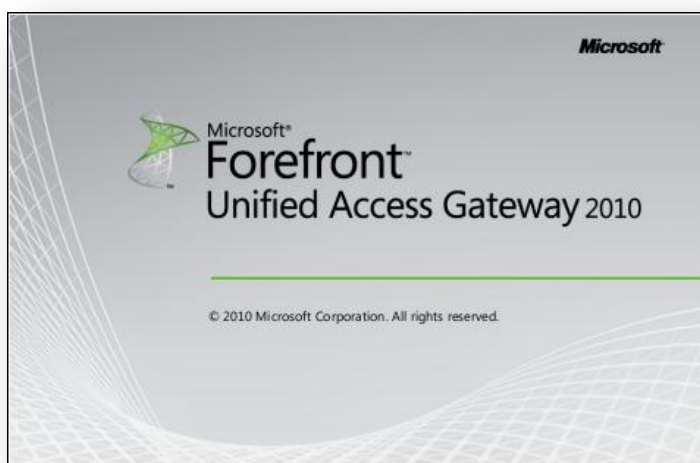


Microsoft Forefront UAG 2010 SP1

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

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

3	<i>Préparation de l'infrastructure</i>	3
3.1	Préparation de l'environnement	3
3.1.1	Serveur DC1	3
3.1.2	Serveur APP1	4
3.1.3	Serveur UAG1	4
3.2	Préparation réseau	5
3.3	Préparation du DNS	6
3.4	Préparation Active Directory	8
3.4.1	Organisation de l'annuaire Active Directory	8
3.4.2	L'activation d'ICMP pour IPv4 et IPv6	9
3.5	Paramétrage du client Network Access Protection	17

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	131.107.0.2 131.107.0.3
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

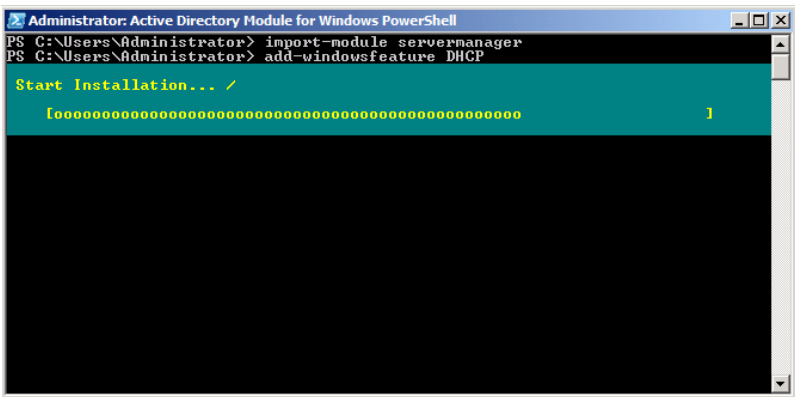
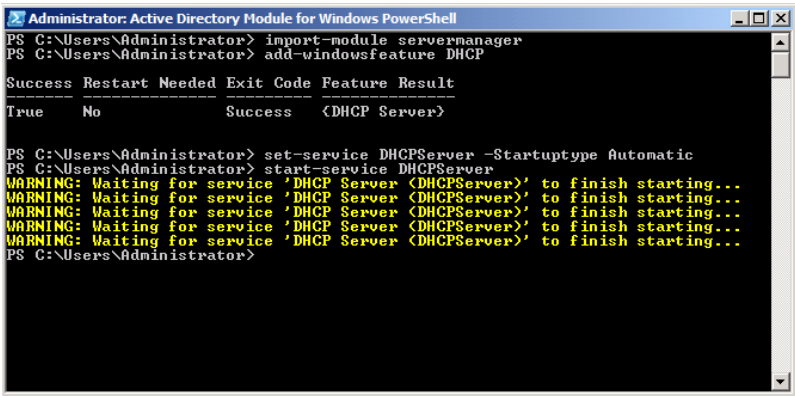
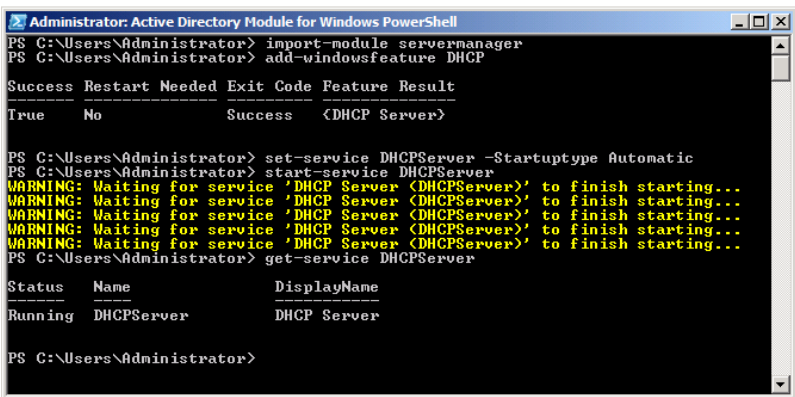
Il est impératif d'installer UAG 2010 sur un système d'exploitation en langue anglaise. De plus, il est impératif que :



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

```

Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> netsh dhcp add server dc1.corp.contoso.com 192.168.0.100
Adding server dc1.corp.contoso.com, 192.168.0.100
Command completed successfully.
PS C:\Users\Administrator> restart-service DHCPService
WARNING: Waiting for service 'DHCP Server (DHCPService)' to finish starting...
WARNING: Waiting for service 'DHCP Server (DHCPService)' to finish starting...
PS C:\Users\Administrator> netsh dhcp show server
1 Servers were found in the directory service:
    Server [dc1.corp.contoso.com] Address [192.168.0.100] Ds location: cn=dc1.corp.contoso.com
Command completed successfully.
PS C:\Users\Administrator>

```

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

```

Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> netsh
netsh>dhcp
netsh dhcp>server \\dc1.corp.contoso.com
netsh dhcp server>v4
netsh dhcp server v4>add scope 192.168.0.0 255.255.255.0 "Plage DHCP LAN"
Command completed successfully.
netsh dhcp server v4>scope 192.168.0.0
Changed the current scope context to 192.168.0.0 scope.
netsh dhcp server v4 scope>add iprange 192.168.0.150 192.168.0.160
Command completed successfully.
netsh dhcp server v4 scope>set optionvalue 003 IPADDRESS 192.168.0.1
Command completed successfully.
netsh dhcp server v4 scope>set optionvalue 006 IPADDRESS 192.168.0.100
Command completed successfully.
netsh dhcp server v4 scope>set optionvalue 015 STRING corp.contoso.com
Command completed successfully.
netsh dhcp server v4 scope>_

```

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

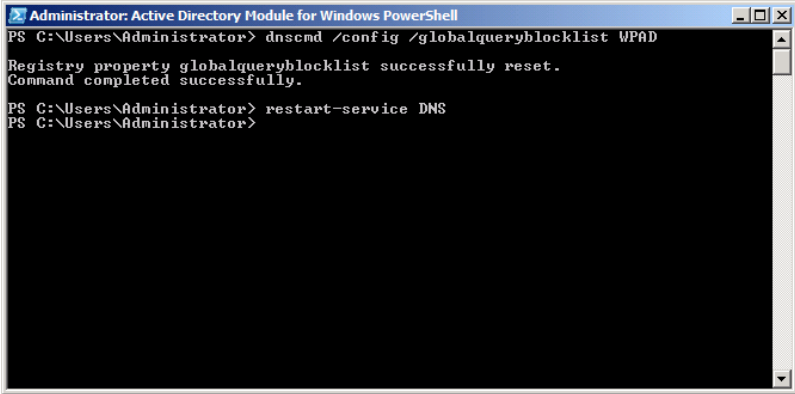
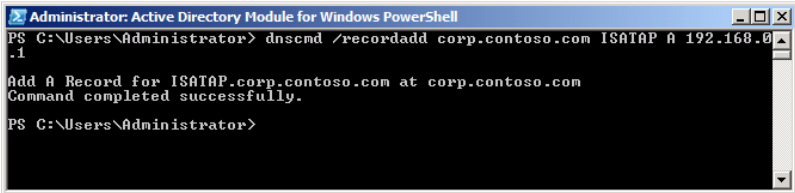
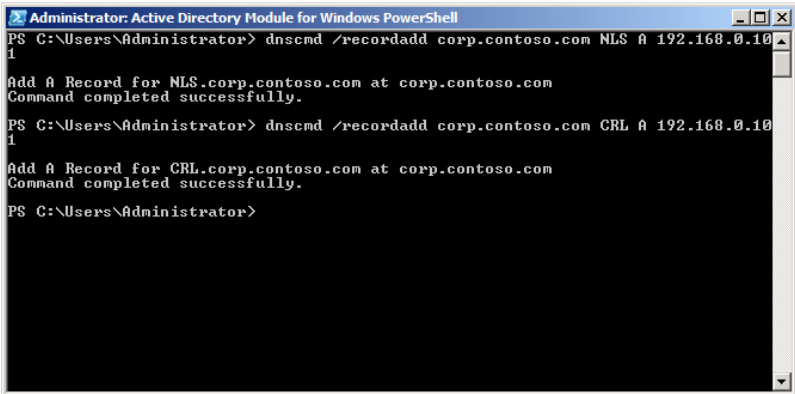
3.3 Préparation du DNS

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

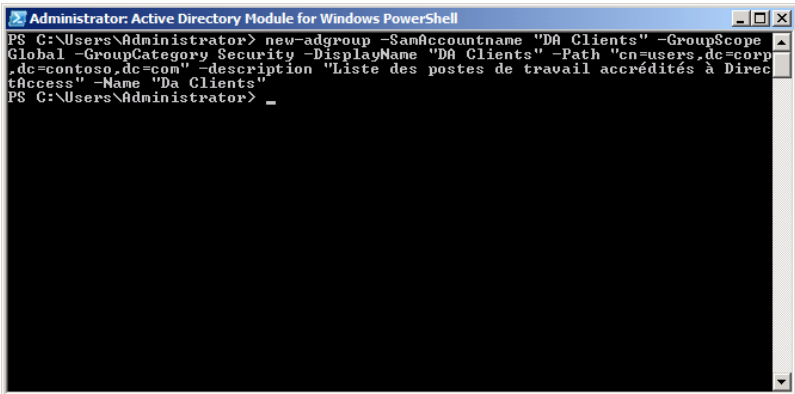
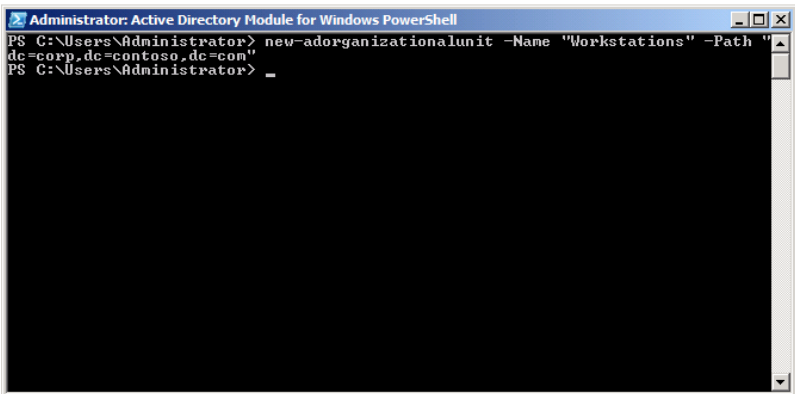
Le seul réel prérequis coté Active Directory, c'est de disposer d'un contrôleur de domaine opérant sous Windows 2008 SP1 au minimum. Après, nous n'avons besoin que d'aménagements ayant pour objectif de nous faciliter la vie. On distingue deux types d'aménagements :

- 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
 <pre>Administrator: Active Directory Module for Windows PowerShell PS C:\Users\Administrator> new-adgroup -samaccountname "DA Clients" -GroupScope Global -GroupCategory Security -DisplayName "DA Clients" -Path "cn=users,dc=corp ,dc=contoso,dc=com" -description "Liste des postes de travail accrédités à Direc tAccess" -Name "Da Clients" PS C:\Users\Administrator> _</pre>	<p>Le groupe de filtrage sera créé par une simple commande PowerShell. Ce groupe va nous permettre d'identifier les systèmes autorisés pour DirectAccess.</p>
 <pre>Administrator: Active Directory Module for Windows PowerShell PS C:\Users\Administrator> new-adorganizationalunit -Name "Workstations" -Path " dc=corp,dc=contoso,dc=com" PS C:\Users\Administrator> _</pre>	<p>Le conteneur créé permettra de positionner la stratégie de groupe dédiée aux clients DirectAccess. Un annuaire, ça se range.</p>

```

Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> new-adorganizationalunit -name "Servers" -Path "Dc=corp,dc=contoso,dc=com"
PS C:\Users\Administrator> new-adorganizationalunit -name "UAGDA" -Path "ou=servers,dc=corp,dc=contoso,dc=com"
PS C:\Users\Administrator> _

```

Coté serveurs, même combat, on les range.

```

Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> new-adgroup -SamAccountName "NAP Exceptions" -GroupScope Global -GroupCategory Security -DisplayName "NAP Exceptions" -Path "cn=Users,dc=corp,dc=contoso,dc=com" -description "Groupe identifiant les systèmes exemptés de présenter un état de santé" -name "NAP Exception"
PS C:\Users\Administrator> _

```

On va créer notre groupe de filtrage NAP.

```

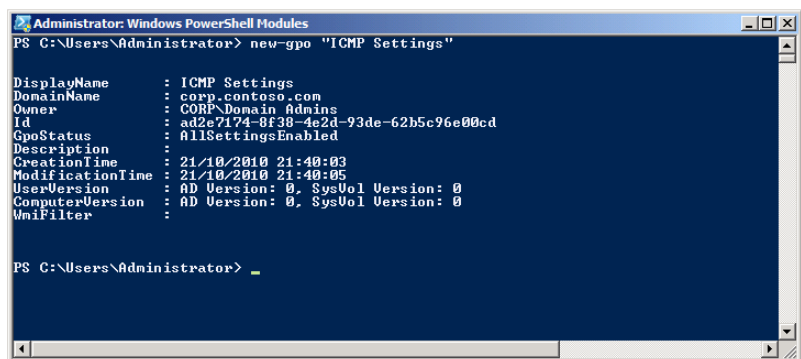
Administrator: Active Directory Module for Windows PowerShell
PS C:\Users\Administrator> add-adgroupmember -identity "NAP Exceptions" -members DC1$, APP1$, UAG1$
PS C:\Users\Administrator> _

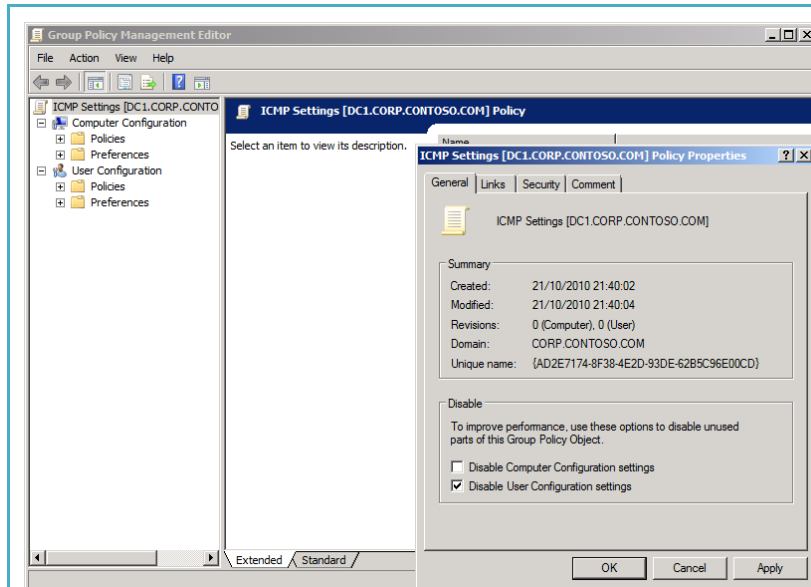
```

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

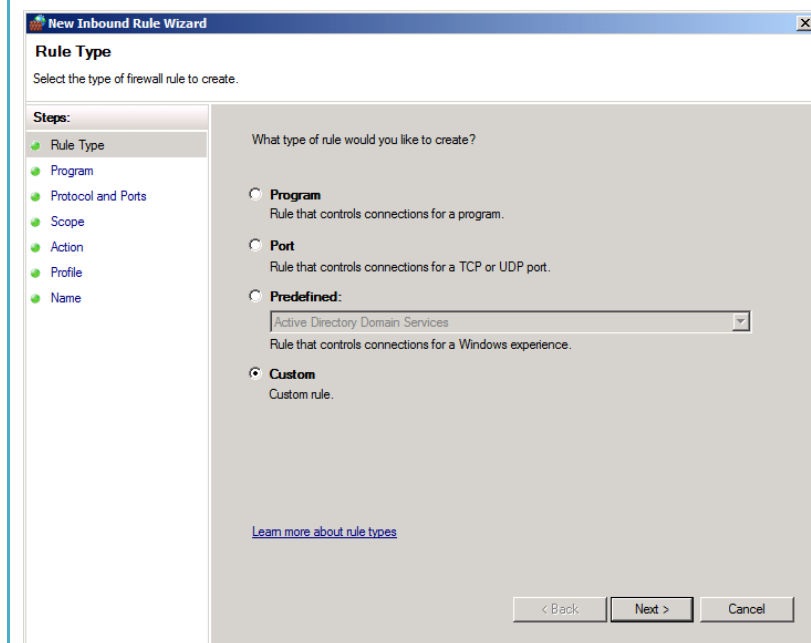
3.4.2 L'activation d'ICMP pour IPv4 et IPv6

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
 <pre> Administrator: Windows PowerShell Modules PS C:\Users\Administrator> new-gpo "ICMP Settings" DisplayName : ICMP Settings DomainName : corp.contoso.com Owner : CORP\Domain Admins Id : ad2e7174-8f38-4e2d-93de-62b5c96e00cd GpoStatus : AllSettingsEnabled Description : CreationTime : 21/10/2010 21:40:03 ModificationTime : 21/10/2010 21:40:05 UserVersion : AD Version: 0, SysVol Version: 0 ComputerVersion : AD Version: 0, SysVol Version: 0 WmiFilter : PS C:\Users\Administrator> _ </pre>	<p>Ici encore nous allons créer une nouvelle stratégie de groupe avec la CommandLet « New-GPO ».</p>



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



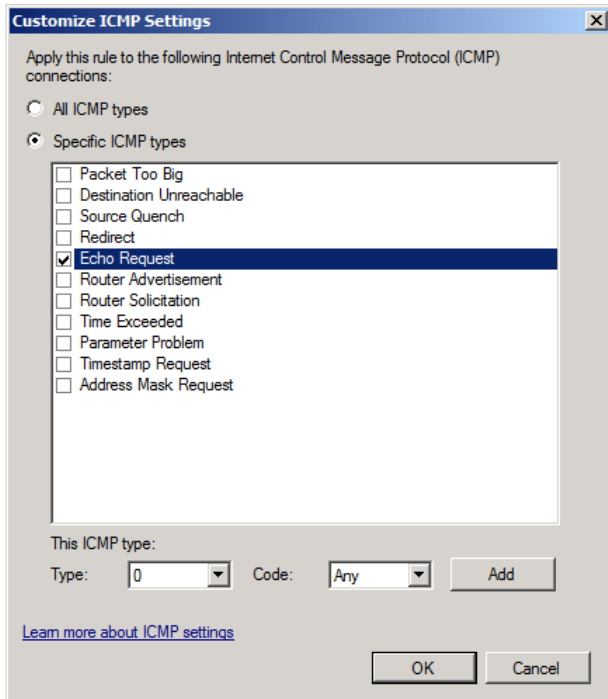
On va commencer par créer une règle de pare-feu personnalisée pour ICMPV4 en entrée.

The screenshot shows the 'Program' step of the 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program (selected), Protocol and Ports, Scope, Action, Profile, and Name. The main area asks 'Does this rule apply to all programs or a specific program?'. The 'All programs' radio button is selected, with the subtext 'Rule applies to all connections on the computer that match other rule properties.' The 'This program path:' option is unselected, with a text box and a 'Browse...' button. Below this, an example path is shown: 'c:\path\program.exe' and '%ProgramFiles%\browser\browser.exe'. The 'Services' section is also unselected, with a 'Customize...' button. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

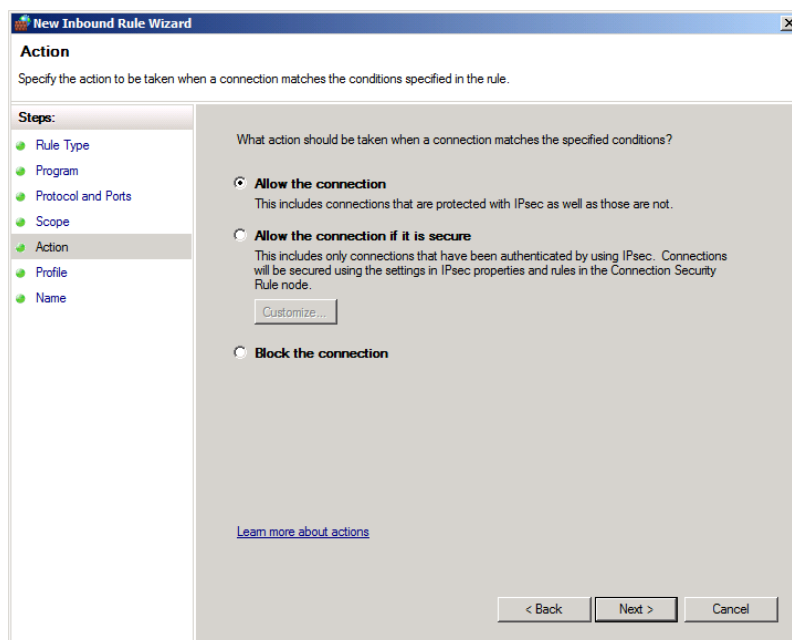
Cette règle va concerner tous les programmes sans distinction.

The screenshot shows the 'Protocol and Ports' step of the 'New Inbound Rule Wizard'. The left sidebar lists the steps: Rule Type, Program, Protocol and Ports (selected), Scope, Action, Profile, and Name. The main area asks 'To which ports and protocols does this rule apply?'. The 'Protocol type' dropdown is set to 'ICMPv4'. The 'Protocol number' is set to '1'. The 'Local port' dropdown is set to 'All Ports'. The 'Remote port' dropdown is also set to 'All Ports'. Below these, an example range '80, 443, 5000-5010' is shown. The 'Internet Control Message Protocol (ICMP) settings:' section has a 'Customize...' button. At the bottom, there are '< Back', 'Next >', and 'Cancel' buttons.

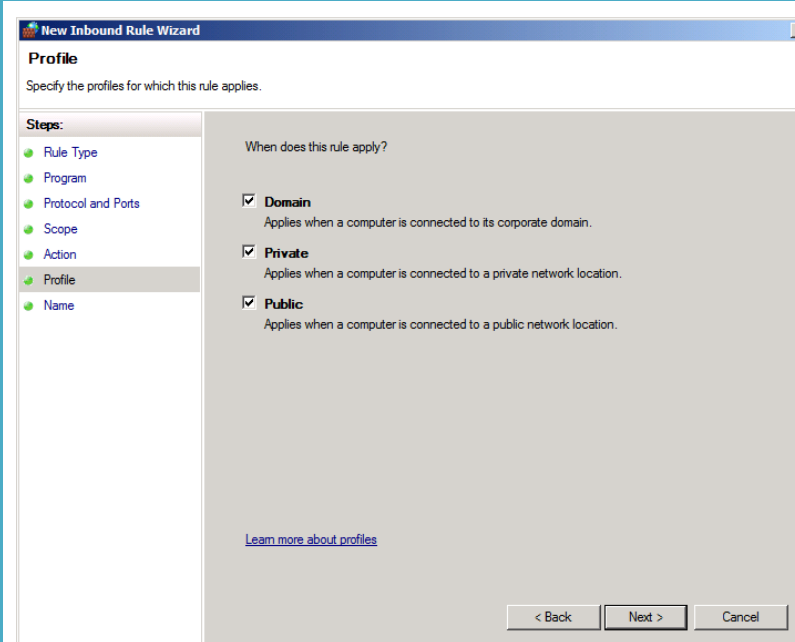
Mais précisément le protocole ICMPv4.



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.

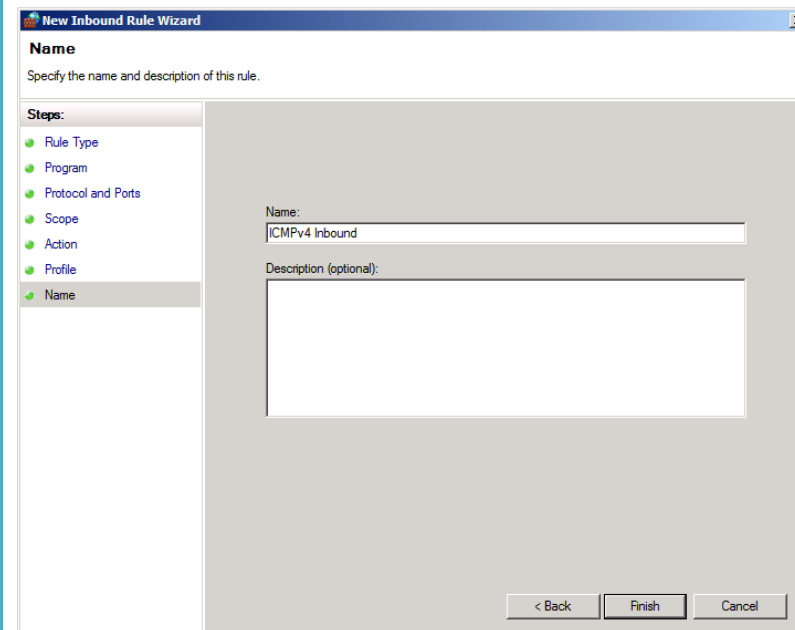


Cette règle va autoriser ICMPv4 en entrée.



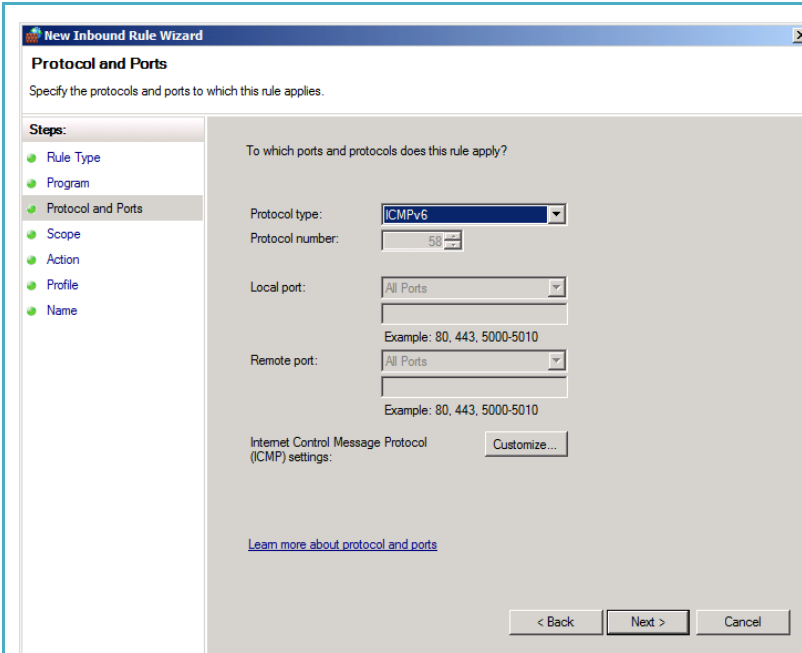
The screenshot shows the 'New Inbound Rule Wizard' window at the 'Profile' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Profile' with the instruction 'Specify the profiles for which this rule applies.' On the left, a 'Steps:' list includes 'Rule Type', 'Program', 'Protocol and Ports', 'Scope', 'Action', 'Profile' (highlighted), and 'Name'. The main area is titled 'When does this rule apply?' and contains three checked options: 'Domain' (Applies when a computer is connected to its corporate domain.), 'Private' (Applies when a computer is connected to a private network location.), and 'Public' (Applies when a computer is connected to a public network location.). A link 'Learn more about profiles' is at the bottom left. Navigation buttons '< Back', 'Next >', and 'Cancel' are at the bottom right.

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.



The screenshot shows the 'New Inbound Rule Wizard' window at the 'Name' step. The title bar reads 'New Inbound Rule Wizard'. The main heading is 'Name' with the instruction 'Specify the name and description of this rule.' On the left, the 'Steps:' list is the same as the previous step, with 'Name' highlighted. The main area has a 'Name:' label followed by a text box containing 'ICMPv4 Inbound'. Below it is a 'Description (optional):' label followed by a larger text box. Navigation buttons '< Back', 'Finish', and 'Cancel' are at the bottom right.

Reste plus qu'à la nommer.



New Inbound Rule Wizard

Protocol and Ports

Specify the protocols and ports to which this rule applies.

Steps:

- Rule Type
- Program
- Protocol and Ports**
- Scope
- Action
- Profile
- Name

To which ports and protocols does this rule apply?

Protocol type: **ICMPv6**

Protocol number: **58**

Local port: **All Ports**

Example: 80, 443, 5000-5010

Remote port: **All Ports**

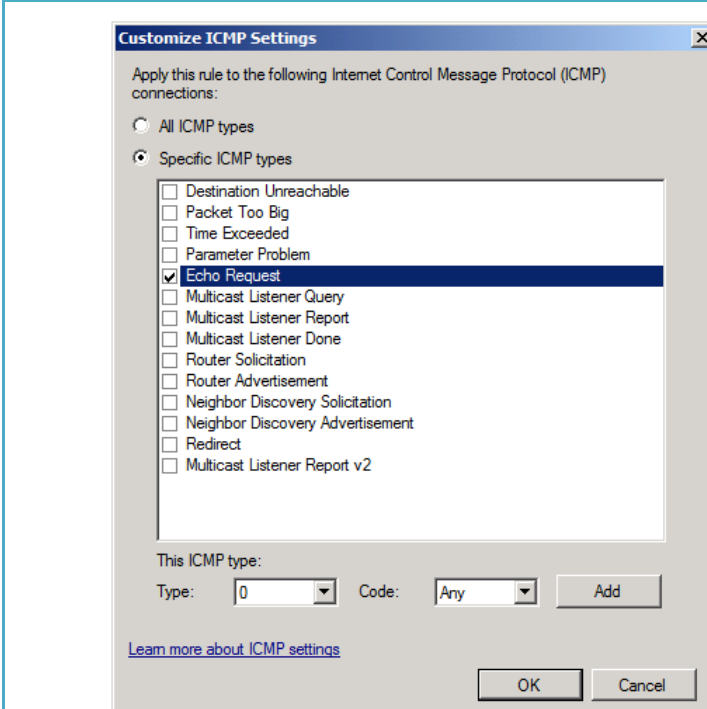
Example: 80, 443, 5000-5010

Internet Control Message Protocol (ICMP) settings: **Customize...**

[Learn more about protocol and ports](#)

< Back Next > Cancel

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



Customize ICMP Settings

Apply this rule to the following Internet Control Message Protocol (ICMP) connections:

☐ All ICMP types

☒ Specific ICMP types

- ☐ Destination Unreachable
- ☐ Packet Too Big
- ☐ Time Exceeded
- ☐ Parameter Problem
- ☒ **Echo Request**
- ☐ Multicast Listener Query
- ☐ Multicast Listener Report
- ☐ Multicast Listener Done
- ☐ Router Solicitation
- ☐ Router Advertisement
- ☐ Neighbor Discovery Solicitation
- ☐ Neighbor Discovery Advertisement
- ☐ Redirect
- ☐ Multicast Listener Report v2

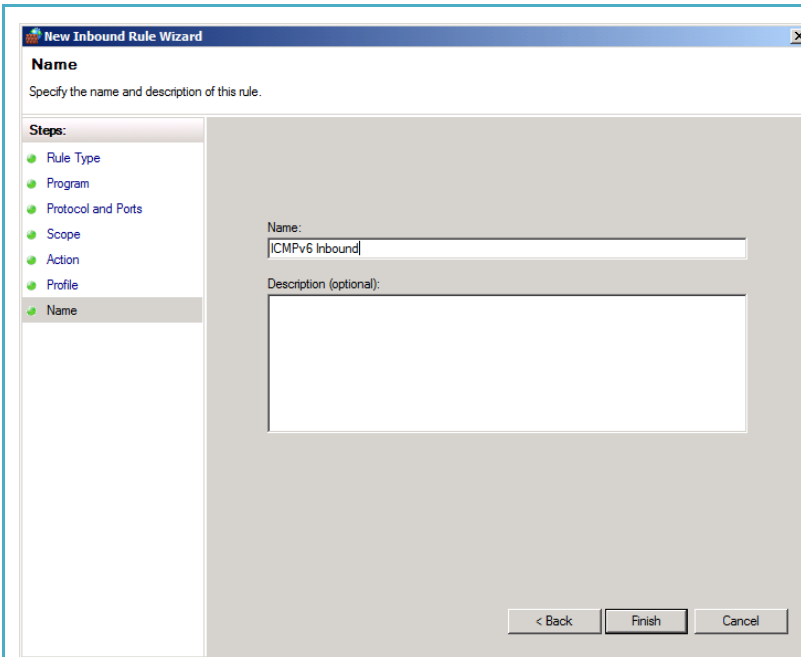
This ICMP type:

Type: **0** Code: **Any** **Add**

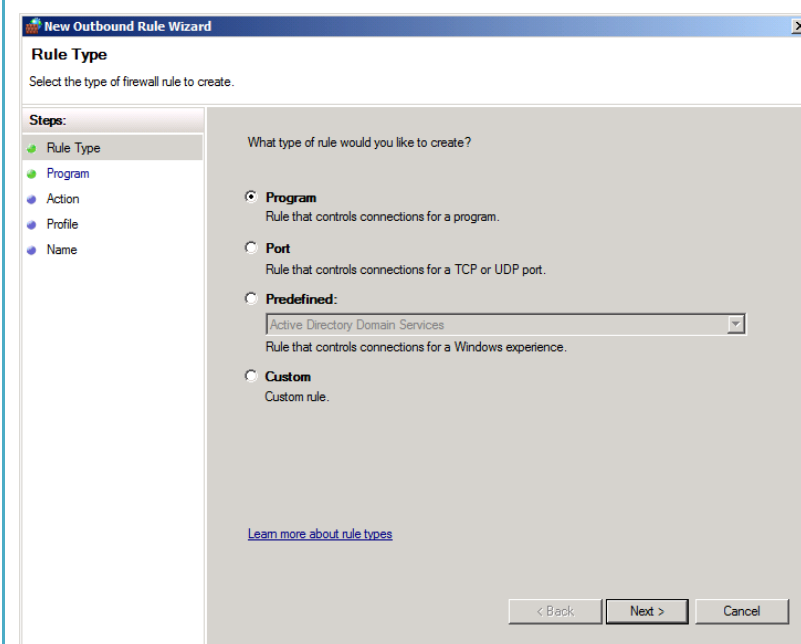
[Learn more about ICMP settings](#)

OK **Cancel**

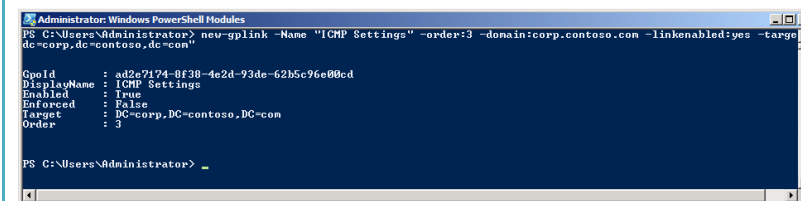
Toujours pour le même type de message ICMP.



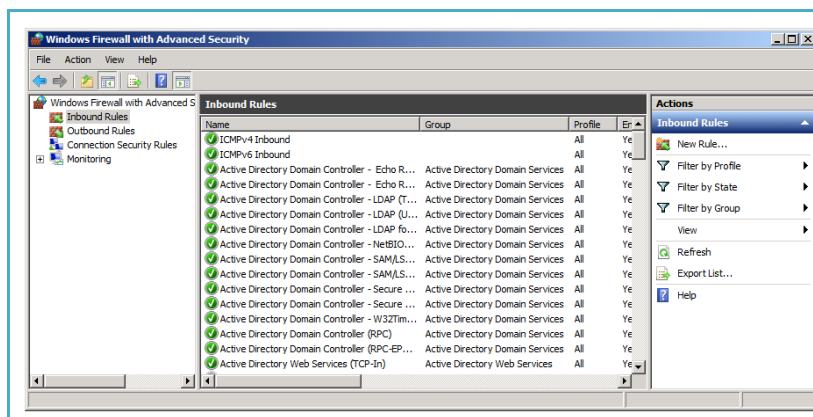
Et la nommer.



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.

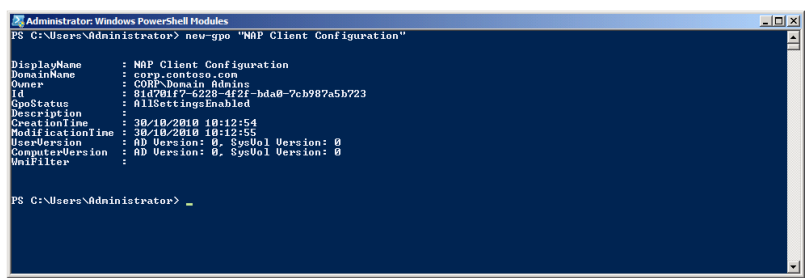
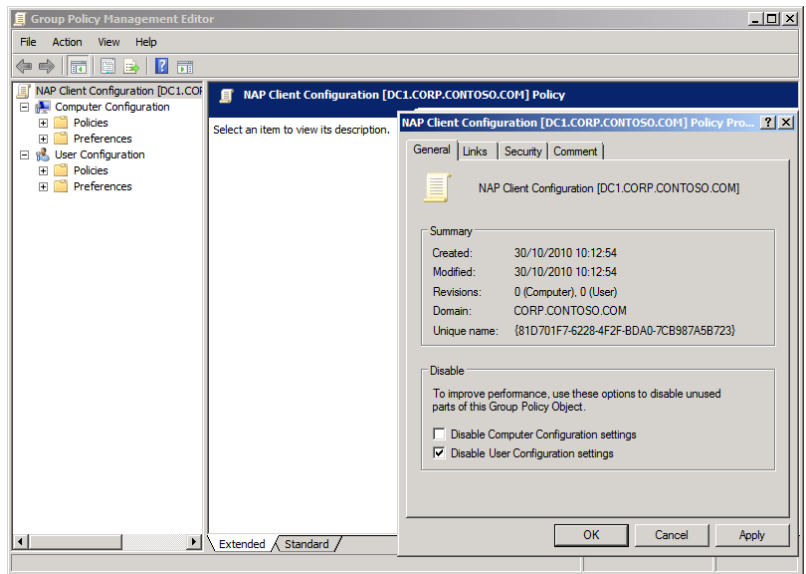
3.5 Paramétrage du client Network Access Protection

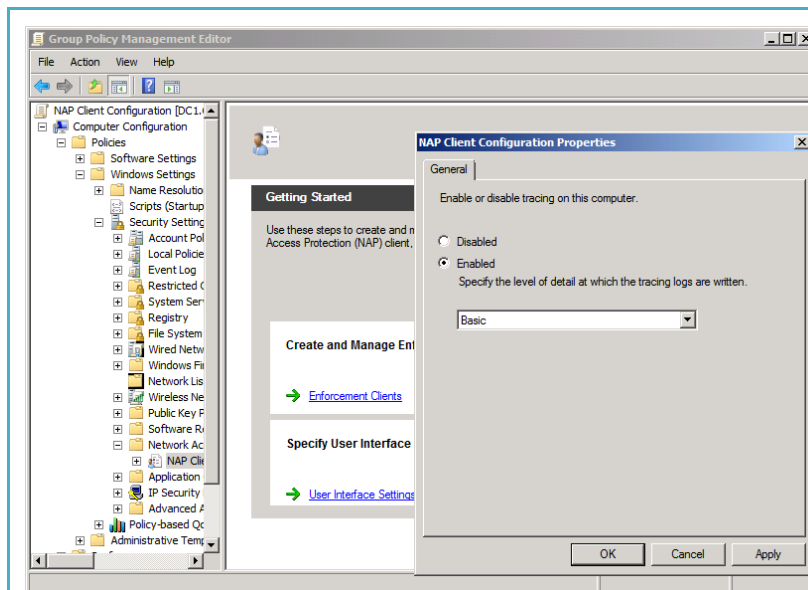
La configuration de Network Access Protection qui sera mise en œuvre par UAG contiendra :

- 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

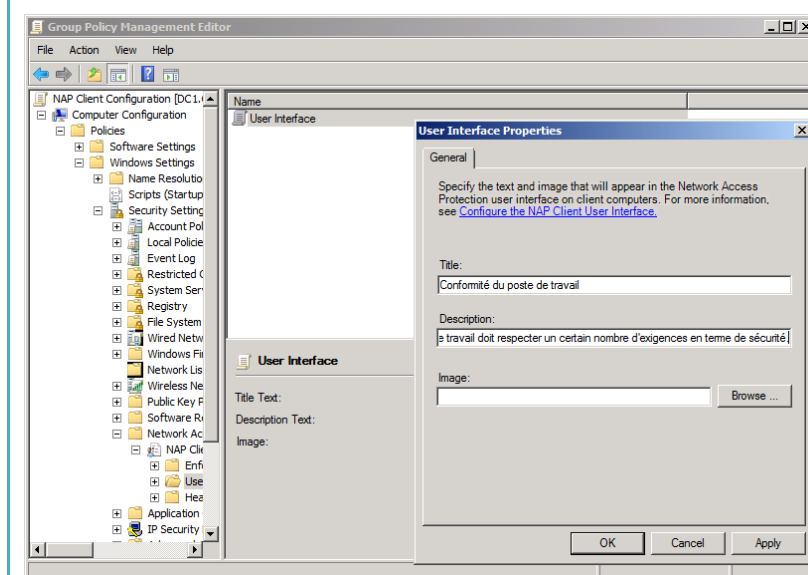
Même si cette configuration fonctionne, il manque quelques détails d'ordre esthétique :

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

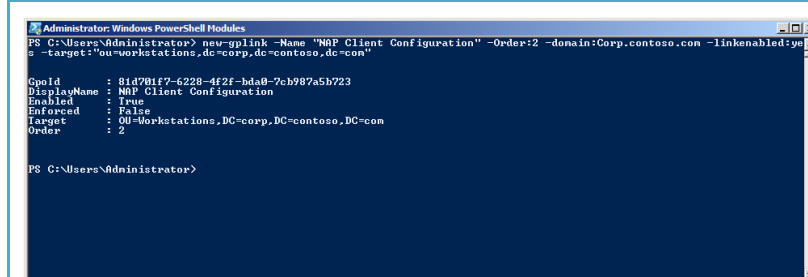
Impression écran	Description
 <pre> Administrator: Windows PowerShell Modules PS C:\Users\Administrator> new-gpo "NAP Client Configuration" DisplayName : NAP Client Configuration DomainName : corp.contoso.com Owner : CORP\Domain Admins Id : 81D701F7-6228-4F2F-BDA0-7CB987A5B723 GpoStatus : AllSettingsEnabled Description : CreationTime : 30/10/2010 10:12:54 ModificationTime : 30/10/2010 10:12:55 UserVersion : AD Version: 0, SysVol Version: 0 ComputerVersion : AD Version: 0, SysVol Version: 0 Unifilter : </pre>	<p>On va donc commencer par créer une stratégie de groupe qui sera dédiée à la mise en place de notre paramétrage.</p>
	<p>Cette stratégie de groupe n'a pas besoin de paramètres utilisateurs, on va donc désactiver la section.</p>



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 !