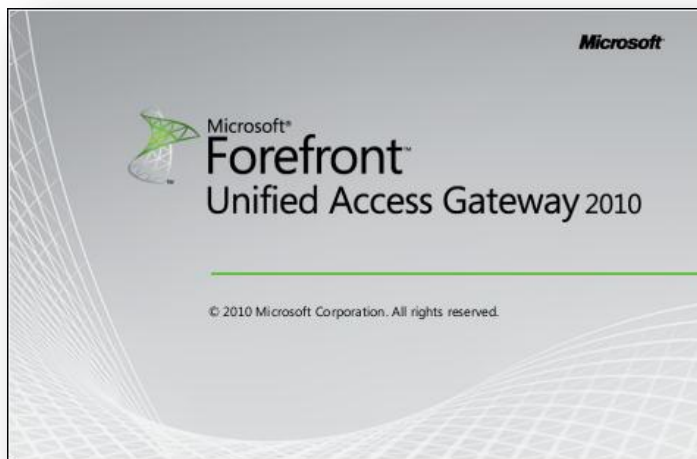


Microsoft Forefront UAG 2010 SP1

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

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

6	Configuration du serveur APP1	3
6.1	Configuration initiale du système d'exploitation	3
6.2	Installation du rôle WebServer	4
6.3	Publication de la CRL	6
6.4	Fichier de demande du certificat NLS	9
6.5	Soumission de la demande de certificat NLS	10
6.6	Installation du certificat NLS	12



6 CONFIGURATION DU SERVEUR APP1

Etant donné que ce serveur n'aura finalement que peu d'utilisation sinon d'héberger un simple site web en HTTPS pour le Network Location Server de DirectAccess, on va installer ce serveur avec « Windows Server 2008 R2 Standard » mais en « Core ». Pour le coup, c'est « complex by design ». La configuration comprendra les étapes suivantes :

- La configuration initiale du système d'exploitation
- L'installation du rôle WebServer
- La publication de la CRL
- La mise en œuvre du NLS



Core, c'est très bien et il faudra vous y faire. L'avenir, c'est PowerShell !

6.1 Configuration initiale du système d'exploitation

A ce stade, rien de bien difficile, sinon l'utilisation de SCONFIG.EXE pour réaliser les opérations suivantes :

- Nommer le serveur en APP1
- Configurer l'interface réseau
- Configurer le client DNS
- Effectuer la jointure au domaine
- Activer l'administration à distance avec les consoles d'administration
- Activer la prise en charge de PowerShell en mode sécurité (remotesigned)
- Autoriser l'utilisation de la console Server Manager pour une administration distante
- Configurer la stratégie pour Windows Update
- Installer les mises à jour disponibles depuis Windows Update
- Activer le bureau à distance mais uniquement pour les clients capables de s'authentifier en Network Local Authentication

Bref, c'est fou ce qu'on arrive à faire avec « SCONFIG.EXE ». Sous Windows 2008, le nombre de commandes à exécuter pouvait rebuter n'importe qui.

```
Administrator: C:\Windows\system32\cmd.exe - sconfig
Enabling Remote Desktop...

Server Configuration
-----
1) Domain/Workgroup:          Domain: corp.contoso.com
2) Computer Name:            APP1
3) Add Local Administrator
4) Configure Remote Management
5) Windows Update Settings:   Manual
6) Download and Install Updates
7) Remote Desktop:           Enabled (more secure clients only)
8) Network Settings
9) Date and Time
10) Log Off User
11) Restart Server
12) Shut Down Server
13) Exit to Command Line

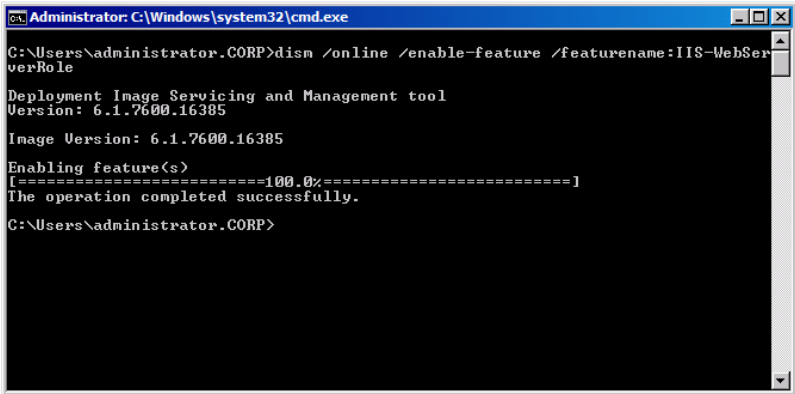
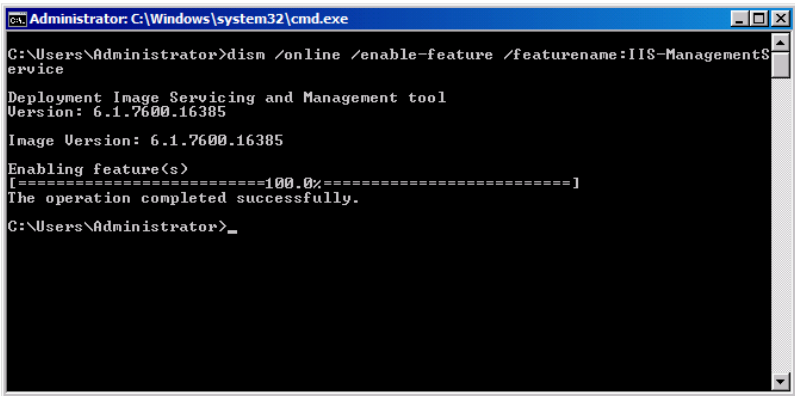
Enter number to select an option:
```



Pour rappel, la documentation relative à « SCONFIG.EXE » est disponible à cette adresse [http://technet.microsoft.com/en-us/library/ee441254\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee441254(WS.10).aspx). Les nostalgiques de Windows 2008 Core pourront se consoler avec la documentation relative aux commandes « NETSH.EXE » pour arriver au même résultat [http://technet.microsoft.com/en-us/library/ee441257\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/ee441257(WS.10).aspx).

6.2 Installation du rôle WebServer

Maintenant que les bases du serveur sont posées, continuons avec le composant principal, à savoir le serveur web, toujours dans sa version « Core ».

Impression écran	Description
 <pre> Administrator: C:\Windows\system32\cmd.exe C:\Users\administrator.CORP>dism /online /enable-feature /featurename:IIS-WebServerRole Deployment Image Servicing and Management tool Version: 6.1.7600.16385 Image Version: 6.1.7600.16385 Enabling feature(s) [=====100.0%=====] The operation completed successfully. C:\Users\administrator.CORP> </pre>	<p>On va commencer par installer le rôle WebServer, avec « DSIM.EXE ».</p>
 <pre> Administrator: C:\Windows\system32\cmd.exe C:\Users\Administrator>dism /online /enable-feature /featurename:IIS-ManagementService Deployment Image Servicing and Management tool Version: 6.1.7600.16385 Image Version: 6.1.7600.16385 Enabling feature(s) [=====100.0%=====] The operation completed successfully. C:\Users\Administrator>_ </pre>	<p>Histoire de se faciliter la vie, on va activer l'administration du site à distance au travers de la console d'administration de IIS et dépendances associées.</p>

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator.CORP>dism /online /enable-feature /featurename:WAS-Window
sActivationService
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Image Version: 6.1.7600.16385
Enabling feature(s)
[=====99.8%===== ]
The operation completed successfully.
C:\Users\administrator.CORP>dism /online /enable-feature /featurename:WAS-Config
urationAPI
Deployment Image Servicing and Management tool
Version: 6.1.7600.16385
Image Version: 6.1.7600.16385
Enabling feature(s)
[=====99.8%===== ]
The operation completed successfully.
C:\Users\administrator.CORP>

```

Note : Attention DISM.EXE est chatouilleux sur la case des noms des rôles et fonctionnalités !

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator.CORP>reg add HKLM\Software\Microsoft\WebManagement\Server
/v EnableRemoteManagement /T REG_DWORD /D 1
Value EnableRemoteManagement exists, overwrite(Yes/No)? y
The operation completed successfully.
C:\Users\administrator.CORP>_

```

Il ne reste plus qu'à activer l'administration à distance en mettant à jour une clé de registre.

```

Administrator: C:\Windows\system32\cmd.exe
C:\Users\administrator.CORP>sc config wmsvc start= auto
[SC] ChangeServiceConfig SUCCESS
C:\Users\administrator.CORP>net start wmsvc
The Web Management Service service is starting.
The Web Management Service service was started successfully.
C:\Users\administrator.CORP>_

```

Il ne reste plus qu'à configurer le service d'administration à distance pour un démarrage automatique puis de le démarrer.

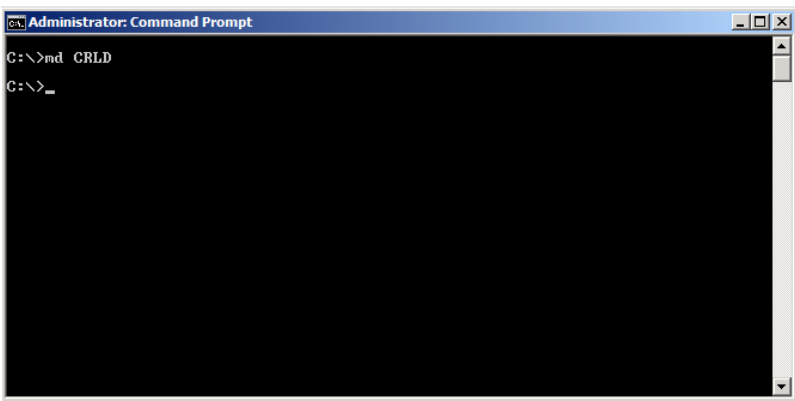
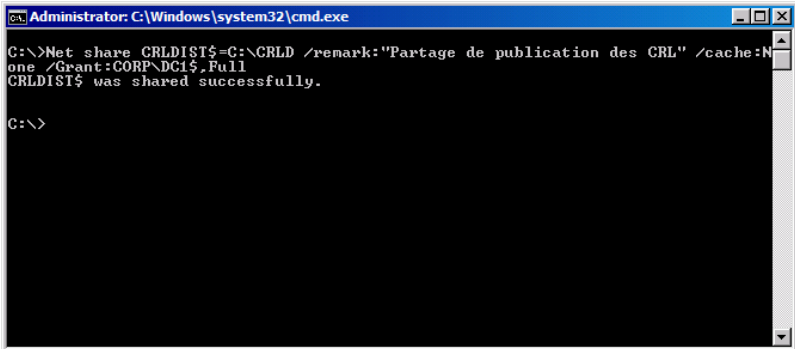
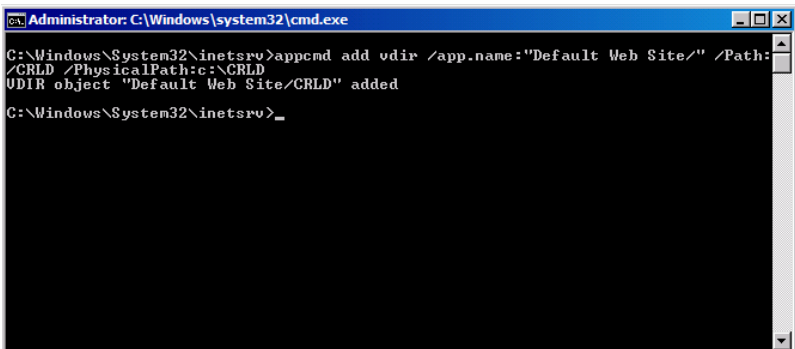
Note : Attention au SC CONFIG, il faut bien un espace après le caractère « = ».

6.3 Publication de la CRL

Nous avons laissé notre autorité de certification en pleine configuration. Plus précisément au niveau de la publication des listes de révocations. Pour rappel, l'autorité de certification a été configurée pour :

- Publier la CRL dans le partage CRLDIST\$
- Publier la CRL « Delta » dans le partage CRLDIST\$
- Référencer l'emplacement de stockage de la CRL à <http://crl.corp.contoso.com>

Il ne reste donc plus qu'à mettre en place toute la structure pour accueillir les listes de révocations. Ces opérations seront donc réalisées sur le serveur « APP1.CORP.CONTOSO.COM ».

Impression écran	Description
	<p>On va commencer par créer le répertoire qui va héberger nos listes de révocations. Les permissions NTFS seront donc héritées de la racine, donc minimalistes, parfait !</p>
	<p>Ce répertoire doit être partagé sous le nom référencé dans l'extension préalablement déclaré dans l'autorité de certification.</p> <p>On va même s'assurer que le partage ne soit accessible en écriture que pour le serveur hébergeant l'autorité de certification.</p>
	<p>Passons maintenant à la publication. Il nous faut un répertoire virtuel nommé « CRLD » à la racine du site web et pointant sur le répertoire « CLRD ».</p> <p>Note : Attention APPCMD.EXE n'est pas dans un répertoire référencé dans la variable d'environnement « Path ».</p>


```
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\System32\inetsrv>appcmd set config http://localhost/crld/ /Section:DirectoryBrowse /Enabled:True /Commit:Site
Applied configuration changes to section "system.webServer/directoryBrowse" for "MACHINE/WEBROOT/APPHOST/Default Web Site/crld/" at configuration commit path "MACHINE/WEBROOT/APPHOST/Default Web Site"
C:\Windows\System32\inetsrv>
```

IIS est tellement sécurisé par défaut qu'il interdit le parcours de répertoire. C'est bloquant pour les clients qui viennent télécharger les listes de révocation, donc on rétablit le parcours de répertoire sur le répertoire virtuel.

```
Administrator: C:\Windows\system32\cmd.exe
C:\Windows\System32\inetsrv>appcmd set config "Default Web Site/CRLD" -Section:system.webServer/Security/RequestFiltering -AllowDoubleEscaping:True
Applied configuration changes to section "system.webServer/security/requestFiltering" for "MACHINE/WEBROOT/APPHOST/Default Web Site/CRLD" at configuration commit path "MACHINE/WEBROOT/APPHOST/Default Web Site/CRLD"
C:\Windows\System32\inetsrv>
```

Subtilité d'IIS, par défaut, il n'autorise pas l'utilisation du « Double Escaping » dans les noms de fichiers. Dommage, le caractère « + » tombe dans cette catégorie. Il faut donc désactiver la fonctionnalité.

<http://support.microsoft.com/kb/942076/en-us>

A ce stade, notre serveur « APP1.CORP.CONTOSO.COM » est opérationnel pour la publication des listes de révocation. Encore faut-il s'assurer que tout est bien opérationnel. Tant qu'il n'y a pas de certificats révoqués, il n'y a pas encore de liste de révocation. On va donc forcer la publication pour s'assurer du bon fonctionnement.

Impression écran	Description
<pre>Administrator: Command Prompt C:\Users\Administrator>certutil -crl CertUtil: -CRL command completed successfully. C:\Users\Administrator></pre>	<p>Certes, il est possible d'utiliser la console d'administration mais étant donné qu'on va passer du temps dans « CERTUTIL.EXE », autant commencer tout de suite avec la publication de la CRL depuis le serveur DC1.CORP.CONTOSO.COM.</p>

```

Administrator: C:\Windows\system32\cmd.exe
C:\CRLD>dir
Volume in drive C has no label.
Volume Serial Number is 3091-8291

Directory of C:\CRLD

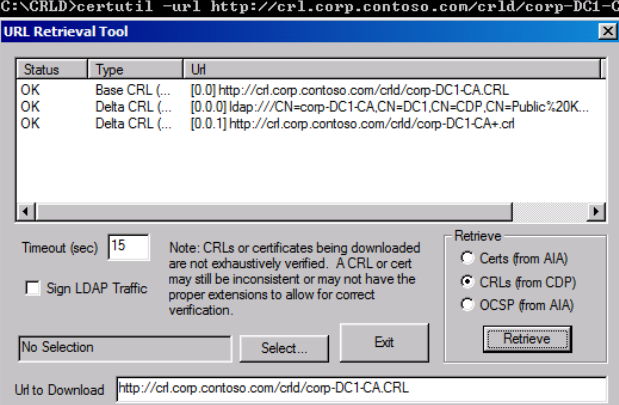
09/10/2010  18:47    <DIR>          .
09/10/2010  18:47    <DIR>          ..
09/10/2010  18:47                748 corp-DC1-CA+.crl
09/10/2010  18:47                992 corp-DC1-CA.crl
09/10/2010  18:40                226 web.config
               3 File(s)              1 966 bytes
               2 Dir(s)    132 197 900 480 bytes free

C:\CRLD>_
    
```

Pour s'en assurer, on peut aller voir le contenu du répertoire sur le serveur APP1.CORP.CONTOSO.COM pour constater la présence des deux listes de révocation.

```

Administrator: C:\Windows\system32\cmd.exe - certutil -url http://crl.corp.contoso.com/crl/corp-DC1-CA.CRL
C:\CRLD>certutil -url http://crl.corp.contoso.com/crl/corp-DC1-CA.CRL
    
```



Status	Type	URL
OK	Base CRL (...)	[0.0] http://crl.corp.contoso.com/crl/corp-DC1-CA.CRL
OK	Delta CRL (...)	[0.0.0] ldap://CN=corp-DC1-CA,CN=DC1,CN=CDP,CN=Public%20K...
OK	Delta CRL (...)	[0.0.1] http://crl.corp.contoso.com/crl/corp-DC1-CA+.crl

Timeout (sec) 15 Note: CRLs or certificates being downloaded are not exhaustively verified. A CRL or cert may still be inconsistent or may not have the proper extensions to allow for correct verification.

Sign LDAP Traffic

Retrieve: Certs (from AIA) CRLs (from CDP) OCSP (from AIA)

URL to Download: http://crl.corp.contoso.com/crl/corp-DC1-CA.CRL

On peut aussi utiliser notre navigateur Internet pour aller consulter la liste des fichiers mis à disposition mais la meilleure validation reste celle de « CERUTIL.EXE ».

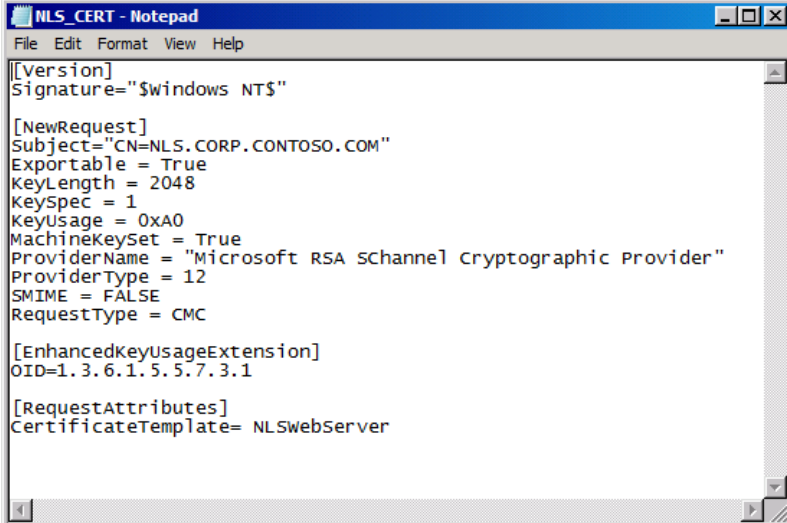
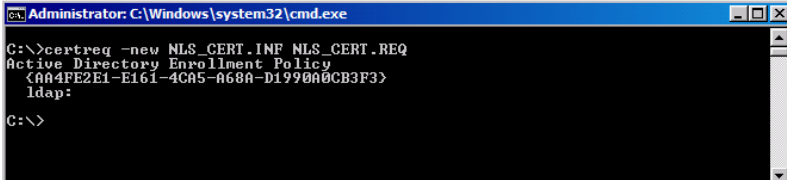
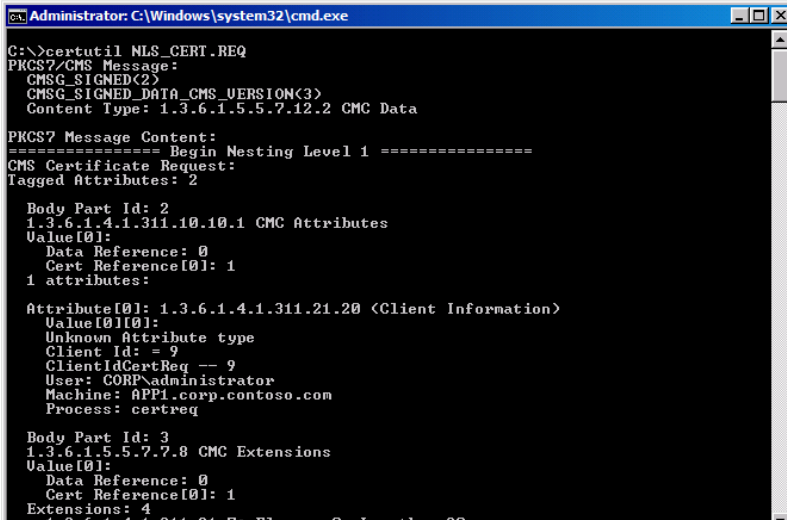
6.4 Fichier de demande du certificat NLS

C'est maintenant que les choses commencent à se corser, puisqu'on va parler de certificats et de configuration de IIS, le tout toujours en ligne de commande. Le fichier de demande de certificat doit être correctement formaté. Sans cela, la demande ne pourra être convenablement interprétée.

Contenu du fichier de demande de certificat	Description
[Version] Signature= "\$Windows NT\$" [NewRequest]	
Subject= "CN=NLS.CORP.CONTOSO.COM"	Indique le nom qui sera inscrit dans le certificat
Exportable = True	Indique que la clé privée sera exportable.
KeyLength = 2048	Indique une longueur de clé de 2048 bits
KeySpec = 1	La clé peut être utilisée pour signer
KeyUsage = 0xA0	Indique les usages suivants pour le certificat : <ul style="list-style-type: none"> ■ Digital Signature ■ Key Encipherment
MachineKeySet=True	Indique que le certificat sera placé dans le magasin ordinateur
ProviderName="Microsoft RSA SChannel Cryptographic Provider"	Indique le nom du « Cryptographic Service Provider » à utiliser.
ProviderType=12	Identifiant représentant le CSP ci-dessus.
SMIME = FALSE	Le certificat ne sera pas utilisé pour chiffrer un email
RequestType= CMC	Détermine le standard utilisé pour générer et soumettre la demande de certificat.
[EnhancedKeyUsageExtension] OID=1.3.1.5.5.7.3.1	Désigne le rôle « Server Authentication »
[RequestAttributes] CertificateTemplate= NLSWebServer	Désigne le gabarit de certificat pour le NLS

6.5 Soumission de la demande de certificat NLS

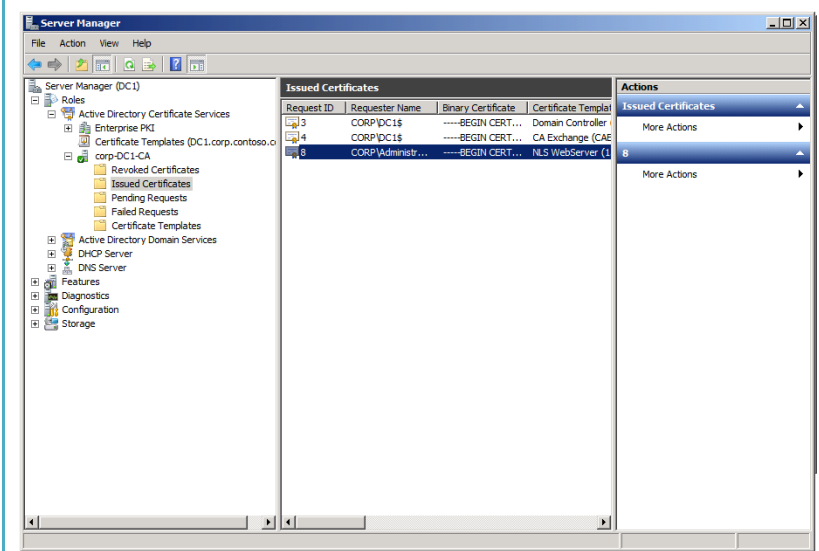
Le fichier de demande n'est rien tant qu'il n'est pas convenablement formaté. Celui-ci sera soumis à l'autorité de certification. La demande devra être approuvée au niveau de l'autorité de certification. Le certificat délivré devra être accepté et placé dans le magasin « Computer ».

Impression écran	Description
 <pre> NLS_CERT - Notepad File Edit Format View Help [[Version] Signature="\$windows NTS" [NewRequest] Subject="CN=NLS.CORP.CONTOSO.COM" Exportable = True KeyLength = 2048 KeySpec = 1 KeyUsage = 0xA0 MachineKeySet = True ProviderName = "Microsoft RSA Schannel Cryptographic Provider" ProviderType = 12 SMIME = FALSE RequestType = CMC [EnhancedKeyUsageExtension] OID=1.3.6.1.5.5.7.3.1 [RequestAttributes] CertificateTemplate= NLSwebServer </pre>	<p>Notre demande de certificat est prête.</p>
 <pre> Administrator: C:\Windows\system32\cmd.exe C:\>certreq -new NLS_CERT.INF NLS_CERT.REQ Active Directory Enrollment Policy <AA4FE2E1-E161-4CA5-A68A-D1990A0CB3F3> ldap: C:\> </pre>	<p>On va commencer par formater notre demande.</p>
 <pre> Administrator: C:\Windows\system32\cmd.exe C:\>certutil NLS_CERT.REQ PKCS7/CMS Message: CMSG_SIGNED(2) CMSG_SIGNED_DATA_CMS_VERSION(3) Content Type: 1.3.6.1.5.5.7.12.2 CMC Data PKCS7 Message Content: ===== Begin Nesting Level 1 ===== CMS Certificate Request: Tagged Attributes: 2 Body Part Id: 2 1.3.6.1.4.1.311.10.10.1 CMC Attributes Value[0]: Data Reference: 0 Cert Reference[0]: 1 1 attributes: Attribute[0]: 1.3.6.1.4.1.311.21.20 <Client Information> Value[0][0]: Unknown Attribute type Client Id: = 9 ClientIdCertReq = 9 User: CORP\Administrator Machine: APP1.corp.contoso.com Process: certreq Body Part Id: 3 1.3.6.1.5.5.7.7.8 CMC Extensions Value[0]: Data Reference: 0 Cert Reference[0]: 1 Extensions: 4 1.3.6.1.4.1.311.21.7: Flags = 0, Length = 30 </pre>	<p>Pour vérification, on va demander l'interprétation de notre demande, histoire de vérifier qu'on a bien toutes les informations requises.</p>

```

Administrator: C:\Windows\system32\cmd.exe
C:\>certreq -submit -config dc1.corp.contoso.com\corp-DC1-CA NLS_CERT.REQ NLS_CER
RT.CER
RequestId: 0
RequestId: "0"
Certificate retrieved(Issued) Issued
C:\>_
    
```

Cette demande va être soumise à notre autorité de certification intégrée à l'annuaire Active Directory.



On peut constater que la demande a bien été traitée par l'autorité de certification.

Toutes les informations nécessaires étaient bien renseignées et le soumissionnaire avait bien la permission d'obtenir ce type de certificat.

```

Administrator: C:\Windows\system32\cmd.exe
C:\>certutil -addstore MY NLS_CERT.CER
MY
Certificate "CN=NLS.CORP.CONTOSO.COM" added to store.
CertUtil: -addstore command completed successfully.
C:\>
    
```

On peut maintenant stocker le certificat dans son magasin ordinateur.

```

Administrator: C:\Windows\system32\cmd.exe
C:\>certreq -accept NLS_CERT.CER
C:\>_
    
```

On peut maintenant accepter la demande.

```

Administrator: C:\Windows\system32\cmd.exe
C:\>certutil -store MY
MY
===== Certificate 0 =====
Serial Number: 14cc049f7e645aa42cc2e86ff07f943
Issuer: CN=WMSvc-APP1
NotBefore: 09/10/2010 17:09
NotAfter: 06/10/2020 17:09
Subject: CN=WMSvc-APP1
Signature matches Public Key
Root Certificate: Subject matches Issuer
Template:
Cert Hash(Sha1): de 3f de 10 92 f5 43 d6 6b b0 fd 27 2e b0 53 47 0c 3b a3 d9
Key Container = WMSvc Certificate Key Container
Unique container name: bedbf0b4da5f8061b6444baedf4c00b1_3f492d5a-7b42-4270-95b7-809587c80b1a
Provider = Microsoft RSA SChannel Cryptographic Provider
Encryption test passed

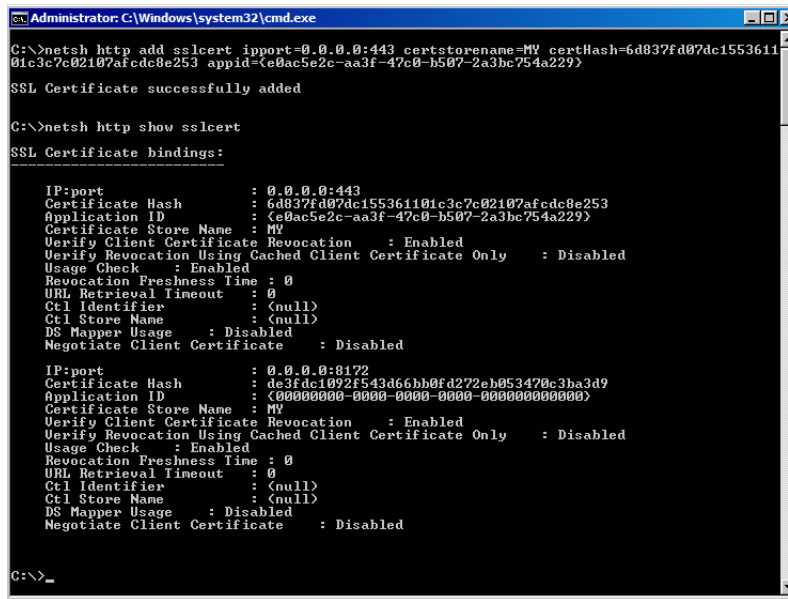
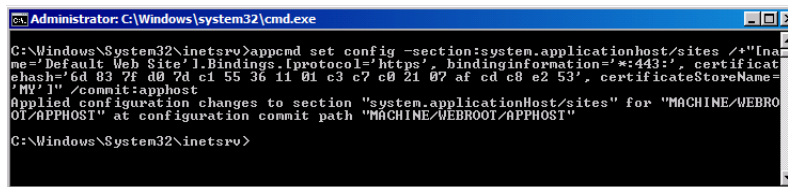
===== Certificate 1 =====
Serial Number: 61109685000100000000
Issuer: CN=corp-DC1-CA, DC=corp, DC=contoso, DC=com
NotBefore: 12/10/2010 08:12
NotAfter: 11/10/2012 08:12
Subject: CN=NLS.CORP.CONTOSO.COM
Non-root Certificate
Template: NLSWebServer, NLS_WebServer
Cert Hash(Sha1): 6d 03 7f d0 2d e1 55 36 11 01 c3 c7 e0 21 07 af cd e0 e2 53
Key Container = 824235764507e8db85762ec9bifa4d29_3f492d5a-7b42-4270-95b7-809587c88b1a
Simple container name: CertReq-NLSWebServer-e0ac5e2c-aa3f-4760-b507-2a3bc754a229
Provider = Microsoft RSA SChannel Cryptographic Provider
Encryption test passed
CertUtil: -store command completed successfully.
C:\>
    
```

On peut constater la présence de plusieurs certificats, mais un seul nous intéresse, plus particulièrement. On va conserver dans un coin le « Hash » et le « Simple Container Name » que l'on va immédiatement réutiliser.



6.6 Installation du certificat NLS

Maintenant qu'on dispose du certificat NLS dans le magasin ordinateur, il reste à le déclarer dans IIS puis de le positionner dans les « Bindings » du site web par défaut pour le protocole HTTPS, tout un programme.

Impression écran	Description
 <pre>Administrator: C:\Windows\system32\cmd.exe C:\>netsh http add sslcert ipport=0.0.0.0:443 certstorename=MY certHash=6d837fd07dc155361101c3c7e02107afcdc8e253 appid={e0ac5e2c-aa3f-47c0-b507-2a3bc754a229} SSL Certificate successfully added C:\>netsh http show sslcert SSL Certificate bindings: IP:port : 0.0.0.0:443 Certificate Hash : 6d837fd07dc155361101c3c7e02107afcdc8e253 Application ID : {e0ac5e2c-aa3f-47c0-b507-2a3bc754a229} Certificate Store Name : MY Verify Client Certificate Revocation : Enabled Verify Revocation Using Cached Client Certificate Only : Disabled Usage Check : Enabled Revocation Freshness Time : 0 URL Retrieval Timeout : 0 Ctl Identifier : <null> Ctl Store Name : <null> DS Mapper Usage : Disabled Negotiate Client Certificate : Disabled IP:port : 0.0.0.0:8172 Certificate Hash : de3fdc1092f543d66bb0fd272eb053470c3ba3d9 Application ID : {00000000-0000-0000-0000-000000000000} Certificate Store Name : MY Verify Client Certificate Revocation : Enabled Verify Revocation Using Cached Client Certificate Only : Disabled Usage Check : Enabled Revocation Freshness Time : 0 URL Retrieval Timeout : 0 Ctl Identifier : <null> Ctl Store Name : <null> DS Mapper Usage : Disabled Negotiate Client Certificate : Disabled C:\>_</pre>	<p>On va commencer par s'assurer que le moteur HTTP.SYS créé un « Listener » sur le port 443 et utilise le certificat contenu dans le magasin MY, identifié par son « Hash ». La valeur de l'attribut « APPID » est celle identifiée au niveau du « Simple Container Name ».</p>
 <pre>Administrator: C:\Windows\system32\cmd.exe C:\Windows\System32\inetsrv>append set config -section:system.applicationhost/sites /*[Name='Default Web Site'].Bindings.IpProtocol='https', bindingInformation='*:443:', certificat ehash='6d 83 7f d0 7d c1 55 36 11 01 c3 c7 c0 21 07 af cd c8 e2 53', certificateStoreName=' MY' /commit:apphost Applied configuration changes to section "system.applicationhost/sites" for "MACHINE/WEBRO OT/APPHOST" at configuration commit path "MACHINE/WEBROOT/APPHOST" C:\Windows\System32\inetsrv></pre>	<p>dernière étape, indiquer à IIS que le site web par défaut devra écouter aussi en HTTPS avec le même certificat.</p> <p>Note : Attention à bindinginformation : '* :443' n'est pas une erreur.</p>

A ce stade, notre site web NLS doit être accessible depuis un autre système situé sur le réseau LAN de l'entreprise. Pour être valide par la suite, notre NLS doit :



- Répondre selon un nom DNS interne pleinement qualifié
- Répondre en HTTPS avec un certificat dont l'autorité de certification est clairement reconnue
- Afficher un contenu.

Ce n'est finalement pas si difficile le « Core ». Prochaine étape, le plat de résistance avec une partie entièrement dédiée à la mise en œuvre d'UAG.