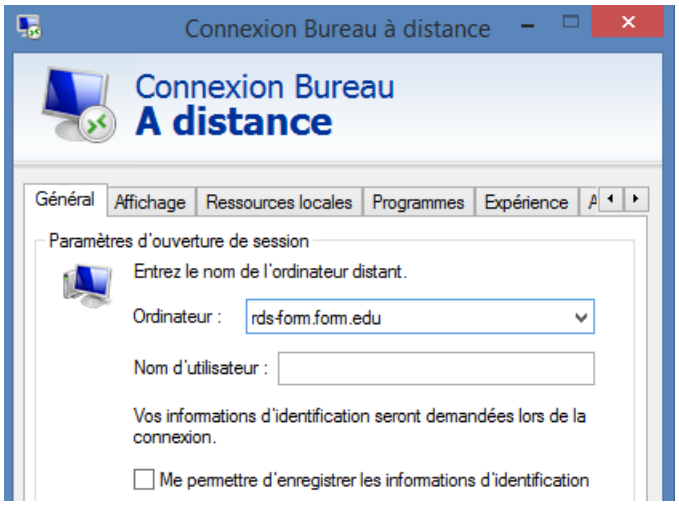
il faut demander depuis le LAN alors que via WAN, c'est automatique





et il ne faut pas cocher **Ignorer le serveur de passerelle Bureau à distance pour les adresses locales**

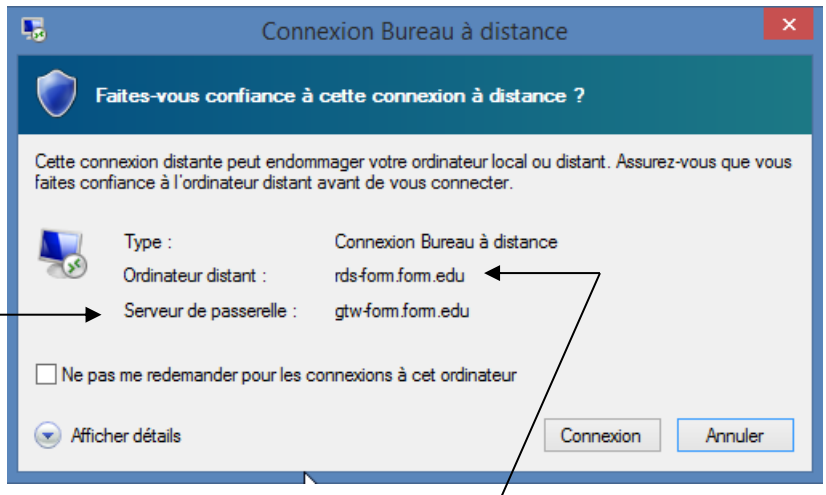
Puis onglet **Général / Paramètres d'ouverture de session**



N.B:il faut indiquer ici un serveur RDS (et non pas la Gateway, qui n'est qu'un intermédiaire) C'est pour cela que on l'a paramétrée en arrière plan !

Si on indiquait la Gateway, si tant est que l'on puisse y avoir 1 accès ouvert, on s'y arrêterait !

et donc on voit bien que l'on demande un login pour 2 connexions



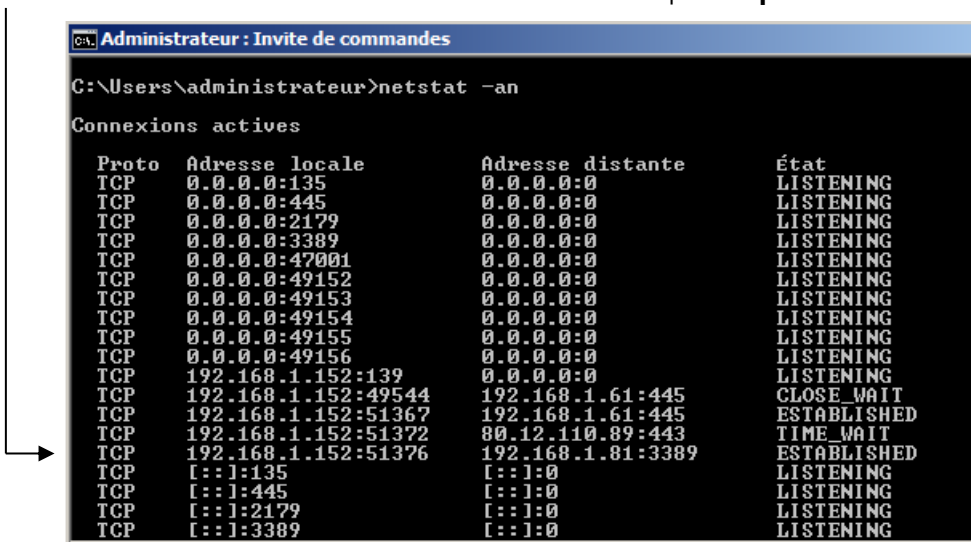
1) la passerelle

2) le serveur RDS que l'on atteindra

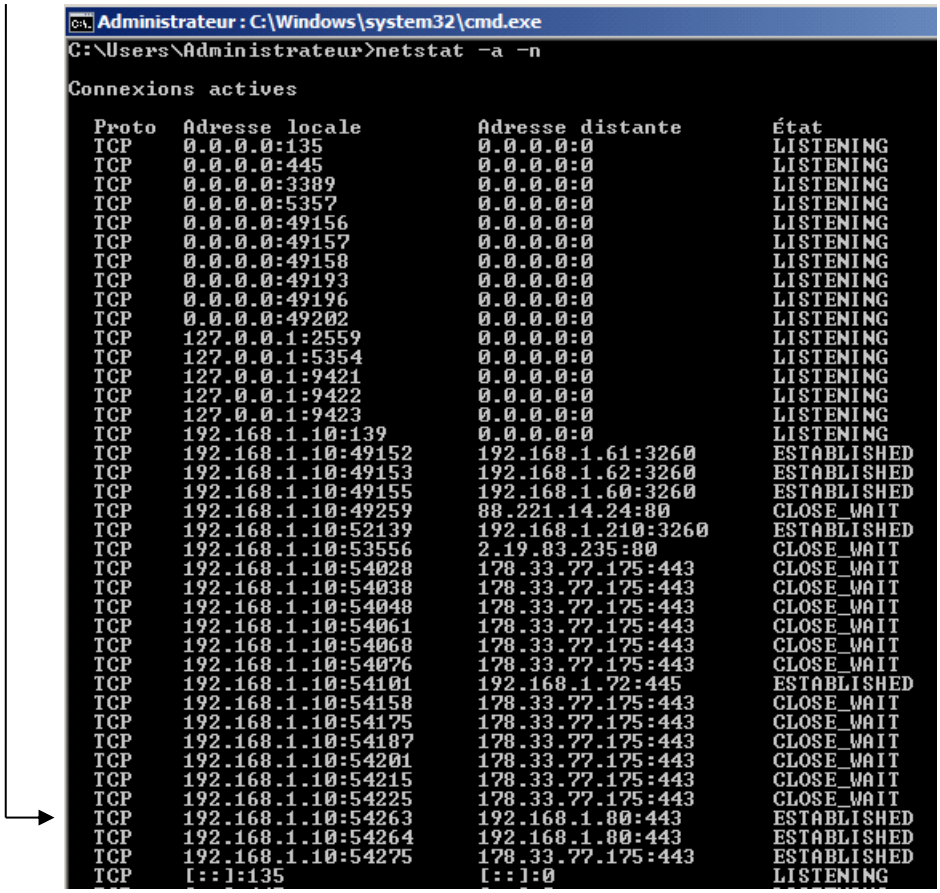
On peut depuis le client connecté savoir si on passe par le **port RDP 3389** ou plutôt sur le **port HTTPS 443** translaté en **NAT** pour atteindre le serveur :

N.B: il faut effectuer ces test depuis la machine cliente sur laquelle on a lancé le client RDP, et non pas dans la connexion RDP ouverte (qui se trouve donc sur le serveur RDS...)

ici on atteint le **serveur RDS** situé en 192.168.1.81 par le **port 3389**

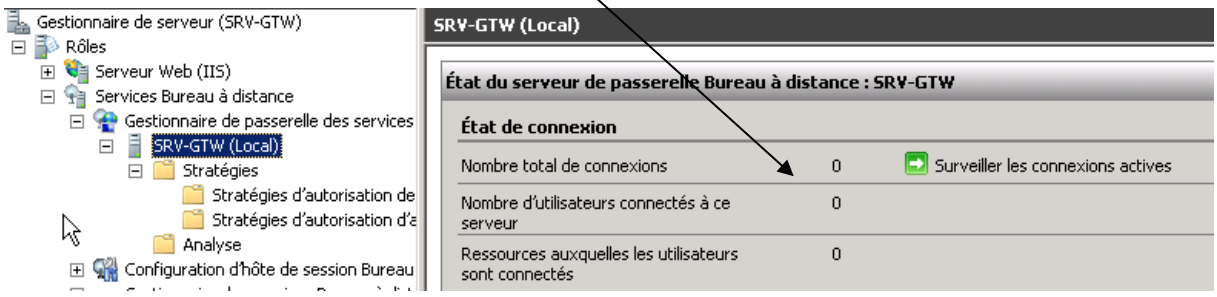


ici on atteint le **serveur RDS** situé en 192.168.1.81 via la **Gateway** située en 192.168.1.80 par le **port 443,** nulle par le **port 3389 n'**est utilisé ! (et encore moins une connexion sur l'adresse IP du serveur RDS 192.168.1.81...

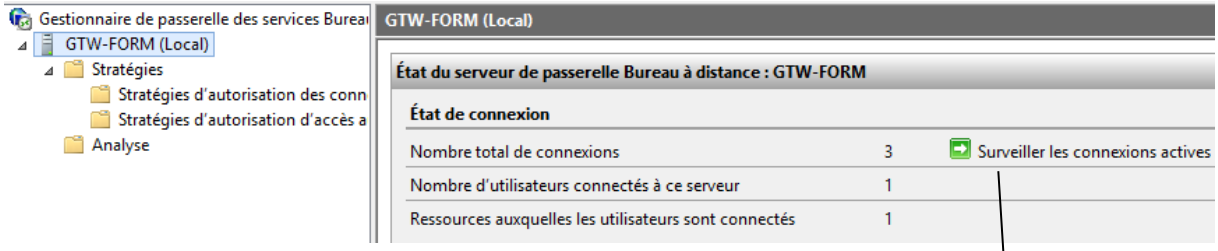


Test connexion depuis passerelle

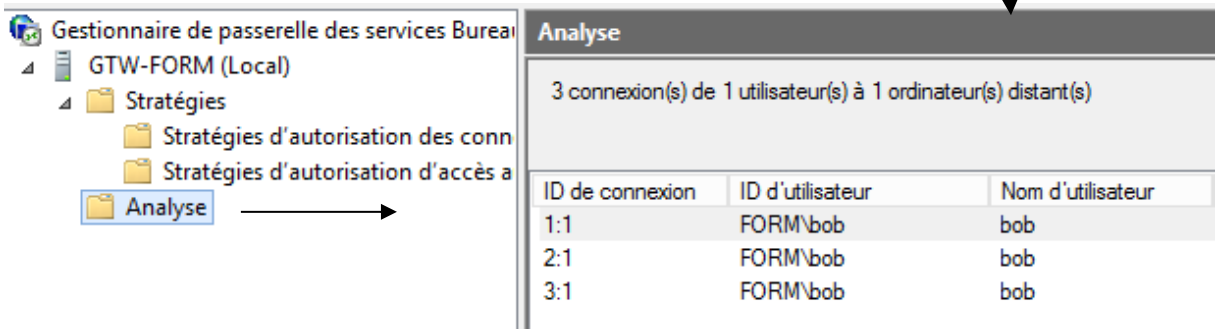
On peut du côté de la passerelle RDS vérifier si le flux passe bien par la passerelle en surveillant l'**Etat de connexion**



lorsqu'un utilisateur se connecte, via la passerelle on note



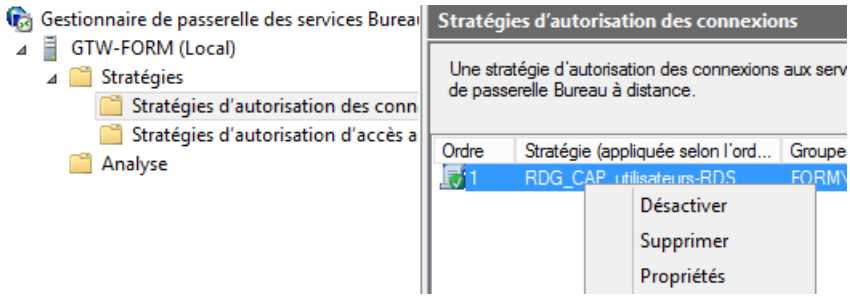
et on aura le détail via **Analyse ou Surveiller les connexions Actives**

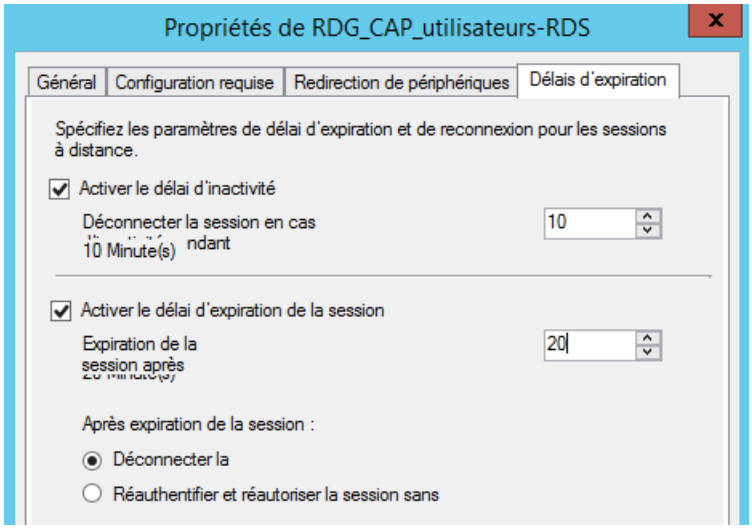


PARAMETRES PASSERELLE GPO COLLECTION

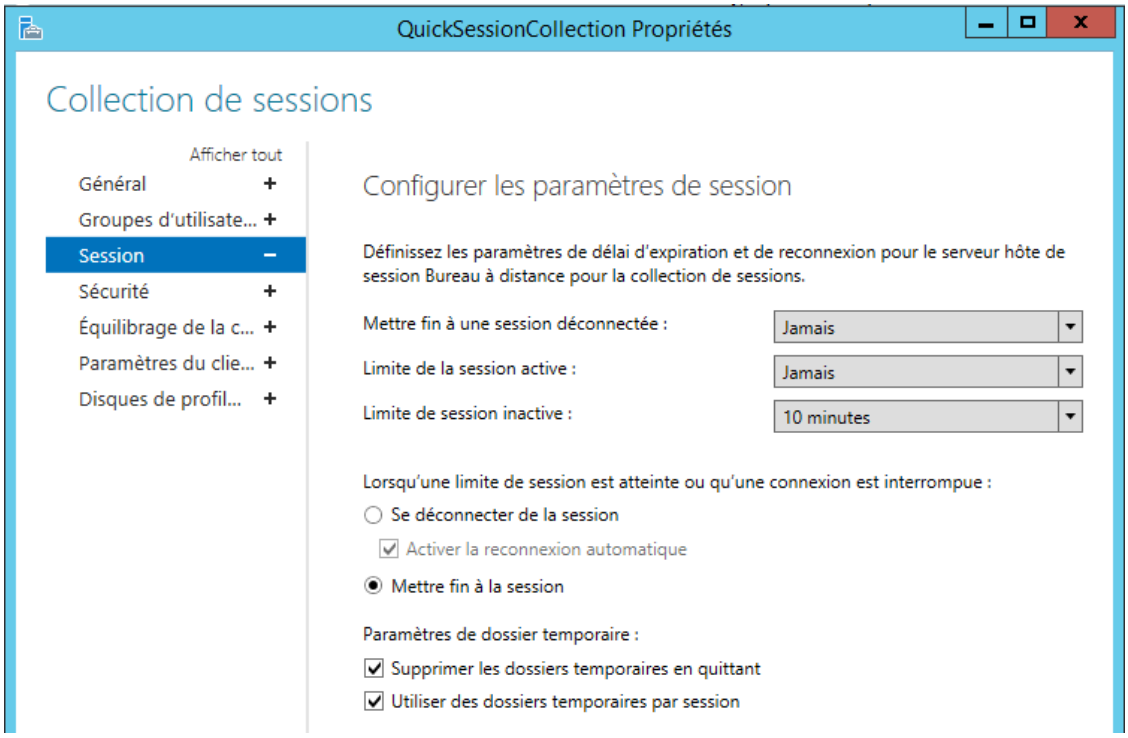
GPO CAO Délais deconnexion

sur notre GPO CAP on demande les propriétés



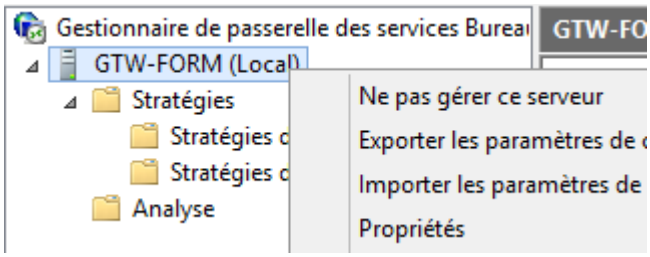


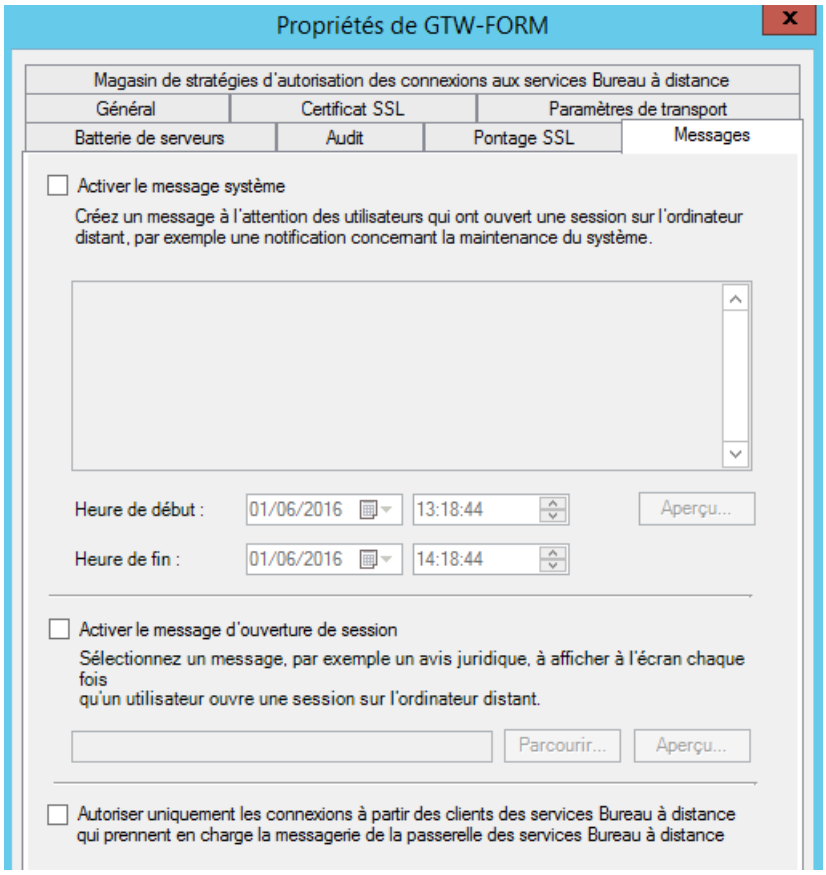
collection session



Paramètres passerelle

sur notre passerelle on demande les **propriétés**

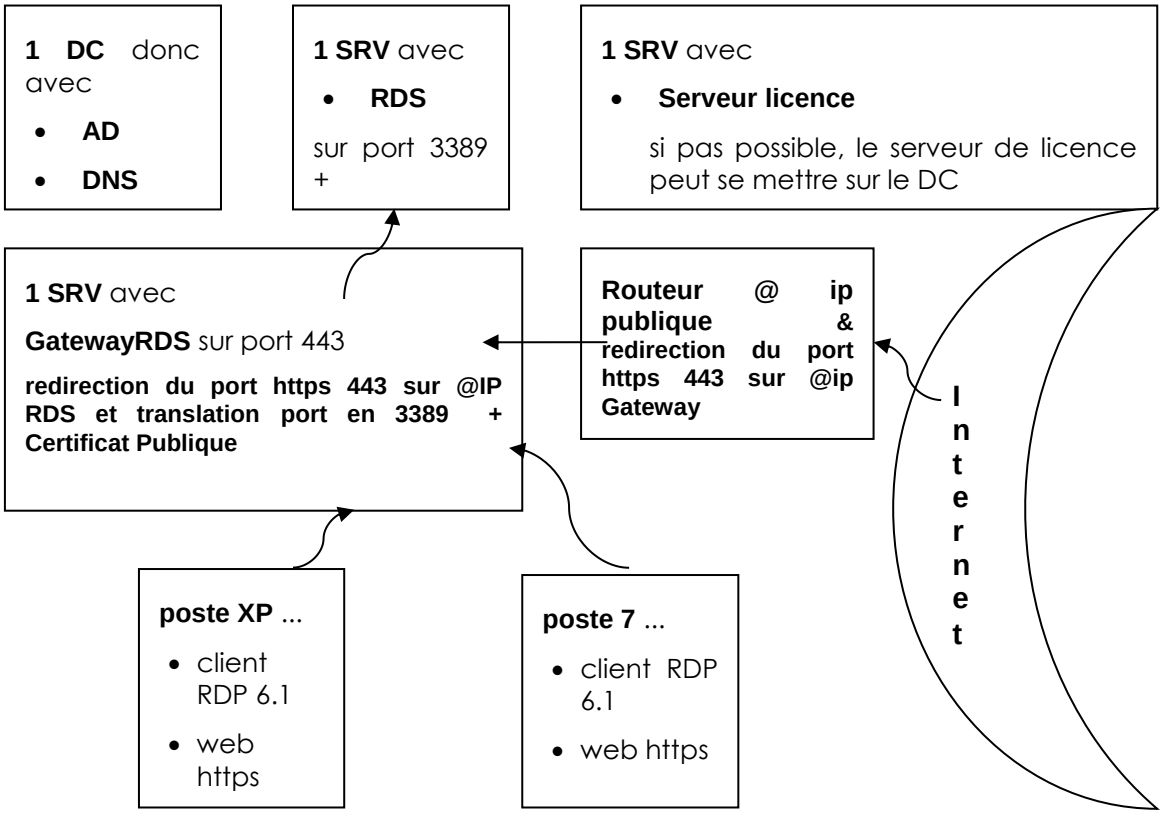



Propriétés de GTW-FORM
Magasin de stratégies d'autorisation des connexions aux services Bureau à distance
Général
Certificat SSL
Paramètres de transport
Batterie de serveurs
Audit
Pontage SSL
Messages
Activer le message système
Créez un message à l'attention des utilisateurs qui ont ouvert une session sur l'ordinateur distant, par exemple une notification concernant la maintenance du système.
Heure de début :
01/06/2016
13:18:44
Aperçu...
Heure de fin :
01/06/2016
14:18:44
Activer le message d'ouverture de session
Sélectionnez un message, par exemple un avis juridique, à afficher à l'écran chaque fois
qu'un utilisateur ouvre une session sur l'ordinateur distant.
Parcourir...
Aperçu...
Autoriser uniquement les connexions à partir des clients des services Bureau à distance qui prennent en charge la messagerie de la passerelle des services Bureau à distance

UTILISATION RDS VIA HTTPS

Ce que l'utilisateur ne peut plus faire

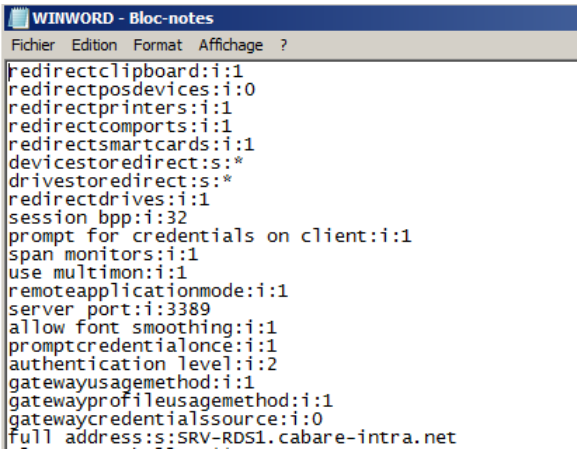
On ne peut plus se connecter directement sur le serveur RDP, on doit passer par la passerelle



les clients "internes" du LAN, eux, peuvent accéder aussi par la passerelle..., ou accéder directement au serveur RDS

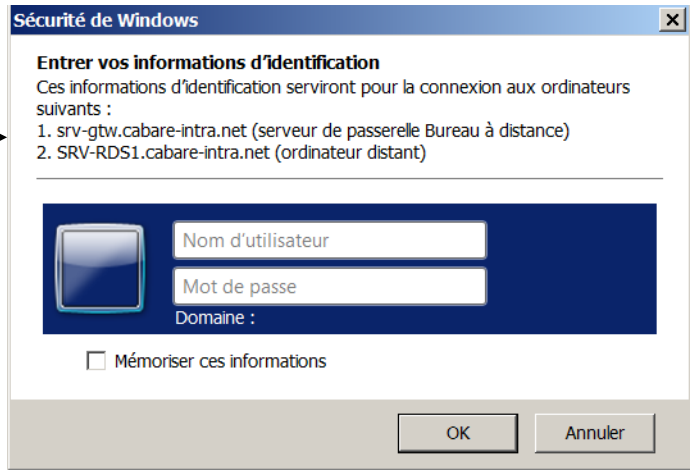
Ce que l'utilisateur peut faire

si l'utilisateur dispose sur son bureau d'un raccourcis fournis par l'administrateur permettant de lancer une application **remoteapp**, genre



alors il peut tout simplement effectuer un double clic dessus...

et s'authentifier sur le portail... il aura une demande de login

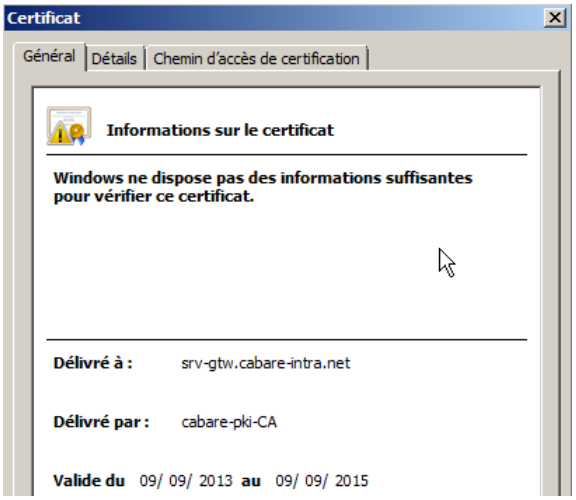


puis ...

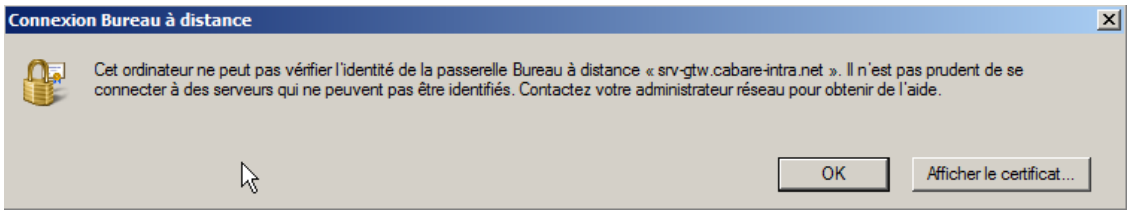
Certificat et domaine

machine hors domaine - certificat de domaine

si on installé juste un certificat auto-signé sur notre passerelle, ou même un certificat de domaine, et que notre machine cliente ne fait pas partie du domaine,

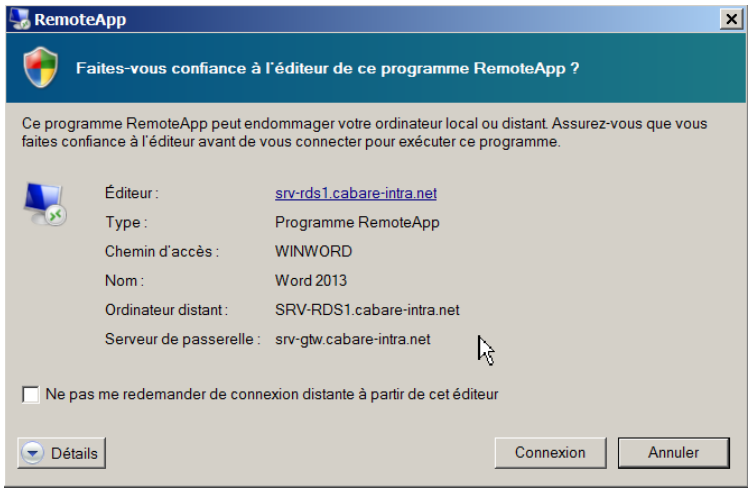


on ne peut se connecter depuis l'extérieur.

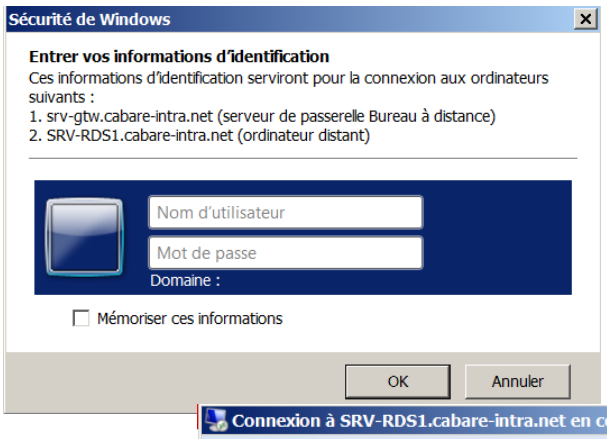


machine du domaine - certificat de domaine

le lancement de la remote app demande la confiance de l'éditeur (on non selon les GPO appliquées sur le client)

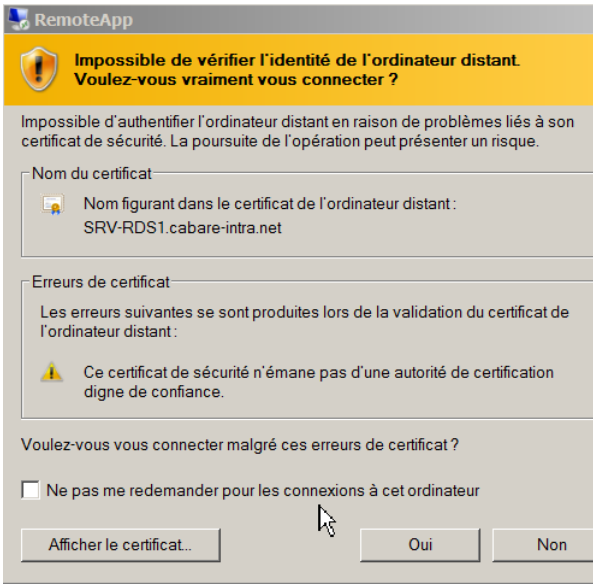


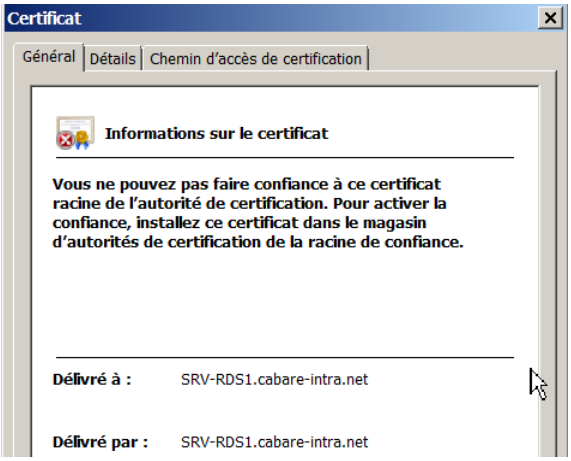
puis evidemment authentification



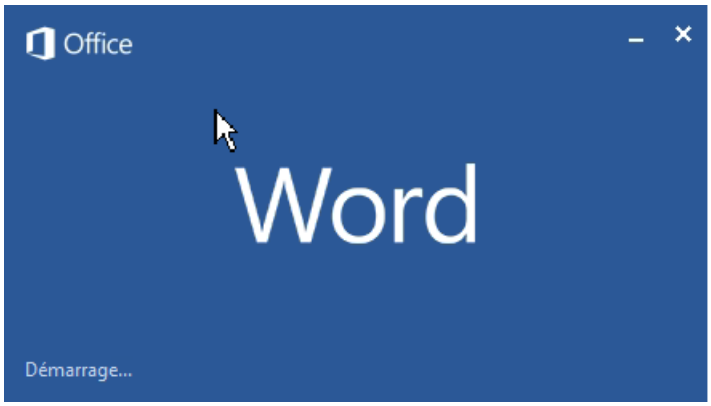
lancement de la remote app

warning sur certificat de domaine,





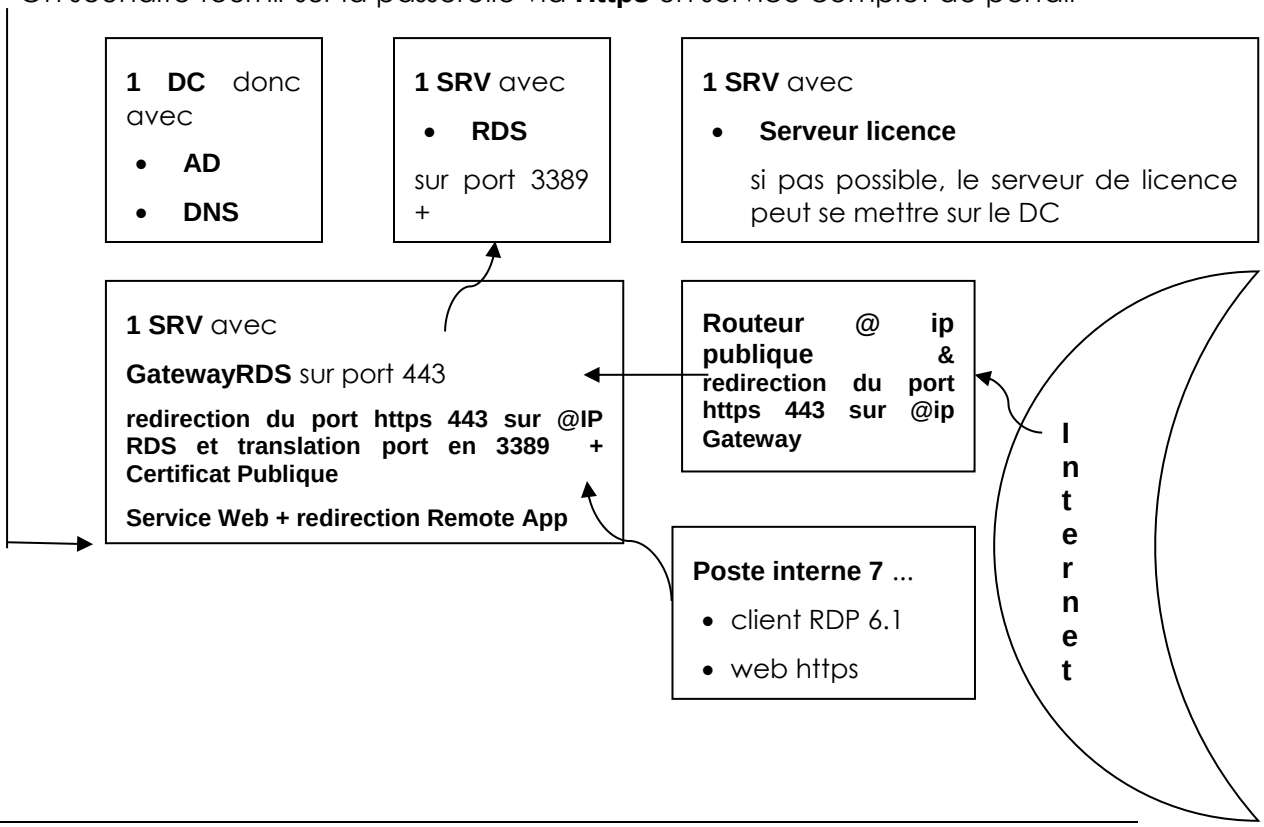
mais on peut continuer...et lancement de la **remoteapp**..



PORTAIL WEB VIA HTTPS

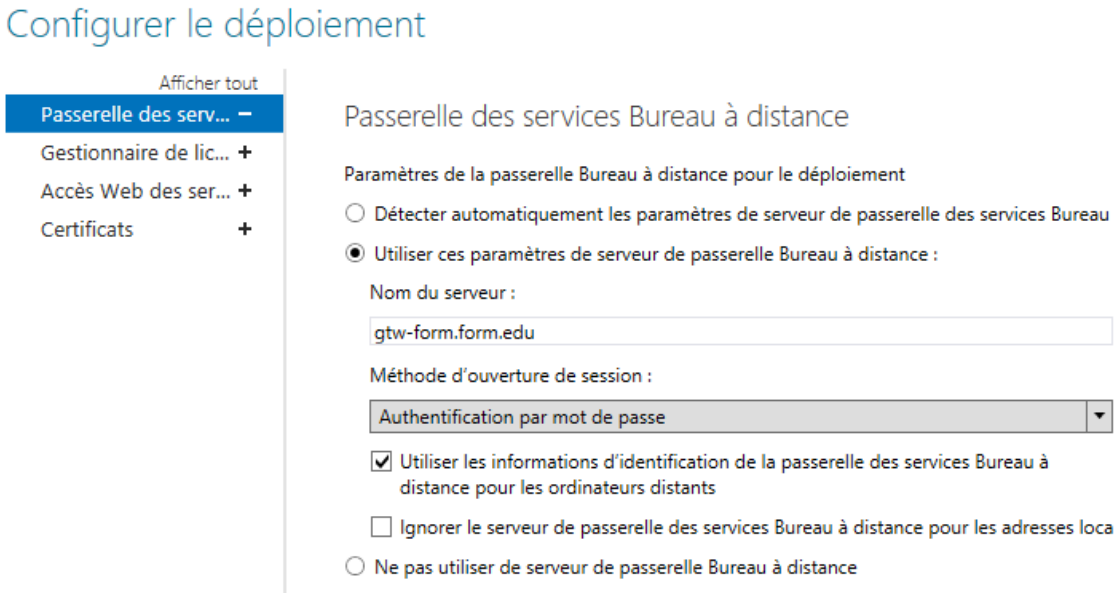
Accès Via portail web en https

On souhaite fournir sur la passerelle via **Https** un service complet de portail



Configuration Accès Web des Services Bureau à Distance:

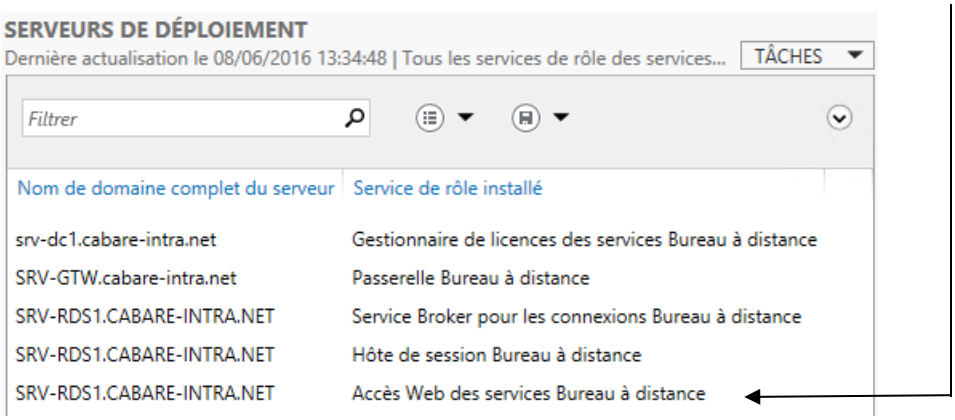
Il faut penser à indiquer dans notre vue d'ensemble, que on utilise désormais une passerelle. Dans la vue d'ensemble dans le **gestionnaire de serveur**, et demander dans les **taches** de modifier les **propriétés de déploiement**



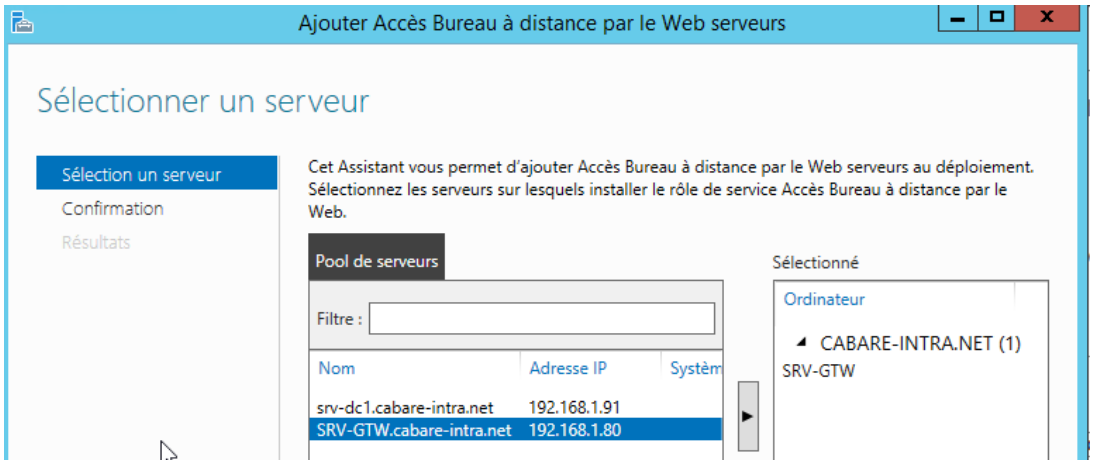
Ajout service Accès Web sur la passerelle:

Si on ne veut pas obtenir un message du type

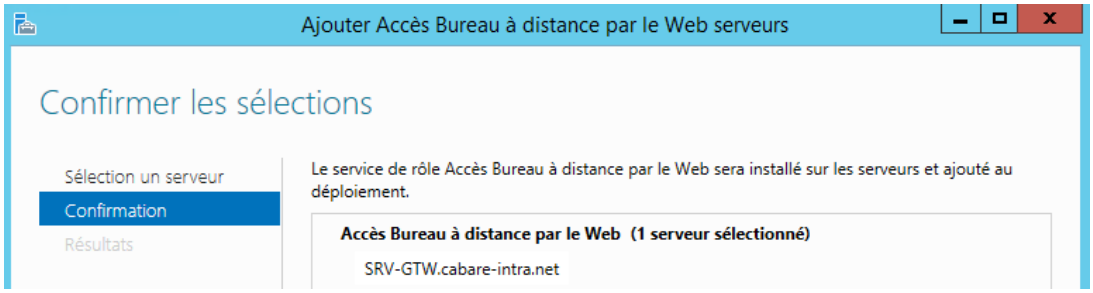
Et il faut pense à installer sur notre passerelle un RDWA, en effet pour l'instant sa seule machine qui héberge un rôle de portail Web c'est le serveur RDSH…



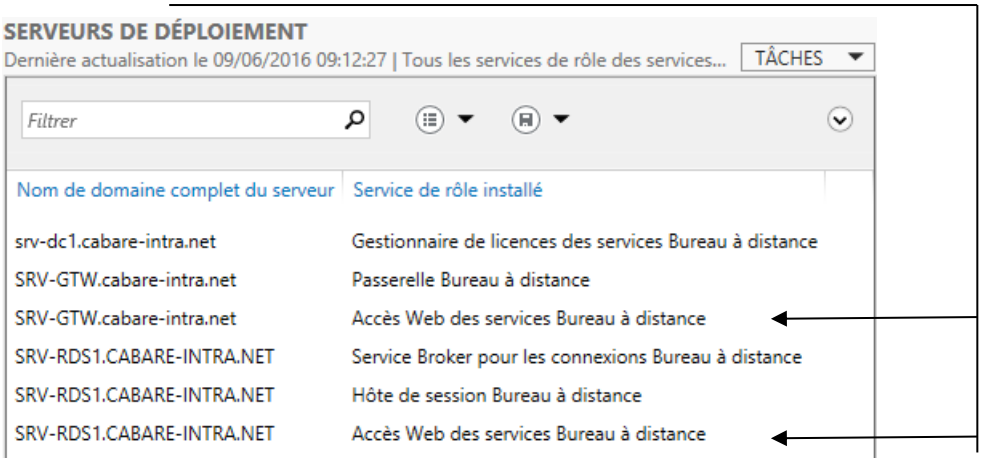
On demande donc d'ajouter un **accès bureau à distance par le Web** sur la machine qui héberge déjà les services de passerelle



Et on confirme



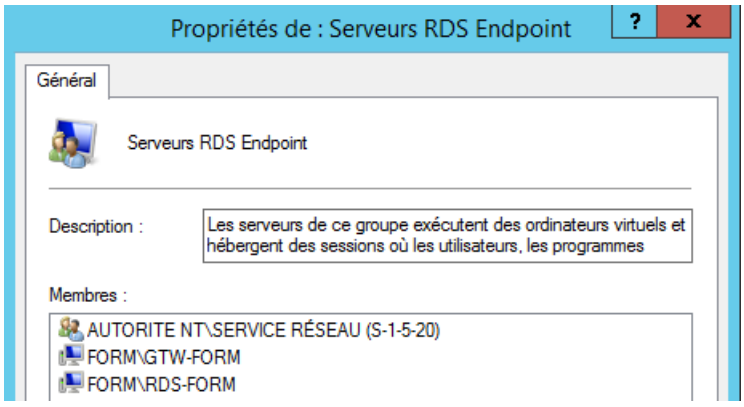
Pour obtenir

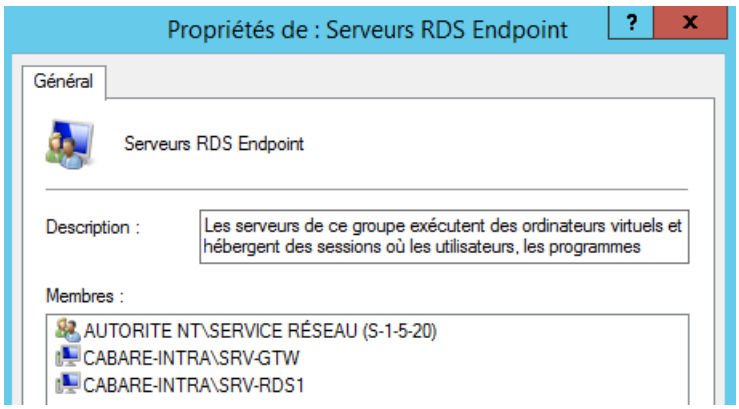


Ajout compte ordinateur dans groupe local RDS Endpoint:

Si on ne veut pas obtenir un message du type

N.B: il faut penser à ajouter le compte ordinateur de la passerelle **gtw-form** dans le groupe des **Serveurs RDS Endpoint** sur notre serveur RDS

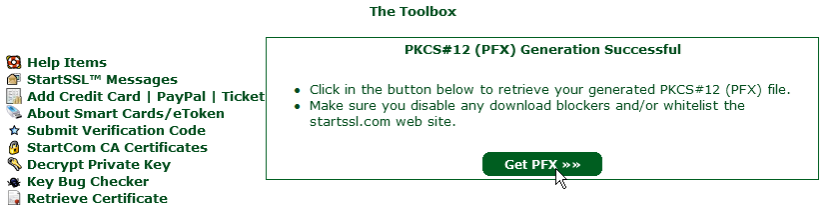




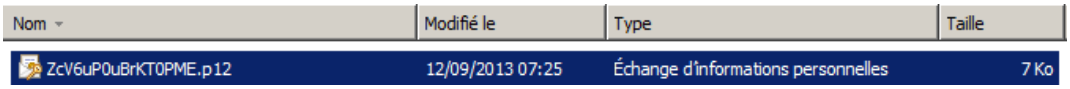
CERTIFICAT PUBLIC

Certificat public

imaginons avoir ne main un certificat public pour notre domaine, crée par exemple auprès de **startssl**...



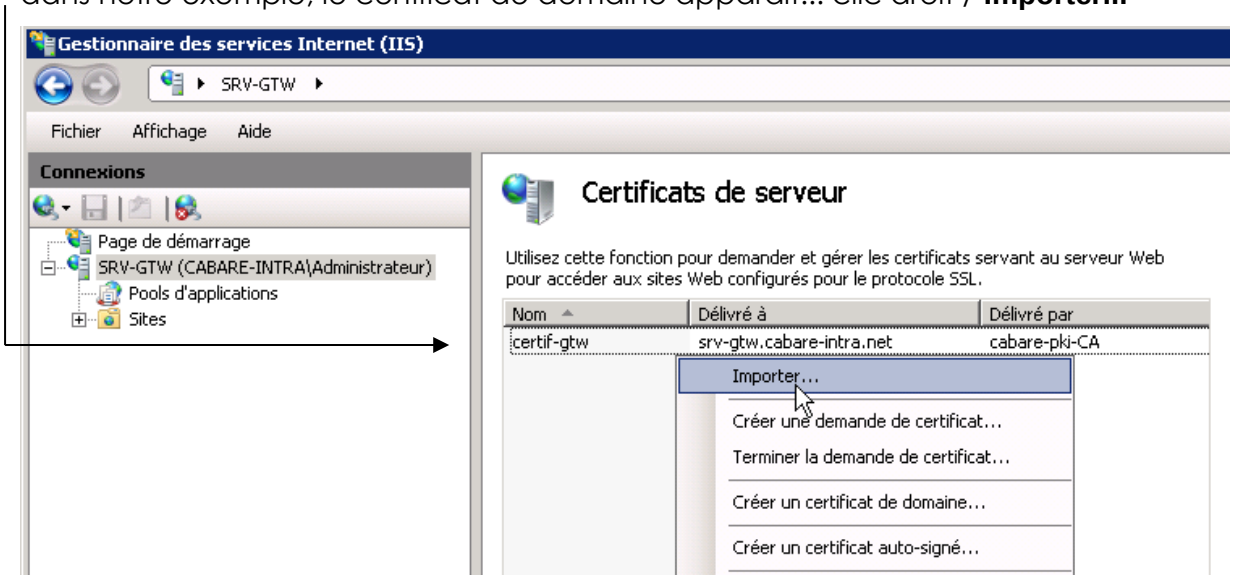
Voila notre certificat dans un fichier au format PFX



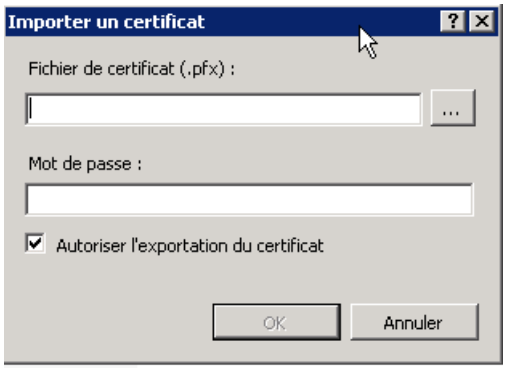
importer le certificat dans IIS:

il faut se mettre sur le **gestionnaire des services internet**, et demander d'importer le certificat.

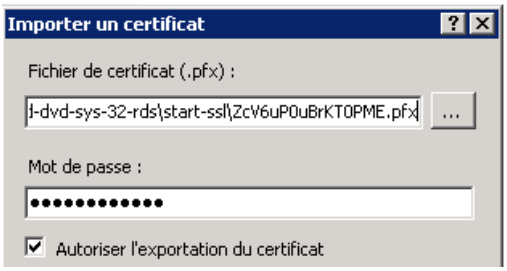
dans notre exemple, le certificat de domaine apparaît... clic droit / **Importer...**



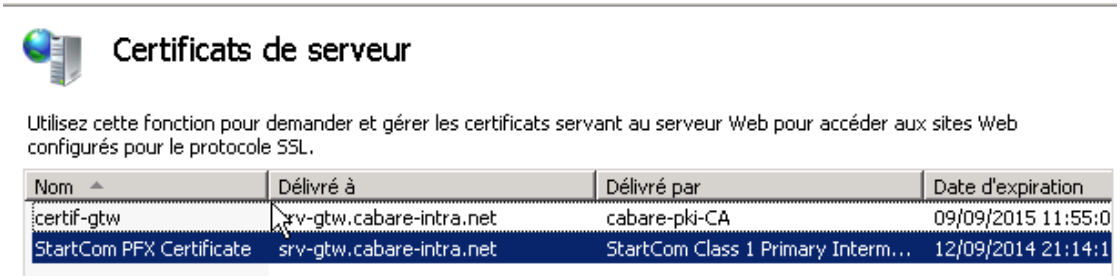
et il suffit de ramener le certificat



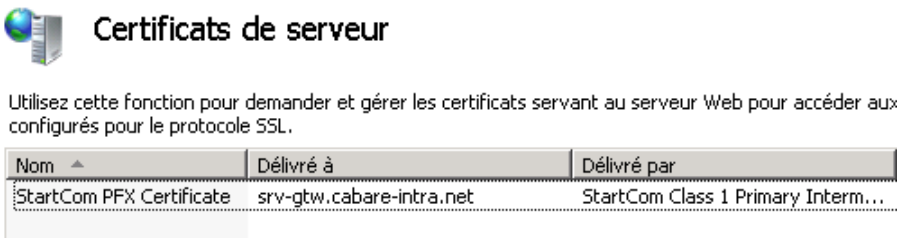
..



pour obtenir

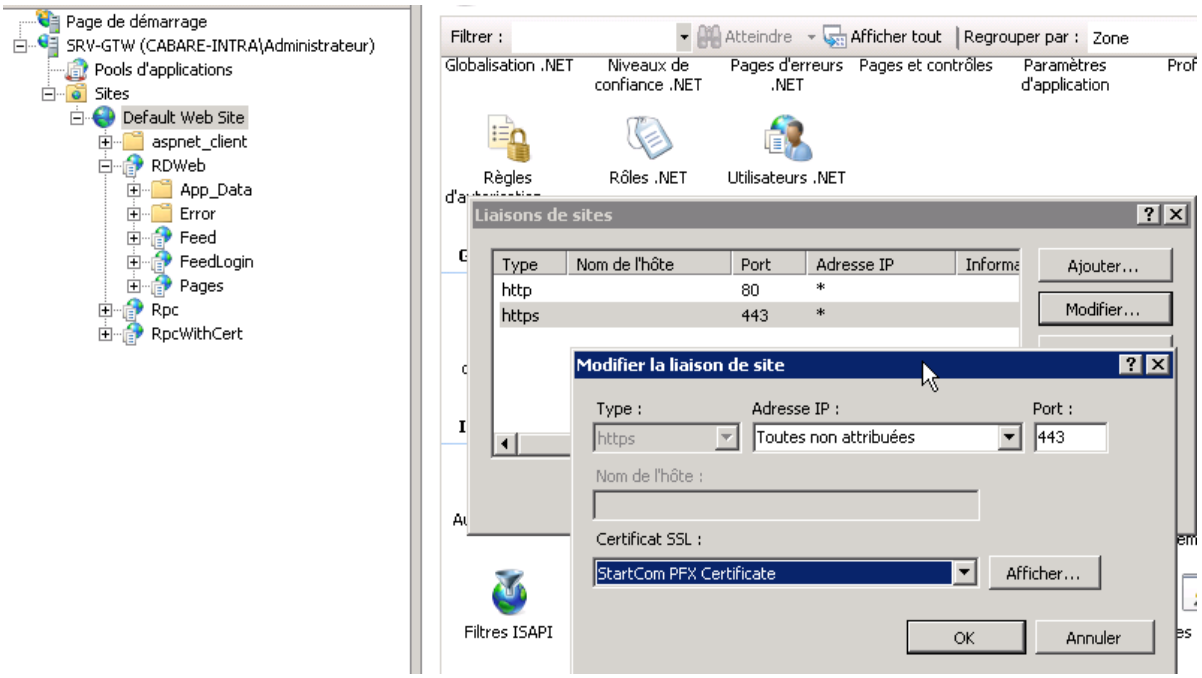


il ne reste plus qu'à supprimer le certificat de domaine pour ne garder que le certificat public...



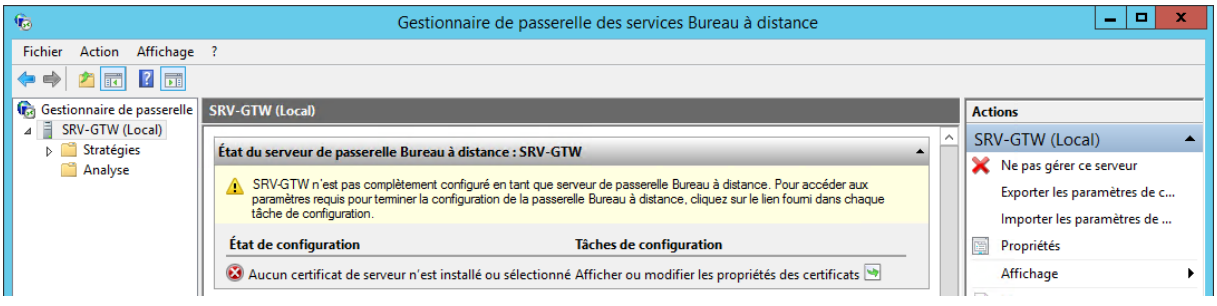
ensuite il faut simplement appliquer le certificat sur le site web..

via modifier les liaisons

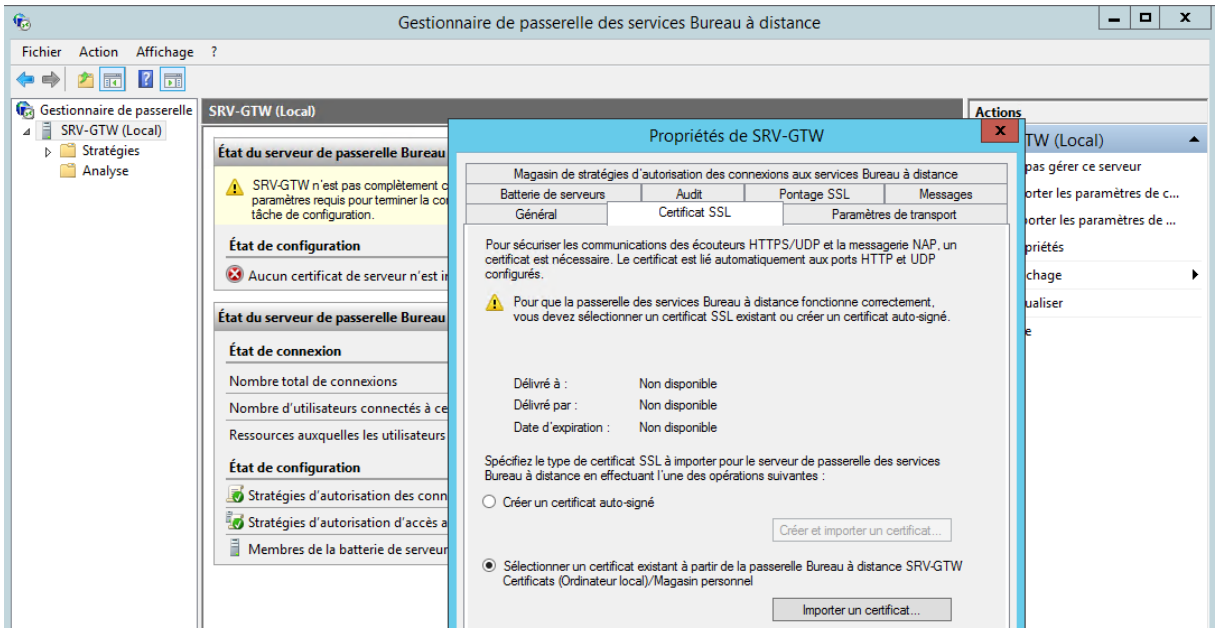


importer le certificat dans gestionnaire de passerelle:

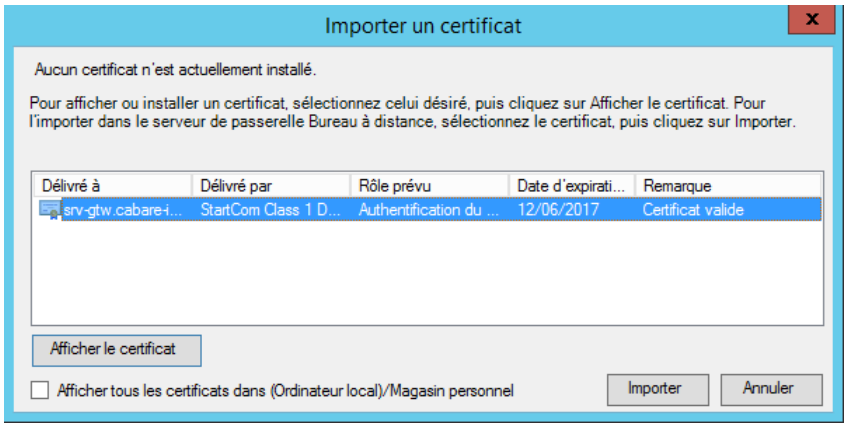
Mais il faut aussi l'importer le certificat depuis notre interface gestionnaire de passerelle



On obtient



On demande **importer un certificat**



N.B: le certificat public préalablement importé via IIS doit apparaître.

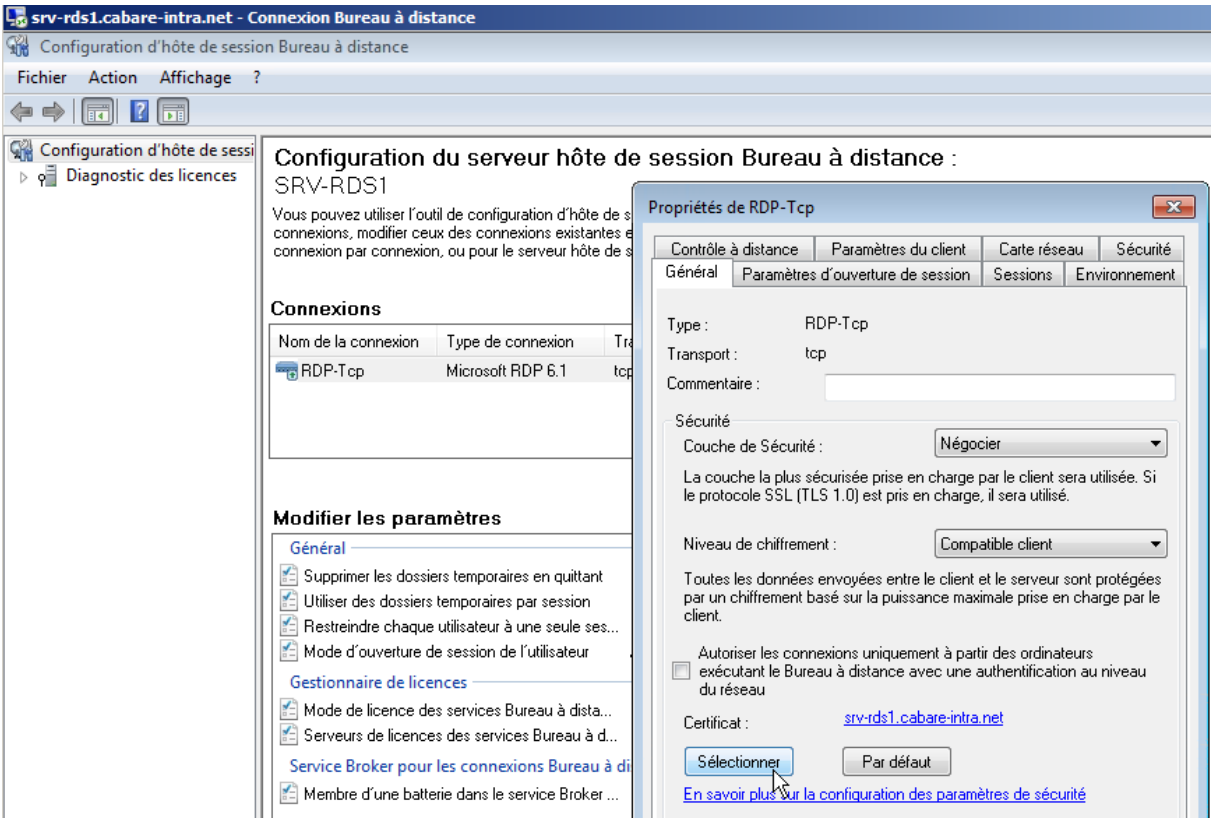
1 serveur = 1 certificat:

N.B: il faut avoir un certificat par serveur, autrement dit dans notre configuration, il faut au minimum 1 certificat pour notre passerelle ***srv-gtw*** et 1 certificat pour notre serveur RDS ***srv-rds1***.

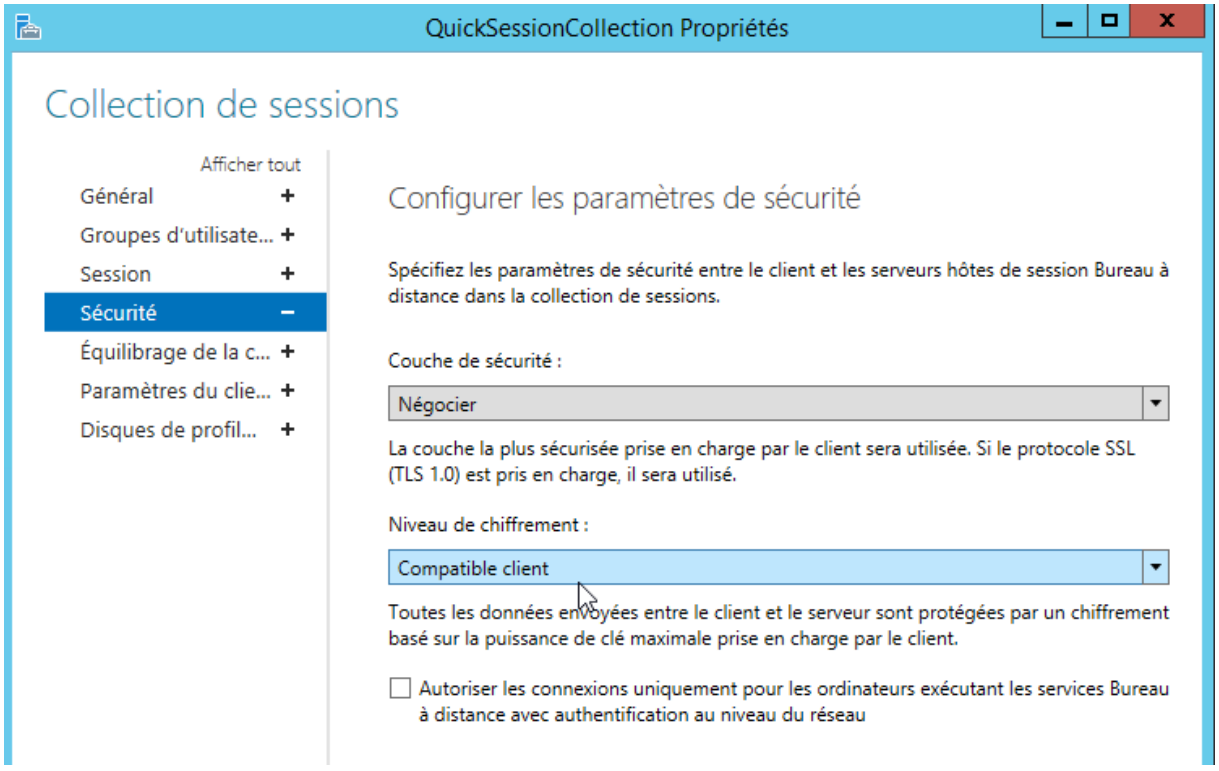
Si on passe en mode brooker haute disponibilité et que l'on ajoute un 2° serveur RDS il faudra bien sûr un certificat pour ce 2° serveur ***srv-rds2***...

N.B: en plus de ce que l'on a fait sur notre gateway (à savoir importer le certificat, et l'appliquer au site web)

pour le (les ?) serveurs RDS il faut non seulement importer le certificat, l'appliquer au site web mais en plus appliquer le certificat au niveau RDP



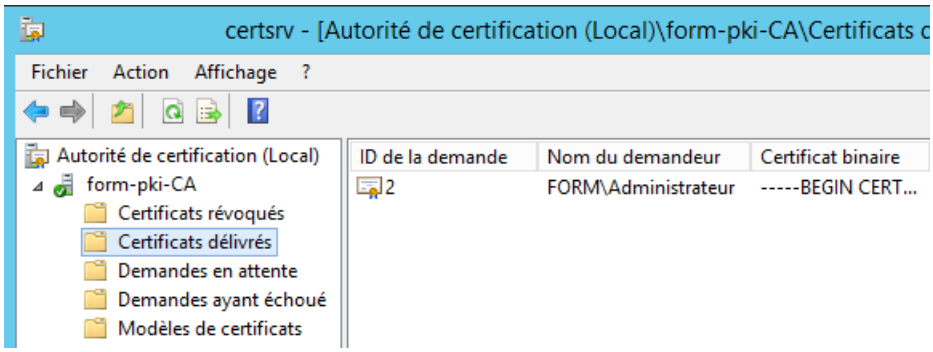
J'irais bien chercher par la sous 2012 mais je ne vois pas ou indiquer le certificat à utiliser



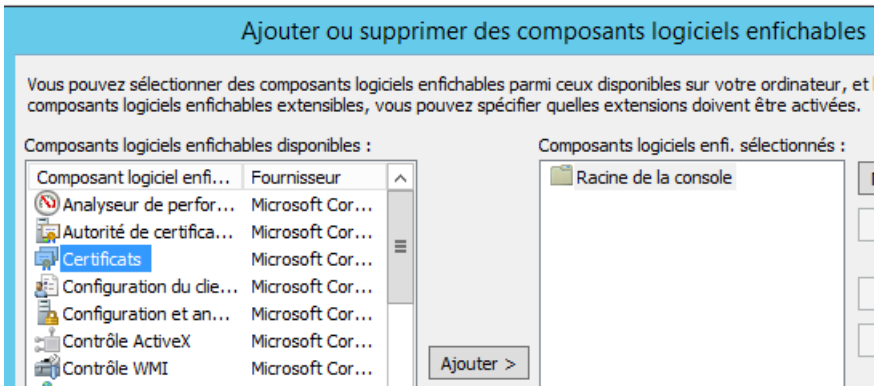
ANNEXE 4 – MMC CERTSRV

Console Certificats

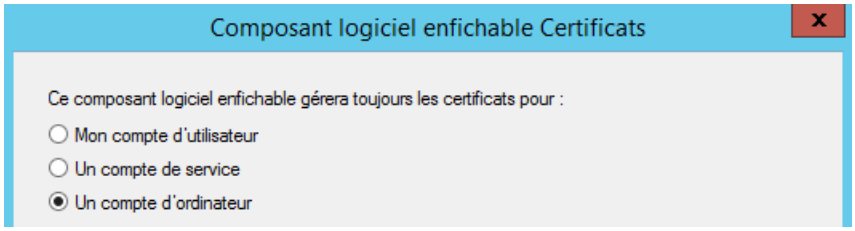
Lorsque sur notre serveur on a installé notre **pki racine** de domaine, on a bien un outil **autorité de certification** qui apparaît disponible

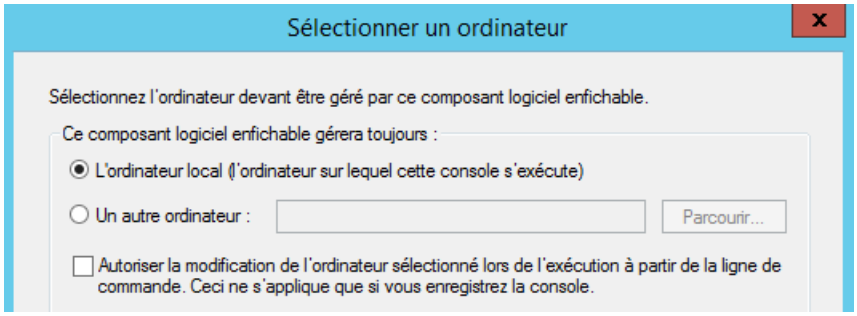


Pour gérer les certificats (demandes) autrement que en passant via IIS, il est possible d'installer une mmc certificats. Sur cette même machine (qui connait donc notre **pki**) on exécute **mmc.exe**

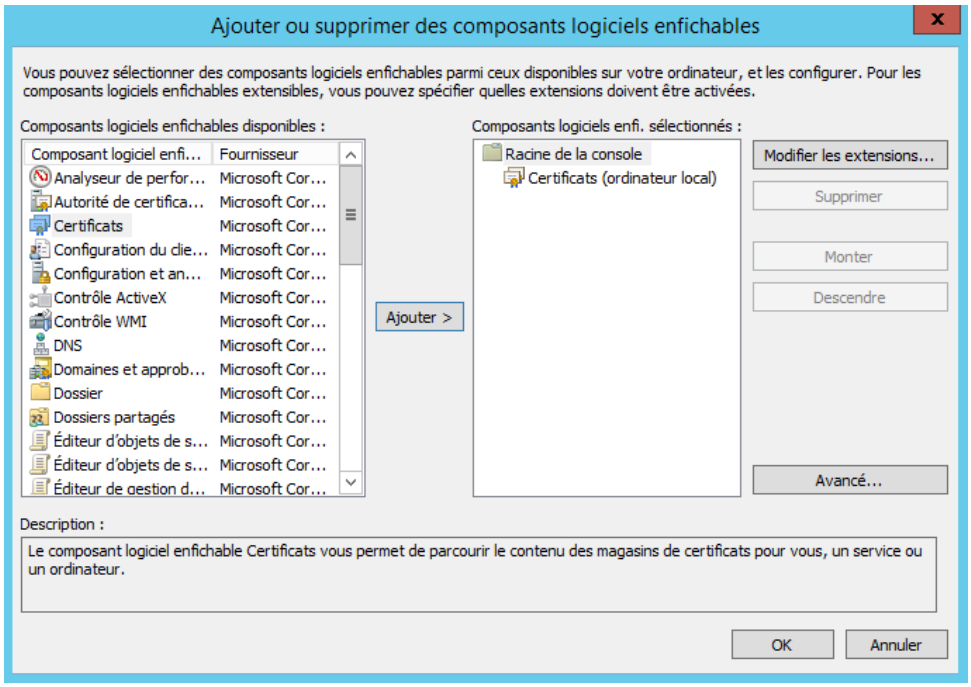


On demande un **compte ordinateur**, et **ordinateur local**





Et on valide



On peut vérifier que