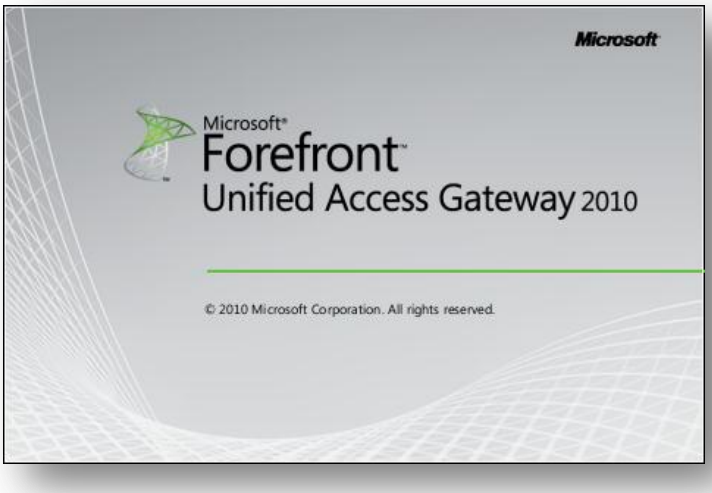
# Microsoft Forefront UAG 2010 SP1

## Mise en œuvre d'une plateforme DirectAccess pas à pas - Préparation

Advanced architecture and Design for DirectAccess




**jeudi, 14 avril 2011**

**Version 1.2**

*Rédigé par*

**benoits@exakis**.com

**MVP Enterprise Security 2010**

Benoits@exakis.com

# 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 Entreprise Security | 16/01/2011 |
| Benoît SAUTIERE | 1.1 | MVP Entreprise Security | 20/11/2010 |
| Benoît SAUTIERE | 1.0 | MVP Entreprise Security | 06/11/2010 |

# Sommaire

# 3 PREPARATION DE L'INFRASTRUCTURE

Les fondamentaux sont posés, maintenant, on rentre dans le vif du sujet avec la mise en œuvre de notre environnement. A ce stade, le plus difficile, ce sera l'infrastructure de clé publique. Désolé,ce sera un peu détaillé.

## 3.1 Préparation de l'environnement

### 3.1.1 Serveur DC1

Notre premier serveur sera un contrôleur de domaine opérant sous Windows Server 2008 R2 Edition standard. Ce serveur disposera d'une unique carte réseau connectée au réseau LAN de notre maquette. Le paramétrage réseau est documenté dans le tableau ci-dessous :

| Paramètre | Configuration |
|---|---|
| Nom NETBIOS | **DC1** |
| Adresse IPv4 | **192.168.0.100** |
| Masque de sous-réseau | **24 bits** |
| Passerelle par défaut | **192.168.0.1** |
| Suffixe DNS | **Corp.Contoso.com** |

***L'environnement de démonstration ne comprend qu'un seul contrôleur de domaine et donc DNS. Dans un environnement de production, il sera vivement recommandé de disposer d'au moins deux contrôleurs de domaine.***

***Il est impératif de conserver la couche réseau IPv6 sur le serveur. Elle sera utile.***

### 3.1.2 Serveur APP1

Notre second serveur ne sera utilisé que pour héberger notre Network Location Server. Pour rappel, c'est un site web en HTTPS qui est utilisé comme un phare pour déterminer que le poste de travail est connecté au réseau interne de l'entreprise. Etant donné son usage limité, nous allons mettre en œuvre ce NLS sur un Windows Server 2008 R2 standard mais installé en « Core ». Ce serveur ne disposera que d'une seule interface réseau, connectée au réseau LAN de notre maquette.

| Paramètre | Configuration |
|---|---|
| Nom NETBIOS | **APP1** |
| Adresse IPv4 | **192.168.0.101** |
| Masque de sous-réseau | **24 bits** |
| Passerelle par défaut | **192.168.0.1** |
| Suffixe DNS | **Corp.Contoso.com** |

### 3.1.3 Serveur UAG1

Le serveur UAG représentera le cœur de la maquette. Sa configuration sera un peu plus complexe que pour les autres. D'une part par ses exigences en termes de quantité de mémoire vive (2048Mb), d'autre part en terme d'interfaces réseau. En effet, le serveur dispose d'une interface réseau connectée au réseau LAN de la maquette ainsi que d'une interface connectée à Internet. Enfin, dernière subtilité, le système d'exploitation doit impérativement être de type Windows Server 2008 R2, mais en langue anglaise.

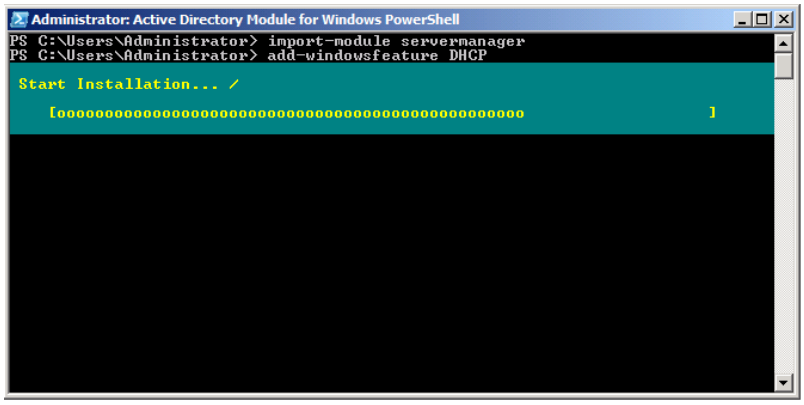
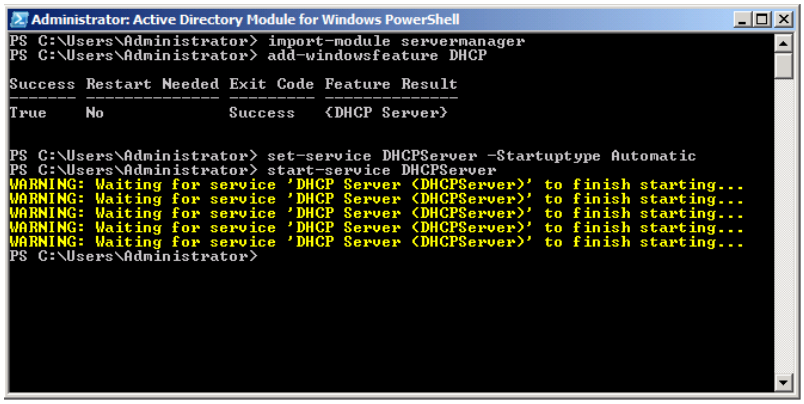
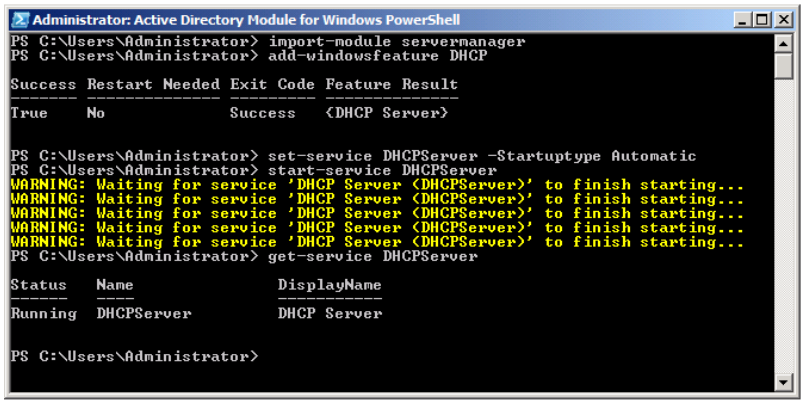
| Paramètre | Interface LAN | Interface publique |
|---|---|---|
| Nom NETBIOS | **APP1** | |
| Adresse IPv4 | **192.168.0.101** | **131.107.0.2**<br>**131.107.0.3** |
| Masque de sous-réseau | **24 bits** | **255.255.0.0** |
| Passerelle par défaut | **192.168.0.1** | **131.107.0.1** |
| Suffixe DNS | **Corp.Contoso.com** | **Contoso.com** |

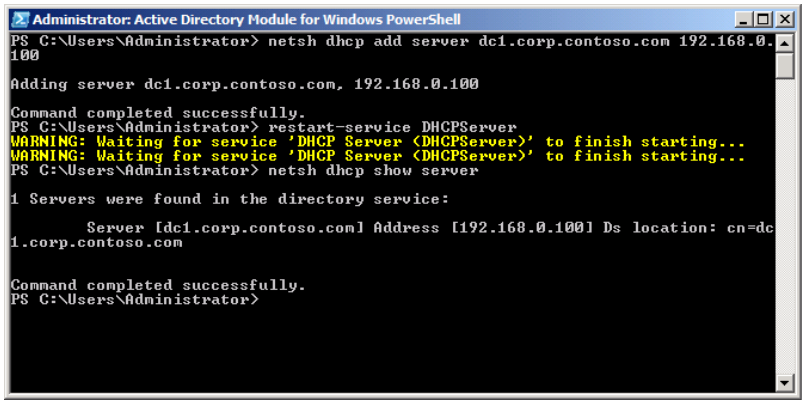
***Il est impératif d'installer UAG 2010 sur un système d'exploitation en langue anglaise. De plus, il est impératif que :***

- ***Les deux adresses IPV4 soient publiques et consécutives***
- ***Qu'il n'y ait pas de translation d'adresse sur l'interface publique***
- ***Qu'il n'y ait pas de translation d'adresse sur l'interface privée***
- ***Que le plan d'adressage interne respecte la RFC1918 ou un plan d'adressage propriété de l'entreprise (Plage IPv4 acquise par la société)***

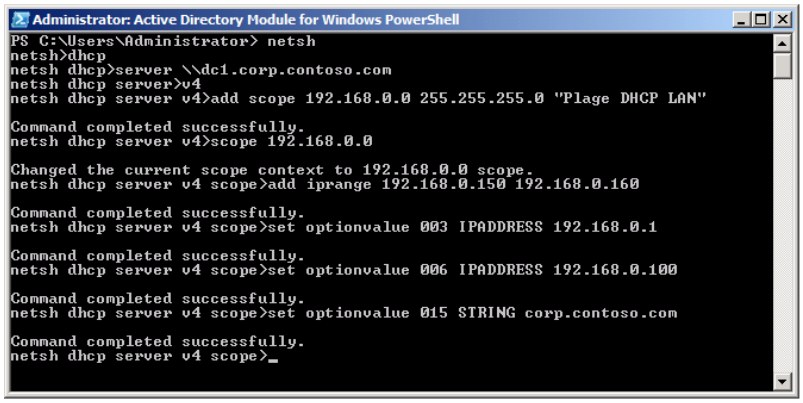
## 3.2 Préparation réseau

Coté réseau, il n'y a rien de particulier coté LAN, sinon qu'il est impératif de conserver la couche réseau IPv6 sur les systèmes d'exploitation. Sans cela, les systèmes d'exploitation ne pourront utiliser ISATAP pour générer une adresse IPv6. De ce fait, les serveurs ne seront accessibles qu'au travers de NAT64/DNS64 avec pour conséquence que seul le client en situation de mobilité pourra initier la communication. Après, le second prérequis, ce sera de disposer d'un simple serveur DHCP sur le réseau interne, donc rien d'insurmontable. Si nécessaire, c'est réalisable sans même toucher à la souris.

| Impression écran | Description |
|---|---|
|  | **On commence par demander l'importation du CommandLet « ServerManager » pour installer le rôle DHCP.** |
|  | **Une fois le rôle installé, on doit commencer par démarrer le service et le configurer en mode de démarrage automatique.** |
|  | **Notre serveur DHCP est opérationnel, il ne reste plus qu'à le configurer.** |




**La première étape sera de l'autoriser dans l'annuaire Active Directory.**




**Puis de :**

- **Créer une étendue DHCP**
- **Y référencer une plage d'adresses**
- **De préciser la passerelle**
- **De préciser le serveur DNS**
- **De préciser le suffixe DNS**

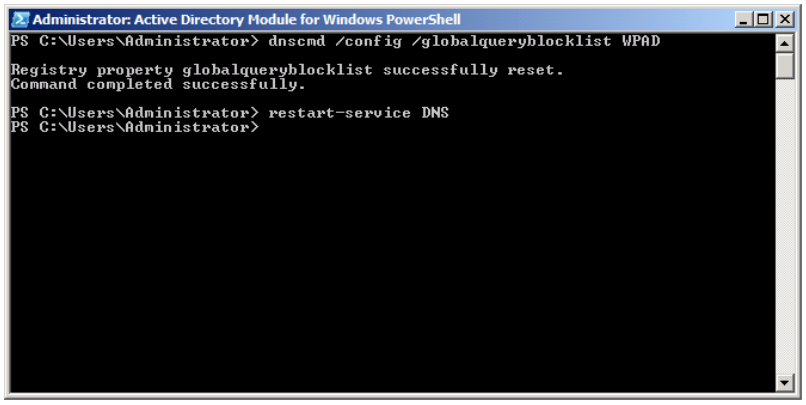
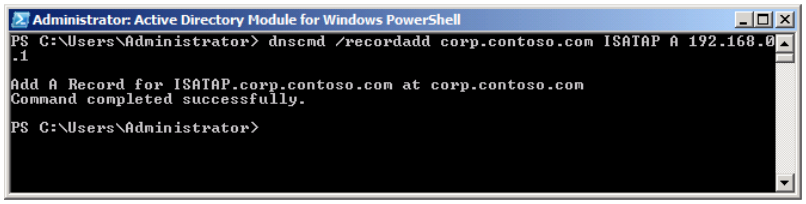
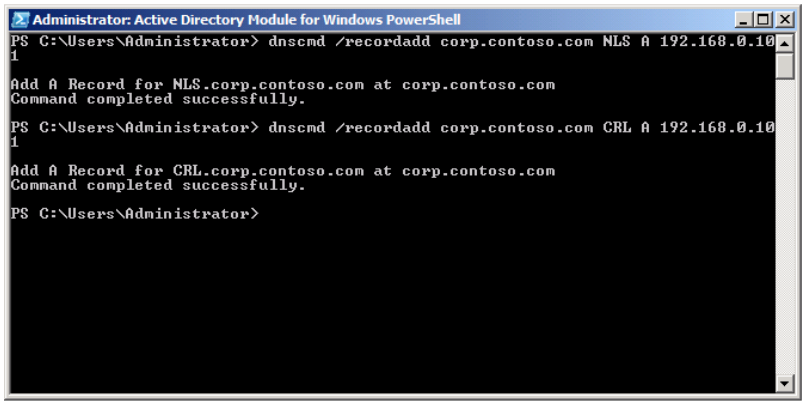
## 3.3 Préparation du DNS

Le DNS est un élément primordial pour DirectAccess. Un client en situation de mobilité ne pourra accéder à une ressource interne que si celle-ci est référencée dans le DNS. La préparation du DNS interne comprend :

- L'autorisation de l'enregistrement DNS ISATAP
- Création de l'enregistrement ISATAP
- La création de l'enregistrement DNS pour la CRL
- La création d'enregistrement DNS pour le NLS

Par défaut, il est considéré qu'il n'est pas opportun de répondre à la résolution de l'enregistrement DNS ISATAP. Pourquoi ? Car il référence le routeur IPv6 en charge de la propagation du préfixe IPv6 sur le réseau interne. Ce blocage est opéré par une fonctionnalité nommée « Global Query Block List » qui référence deux enregistrements (WPAD et ISATAP). On va donc commencer par actualiser cette liste pour retirer ISATAP. Ce n'est qu'à ce moment qu'on pourra créer l'enregistrement ISATAP qui référencera l'interface LAN de notre serveur ForeFront Unified Access Gateway 2010.

Par la suite, on pourra créer les enregistrements DNS additionnels dont on va avoir besoin. Le premier sera utilisé pour référencer le serveur APP1 sous le nom de « CRL » pour les listes de révocations de l'autorité de certification. Le second sera utilisé pour référencer ce même serveur APP1 comme Network Location Server.

| Impression écran | Description |
|---|---|
|  | **La reconfiguration de la Global Query Block List implique un redémarrage du serveur DNS.** |
|  | **Dès lors, on peut créer notre enregistrement DNS ISATAP qui va référencer l'interface LAN de notre serveur UAG1.** |
|  | **Il ne reste plus qu'à créer les enregistrements DNS CRL et NLS qui référenceront le serveur APP1** |

## 3.4 Préparation Active Directory

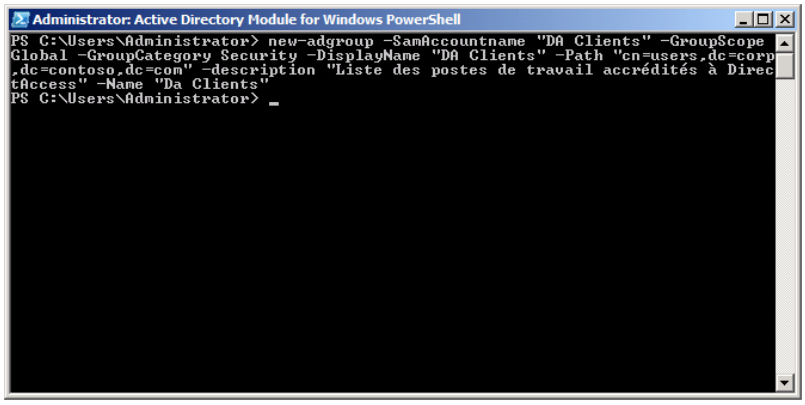
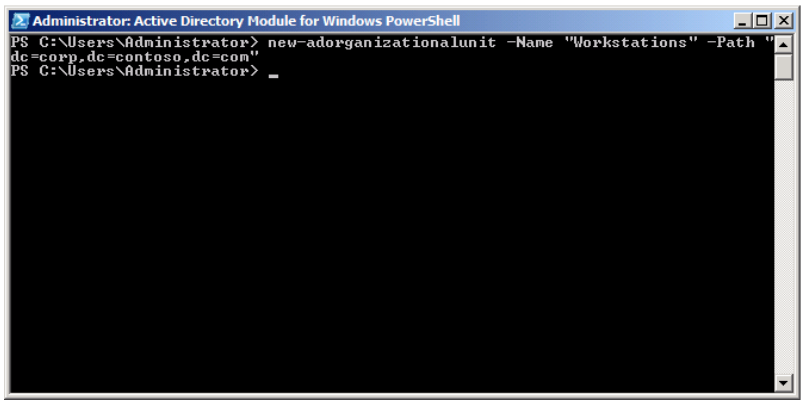
Le seul réel prérequis coté Active Directory, c'est de disposer d'un contrôleur de domaine opérant sous Windows 2008 SP1 au minimum. Après, nous n'avons besoin que d'aménagements ayant pour objectif de nous faciliter la vie. On distingue deux types d'aménagements :

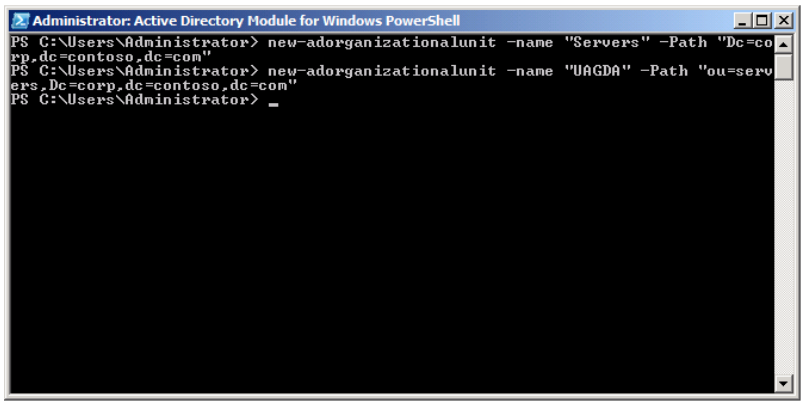
- L'organisation de l'annuaire Active Directory
- L'activation d'ICMP pour IPv4 et IPv6

### 3.4.1 Organisation de l'annuaire Active Directory

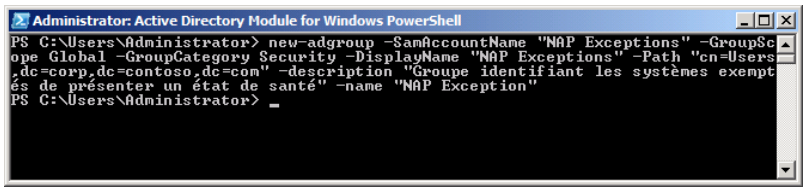
Côté organisation de l'annuaire, les aménagements ont pour objectif de ranger les objets dans l'annuaire afin de faciliter l'utilisation des futures stratégies de groupe. Ces aménagements sont les suivants :

- La création d'un groupe de filtrage pour les clients DirectAccess
- La création d'un conteneur pour les postes de travail
- La création d'un conteneur pour le serveur UAG et y appliquer des stratégies de groupe plus facilement
- La création d'un groupe de filtrage pour les systèmes dispensés de présenter un état de santé (optionnel).

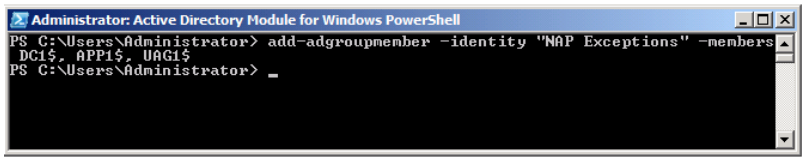
| Impression écran | Description |
|---|---|
|  | **Le groupe de filtrage sera créé par une simple commande PowerShell. Ce groupe va nous permettre d'identifier les systèmes autorisés pour DirectAccess.** |
|  | **Le conteneur créé permettra de positionner la stratégie de groupe dédiée aux clients DirectAccess. Un annuaire, ça se range.** |




**Coté serveurs, même combat, on les range.**



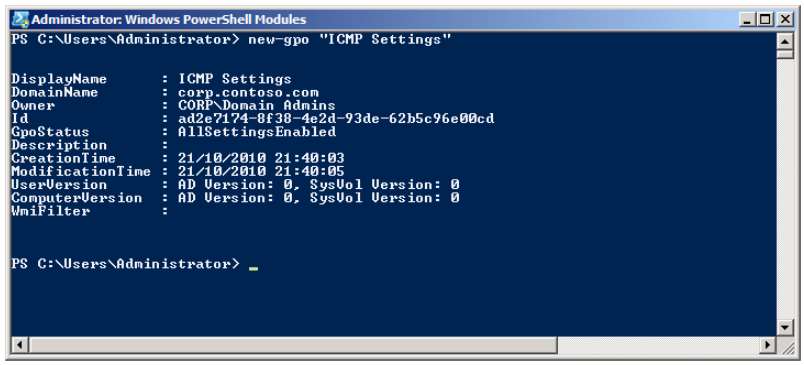

**On va créer notre groupe de filtrage NAP.**

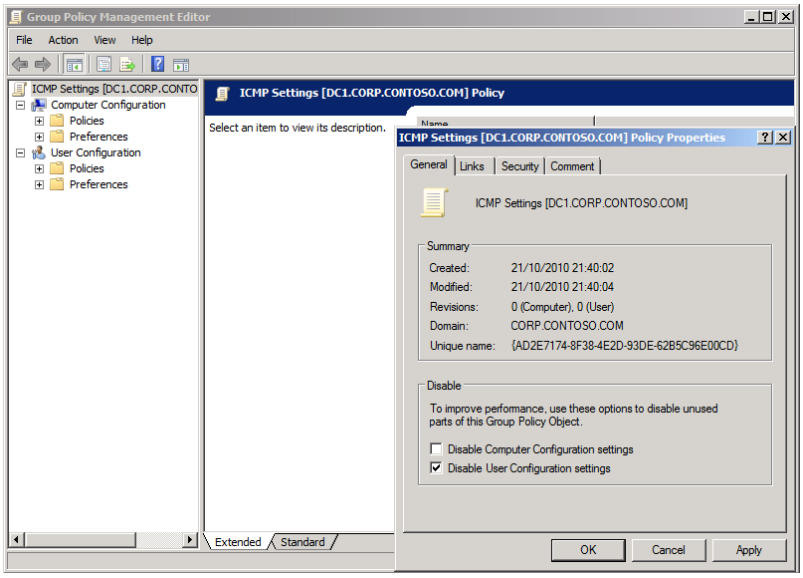



**Et y positionner comme membre des systèmes qui n'auront pas à présenter un état de santé pour obtenir un certificat.**

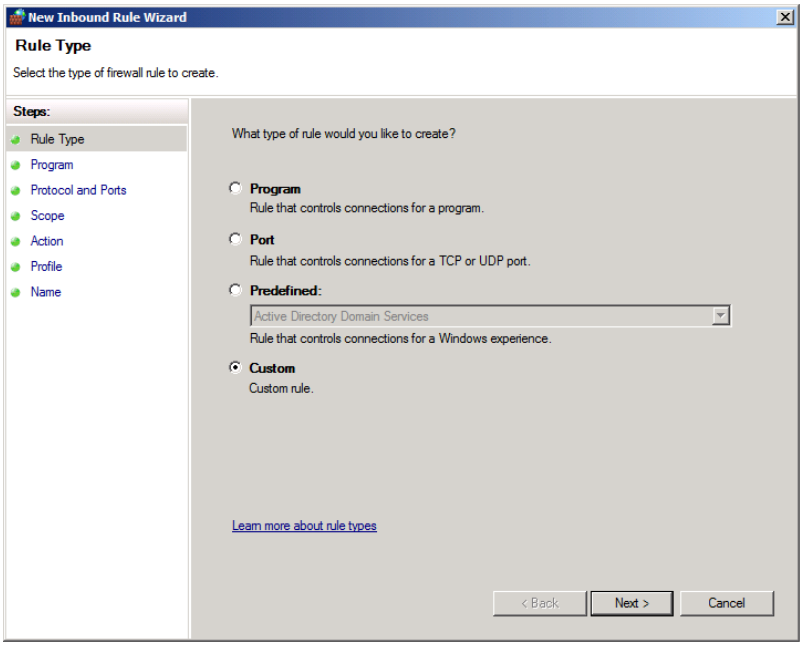
## 3.4.2 L'activation d'ICMP pour IPv4 et IPv6

Pour faciliter le dépannage de l'infrastructure, on a rien trouvé de mieux que « PING.EXE ». On aura donc besoin du protocole ICMPv4 mais aussi ICMPv6 et ce aussi bien en entrée qu'en sortie. A ce stade, on va faire « Simple by Design » et activer ces protocoles pour l'ensemble des systèmes du domaine.

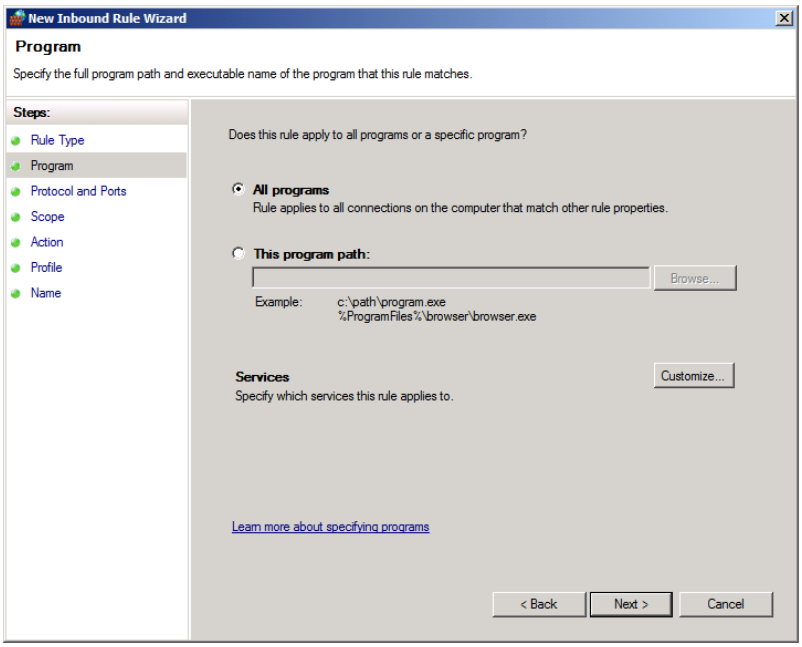
| Impression écran | Description |
|---|---|
|  | **Ici encore nous allons créer une nouvelle stratégie de groupe avec la CommandLet « New-GPO ».** |



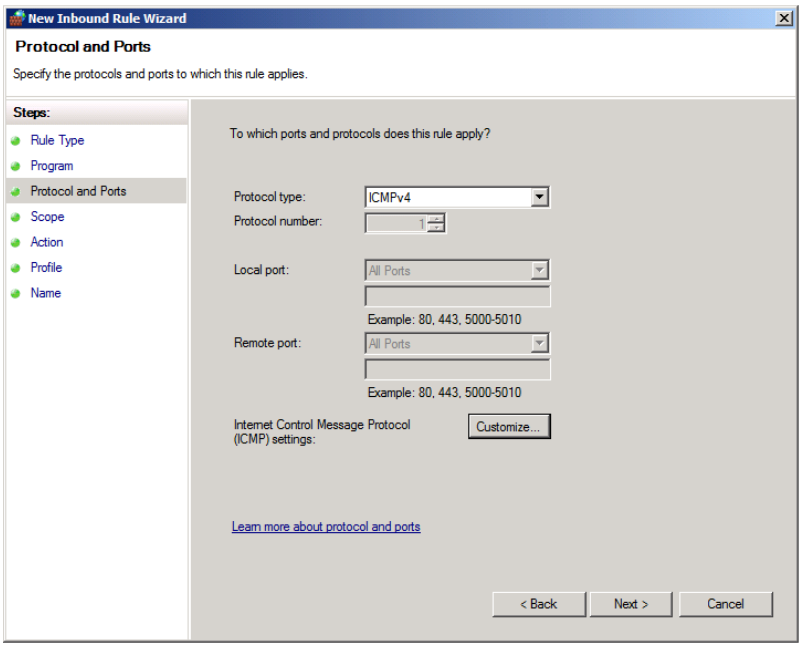

**Cette stratégie de groupe n'a pas besoin de sa partie « Configuration utilisateur ».**



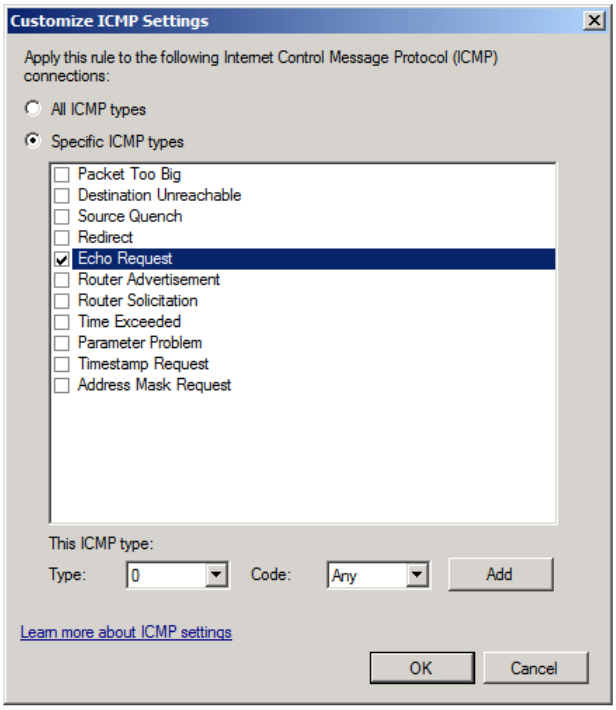

**On va commencer par créer une règle de pare-feu personnalisée pour ICMPV4 en entrée.**



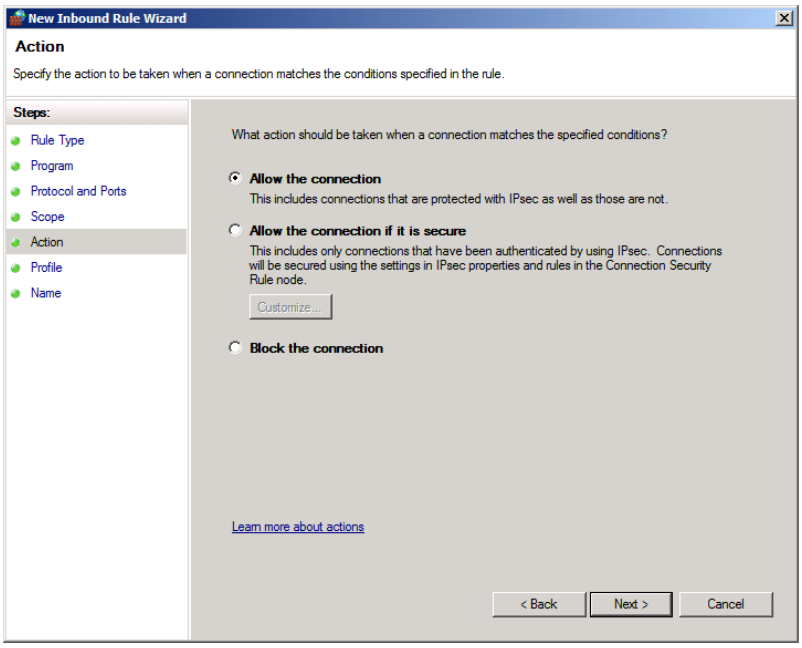

**Cette règle va concerner tous les programmes sans distinction.**



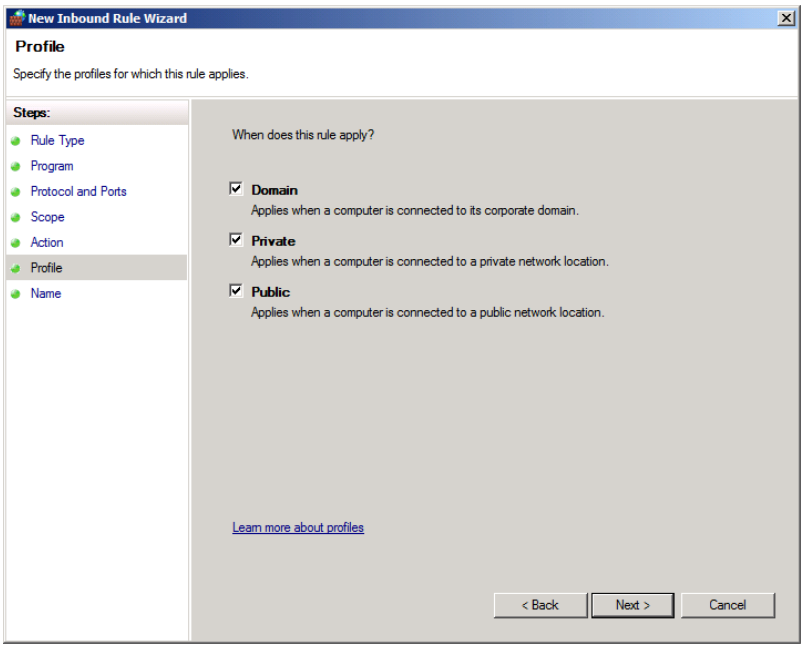

**Mais précisément le protocole ICMPv4.**



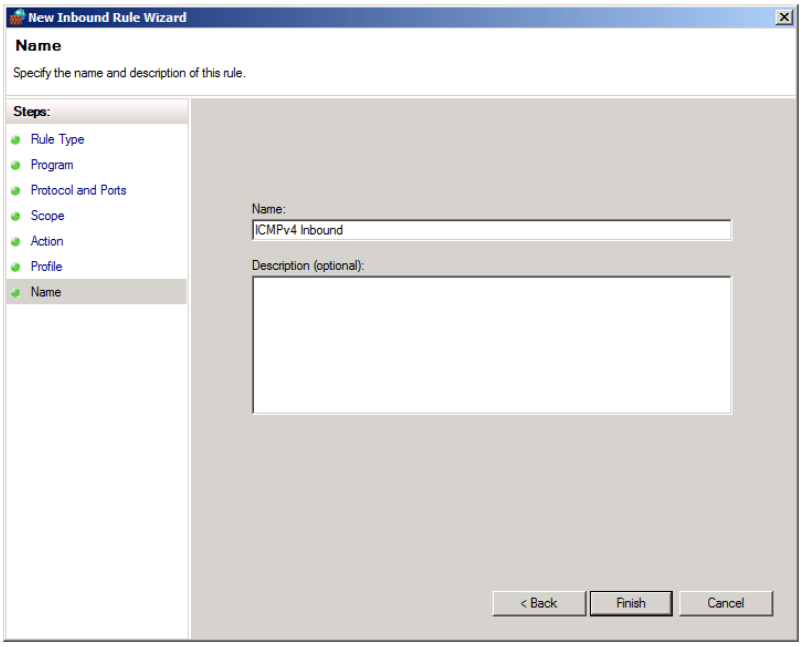

**Comme on veut faire les choses bien, on va se limiter au seul type de message ICMP dont nous allons avoir besoin pour le PING.**



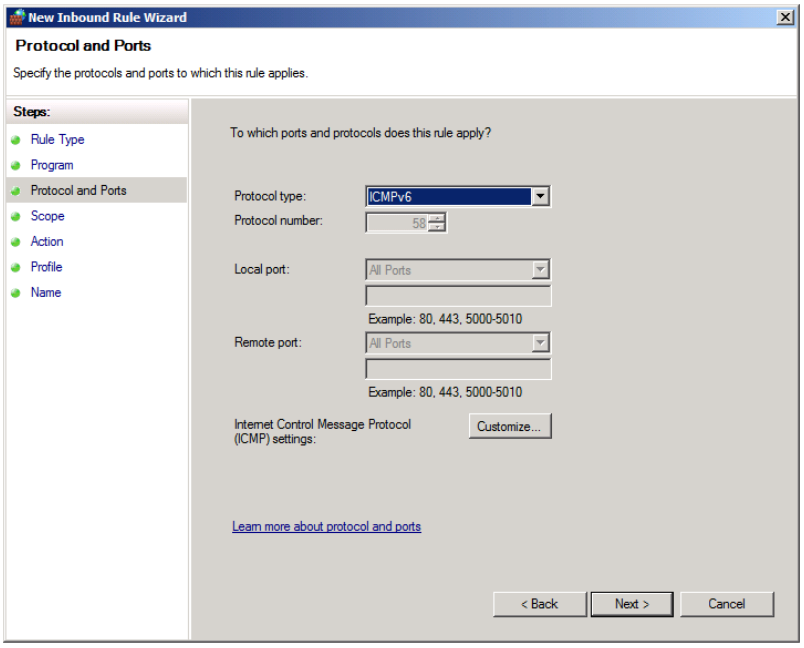

**Cette règle va autoriser ICMPv4 en entrée.**



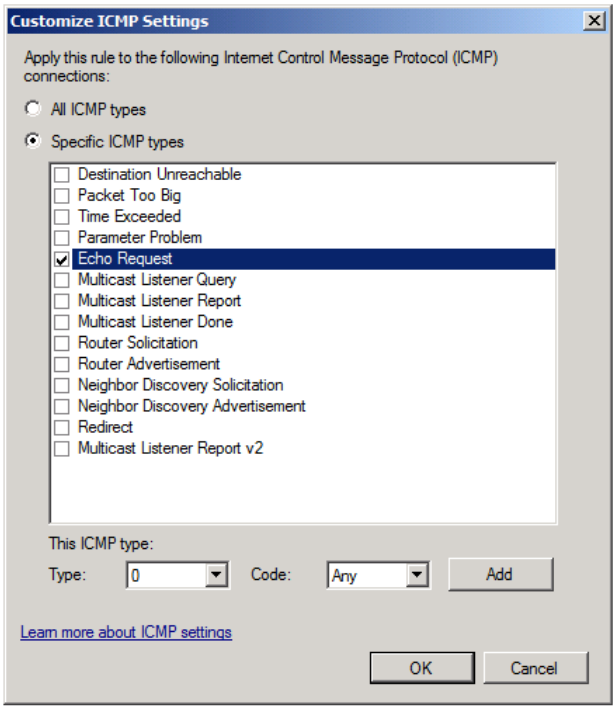

**La règle va concerner tous les profils de pare-feu. Je l'accorde, c'est un peu simpliste et cela pourrait être affiné. Ce n'est qu'une maquette après tout.**



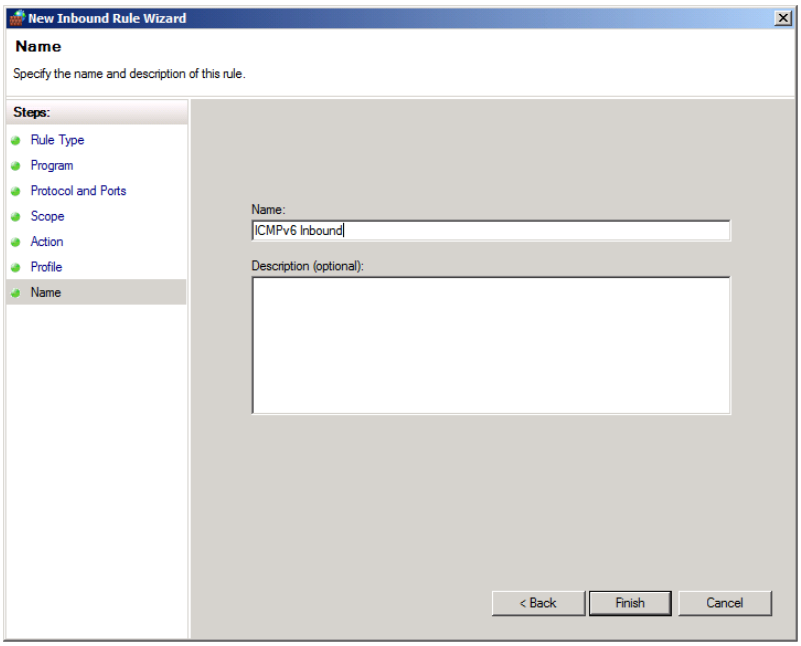

**Reste plus qu'à la nommer.**



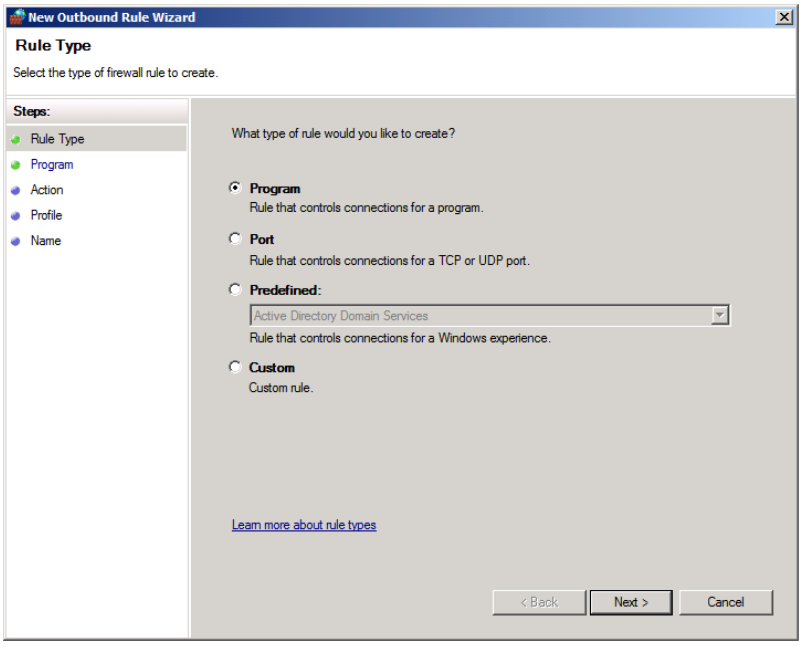

**On créé le même type de règle pour ICMPv6 en entrée.**



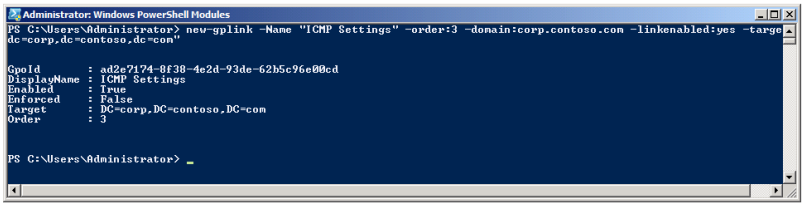

**Toujours pour le même type de message ICMP.**



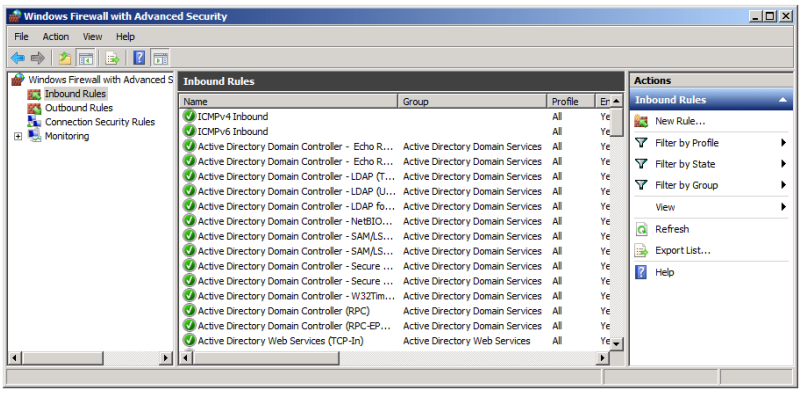

**Et la nommer.**




**Maintenant qu'on a fait cela pour ICMP en entrant, ne reste plus qu'à faire de même en sortie.**




**La stratégie de groupe est maintenant opérationnelle, ne reste plus qu'à la positionner au niveau de la racine du domaine.**




**Après actualisation des stratégies de groupe, on constate la présence dans la configuration du pare-feu local des systèmes.**

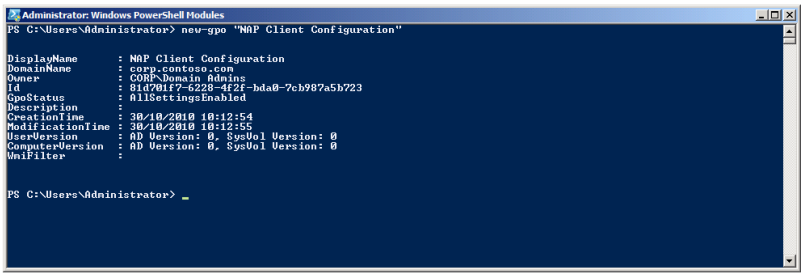
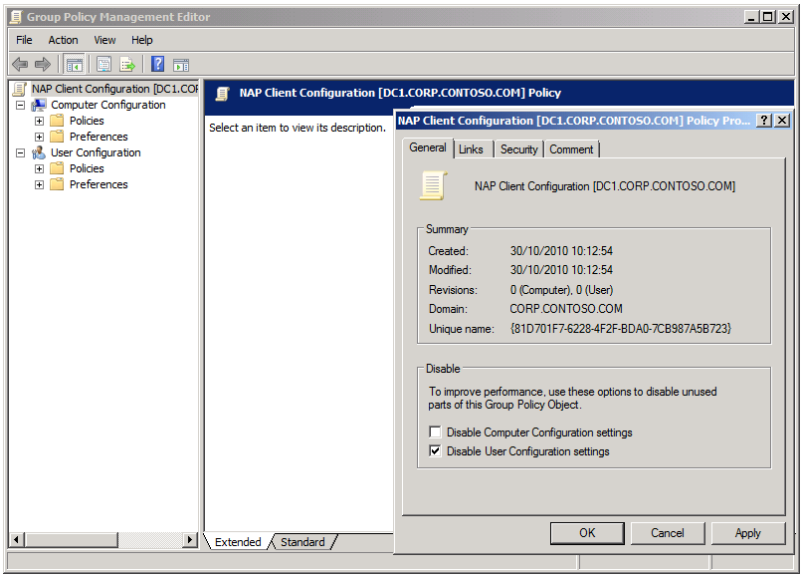
## 3.5 Paramétrage du client Network Access Protection

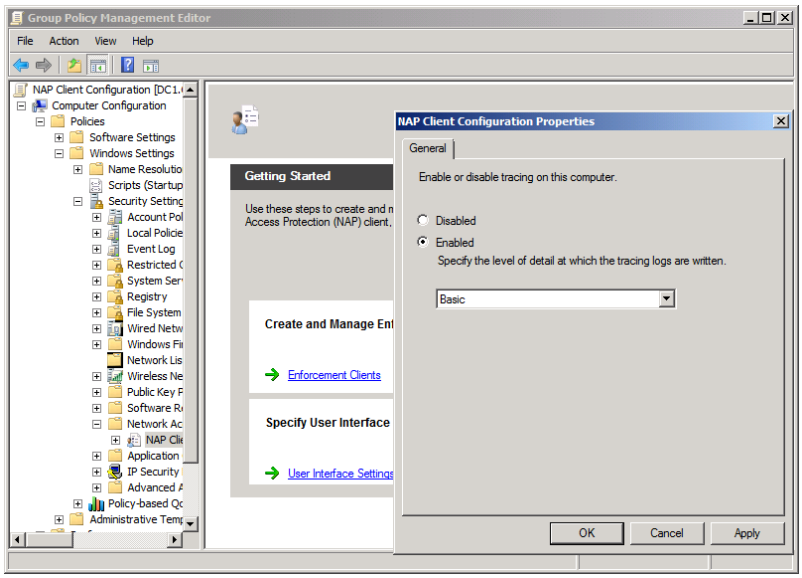
La configuration de Network Access Protection qui sera mises œuvre par UAG contiendra :

- La réactivation du centre de sécurité du système d'exploitation
- La configuration du service « Network Access Protection Agent » en mode de démarrage automatique
- La configuration du client IPSEC pour Network Access Protection
- La déclaration du Health Registration Authority

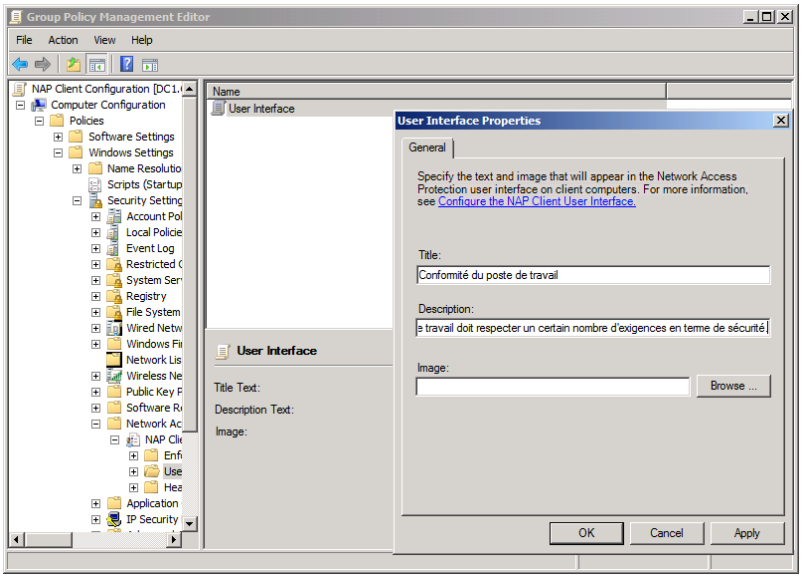
Même si cette configuration fonctionne, il manque quelques détails d'ordre esthétique :

- La réactivation de la journalisation de Network Access Protection coté client (UAG le désactive)
- La configuration de l'interface de l'agent NAP sur le client

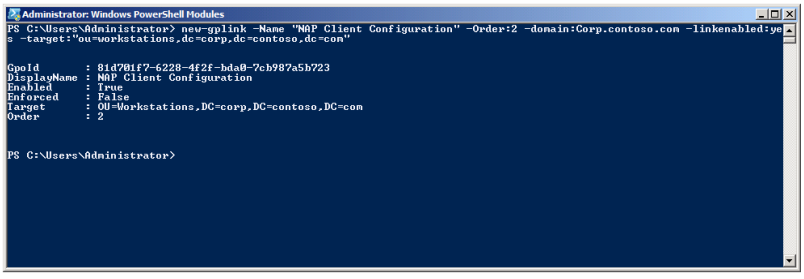
| Impression écran | Description |
|---|---|
|  | **On va donc commencer par créer une stratégie de groupe qui sera dédiée à la mise en place de notre paramétrage.** |
|  | **Cette stratégie de groupe n'a pas besoin de paramètres utilisateurs, on va donc désactiver la section.** |




**La réactivation de l'audit coté client permet de mieux comprendre les problématiques de non-conformité.**




**Ne reste plus que l'aspect cosmétique. Il est même possible d'afficher un logo représenté par un fichier JPG de taille 64*64.**




**Il ne reste plus qu'à lier la stratégie de groupe au conteneur « Workstations ».**

On est maintenant prêt à rentrer dans le vif du sujet avec un sujet qui pique : la PKI !