Titre	Installation et configuration d'une CA sous Windows Server 2008
Propriétaire	Tavares José
Classification	Interne
Date dernière modification	28 Septembre 2009
Chemin\NomFichier	\\10.1.1.1\FilesTD\Group4\Personnel\Tavares\00_EIG\CA_LaboTD.doc

CA Microsoft sous Windows Server 2008

0 But

Configurer l'autorité de certification (CA) **LaboTD** à partir de Windows Server 2008 ; mises à jour des configurations DNS et firewall Clavister

Remarques

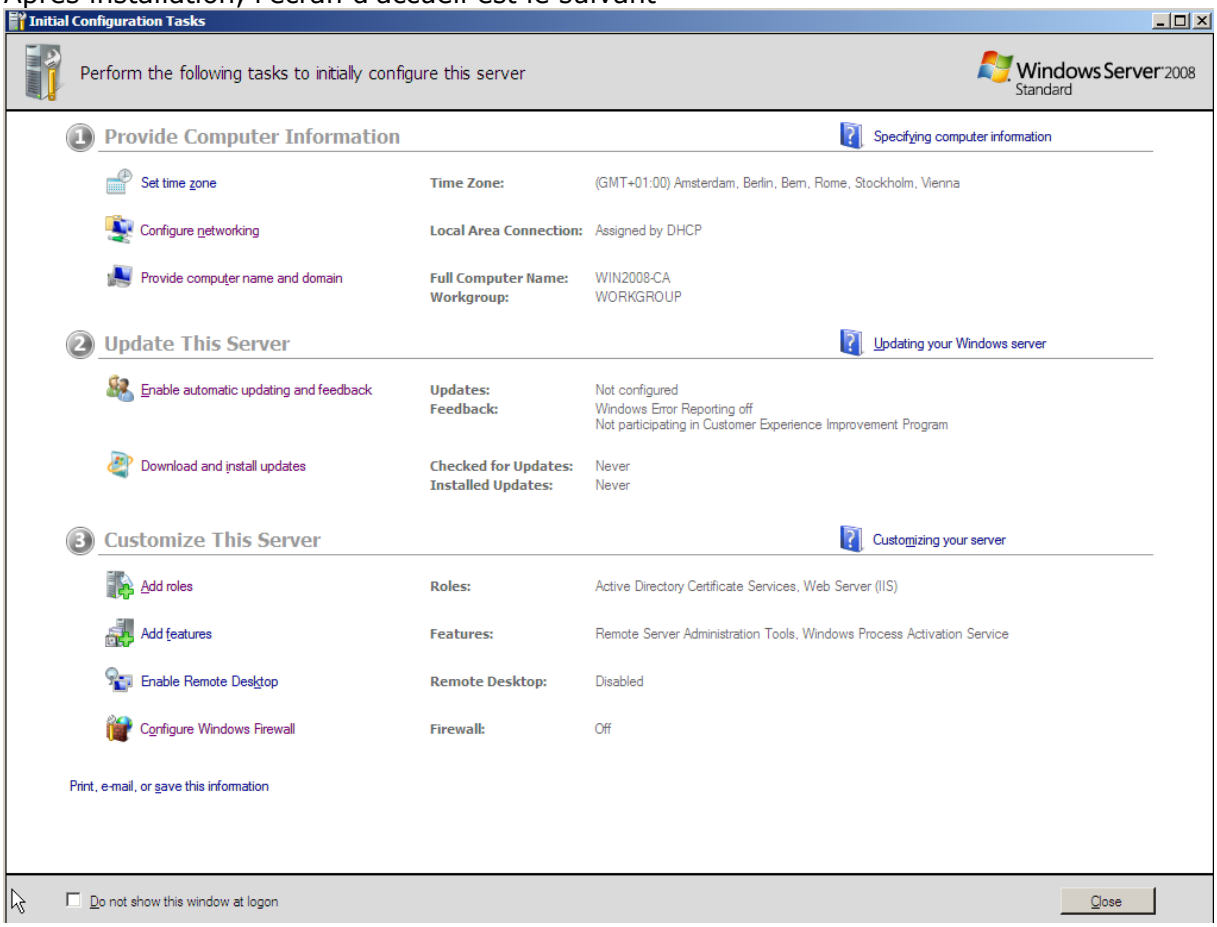
- Utilisation d'une architecture virtualisée ESXi 4 (PC-G16)
- Accès depuis http://ca.tdeig.ch

1 Installation de Windows Server 2008

Une installation par défaut a été faite, sur une base
Windows Server 2008 64bits Standard Edition

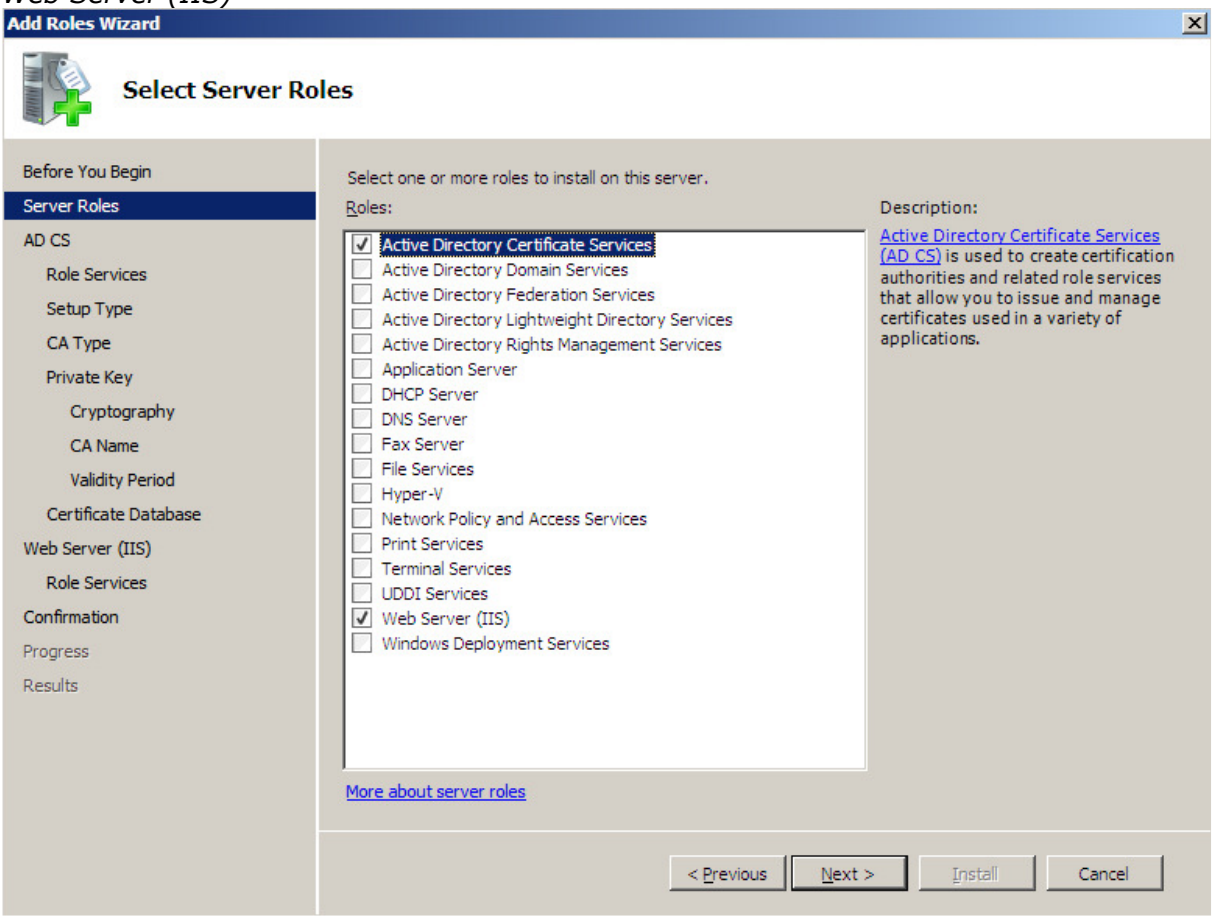
Cette installation c'est effectuée dans une machine virtuelle, sur un disque virtuel de 20GB, et a nécessité environ 45minutes

Après installation, l'écran d'accueil est le suivant



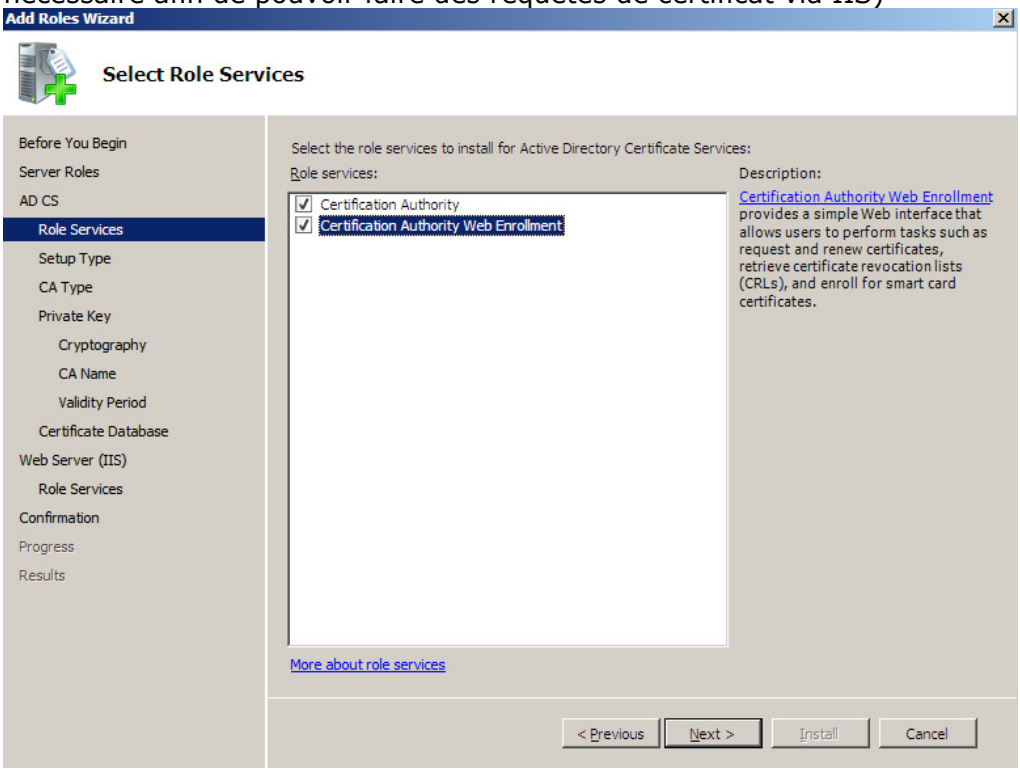
2 Installation d'une CA

Cliquer sur *Add roles* puis sélectionner *Active Directory Certificate Services*, ainsi que *Web Server (IIS)*

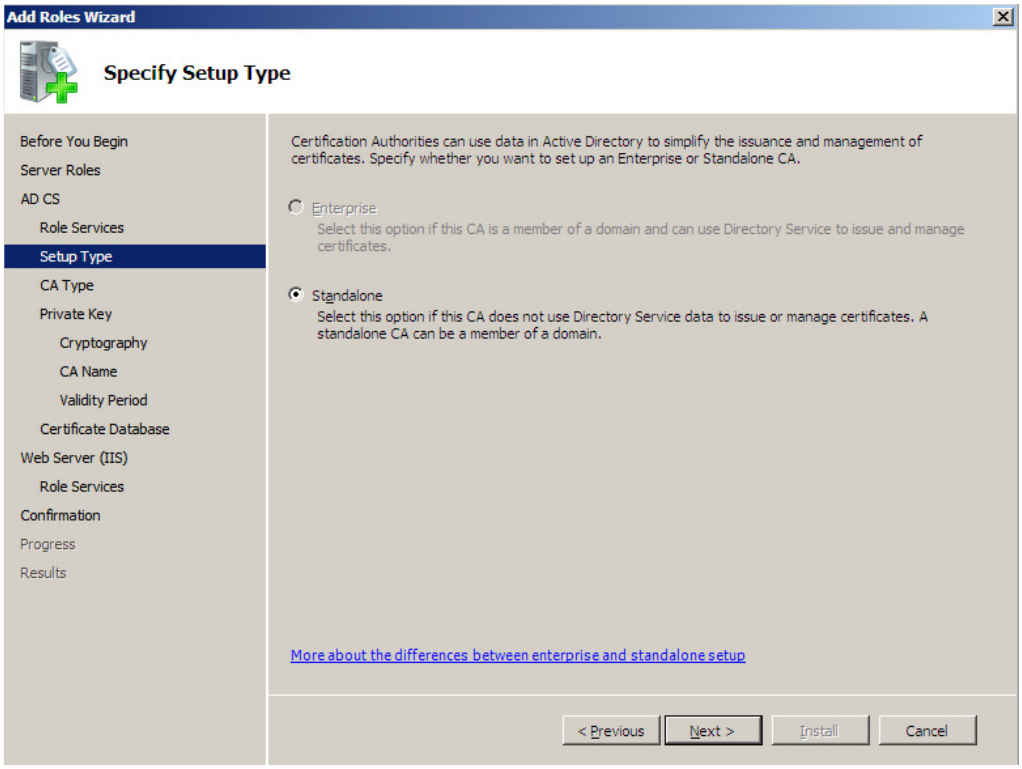


Le serveur web IIS est en effet nécessaire pour faire des demandes de certificats à notre CA

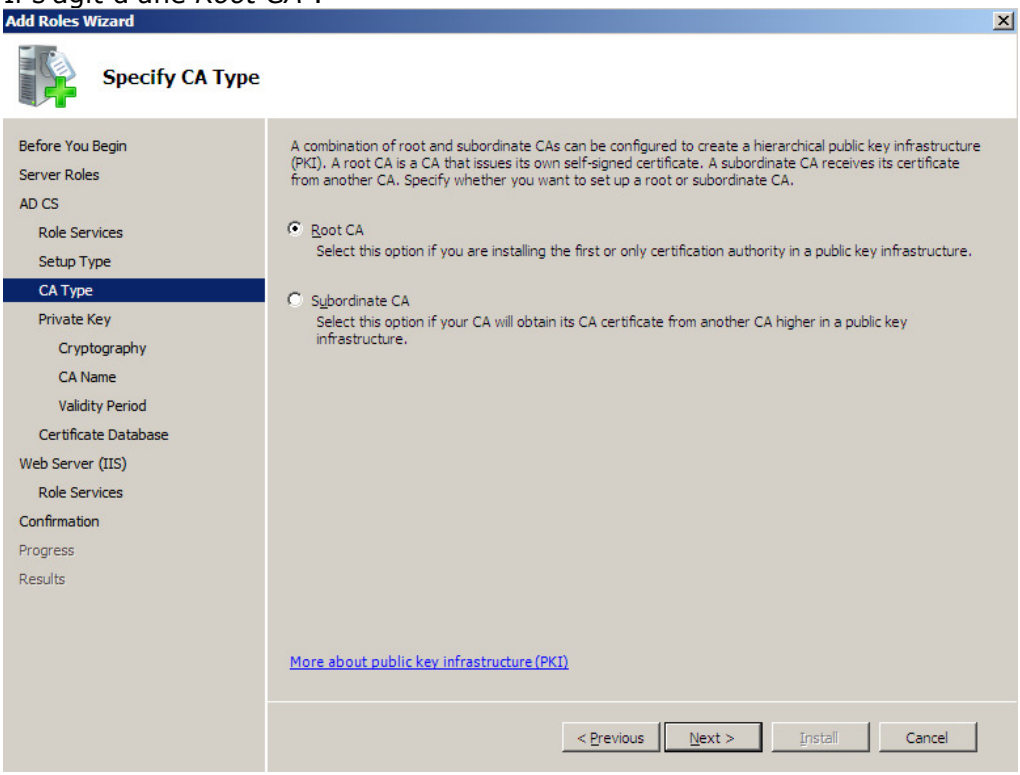
Sélectionner les 2 champs ci-dessous (*Certification Authority Web Enrollment* est nécessaire afin de pouvoir faire des requêtes de certificat via IIS)



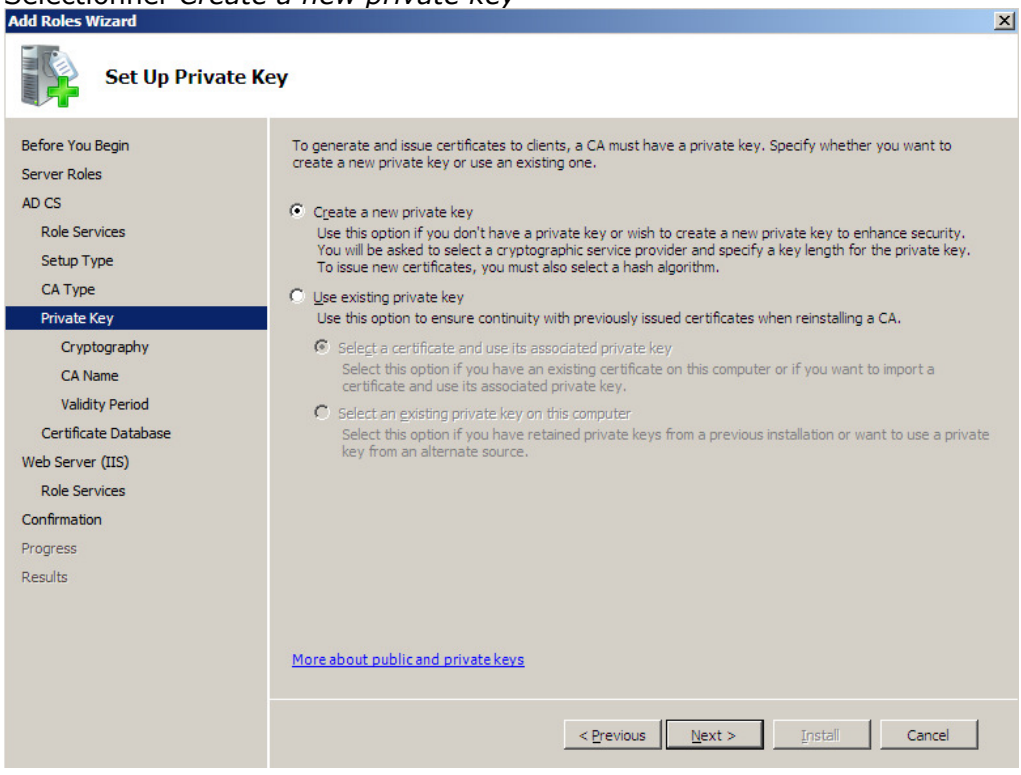
Sélectionner *Standalone*



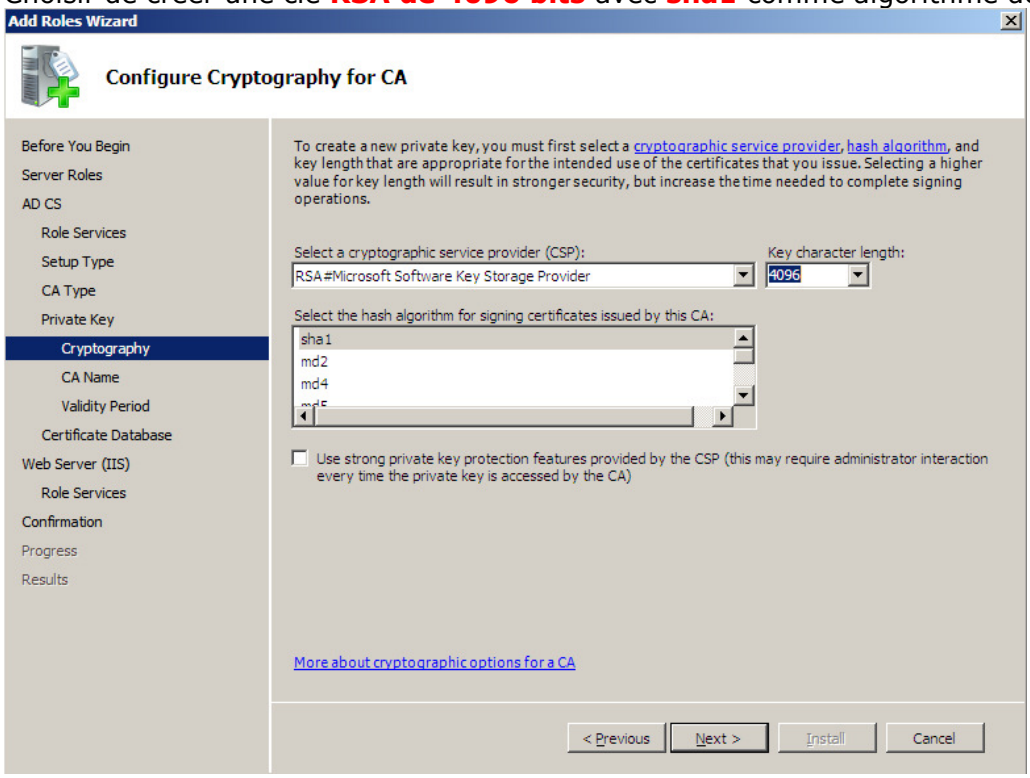
Il s'agit d'une *Root CA* :



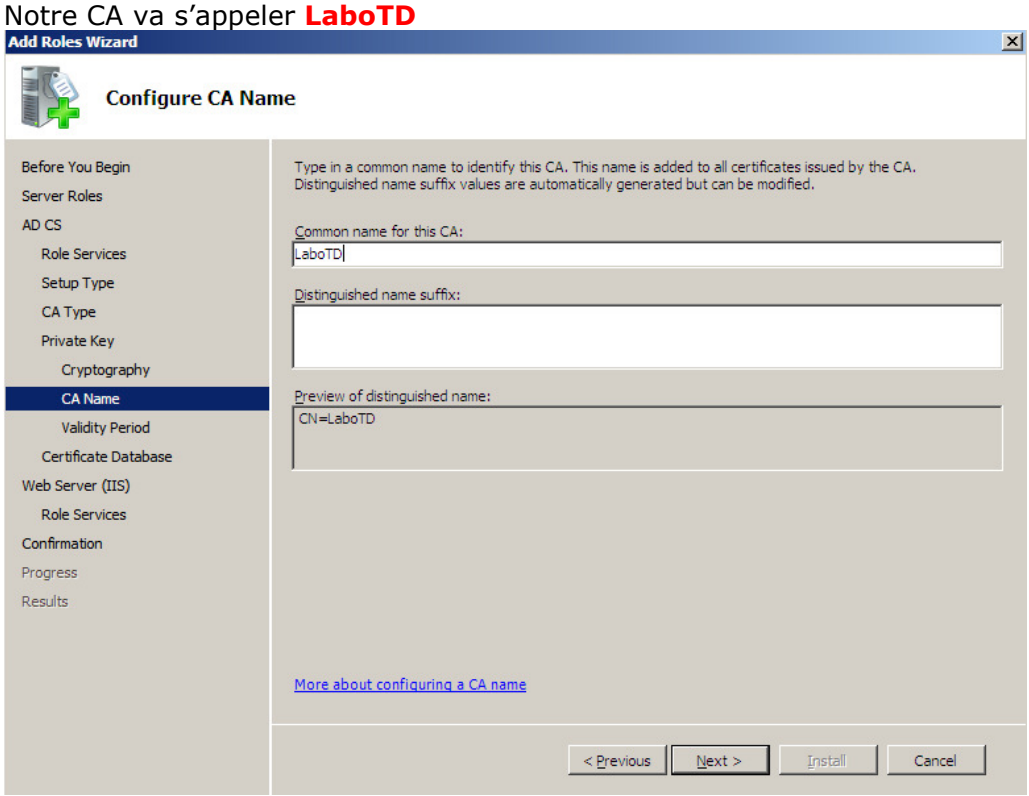
Sélectionner *Create a new private key*



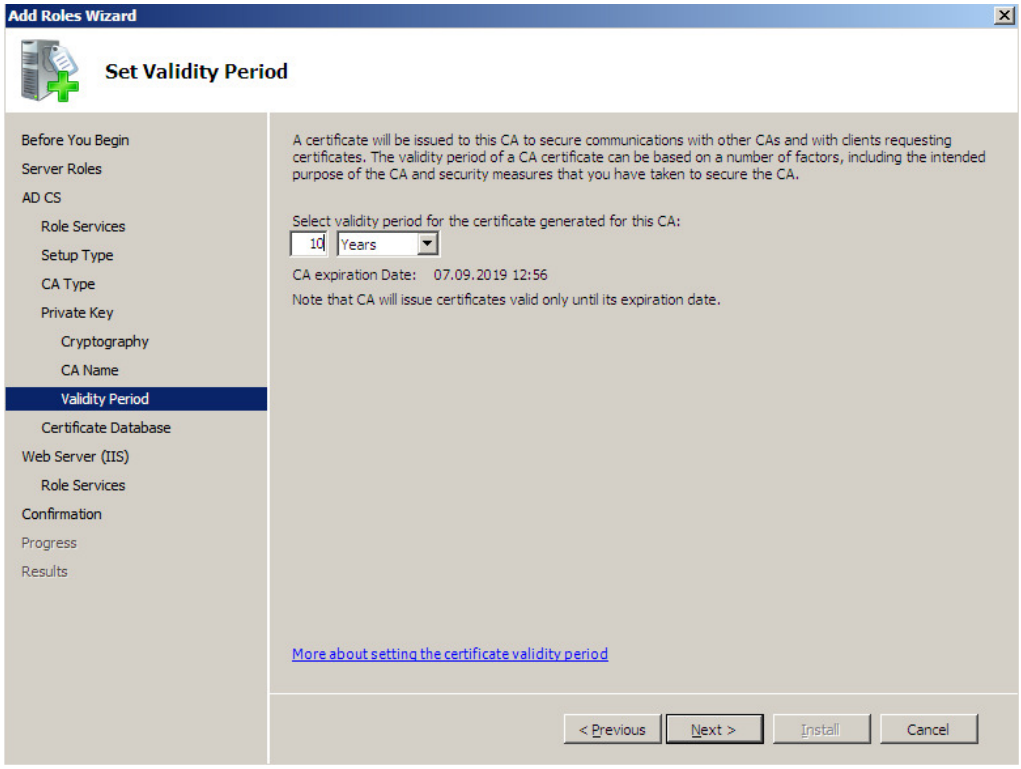
Choisir de créer une clé **RSA de 4096 bits** avec **sha1** comme algorithme de hash



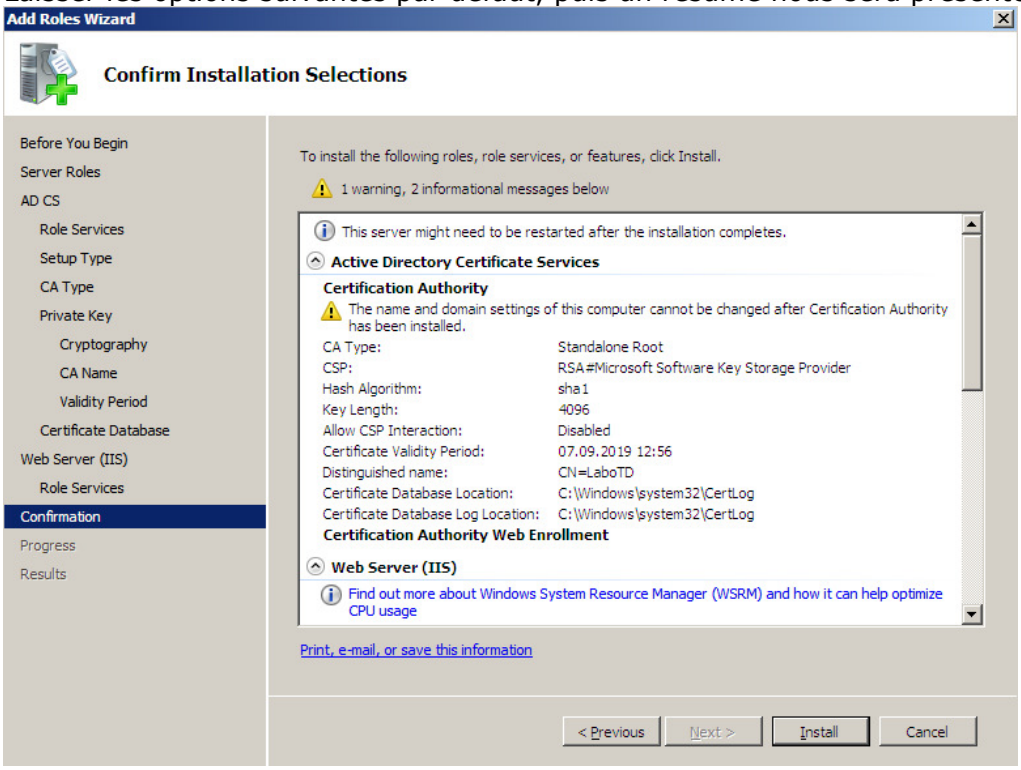
Notre CA va s'appeler **LaboTD**



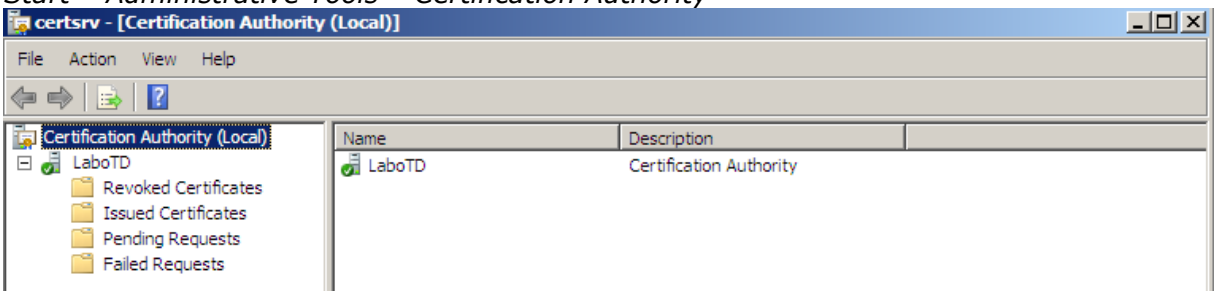
Le certificat root aura une **validité de 10 ans** :



Laisser les options suivantes par défaut, puis un résumé nous sera présenté :



La CA peut ensuite être administrée sur le serveur, sous
Start – Administrative Tools – Certification Authority

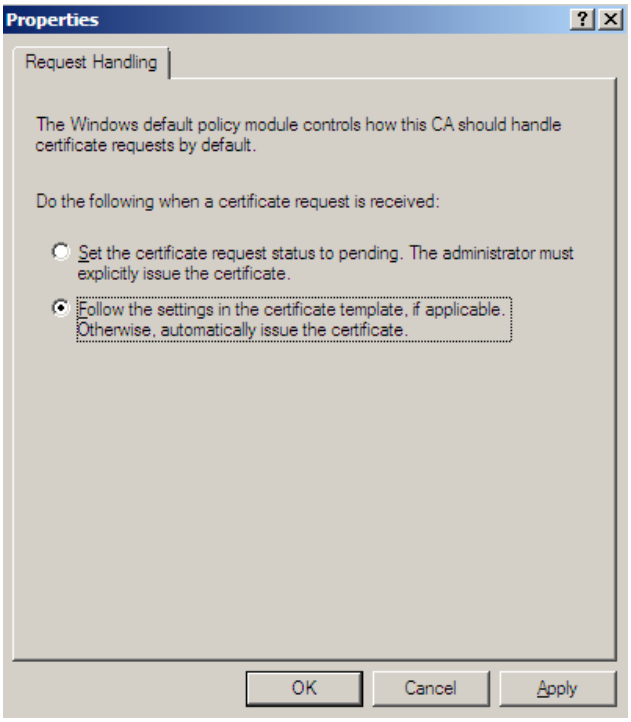


3 Accepter automatiquement les requêtes de certificats

Start – Administrative Tools – Certification Authority

Clic-droit sur la CA – *Properties* – Onglet *Policy Module* – *Properties…*

Sélectionner la valeur ci-dessous



OK

Redémarrer la CA pour appliquer les changements

4 Configuration IP, login et mot de passe

Adresse IP = 129.194.184.89
Netmask = 255.255.252.0
Gateway = 129.194.184.1
DNS = 129.194.184.84 – 129.194.4.6

Login = Administrator
Pass = carte CryptMe

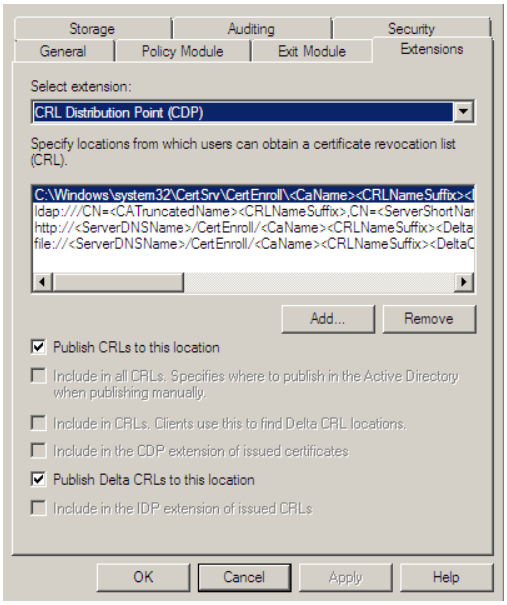
5 Configurer les chemins de CRL et AIA

Par défaut, les chemins de **CRL** (*Certificate Revocation List*) et AIA (*Authority Information Access*) sont désignés par le nom PC ou s'exécute la CA.
Le paramètre AIA pointe en réalité sur le certificat root de la CA

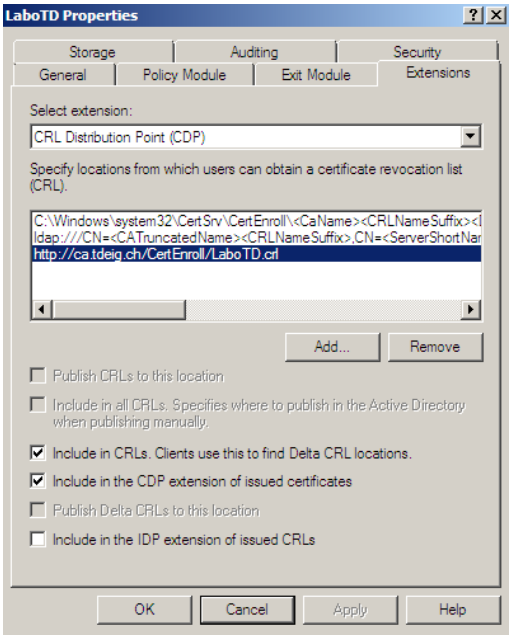
Dans notre cas, il a fallu reconfigurer ces chemins dans la CA :
Start – Administrative Tools – Certification Authority

Clic-droit sur la CA – *Properties* – Onglet *Extensions*

Effectuer un *Remove* des 2 dernières entrées (http://... et file://...)



Puis à l'aide du bouton *Add…*, ajouter la bonne url sans oublier de cocher les 2 cases comme ci-dessous :



Source
http://technet.microsoft.com/en-us/library/cc773036(WS.10).aspx

6 Se faire délivrer un certificat serveur

Remarques importantes (problèmes rencontrés)
La durée de vie du certificat a été modifiée à 9 ans
http://support.microsoft.com/kb/254632/
Puis redémarrer la CA (Clic droit sur la CA – *All tasks* – Stop…)

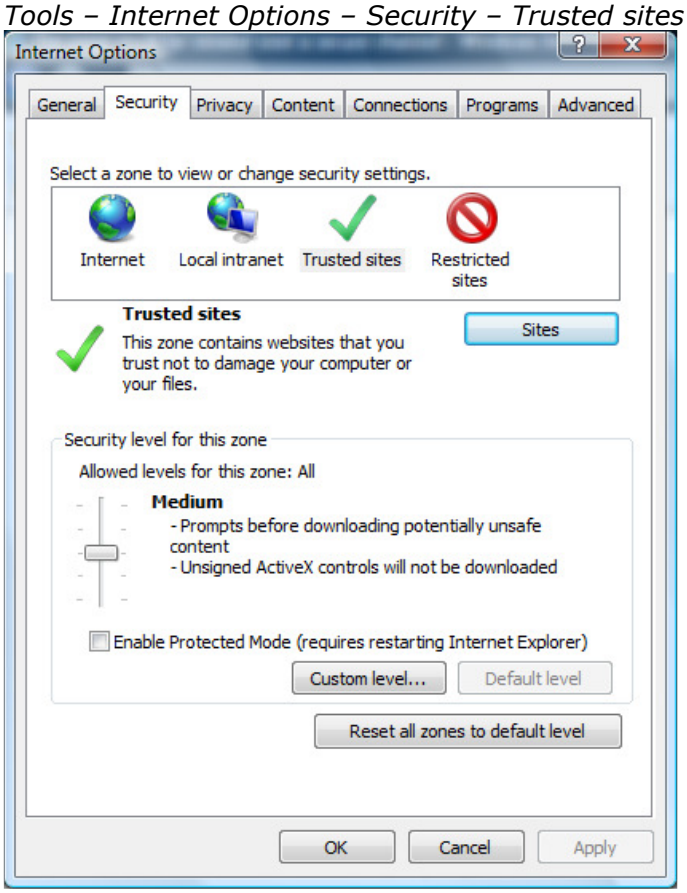
Lors d'une demande de certificat depuis un poste Vista exécutant IE7, on obtient une erreur :
An error occurred while creating the certificate request. Please verify that your CSP supports any settings you have made and that your input is valid. Suggested cause: No suggestion. Error: 0x80070005 - (unknown)

Ceci se produit car IE7 est lancé avec peu de privilèges sous Vista, ce problème a été corrigé avec IE8 qui fonctionne déjà différemment.

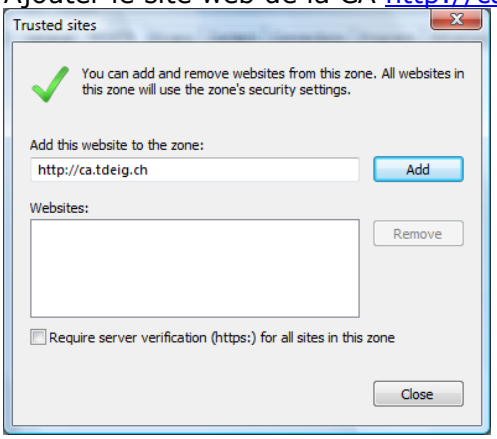
Il est cependant possible de résoudre cette erreur sous IE7, en ajoutant le site web de la CA à la zone *Trusted sites*
Lorsqu'un essaie d'ouvrir un site faisant partie de la zone *Trusted*, IE7 lance une nouvelle fenêtre avec des privilèges différents, ce qui résout le problème !

Sources :
http://social.technet.microsoft.com/Forums/en-US/itprovistaie/thread/75b0450e-4926-47df-8885-b8e209919c16
http://support.microsoft.com/kb/922706/en-us

Tools – Internet Options – Security – Trusted sites



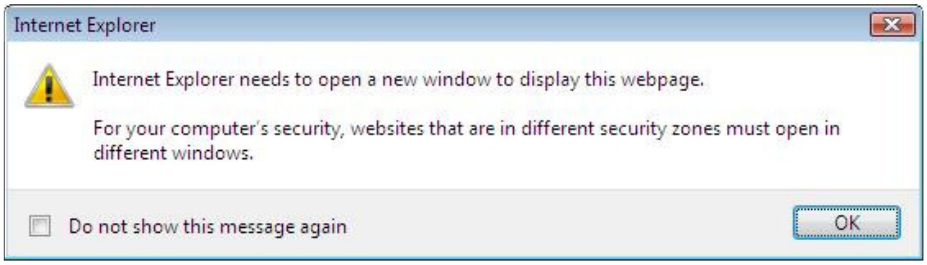
Cliquer sur le bouton *Sites*
Décocher la case *Require server verification (https:) for all sites in this zone*
Ajouter le site web de la CA http://ca.tdeig.ch



Close – OK

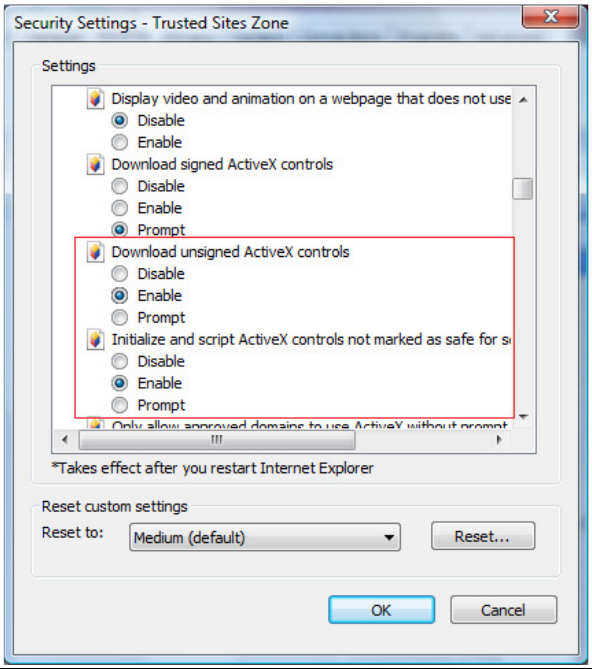
Puis ouvrir http://ca.tdeig.ch avec IE7

On obtient l'avertissement suivant :



Il ne reste plus qu'à autoriser les contrôles ActiveX (voir ci-dessous) pour la zone **Trusted sites** !
Cela est d'ailleurs préférable d'un point de vue sécurité, plutôt que d'autoriser pour tous les sites web ces contrôles ActiveX qui ne sont pas marqués comme sûrs !!

Tools – Internet Options – onglet Security – Trusted sites - Custom level…
Modifier les valeurs ci-dessous :



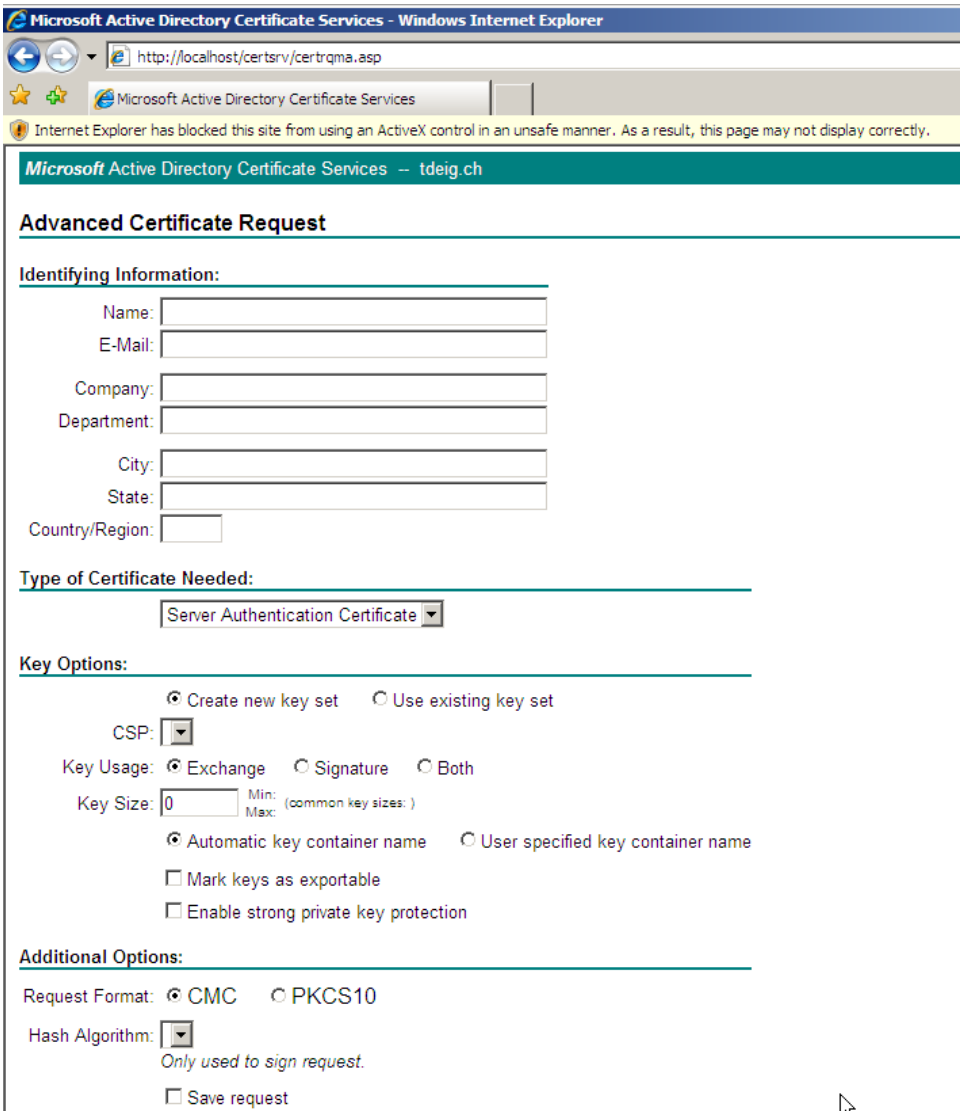
Création du certificat serveur
L'objectif est de créer une connexion SSL (https) sur le site web de la CA, et pour cela on a besoin de se faire délivrer un certificat serveur.

On va donc demander à la CA (nommée LaboTD) de nous délivrer un certificat serveur que l'on puisse associer à notre site web

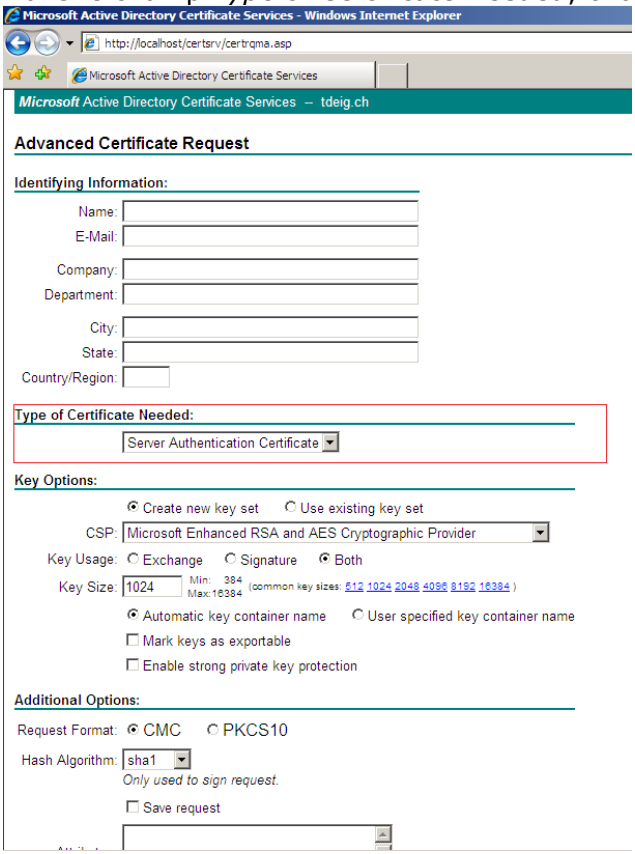
Cette opération a pu se faire depuis le navigateur du serveur (ici c'est le même PC que la CA), en se connectant sur http://localhost/certsrv (ajouter ce site dans la zone *Trusted* et activer les contrôles ActiveX, voir pages 10-11)

Cliquer sur *Request a certificate – advanced certificate request – Create and submit a request to this CA*

On obtient le formulaire ci-dessous que l'on doit compléter (le champ Name est nécessaire) :



Dans le champ *Type of Certificate Needed*, choisir ***Server Authentication Certificate***



Cliquer sur submit pour soumettre la demande à la CA

7 Configurer le DNS

Se connecter au DNS debian via par exemple vShere Client (IP=10.1.1.52)
Modifier le fichier **/etc/bind/db.tdeig**

Attention, les espaces sont des TAB :

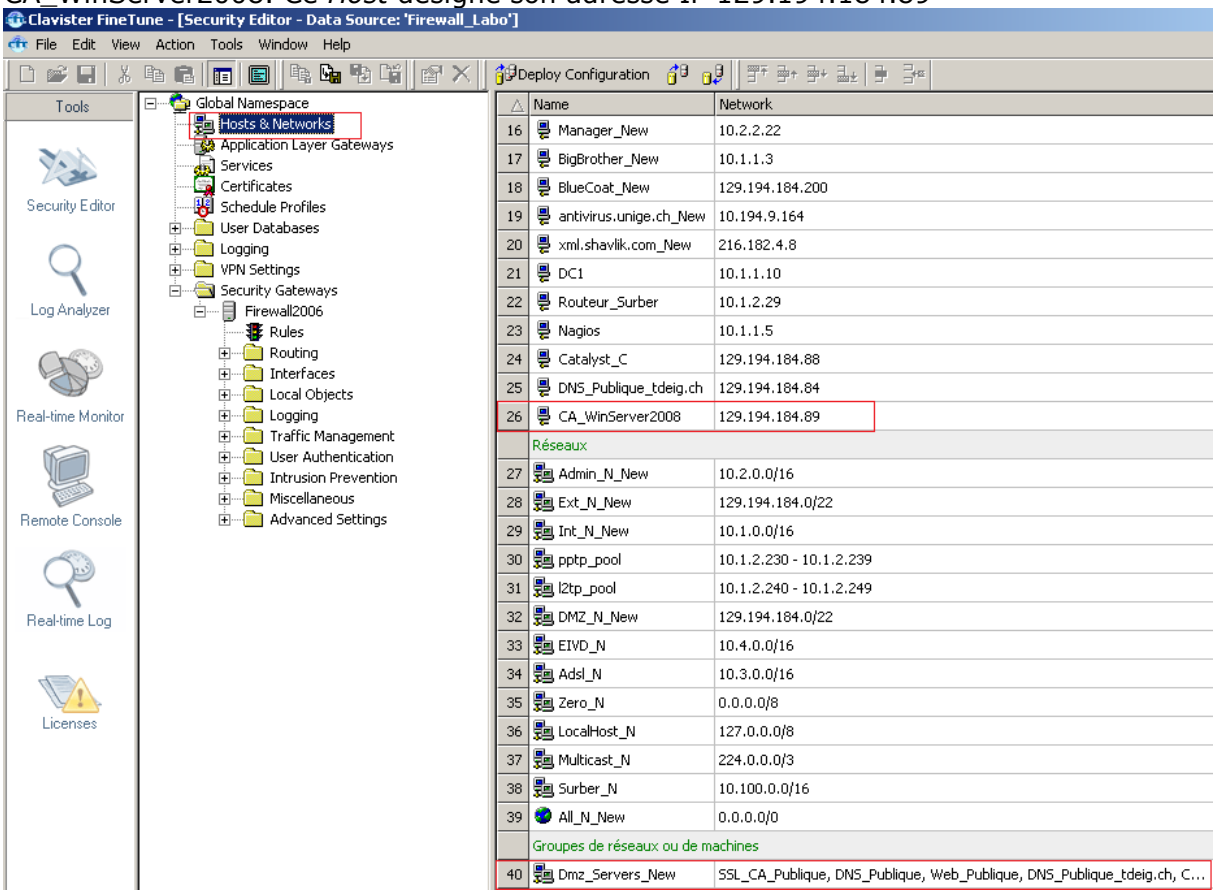
```
;
; BIND data file for tdeig.ch
;
$TTL    604800
@       IN      SOA     ns1.tdeig.ch. root.tdeig.ch. (
   6            ; Serial
                         604800         ; Refresh
                          86400         ; Retry
                        2419200         ; Expire
                         604800 )       ; Negative Cache TTL
;

        NS      ns1.tdeig.ch.
;*      A       129.194.184.80
;tdeig.ch.      A       129.194.184.80
ns1     A       129.194.184.84
www     A       129.194.184.80
ftp     A       129.194.184.80
secure  A       129.194.184.81
ca      A       129.194.184.89
lb      A       129.194.184.92
lb      A       129.194.184.93
lb      A       129.194.184.94
```

Redémarrer le service bind9
/etc/init.d/bind9 restart

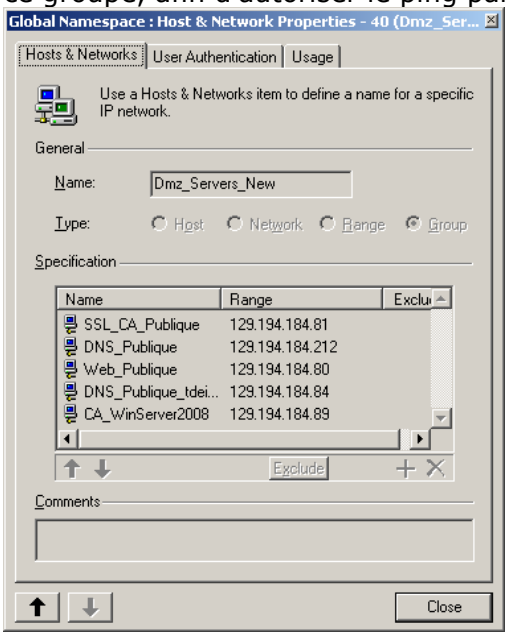
8 Configuration du firewall Clavister

Il a fallu ajouter des règles sur le firewall du labo pour permettre de communiquer avec la nouvelle CA

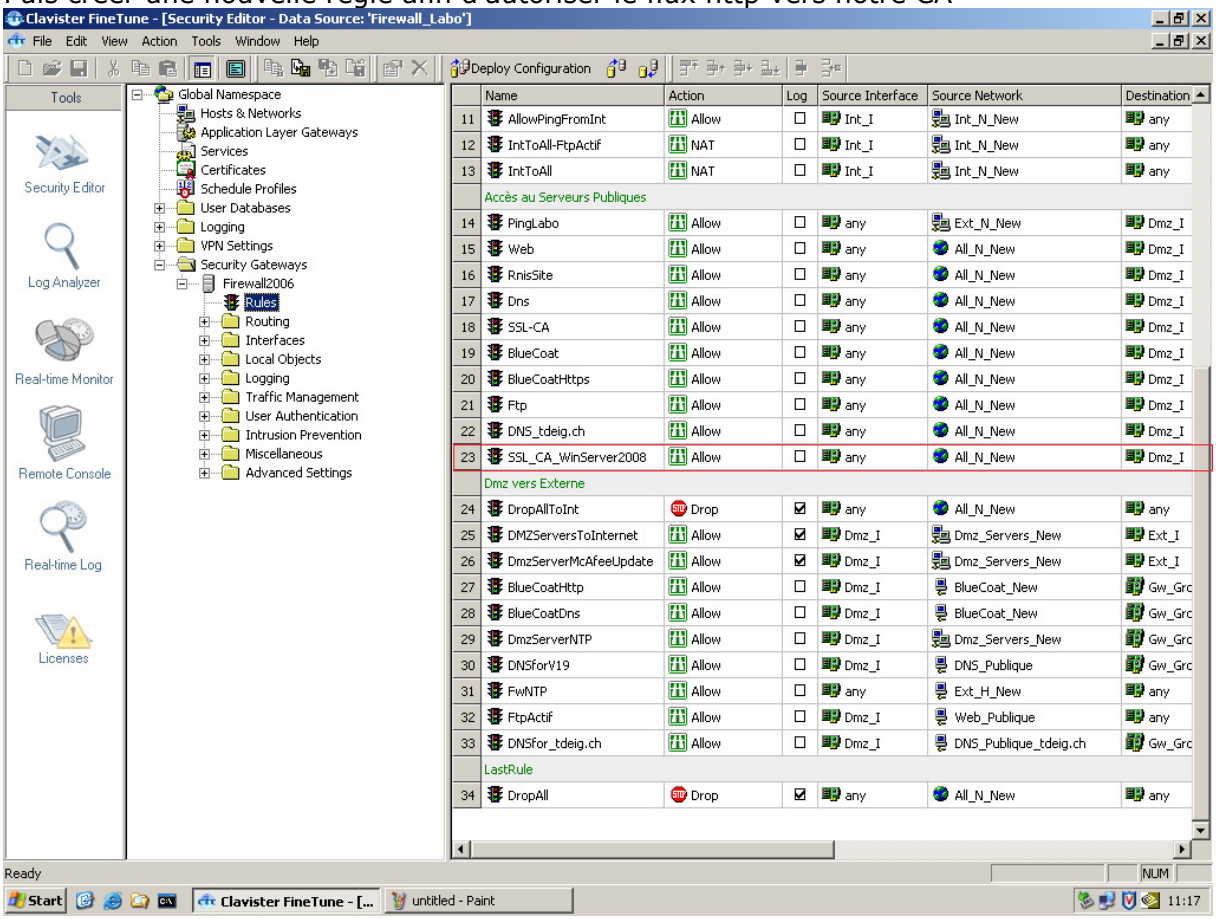
Aller sur le Manager, puis créer un nouveau *Host* sous *Hosts & Networks*, que j'ai nommé CA_WinServer2008. Ce *Host* désigne son adresse IP 129.194.184.89

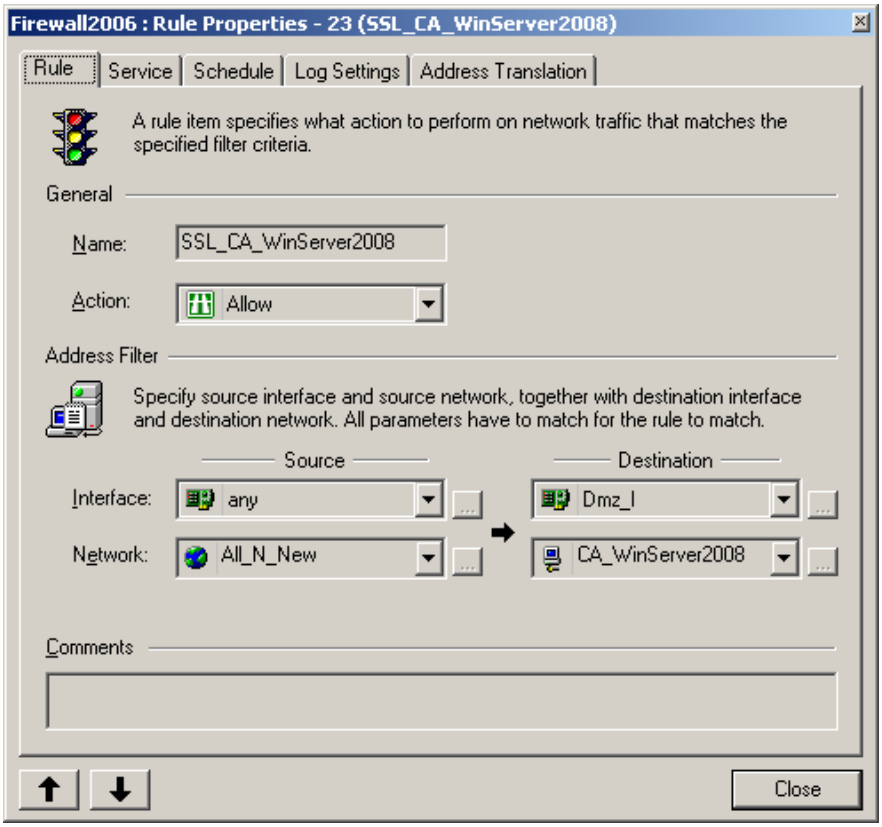


On va aussi ajouter notre Host au groupe de serveurs DMZ (des règles sont créées pour ce groupe, afin d'autoriser le ping par exemple)



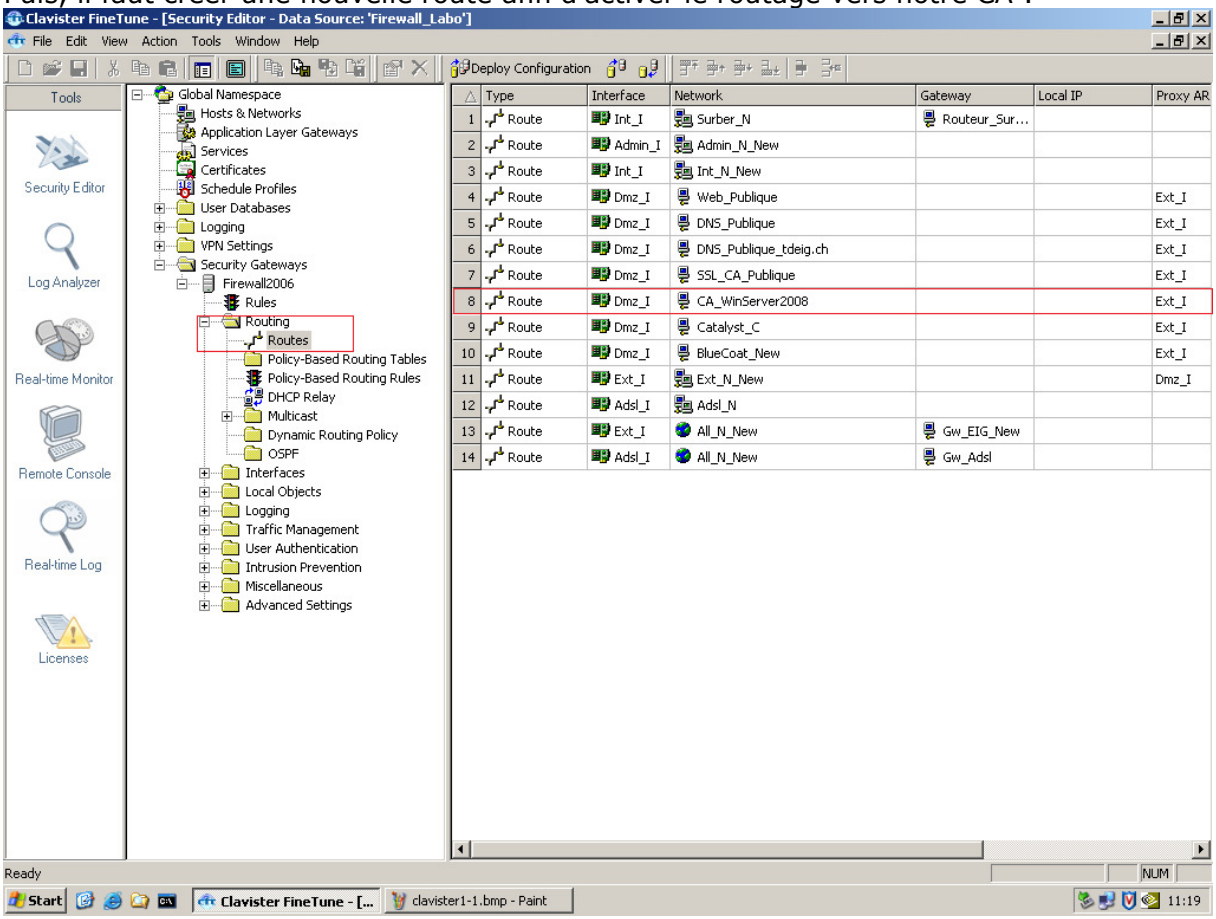
Puis créer une nouvelle règle afin d'autoriser le flux http vers notre CA

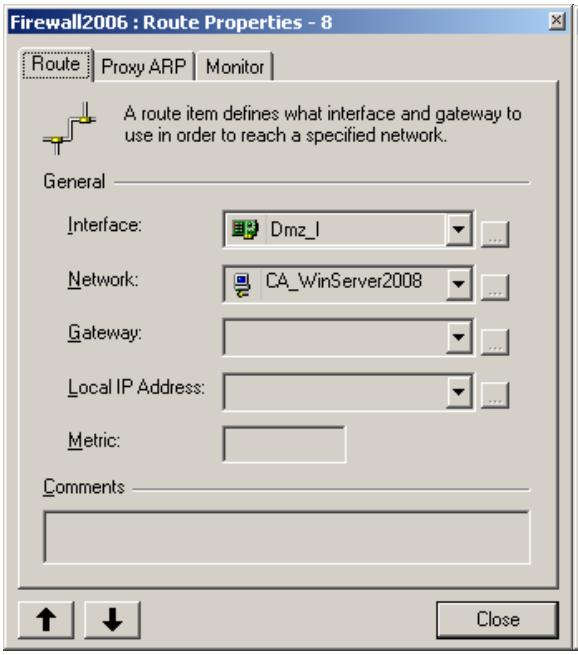


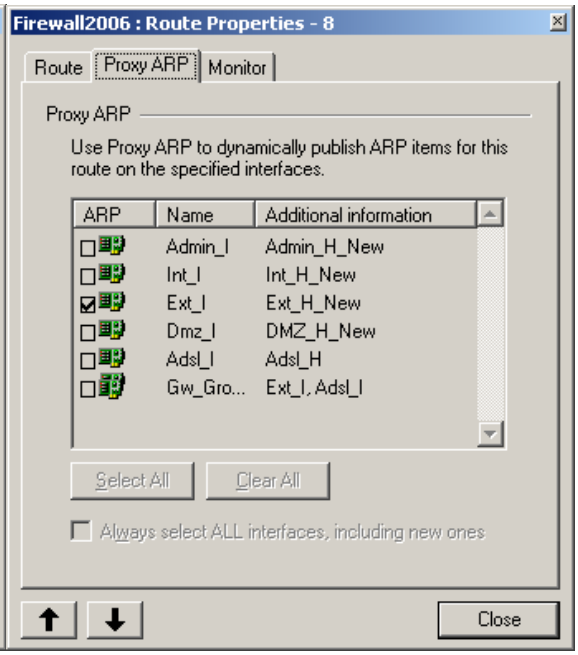


Sous l'onglet *Service* ci-dessus, sélectionner http-in-all

Puis, il faut créer une nouvelle route afin d'activer le routage vers notre CA :







Il ne reste plus qu'à uploader la nouvelle config sur le firewall !