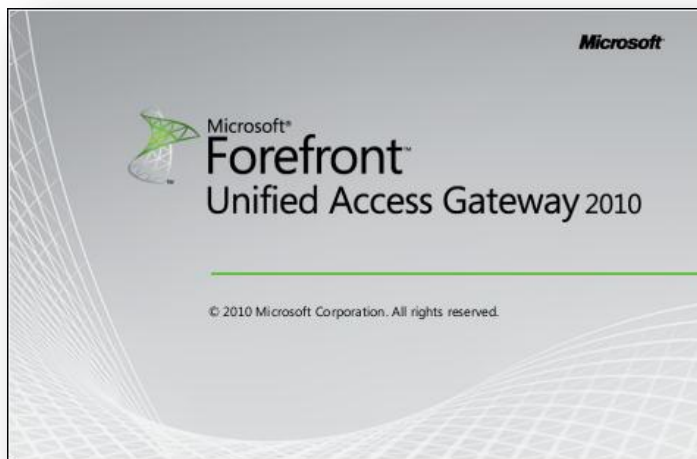


Microsoft Forefront UAG 2010 SP1

Mise en œuvre d'une plateforme DirectAccess pas à pas - PKI

Advanced architecture and Design for DirectAccess



jeudi, 14 avril 2011

Version 1.2

Rédigé par

benoits@exakis.com

MVP Enterprise Security 2010

Benois@exakis.com

© 2009 Microsoft Corporation. All rights reserved. *MICROSOFT CONFIDENTIAL – FOR INTERNAL USE ONLY*. The information contained in this document represents the current view of Microsoft Corporation on the issues discussed as of the date of publication and is subject to change at any time without notice to you. This document and its contents are provided AS IS without warranty of any kind, and should not be interpreted as an offer or commitment on the part of Microsoft, and Microsoft cannot guarantee the accuracy of any information presented. MICROSOFT MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft Corporation.

Microsoft may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The descriptions of other companies' products in this document, if any, are provided only as a convenience to you. Any such references should not be considered an endorsement or support by Microsoft. Microsoft cannot guarantee their accuracy, and the products may change over time. Also, the descriptions are intended as brief highlights to aid understanding, rather than as thorough coverage. For authoritative descriptions of these products, please consult their respective manufacturers.

We will not knowingly provide advice that conflicts with local, regional, or international laws, however, it is your responsibility to confirm your implementation of our advice is in accordance with all applicable laws.



Fiche de révision et de signature

Historique des versions

Date	Auteur	Version	Modification
16/01/2011	Benoît SAUTIERE	1.2	Corrections mineures
20/11/2010	Benoît SAUTIERE	1.1	Découpage en parties
06/11/2010	Benoît SAUTIERE	1.0	Création du document

Relecteur

Nom	Version approuvée	Fonction	Date
Benoît SAUTIERE	1.2	MVP Enterprise Security	16/01/2011
Benoît SAUTIERE	1.1	MVP Enterprise Security	20/11/2010
Benoît SAUTIERE	1.0	MVP Enterprise Security	06/11/2010

Sommaire

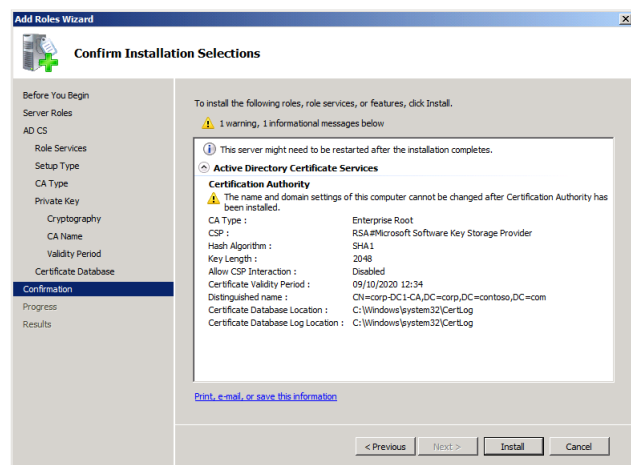
4	<i>Préparation Active Directory Certificates Services</i>	3
4.1	Installation.....	3
4.2	Publication de la CRL	4
4.3	Subtilité de la sauvegarde de la clé privée.....	7
4.4	Subtilité du Health Registration Authority.....	8
4.5	Subtilité du Health Registration Authority bis repetita	9
5	<i>Préparation des gabarits de certificat</i>	10
5.1	Certificats d'authentification IPSEC.....	10
5.2	Certificats d'état de santé	13
5.3	Certificat Network Location Server	16
5.4	Activation de l'auto-Enrollment.....	19

4 PREPARATION ACTIVE DIRECTORY CERTIFICATES SERVICES

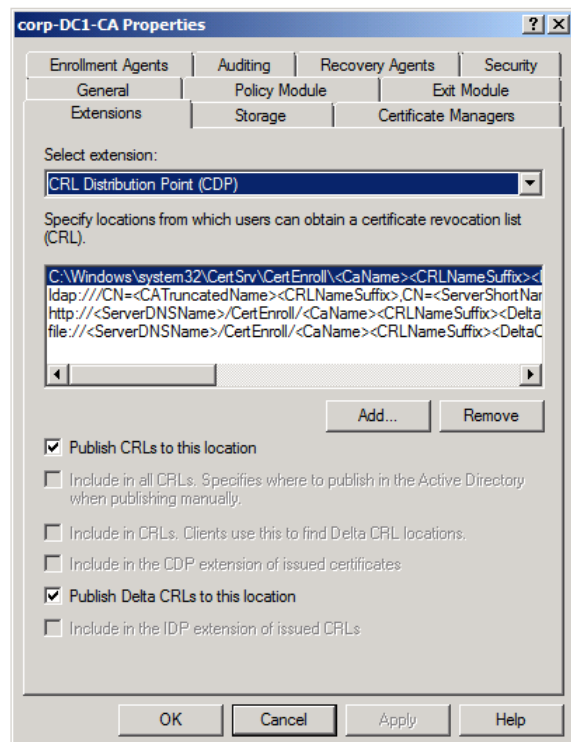
4.1 Installation

Dans le cadre de notre plateforme de démonstration de DirectAccess, nous avons besoin d'une autorité de certification. Etant donné que nous ne sommes pas dans le cadre d'un environnement de production, nous pouvons nous permettre des écarts tels que la non mise hors ligne de l'autorité racine de confiance dite « Root ». Par contre, on ne va pas faire l'impasse sur la publication des listes de révocation sur un serveur distinct. Voilà ci-dessous le résumé de mon installation du rôle ADCS.

Installer le rôle ADCS c'est bien mais correctement publier les listes de révocation, c'est mieux. Pour cela, un peu de travail est nécessaire. Lorsqu'on observe la configuration par défaut de l'autorité de certification nouvellement installée, on constate que les listes de révocation sont publiées sous plusieurs formes (fichier, http et même LDAP).

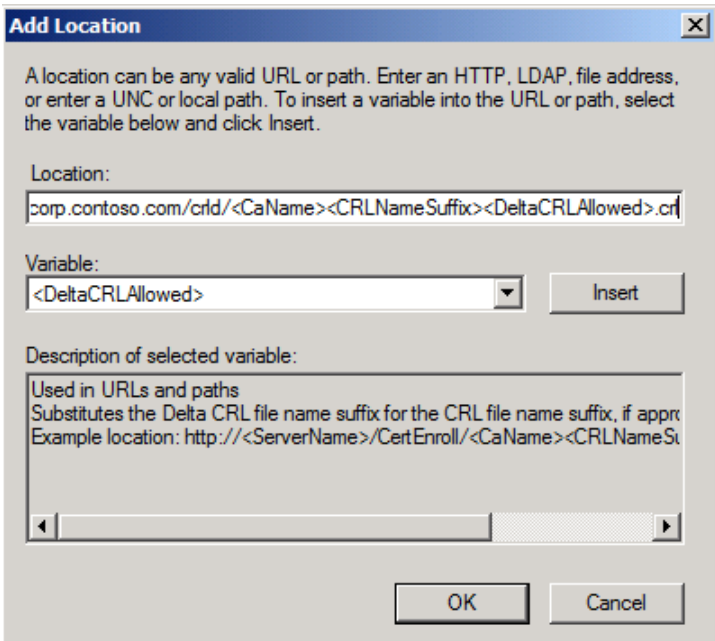
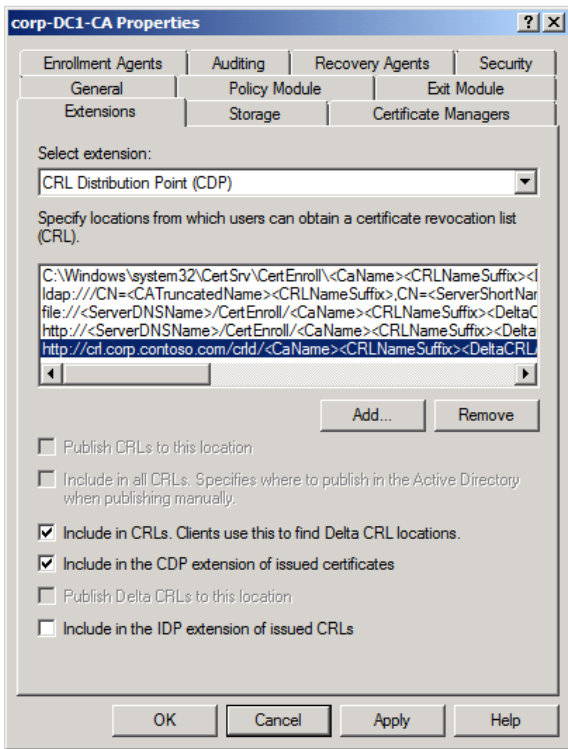


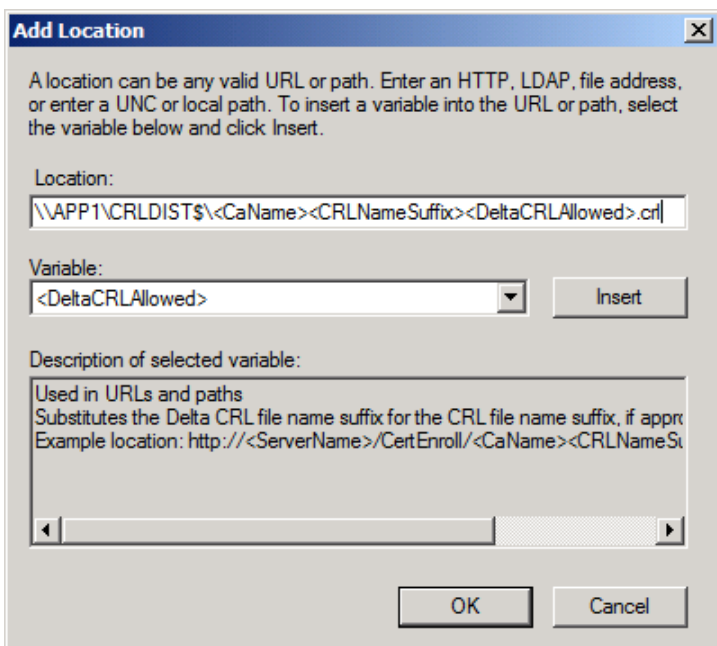
Pendant cette configuration pose un problème. Il sera référencé que la révocation des certificats émis pourra être validée en http. Pourtant, il n'y a pas de serveur web sur mon contrôleur de domaine (c'est le mal!).



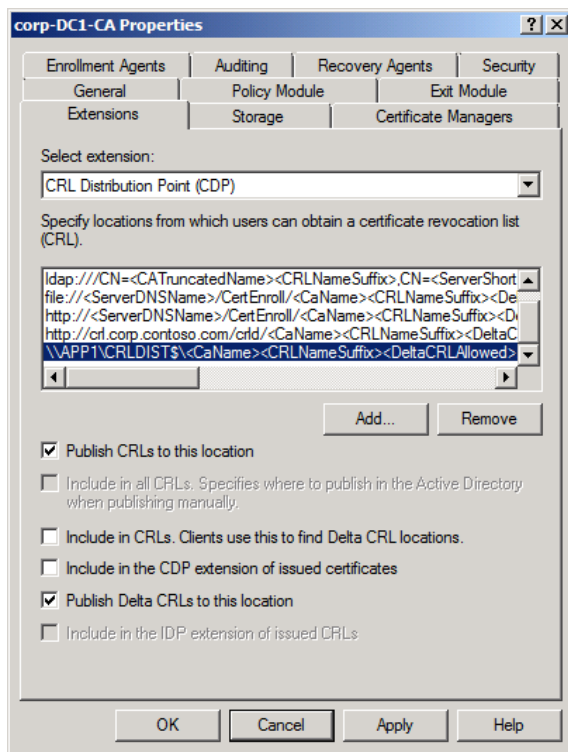
4.2 Publication de la CRL

Pour finaliser l'installation de l'autorité de certification, il faut donc publier les listes de révocation mais pas sur le même serveur. Dans les scénarios classiques de déploiement d'une autorité de certification, celle-ci est mise hors ligne. Or, comment peut-on accéder aux listes de révocation si celles-ci sont hébergées sur un serveur inaccessible. On va donc s'assurer que nos listes de révocation soient publiées sur le serveur APP1.

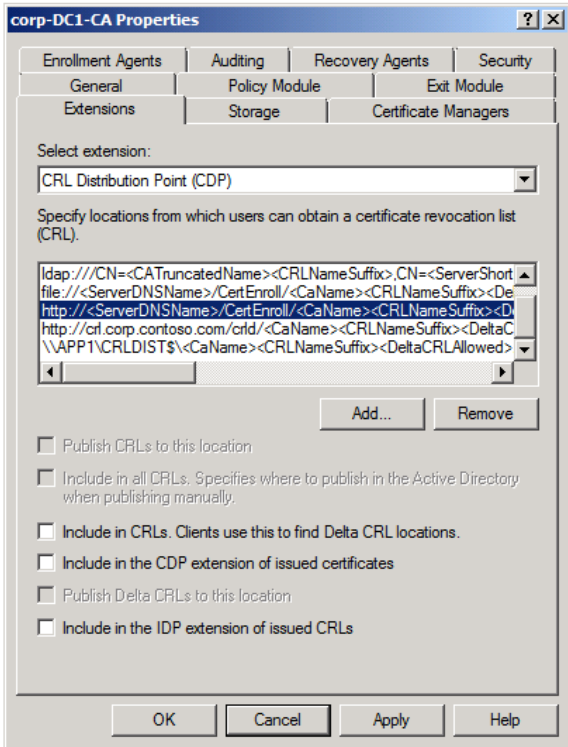
Impression écran	Description
	<p>On a vu que la publication http n'est pas conforme. On va donc la remplacer par une nouvelle qui va référencer : <code>http://crl.corp.contoso.com/crld/<CaName><CRLNameSuffix><DeltaCRLAllowed>.crl</code> comme emplacement de publication.</p>
	<p>Pour cette première extension, les cases à cocher « Include in CRLs. Clients use this to find Delta CRL locations » et « Include in the CDP extensions of issued certificates » doivent être cochées.</p>



Pour la seconde extension, on va indiquer à l'autorité de certification à quel emplacement publier ses listes de révocation.

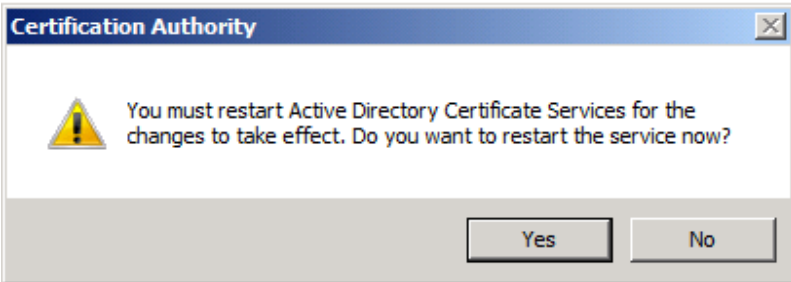


Ce nouvel emplacement doit permettre de publier à la fois la CRL mais aussi la CRL Delta.



The image shows the 'corp-DC1-CA Properties' dialog box, specifically the 'General' tab. The 'Select extension:' dropdown is set to 'CRL Distribution Point (CDP)'. Below it, a list of CRL locations is shown, with the following URL selected: 'http://<ServerDNSName>/CertEnroll/<CaName><CRLNameSuffix><DeltaCRLAllowed>'. There are 'Add...' and 'Remove' buttons. At the bottom, there are 'OK', 'Cancel', 'Apply', and 'Help' buttons.

Il ne nous reste plus qu'à supprimer le point de distribution initial.



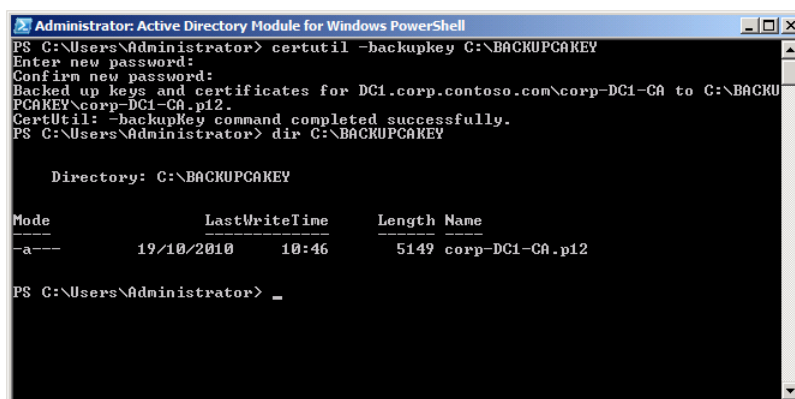
The image shows a 'Certification Authority' warning dialog box. It contains a yellow warning icon and the text: 'You must restart Active Directory Certificate Services for the changes to take effect. Do you want to restart the service now?'. There are 'Yes' and 'No' buttons at the bottom.

Il est nécessaire de redémarrer l'autorité de certification pour les modifications soient prises en compte.

A ce stade, l'autorité de certification est presque prête. Le serveur APP1 n'étant pas encore opérationnel, on devra attendre son installation pour finaliser la publication de la liste de révocation.

4.3 Subtilité de la sauvegarde de la clé privée

Jusqu'à Windows 2003, l'outil de sauvegarde de Microsoft prenait en charge la sauvegarde de l'autorité de certification sans aucun problème. C'est toujours vrai sous Windows Server 2008/2008 R2, avec une petite subtilité. L'emplacement de stockage de la clé privée ayant été déplacé dans le répertoire caché suivant : « %systemdrive%\ProgramData\Microsoft\Crypto\Keys ». La conséquence, c'est que l'outil de sauvegarde Windows Server Backup n'est plus en mesure de sauvegarder cette clé privée, ce qui est plutôt gênant. On va donc s'assurer de la sauvegarde de la clé privée.



```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> certutil -backupkey C:\BACKUPCAKEY
Enter new password:
Confirm new password:
Backed up keys and certificates for DC1.corp.contoso.com\corp-DC1-CA to C:\BACKU
PCAKEY\corp-DC1-CA.p12.
CertUtil: -backupkey command completed successfully.
PS C:\Users\Administrator> dir C:\BACKUPCAKEY

Directory: C:\BACKUPCAKEY

Mode                LastWriteTime         Length Name
----                -
-a-----          19/10/2010   10:46           5149 corp-DC1-CA.p12

PS C:\Users\Administrator> _
```

La sauvegarde de la clé privée de l'autorité de certification est essentielle car sans elle, il ne sera pas possible d'effectuer une restauration ou une migration vers un autre système. La recommandation est bien entendu de conserver la clé privée ainsi que le mot de passe associé de manière sécurisée et non la laisser sur le serveur.

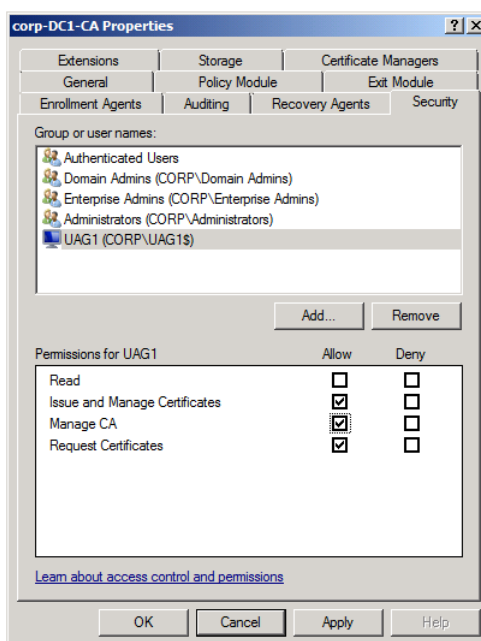
4.4 Subtilité du Health Registration Authority

La PKI est pleine de subtilité, surtout lorsqu'on s'attaque à des sujets comme DirectAccess et Network Access Protection. Quand on s'attaque aux deux, c'est évident que cela ne sera pas simple. Le Health Registration Authority sera l'interface au travers de laquelle le client NAP va se voir attribuée un certificat prouvant son bon état de santé. Pour cela, notre HRA devra disposer des privilèges nécessaires sur l'autorité de certification. On peut distinguer deux scénarios :

- Le rôle HRA est installé sur un serveur distinct de l'autorité de certification
- Le rôle HRA est installé sur le même serveur que l'autorité de certification

Dans le premier cas, il faut positionner des permissions pour le compte ordinateur hébergeant le rôle HRA. Dans le second cas, il faut positionner des permissions pour le compte « Network Service ». Dans les deux cas, les permissions sont les mêmes, à savoir :

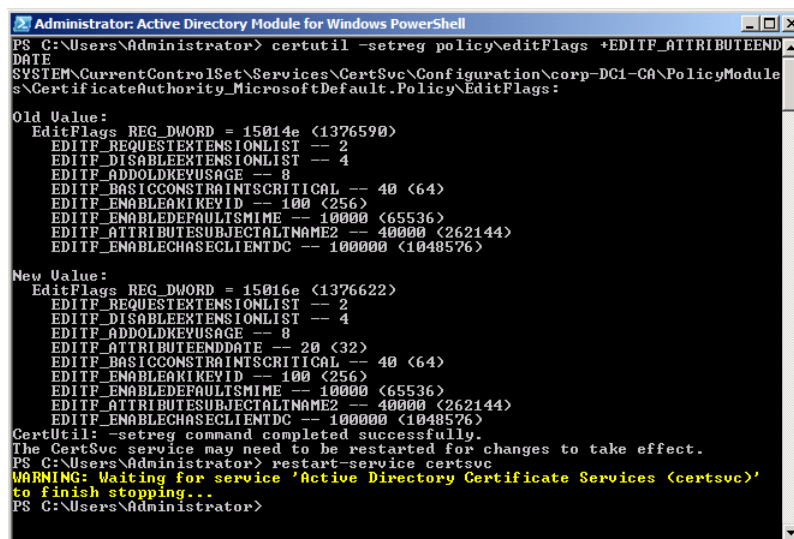
- Issue and Manage Certificates
- Manage CA
- Request Certificates



Note : Le rôle HRA aura aussi pour responsabilité de révoquer les certificats correspondants à des clients NAP ne présentant plus le niveau de conformité requis.

4.5 Subtilité du Health Registration Authority bis repetita

Lorsque le Health Registration Authority va demander un certificat d'état de santé pour le compte d'un poste de travail, sa demande est un peu particulière puisqu'il demande un certificat pour une durée de vie inférieure à la durée inscrite dans le gabarit du certificat. Par défaut, notre autorité de certification ignore cette subtilité. Il faut donc la reconfigurer pour prendre en compte ce besoin.



```
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> certutil -setreg policy\editFlags +EDITF_ATTRIBUTEEND
DATE
SYSTEM\CurrentControlSet\Services\CertSvc\Configuration\corp-DC1-CA\PolicyModule
s\CertificateAuthority_MicrosoftDefault.Policy>EditFlags:
Old Value:
EditFlags REG_DWORD = 15014e (1376590)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_DISABLEEXTENSIONLIST -- 4
EDITF_ADDOLDKEYUSAGE -- 8
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEAKIKEYID -- 100 (256)
EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
EDITF_ENABLECHASECLIENITDC -- 100000 (1048576)
New Value:
EditFlags REG_DWORD = 15016e (1376622)
EDITF_REQUESTEXTENSIONLIST -- 2
EDITF_DISABLEEXTENSIONLIST -- 4
EDITF_ADDOLDKEYUSAGE -- 8
EDITF_ATTRIBUTEENDDATE -- 20 (32)
EDITF_BASICCONSTRAINTSCRITICAL -- 40 (64)
EDITF_ENABLEAKIKEYID -- 100 (256)
EDITF_ENABLEDEFAULTSMIME -- 10000 (65536)
EDITF_ATTRIBUTESUBJECTALTNAME2 -- 40000 (262144)
EDITF_ENABLECHASECLIENITDC -- 100000 (1048576)
CertUtil: -setreg command completed successfully.
The CertSvc service may need to be restarted for changes to take effect.
PS C:\Users\Administrator> restart-service certsvc
WARNING: Waiting for service 'Active Directory Certificate Services (certsvc)'
to finish stopping...
PS C:\Users\Administrator>
```

Une fois l'opération réalisée et l'autorité de certification redémarrée, on peut passer à la suite, à savoir les gabarits de certificats.

5 PREPARATION DES GABARITS DE CERTIFICAT

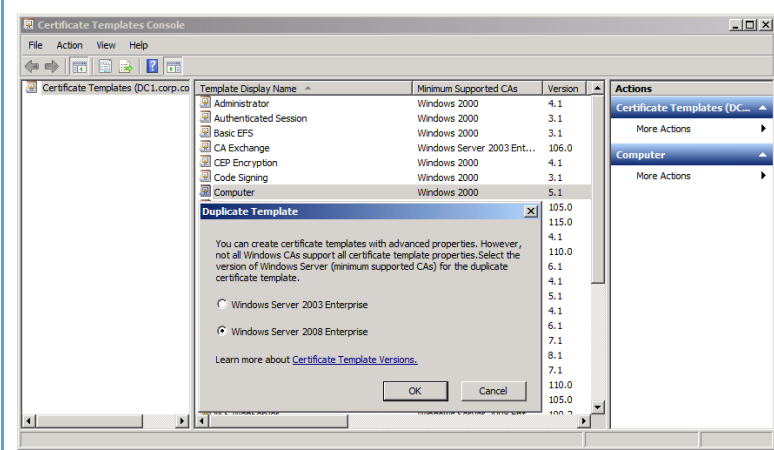
Notre autorité de certification doit mettre à disposition plusieurs gabarits de certificats :

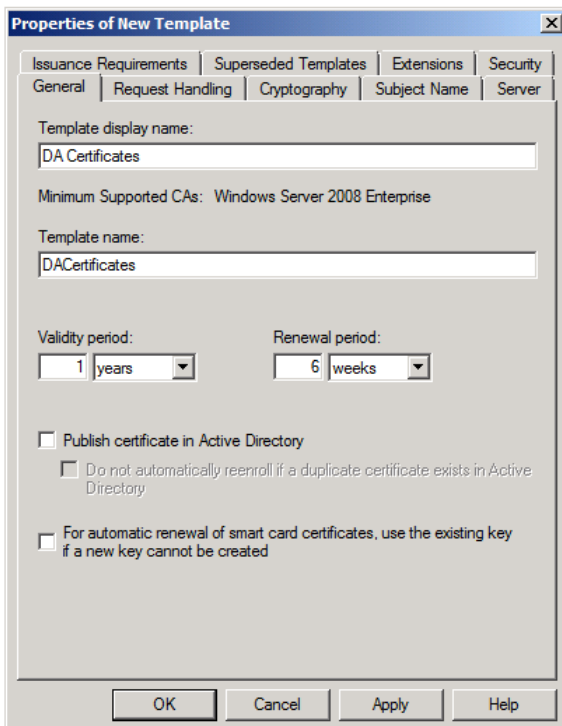
- Un gabarit de certificat permettant aux systèmes de s'authentifier
- Un gabarit de certificat permettant aux systèmes de prouver leur état de santé
- Un gabarit de certificat pour le Network Location Server

Dans les trois cas, nous allons dériver des gabarits de certificats standards pour développer nos propres gabarits, intégrant nos besoins.

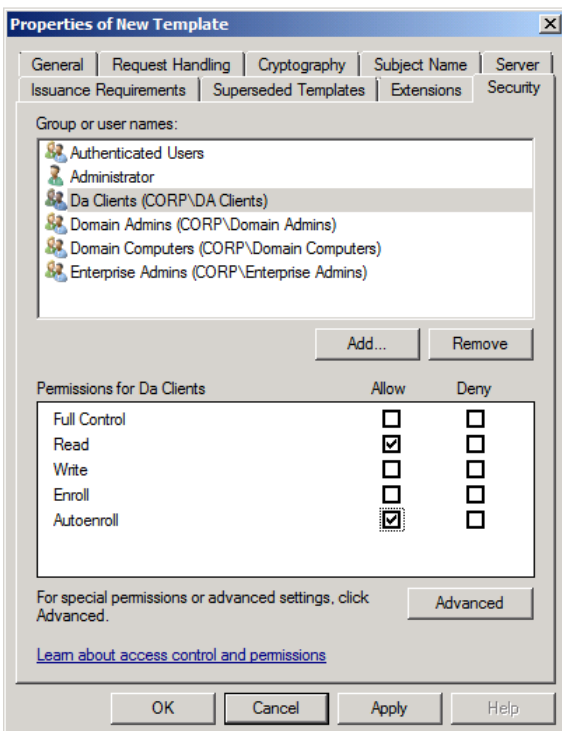
5.1 Certificats d'authentification IPSEC

A ce niveau, on aurait presque pu utiliser le gabarit de certificat « Computer » initialement mis à disposition par l'autorité de certification. Cependant, nous allons tout de même mettre en place un gabarit de certificat personnalisé, même s'il ne contient aucune personnalisation.

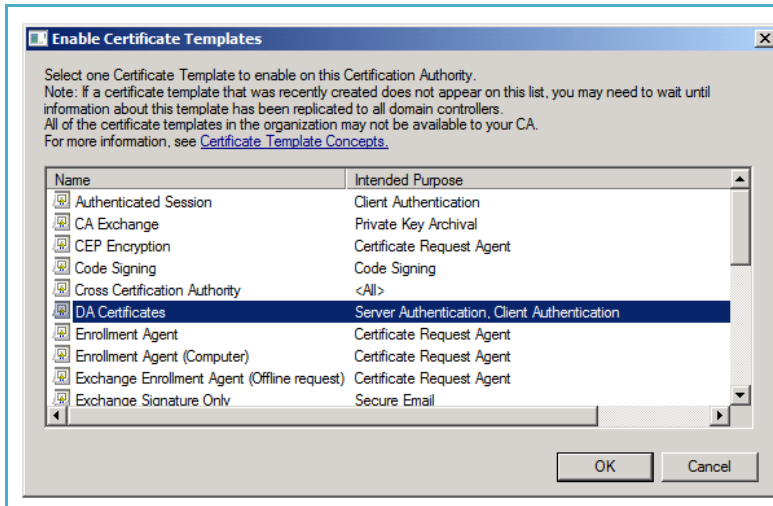
Impression écran	Description
	<p>On va donc commencer par dupliquer notre gabarit Computer pour y intégrer notre personnalisation.</p>



On va nommer notre gabarit de certificat de manière clairement identifiable.



Des permissions sont positionnées sur le gabarit de certificat. Les membres du groupe « DA Clients » pourront obtenir un certificat automatiquement.

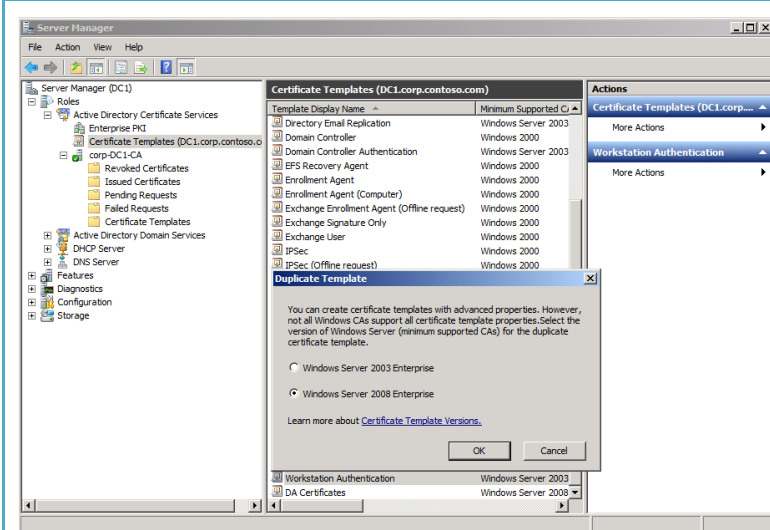
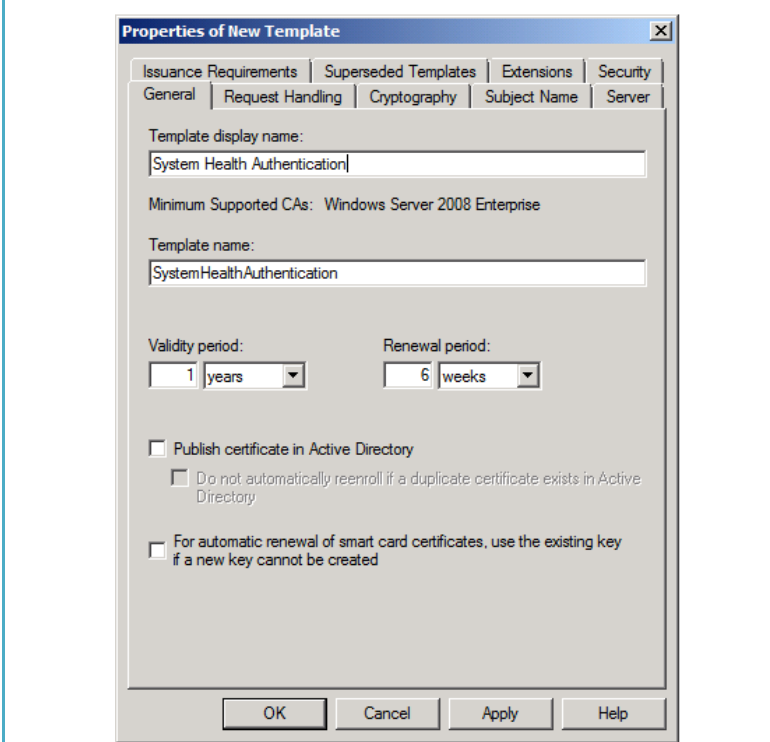


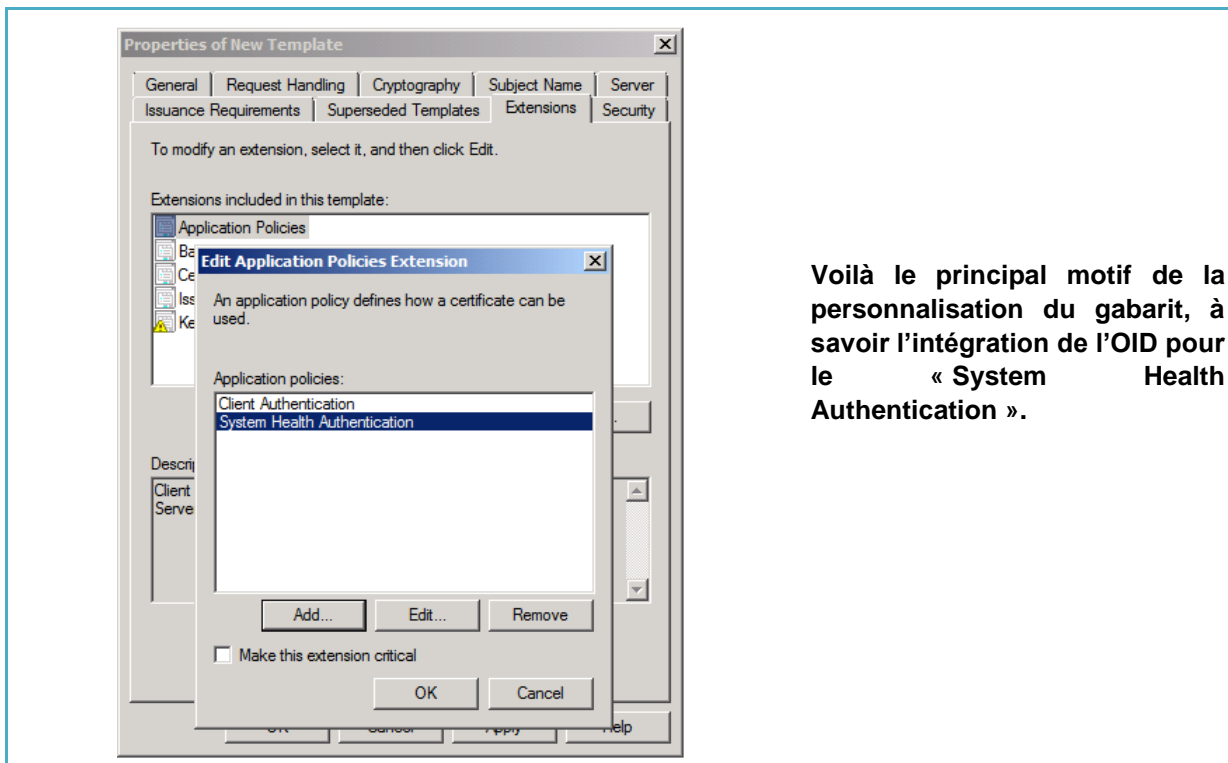
Maintenant que le gabarit est prêt, encore faut-il le publier.

5.2 Certificats d'état de santé

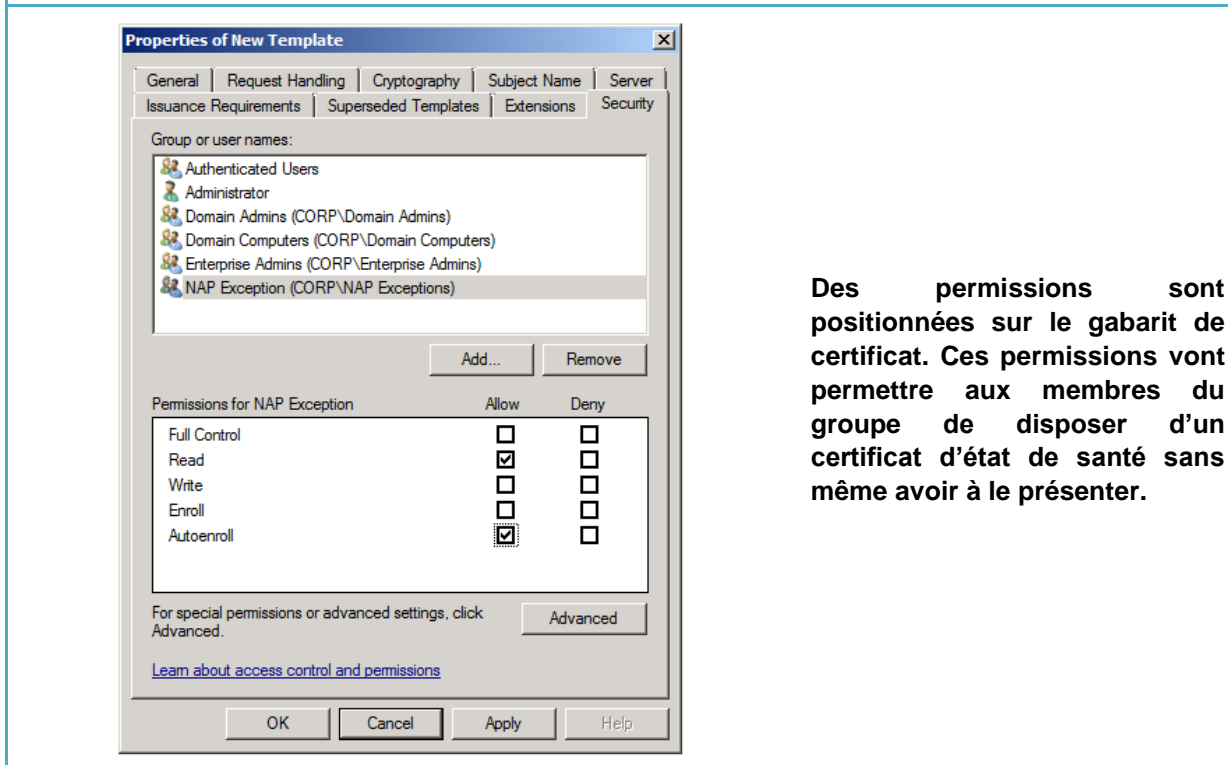
Dans une infrastructure Network Access Protection, les systèmes doivent soumettre leur état de santé à un serveur central pour interprétation. Dans le cas DirectAccess, c'est le Health Registration Authority qui reçoit l'état de santé. Si l'état de santé est conforme aux exigences imposées par le Network Policy Server, alors un certificat d'état de santé doit être délivré. Le client va utiliser ce certificat dans le tunnel IPSEC utilisateur / application de DirectAccess. Coté certificat, ce n'est ni plus ni moins qu'un gabarit de certificat « Computer » que l'on va personnaliser pour intégrer :

- L'OID 1.3.6.1.4.1.311.47.1.1 représentant le System Health Authentication
- La mise en place d'un filtrage pour les exceptions à la soumission de l'état de santé

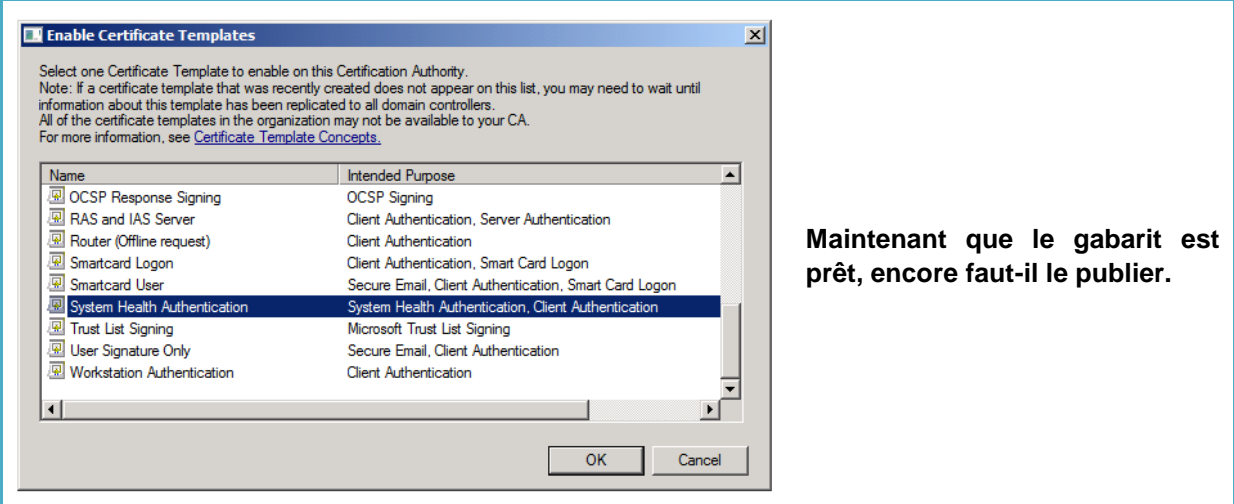
Impression écran	Description
	<p>On va donc commencer par dupliquer notre « Workstation Authentication » pour y intégrer nos personnalisations.</p>
	<p>Ce gabarit sera nommé « System Health Authentication »</p>



Voilà le principal motif de la personnalisation du gabarit, à savoir l'intégration de l'OID pour le « System Health Authentication ».



Des permissions sont positionnées sur le gabarit de certificat. Ces permissions vont permettre aux membres du groupe de disposer d'un certificat d'état de santé sans même avoir à le présenter.



Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see [Certificate Template Concepts](#).

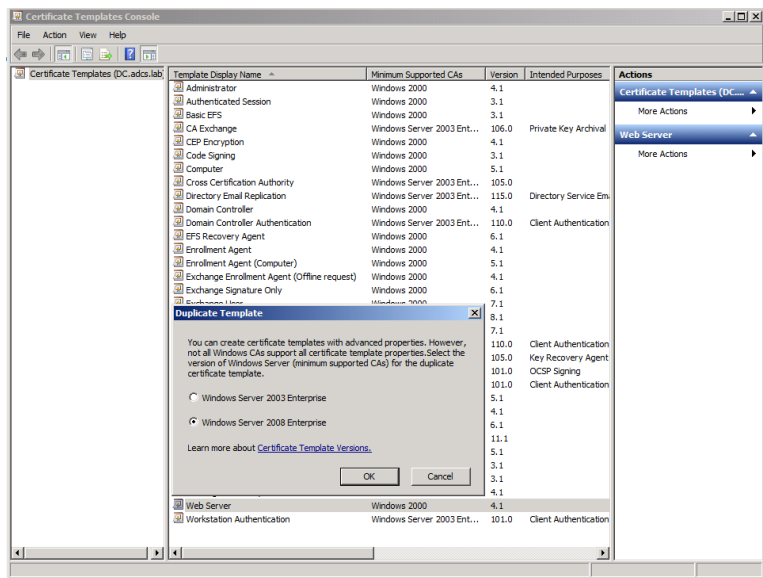
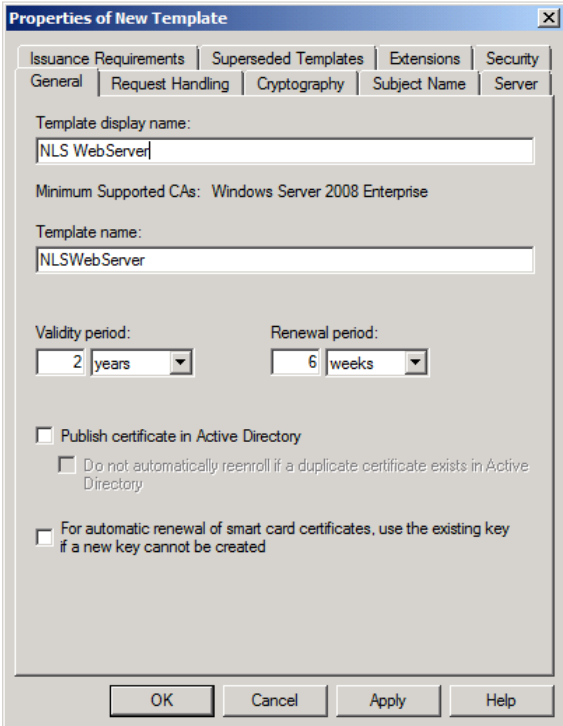
Name	Intended Purpose
OCSP Response Signing	OCSP Signing
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon
System Health Authentication	System Health Authentication, Client Authentication
Trust List Signing	Microsoft Trust List Signing
User Signature Only	Secure Email, Client Authentication
Workstation Authentication	Client Authentication

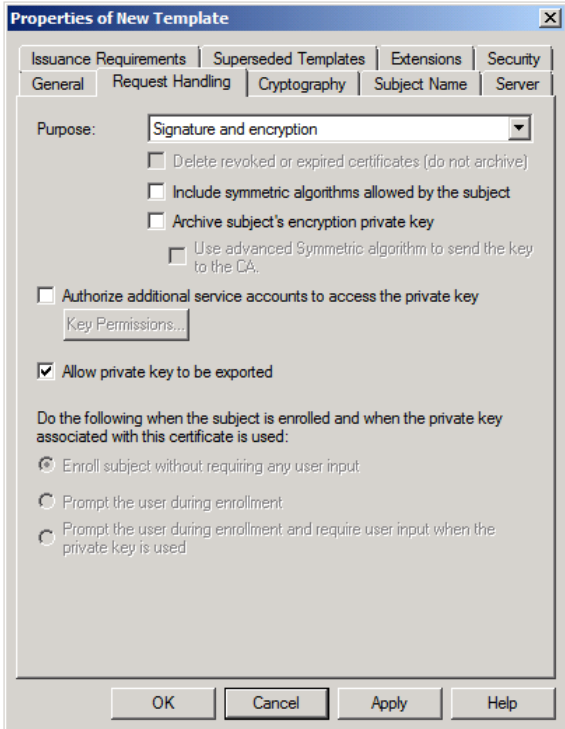
OK Cancel

Maintenant que le gabarit est prêt, encore faut-il le publier.

5.3 Certificat Network Location Server

Notre autorité de certification devra délivrer un certain nombre de certificats. L'un des usages sera de proposer des certificats de serveurs web (SSL). Dans le domaine des infrastructures à clés publiques, c'est une bonne pratique de ne pas personnaliser les gabarits standards et donc de réaliser les personnalisations dans des gabarits de certificats dédiés.

Impression écran	Description
	<p>On va donc commencer par dupliquer notre gabarit Web Server pour y intégrer nos personnalisations.</p>
	<p>On va nommer notre gabarit de certificat de manière clairement identifiable.</p>



Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security

General | Request Handling | Cryptography | Subject Name | Server

Purpose: **Signature and encryption**

- Delete revoked or expired certificates (do not archive)
- Include symmetric algorithms allowed by the subject
- Archive subject's encryption private key
 - Use advanced Symmetric algorithm to send the key to the CA.
- Authorize additional service accounts to access the private key
Key Permissions...
- Allow private key to be exported

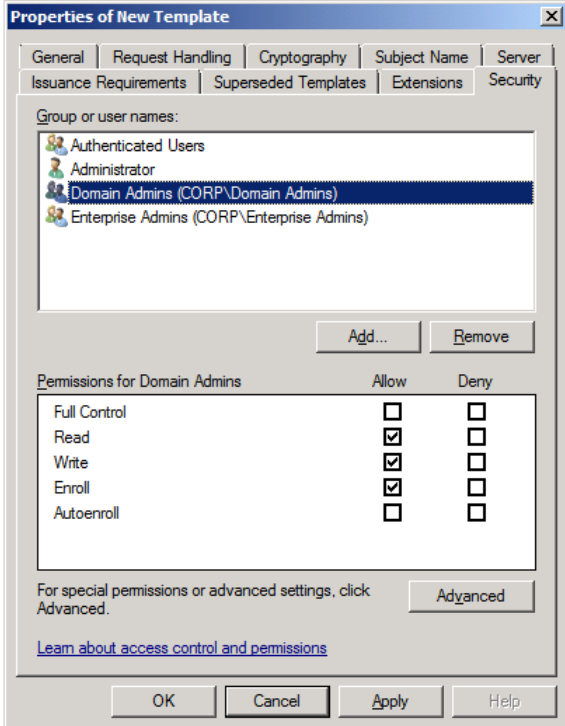
Do the following when the subject is enrolled and when the private key associated with this certificate is used:

- Enroll subject without requiring any user input
- Prompt the user during enrollment
- Prompt the user during enrollment and require user input when the private key is used

OK Cancel Apply Help

Voilà le principal motif de la personnalisation du gabarit, à savoir la capacité à exporter la clé privée du certificat.

Dans le cadre de la mise en œuvre de DirectAccess, cela peut s'avérer utile pour la mise en haute disponibilité du Network Location Server.



Properties of New Template

General | Request Handling | Cryptography | Subject Name | Server

Issuance Requirements | Superseded Templates | Extensions | Security

Group or user names:

- Authenticated Users
- Administrator
- Domain Admins (CORP\Domain Admins)**
- Enterprise Admins (CORP\Enterprise Admins)

Add... Remove

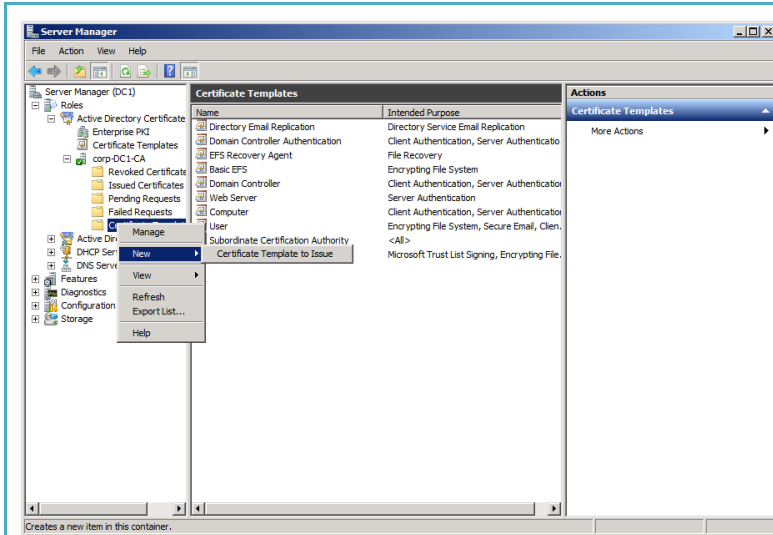
Permissions for Domain Admins	Allow	Deny
Full Control	<input type="checkbox"/>	<input type="checkbox"/>
Read	<input type="checkbox"/>	<input type="checkbox"/>
Write	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Enroll	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Autoenroll	<input type="checkbox"/>	<input type="checkbox"/>

For special permissions or advanced settings, click Advanced.

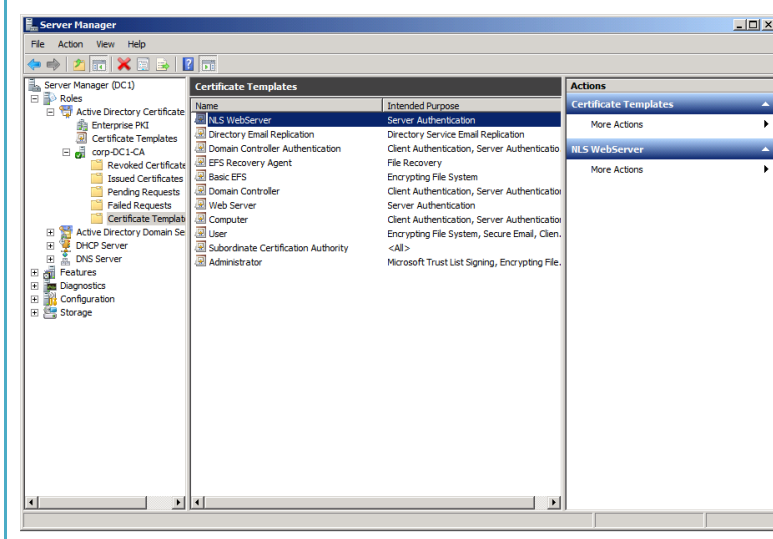
[Learn about access control and permissions](#)

OK Cancel Apply Help

Des permissions sont positionnées sur le gabarit de certificat. Mon infrastructure de clés publiques ne respectant déjà pas la mise hors ligne de la racine, je n'ai pas non plus effectué la séparation des rôles, encore moins la mise en œuvre de la délégation, honte à moi !



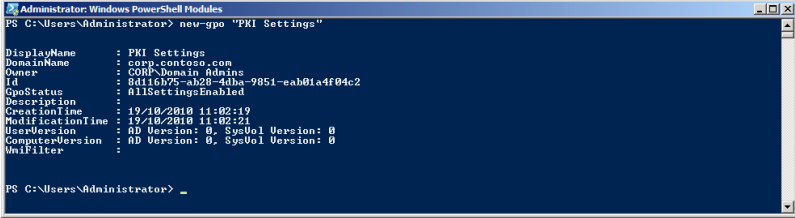
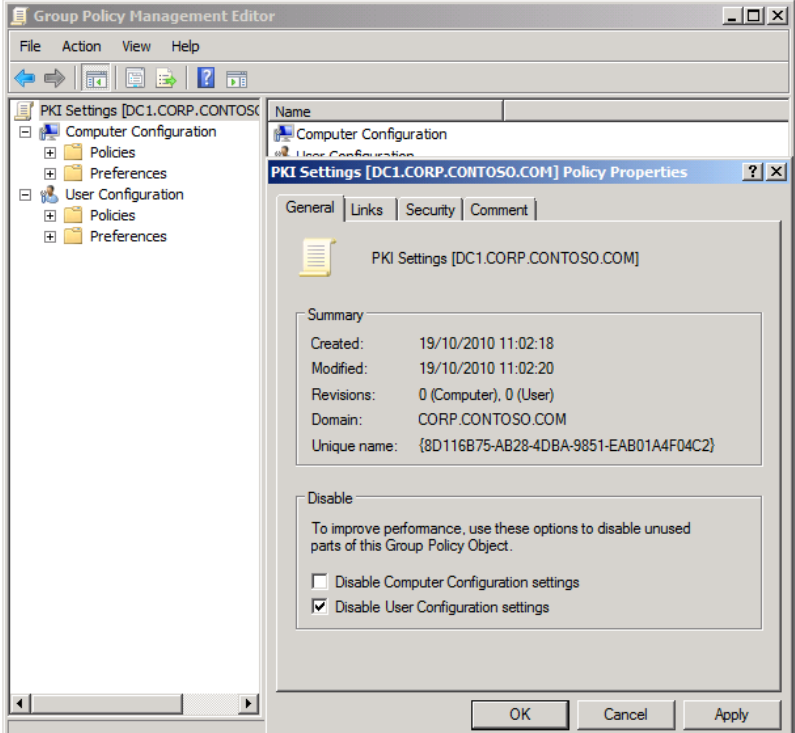
Maintenant que le gabarit est prêt, encore faut-il le publier.

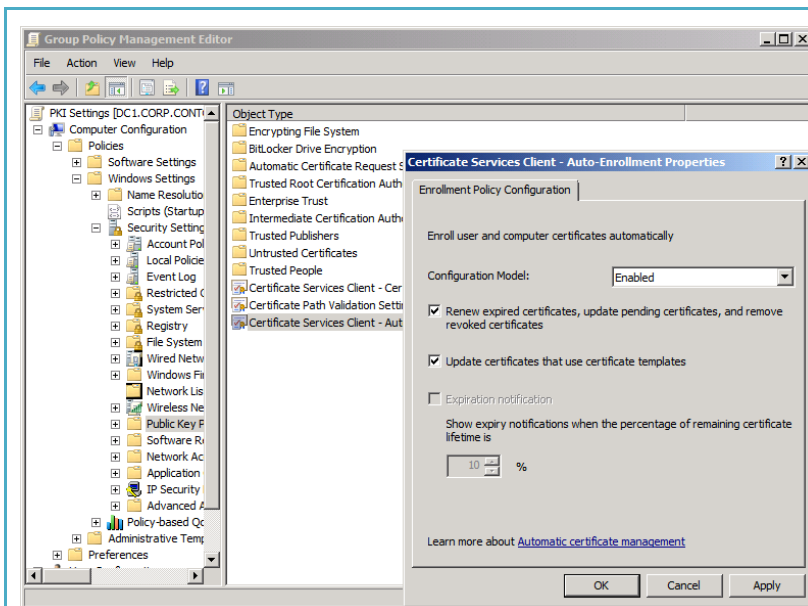


Une fois le gabarit publié, on pourra s'attaquer la mise en œuvre du Network Location Server.

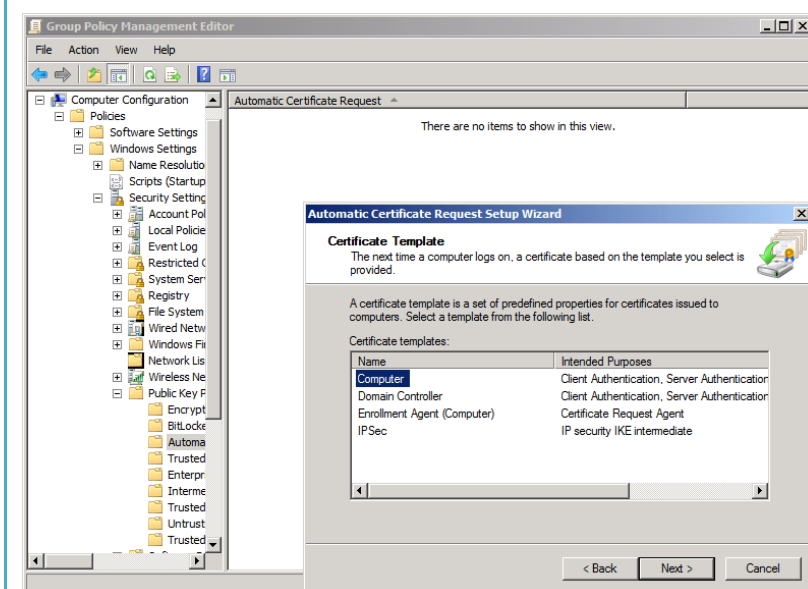
5.4 Activation de l'auto-Enrollment

Maintenant que nous avons nos gabarits de certificats, il faut que les systèmes puissent effectuer des demandes de certificats. Pour cela, on va utiliser la fonctionnalité « d'autoenrollment » dans les stratégies de groupe.

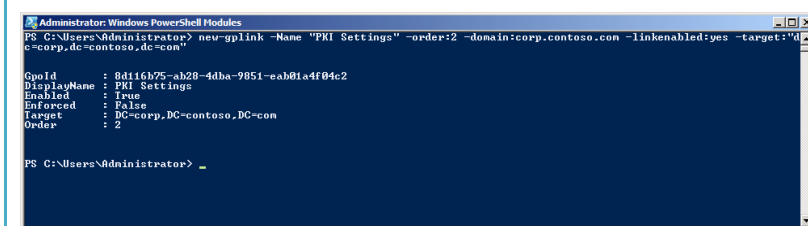
Impression écran	Description
 <pre> Administrator: Windows PowerShell Modules PS C:\Users\Administrator> new-gpo "PKI Settings" DisplayName : PKI Settings DomainName : corp.contoso.com Owner : CORP\Domain Admins Id : 8D116B75-AB28-4DBA-9851-EAB01A4F04C2 GpoStatus : AllSettingsEnabled Description : CreationTime : 19/10/2010 11:02:19 ModificationTime : 19/10/2010 11:02:21 UserVersion : AD Version: 0, SysUoi Version: 0 ComputerVersion : AD Version: 0, SysUoi Version: 0 WmiFilter : PS C:\Users\Administrator> </pre>	<p>Pour aller vite, on va créer notre stratégie de groupe en PowerShell avec la commandlet « New-GPO ».</p>
	<p>Dans cette stratégie de groupe nous n'avons pas besoin de la section « Configuration de l'utilisateur ».</p>



L'activation de l'« Auto-Enrollment » inclus aussi le renouvellement et l'actualisation des certificats déjà déployés.



Il ne reste plus qu'à sélectionner le gabarit de certificats « Computer » pour que l'« auto-enrollment » soit pris en charge pour ce gabarit de certificats.



Il ne nous reste plus qu'à lier la stratégie de groupe à la racine du domaine, juste après la stratégie de groupe du domaine.

Ouf, on est venu à bout de l'infrastructure de clé publique. Effectivement, ce n'était pas simple. Prochaine étape, on pose la souris, on s'occupe du « Network Location Server » qui pour rappel est installé sur un système en « Core » - 😊.