**Formation Windows 10/11 et la gestion à distance - Sr10-Sr11 –**

Michel Cabaré / www.cabare.net / michel@cabare.net

Windows 10-11 Accès et gestion à Distance , Firewall, Rdp …  
 - Sr 10 – Sr11- Aout 2022

|  |  |  |
| --- | --- | --- |
| https://WWW.CABARE.NET © |  |  |

|  |  |
| --- | --- |
|  |  |

**table des matiÈres**

Pare-Feu Windows 4

Activation - Désactivation : 4

Via l’interface 4

Via GPO 5

Via Powershell 5

Version Avancée : 6

Règles groupes et filtrage  : 7

Règles entrantes  prédéfinies recherche: 7

Règles Propriétés: 10

Création Règles entrantes  personnelles: 11

Stratégies gestion Pare-Feu 14

importer Exporter une stratégie  : 14

Stratégie Profil Domaine – standard via gpedit.msc  : 14

Stratégie de Domaine  : 16

Netstat & Tasklist 17

Liste des ports en cours d'utilisation  : 17

Liste des processus par PID  : 17

Administration distante via RDP 18

Terminal Server – bureau à Distance: 18

Bureau à Distance sur Serveur 2008r2: 18

Versions - options du Client Bureau à Distance 19

Services Bureau à Distance 2008 21

Utiliser le Bureau à Distance depuis un client: 22

Pare-Feu et N° Port par défaut 23

Port TCP du Bureau à Distance (modification) 24

MMC à Distance 26

Gestion de l'ordinateur: 26

MSG – (netsend) 27

MSG n'est pas NetSend: 27

Syntaxe MSG: 27

MSG hors TSE dans domaine: 28

Partages Administratifs - UAC 29

Utiliser les partages Administratifs: 29

Effet de l’UAC: 30

SC - Service à distance 33

Sc en ligne de commande : 33

Nom d'un service 33

Etat d' un service sc query 34

Démarrer arrêter un service local sc start stop 35

Démarrer arrêter un service distant 36

MBSA poste distant 37

MBSA 2.3 : pas de successeur à venir : 37

Lancement MBSA 2.3 en local: 37

Analyse depuis WSUS 39

Analyse depuis site de Microsoft 40

Adressage IP – Pare-feu: 41

Comptes Utilisateurs: 41

Services et paramétrages: 42

Agent Windows Update: 42

Récapitulatif procédure MBSA poste Distant: 43

Procédure MBSA sur Seven: 44

Netstat & Tasklist 48

Liste des ports en cours d'utilisation  : 48

Liste des processus par PID  : 48

Netsh - Advfirewall 49

Activer – Désactiver le pare-feu 49

Netsh Advfirewall – nouvelle commande 49

Restaurer les paramètres par défaut du Firewall 49

Activer – désactiver le pare feu par profil 49

Activer – désactiver ICMP 50

Ouvrir un Port 50

Autoriser un programme 51

Activer – désactiver des services 51

importer-exporter un profil .wfw : 51

Activer Désactiver le pare-feu  7: 52

Netsh 53

Principe de netsh – contexte 53

Netsh dump Mémorisation – Récupération d’une configuration : 55

Nom des interfaces réseau  : 55

Modification d’une adresse IP et de son masque : 55

En une seule commande : 56

En descendant les niveaux : 56

En une seule commande : 56

En descendant les niveaux : 56

insertion dans un batch : 56

Modification d’une adresse DNS : 57

Changer une Adresse IP en Powershell 58

Lister les cartes réseau - Get-NetAdapter 58

Créer une Adresse Ip – New-NetIpAddress 58

Changer le DNS – Set-DnsClientServerAddress 59

Vérif configuration - Get-NetIPConfiguration 59

Changer une Adresse Ip – New-NetIpAddress 60

Valider Dévalider DCHP – Set-NetIpAddress 60

Reset carte réseau – Restart-Netadapter 60

Supprimer une Adresse IP – Restart-Netadapter 60

# Pare-Feu Windows

## Activation - Désactivation :

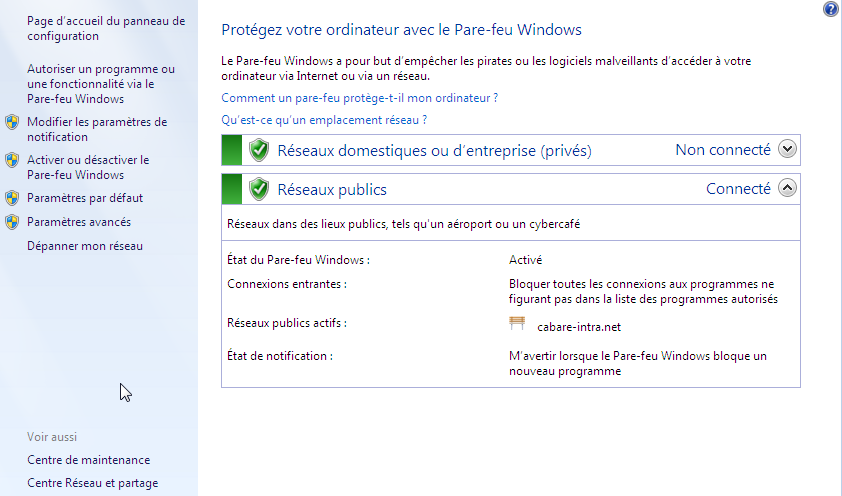
### Via l’interface

L'accès standard, permettant l'activation ou la désactivation, et la gestion de quelques exceptions "prévues", se trouve dans **windows 10** via

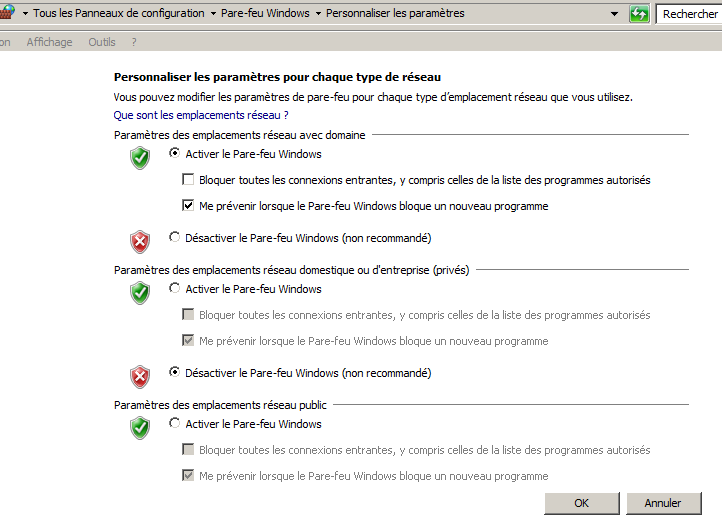
**Paramètres / Réseau et Internet / Ethernet**

Anciennement dans le **Panneau de Configuration / Pare feu Windows**

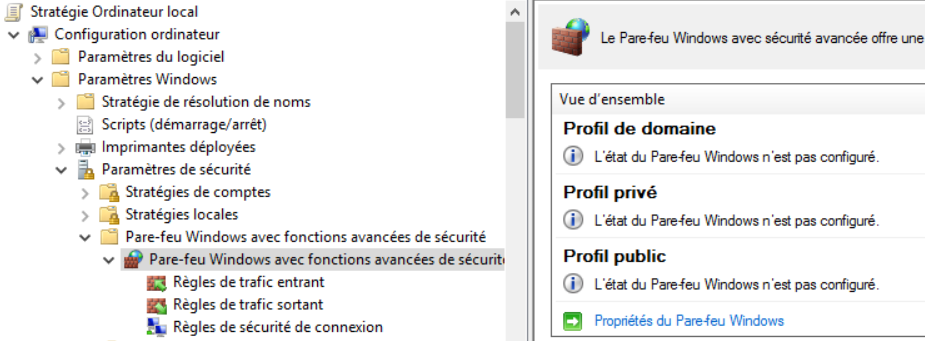


On peut l’ **Activer – Désactiver** selon les profils existants…

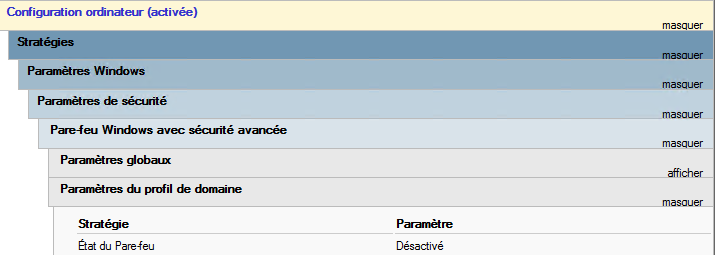


### Via GPO

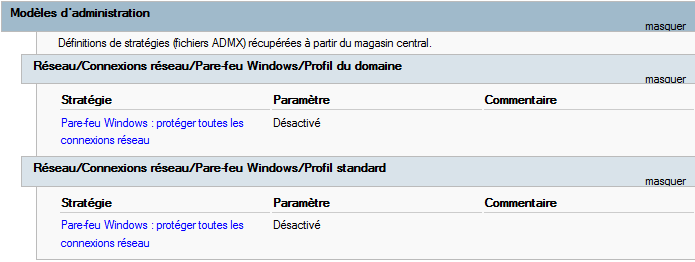
Soit Locale



Soit via une GPO classique



Mieux avec un 2° réglage cette fois-ci dans les modèles d’administration **Ordinateur / Réseau/Connexion Réseau/Pare-feu Windows**…



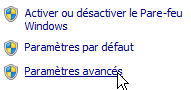
### Via Powershell

Une commande existe du type en spécifiant **True** ou **False** selon le besoin…

**Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True**



## Version Avancée :

La version avancée, permettant des réglages plus fins, (règles entrantes, sortantes) est disponible via les **Paramètres avancés** du **Pare-feu standard**…

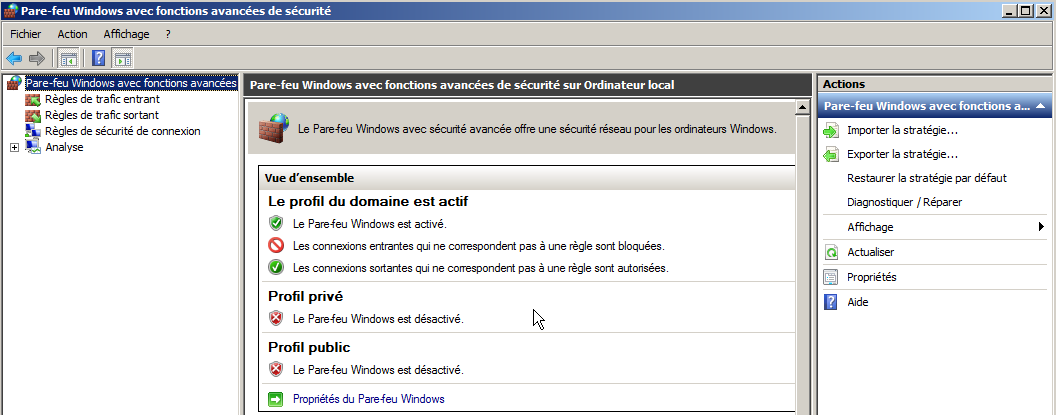
Cette version se trouve également accessible directement dans les outils d'administration

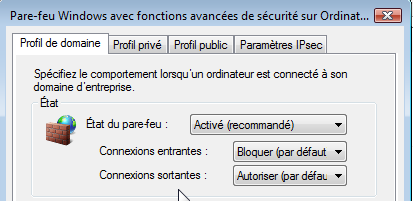
**Panneau de Configuration / outils d'Administration**

**Pare-feu Windows avec fonctions avancées de sécurité**

****

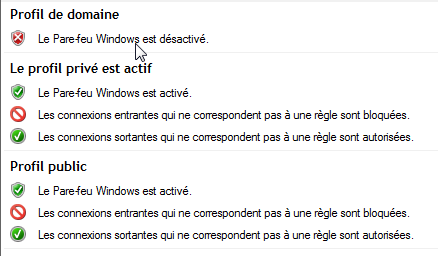
Donnant



à travers les **propriétés du pare-feu** on peut choisir d'armer ou non le pare-feu selon le type réseau …

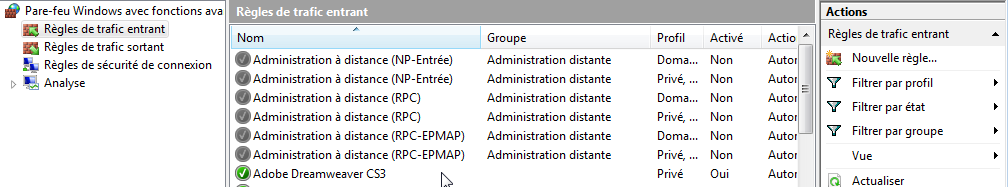
…

pour le désactiver par exemple dans le cas d'un domaine…



## Règles groupes et filtrage  :

il existe des règles entrantes pré-définies :



pour afficher une liste plus restrictive on peut filtrer par

* profil réseau :

**Domaine – Prive – Public**

* état de la règle :

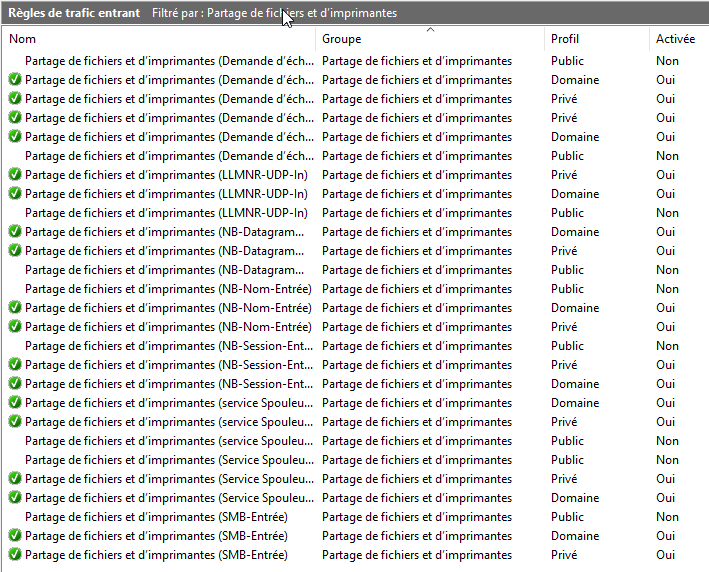
**Activée – non Activée**

* Groupe de classification de la règle :

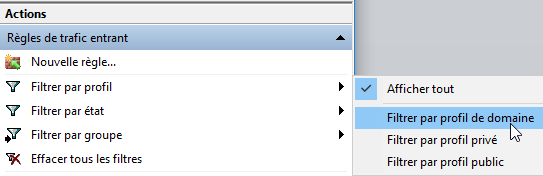
**Réseau de Base – Administration distante – partage fichiers et imprimantes…**

## Règles entrantes  prédéfinies recherche:

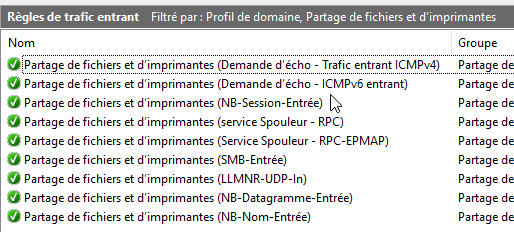
il existe des règles entrantes pré-définies : Cherchons par exemple la règle autorisant **ICMP** en **IP** version **4**, il y a beaucoup de règles, qui sont regroupées dans la catégorie **Partage fichiers et imprimantes**)



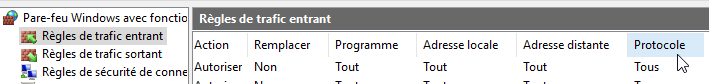
Pour limiter notre affichage, on va demander uniquement les règles applicables sur un Domaine



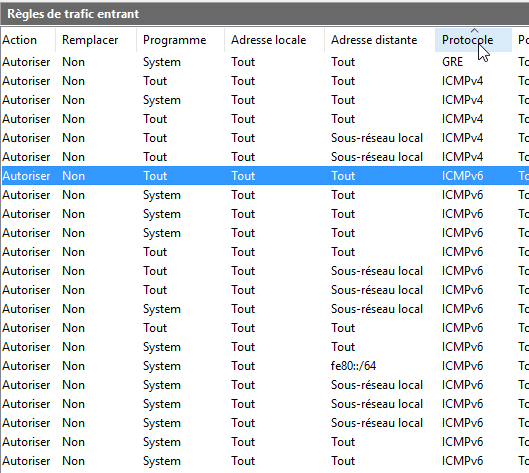
qui seront valables selon le profil réseau:



On peut chercher autrement que par filtre et Profil, puisque plusieurs propriétés sont disponible…

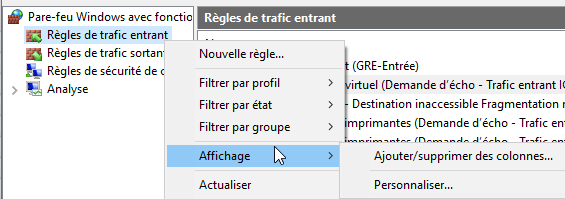


Si on classe les règles par protocole, alors on obtient et il est facile de chercher ICMP V4!

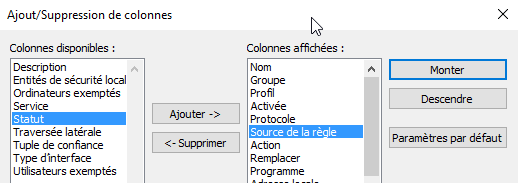


On peut aussi modifier l'aspect / l'information pour l'affichage des règles

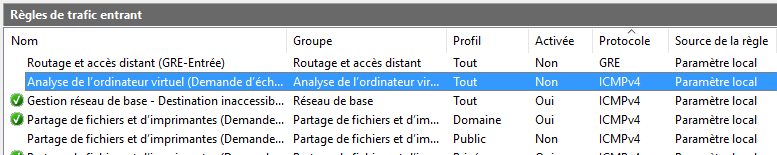
Dan **Règles de trafic entrant** clic droit / **Affichage**



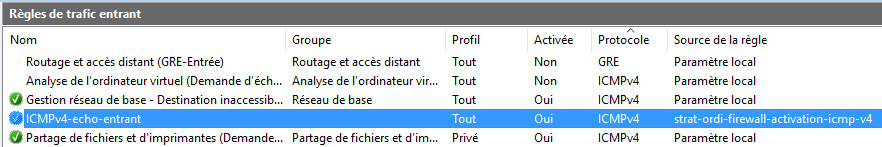
On ajoute / supprime ou modifie l'ordre des colonnes



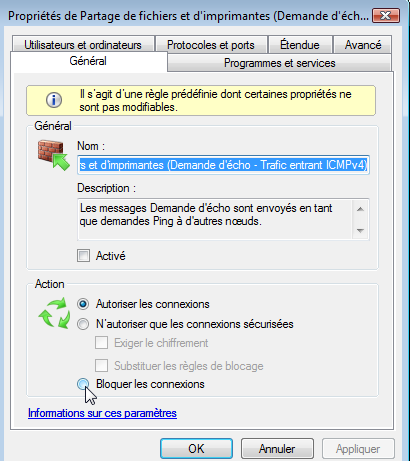
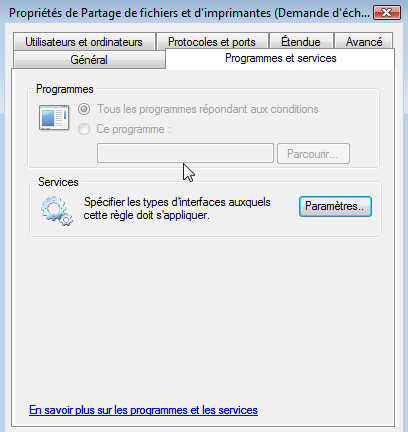
Par exemple ici on rapproche la colonne **protocole**, et on ajoute une nouvelle colonne **Source de la règle**



Cela permet de mieux voir ce qui est géré localement, et ce qui est dirigé via le domaine ! le nom exact de la GPO apparaît !

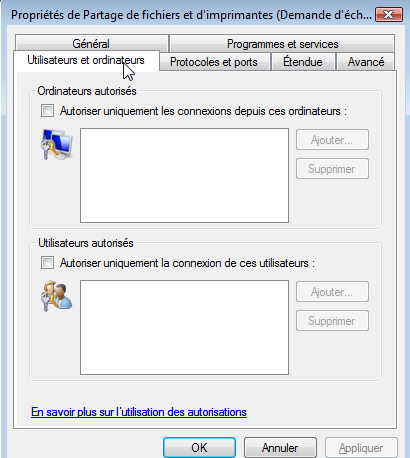
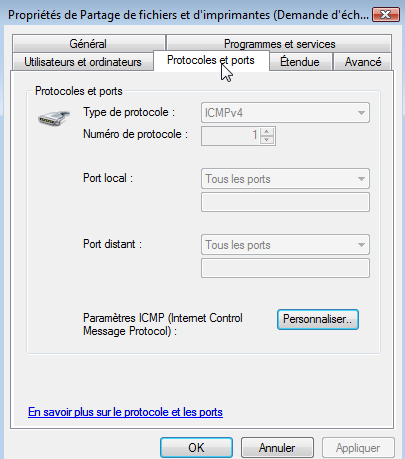


## Règles Propriétés:

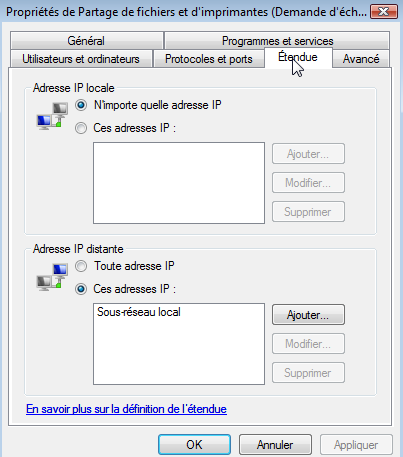
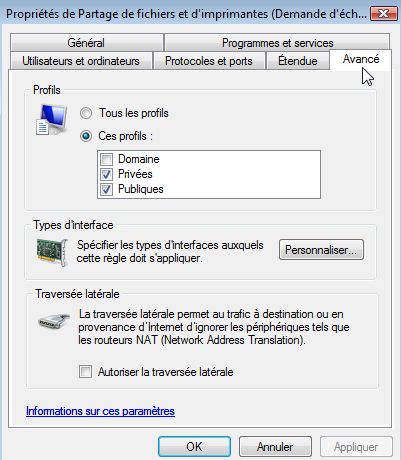


plusieurs onglets permettent d'affiner la règle:

des machines, des users

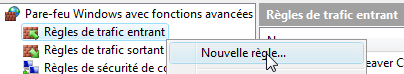


Des adresses IP des profils réseau



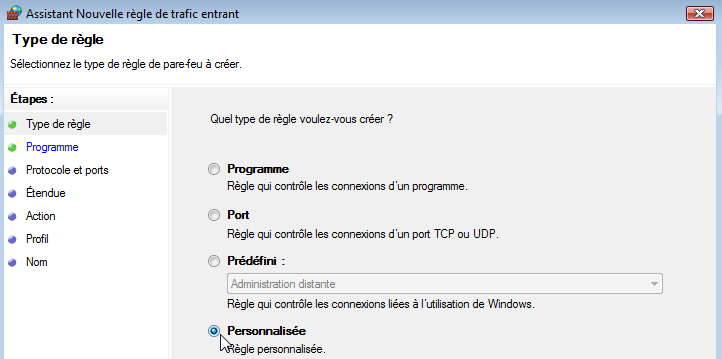
**N.B:** Selon que la règle soit prédéfinie ou non, ces onglets ne sont pas tous modifiables dans leur intégralité.

## Création Règles entrantes  personnelles:

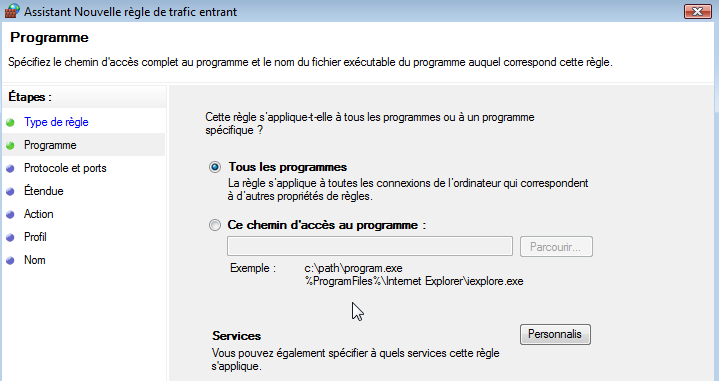
On peut se créer de nouvelles règles, soit pour être plus fins que les règles prédéfinies, soit gérer d'autres filtrages :

Par exemple, on veut créer une Règle entrante  protocole ICMP – V4 de base:

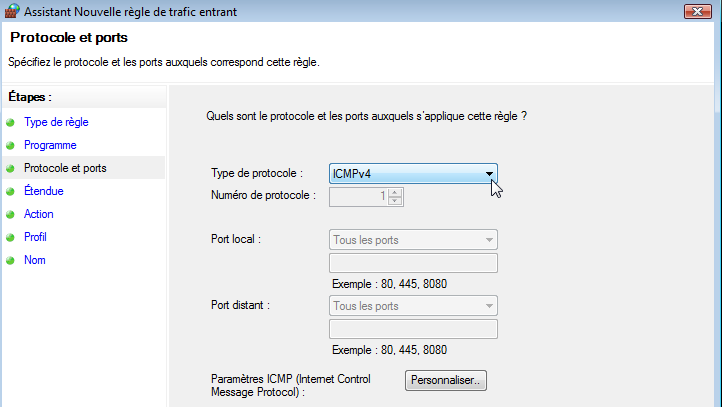
On demande **personnalisée**

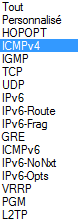
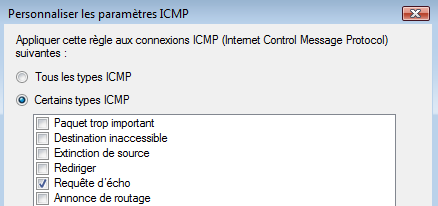


A **Tous les programmes**

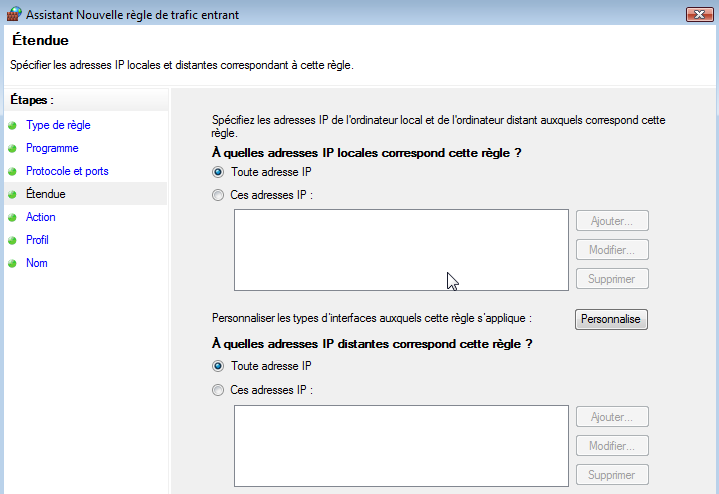


On affine les réglages

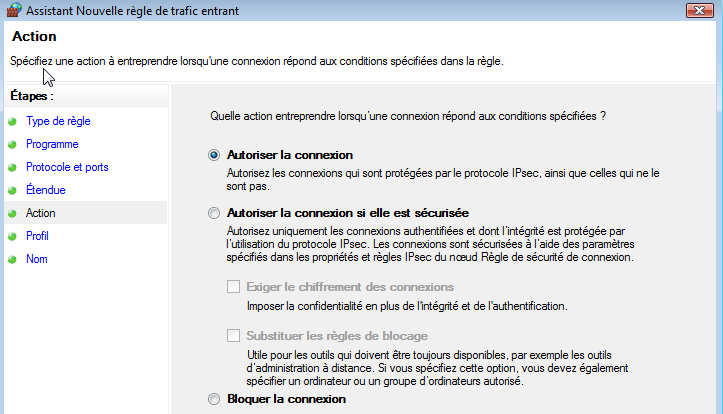




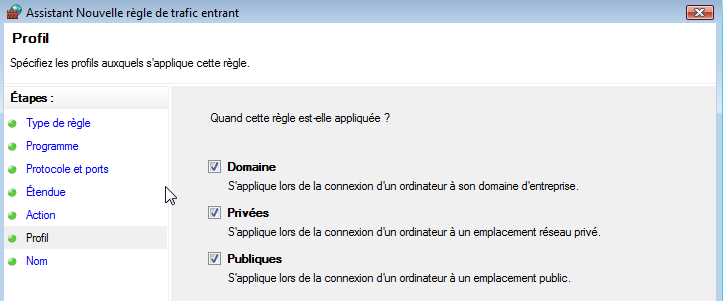
On indique toutes les adresses ip



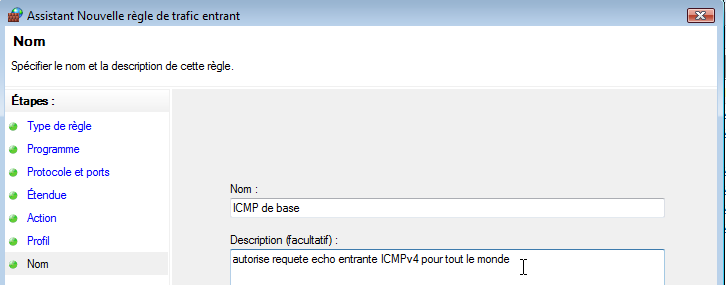
Et le comportement de la règle - **Autoriser**



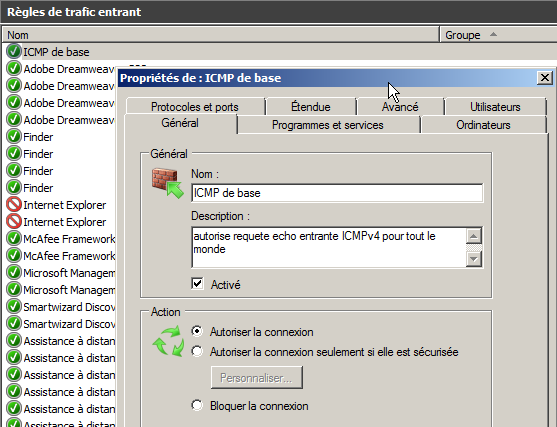
Selon le profil réseau- les 3



Il ne reste plus qu'a lui donner un nom

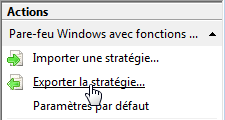


Et voici notre nouvelle règle !



# Stratégies gestion Pare-Feu

## importer Exporter une stratégie  :

On peut importer ou exporter une configuration de pare-feu via des fichiers ….**wfw** spécifiques:

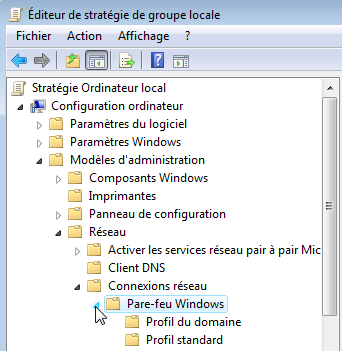
cela marche à partir de **Seven** et **2008**…et cela peut s'appliquer par batch via **netsh**

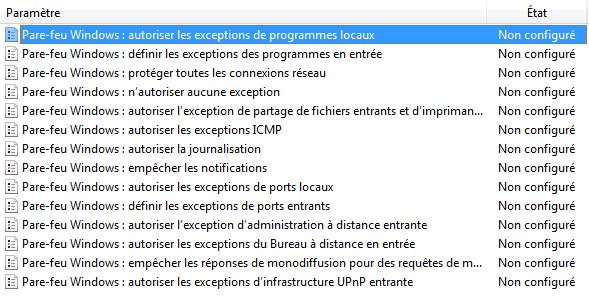
(cf chapitre netsh)

## Stratégie Profil Domaine – standard via gpedit.msc  :

au niveau **ordinateur**…

**Modèles / Réseau / Connexions réseau / Pare-feu Windows / Profil…**

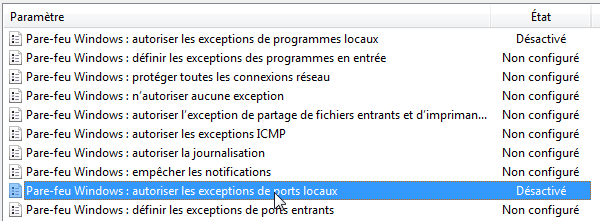
 donnant sous **XP+sp2** ou **Vista**



le pare-feu peut être paramétré sur le **domaine**, ou en **standard (workgroup)**

Il prend de manière générale deux listes, une définie par stratégies, et l'autre définie localement.

Il est possible de désactiver la possibilité de modifier les listes localement…

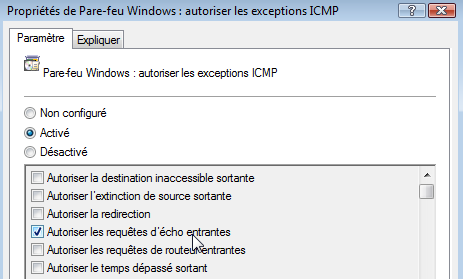


et du coup dans le pare-feu, on ne peut plus modifier la configuration…



On peut autoriser ICMP juste avec réponse de ECHO

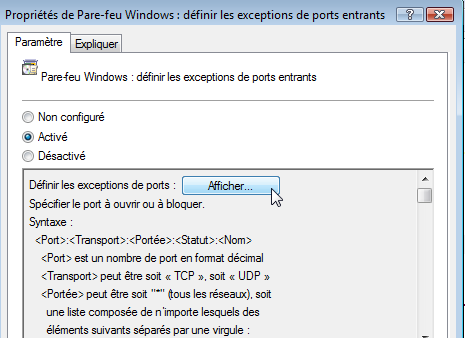




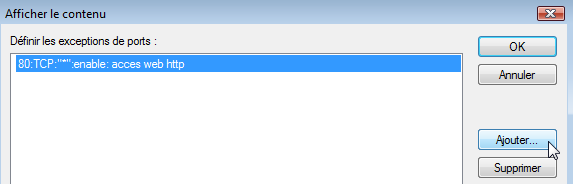
On peut définir un N° de port entrant :



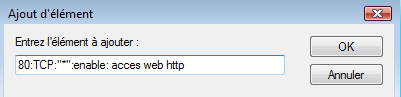
ce qui amène :



Avec des règles qui suivent une syntaxe particulière :



Avec des règles qui suivent une syntaxe particulière :

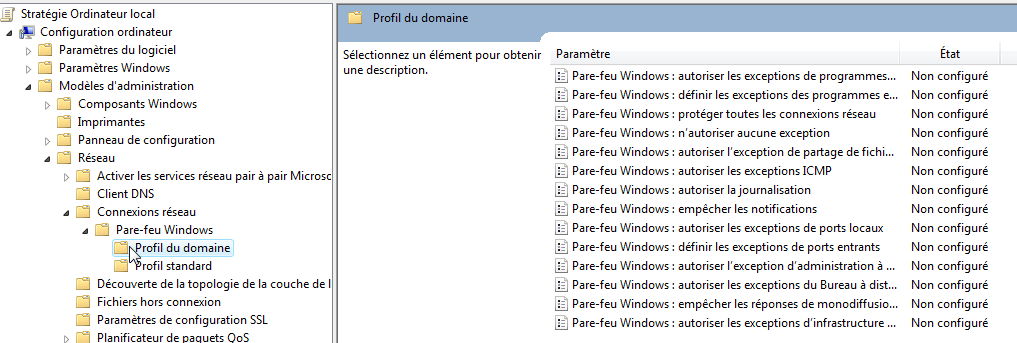


**80:TCP:"\*":enable: acces web http**

**6800:TCP:"\*":enable: vnc**

## Stratégie de Domaine  :

Bien sur elles sont utilisables : au niveau **ordinateur**…



# Netstat & Tasklist

## Liste des ports en cours d'utilisation  :

La commande **netstat** permet avec les options **–ano** de connaitre les n° de pid des processus associés aux n° de ports

**netstat –ano**

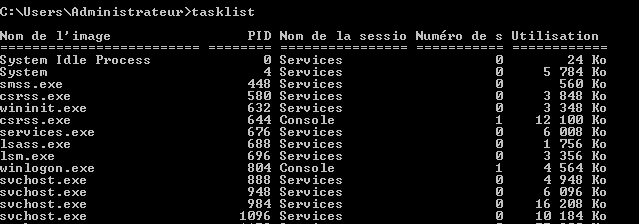


qui utilise le port 668 ?

le PID 1984…

## Liste des processus par PID  :

La commande **tasklist** permet d'avoir les processus associés aux PID,



le PID 1984…

c'est Carbonite !



et les services sont affichables, avec l'options **/SVC** par exemple ici svchost en PID ***984*** correspondrait à Windows defender… !



# Administration distante via RDP

## Terminal Server – bureau à Distance:

Le principe est le même, on utilise en effet le protocole **RDP Remote Desktop Protocol** pour accéder à une machine distante.

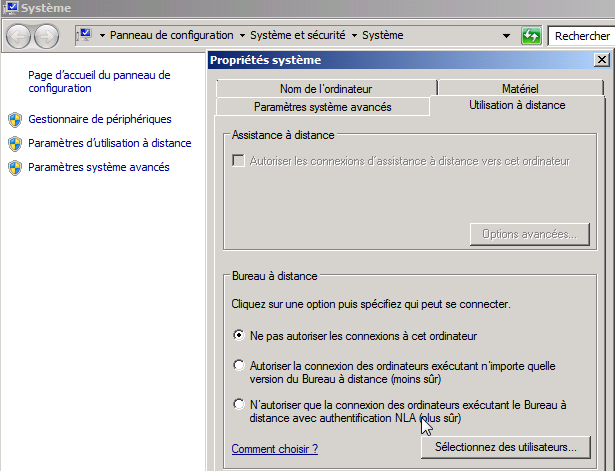
Ce protocole est celui utilisé pour configurer les services Terminal Server, services qui ont fait l'objet de plusieurs évolutions …

Quelques règles pour se repérer :

* Sous 2008 SRV : il faut activer le Bureau à distance
* Sous 2003 SRV : Si les services Terminal Server sont déjà opérationnels, il n'y à pas à activer le Bureau à Distance
* Sous 2000 SRV : Si les services Terminal Server sont déjà opérationnels, il n'y a rien à faire de plus
* Sous 2000 SRV : Terminal Server peut s'installer en mode Administration à Distance, ne nécessitant pas de licences spécifiques supplémentaires. Ce mode restreint est réservé aux administrateurs pour … l'administration !

## Bureau à Distance sur Serveur 2008r2:

Dans les propriétés de **ordinateur**, via **Paramètres d'utilisation à distance**, dans l'onglet **Utilisation à Distance**

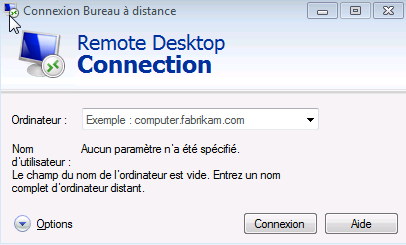
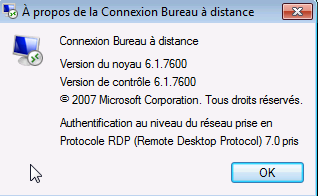


A priori si on veut se laisser la possibilité d'administrer le serveur depuis des postes XP ou Seven, il faut demander … **n'importe quelle version du Bureau à distance**…

## Versions - options du Client Bureau à Distance

Seven apporte sa mise à jours… Le fichier client rdp est **mstsc.exe**

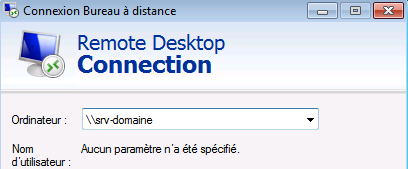
Pour connaître la version de RDP il suffit de demander "**A propos**" via le menu contextuel sur la boite de dialogue **Tous les programmes / Accessoires /** **Connexion Bureau à distance**



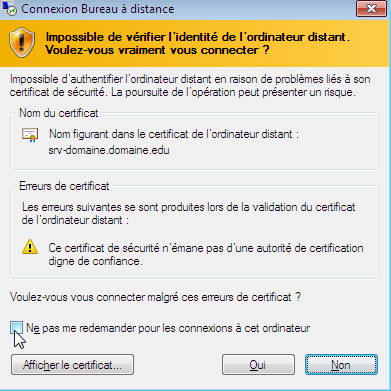
Il faut bien sur se connecter et s'identifier

**N.B**: Par défaut est que les administrateurs de Domaine peuvent ouvrir une session Bureau à Distance.

**N.B**: Si une session locale est ouverte avec le compte homonyme, elle est fermée automatiquement (il faut plutôt créer un autre compte spécifique…).



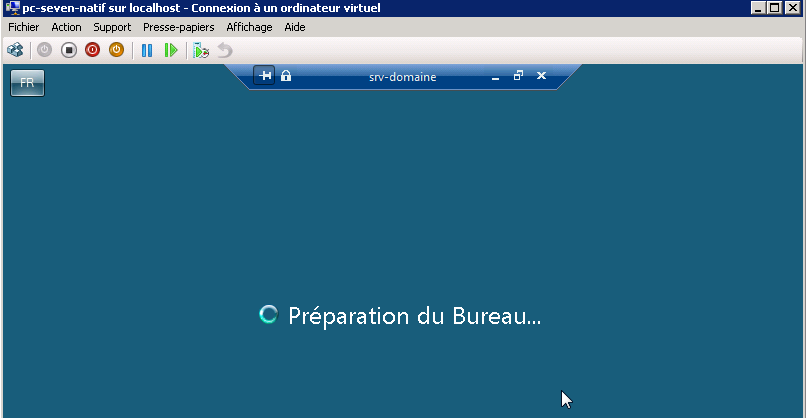
L'authentification est immédiate si on est dans le même domaine



Mais elle peut demander une confirmation si on n'est pas dans le même domaine

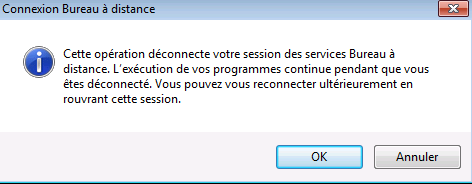
On peut éviter une re-confirmation pour la prochaine session

L'ouverture de session amène:

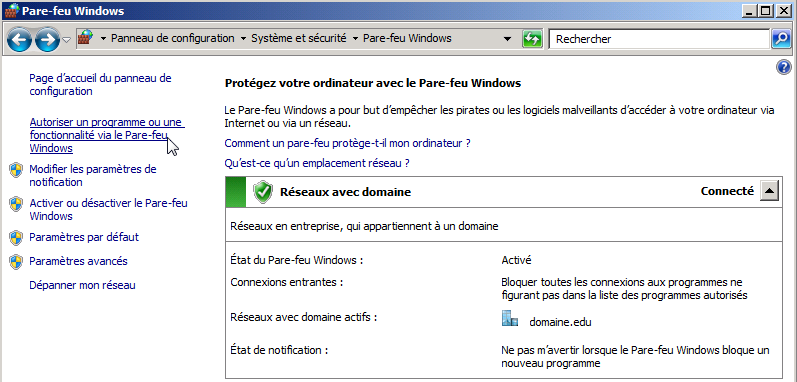


Il ne faut jamais quitter une session en fermant…

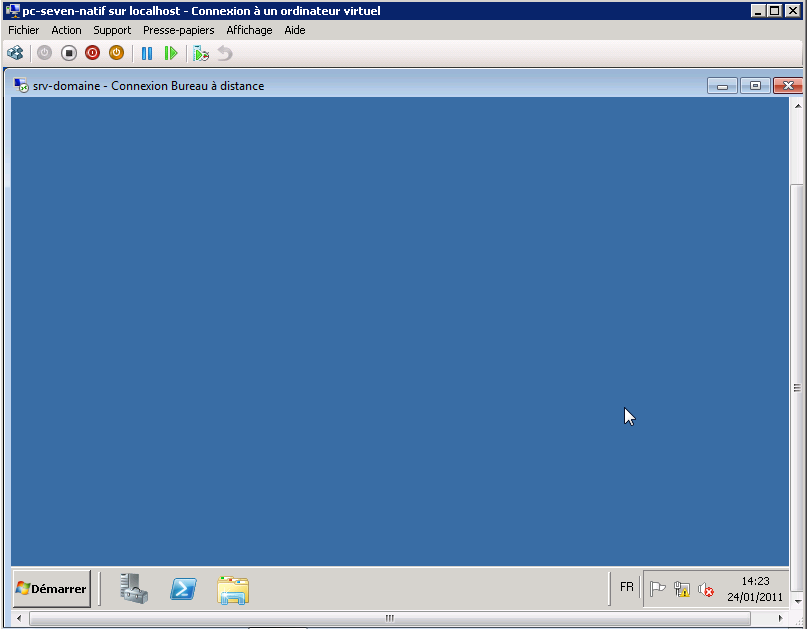


D'ailleurs Windows vous en informe … VOUS LAISSERIEZ VOTRE TRAVAIL EN COURS SUR LE SERVEUR

MAIS en fermant la session proprement sur le serveur…

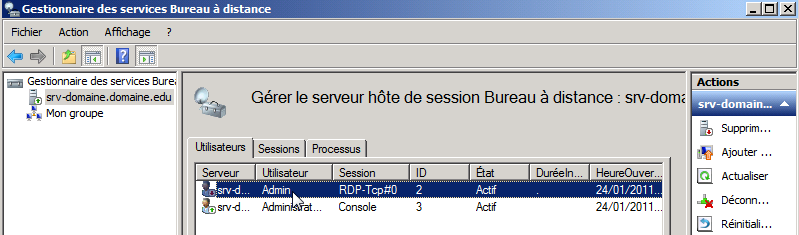


## Services Bureau à Distance 2008

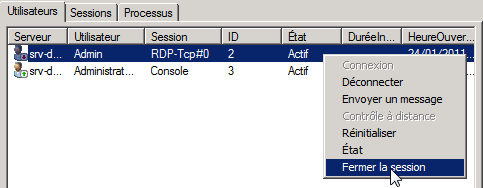


Encore plus si on demande plein écran…

Depuis le poste Serveur 2008R2 dans les **outils d'administration**, dans les S**ervices de Bureaux à distance**, On peut utiliser le **Gestionnaire des services Bureau à distance**



Un clic – droit sur la connexion **rdp** voulue permet de faire l'essentiel…



## Utiliser le Bureau à Distance depuis un client:

Selon l'option, la connexion sera possible depuis



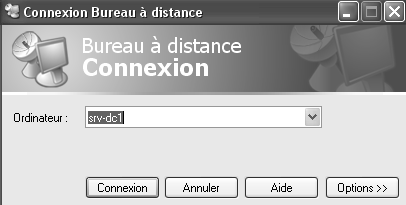
* Tout poste windows avec un client RDP
* Uniquement des postes ayant un client RDP version 7.0 ( Seven mini…)

Depuis un poste XP, on demande

**programmes / accessoires / outils de communication / Connexion Bureau à distance**



Cela amène une fenêtre

 puis **Connexion**

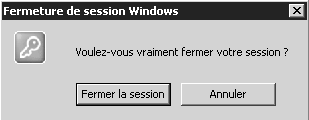
On peut rentrer un nom, ou une adresse ip



Une connexion se crée alors. POUR SORTIR demander **Fermer la session**!

**Soit quelque chose du genre** : Démarrer / Fermer la session

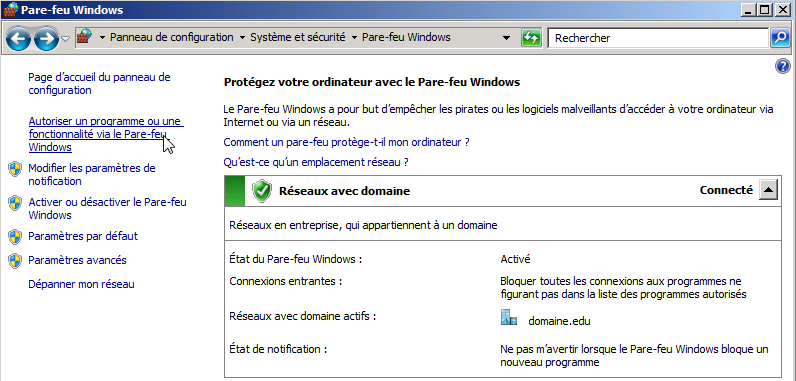
 puis



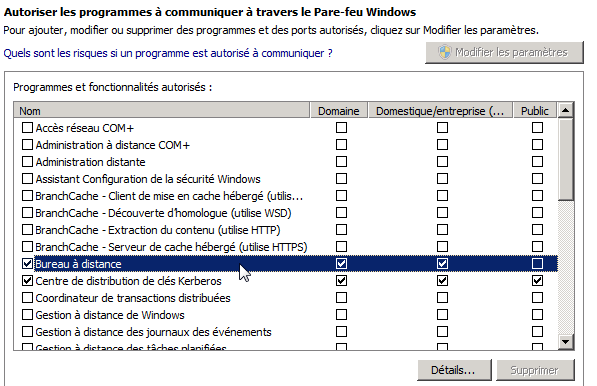
SURTOUT PAS DE DECONNEXION, (en fermant la fenêtre par la croix en haut à droite) VOUS LAISSERIEZ VOTRE TRAVAIL EN COURS SUR LE SERVEUR

## Pare-Feu et N° Port par défaut

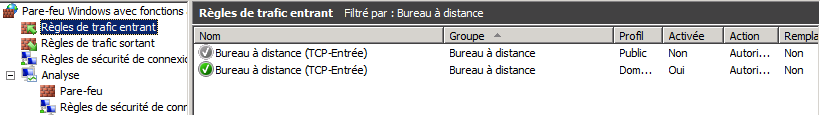
Si on laisse Windows activer les réglages pour passer le pare-feu incorporé de Windows Server (ici 2008R2),

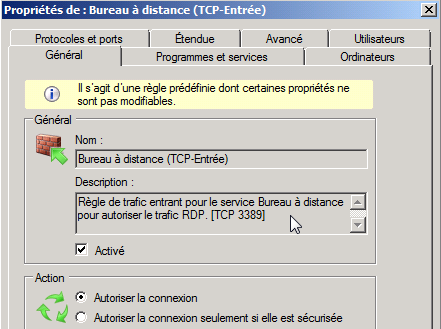


Alors on observe



Dans les **règles de trafic entrant**, filtrées par **bureau à distance**…

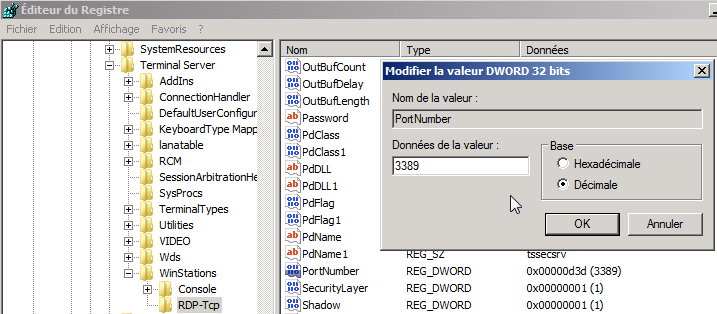


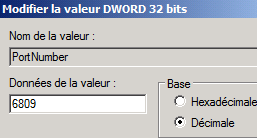


On voit que le port TCP-3389 est concerné

## Port TCP du Bureau à Distance (modification)

Le Bureau à Distance port **TCP** **3389** par défaut est modifiable via la base de registre Clé **HKLMACHINE\System\CurrentControlSet\Control\TerminalServer  
WinStation\RDp-Tcp\PortNumber**

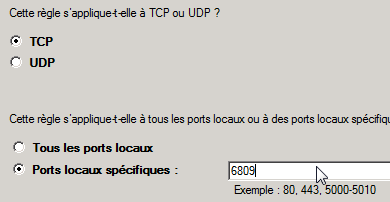


et on peut spécifier un autre N° de port pour accéder au bureau à distance qui écouterais sur un n° de port non configuré par défaut

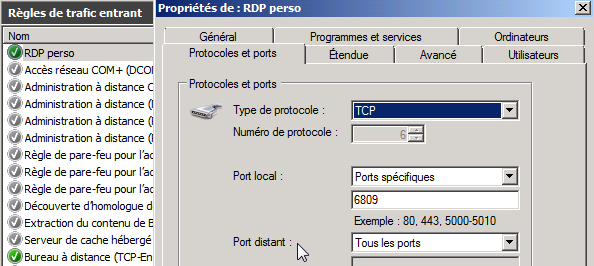
dans l'exemple ici ***6809***

Il faut créer une règle spécifique ***RDP perso*** dans le Pare-feu …

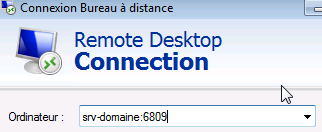
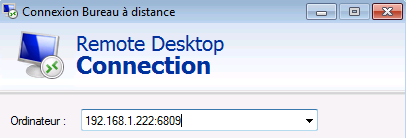
 type Port



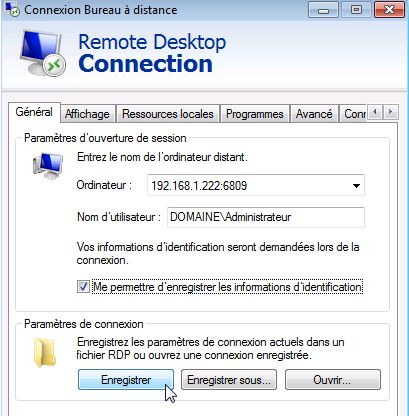
donnant



Pour y accéder depuis un client, en ajoutant : 'deux-points' comme dans



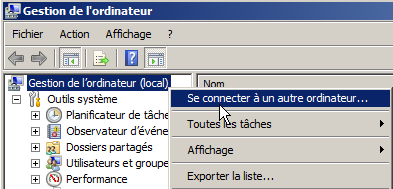
Configuration que l'on peut enregistrer…



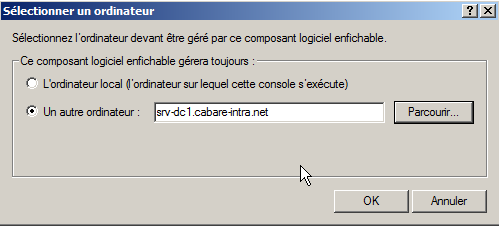
# MMC à Distance

## Gestion de l'ordinateur:

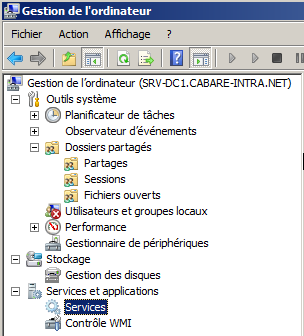
Dans pratiquement toutes les mmc par défaut on travaille sur l'ordinateur local, mais on peut demander de se connecter à un autre ordinateur…



Et choisir une machine sur laquelle on ait des droits…



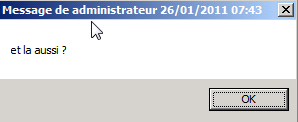
Et voilà…



# MSG – (netsend)

## MSG n'est pas NetSend:

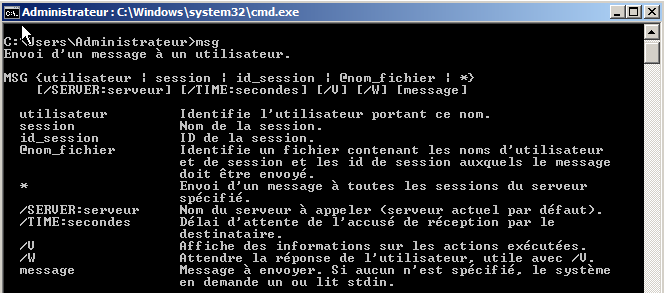
La commande **netsend** n'existe plus depuis SEVEN, et il ne faut pas chercher une commande de remplacement…

MSG peut être utilisé à des fins un peu similaires, MSG est utilisé de base pour envoyer un message à des clients Terminal Server… et pourra être utilisé pour envoyer un message sur une machine distante.

**N.B**: On ne pourra plus envoyer des messages anonymes à tous les utilisateurs de toutes les machines…

## Syntaxe MSG:

La syntaxe est la suivante



Si le poste se nomme "travail" et le login de l'utilisateur connecté est "administrateur"



Si on ne connait pas le login, on peut cibler la sortie console n° ***1*** (écran standard) via la commande



Si on veut envoyer un message à toutes les sessions du poste travail, cad …***\****



**N.B:** Mais si le poste n'est pas le poste local… alors on a une erreur



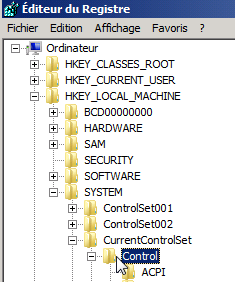
***Erreur 5*** – ou ***1722*** signifie problèmes de droits d'accès…

## MSG hors TSE dans domaine:

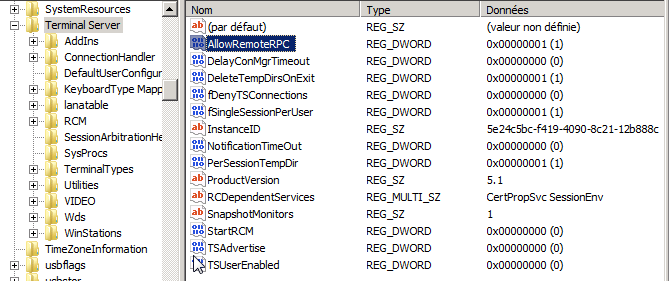
Il faut autoriser le Bureau à distance de la machine visée !

Et effectuer les modifications suivantes pour chaque machine devant recevoir un message.

**Dans la clé HKLM\SYSTEM\CurrentControlSet\Control\...**



Il faut trouver l'entrée **Terminal Server**



Et modifier la clé **AllowRemoteRPC** avec la valeur 1

La commande MSG fonctionnera dans un Domaine (ou éventuellement entre machine ayant même workgroup…)

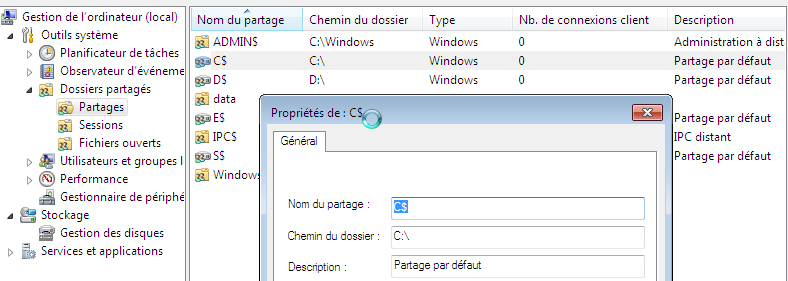
**N.B**: penser à exécuter la commande MSG avec des pouvoirs élevés, en cas de présence d'UAC…

**N.B**: penser à exécuter la commande MSG sous un login de domaine, et pas un login local…

# Partages Administratifs - UAC

## Utiliser les partages Administratifs:

Sur un poste Windows il existe des partages administratifs… chaque lecteur est partagé de manière discrète (avec un $) et réservée au système ET à l'administrateur intégré de l'OS.

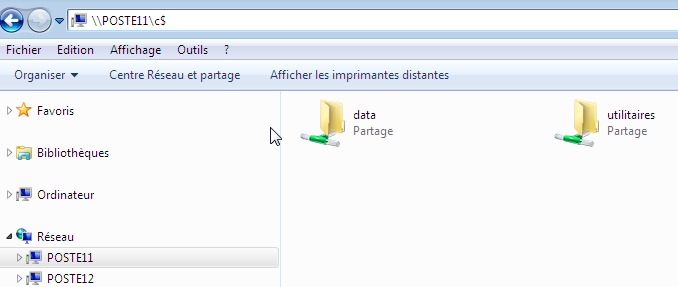


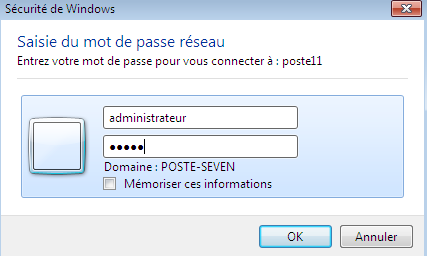
Pour les utiliser depuis un autre poste, il faut connaître

Le nom du poste ***poste11***

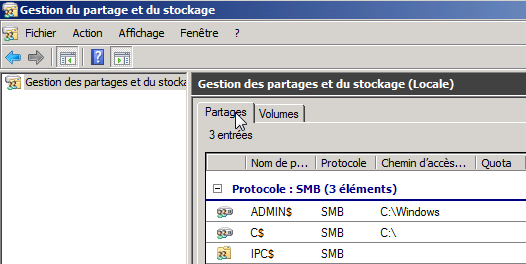
Le nom du partage administratif **c$**

Et le login de l'administrateur intégré du poste visé…





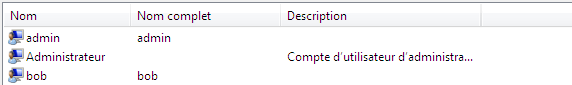
Cela marche très bien sur un Serveur 2008r2 également, on vérifie les partages administratifs dans **Gestion du partage et du stockage**



## Effet de l’UAC:

Tout compte externe qui se connecte à distance à un ordinateur sous Seven, même s'il est administrateur reconnu en LOCAL sur cette machine, ne reçoit qu'un jeton "filtré" , c'est à dire sans les privilèges réservés aux administrateurs !

Et à distance, la procédure d'élévation de privilèges ne se déclenche pas, donc empêchant l'utilisation d'un jeton "complet".



Sur le poste « de départ »

* + le compte ***Administrateur/local*** est l’administrateur intégré
  + le compte ***Admin/localdep*** fait partie du groupe local des administrateurs
  + le compte ***bob/b*** fait partie du groupe local des utilisateurs avec pouvoir.

Sur le poste « cible »

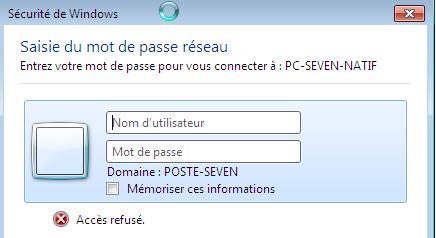
* + le compte ***Administrateur/local*** est l’administrateur intégré
  + les comptes ***Admin/localcib*** et ***bob/b*** font partie du groupe local des administrateurs

**Exemple 1**: **administrateur intégré**

On se logue sur le poste « de départ » en tant qu’administrateur intégré… ***Administrateur/local***

On accède au partage administratif du poste cible "pc-seven-natif" naturellement, car l'UAC ne s'applique pas au compte administrateur intégré et les comptes sont homonymes

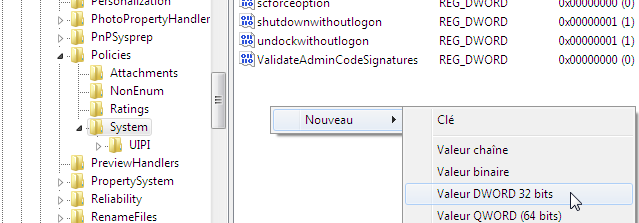
**Exemple 2**: **administrateur local**

On se logue sur le poste « de départ » en tant qu’administrateur local… ***Admin/localdep***

On n'accède pas au partage administratif du poste cible "pc-seven-natif" car l'UAC s'applique

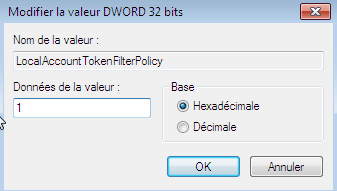
Si on veut un fonctionnement identique à celui de XP (PRO) et précédents, il faut modifier la BDR de la machine "cible" sous Windows en ajoutant l'entrée de type **REG\_DWORD** valant **LocalAccountTokenFilterPolicy** = 1 dans la clef

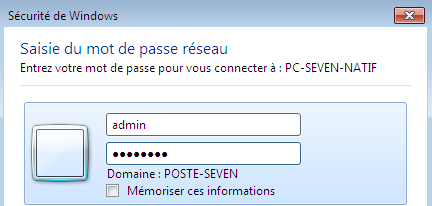
**HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**





Et on lui donne la valeur 1… (et on re-démarre le poste)



Désormais tout utilisateur externe se connectant sous un Username+Password reconnu en local comme appartenant au groupe des administrateurs se verra attribuer un jeton "complet"…

Et **admin/localcib** passe…

**Exemple 3**: **utilisateur avec pouvoir local**

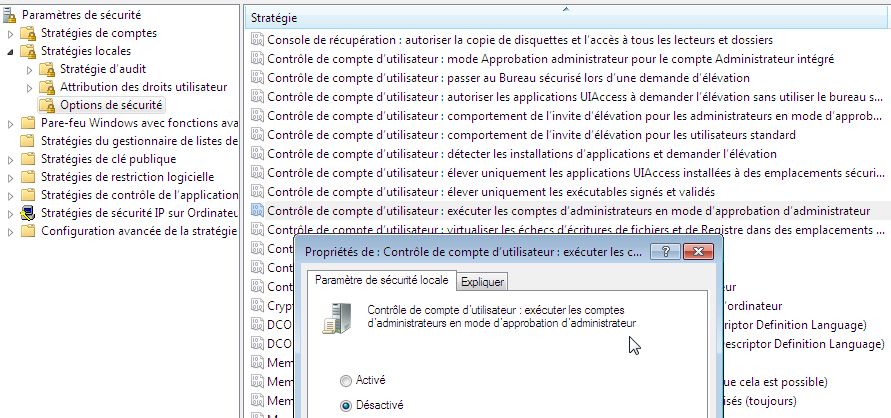
On se logue sur le poste « de départ » en tant qu’utilisateur avec pouvoir … ***bob/b***

On accède au partage administratif du poste cible "pc-seven-natif" naturellement, car l'UAC à été désactivé via la modification de la base de registre, et les comptes sont homonymes…

**Exemple 4**: **utilisateur avec pouvoir local – poste cible sans UAC**

On se logue sur le poste « de départ » en tant qu’utilisateur avec pouvoir … ***bob/b***

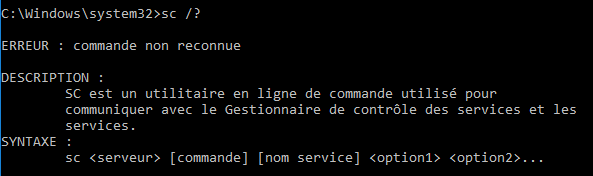
Suir le poste cible on rétabli la clé de la base de registre à 0 (ou on l’efface) et on désactive l’UAC… dans les **outils d’administration**, **stratégies de sécurité locale**

****

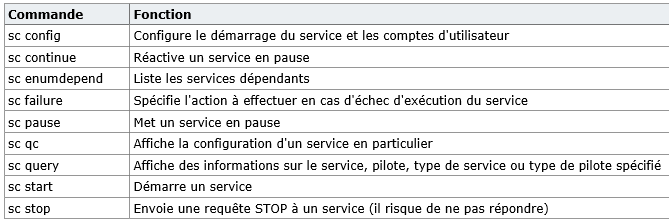
On accède au partage administratif du poste cible "pc-seven-natif" naturellement, car l'UAC a été désactivé totalement, et les comptes sont homonymes…

# SC - Service à distance

## Sc en ligne de commande :



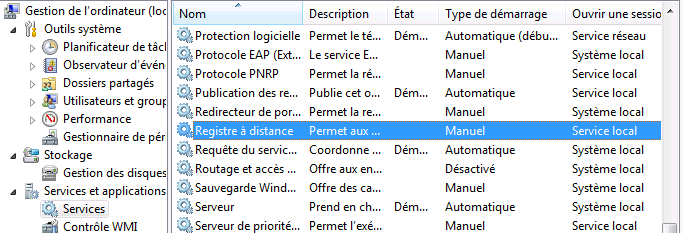
avec



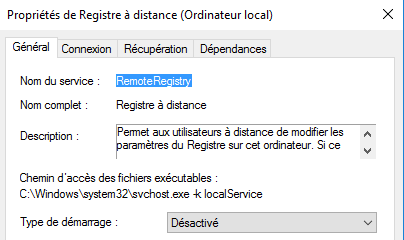
## Nom d'un service

Imaginons devoir localement démarrer le service de registre distant

* **Registre à distance** (manuel par défaut)



Pour démarrer gérer le service il faut connaitre son nom, ici **RemoteRegistry**



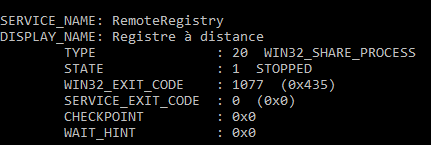
On peut demander si le service en cours de fonctionnement



Ou pour lister tous les services

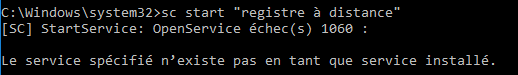


On trouvera

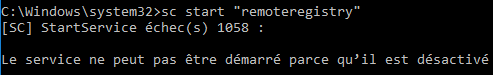


## Etat d' un service sc query

On veut donc gérer notre service **Registre à distance**

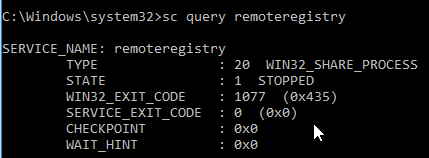


Qui s'appelle en fait **RemoteRegistry.** Si on essaye de le démarré, on peut obtenir un message d'erreur



On voit qu'il est stoppé

**sc query "Name of Service"**



On peut changer son état de démarrage **auto, demand**, ou **disabled**

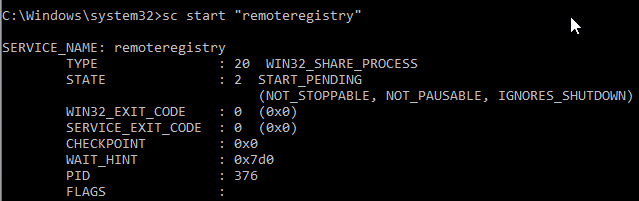
**sc config "Name of Service" start=**



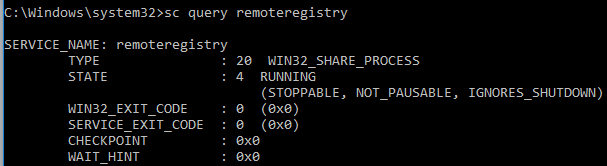
## Démarrer arrêter un service local sc start stop

On va pouvoir le démarrer avec la commande

**sc start "Name of Service"**

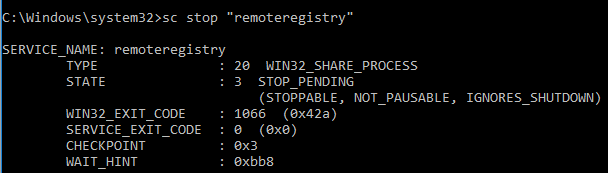


Et si tout va bien on vérifie

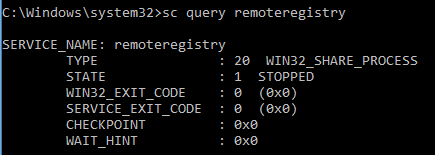


On va pouvoir le stopper avec la commande

**sc stop "Name of Service"**



Et si tout va bien on vérifie



## Démarrer arrêter un service distant

Il faut ajouter un paramètre

**\\Server**

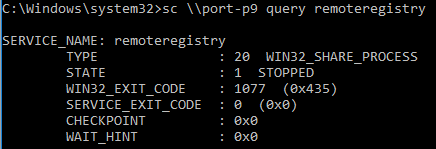
à partir du moment bien sûr ou l'on a les droits sur la machine distante

par exemple

**sc** [**\\nom-unc**](file:///\\nom-unc) **query "Name of Service"**

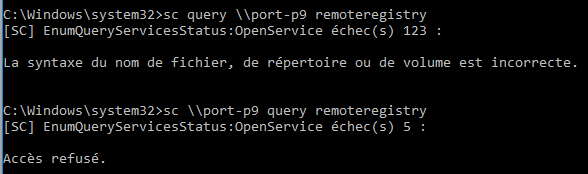
Comme dans

**sc start "Name of Service"**



**N.B**: Attention à l'UAC sur la machine que l'on essaye de gérer !

**sc stop "Name of Service"**

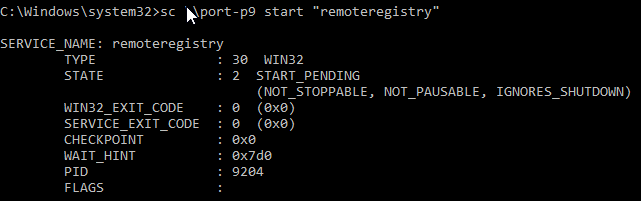


Donc la même séquence va fonctionner à distance en pré-fixant ***\\port-p9***

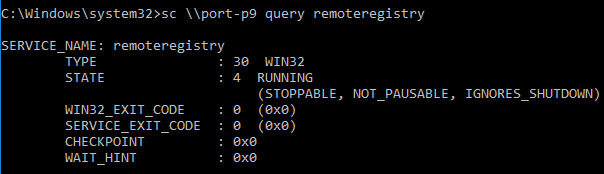
Option de démarrage



démarrage



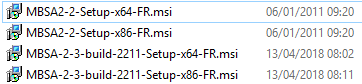
Vérification



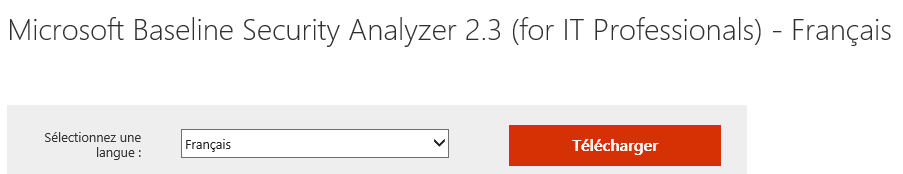
# MBSA poste distant

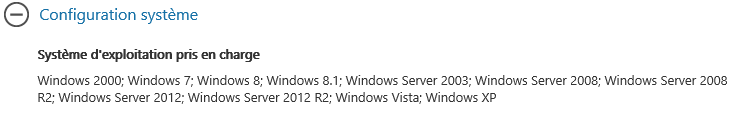
## MBSA 2.3 : pas de successeur à venir :

Une fois MBSA installé sur notre poste Windows 10,

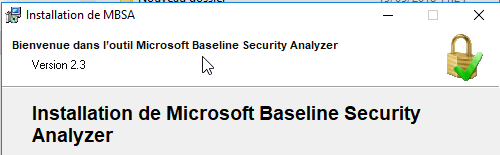


Actuellement aucune version de MBSA (2.3 dernière release) ne supporte officielment Windows 10 ou Windows 2016 Server. Et aucune mise a jours n’est prévue. Il semble cependant que l’utilisation « locale » de MBSA, soit « tolérée »…





On l’installe simplement

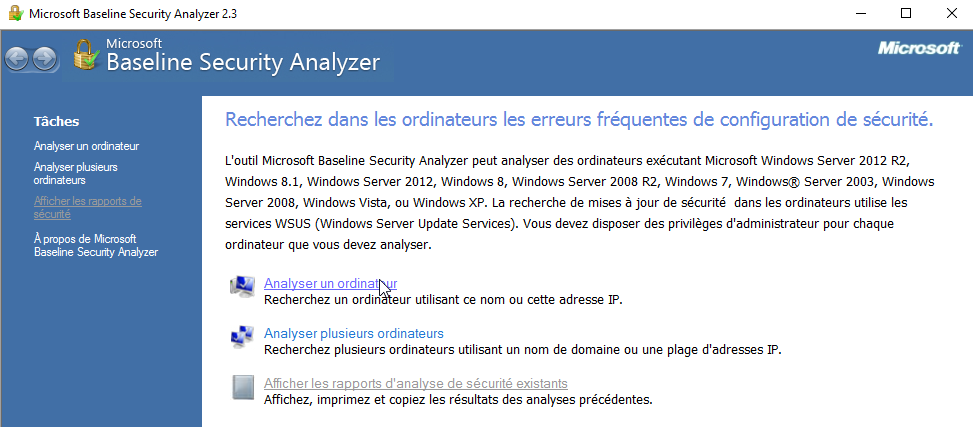


## Lancement MBSA 2.3 en local:

on lance le raccourci

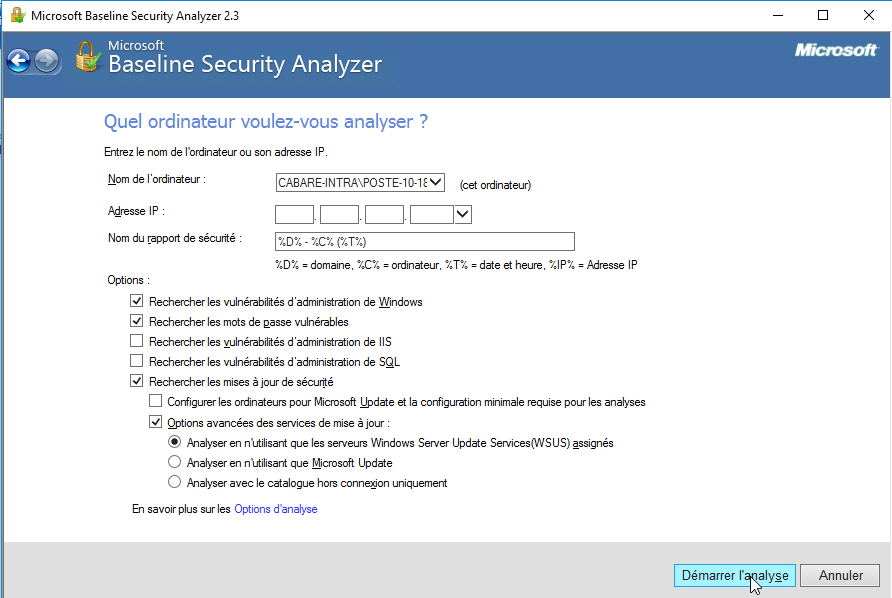


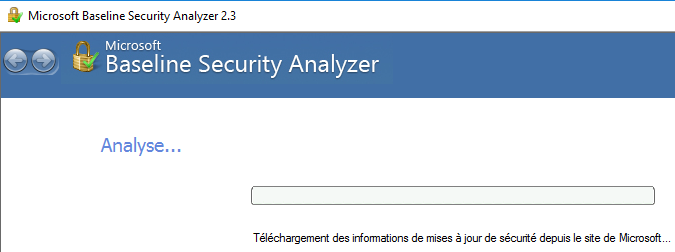
qui peut effectuer l'analyse locale de systèmes **Windows 10 ( ?) -SEVEN**



Peu de réglages sont indispensables à ce niveau,

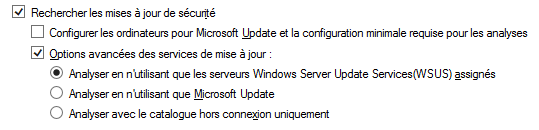
* on décoche **IIS** et **SQL**
* et on demande de **Rechercher les mises à jour de Sécurité**…



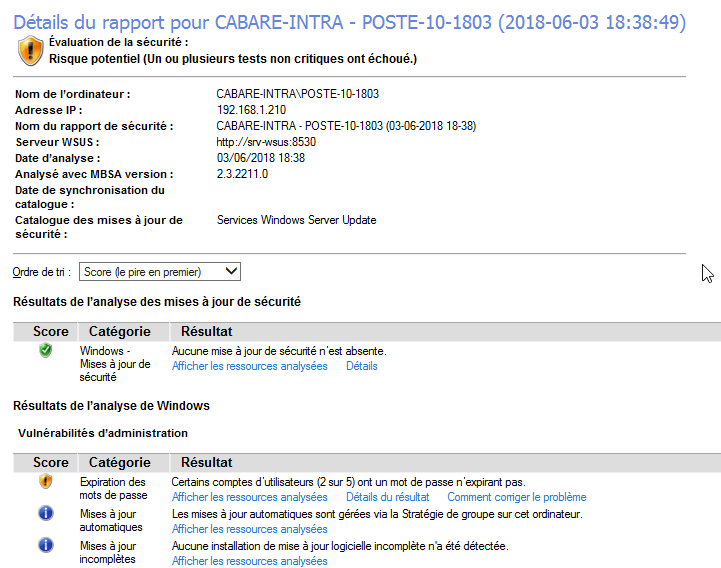
Après téléchargement (cela peut être long) d'une base de signature depuis le site de microsoft, (elle est toujours chargée)

### Analyse depuis WSUS

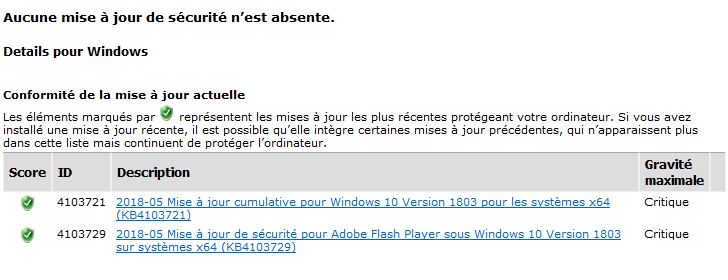
Une analyse est rendue soit en s’interfaçant avec le serveur **WSUS**



Donnant par exemple

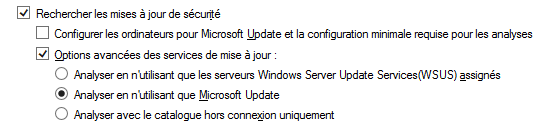


Le résultat est donné avec des indications sur les actions éventuelles

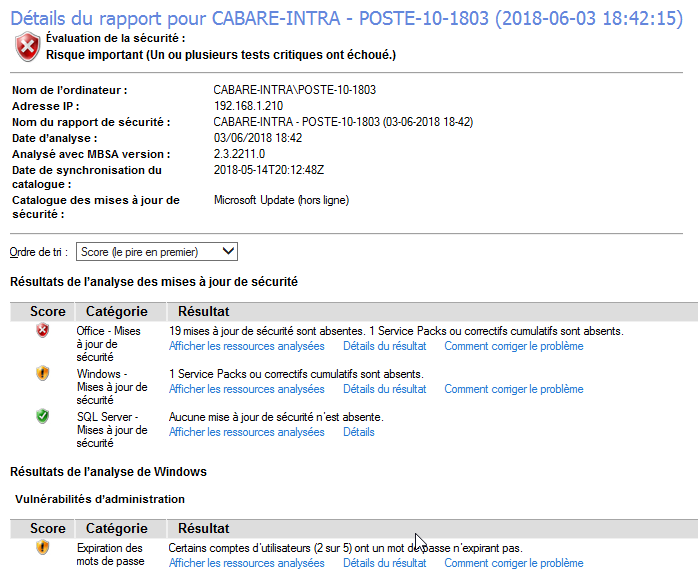


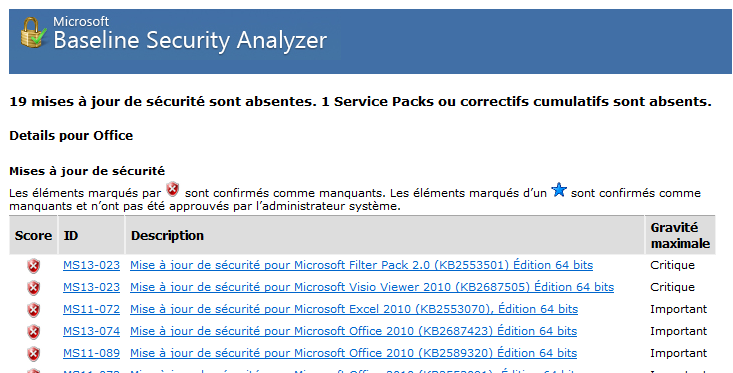
### Analyse depuis site de Microsoft

Une analyse est rendue soit en s’interfaçant avec le site de **MICROSOFT**



Donnant par exemple pour la même machine



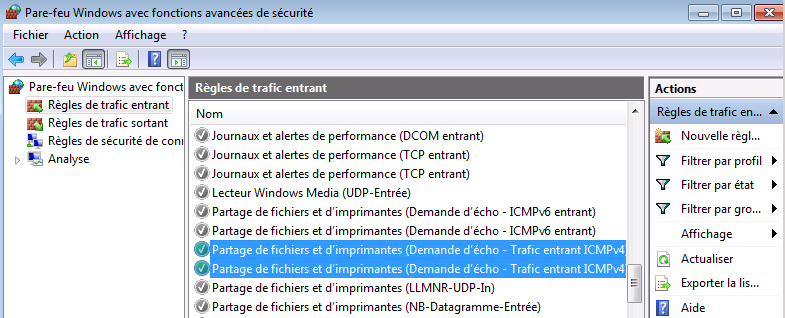


## Adressage IP – Pare-feu:

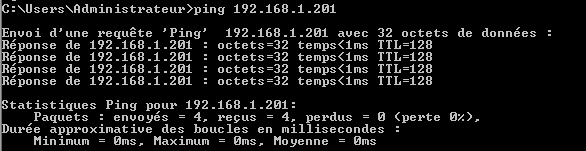
Une fois MBSA installé sur notre poste, on vérifie au niveau IP la bonne communication entre les deux machines.

Bien sur pour pinger une machine Windows, il faut soit désactiver le Pare-Feu, soit activer les règles par défaut

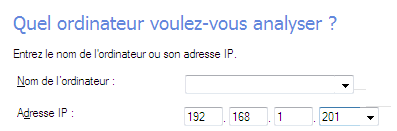
Partage de Fichier et d'imprimantes (Demande d'écho – Traffic entrant ICMPv4)



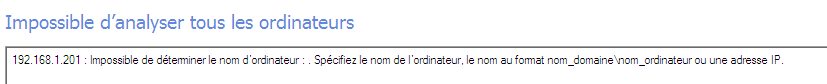
Imaginons que nous souhaitions lancer MBSA sur le poste 192.168.1.201



Si on lance l'analyse telle que



On obtiendra probablement si son pare-feu est actif…



Les ports TCP 139 et 445 ainsi que UDP 137 et 138 doivent être ouverts…

## Comptes Utilisateurs:

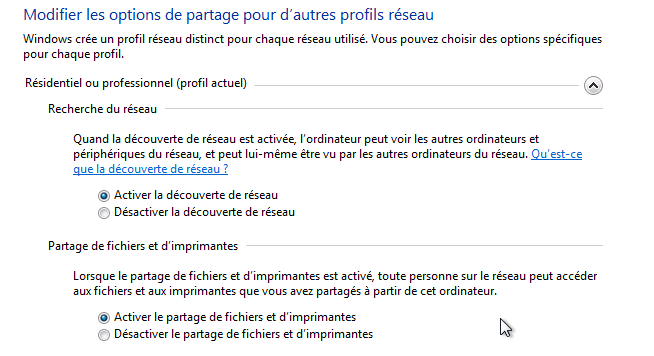
On obtient si le pare-feu est inactif…(ou les ports ouverts correctement)



Le compte utilisateur "lanceur" de MBSA doit être administrateur non seulement sur la machine ou MBSA est installé, mais aussi administrateur sur la poste que l'on essaye d'analyser…

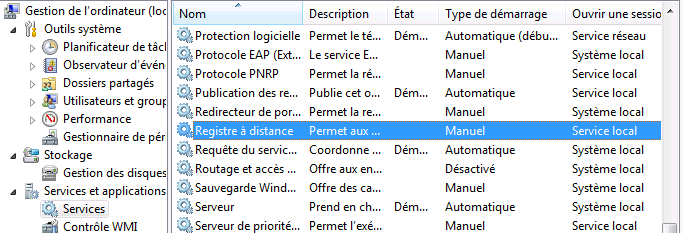
## Services et paramétrages:

Le profil réseau utilisé sur la machine que l'on essaye d'analyser ET le poste sur lequel MBSA est installé, doit autoriser les partages de fichiers et d'imprimantes



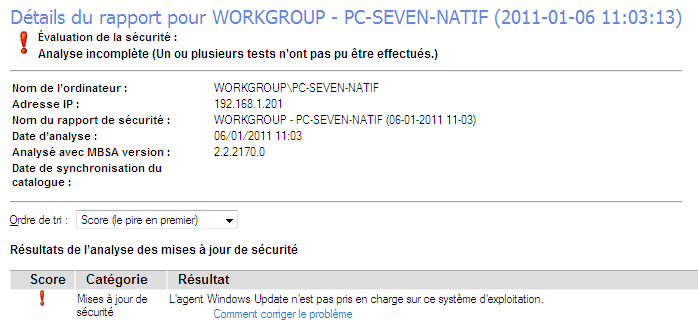
Les services suivants sont nécessaires :

* **Registre à distance** (manuel par défaut)
* **Serveur** (démarré par défaut)
* **Windows update** (démarré par défaut)

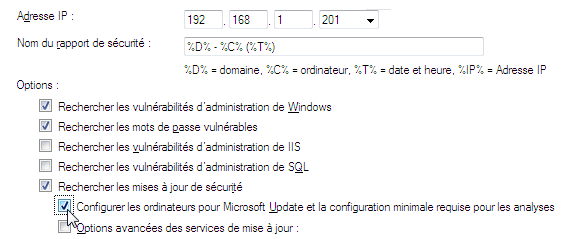


## Agent Windows Update:

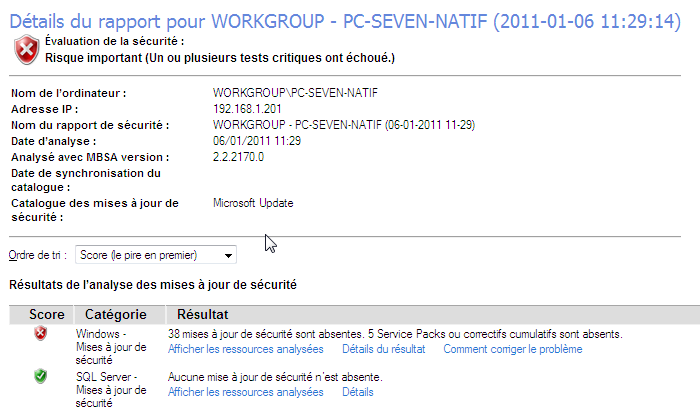
Un agent Windows Update peut être requis…



MBSA peut installer l'agent Windows Update en activant la case à cocher **Configurer les ordinateurs pour Microsoft Update et la configuration minimale requise pour les analyses** avant d'effectuer une analyse des mises à jour de sécurité



Et voilà …



## Récapitulatif procédure MBSA poste Distant:

* Compte Utilisateur : Il doit être Administrateur des 2 coté, c'est à dire

**Administrateur** : sur la machine ou MBSA est installé

**Administrateur** : sur la machine que l'on essaye d'analyser avec MBSA

**N.B**: pour une machine attention à l'UAC

Il ne faut pas que le compte qui essaye d'accéder à distance soit soumis à l'UAC, autrement dit utiliser de préférence le compte administrateur intégré si l'UAC est actif et paramétré par défaut sur le poste

* Autorisations profil Réseau :

Il faut **autoriser les partages de fichiers et d'imprimantes**

* Services Requis :

**Registre à distance** (manuel par défaut)

**Serveur** (démarré par défaut)

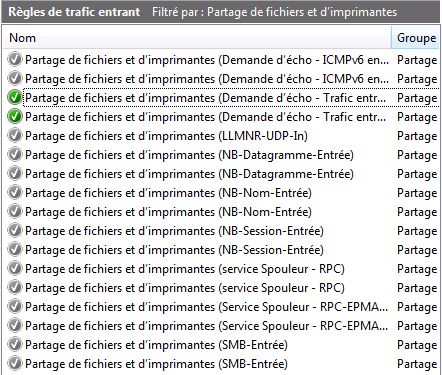
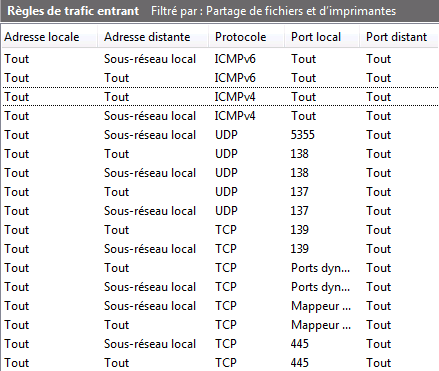
**Windows update** (démarré par défaut)

* Pare-Feu: Soit on le désactive…

Soit on ouvre les Règles **Partage de fichiers et d'imprimantes**

**TCP 139 TCP 445**

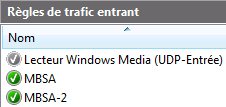
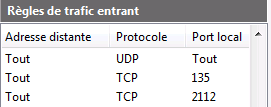
**UDP 137 UDP 138 UDP 139**



Et on Crée les Exceptions suivantes **Nouvelles Règles MBSA-1** et **MBSA-2**

**TCP 135**

**TCP 2112 (par exemple)**

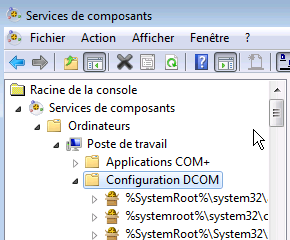
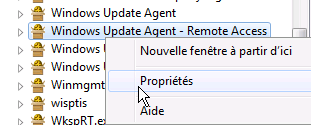
 

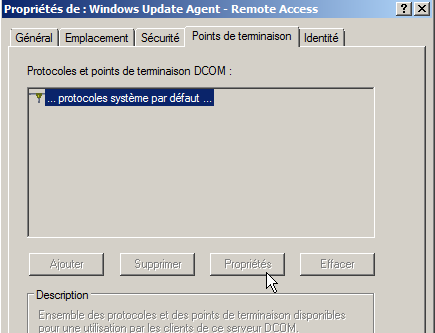
## Procédure MBSA sur Seven:

**N.B**: pour une machine Seven attention à l'UAC

Il ne faut pas que le compte qui essaye d'accéder à distance soit soumis à l'UAC, autrement dit utiliser de préférence le compte administrateur intégré si l'UAC est actif sur le poste

La configuration de N° Port statique pour WUA, Windows Update Agent (ou désactivation du Pare-feu …). Repose exactement sur les mêmes mécanismes





Mais l'accès aux propriétés n'est pas possible par défaut…

Ceci car l'administrateur ne peut pas modifier les fichiers systèmes sous SEVEN, seul le groupe prédéfini **TrustedInstaller** le peut…

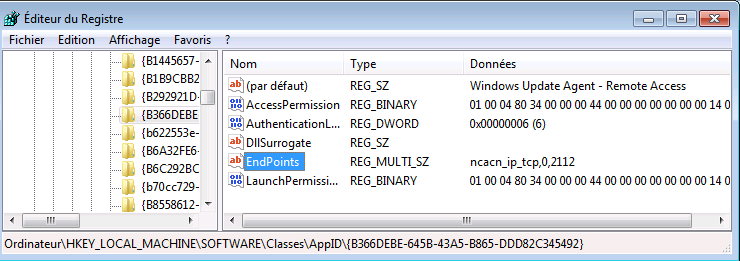


Sachant que les propriétés DCOM pour l'objet **Windows Update Agent** sont en fait stockées dans la base de registre ….

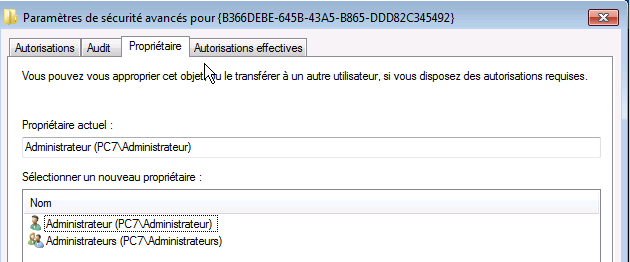
**HKLM\SOFTWARE\CLASSES**

Et plus précisément dans **AppID\{B366DEBE………..DDD82C345492}**

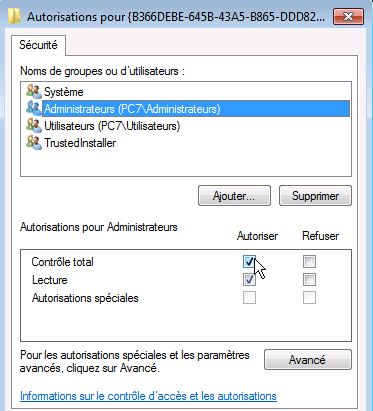




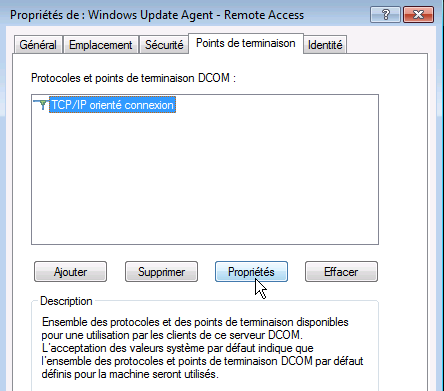
On demander les propriétés de la clé…

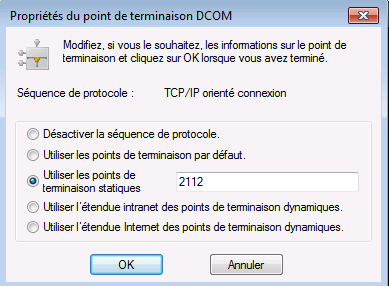


Et on s'approprie en NTFS l'objet, (à la place de **TrustedInstaller**) pour pouvoir ensuite s'y rajouter…

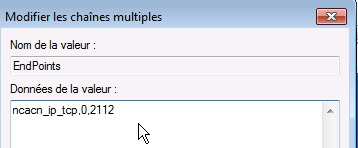


Maintenant les propriétés dcom de l'objet devraient être accessibles…





Ce qui correspond à la clé suivante



**N.B**: si on veut redonner **TrustedInstaller** comme identifiant de sécurité, pour redonner la propriété ou les autorisations de sécurité, il faut spécifier

**NT SERVICE\TrustedInstaller**

# Netstat & Tasklist

## Liste des ports en cours d'utilisation  :

La commande **netstat** permet avec les options **–ano** de connaitre les n° de pid des processus associés aux n° de ports

**netstat –ano**

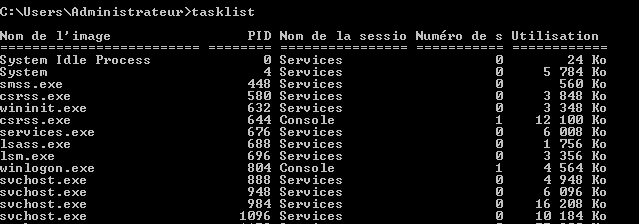


qui utilise le port 668 ?

le PID 1984…

## Liste des processus par PID  :

La commande **tasklist** permet d'avoir les processus associés aux PID,



le PID 1984…

c'est Carbonite !



et les services sont affichables, avec l'options **/SVC** par exemple svchost en PID 984 correspondrait à Windows defender… !



# Netsh - Advfirewall

## Activer – Désactiver le pare-feu

Il est possible globalement de

Activer tous les profils du Pare-feu Windows :

**Netsh advfirewall set allprofiles state on**



Désactiver tous les profils du Pare-feu Windows :

**Netsh advfirewall set allprofiles state off**



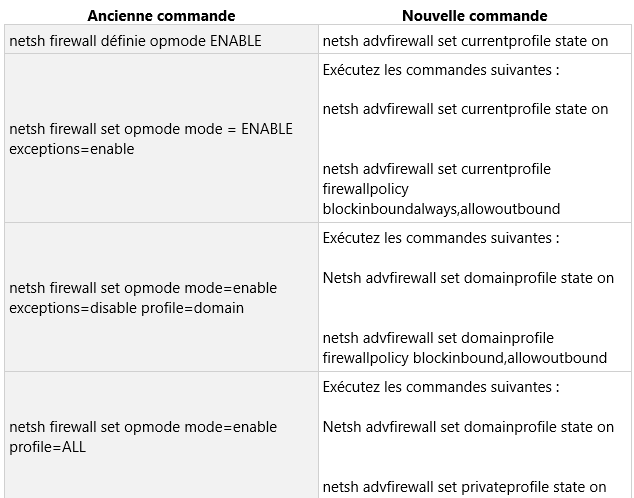
## Netsh Advfirewall – nouvelle commande

### Restaurer les paramètres par défaut du Firewall



### Activer – désactiver le pare feu par profil

En jouant sur la possibilité de travailler sur les profils spécifiques avec les mots clé **Domainprofile / Privateprofile /Publicprofile**



Activer le profil « Public » du Pare-feu Windows :

**Netsh advfirewall set publicprofile state on**

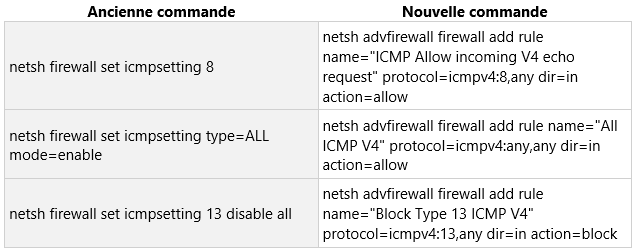
Désactiver le profil « Privé » du Pare-feu Windows :

**Netsh advfirewall set privateprofile state off**

Activer le profil « Domaine » du Pare-feu Windows :

**Netsh advfirewall set domainprofile state on**

### Activer – désactiver ICMP



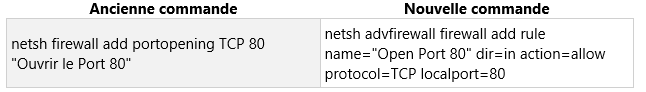
Pour autoriser ICMP en V4 donc

**netsh advfirewall firewall add rule name= "ICMP\_V4" dir=in action=allow protocol=icmpv4**

Pour désactiver ICMP en V4

**netsh advfirewall firewall add rule name= "pas\_ICMP\_V4"dir=in action=block protocol=icmpv4**

### Ouvrir un Port

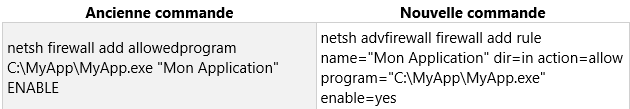


**netsh advfirewall firewall add rule name= "Autoriser\_intranet" dir=in action=allow protocol=TCP localport=8080**

Pour fermer le port il suffit de mettre **delete** à la place de **add**

**netsh advfirewall firewall delete rule name= "Autoriser\_intranet" protocol=tcp localport=8080**

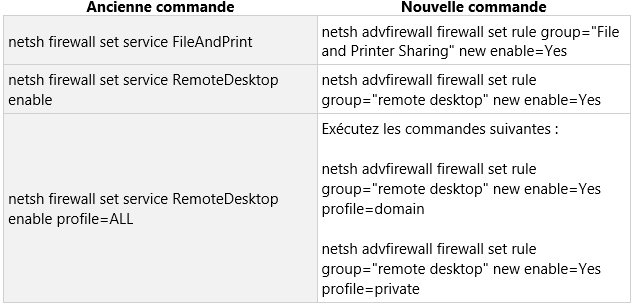
### Autoriser un programme



Par exemple pour autoriser un programme ***xxxx.exe*** installé en C***:\Program Files\editeur\xxxx.exe*** alors

**netsh advfirewall firewall add rule name="Autoriser\_IPScan" dir=in action=allow program= »%ProgramFiles%\editeur\xxxx.exe**

### Activer – désactiver des services



Pour autoriser le **bureau à distance**

**netsh advfirewall firewall set rule group= "Bureau à distance" new enable=Yes**

**N.B**: attention à la régionalisation et au nom des services !

## importer-exporter un profil .wfw :

on peut exporter un profil via

**netsh advfirewall export "c:\backup-firewall.fwf"**

ou si on est dans le contexte **netsh advfirewall** simplement par la commande

**export "c:\backup-firewall.fwf"**

L'importation se faisant via **import**, comme dans

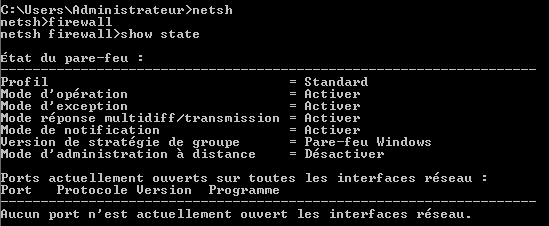
**netsh advfirewall import "c:\backup-firewall.fwf"**

**N.B:** il est conseillé entre les deux de faire un reset, via **netsh advfirewall reset**

## Activer Désactiver le pare-feu  7:

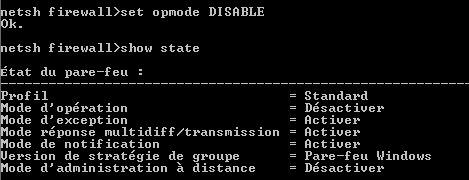
la gestion du pare-feu se fait via: **netsh firewall set /?**

Vérifions :



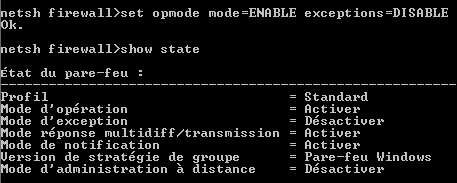
pour désactiver le pare-feu on passe :

**set opmode DISABLE**



Pour Activer le pare-feu, et désactiver les exceptions, on passe :

**set opmode MODE=DISABLE exceptions=DISABLE**



# Netsh

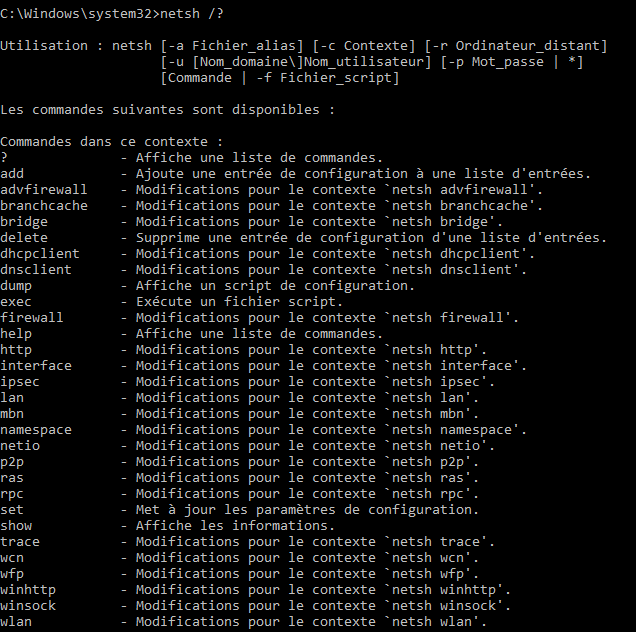
Cet utilitaire est présent sur tous les postes depuis 2000

## Principe de netsh – contexte

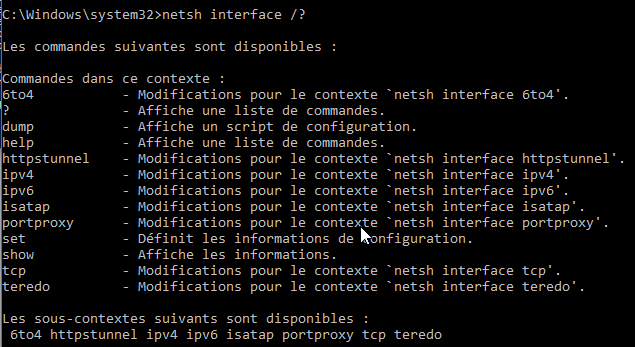
L’utilitaire **netsh** est un utilitaire qui fonctionne en différents niveaux de commande. A chaque **niveau – contexte de commande** est associée toute une liste de sous-commandes. on descend dans un niveau en tapant le **nom du niveau**.

On peut remonter d’un niveau en tapant **..** et sortir de netsh par **exit**

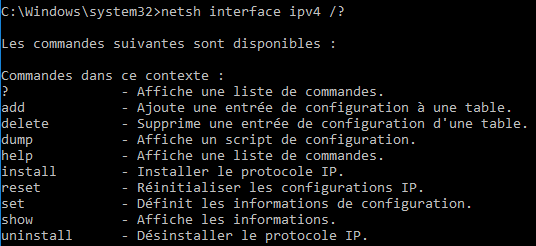
L’aide en ligne est accessible via **netsh / ? .**Le niveau qui nous intéresse c'est **interface.**



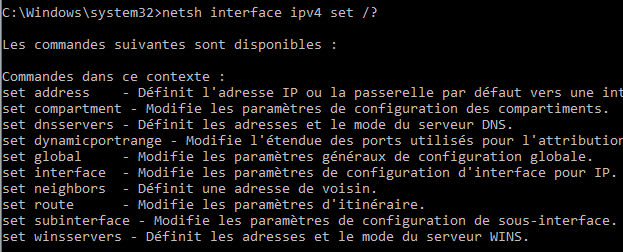
dans le niveau **netsh interface**, L’aide en ligne est accessible classiquement via **netsh interface / ?** C'est sous niveau **ipv4** nous intéresse



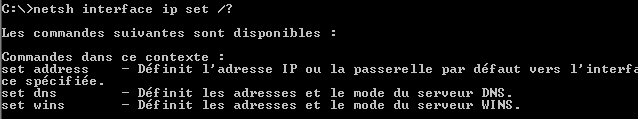
dans le niveau **netsh interface ipv4**, L’aide en ligne est accessible classiquement via **netsh interface ipv4 / ?**C'est le sous niveau **set** nous intéresse :



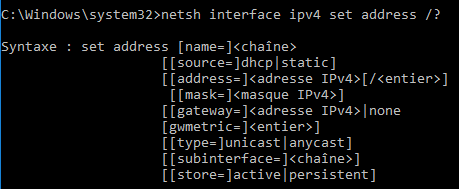
Les commandes qui nous intéresse dans le niveau **netsh interface ipv4 set** vont être essentiellement **address** et éventuellement **dns**



dans le niveau **netsh interface ip set** L’aide en ligne est accessible classiquement **netsh interface ip set / ?**



dans le niveau **netsh interface ip set address** L’aide en ligne est accessible classiquement **netsh interface ip set address / ?**



On trouve finalement notre bonheur !

## Netsh dump Mémorisation – Récupération d’une configuration :

Son utilisation est un peu délicate, mais on peut déjà s’en servir de manière un peu « bestiale » à l’aide des 2 paramètres **–f** et **–c**

Pour mémoriser une configuration complète IP sur une machine, il suffit de créer un fichier texte via la commande suivante :

**Netsh –c interface dump>config-ip-locale.txt**

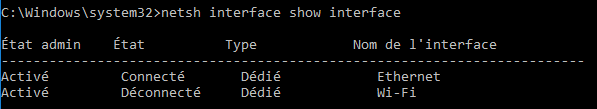
Ce fichier est capable de modifier la configuration de l’adressage IP lorsqu'on le rappellera par la commande

**Netsh –f maconfig.txt**

## Nom des interfaces réseau  :

Pour connaitre les interfaces en cours

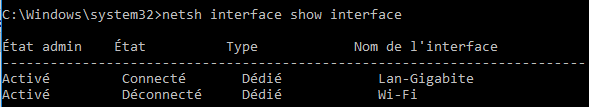
**Netsh interface show interface**



Pour renommer une interface



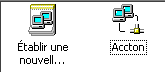
Et on vérifie par



## Modification d’une adresse IP et de son masque :

Pour modifier donc une adresse IP et le masque, il est nécessaire de passer une commande du type :

**Netsh interface ip set address name=”LAN” addr=192.168.3.1 mask=255.255.255.0 gateway=192.168.3.99 gwmetric=x**

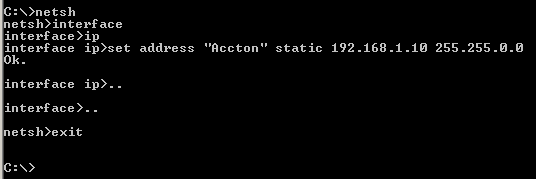
* 1° exemple : sur une machine dont l’interface réseau est nommée **Accton** et pour laquelle on veut donner l’adresse IP 192.168.1.10 masque 255.255.0.0

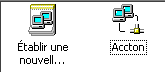
### En une seule commande :

****

### En descendant les niveaux :

Si on veut être plus progressif dans la commande et “descendre” niveau par niveau, on peut aussi alors taper

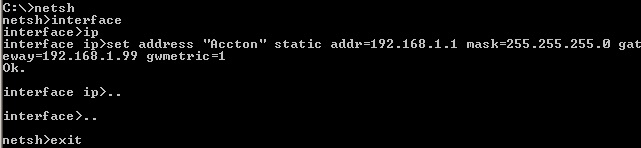


* 2° exemple : toujours sur une machine dont l’interface réseau est nommée **Accton** et pour laquelle on veut donner l’adresse IP 192.168.1.2 masque 255.255.255.0 passerelle 192.168.1.99

### En une seule commande :



### En descendant les niveaux :



## insertion dans un batch :

ce qui serait le mieux, c’est de faire un fichier batch qui pourrait effectuer instantanément la modification…

la commande à passer étant donc la suivante :



on structure le fichier batch de la manière suivante :

batch le plus simple :

**netsh interface ip set address name=Accton static addr=192.168.1.1 mask=255.255.255.0 gateway=129.168.1.99 gwmetric=1**

batch plus "structuré":

**@echo off**

**set name= "Accton"**

**set addr=192.168.1.1**

**set mask=255.255.255.0**

**set gateway=192.168.1.99**

**netsh interface ip set address name=%name% static addr=%addr% mask=%mask% gateway=%gateway% gwmetric=1**

batch "paramétrable" sur l'adresse IP donnée en 1° paramètre :

**@echo off**

**set name= "Accton"**

**set addr=%1**

**set mask=255.255.255.0**

**set gateway=192.168.1.99**

**rem definition adresse ip**

**netsh interface ip set address name=%name% static addr=%addr% mask=%mask% gateway=%gateway% gwmetric=1**

idem mais avec une valeur 192.168.1.10 par défaut si on oubli le paramètre :

**@echo off**

**set name= "Accton"**

**set addr=%1**

**if %1.==. set addr=192.168.1.10**

**set mask=255.255.255.0**

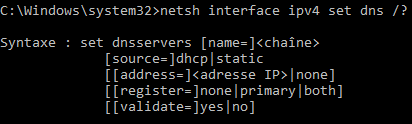
**set gateway=192.168.1.99**

**rem definition adresse ip**

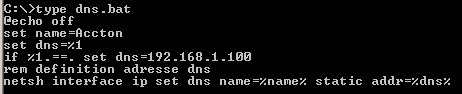
**netsh interface ip set address name=%name% static addr=%addr% mask=%mask% gateway=%gateway% gwmetric=1**

## Modification d’une adresse DNS :

Son utilisation se trouve dans le niveau **netsh interface ipv4 set dns**



ce qui pourrait donner dans un script



**Mémorisation – Récupération d’une configuration :**

son utilisation est un peut délicate, mais on peut déjà s’en servir de manière un peu « bestiale » à l’aide des 2 paramètres **–f** et **–c**

Pour mémoriser une configuration complète IP sur une machine, il suffit de créer un fichier texte via la commande suivante :

**Netsh –c interface dump>config-ip-locale.txt**

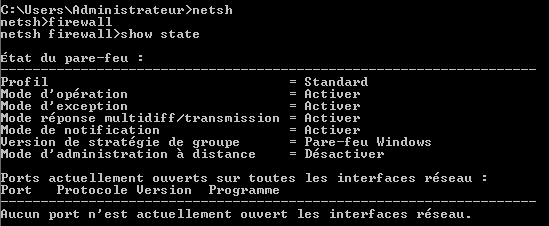
Ce fichier est capable de modifier la configuration de l’adressage IP lorsque on le rappellera par la commande

**Netsh –f maconfig.txt**

**Activer Désactiver le pare-feu :**

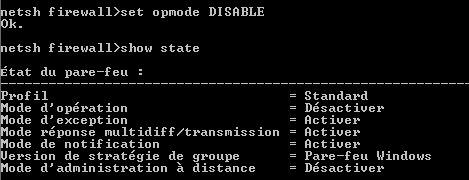
la gestion du pare-feu se fait via: **netsh firewall set /?**

Vérifions :



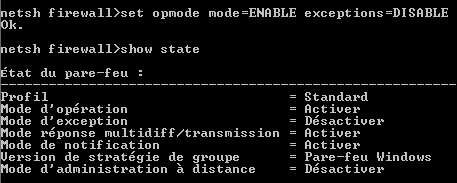
pour désactiver le pare-feu on passe :

**set opmode DISABLE**



Pour Activer le pare-feu, et désactiver les exceptions, on passe :

**set opmode MODE=DISABLE exceptions=DISABLE**



**importer-exporter un profil .wfw :**

on peut exporter un profil via

**netsh advfirewall export "c:\backup-firewall.fwf"**

ou si on est dans le contexte **netsh advfirewall** simplement par la commande

**export "c:\backup-firewall.fwf"**

L'importation se faisant via **import**, comme dans

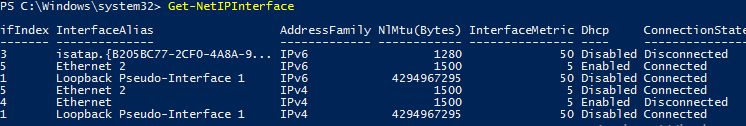
**netsh advfirewall import "c:\backup-firewall.fwf"**

**N.B:** il est conseillé entre les deux de faire un reset du pare-feu, via **reset**

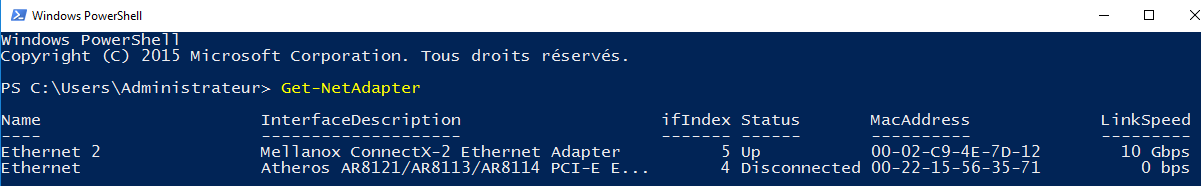
# Changer une Adresse IP en Powershell

## Lister les cartes réseau - Get-NetAdapter

En **powershell** on peut simplement lister les cartes réseaux présentes par la commande **Get-NetIpInterface**

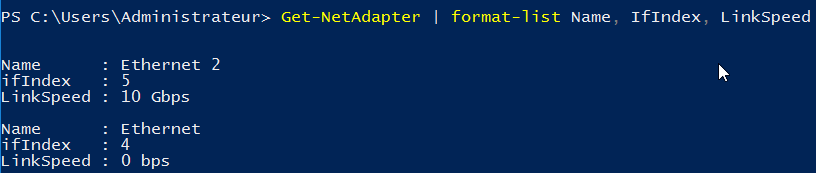


Mais on peut a aussi lister les propriétés des cartes réseaux présentes par la commande **Get-NetAdapter**



Si on trouve le résultat trop verbeux, on peut réduite la réponse aux seules informations qui nous intéressent, par exemple

**Get-NetAdapter | format-list Name, IfIndex, LinkSpeed**



Dans les 2 cas la propriété à noter pour la suite c'est **Ifindex**

**N.b**: il faut qu'il y ait une connexion active, câble branché (ce qui n'est pas nécessaire avec la commande **netsh**)

## Créer une Adresse Ip – New-NetIpAddress

On peut donner une Adresse sur une carte réseau par la commande

**New-NetIPAddress -InterfaceIndex** 4 **-IPAddress** 192.168.1.254 **-PrefixLength** 24 **-DefaultGateway** 192.168.1.1

avec

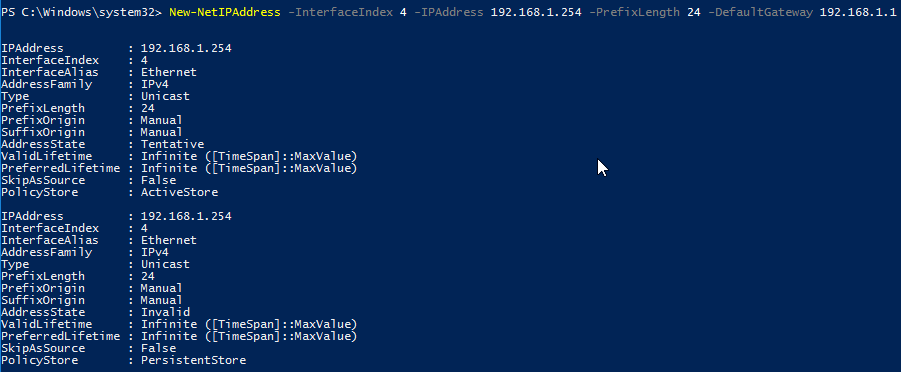
**-InterfaceIndex** : Numéro d’index de la carte à modifier (on peut utiliser à la place **–InterfaceAlias** suivit du nom de l’interface)

**- IPAddress** : Adresse IP à attribuer à la carte

**- PrefixLength** : Longueur du masque de sous réseau

**- DefaultGateway** : Passerelle par défaut

On obtient alors



## Changer le DNS – Set-DnsClientServerAddress

On continue en indiquant un serveur DNS « 8.8.8.8 » sur notre carte, puis, on vérifie que le changement est bien pris en compte :

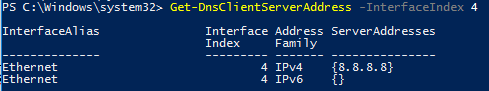
**Set-DnsClientServerAddress -InterfaceIndex** 4 **-ServerAddresses** 8.8.8.8

Ou avec une virgule si 2 adresses DNS,  **Set-DnsClientServerAddress -InterfaceIndex** 4 **-ServerAddresses** 8.8.8.8,4.4.4.4



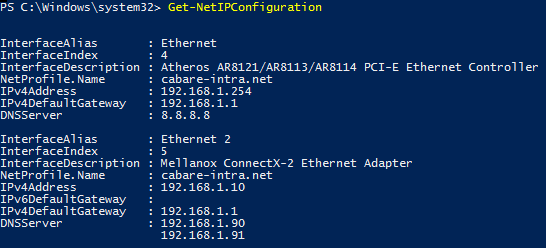
Pour la vérification :

**Get-DnsClientServerAddress -InterfaceIndex** 4



## Vérif configuration - Get-NetIPConfiguration

donne



## Changer une Adresse Ip – New-NetIpAddress

On peut changer une Adresse exista,te sur une carte réseau par la commande

Set-NetIPAddress -InterfaceIndex 14 -IPAddress 172.31.25.4 -PrefixLength 16 -DefaultGateway 172.31.140.1 -AddressFamily IPv4

## Valider Dévalider DCHP – Set-NetIpAddress

Comme dans

**Set-NetIPInterface -InterfaceIndex 14 -Dhcp {Enabled/Disabled}**



## Reset carte réseau – Restart-Netadapter

Comme dans

**Restart-NetAdapter -Name** LAN

L’exemple ci-dessus permet de redémarrer la carte nommée « LAN »

## Supprimer une Adresse IP – Restart-Netadapter

Comme dans

Imaginons que sur ma carte d’index 4, j’ai une ancienne adresse IP qui est « 10.10.10.10 » et que l'on souahite supprimer

Remove-NetIPAddress –InterfaceIndex 4 –IPAddress 10.10.10.10 –PrefixLength 16 –DefaultGateway 10.10.10.254

Confirmez la demande de suppression avec « T » ou deux fois avec « O ».