http://WWW.CABARE.NET ©

Firewall - Gestion Distante - Lan Windows 10 - 7 – sys 40 – Cours & TP-

Gestion Distante de Windows 10 et Seven

Michel Cabaré – Ver 2.3 – Mai 2018-

Fire-Wall Gestion Distante Lan Windows 10-7

Cours - TP

Michel Cabaré – Ver 2.3 – Mai 2018

www.cabare.net ©

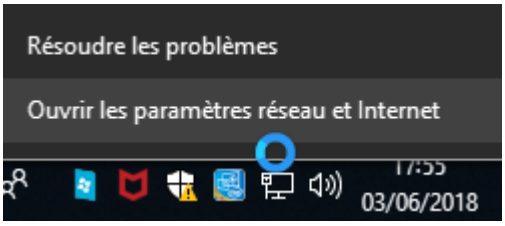
TABLE DES MATIÈRES

Centre réseau Windows 10

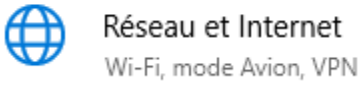
Evolution selon les version - v1803:

Concernant Windows 10, une myriade d'assistant se déclenchent à tous moments, les interfaces sont très "fluctuantes" et "fournies"…

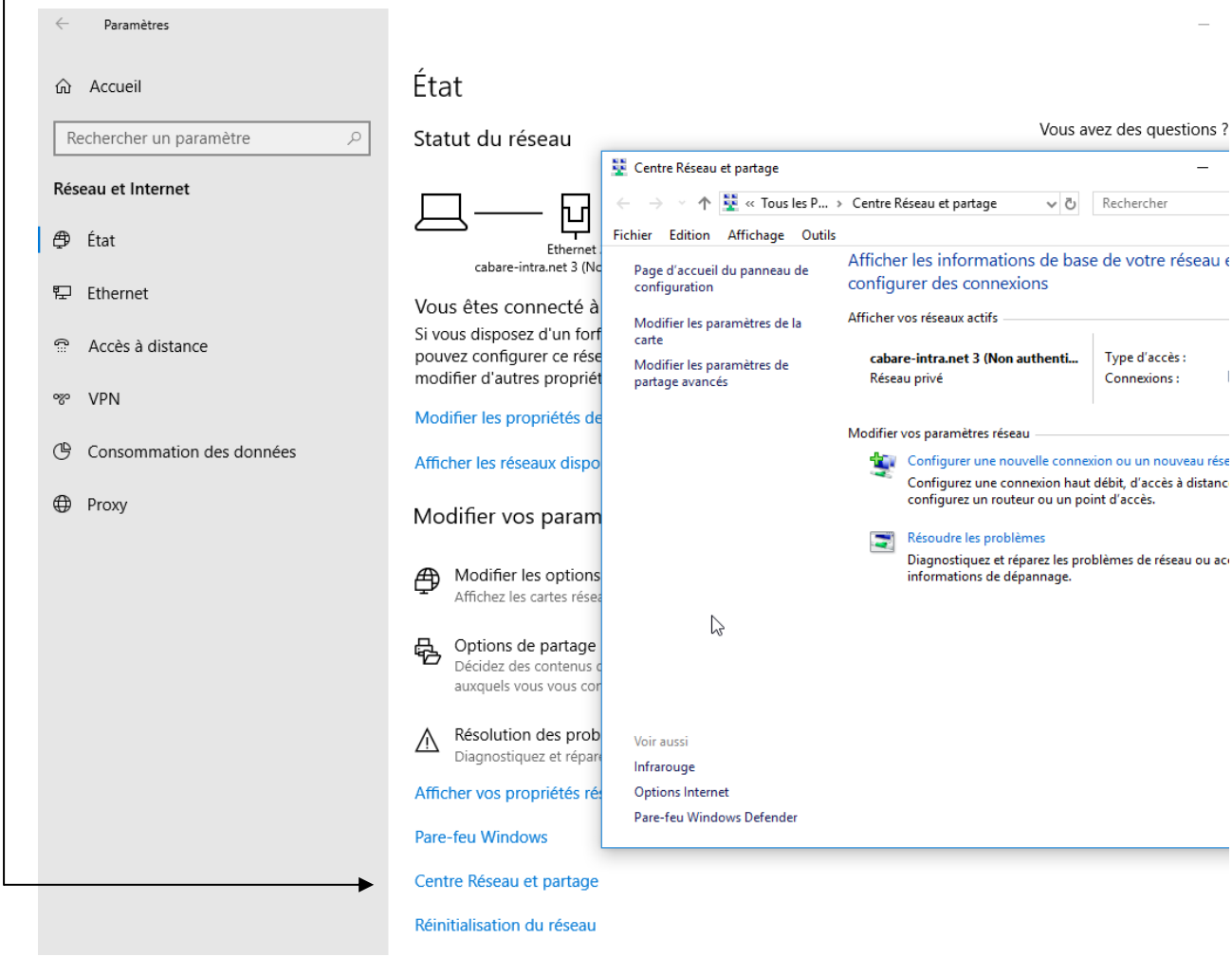
Lorsque l'on clique sur l'icône **réseau** de la barre des tâches, on a désormais **Ouvrir les paramètres réseau et Internet**, ce qui correspond en fait à



L'entrée **Paramètre** de Windows 10 dasn laquelle on demanderais **Réseau et internet**



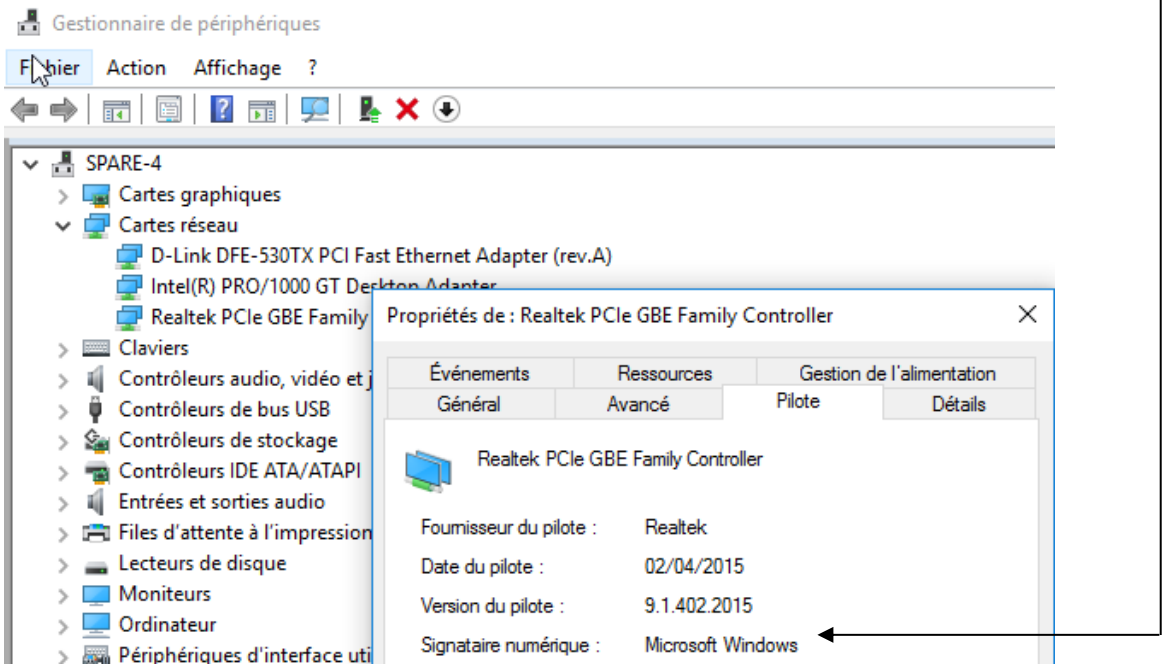
Dans laquelle on pourrait retrouver le **Centre réseau et partage**



Gestion Carte Réseau:

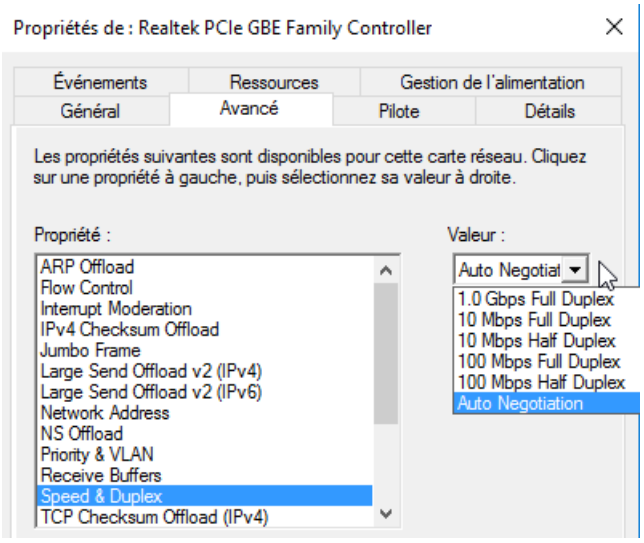
Depuis Windows 10, une myriade d'assistant se déclenchent à tous moments, les interfaces sont assez "fluctuantes" (selon les versions 1511, 1607, 1703, 1709) et "fournies"…

Si aucune carte réseau n'est détectée, il faut installer un driver certifié …

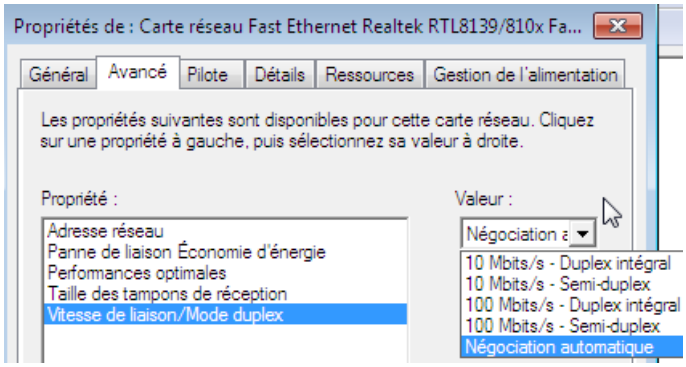


En cas de problème "physiques", on peut vérifier que le driver gère correctement nos flux Ethernet selon notre connectique (et passer en vitesse de remplis si besoin)

Carte **Gb/s**

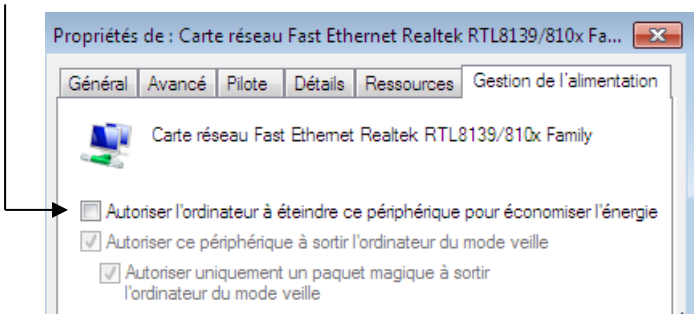


Carte **100Mb/s**



N.B : ces réglages sont parfois difficiles à trouver, ils dépendent des drivers …

On peut aussi éviter pour des raisons **ACPI** d'éteindre la carte réseau…



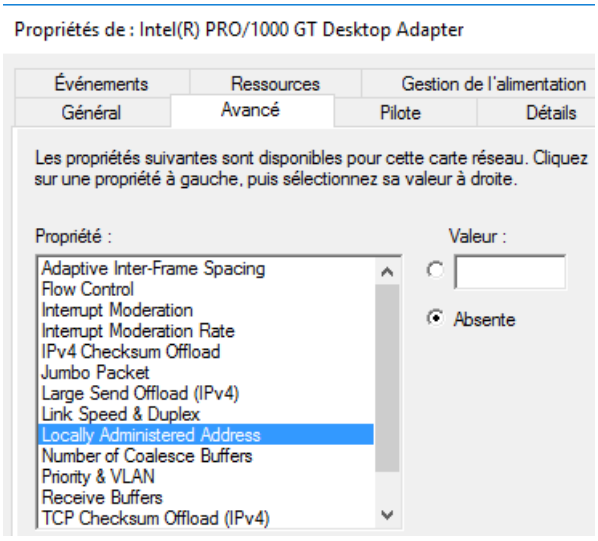
Toutes les cartes n'offrent pas tous les réglages, ni sous les mêmes libellés :

Ainsi pour **Adresse Mac**, **Vitesse + Mode**, **MTU**, on peut trouver par exemple

Locally Administered Address

Link Speed & Duplex

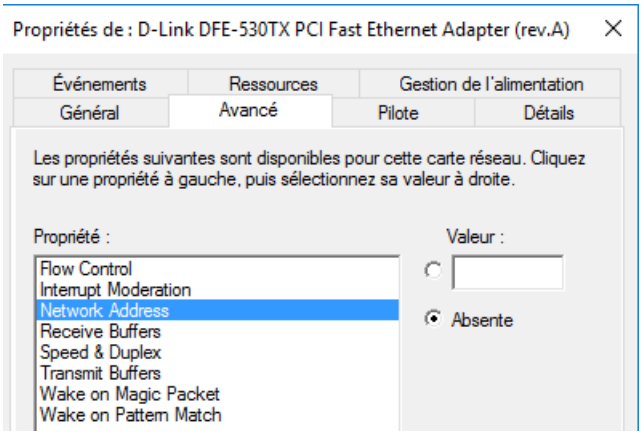
Jumbo packet



Network Address

Speed & Duplex

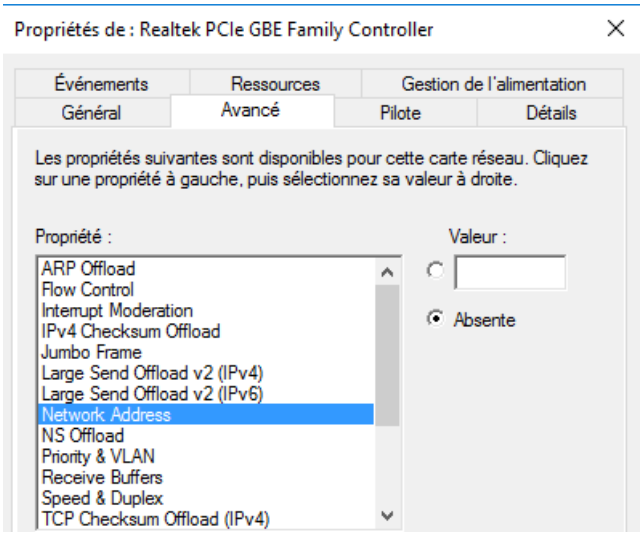
- non disponible



Network Address

Speed & Duplex

Jumbo Frame



Désactivation Media Sense:

Windows dispose de la fonction de « Détection de support ». **Media Sense**

Un « état de la liaison » est défini comme étant le support physique connecté ou inséré sur le réseau. Chaque fois que Windows détecte un état « inactif »  sur le support, il supprime les protocoles liés de cette carte jusqu'à ce que l'état détecté soit de nouveau « actif ». Une telle carte, génère en réponse à un ping local (par exemple une application locale qui détecterait la présence d'un réseau) une défaillance générale

```
C:\Windows\system32>ping 192.168.1.170

Envoi d'une requête 'Ping'  192.168.1.170 avec 32 octets de données :
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.
PING : échec de la transmission. Défaillance générale.
```

Pour que votre carte réseau ne désactive plus IP lors de cette situation, et **réponde sur un ping de l'adressse IP en local**

```
C:\Windows\system32>ping 192.168.1.170

Envoi d'une requête 'Ping'  192.168.1.170 avec 32 octets de données :
Réponse de 192.168.1.170 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.170 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.170 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.170 : octets=32 temps<1ms TTL=128
```

il faut utiliser en invite de commande la commande **netsh** . On peut voir l'état de la situation **Détection de médias DHCP**, dans la commande

Netsh interface ipv4 show global

```
C:\Windows\system32>netsh interface ipv4 show global
Recherche du statut actif...

Paramètres généraux globaux
----------------------------------------
Limite de sauts par défaut          : 128 sauts
Limite de cache du voisin           : 256 entrées par interface
Limite de cache d'itinéraire        : 128 entrées par compartiment
Limite de réassemblage              : 125348608 octets
Redirections ICMP                   : enabled
Comportement du routage source      : dontforward
Déchargement de tâches              : enabled
Détection de médias DHCP           : enabled
Enregistrement de détection de supports : disabled
Niveau MLD                          : all
Version MLD                         : version3
Transmission en multidiffusion      : disabled
Fragments transmis en groupe        : disabled
Identificateurs aléatoires          : enabled
Réponse au masque d'adresses        : disabled
MTU minimum                         : 576
```

On désactive la fonctionnalité en IPV4 et IPV6 avec la commande

Netsh interface ipv4 set global dhcpmediasense = disabled

```
C:\Windows\system32>netsh interface ipv4 set global dhcpmediasense = disabled
Ok.
```

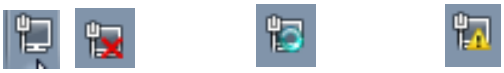
```
C:\Windows\system32>netsh interface ipv6 set global dhcpmediasense=disabled
Ok.
```

Puis reboot du poste !

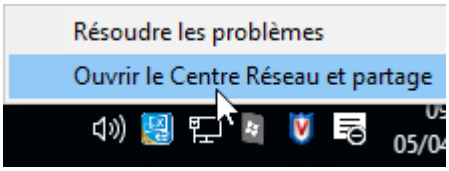
Accès au Centre Réseau et partage :

Si une carte réseau (minimum) est installée correctement, une icône "réseau" devrait apparaître en bas à droite…

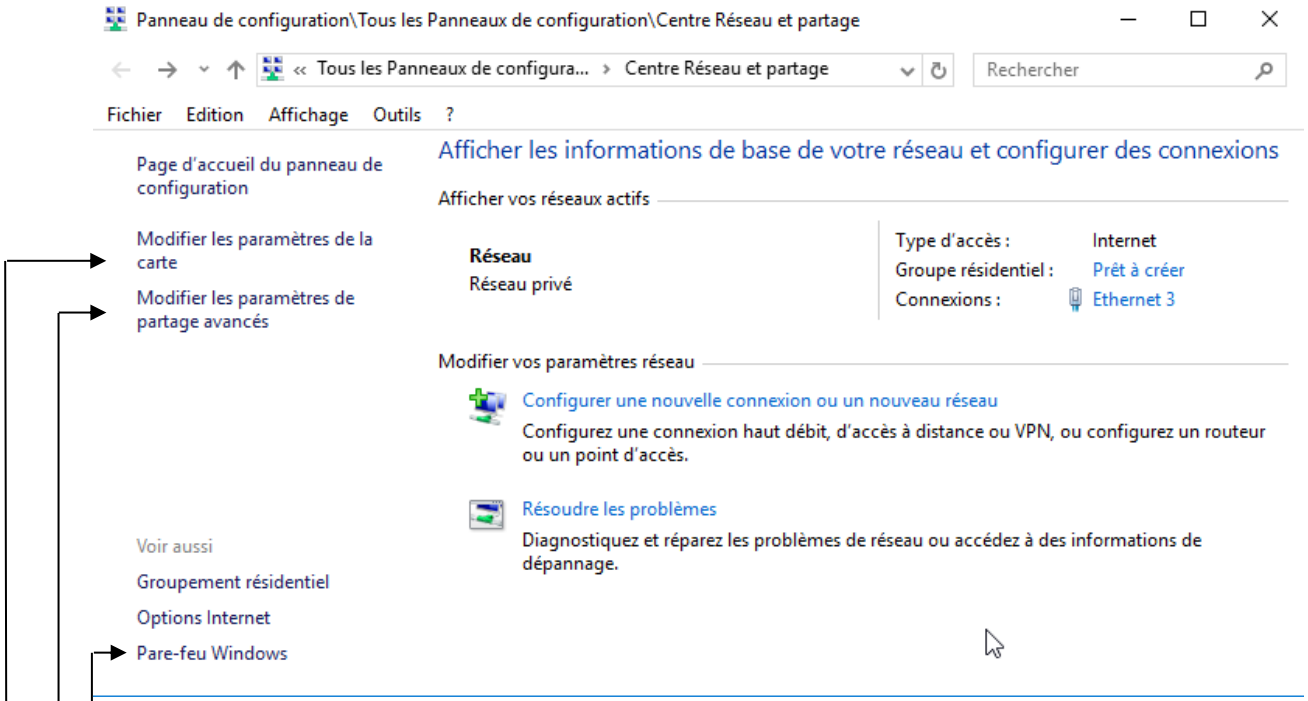
Quel que soit son aspect…



Un clic dessus puis "**Ouvrir le Centre Réseau et partage**"



Devrait amener



On peut aller aussi **Pare-feu Windows**

Modifier les paramètres de partage avancés

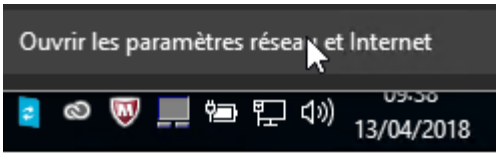
Permet de gérer les paramètres des "profils réseaux". On est depuis windows 10 toujours dans un profil réseau…

N.B: Il existe trois type de "profils" réseau au sens Windows, mais l'utilisateur ne peut choisir que entre **Privé / Public** , car si **Domaine** existe, il ne peut être remis en cause:

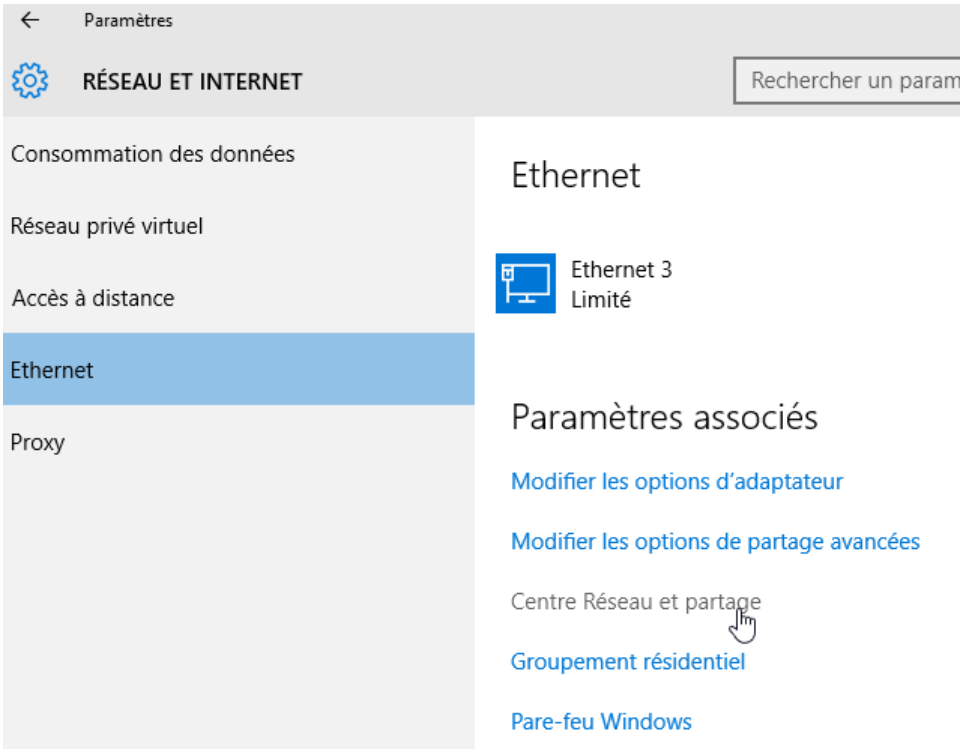
Modifier les paramètres de la carte

Permet pour chaque carte, de configurer les protocoles, dont TCP-IP…

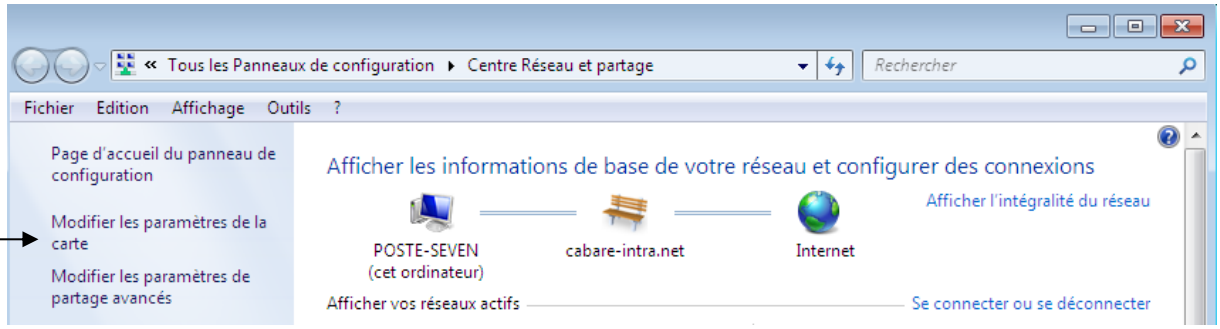
N.B : sous la version **Windows 10 - 1709** la boite de dialogue change, et on n'accède au **Centre de réseau et partage** qu'après être passé d'abord via **Ouvrir les paramètres réseaux et internet** (équivalent du menu paramètre **Windows 10 / réseau et internet**)



Et on retrouve le **Centre de Réseau et partage** ensuite

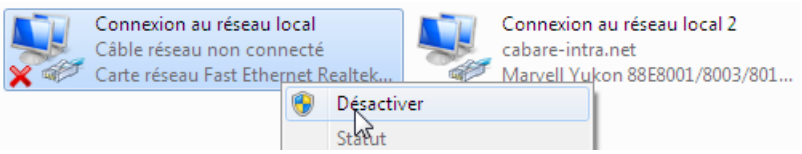


Désactivation Carte Excédentaire :



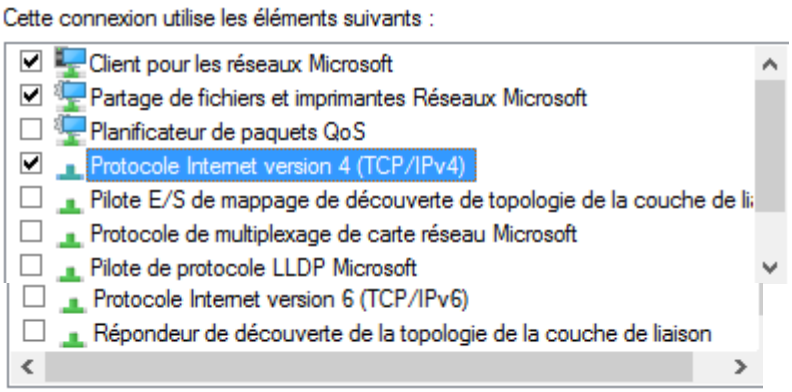
Modifier les paramètres de la carte donne accès en faitâ toutes les cartes physiques… Si plusieurs cartes réseaux sont présentes, il est plus judicieux de désactiver celle que l'on n'utilise pas.

Clic droit **Désactiver**



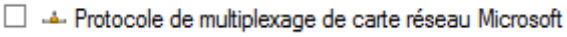
Protocoles LLDP - multiplexage - Topologie réseau Windows:

Lorsque l'on affiche les protocoles disponibles pour une carte réseau sous Windows 10, il y a beaucoup de protocoles disponibles

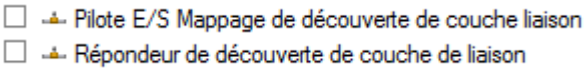


Protocoles présents (à ne pas activer)

LLDP Link Layer Discovery Protocol (LLDP) est un protocole 802.1ab. C'est un protocole destiné à remplacer un bon nombre de protocoles propriétaires (Cisco CDP, Extreme EDP, etc.) utilisés dans la découverte des topologies réseau de proche en proche



Protocole de multiplexage de carte réseau Microsoft utilisé pour deux scénarios d'utilisation typiques, chacun nécessitant au moins deux adaptateurs réseau fonctionnant (et connectés) sur un même PC. Le premier scénario s'appelle l'association d'adaptateurs, ce qui signifie l'utilisation simultanée de deux adaptateurs (trunk). Le second scénario est appelé basculement de l'adaptateur / haute disponibilité, où un adaptateur de secours prend en charge la connexion réseau en cas d'échec du serveur principal. (ha high availability)

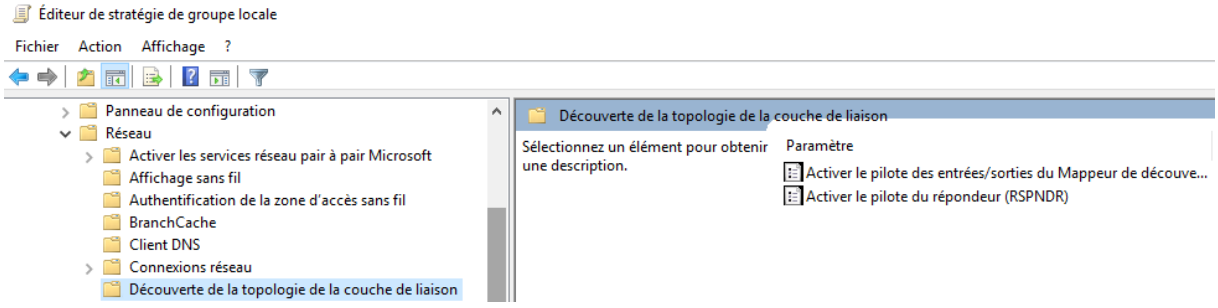


Pilote E/S de mappage de découverte de topologie de la couche de liaison

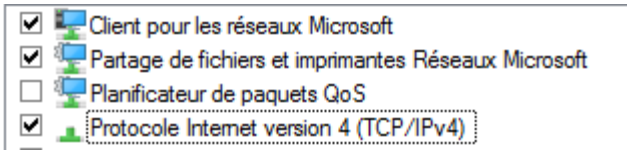
Répondeur de découverte de la topologie de la couche liaison

Ces pilote permet de remonter sur une machine tous les partages et les accès sur un réseau local, comme on pouvait l'avoir sous Vista et les premiers Seven. (afficher l'intégralité du réseau). Associé à un répondeur (forcément)

Peut se gérer via **gpedit.msc / modèle d'administration / réseau/ Decouverte de la topologie réseeau**



Les 3 protocoles absolument indispensables pour une connexion **ipv4** sont



Protocole Internet version 6 (TCP/IPv6)

Microsoft ne recommande pas la désactivation du protocole IPv6. Depuis Windows Vista et Windows Server 2008, IPv6 fait partie intégrante du système d'exploitation. Certains composants utilisent nativement IPv6 : **Remote Assistance** – **DirectAccess** - **Client Side Caching** (offline files) et **BranchCache**

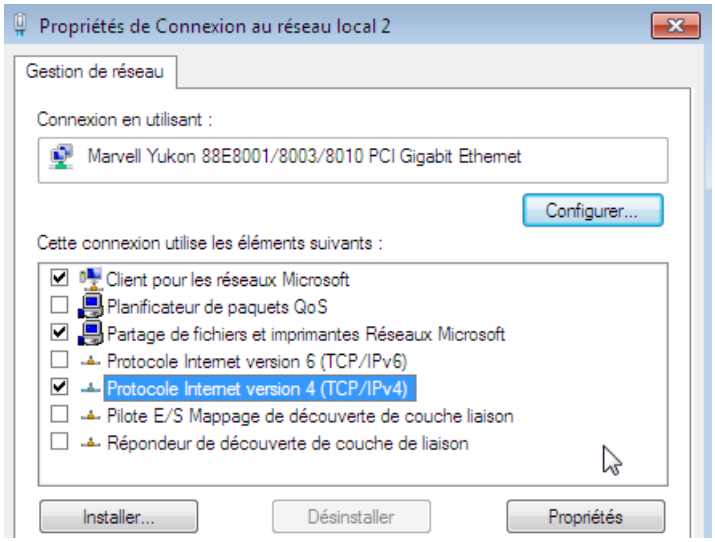
Il ne faut plus prioriser les flux comme on pouvait tenter de le faire sous Windows Seven ou 2008R2 ! Il faut laisser le protocole IPVv6 en client DHCP v6 et ce depuis la version Windows 10 1607.

Planificateur de paquets Qos

A ne pas activer, sauf si on utilise des applications le necessitant

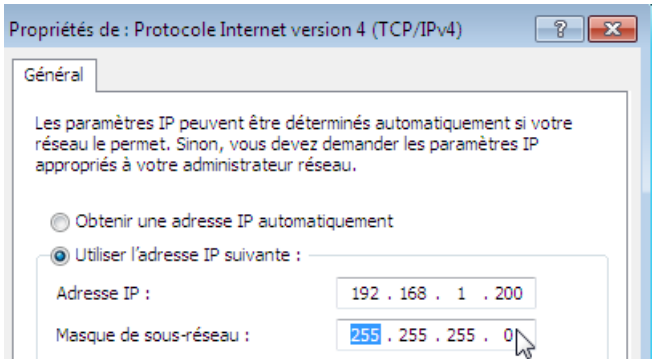
Protocole Internet version 4 (TCP/IPv4)

Pour chaque Icône, les propriétés de la carte permettent de définir les services et les protocoles voulus, notamment le Protocole TCP-IPv4



L'adressage de base Minimum réside en une Adresse IP et un Masque.

N.B: Pour l'identification du profil réseau, une passerelle facilite les choses



Ré-initialiser TCP/IP Sous Windows 10 :

Dans des cas extrêmes, pour réinitialiser la « Pile Ip » on ne peut plus désinstaller le protocole TCP-IP dans l'interface, mais on peut passer une commande en invite de commande.

Il faudra impérativement

- redémarrer le poste et
- reprendre toutes les configurations réseaux existantes

Donc en Invite de commande

netsh int ip reset

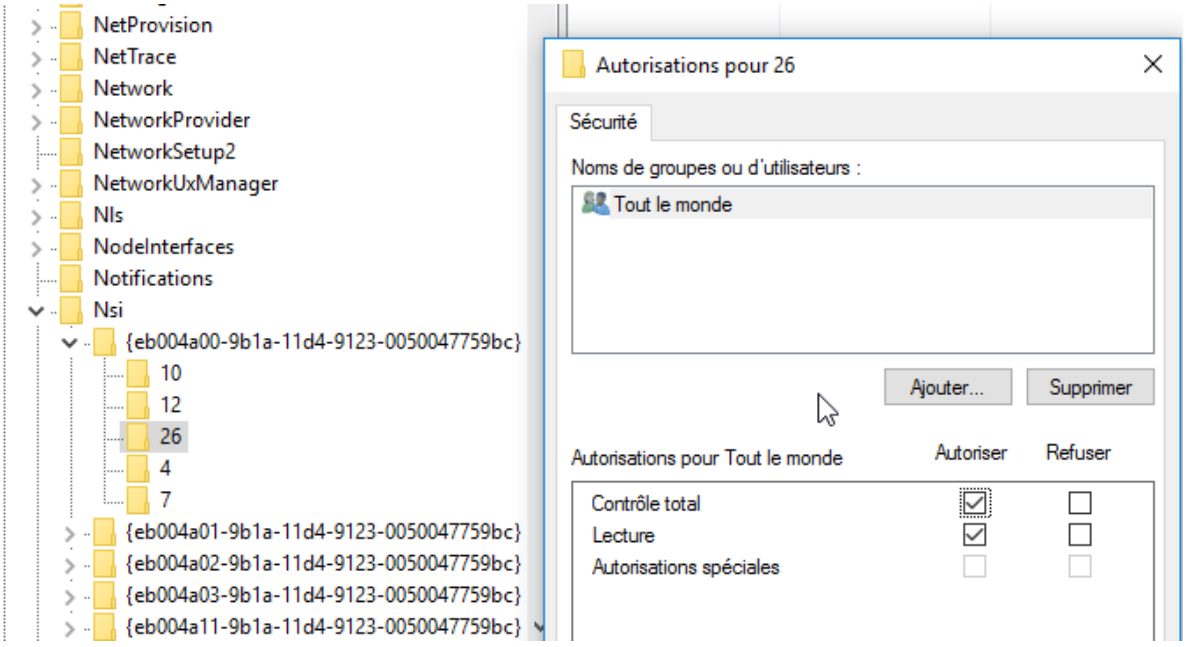
devrait donner

```
C:\Windows\system32>netsh int ip reset
Réinitialisation de Interface réussie.
Réinitialisation de Adresse unicast réussie.
Réinitialisation de Chemin d'accès réussie.
Réinitialisation de  réussie.
Redémarrez l'ordinateur pour terminer cette action.
```

N.B : Il se peut que l'on ait un petit souci sur la composante DHCP, en Workgroup

```
C:\Windows\system32>netsh int ip reset
Réinitialisation de Général réussie.
Réinitialisation de Interface réussie.
Réinitialisation de Adresse unicast réussie.
Réinitialisation de Voisin réussie.
Réinitialisation de Chemin d'accès réussie.
Réinitialisation de Routage réussie.
Échec de la réinitialisation de .
Accès refusé.

Réinitialisation de  réussie.
Redémarrez l'ordinateur pour terminer cette action.
```

Cela peut se résoudre via la Base de Registre où il faut donner les droits en **Contrôle total** à **tout le monde** sur la ruche **26** de la ruche **{eb004a00-xxxxx}** située en **HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Nsi**



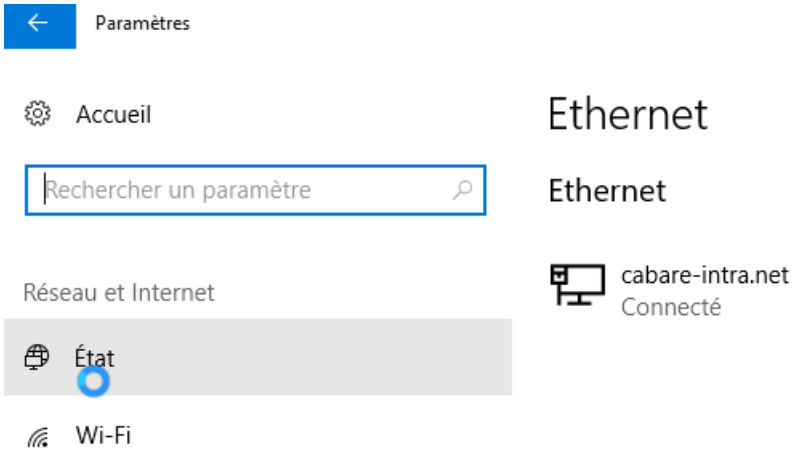
Depuis la version **1607** de windows on peut directement demander depuis l'interface graphique, via les paramètres, une ré-initialisation de TCP-IP.

Il faudra impérativement

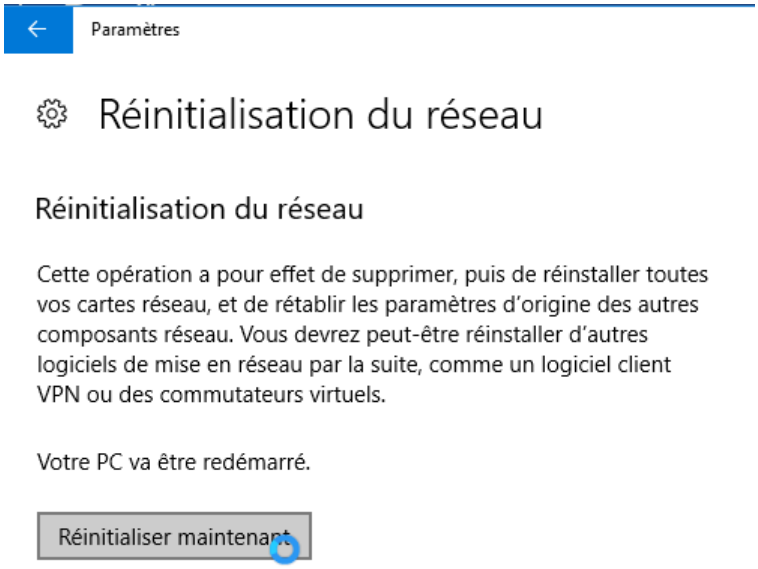
- redémarrer le poste et
- reprendre toutes les configurations réseaux existantes

1. Sélectionnez le bouton **Démarrer**, puis sélectionnez **Paramètres** > **Réseau et Internet** > **État** > **Réinitialisation réseau**.

Dans **Etat** on va chercher (tout en bas) **Réinitialisation du réseau**



Et on demande de **Réinitialiser maintenant**



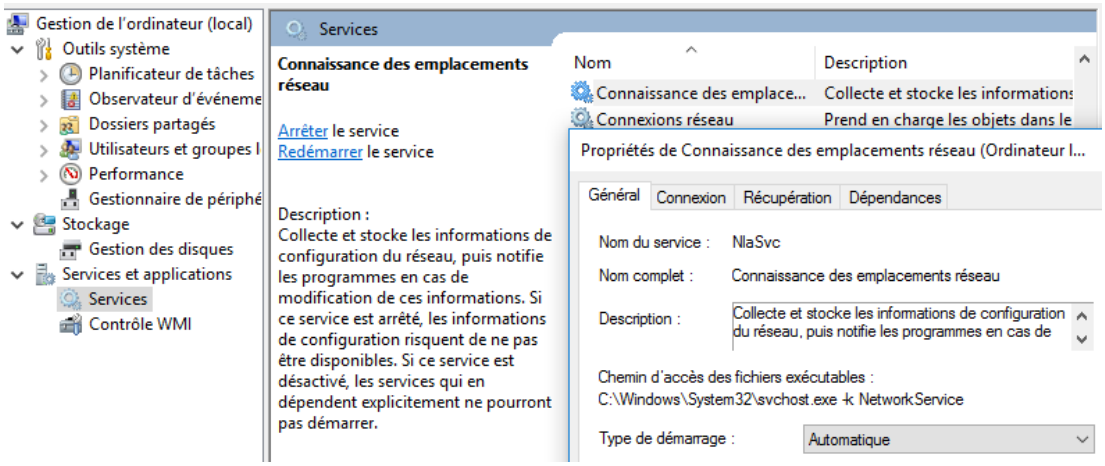
Profil – Type Réseau Windows 10 :

On est avec Windows 10 toujours dans un profil réseau… Dès qu'un réseau est détecté. Il existe trois type de réseau, mais l'utilisateur ne peut choisir que entre **Privé / Public** , car si **Domaine** existe, il ne peut être remis en cause.

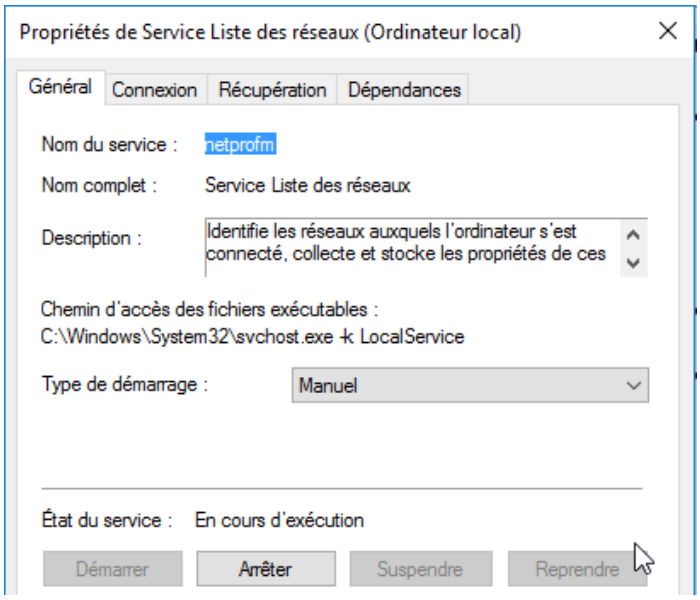
- Domaine
- Privé
- Public

La différence entre **Public / Privé** est une différence des paramétrages par défaut, disponible dans les "partages avancés" et dans le pare-feu.

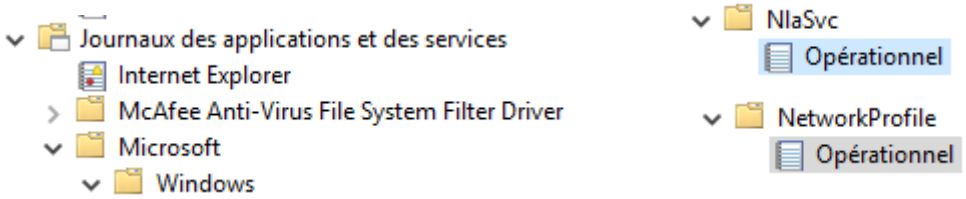
C'est le service "**Connaissance des emplacements réseau**" (**NlaSvc**) qui gère cela. Vérifier qu'il soit bien démarré sur les clients



Il y a un service dépendant également qui intervient c'est "**Service Liste des réseaux**" (**Netprofm**)



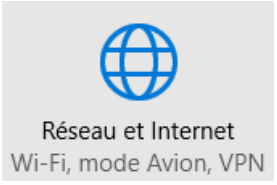
Dans l'observatoire d'évènement les sources: **Microsoft-Windows** avec **NlaSvc** et **NetworkProfile** peuvent aider pour un diagnostic



Changer de type de Profil réseau – interface Paramètre :

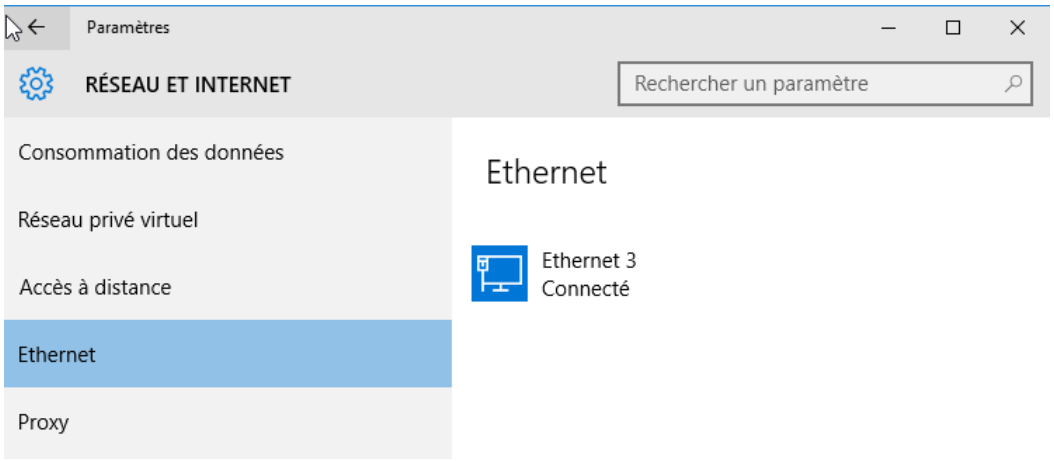
Dans l'interface Windows 10 on demande **Paramètres**

et ensuite **réseau et internet**

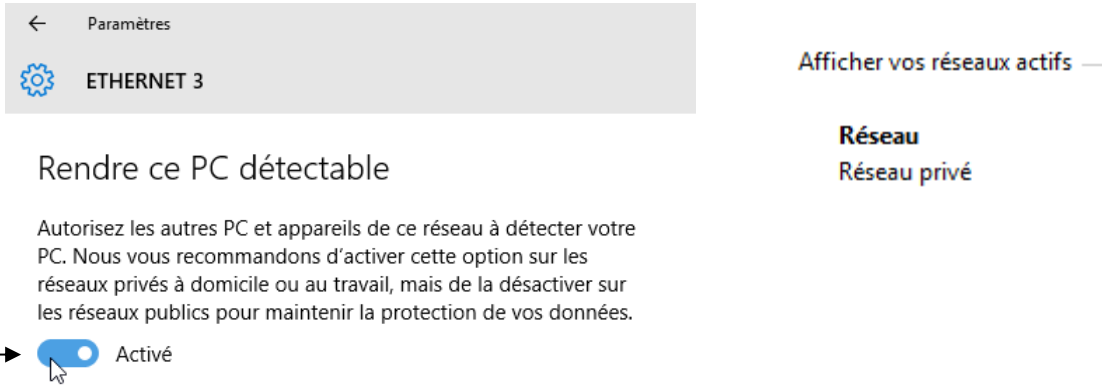


On se place ensuite sur **Ethernet,** et on sélectionne la carte réseau pour laquelle on veut modifier le type de Profil

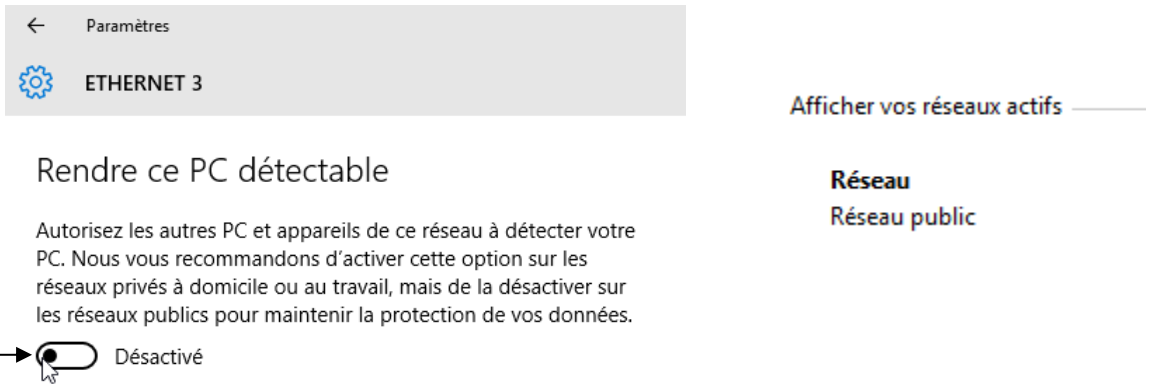
Dans l'exemple **Ethernet 3**



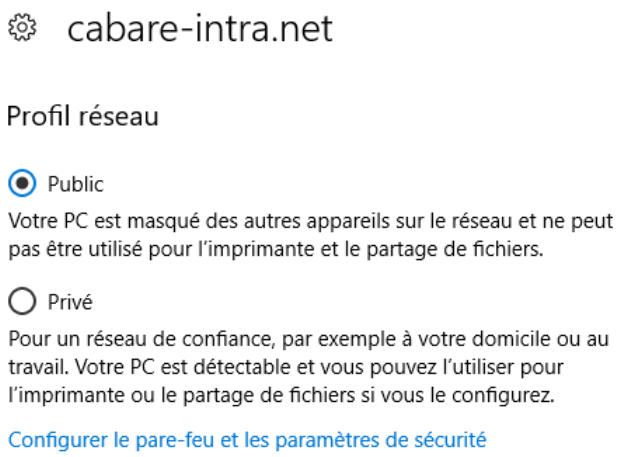
Dans la boite de dialogue qui s'ouvre, on ne choisit pas public ou privé, mais simplement le fait de dire **Rendre ce pc détectable**, fera le réseau de type **Réseau privé**



Et si on indique ne pas vouloir, alors cela fera le réseau de type **Réseau public**



N.B : sous la version **Windows 10 - 1709** la boite de dialogue change, et on a de nouveau la mention **profil réseau public / privé** qui apparaît (à la place de detectable…)



Changer de type de Profil réseau – Powershell :

In faut d'abord récupérer le nom du progfil réseau en cours par la commande • **Get-NetConnectionProfile**

```
PS C:\Users\Administrateur> Get-NetConnectionProfile


Name             : Réseau non identifié
InterfaceAlias   : Ethernet 3
InterfaceIndex   : 6
NetworkCategory  : Public
IPv4Connectivity : NoTraffic
IPv6Connectivity : NoTraffic
```

Puis passer une commande du genre **Set-NetConnectionProfile**

Avec 2 paramètres **- name (et entre guillemets le nom du profil)**

et **- NetworkCategory (avec mot clé Private ou Public)**

```
Set-NetConnectionProfile -name "Réseau non identifié" -NetworkCategory Private
```

Changer de type de Profil réseau WI FI – windows 1709

Cela n'est possible que si la connexion est uniquement en WIFi

Si une connexion en RJ45 est active en parallèle, on ne peut choisir le type de réseau pour la connexion WIFI

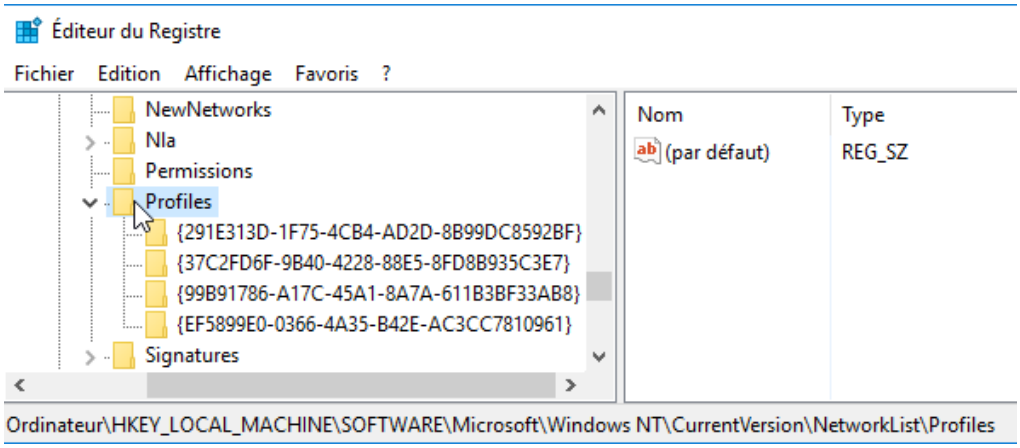
Pour modifier le statut d'un réseau Wi-Fi en public ou privé

1. Sélectionnez **Démarrer**, puis **Paramètres** > **Réseau et Internet** > **Wi-Fi**.
2. Sélectionnez **Gérer les réseaux connus**, sélectionnez le réseau dont vous souhaitez modifier les paramètres, puis sélectionnez **Propriétés**.
3. Sous **Profil réseau**, sélectionnez **Public** ou **Privé**.

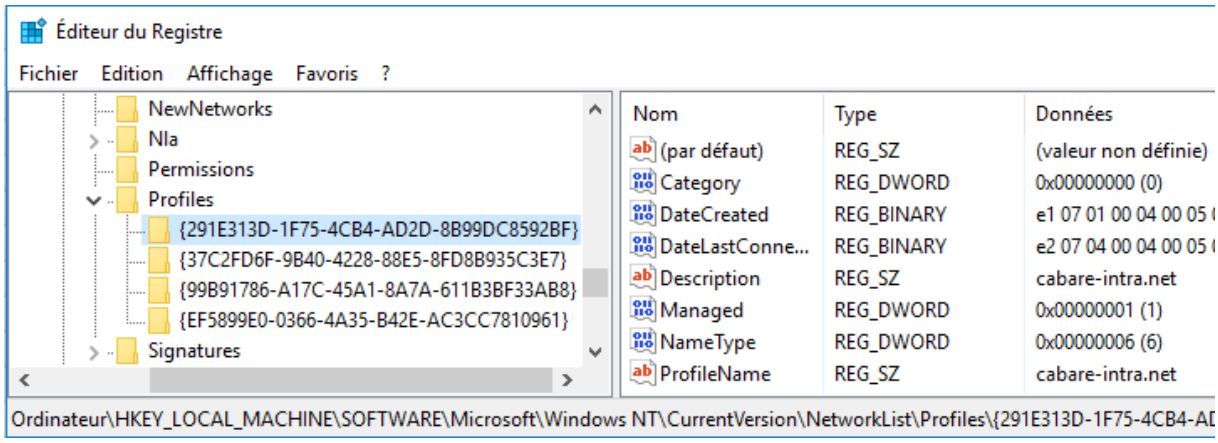
Changer de type de Profil réseau – Regedit :

Se placer dans la clé suivante :

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles

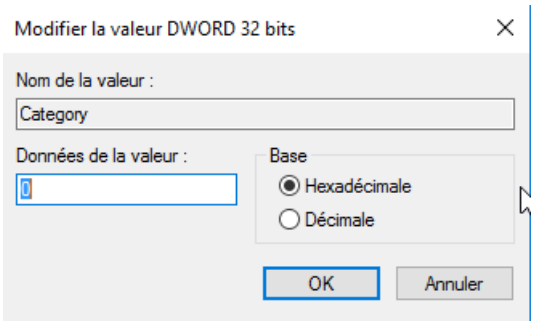


Rechercher dans les sous-clé, (ici dans l'exemple il y en a **4**) celle correspondant à votre réseau (la valeur **ProfileName** doit porter le nom de votre connexion réseau, ici dans l'exemple **cabare-intra.net**)



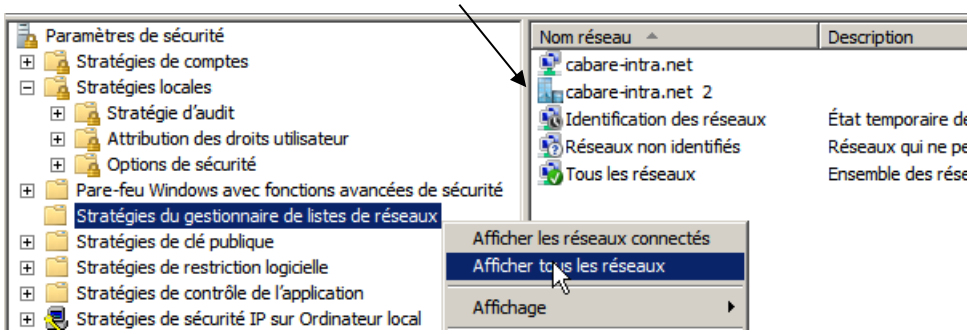
La valeur **DWORD Category** correspond au type de profil (Public/Privé/Domaine) avec les conventions suivantes

Public 0 Privé 1 Domaine 2



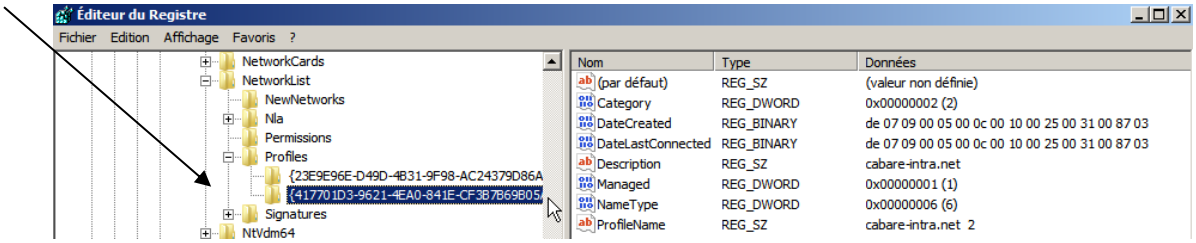
Reset - Listes des réseaux identifiés

N.B : la liste de tous les réseaux détectés par Windows se trouve en demandant dans les **stratégies de sécurité locales**, dans les **stratégie du gestionnaire de liste de réseaux / Afficher tous les réseaux**



N.B : la liste des réseaux détectés par Windows est stockée en dans la base de Registre en

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\NetworkList\Profiles



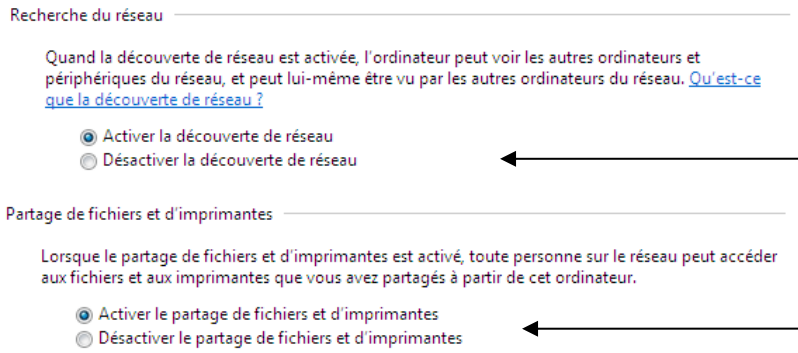
Pour faire un **Reset** de la situation il peut être necéssaire de

- Désactiver la carte réseau
- Modifier l'adressage IP
- Purger les **NetworkList\Profiles** de la base de registre
- Re-demarrer le service **Service Liste des réseaux (netprofm)**
- Réactiver la carte réseau

PARAMETRES PROFIL RESEAU AVANCE

Réglage Disponibles:

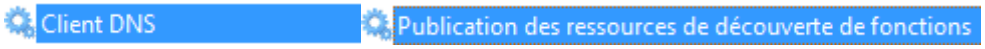
Les réglages suivants existent selon les profils réseaux… Surtout



Pour voir les postes dans les favoris réseaux…

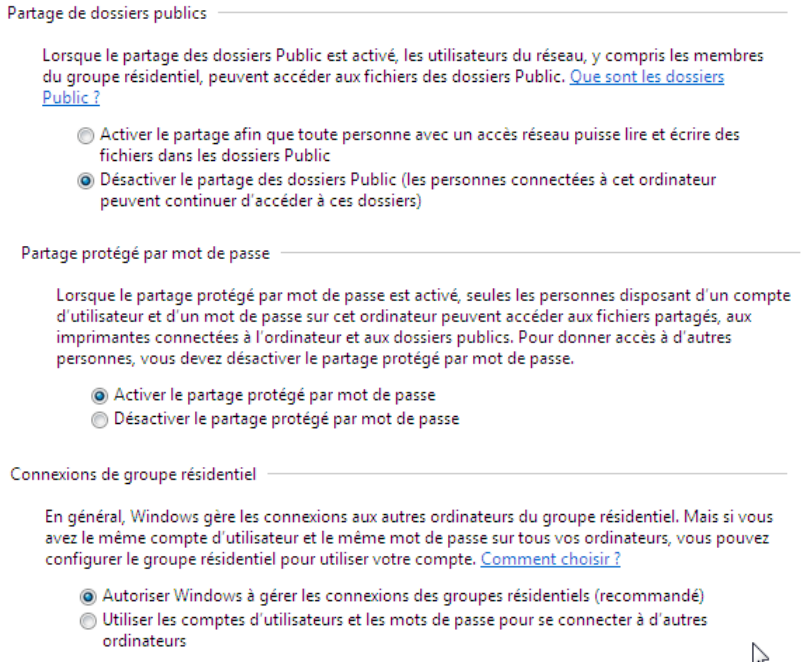
Mais pour que cela soit possible, il faut absolument que les 4 services suivants soient démarrés sur le poste (ce qui n'est pas toujours le cas):

Client DNS **Publication des ressources…**



Découverte SSDP **Hôte de périphérique**

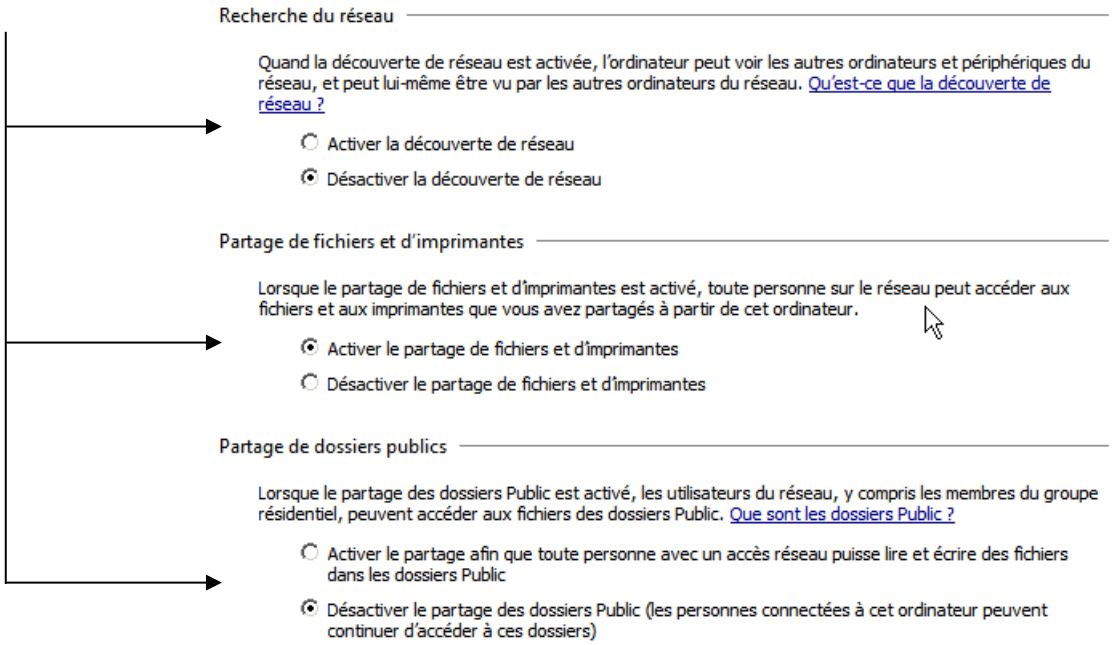
Dossiers publics et **groupe résidentiels** ne devraient pas être activés sur des machines professionnelles…



Jeux de Réglages:

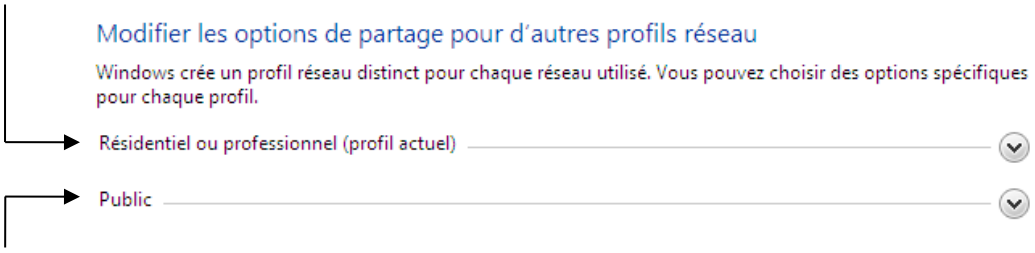
Le jeu des réglages est quasiment le même dans tous les profils...

à chaque emplacement correspond un "jeu de réglage" pré-réglé



Sur une machine en workgroup deux profils type existent

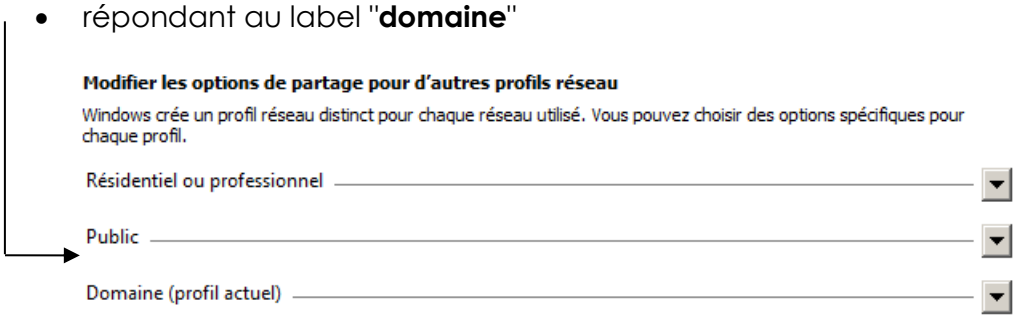
- un répondant au label "**privé**"



- un répondant au label "**public**"

Sur une machine appartenant à un domaine un troisième profil apparaît (et on ne peut pas en choisir un autre)

- répondant au label "**domaine**"



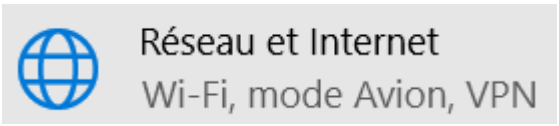
PARE-FEU WINDOWS

Activation - Désactivation :

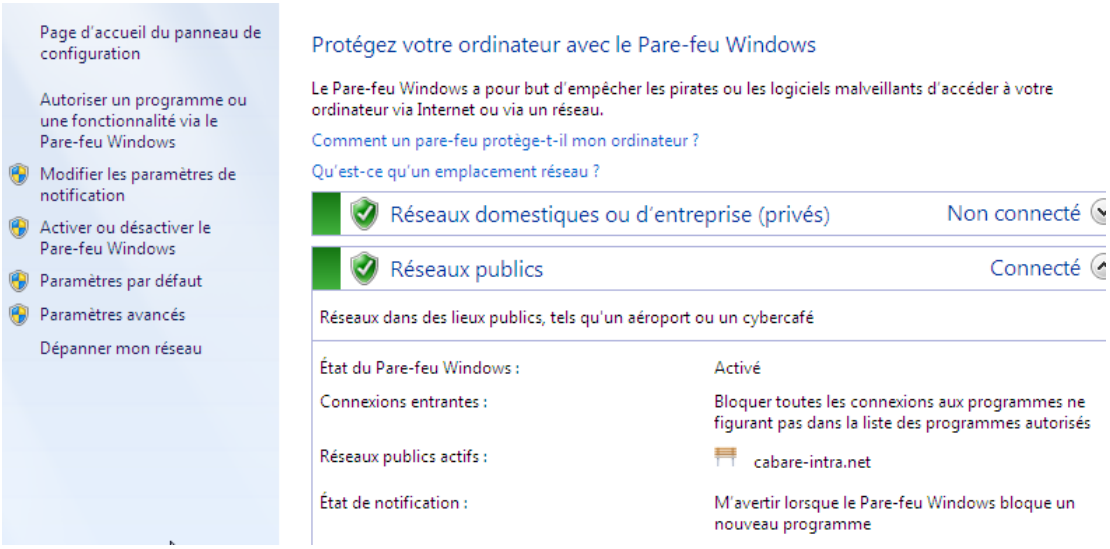
Via l'interface

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

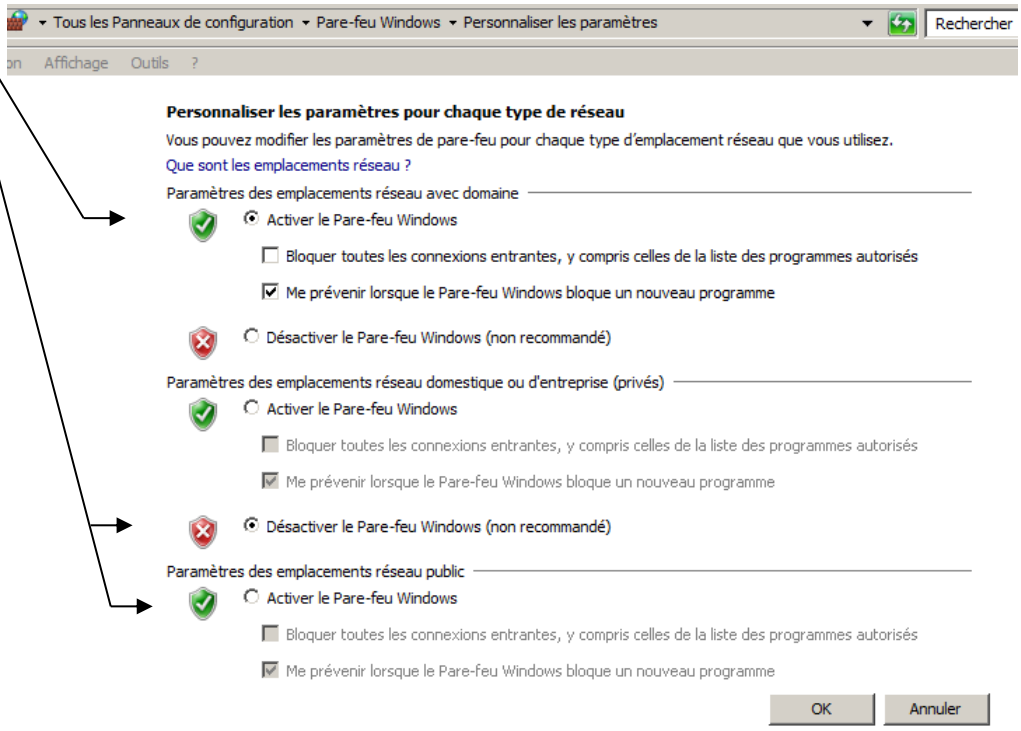
Paramètres / Réseau et Internet / Ethernet



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

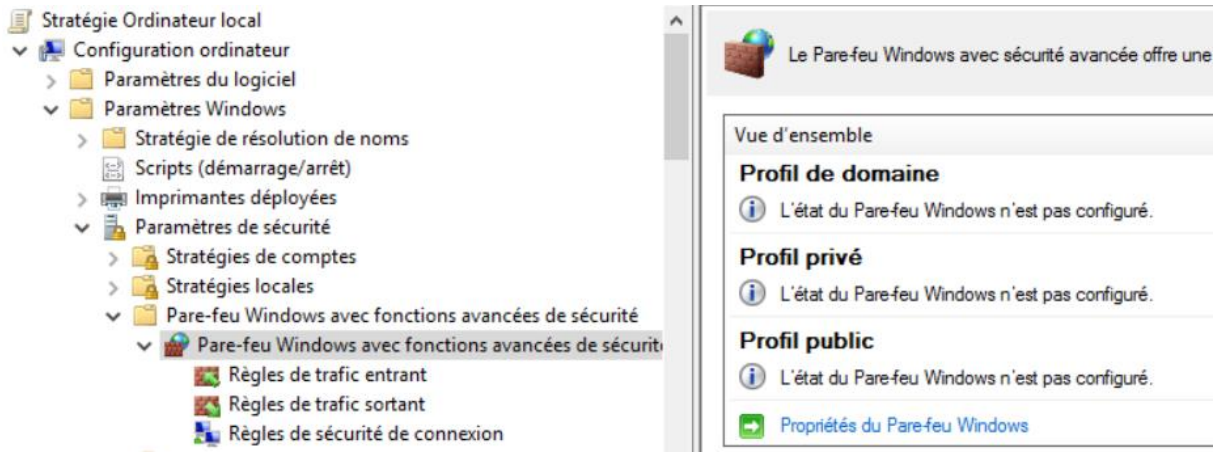


On peut l' **Activer – Désactiver** selon les profils existants…

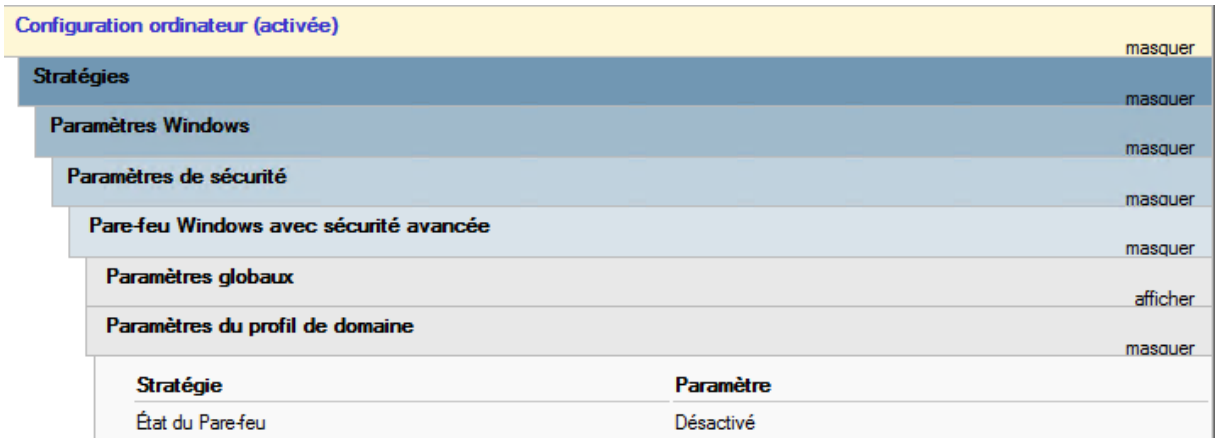


Via GPO

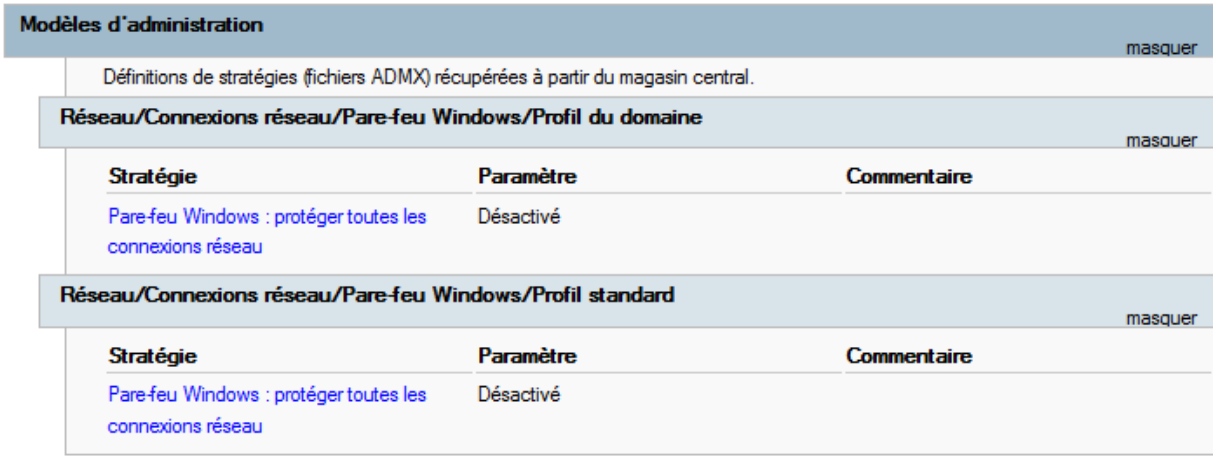
Soit Locale



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

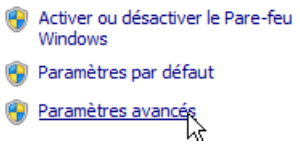
Une commande existe du type en spécifiant **True** ou **False** selon le besoin…

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

```
PS C:\Windows\system32> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled True
PS C:\Windows\system32> Set-NetFirewallProfile -Profile Domain,Public,Private -Enabled false
```

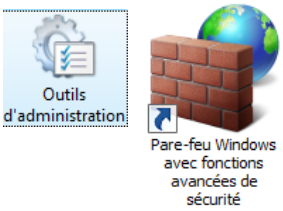
Version Avancée :

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

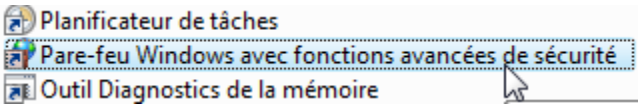


Cette version se trouve également accessible directement dans les outils d'administration

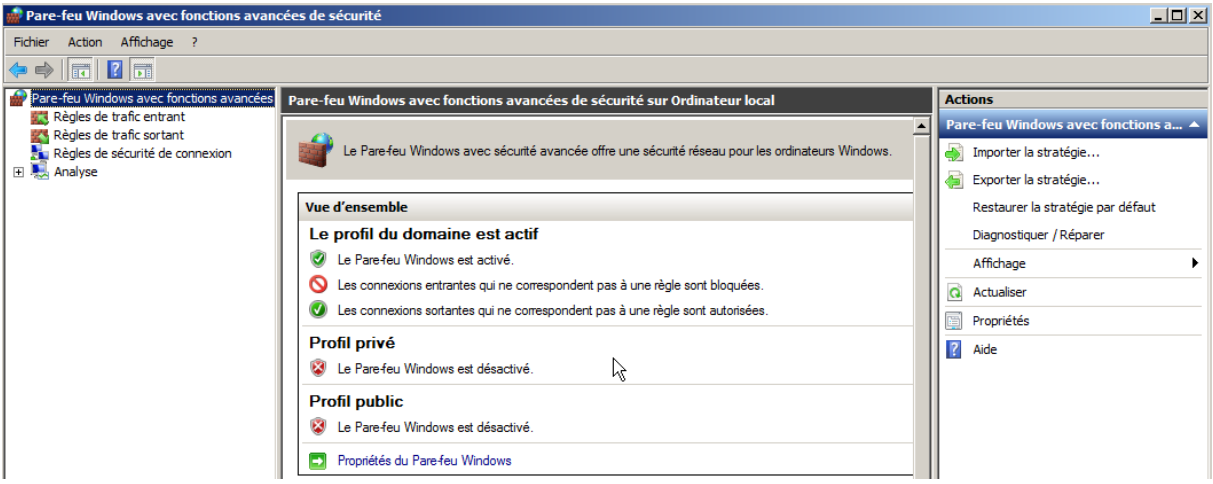
Panneau de Configuration / outils d'Administration



Pare-feu Windows avec fonctions avancées de sécurité

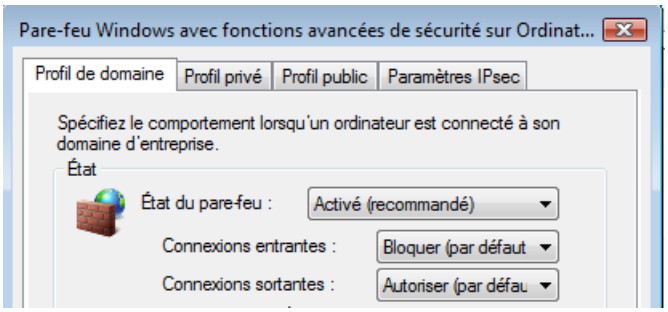


Donnant

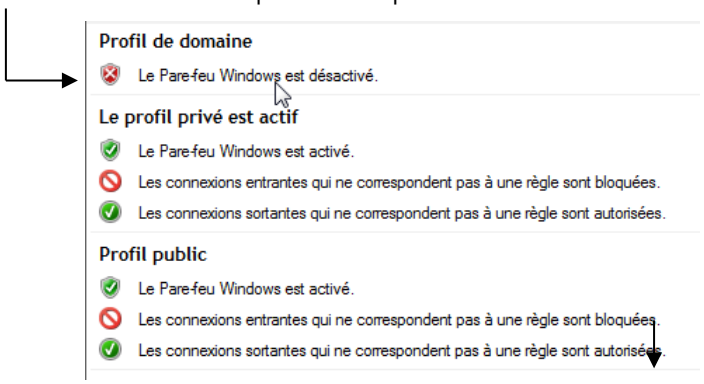


à travers les **propriétés du pare-feu** on peut choisir d'armer ou non le pare-feu selon le type réseau …

…

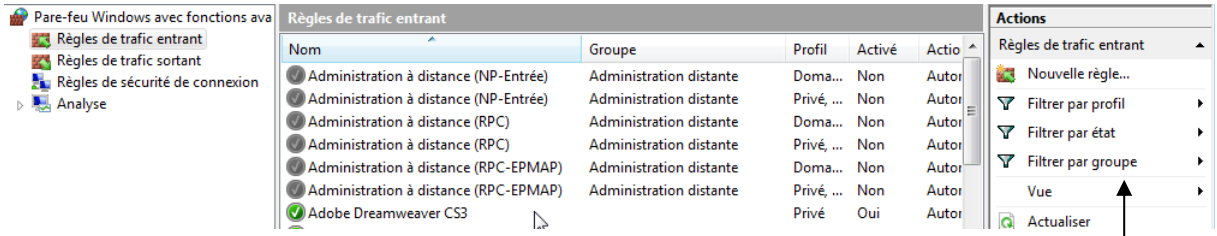


pour le désactiver par exemple dans le cas d'un domaine…



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 :

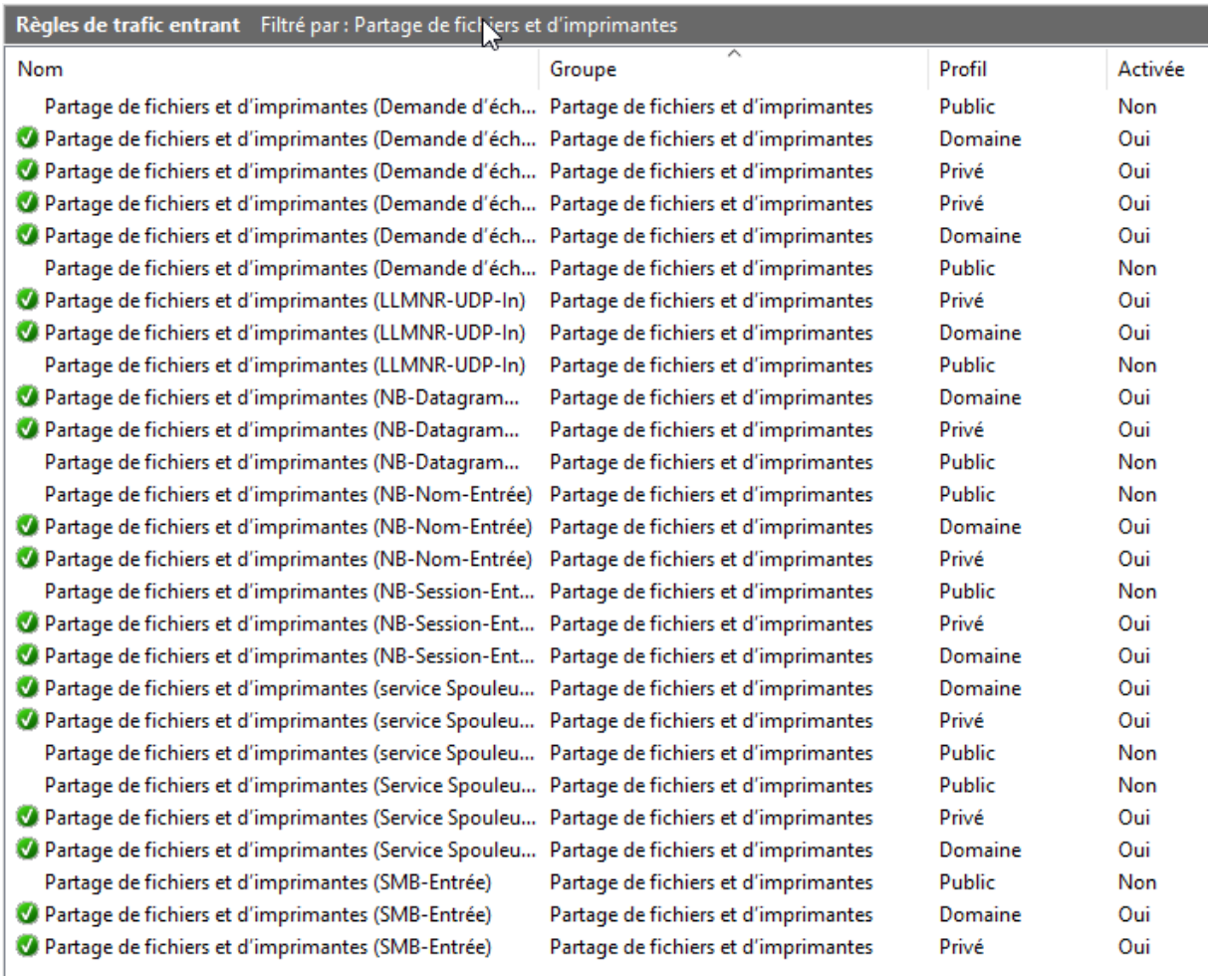
  Activée – non Activée

- Groupe de classification de la règle :

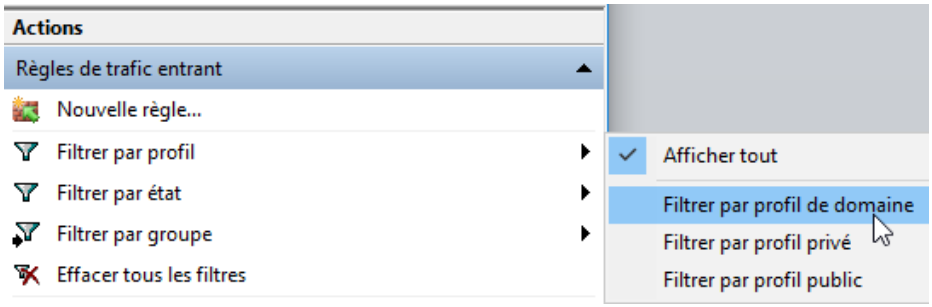
  Réseau de Base – Administration distante – partage fichiers et imprimantes…

Règles entrantes prédéfinies recherche:

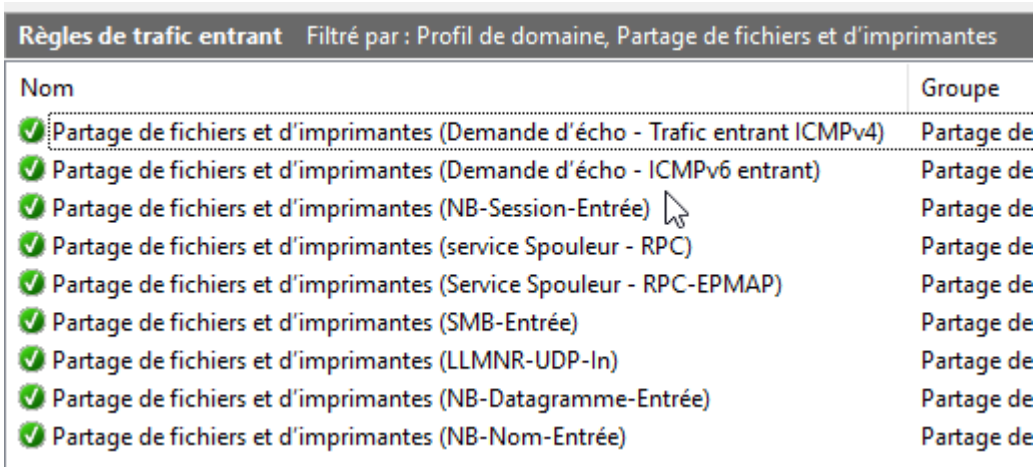
il existe des règles entrantes pré-définies : Cherchons par exemple la règle autorisant **ICMP** en **IP** version **4**, il y a beaucoup de règles, qui sont regroupées dans la catégorie **Partage fichiers et imprimantes**)



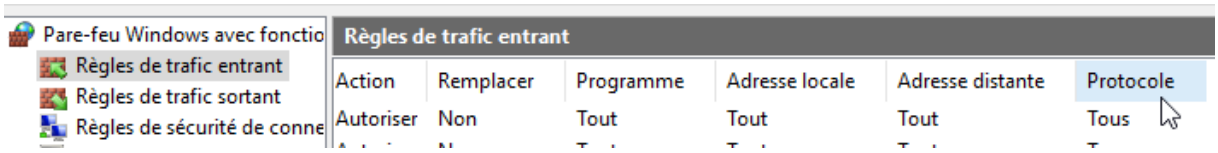
Pour limiter notre affichage, on va demander uniquement les règles applicables sur un Domaine



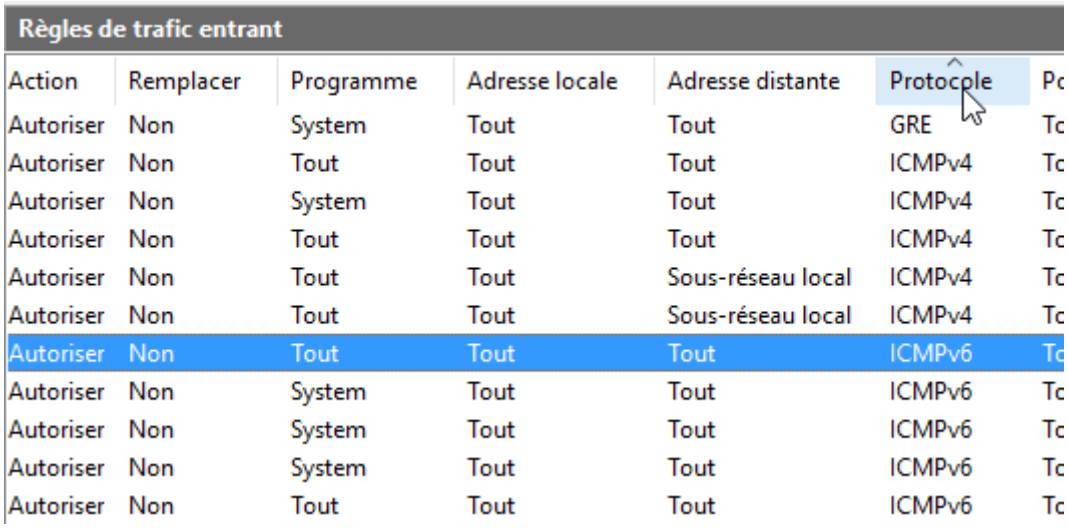
qui seront valables selon le profil réseau:



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

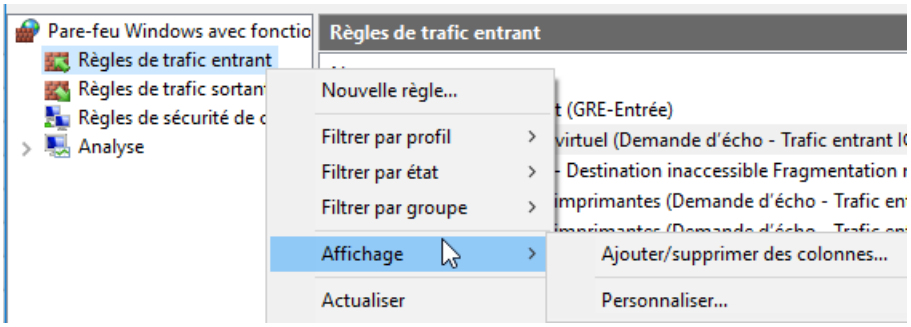


Si on classe les règles par protocole, alors on obtient et il est facile de chercher ICMP V4!

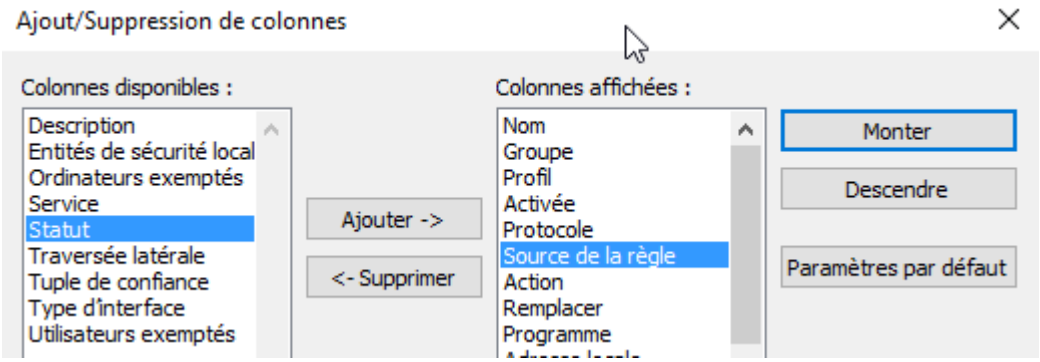


On peut aussi modifier l'aspect / l'information pour l'affichage des règles

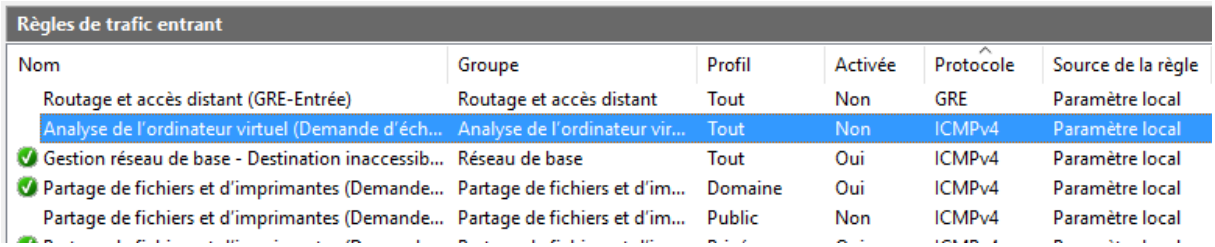
Dan **Règles de trafic entrant** clic droit / **Affichage**



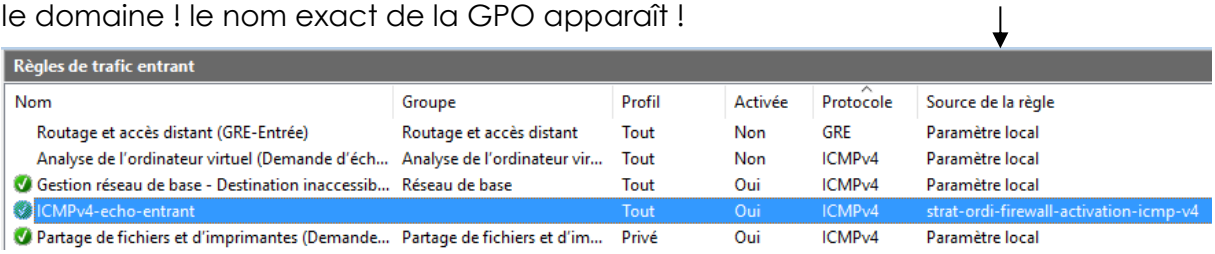
On ajoute / supprime ou modifie l'ordre des colonnes



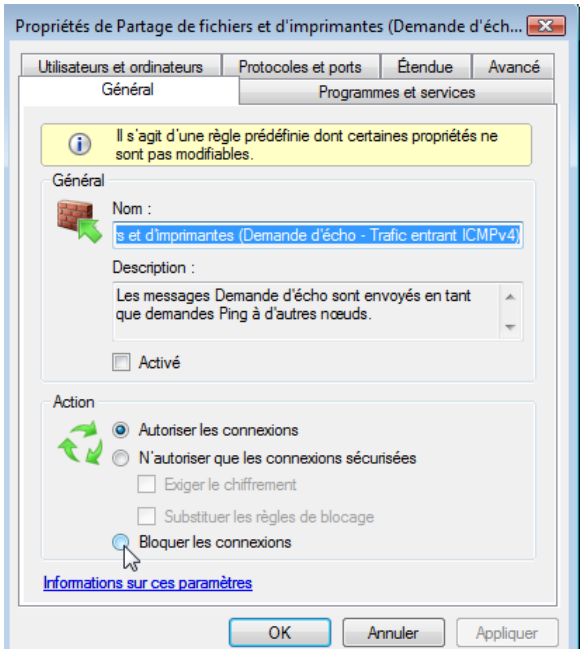
Par exemple ici on rapproche la colonne **protocole**, et on ajoute une nouvelle colonne **Source de la règle**

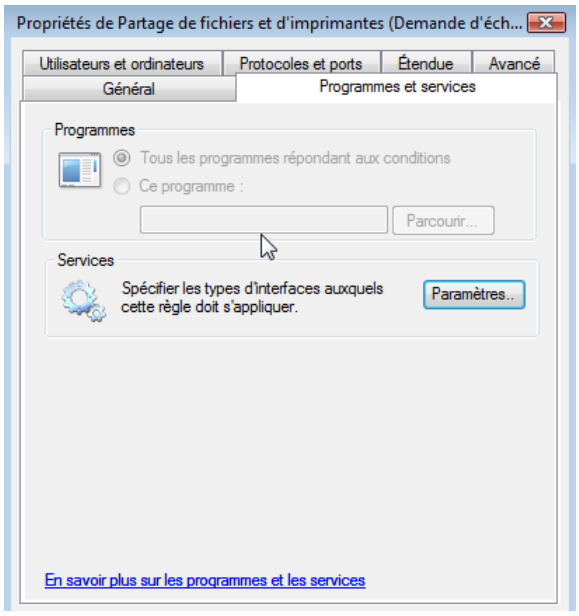


Cela permet de mieux voir ce qui est géré localement, et ce qui est dirigé via le domaine ! le nom exact de la GPO apparaît !



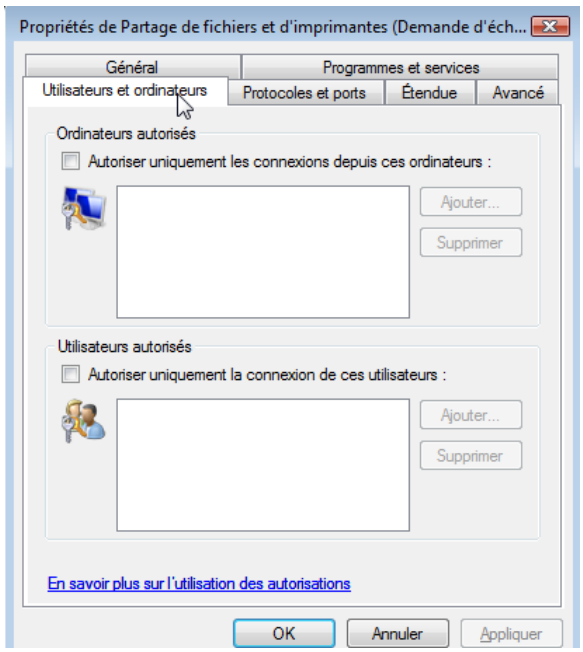
Règles Propriétés:

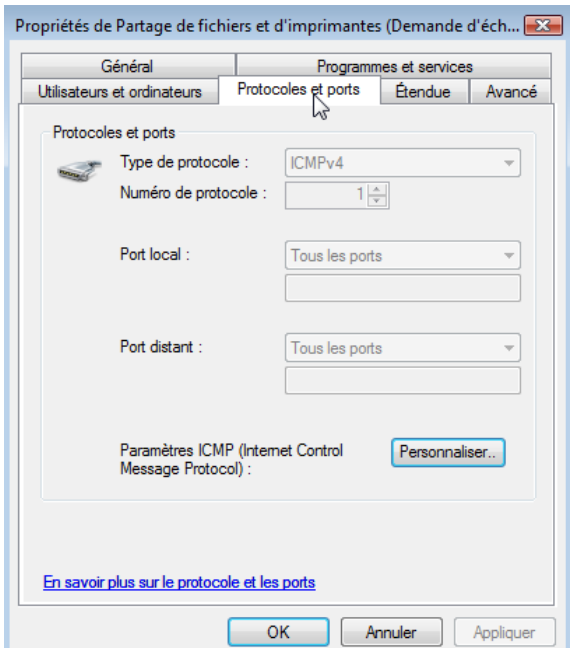




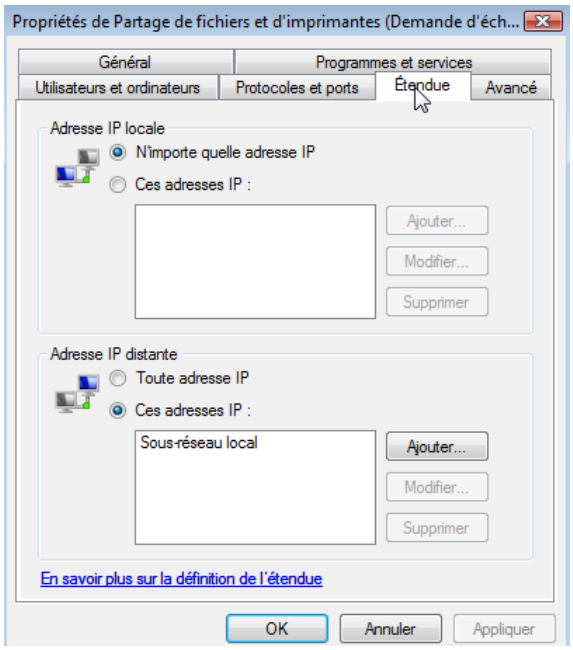
plusieurs onglets permettent d'affiner la règle:

des machines, des users

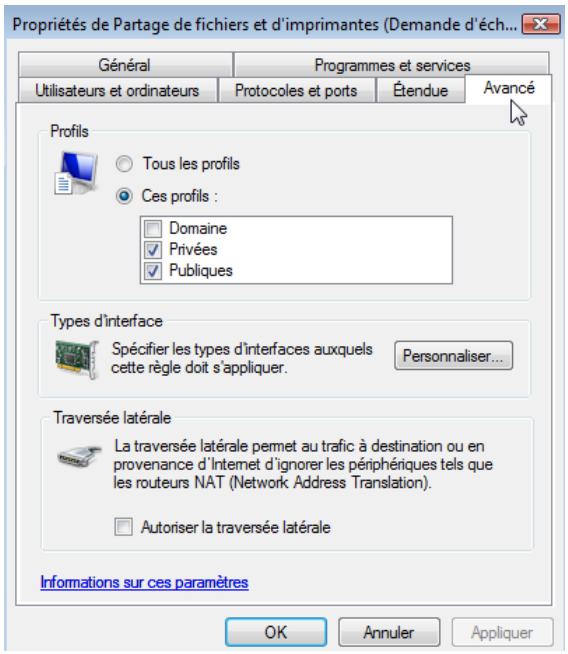




Des adresses IP



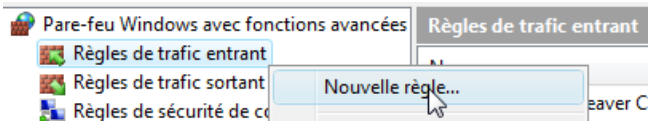
des profils réseau



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

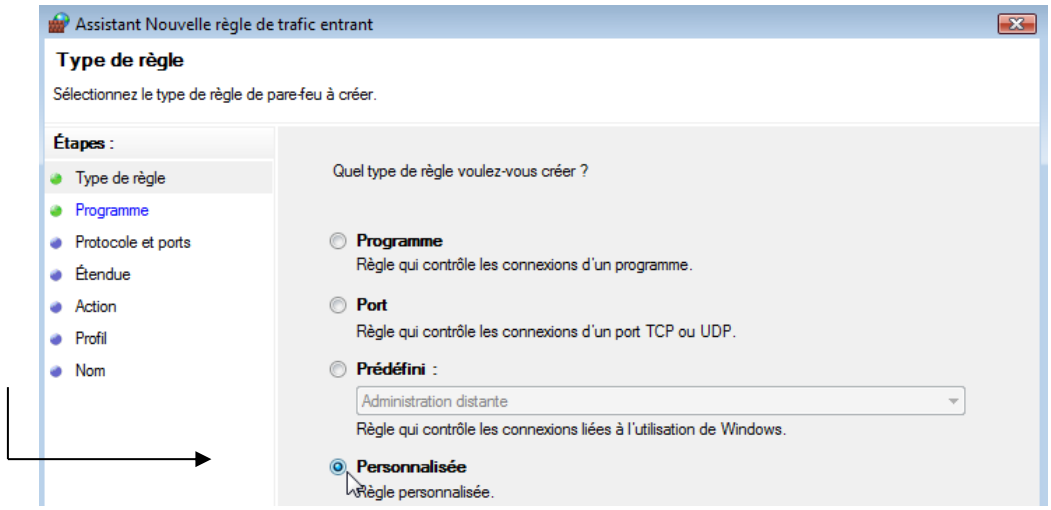
Création Règles entrantes personnelles:

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

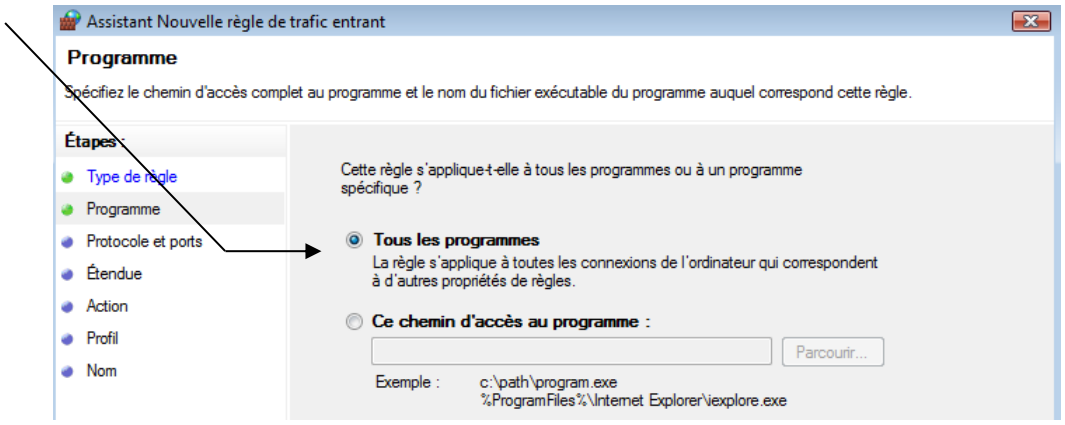


Par exemple, on veut créer une Règle entrante protocole ICMP – V4 de base:

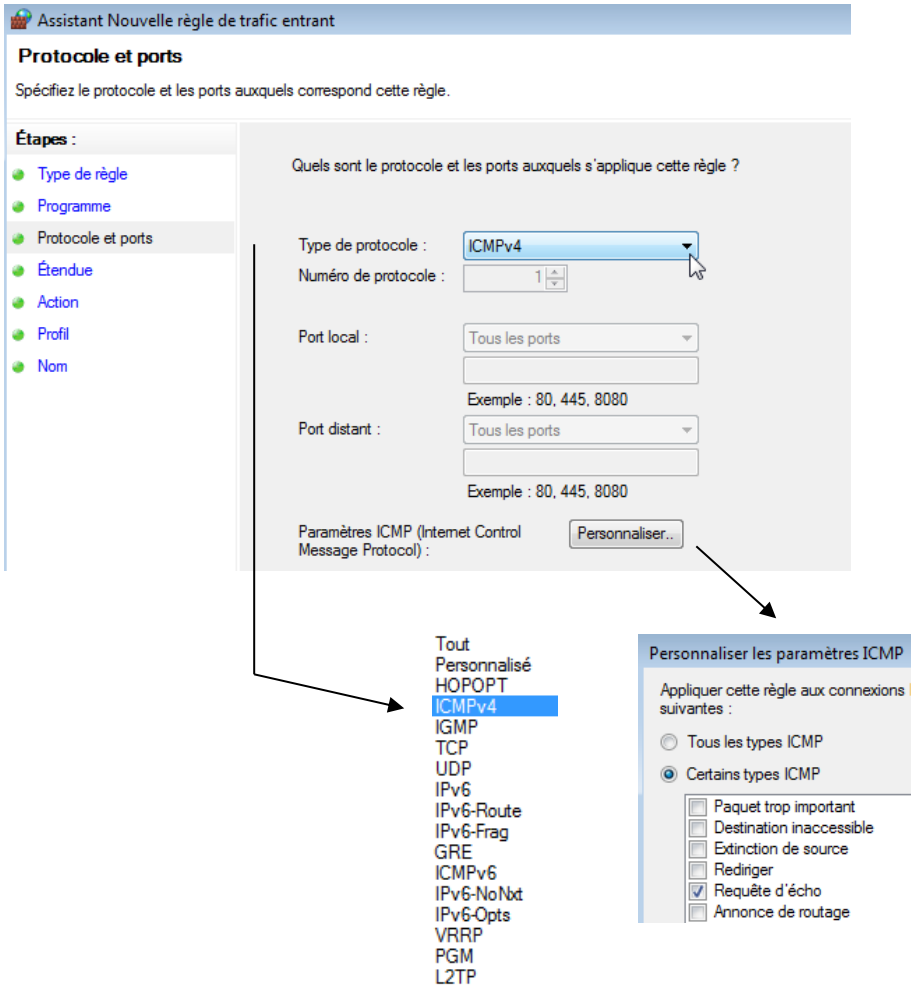
On demande **personnalisée**



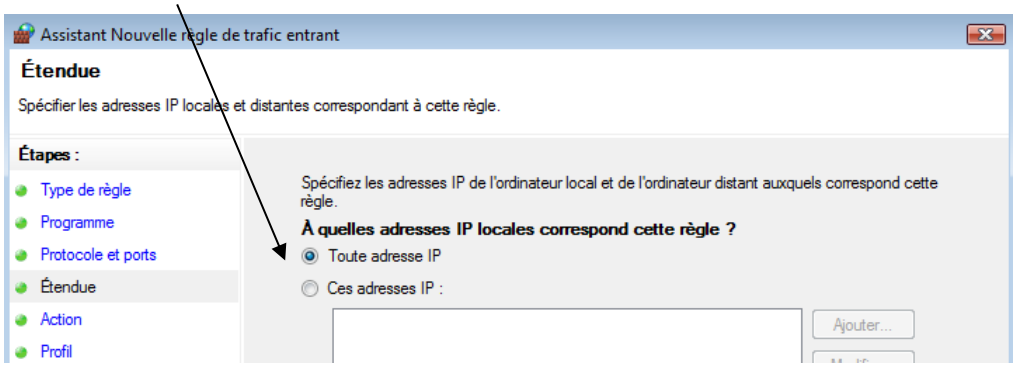
A **Tous les programmes**



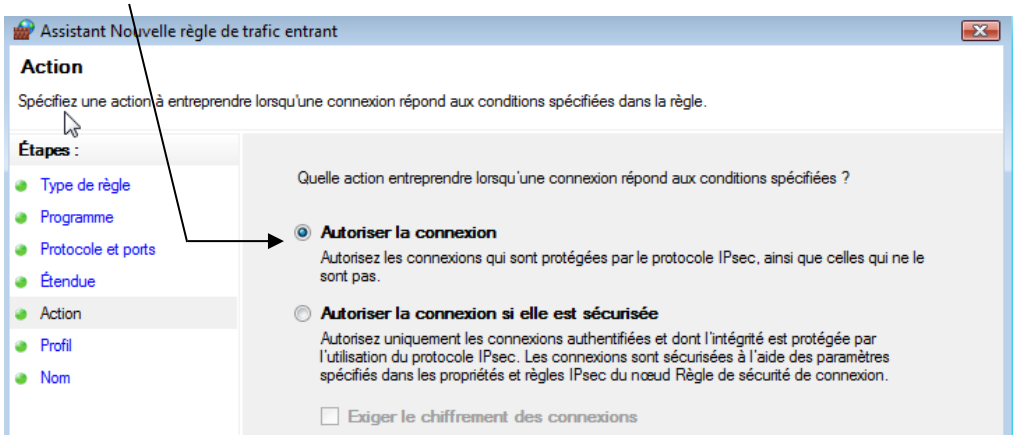
On affine les réglages



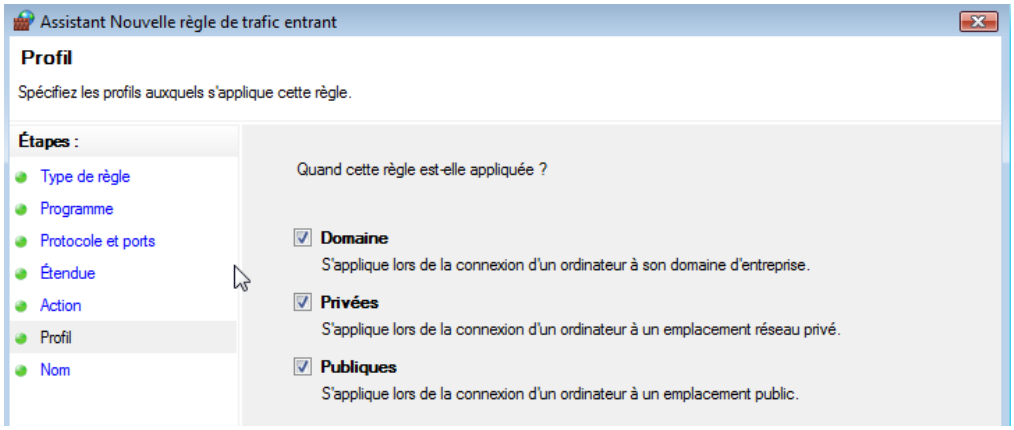
On indique toutes les adresses ip



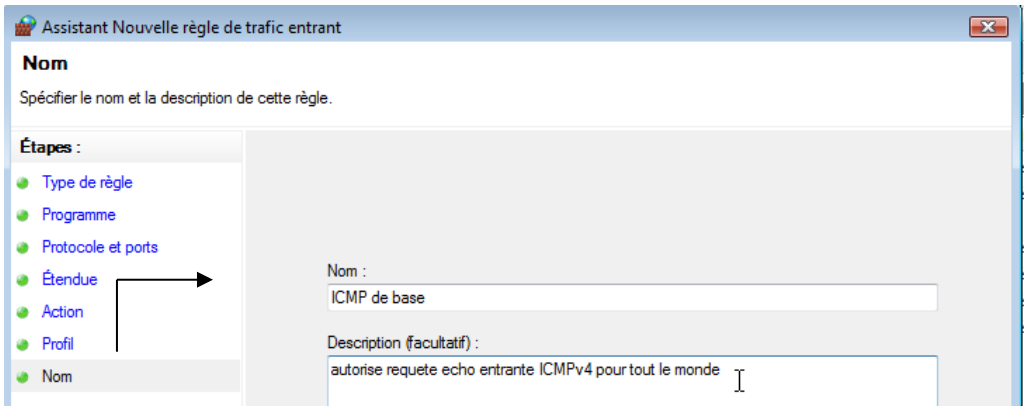
Et le comportement de la règle - **Autoriser**



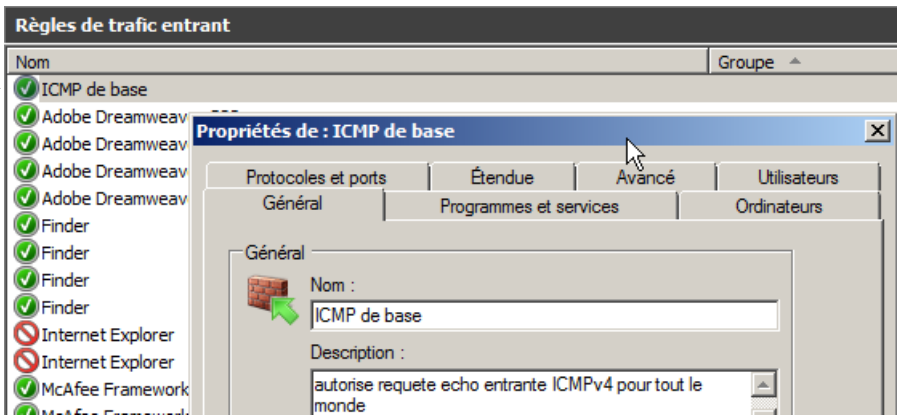
Selon le profil réseau- les 3



Il ne reste plus qu'a lui donner un nom



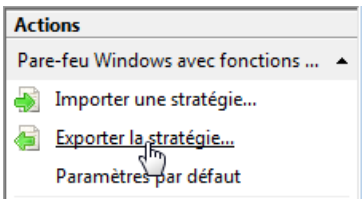
Et voici notre nouvelle règle !



STRATEGIES GESTION PARE-FEU

importer Exporter une stratégie :

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



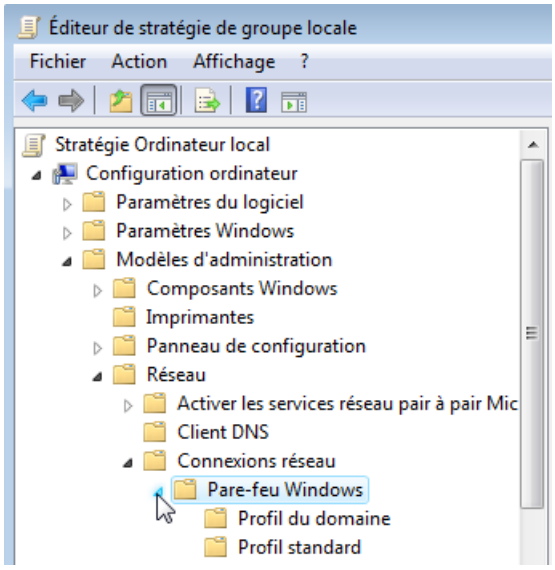
cela marche à partir de **Seven** et **2008**…et cela peut s'appliquer par batch via **netsh**

(cf chapitre netsh)

Stratégie Profil Domaine – standard via gpedit.msc :

au niveau **ordinateur**…

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



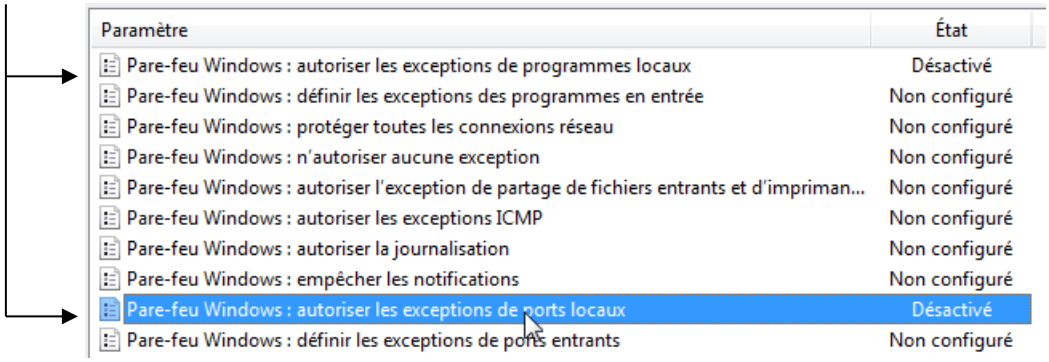
donnant sous **XP+sp2** ou **Vista**

Paramètre	État
Pare-feu Windows : autoriser les exceptions de programmes locaux	Non configuré
Pare-feu Windows : définir les exceptions des programmes en entrée	Non configuré
Pare-feu Windows : protéger toutes les connexions réseau	Non configuré
Pare-feu Windows : n'autoriser aucune exception	Non configuré
Pare-feu Windows : autoriser l'exception de partage de fichiers entrants et d'impriman...	Non configuré
Pare-feu Windows : autoriser les exceptions ICMP	Non configuré
Pare-feu Windows : autoriser la journalisation	Non configuré
Pare-feu Windows : empêcher les notifications	Non configuré
Pare-feu Windows : autoriser les exceptions de ports locaux	Non configuré
Pare-feu Windows : définir les exceptions de ports entrants	Non configuré
Pare-feu Windows : autoriser l'exception d'administration à distance entrante	Non configuré
Pare-feu Windows : autoriser les exceptions du Bureau à distance en entrée	Non configuré
Pare-feu Windows : empêcher les réponses de monodiffusion pour des requêtes de m...	Non configuré
Pare-feu Windows : autoriser les exceptions d'infrastructure UPnP entrante	Non configuré

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

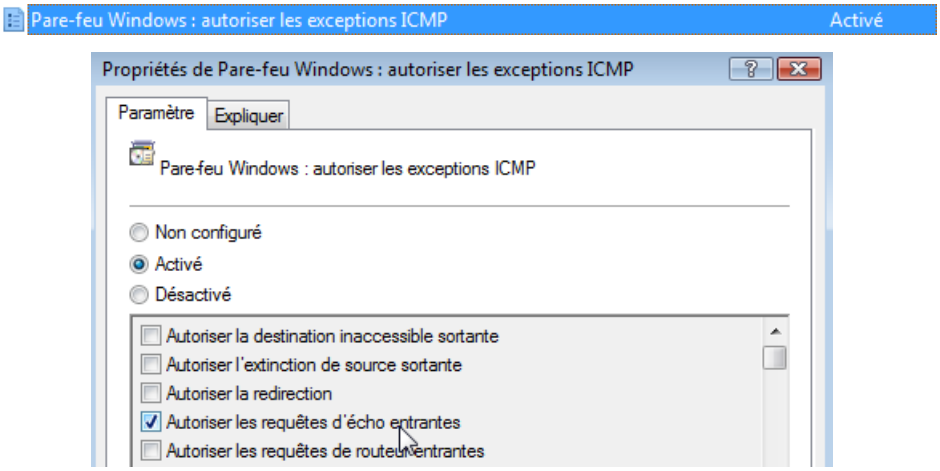
Il prend de manière générale deux listes, une définie par stratégies, et l'autre définie localement.

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

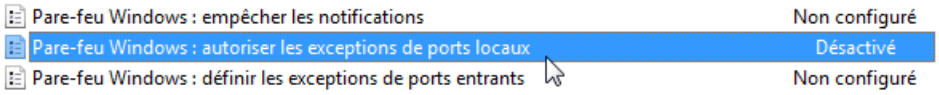


et du coup dans le pare-feu, on ne peut plus modifier la configuration…

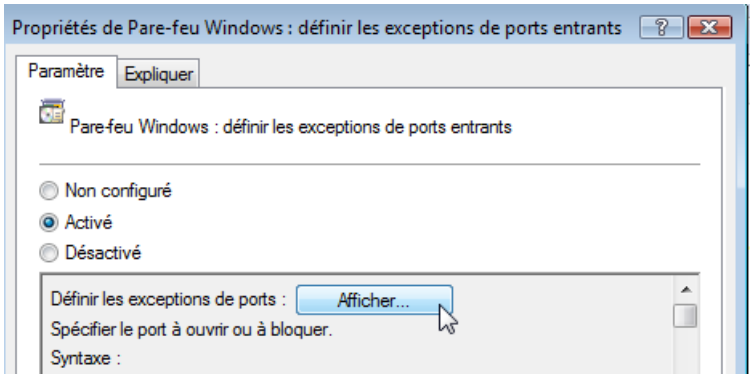
On peut autoriser ICMP juste avec réponse de ECHO



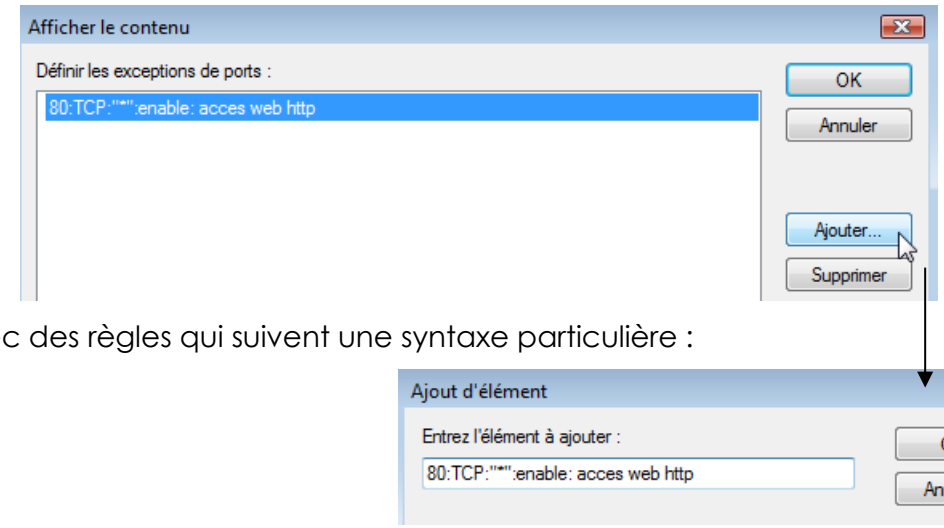
On peut définir un N° de port entrant :



ce qui amène :



Avec des règles qui suivent une syntaxe particulière :



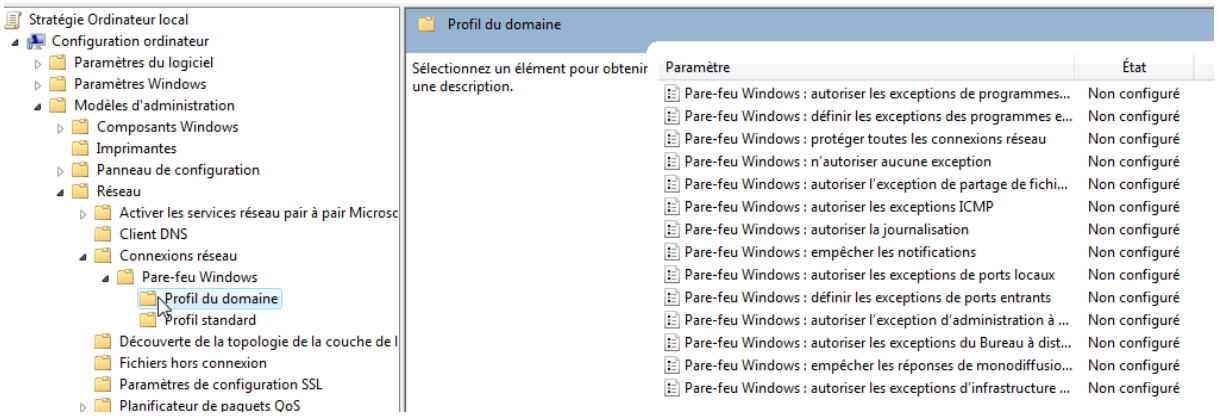
Avec des règles qui suivent une syntaxe particulière :

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…

```
C:\Users\Administrateur>netstat -ano

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       948
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       632
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       1096
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       1164
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       688
  TCP    0.0.0.0:49158          0.0.0.0:0              LISTENING       676
  TCP    127.0.0.1:668          0.0.0.0:0              LISTENING       1984
  TCP    127.0.0.1:668          127.0.0.1:49160        ESTABLISHED     1984
```

Liste des processus par PID :

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

le PID 1984…

c'est Carbonite !

```
C:\Users\Administrateur>tasklist

Nom de l'image                 PID Nom de la sessio Numéro de s Utilisation
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 Ko
System                           4 Services                   0      5 784 Ko
smss.exe                       448 Services                   0        560 Ko
csrss.exe                      580 Services                   0      3 848 Ko
wininit.exe                    632 Services                   0      3 348 Ko
csrss.exe                      644 Console                    1     12 100 Ko
services.exe                   676 Services                   0      6 008 Ko
lsass.exe                      688 Services                   0      1 756 Ko
lsm.exe                        696 Services                   0      3 356 Ko
winlogon.exe                   804 Console                    1      4 564 Ko
svchost.exe                    888 Services                   0      4 948 Ko
svchost.exe                    948 Services                   0      6 096 Ko
svchost.exe                    984 Services                   0     16 208 Ko
svchost.exe                   1096 Services                   0     10 184 Ko
mDNSResponder.exe             1956 Services                   0      3 824 Ko
CarboniteService.exe          1984 Services                   0     18 916 Ko
FrameworkService.exe          2036 Services                   0      5 128 Ko
Mcshield.exe                   492 Services                   0     25 936 Ko
```

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

```
C:\Users\Administrateur>tasklist /svc

Nom de l'image                 PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       448 N/A
csrss.exe                      580 N/A
wininit.exe                    632 N/A
csrss.exe                      644 N/A
services.exe                   676 N/A
lsass.exe                      688 ProtectedStorage, SamSs
lsm.exe                        696 N/A
winlogon.exe                   804 N/A
svchost.exe                    888 DcomLaunch, PlugPlay
svchost.exe                    948 RpcSs
svchost.exe                    984 WinDefend
```

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.

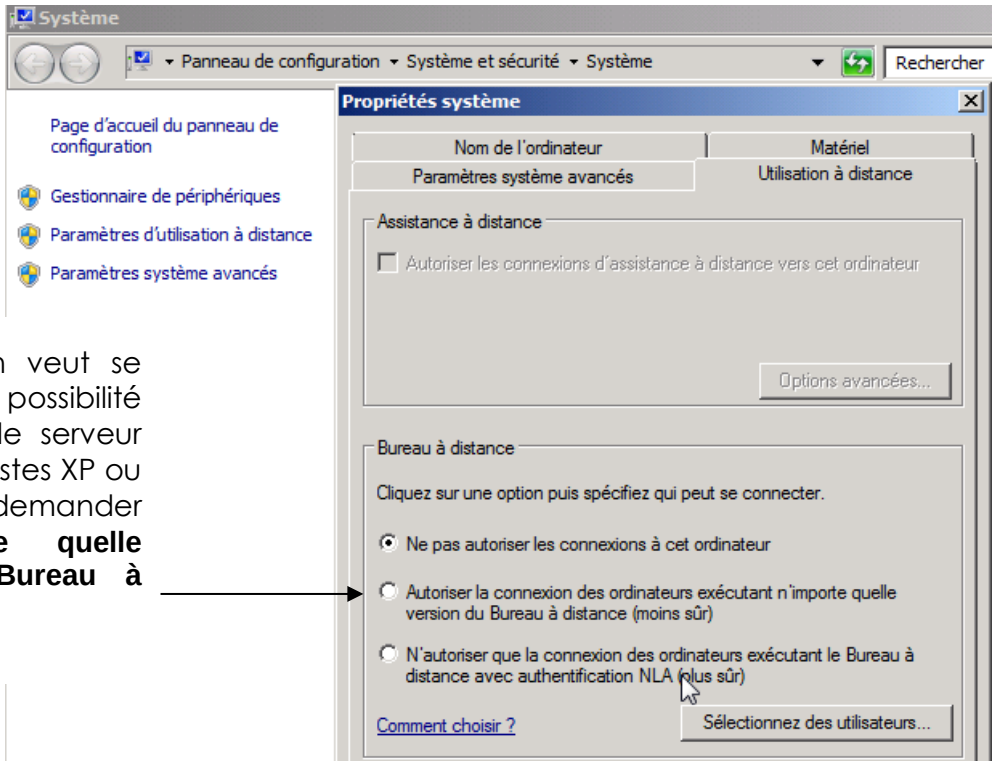
Ce protocole est celui utilisé pour configurer les services Terminal Server, services qui ont fait l'objet de plusieurs évolutions …

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**

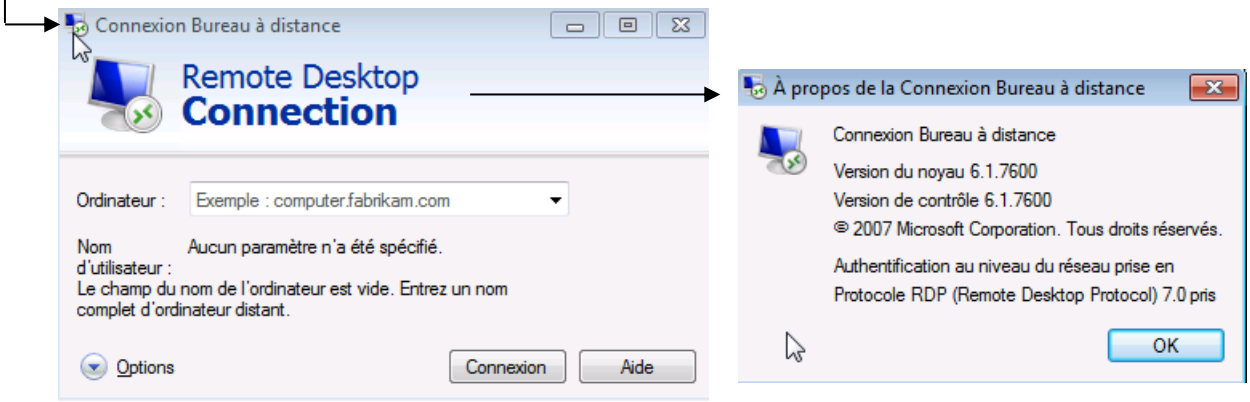


A priori si on veut se laisser la possibilité d'administrer le serveur depuis des postes XP ou Seven, il faut demander … **n'importe quelle version du Bureau à distance**…

Versions - options du Client Bureau à Distance

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

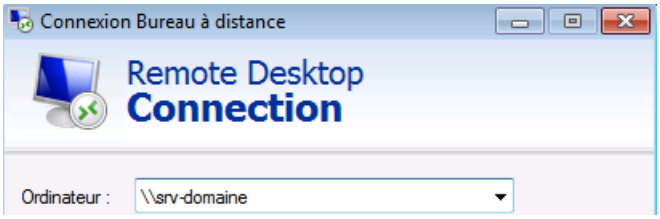
Pour connaître la version de RDP il suffit de demander "**A propos**" via le menu contextuel sur la boite de dialogue **Tous les programmes / Accessoires / Connexion Bureau à distance**



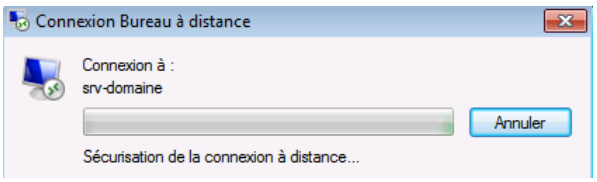
Il faut bien sur se connecter et s'identifier

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…).

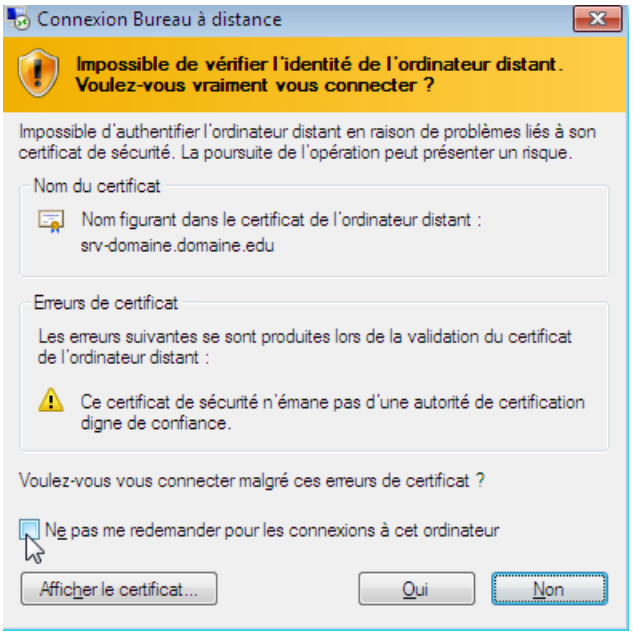


L'authentification est immédiate si on est dans le même domaine

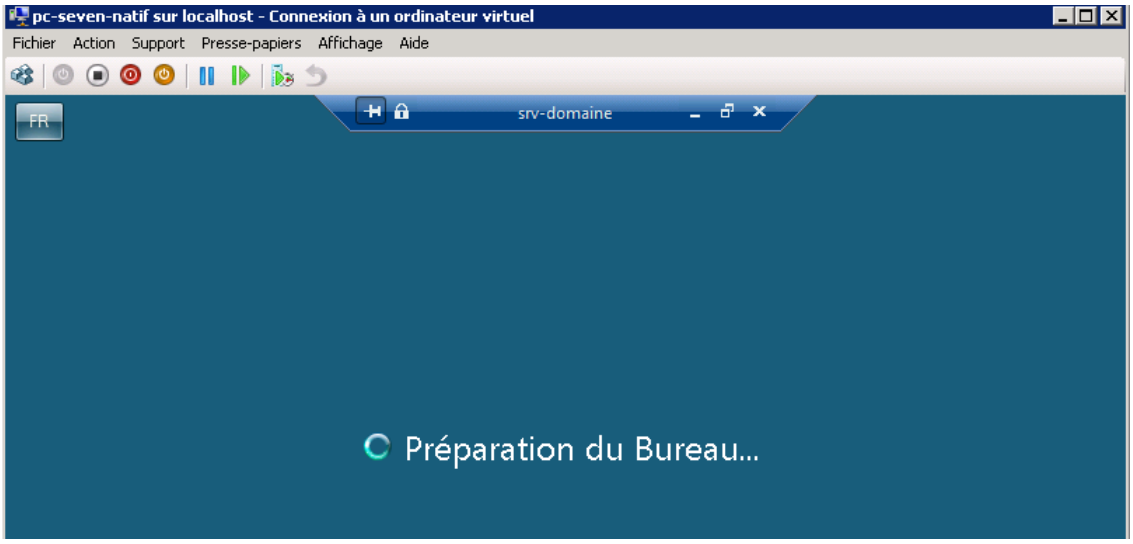


Mais elle peut demander une confirmation si on n'est pas dans le même domaine

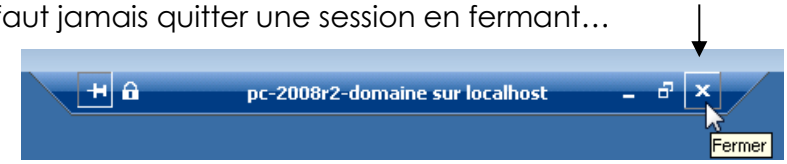
On peut éviter une re-confirmation pour la prochaine session



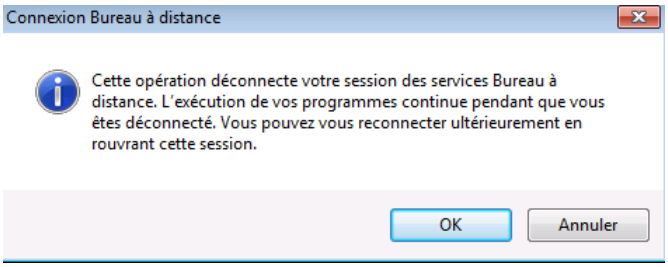
L'ouverture de session amène:



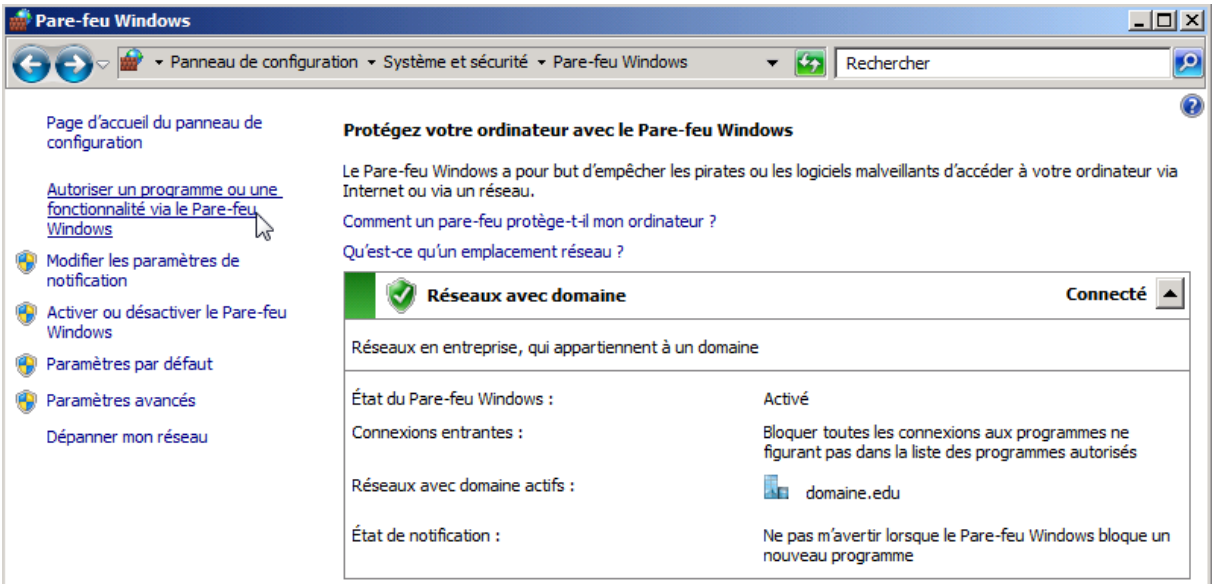
Il ne faut jamais quitter une session en fermant…

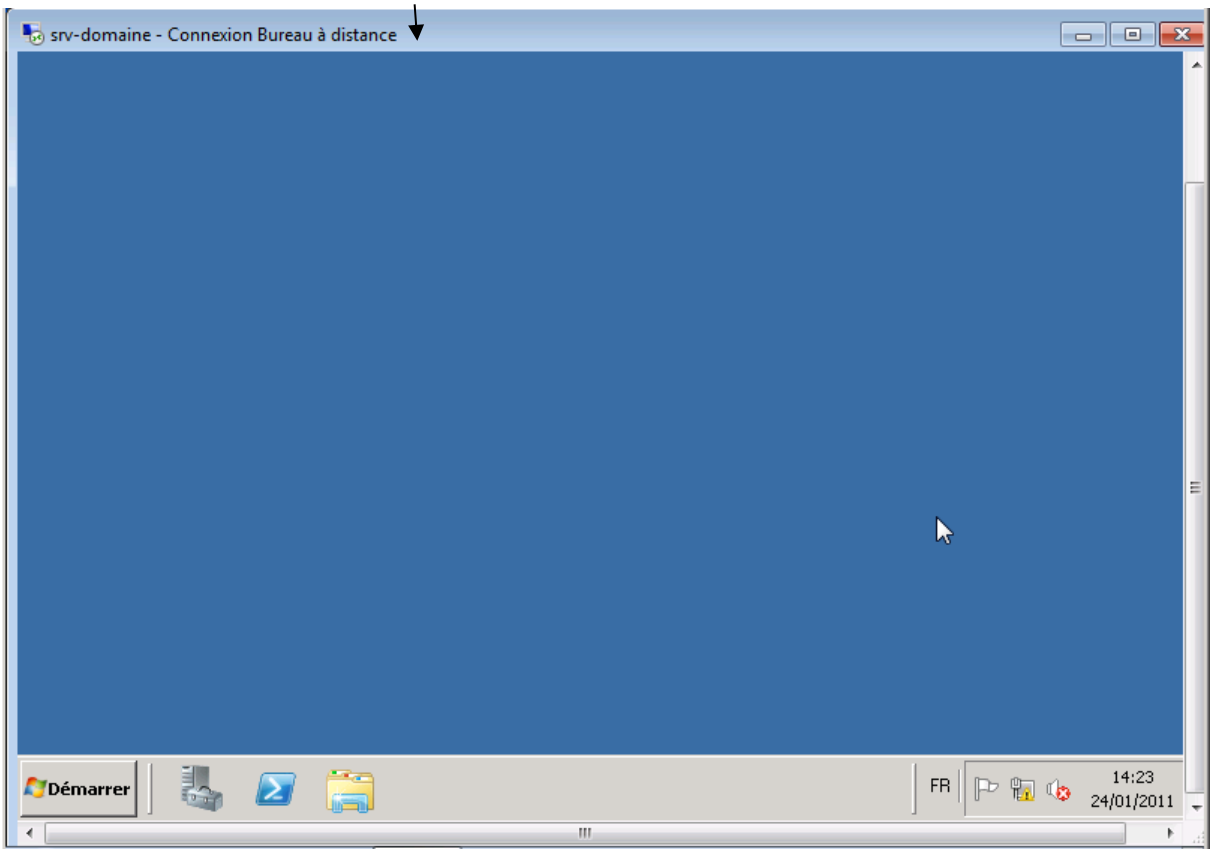


D'ailleurs Windows vous en informe … VOUS LAISSERIEZ VOTRE TRAVAIL EN COURS SUR LE SERVEUR



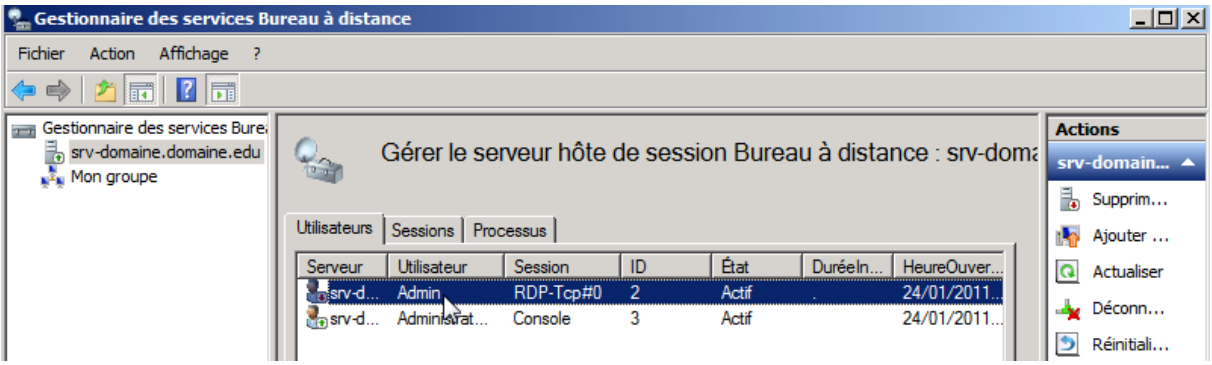
MAIS en fermant la session proprement sur le serveur…



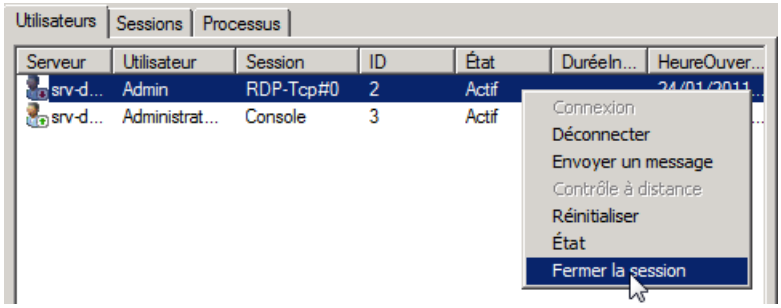


Encore plus si on demande plein écran…

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**

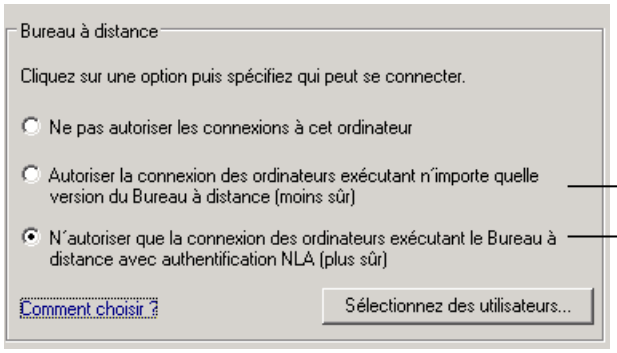


Un clic – droit sur la connexion **rdp** voulue permet de faire l'essentiel…



Utiliser le Bureau à Distance depuis un client:

Selon l'option, la connexion sera possible depuis

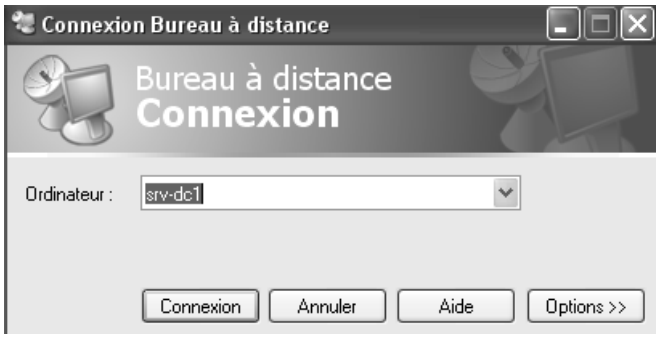


- Tout poste windows avec un client RDP
- Uniquement des postes ayant un client RDP version 7.0 (Seven mini…)

Depuis un poste XP, on demande

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

Cela amène une fenêtre

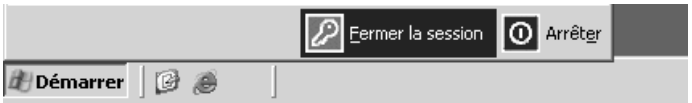


puis **Connexion**

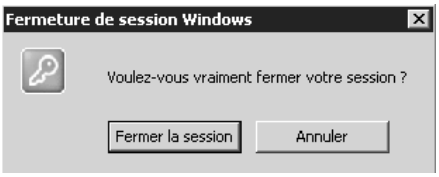
On peut rentrer un nom, ou une adresse ip

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

Soit quelque chose du genre : Démarrer / Fermer la session



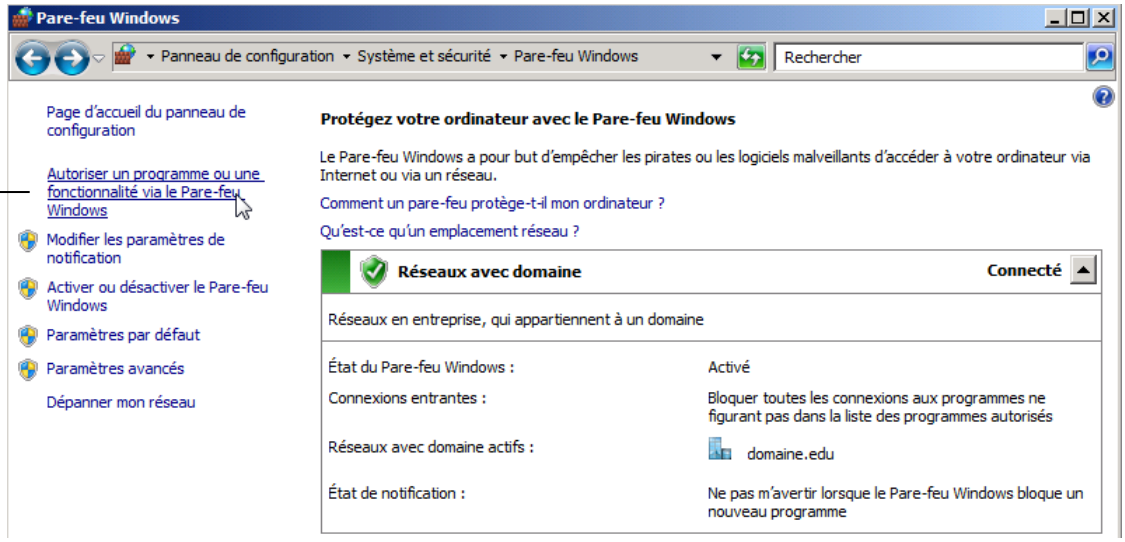
puis



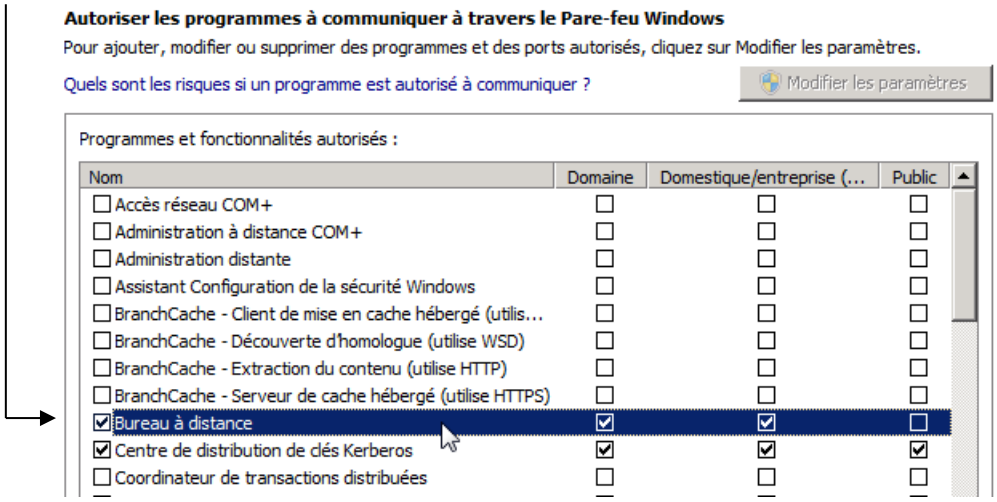
SURTOUT PAS DE DECONNEXION, (en fermant la fenêtre par la croix en haut à droite) VOUS LAISSERIEZ VOTRE TRAVAIL EN COURS SUR LE SERVEUR

Pare-Feu et N° Port par défaut

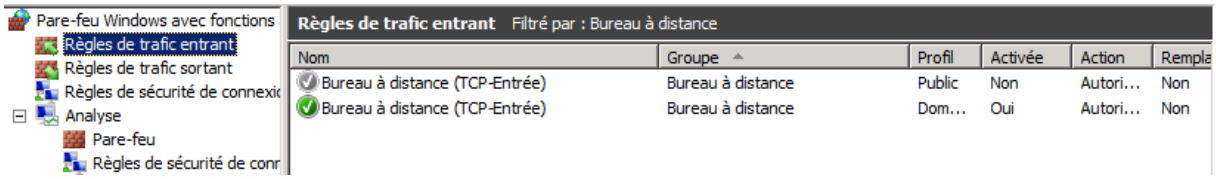
Si on laisse Windows activer les réglages pour passer le pare-feu incorporé de Windows Server (ici 2008R2),



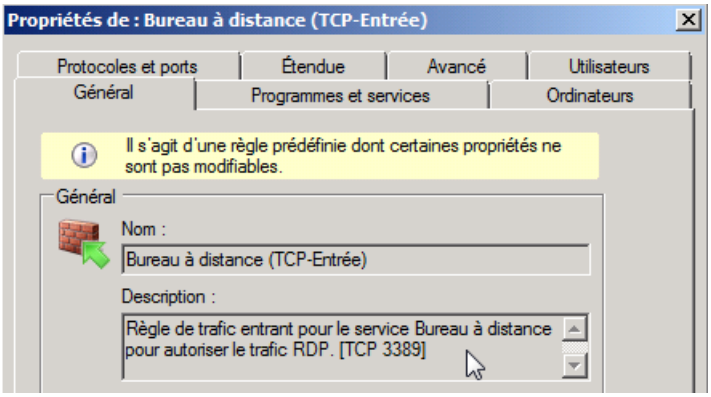
Alors on observe



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

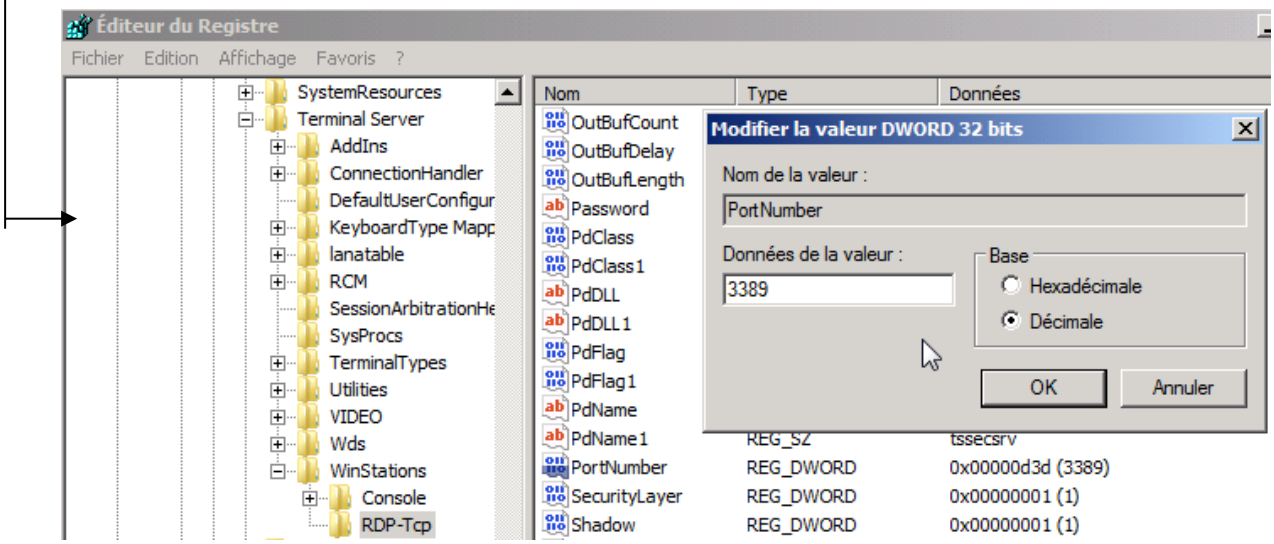


On voit que le port TCP-3389 est concerné



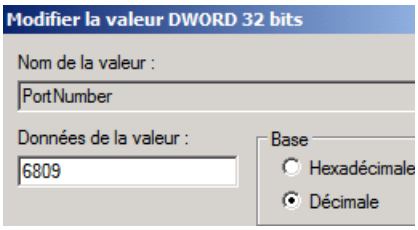
Port TCP du Bureau à Distance (modification)

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**

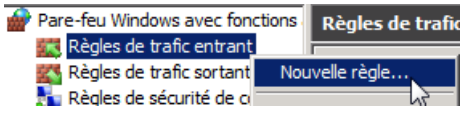


et on peut spécifier un autre N° de port pour accéder au bureau à distance qui écouterais sur un n° de port non configuré par défaut

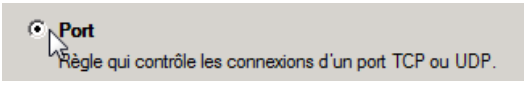
dans l'exemple ici ***6809***

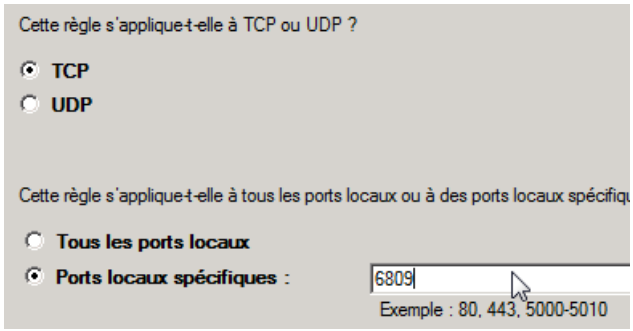


Il faut créer une règle spécifique ***RDP perso*** dans le Pare-feu …

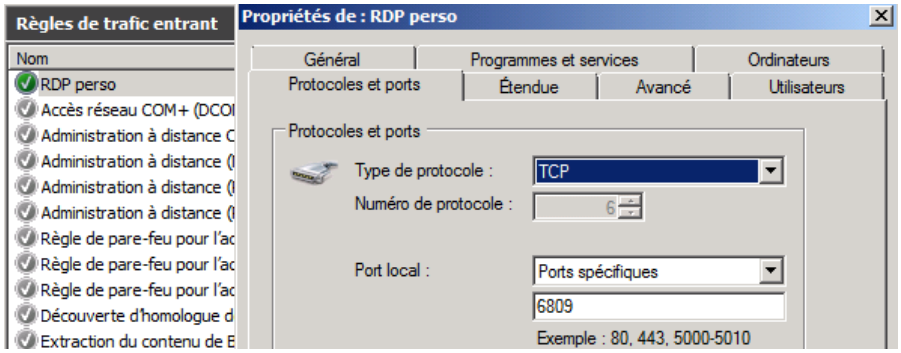


type Port

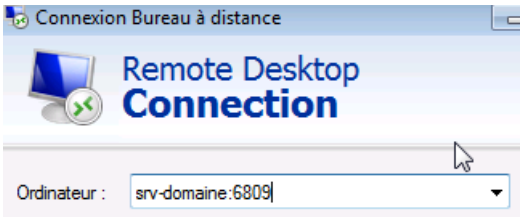


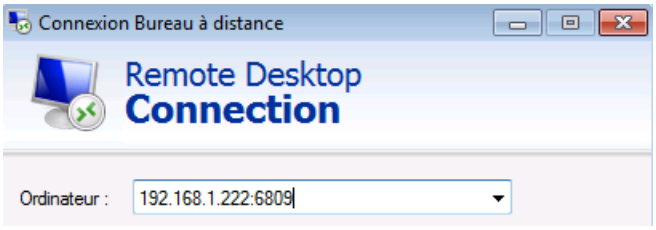


donnant

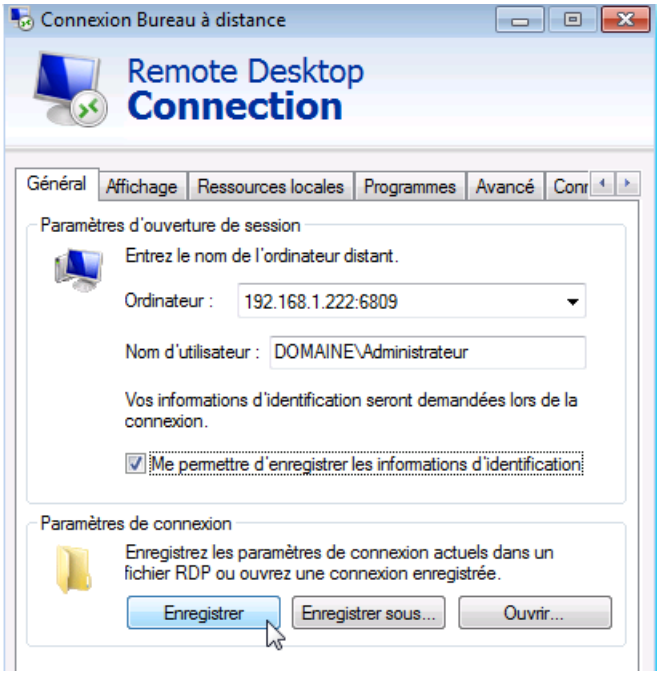


Pour y accéder depuis un client, en ajoutant : 'deux-points' comme dans



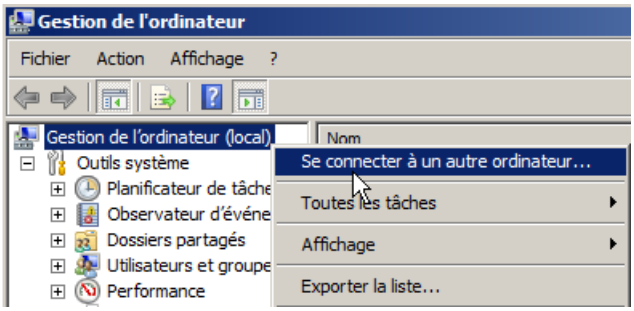


Configuration que l'on peut enregistrer…

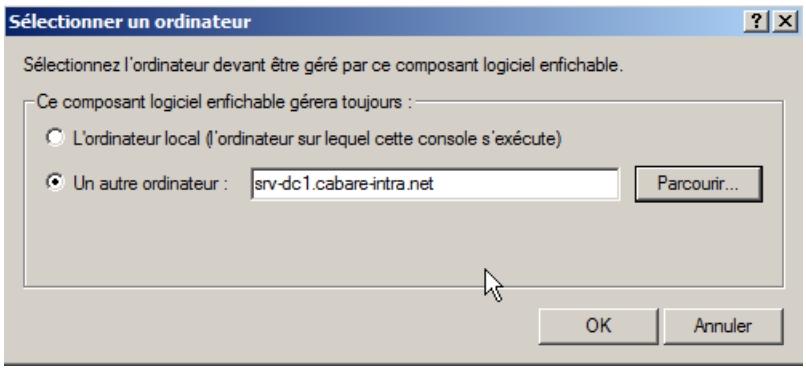


Gestion de l'ordinateur:

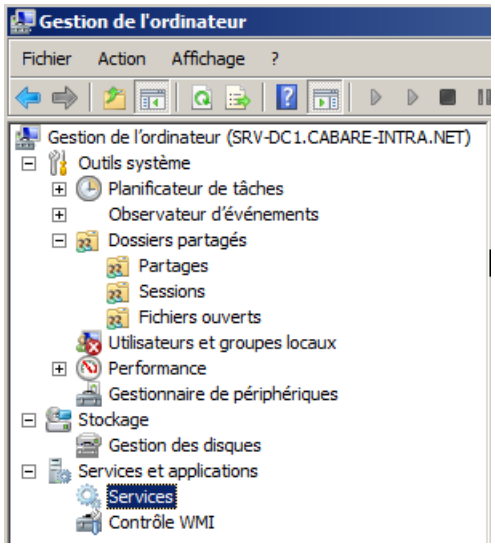
Dans pratiquement toutes les mmc par défaut on travaille sur l'ordinateur local, mais on peut demander de se connecter à un autre ordinateur…



Et choisir une machine sur laquelle on ait des droits…



Et voilà…

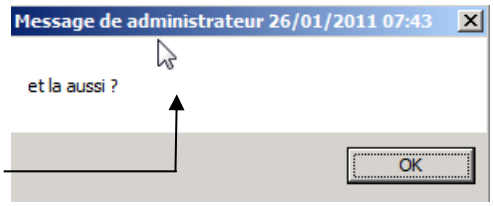


MSG – (NETSEND)

MSG n'est pas NetSend:

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

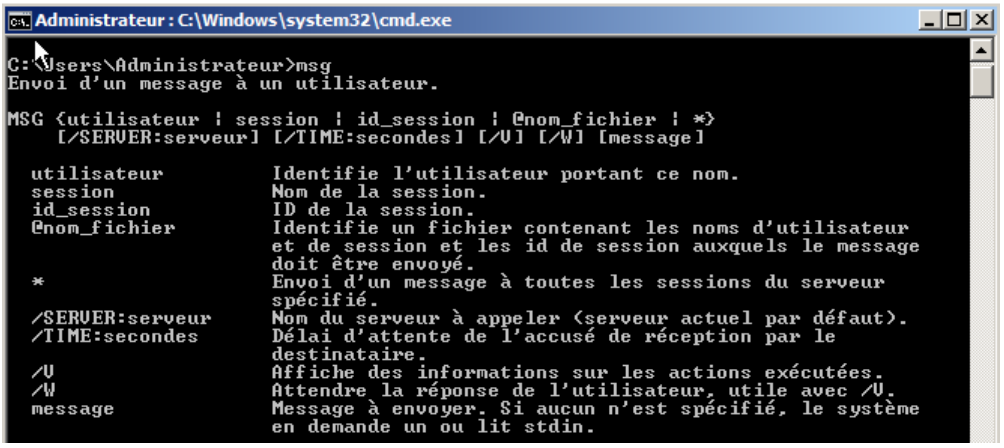
MSG peut être utilisé à des fins un peu similaires, MSG est utilisé de base pour envoyer un message à des clients Terminal Server… et pourra être utilisé pour envoyer un message sur une machine distante.



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"

```
C:\Users\Administrateur>msg /server:travail administrateur "test"
```

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

```
C:\Users\Administrateur>msg /server:travail 1 "test"
```

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

```
C:\Users\Administrateur>msg /server:travail * "test"
```

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

```
C:\Users\Administrateur>msg /server:poste-seven admin "test"
Erreur 5 lors de l'obtention des noms de session
```

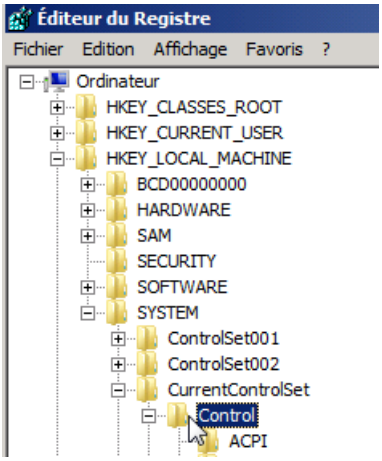
Erreur 5 – ou ***1722*** signifie problèmes de droits d'accès…

MSG hors TSE dans domaine:

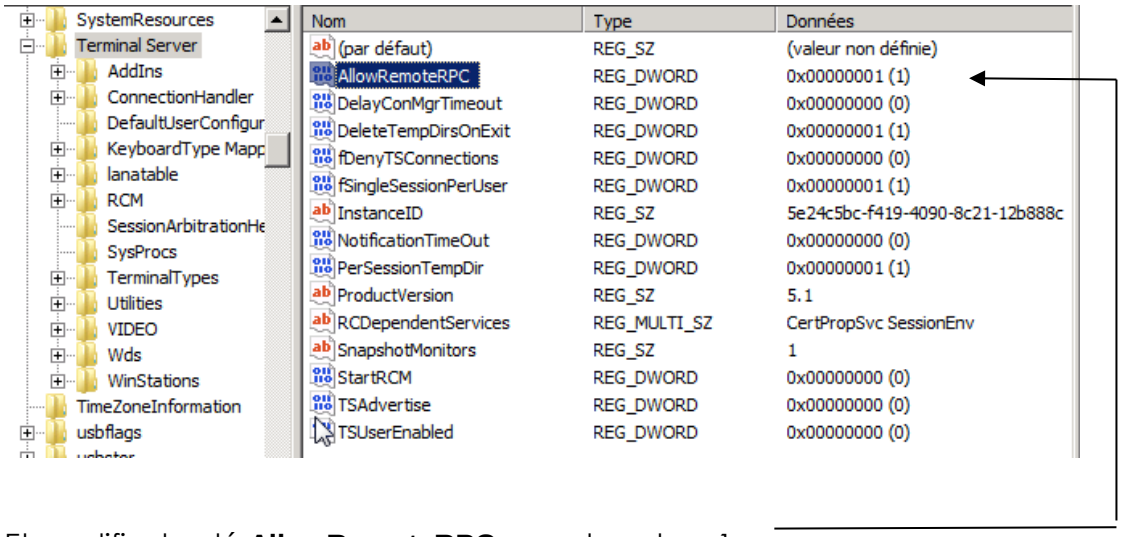
Il faut autoriser le Bureau à distance de la machine visée !

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…)

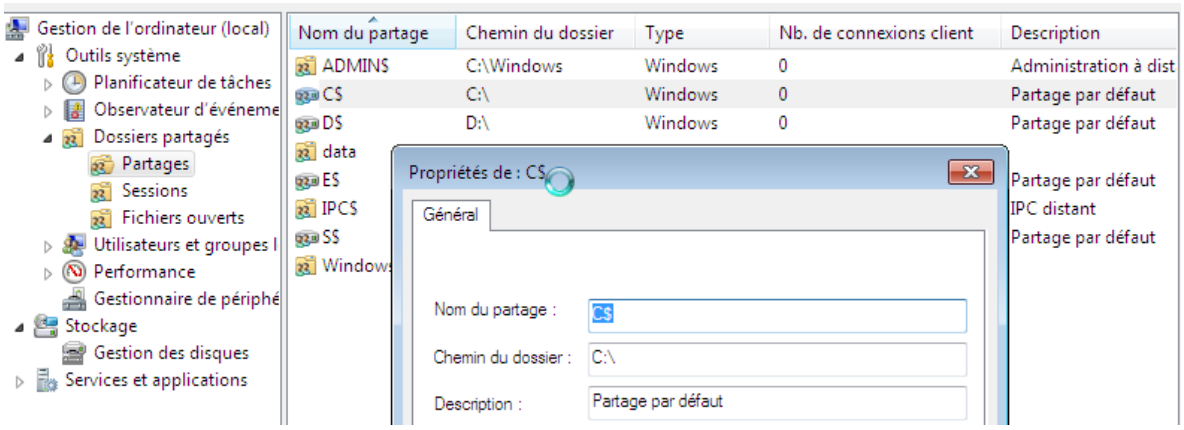
N.B: penser à exécuter la commande MSG avec des pouvoirs élevés, en cas de présence d'UAC…

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.

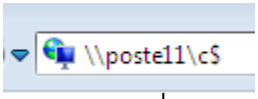


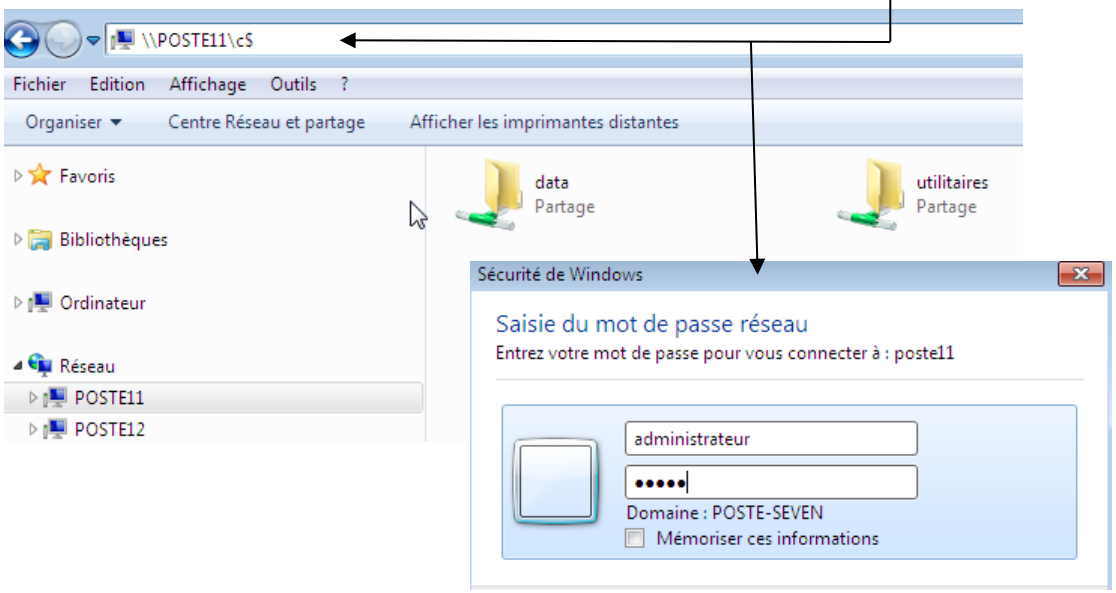
Pour les utiliser depuis un autre poste, il faut connaître

Le nom du poste ***poste11***

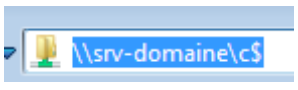
Le nom du partage administratif **c$**

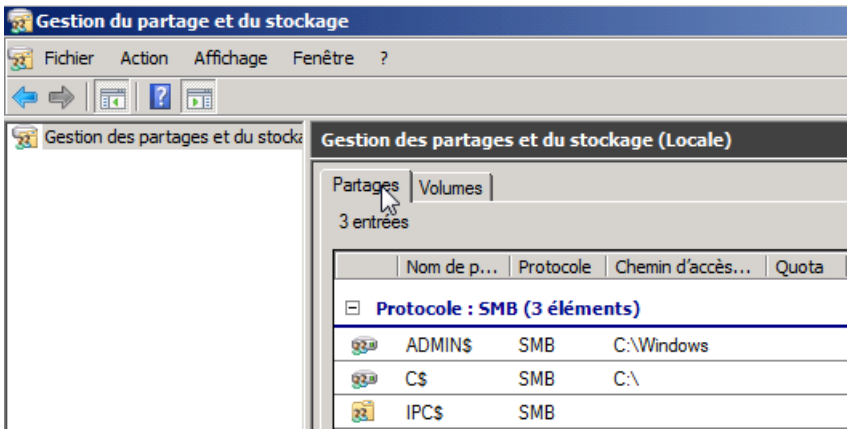
Et le login de l'administrateur intégré du poste visé…





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

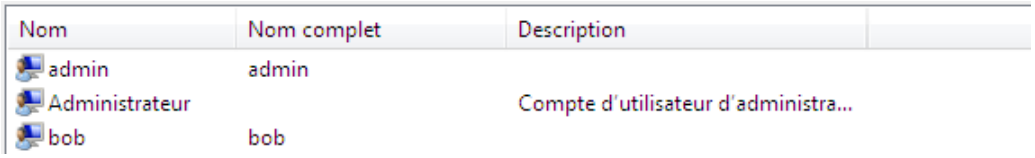




Effet de l'UAC:

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.

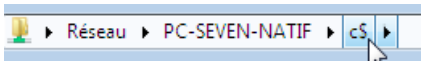
Sur le poste « cible »

- 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***

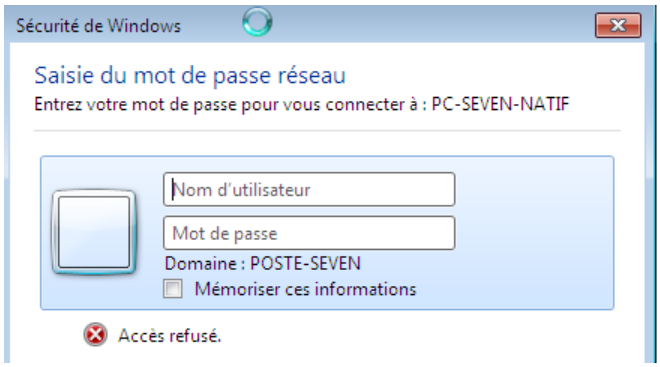
On accède au partage administratif du poste cible "pc-seven-natif" naturellement, car l'UAC ne s'applique pas au compte administrateur intégré et les comptes sont homonymes



Exemple 2: **administrateur local**

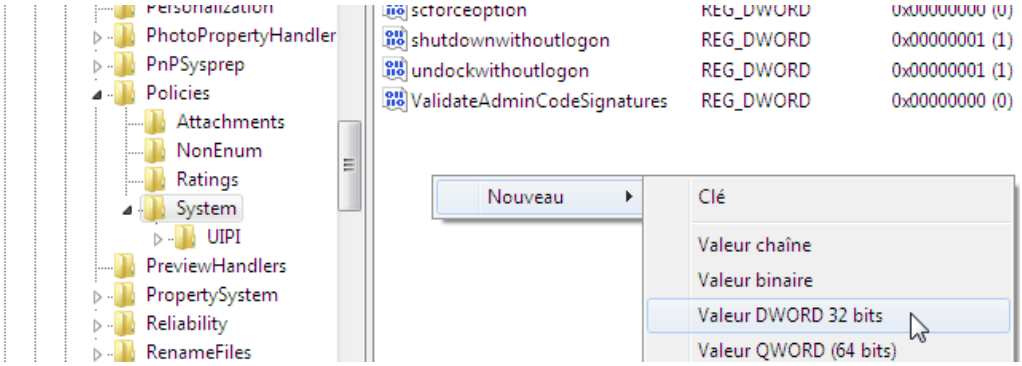
On se logue sur le poste « de départ » en tant qu'administrateur local… ***Admin/localdep***

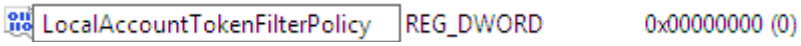
On n'accède pas au partage administratif du poste cible "pc-seven-natif" car l'UAC s'applique



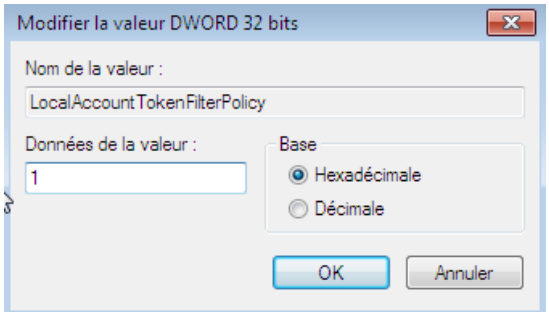
Si on veut un fonctionnement identique à celui de XP (PRO) et précédents, il faut modifier la BDR de la machine "cible" sous Windows en ajoutant l'entrée de type **REG_DWORD** valant **LocalAccountTokenFilterPolicy** = 1 dans la clef

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



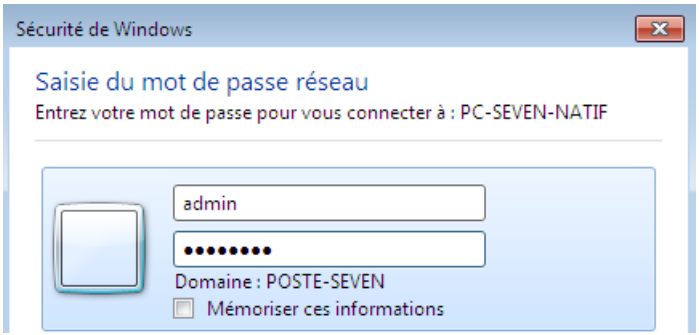


Et on lui donne la valeur 1… (et on re-démarre le poste)



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"…

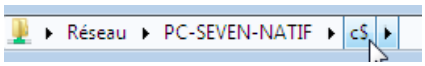
Et **admin/localcib** passe…



Exemple 3: **utilisateur avec pouvoir local**

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

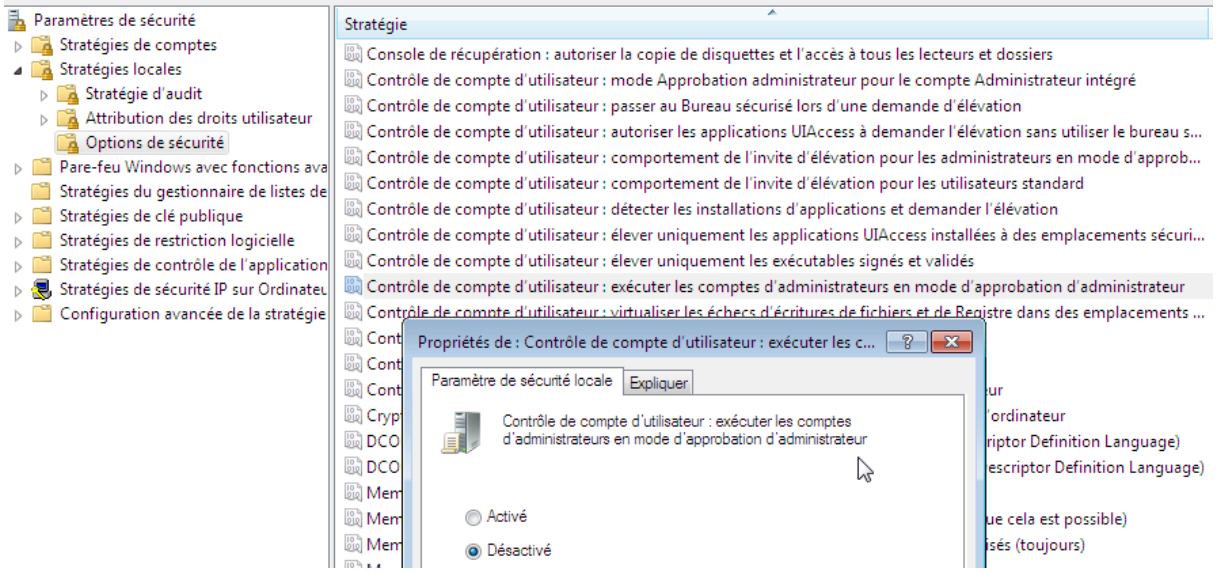
On accède au partage administratif du poste cible "pc-seven-natif" naturellement, car l'UAC à été désactivé via la modification de la base de registre, et les comptes sont homonymes…



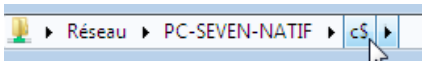
Exemple 4: **utilisateur avec pouvoir local – poste cible sans UAC**

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 A DISTANCE

Sc en ligne de commande :

```
C:\Windows\system32>sc /?

ERREUR : commande non reconnue

DESCRIPTION :
        SC est un utilitaire en ligne de commande utilisé pour
        communiquer avec le Gestionnaire de contrôle des services et les
        services.
SYNTAXE :
        sc <serveur> [commande] [nom service] <option1> <option2>...
```

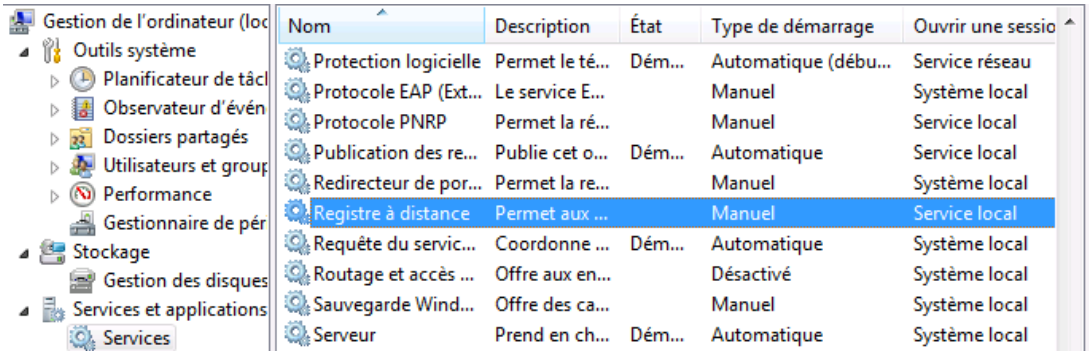
avec

Commande	Fonction
sc config	Configure le démarrage du service et les comptes d'utilisateur
sc continue	Réactive un service en pause
sc enumdepend	Liste les services dépendants
sc failure	Spécifie l'action à effectuer en cas d'échec d'exécution du service
sc pause	Met un service en pause
sc qc	Affiche la configuration d'un service en particulier
sc query	Affiche des informations sur le service, pilote, type de service ou type de pilote spécifié
sc start	Démarre un service
sc stop	Envoie une requête STOP à un service (il risque de ne pas répondre)

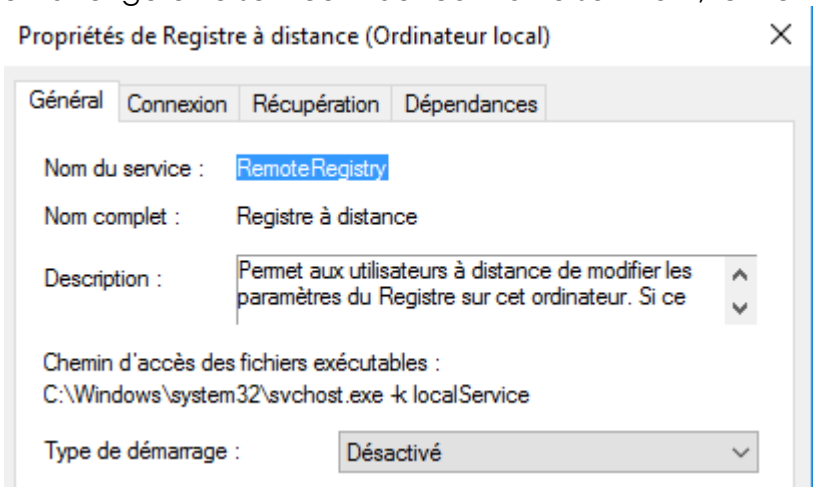
Nom d'un service

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

```
sc query type= service | more
```

Ou pour lister tous les services

```
sc query type= service state= all | more
```

On trouvera

```
SERVICE_NAME: RemoteRegistry
DISPLAY_NAME: Registre à distance
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

Etat d' un service sc query

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

```
C:\Windows\system32>sc start "registre à distance"
[SC] StartService: OpenService échec(s) 1060 :

Le service spécifié n'existe pas en tant que service installé.
```

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

```
C:\Windows\system32>sc start "remoteregistry"
[SC] StartService échec(s) 1058 :

Le service ne peut pas être démarré parce qu'il est désactivé
```

On voit qu'il est stoppé

sc query "Name of Service"

```
C:\Windows\system32>sc query remoteregistry

SERVICE_NAME: remoteregistry
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

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

sc config "Name of Service" start=

```
C:\Windows\system32>sc config remoteregistry start= demand
[SC] ChangeServiceConfig réussite(s)
```

Démarrer arrêter un service local sc start stop

On va pouvoir le démarrer avec la commande

sc start "Name of Service"

```
C:\Windows\system32>sc start "remoteregistry"

SERVICE_NAME: remoteregistry
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 2  START_PENDING
                                (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 376
        FLAGS              :
```

Et si tout va bien on vérifie

```
C:\Windows\system32>sc query remoteregistry

SERVICE_NAME: remoteregistry
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 4  RUNNING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

On va pouvoir le stopper avec la commande

sc stop "Name of Service"

```
C:\Windows\system32>sc stop "remoteregistry"

SERVICE_NAME: remoteregistry
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 3  STOP_PENDING
                                (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 1066  (0x42a)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x3
        WAIT_HINT          : 0xbb8
```

Et si tout va bien on vérifie

```
C:\Windows\system32>sc query remoteregistry

SERVICE_NAME: remoteregistry
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

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 query "Name of Service"

Comme dans

sc start "Name of Service"

```
C:\Windows\system32>sc \\port-p9 query remoteregistry

SERVICE_NAME: remoteregistry
        TYPE               : 20  WIN32_SHARE_PROCESS
        STATE              : 1  STOPPED
        WIN32_EXIT_CODE    : 1077  (0x435)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

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

sc stop "Name of Service"

```
C:\Windows\system32>sc query \\port-p9 remoteregistry
[SC] EnumQueryServicesStatus:OpenService échec(s) 123 :

La syntaxe du nom de fichier, de répertoire ou de volume est incorrecte.


C:\Windows\system32>sc \\port-p9 query remoteregistry
[SC] EnumQueryServicesStatus:OpenService échec(s) 5 :

Accès refusé.
```

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

Option de démarrage

```
C:\Windows\system32>sc \\port-p9 config remoteregistry start= demand
[SC] ChangeServiceConfig réussite(s)
```

démarrage

```
C:\Windows\system32>sc \\port-p9 start "remoteregistry"

SERVICE_NAME: remoteregistry
        TYPE               : 30  WIN32
        STATE              : 2  START_PENDING
                               (NOT_STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x7d0
        PID                : 9204
        FLAGS              :
```

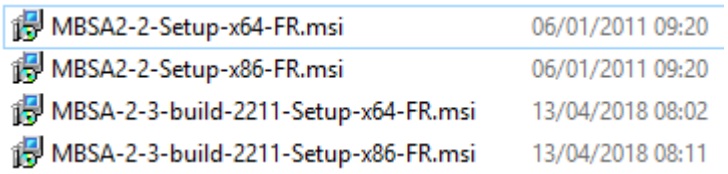
Vérification

```
C:\Windows\system32>sc \\port-p9 query remoteregistry

SERVICE_NAME: remoteregistry
        TYPE               : 30  WIN32
        STATE              : 4  RUNNING
                               (STOPPABLE, NOT_PAUSABLE, IGNORES_SHUTDOWN)
        WIN32_EXIT_CODE    : 0  (0x0)
        SERVICE_EXIT_CODE  : 0  (0x0)
        CHECKPOINT         : 0x0
        WAIT_HINT          : 0x0
```

MBSA POSTE DISTANT

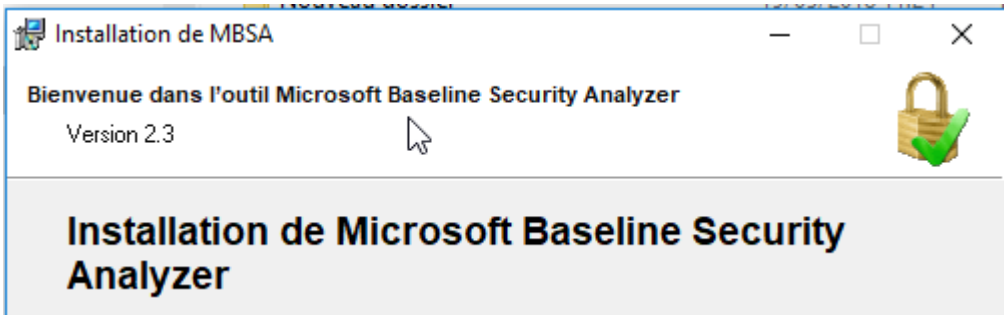
MBSA 2.3 : pas de successeur à venir :

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 »…

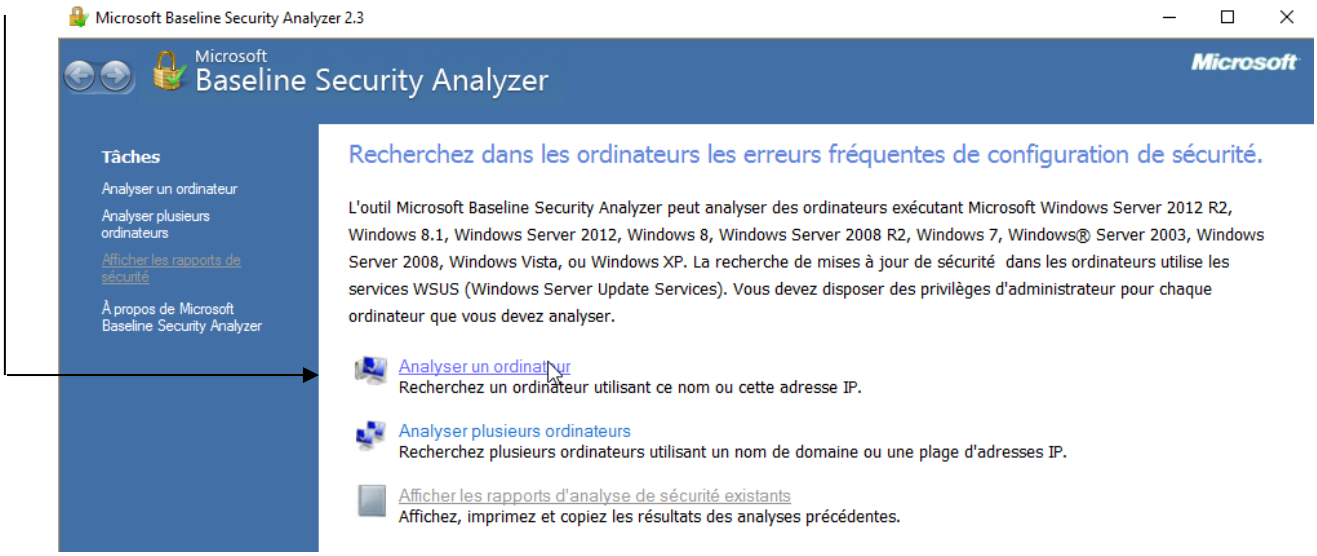
On l'installe simplement



Lancement MBSA 2.3 en local:

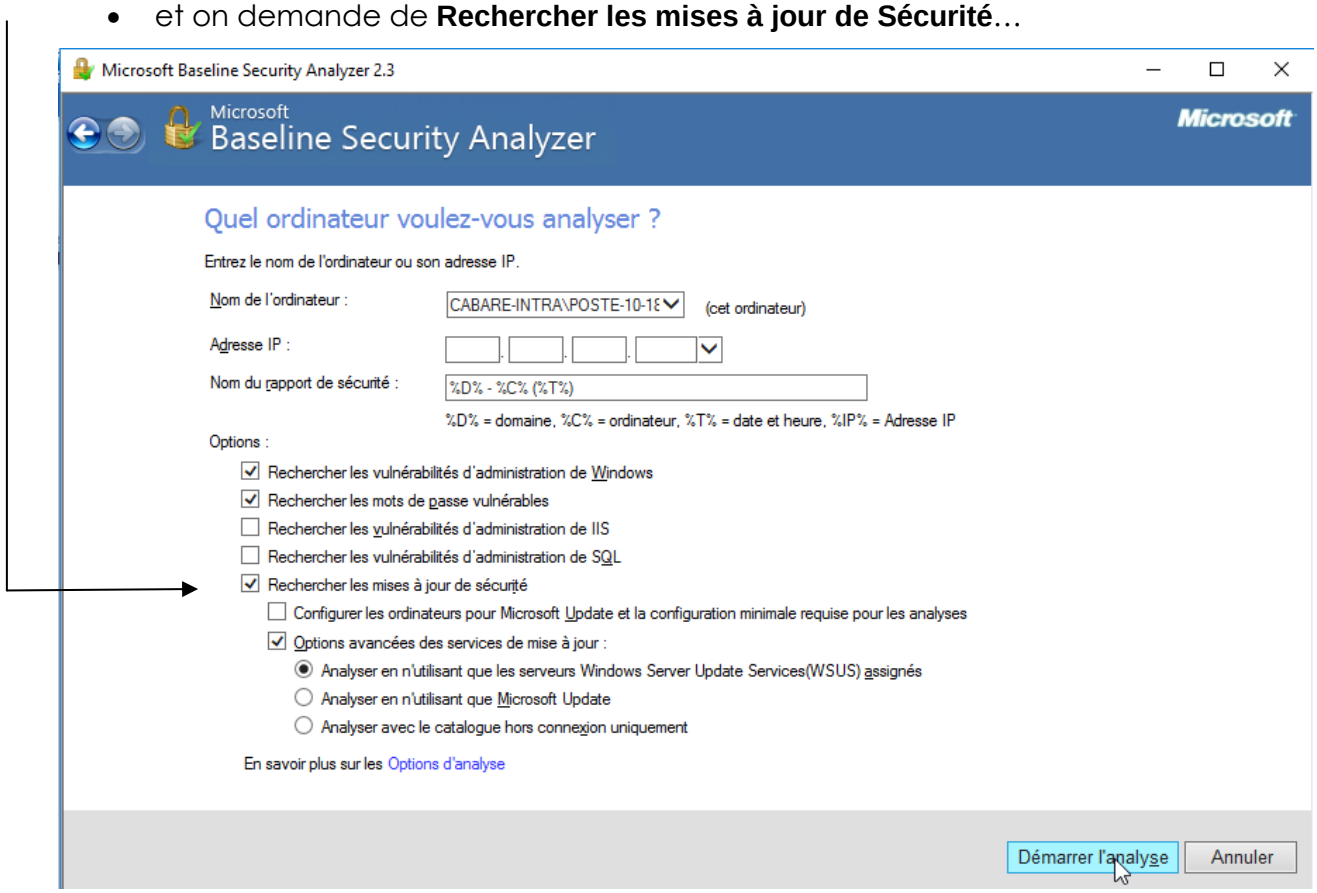
on lance le raccourci

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

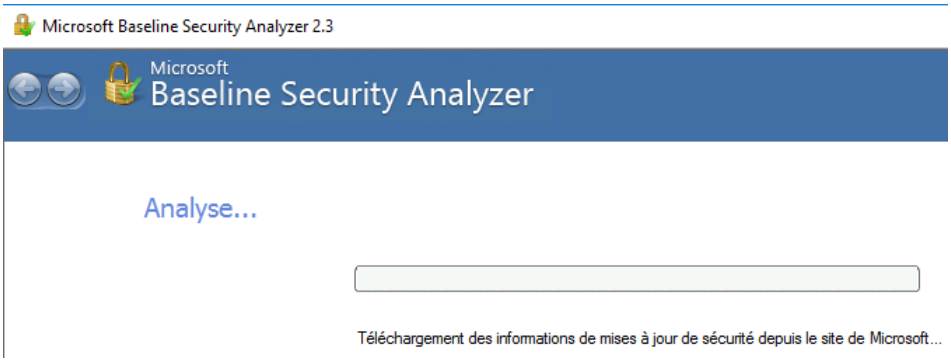


Peu de réglages sont indispensables à ce niveau,

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

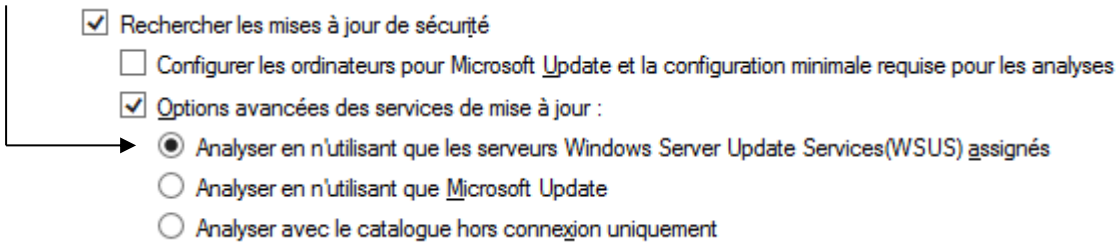


Après téléchargement (cela peut être long) d'une base de signature depuis le site de microsoft, (elle est toujours chargée)



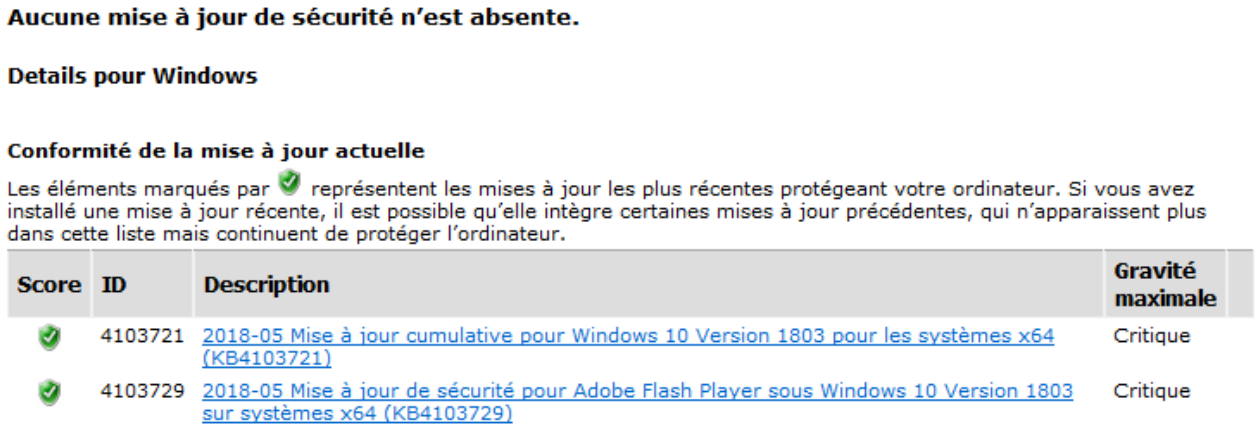
Analyse depuis WSUS

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



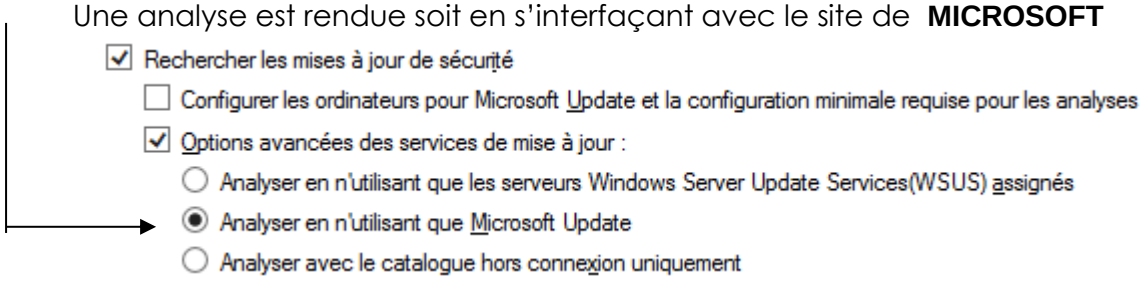
Donnant par exemple

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

Détails du rapport pour CABARE-INTRA - POSTE-10-1803 (2018-06-03 18:42:15)

Évaluation de la sécurité :
Risque important (Un ou plusieurs tests critiques ont échoué.)

Nom de l'ordinateur :	CABARE-INTRA\POSTE-10-1803
Adresse IP :	192.168.1.210
Nom du rapport de sécurité :	CABARE-INTRA - POSTE-10-1803 (03-06-2018 18-42)
Date d'analyse :	03/06/2018 18:42
Analysé avec MBSA version :	2.3.2211.0
Date de synchronisation du catalogue :	2018-05-14T20:12:48Z
Catalogue des mises à jour de sécurité :	Microsoft Update (hors ligne)

Ordre de tri : Score (le pire en premier)

Résultats de l'analyse des mises à jour de sécurité

Score	Catégorie	Résultat
	Office - Mises à jour de sécurité	19 mises à jour de sécurité sont absentes. 1 Service Packs ou correctifs cumulatifs sont absents. Afficher les ressources analysées Détails du résultat Comment corriger le problème
	Windows - Mises à jour de sécurité	1 Service Packs ou correctifs cumulatifs sont absents. Afficher les ressources analysées Détails du résultat Comment corriger le problème
	SQL Server - Mises à jour de sécurité	Aucune mise à jour de sécurité n'est absente. Afficher les ressources analysées Détails

Résultats de l'analyse de Windows

Vulnérabilités d'administration

Score	Catégorie	Résultat
	Expiration des mots de passe	Certains comptes d'utilisateurs (2 sur 5) ont un mot de passe n'expirant pas. Afficher les ressources analysées Détails du résultat Comment corriger le problème

Microsoft Baseline Security Analyzer

19 mises à jour de sécurité sont absentes. 1 Service Packs ou correctifs cumulatifs sont absents.

Details pour Office

Mises à jour de sécurité

Les éléments marqués par sont confirmés comme manquants. Les éléments marqués d'un sont confirmés comme manquants et n'ont pas été approuvés par l'administrateur système.

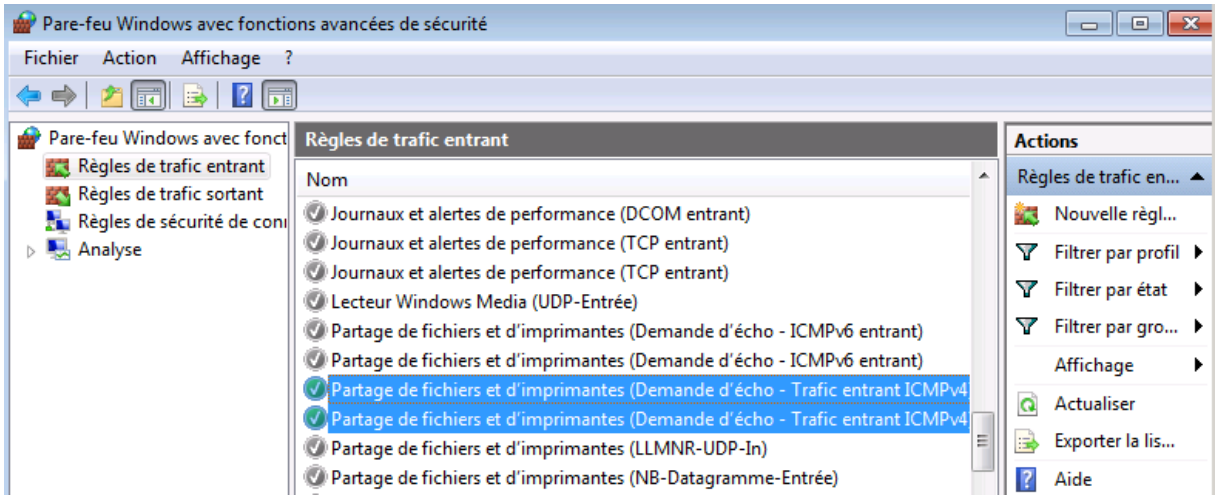
Score	ID	Description	Gravité maximale
	MS13-023	Mise à jour de sécurité pour Microsoft Filter Pack 2.0 (KB2553501) Édition 64 bits	Critique
	MS13-023	Mise à jour de sécurité pour Microsoft Visio Viewer 2010 (KB2687505) Édition 64 bits	Critique
	MS11-072	Mise à jour de sécurité pour Microsoft Excel 2010 (KB2553070), Édition 64 bits	Important
	MS13-074	Mise à jour de sécurité pour Microsoft Office 2010 (KB2687423) Édition 64 bits	Important
	MS11-089	Mise à jour de sécurité pour Microsoft Office 2010 (KB2589320) Édition 64 bits	Important

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

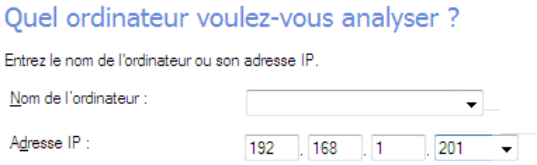
Partage de Fichier et d'imprimantes (Demande d'écho – Traffic entrant ICMPv4)



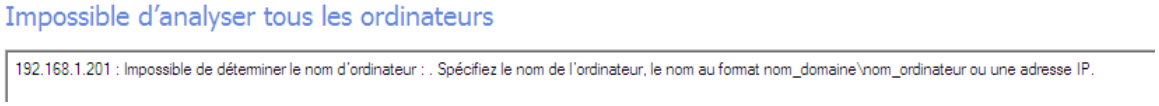
Imaginons que nous souhaitions lancer MBSA sur le poste 192.168.1.201

```
C:\Users\Administrateur>ping 192.168.1.201

Envoi d'une requête 'Ping'  192.168.1.201 avec 32 octets de données :
Réponse de 192.168.1.201 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.201 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.201 : octets=32 temps<1ms TTL=128
Réponse de 192.168.1.201 : octets=32 temps<1ms TTL=128

Statistiques Ping pour 192.168.1.201:
    Paquets : envoyés = 4, reçus = 4, perdus = 0 (perte 0%),
Durée approximative des boucles en millisecondes :
    Minimum = 0ms, Maximum = 0ms, Moyenne = 0ms
```

Si on lance l'analyse telle que



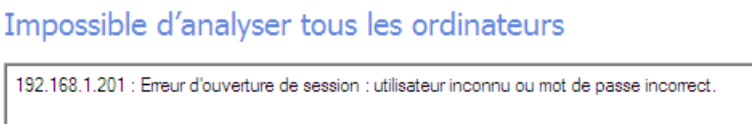
On obtiendra probablement si son pare-feu est actif…



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

Comptes Utilisateurs:

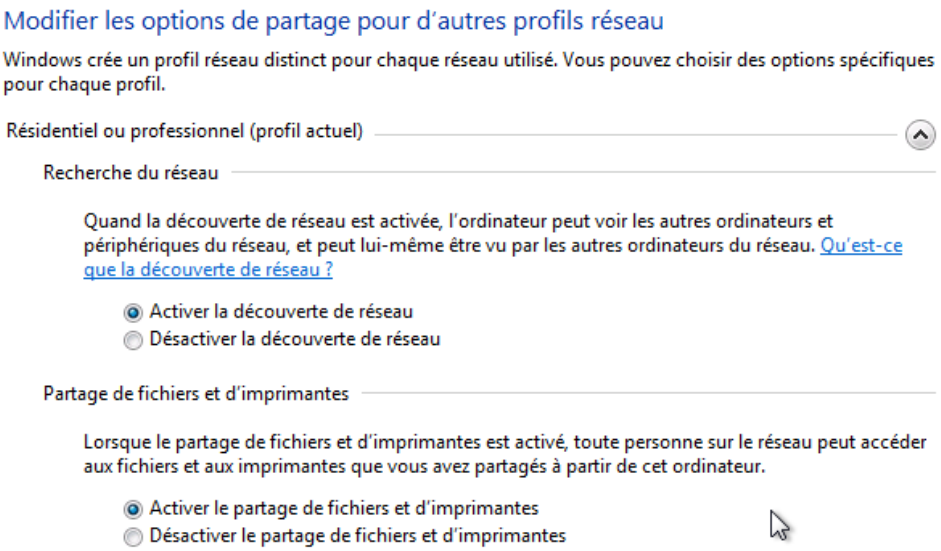
On obtient si le pare-feu est inactif…(ou les ports ouverts correctement)



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…

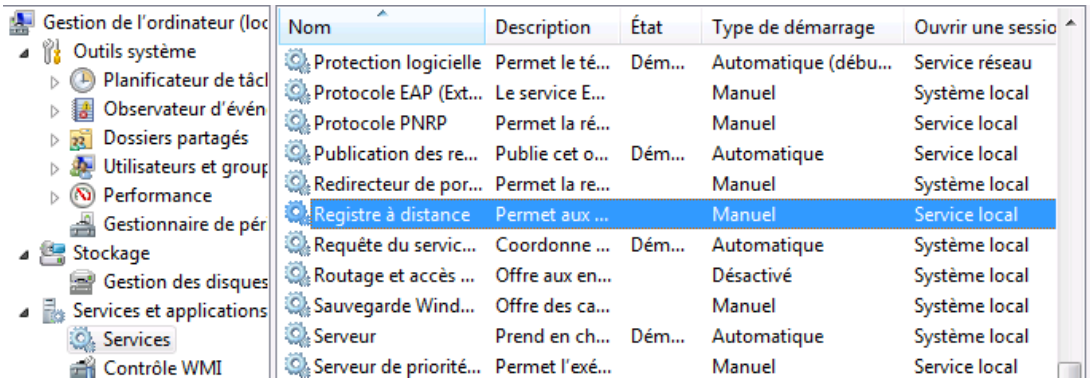
Services et paramétrages:

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



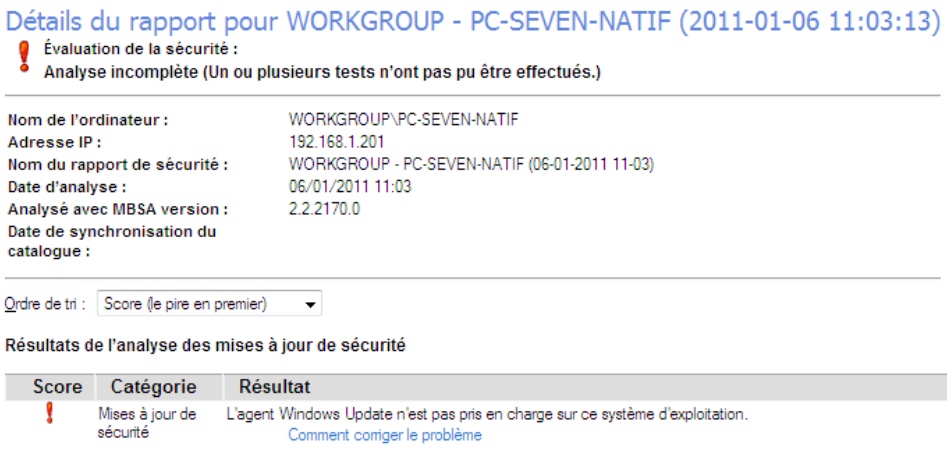
Les services suivants sont nécessaires :

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

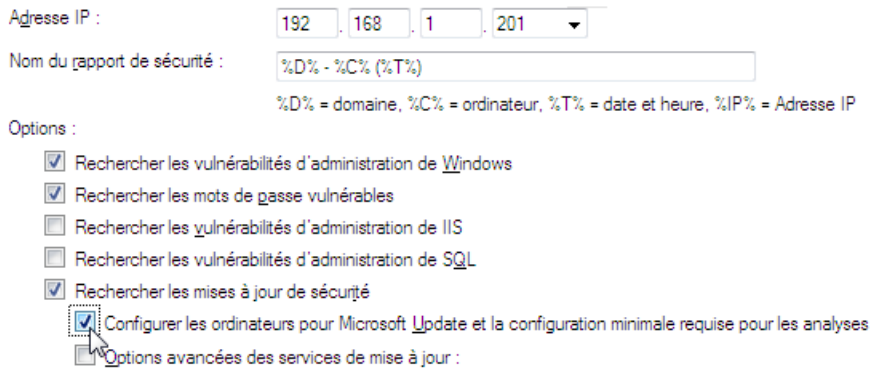


Agent Windows Update:

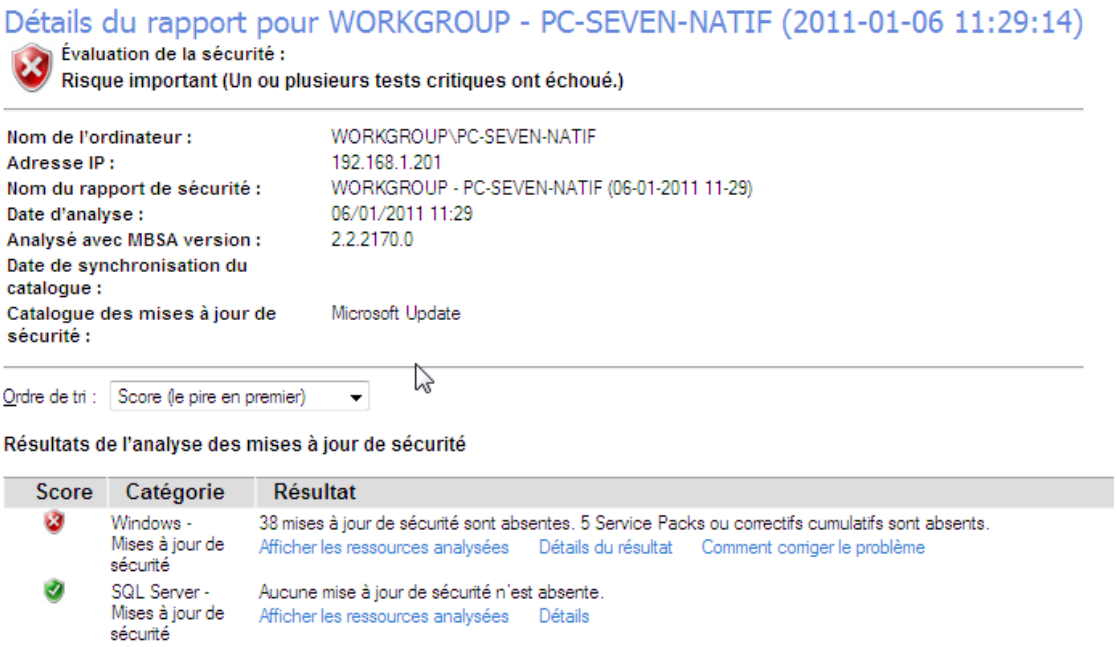
Un agent Windows Update peut être requis…



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)

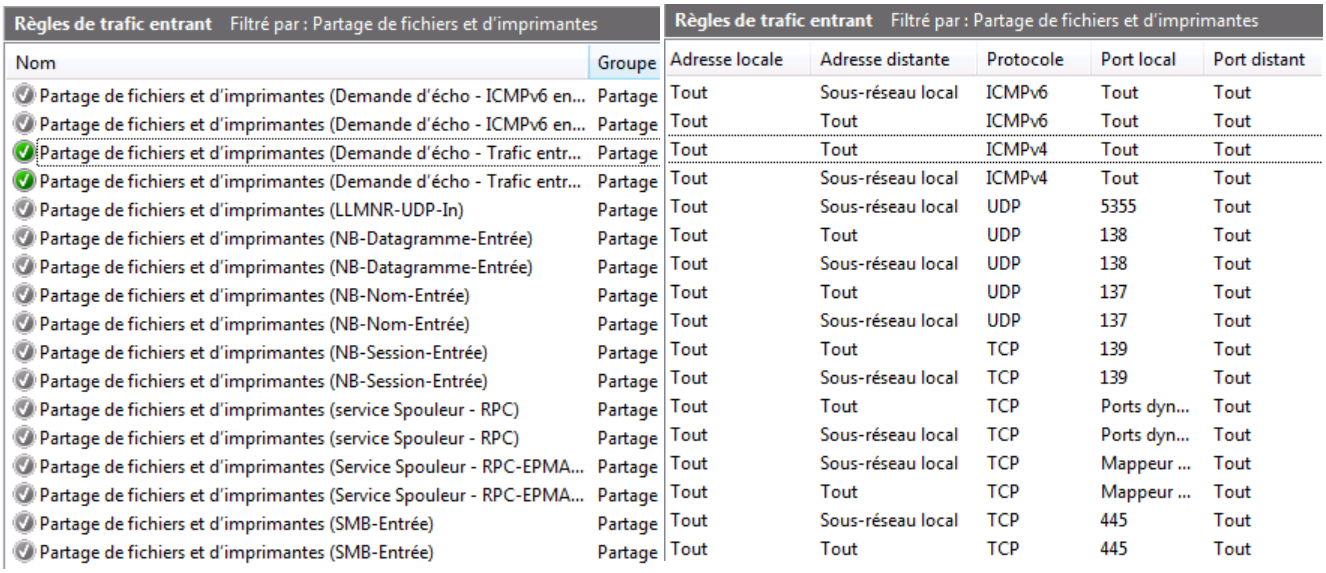
  Windows update (démarré par défaut)

- 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**



Règles de trafic entrant Filtré par : Partage de fichiers et d'imprimantes

Nom	Groupe
Partage de fichiers et d'imprimantes (Demande d'écho - ICMPv6 en...	Partage
Partage de fichiers et d'imprimantes (Demande d'écho - ICMPv6 en...	Partage
Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entr...	Partage
Partage de fichiers et d'imprimantes (Demande d'écho - Trafic entr...	Partage
Partage de fichiers et d'imprimantes (LLMNR-UDP-In)	Partage
Partage de fichiers et d'imprimantes (NB-Datagramme-Entrée)	Partage
Partage de fichiers et d'imprimantes (NB-Datagramme-Entrée)	Partage
Partage de fichiers et d'imprimantes (NB-Nom-Entrée)	Partage
Partage de fichiers et d'imprimantes (NB-Nom-Entrée)	Partage
Partage de fichiers et d'imprimantes (NB-Session-Entrée)	Partage
Partage de fichiers et d'imprimantes (NB-Session-Entrée)	Partage
Partage de fichiers et d'imprimantes (service Spouleur - RPC)	Partage
Partage de fichiers et d'imprimantes (service Spouleur - RPC)	Partage
Partage de fichiers et d'imprimantes (Service Spouleur - RPC-EPMA...	Partage
Partage de fichiers et d'imprimantes (Service Spouleur - RPC-EPMA...	Partage
Partage de fichiers et d'imprimantes (SMB-Entrée)	Partage
Partage de fichiers et d'imprimantes (SMB-Entrée)	Partage

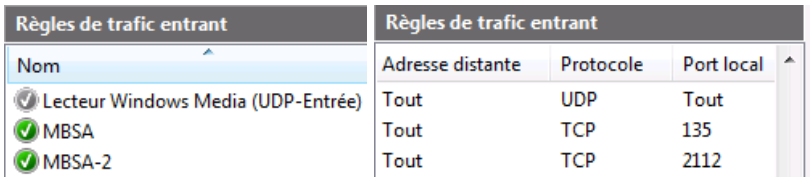
Règles de trafic entrant Filtré par : Partage de fichiers et d'imprimantes

Adresse locale	Adresse distante	Protocole	Port local	Port distant
Tout	Sous-réseau local	ICMPv6	Tout	Tout
Tout	Tout	ICMPv6	Tout	Tout
Tout	Tout	ICMPv4	Tout	Tout
Tout	Sous-réseau local	ICMPv4	Tout	Tout
Tout	Sous-réseau local	UDP	5355	Tout
Tout	Tout	UDP	138	Tout
Tout	Sous-réseau local	UDP	138	Tout
Tout	Tout	UDP	137	Tout
Tout	Sous-réseau local	UDP	137	Tout
Tout	Tout	TCP	139	Tout
Tout	Sous-réseau local	TCP	139	Tout
Tout	Tout	TCP	Ports dyn...	Tout
Tout	Sous-réseau local	TCP	Ports dyn...	Tout
Tout	Sous-réseau local	TCP	Mappeur ...	Tout
Tout	Tout	TCP	Mappeur ...	Tout
Tout	Sous-réseau local	TCP	445	Tout
Tout	Tout	TCP	445	Tout

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

TCP 135

TCP 2112 (par exemple)



Règles de trafic entrant

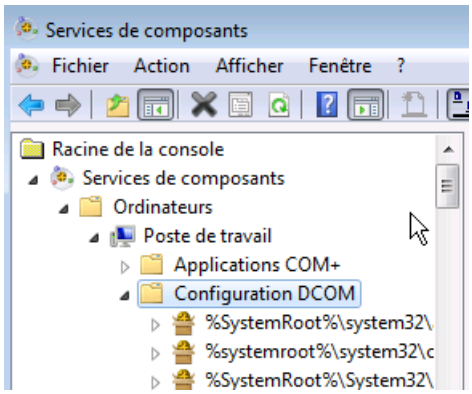
Nom	Adresse distante	Protocole	Port local
Lecteur Windows Media (UDP-Entrée)	Tout	UDP	Tout
MBSA	Tout	TCP	135
MBSA-2	Tout	TCP	2112

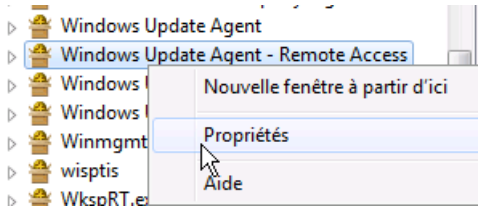
Procédure MBSA sur Seven:

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

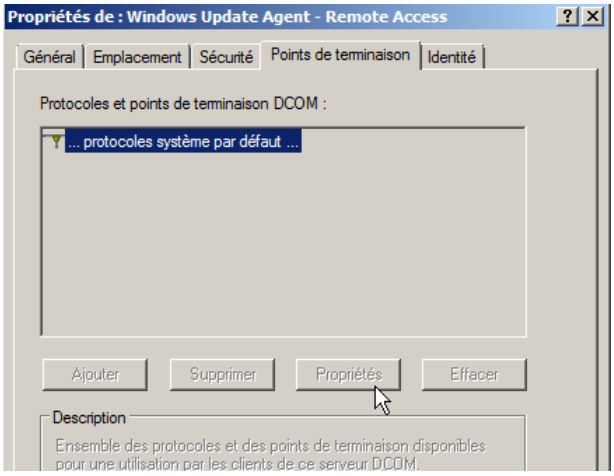
La configuration de N° Port statique pour WUA, Windows Update Agent (ou désactivation du Pare-feu …). Repose exactement sur les mêmes mécanismes

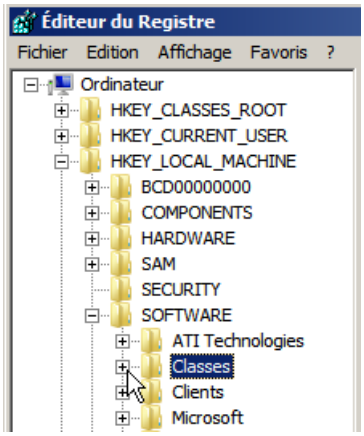




Mais l'accès aux propriétés n'est pas possible par défaut…

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

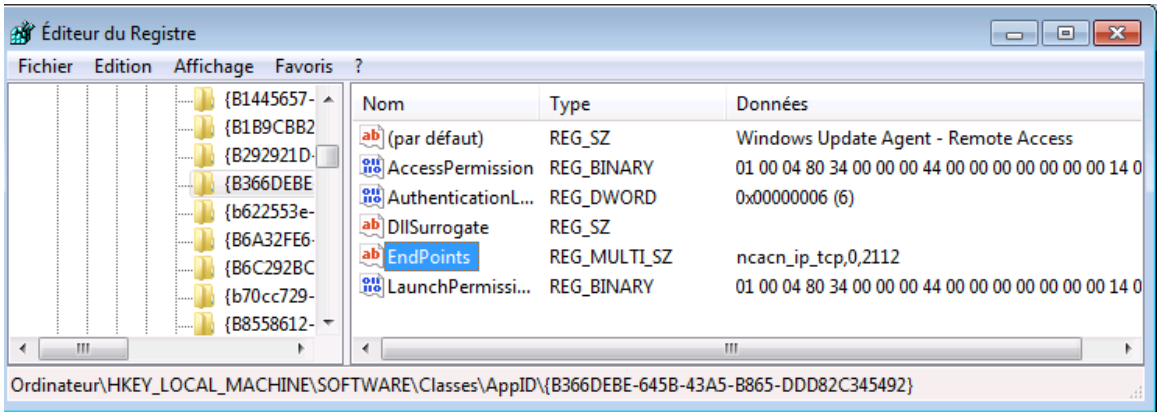




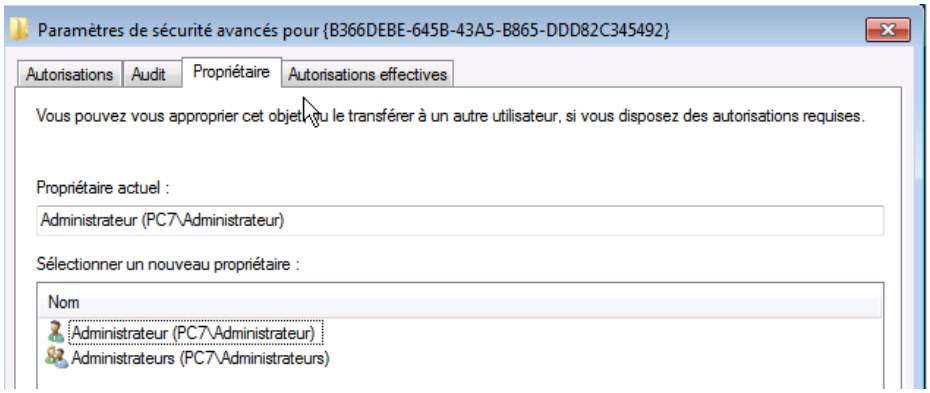
Sachant que les propriétés DCOM pour l'objet **Windows Update Agent** sont en fait stockées dans la base de registre ….

HKLM\SOFTWARE\CLASSES

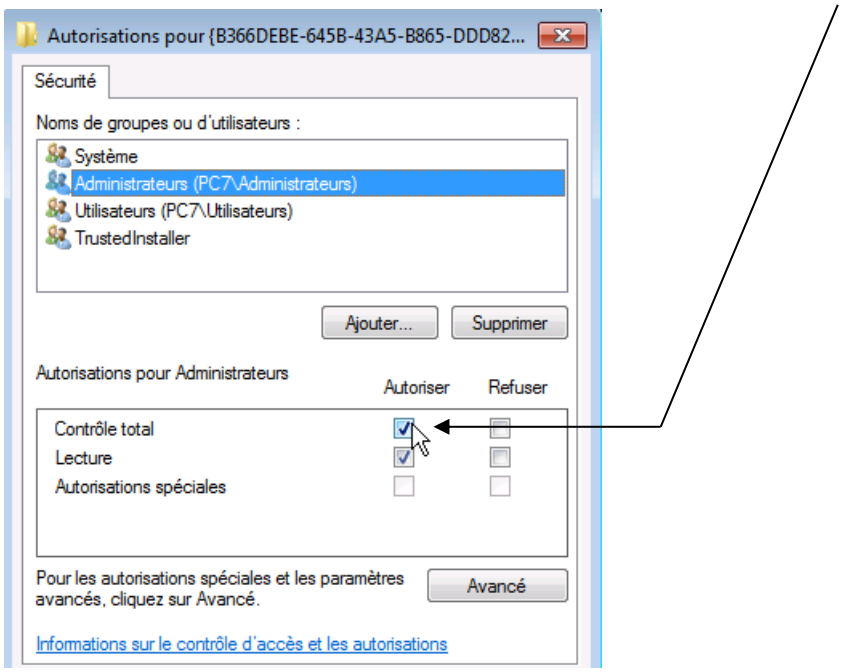
Et plus précisément dans **AppID\{B366DEBE……..DDD82C345492}**



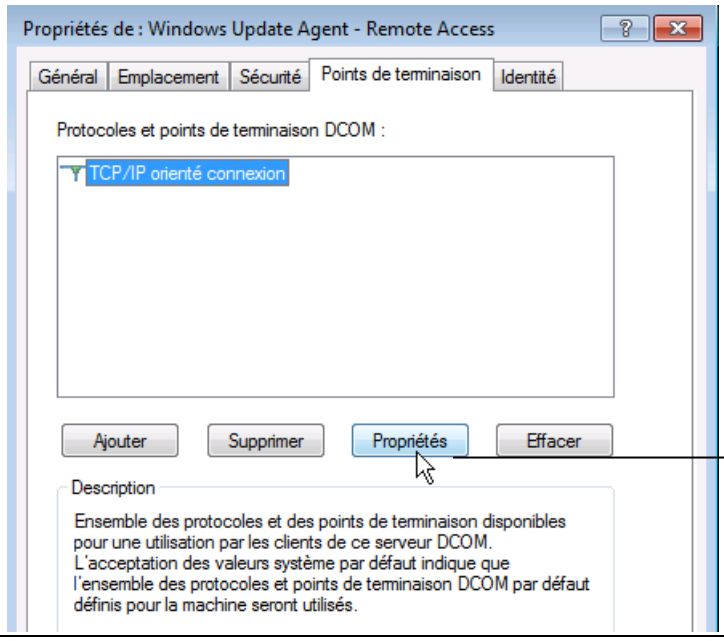
On demander les propriétés de la clé…

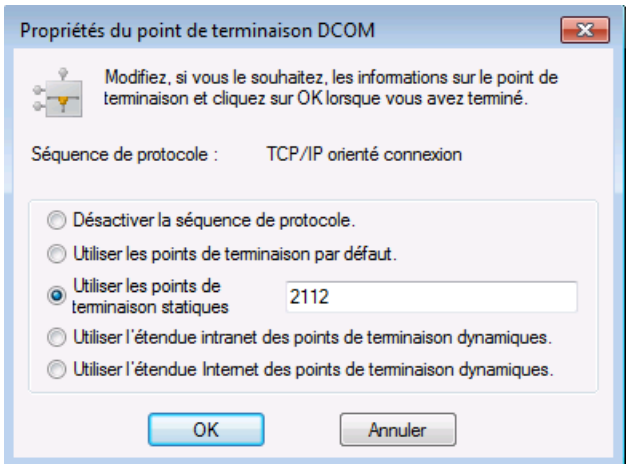


Et on s'approprie en NTFS l'objet, (à la place de **TrustedInstaller**) pour pouvoir ensuite s'y rajouter…

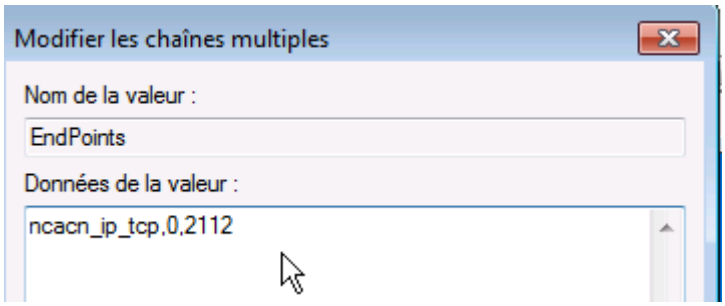


Maintenant les propriétés dcom de l'objet devraient être accessibles…





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…

```
C:\Users\Administrateur>netstat -ano

Connexions actives

  Proto  Adresse locale         Adresse distante       État
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING       948
  TCP    0.0.0.0:445            0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:5357           0.0.0.0:0              LISTENING       4
  TCP    0.0.0.0:49152          0.0.0.0:0              LISTENING       632
  TCP    0.0.0.0:49153          0.0.0.0:0              LISTENING       1096
  TCP    0.0.0.0:49154          0.0.0.0:0              LISTENING       1164
  TCP    0.0.0.0:49155          0.0.0.0:0              LISTENING       688
  TCP    0.0.0.0:49158          0.0.0.0:0              LISTENING       676
  TCP    127.0.0.1:668          0.0.0.0:0              LISTENING       1984
  TCP    127.0.0.1:668          127.0.0.1:49160        ESTABLISHED     1984
```

Liste des processus par PID :

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

le PID 1984…

c'est Carbonite !

```
C:\Users\Administrateur>tasklist

Nom de l'image                 PID Nom de la sessio Numéro de s Utilisation
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         24 Ko
System                           4 Services                   0      5 784 Ko
smss.exe                       448 Services                   0        560 Ko
csrss.exe                      580 Services                   0      3 848 Ko
wininit.exe                    632 Services                   0      3 348 Ko
csrss.exe                      644 Console                    1     12 100 Ko
services.exe                   676 Services                   0      6 008 Ko
lsass.exe                      688 Services                   0      1 756 Ko
lsm.exe                        696 Services                   0      3 356 Ko
winlogon.exe                   804 Console                    1      4 564 Ko
svchost.exe                    888 Services                   0      4 948 Ko
svchost.exe                    948 Services                   0      6 096 Ko
svchost.exe                    984 Services                   0     16 208 Ko
svchost.exe                   1096 Services                   0     10 184 Ko
mDNSResponder.exe             1956 Services                   0      3 824 Ko
CarboniteService.exe          1984 Services                   0     18 916 Ko
FrameworkService.exe          2036 Services                   0      5 128 Ko
Mcshield.exe                   492 Services                   0     25 936 Ko
```

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

```
C:\Users\Administrateur>tasklist /svc

Nom de l'image                 PID Services
========================= ======== ============================================
System Idle Process              0 N/A
System                           4 N/A
smss.exe                       448 N/A
csrss.exe                      580 N/A
wininit.exe                    632 N/A
csrss.exe                      644 N/A
services.exe                   676 N/A
lsass.exe                      688 ProtectedStorage, SamSs
lsm.exe                        696 N/A
winlogon.exe                   804 N/A
svchost.exe                    888 DcomLaunch, PlugPlay
svchost.exe                    948 RpcSs
svchost.exe                    984 WinDefend
```

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

```
C:\Windows\system32>Netsh advfirewall set allprofiles state on
Ok.
```

Désactiver tous les profils du Pare-feu Windows :

Netsh advfirewall set allprofiles state off

```
C:\Windows\system32>Netsh advfirewall set allprofiles state off
Ok.
```

Netsh Advfirewall – nouvelle commande

Restaurer les paramètres par défaut du Firewall

Ancienne commande	Nouvelle commande
netsh firewall reset	netsh advfirewall reset

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**

Ancienne commande	Nouvelle commande
netsh firewall définie opmode ENABLE	netsh advfirewall set currentprofile state on
netsh firewall set opmode mode = ENABLE exceptions=enable	Exécutez les commandes suivantes : netsh advfirewall set currentprofile state on netsh advfirewall set currentprofile firewallpolicy blockinboundalways,allowoutbound
netsh firewall set opmode mode=enable exceptions=disable profile=domain	Exécutez les commandes suivantes : Netsh advfirewall set domainprofile state on netsh advfirewall set domainprofile firewallpolicy blockinbound,allowoutbound
netsh firewall set opmode mode=enable profile=ALL	Exécutez les commandes suivantes : Netsh advfirewall set domainprofile state on netsh advfirewall set privateprofile state on

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

Ancienne commande	Nouvelle commande
netsh firewall set icmpsetting 8	netsh advfirewall firewall add rule name="ICMP Allow incoming V4 echo request" protocol=icmpv4:8,any dir=in action=allow
netsh firewall set icmpsetting type=ALL mode=enable	netsh advfirewall firewall add rule name="All ICMP V4" protocol=icmpv4:any,any dir=in action=allow
netsh firewall set icmpsetting 13 disable all	netsh advfirewall firewall add rule name="Block Type 13 ICMP V4" protocol=icmpv4:13,any dir=in action=block

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

Ancienne commande	Nouvelle commande
netsh firewall add portopening TCP 80 "Ouvrir le Port 80"	netsh advfirewall firewall add rule name="Open Port 80" dir=in action=allow protocol=TCP localport=80

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

Ancienne commande	Nouvelle commande
netsh firewall add allowedprogram C:\MyApp\MyApp.exe "Mon Application" ENABLE	netsh advfirewall firewall add rule name="Mon Application" dir=in action=allow program="C:\MyApp\MyApp.exe" enable=yes

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

Ancienne commande	Nouvelle commande
netsh firewall set service FileAndPrint	netsh advfirewall firewall set rule group="File and Printer Sharing" new enable=Yes
netsh firewall set service RemoteDesktop enable	netsh advfirewall firewall set rule group="remote desktop" new enable=Yes
netsh firewall set service RemoteDesktop enable profile=ALL	Exécutez les commandes suivantes : netsh advfirewall firewall set rule group="remote desktop" new enable=Yes profile=domain netsh advfirewall firewall set rule group="remote desktop" new enable=Yes profile=private

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 :

```
C:\Users\Administrateur>netsh
netsh>firewall
netsh firewall>show state

État du pare-feu :
-------------------------------------------------------------------
Profil                                  = Standard
Mode d'opération                        = Activer
Mode d'exception                        = Activer
Mode réponse multidiff/transmission     = Activer
Mode de notification                    = Activer
Version de stratégie de groupe          = Pare-feu Windows
Mode d'administration à distance        = Désactiver

Ports actuellement ouverts sur toutes les interfaces réseau :
Port   Protocole Version  Programme
-------------------------------------------------------------------
Aucun port n'est actuellement ouvert les interfaces réseau.
```

pour désactiver le pare-feu on passe :

set opmode DISABLE

```
netsh firewall>set opmode DISABLE
Ok.

netsh firewall>show state

État du pare-feu :
-------------------------------------------------------------------
Profil                                  = Standard
Mode d'opération                        = Désactiver
Mode d'exception                        = Activer
Mode réponse multidiff/transmission     = Activer
Mode de notification                    = Activer
Version de stratégie de groupe          = Pare-feu Windows
Mode d'administration à distance        = Désactiver
```

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

set opmode MODE=DISABLE exceptions=DISABLE

```
netsh firewall>set opmode mode=ENABLE exceptions=DISABLE
Ok.

netsh firewall>show state

État du pare-feu :
-------------------------------------------------------------------
Profil                                  = Standard
Mode d'opération                        = Activer
Mode d'exception                        = Désactiver
Mode réponse multidiff/transmission     = Activer
Mode de notification                    = Activer
Version de stratégie de groupe          = Pare-feu Windows
Mode d'administration à distance        = Désactiver
```

NETSH

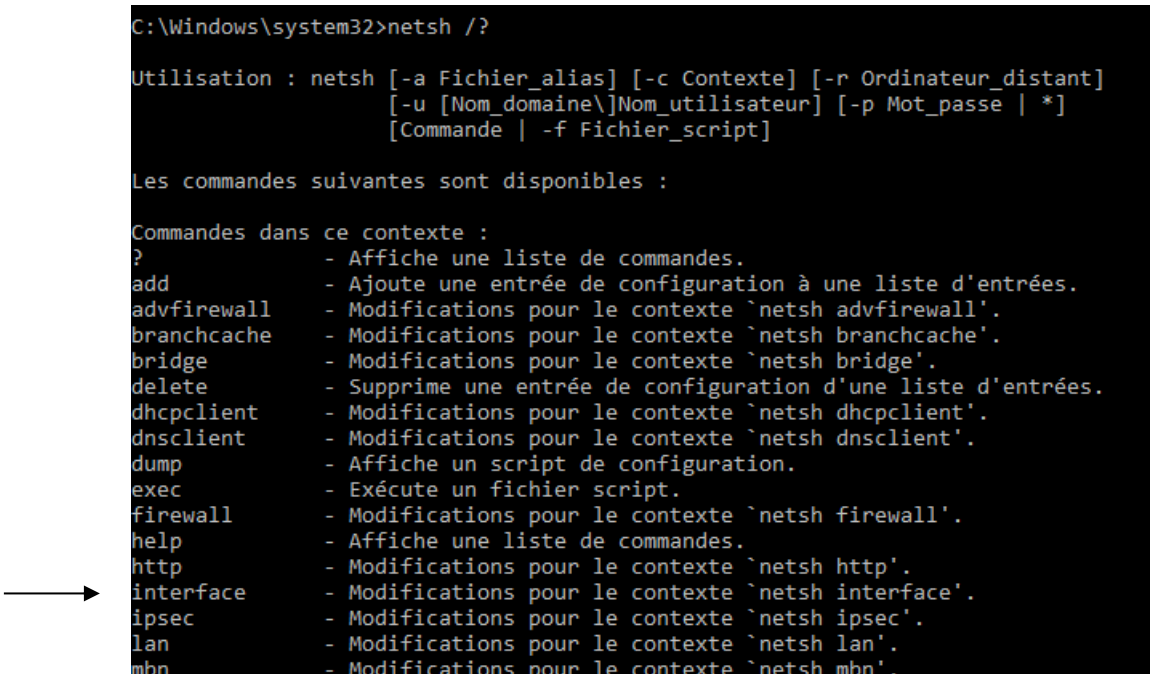
Cet utilitaire est présent sur tous les postes depuis 2000

Principe de netsh – contexte

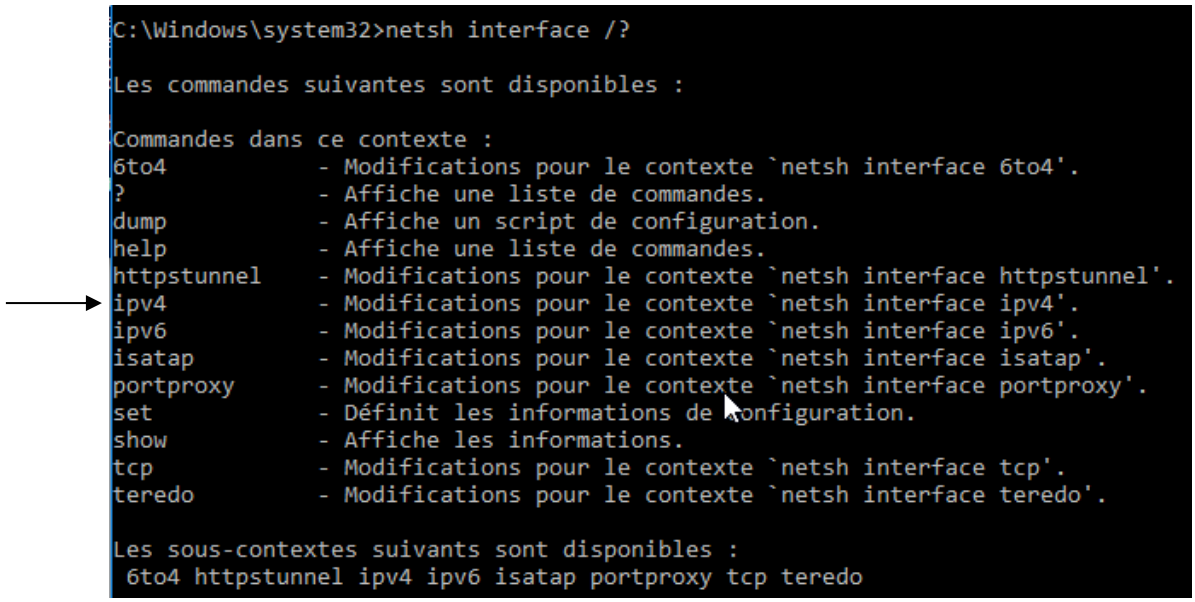
L'utilitaire **netsh** est un utilitaire qui fonctionne en différents niveaux de commande. A chaque **niveau – contexte de commande** est associée toute une liste de sous-commandes. on descend dans un niveau en tapant le **nom du niveau**.

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 :

```
C:\Windows\system32>netsh interface ipv4 /?

Les commandes suivantes sont disponibles :

Commandes dans ce contexte :
?               - Affiche une liste de commandes.
add             - Ajoute une entrée de configuration à une table.
delete          - Supprime une entrée de configuration d'une table.
dump            - Affiche un script de configuration.
help            - Affiche une liste de commandes.
install         - Installer le protocole IP.
reset           - Réinitialiser les configurations IP.
set             - Définit les informations de configuration.
show            - Affiche les informations.
uninstall       - Désinstaller le protocole IP.
```

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

```
C:\Windows\system32>netsh interface ipv4 set /?

Les commandes suivantes sont disponibles :

Commandes dans ce contexte :
set address     - Définit l'adresse IP ou la passerelle par défaut vers une int
set compartment - Modifie les paramètres de configuration des compartiments.
set dnsservers  - Définit les adresses et le mode du serveur DNS.
set dynamicportrange - Modifie l'étendue des ports utilisés pour l'attributior
set global      - Modifie les paramètres généraux de configuration globale.
set interface   - Modifie les paramètres de configuration d'interface pour IP.
set neighbors   - Définit une adresse de voisin.
set route       - Modifie les paramètres d'itinéraire.
set subinterface - Modifie les paramètres de configuration de sous-interface.
set winsservers - Définit les adresses et le mode du serveur WINS.
```

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

```
C:\>netsh interface ip set /?

Les commandes suivantes sont disponibles :

Commandes dans ce contexte :
set address     - Définit l'adresse IP ou la passerelle par défaut vers l'interfa
ce spécifiée.
set dns         - Définit les adresses et le mode du serveur DNS.
set wins        - Définit les adresses et le mode du serveur WINS.
```

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

```
C:\Windows\system32>netsh interface ipv4 set address /?

Syntaxe : set address [name=]<chaîne>
                      [[source=]dhcp|static]
                      [[address=]<adresse IPv4>[/<entier>]
                       [[mask=]<masque IPv4>]
                      [[gateway=]<adresse IPv4>|none
                      [gwmetric=]<entier>]
                      [[type=]unicast|anycast]
                      [[subinterface=]<chaîne>]
                      [[store=]active|persistent]
```

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

```
C:\Windows\system32>netsh interface show interface

État admin    État          Type            Nom de l'interface
-------------------------------------------------------------------------
Activé        Connecté      Dédié           Ethernet
Activé        Déconnecté    Dédié           Wi-Fi
```

Pour renommer une interface

```
C:\Windows\system32>netsh interface set interface name ="Ethernet" newname = "Lan-Gigabite"
```

Et on vérifie par

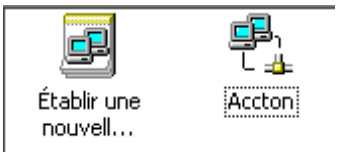
```
C:\Windows\system32>netsh interface show interface

État admin    État          Type            Nom de l'interface
-------------------------------------------------------------------------
Activé        Connecté      Dédié           Lan-Gigabite
Activé        Déconnecté    Dédié           Wi-Fi
```

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 :

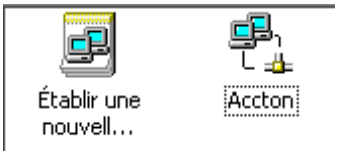
```
C:\>netsh interface ip set address "Accton" static 192.168.1.10 255.255.0.0
```

En descendant les niveaux :

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

```
C:\>netsh
netsh>interface
interface>ip
interface ip>set address "Accton" static 192.168.1.10 255.255.0.0
Ok.

interface ip>..

interface>..

netsh>exit


C:\>
```

- 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 :

```
C:\>netsh interface ip set address "Accton" static 192.168.1.1 255.255.255.0 192
.168.1.99 1
```

En descendant les niveaux :

```
C:\>netsh
netsh>interface
interface>ip
interface ip>set address "Accton" static addr=192.168.1.1 mask=255.255.255.0 gat
eway=192.168.1.99 gwmetric=1
Ok.

interface ip>..

interface>..

netsh>exit
```

---

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 :

```
C:\>netsh interface ip set address "Accton" static 192.168.1.1 255.255.255.0 192
.168.1.99 1
```

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**

```
C:\Windows\system32>netsh interface ipv4 set dns /?

Syntaxe : set dnsservers [name=]<chaîne>
            [source=]dhcp|static
            [[address=]<adresse IP>|none]
            [[register=]none|primary|both]
            [[validate=]yes|no]
```

ce qui pourrait donner dans un script

```
C:\>type dns.bat
@echo off
set name=Accton
set dns=%1
if %1.==. set dns=192.168.1.100
rem definition adresse dns
netsh interface ip set dns name=%name% static addr=%dns%
```

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**

```
PS C:\Windows\system32> Get-NetIPInterface

ifIndex InterfaceAlias                 AddressFamily NlMtu(Bytes) InterfaceMetric Dhcp     ConnectionState
------- -------------                 ------------- ------------ --------------- ----     ---------------
3       isatap.{B205BC77-2CF0-4A8A-9... IPv6                1280              50 Disabled Disconnected
5       Ethernet 2                     IPv6                1500               5 Enabled  Connected
1       Loopback Pseudo-Interface 1    IPv6          4294967295              50 Disabled Connected
5       Ethernet 2                     IPv4                1500               5 Disabled Connected
4       Ethernet                       IPv4                1500               5 Enabled  Disconnected
1       Loopback Pseudo-Interface 1    IPv4          4294967295              50 Disabled Connected
```

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

```
Windows PowerShell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tous droits réservés.

PS C:\Users\Administrateur> Get-NetAdapter

Name                      InterfaceDescription                ifIndex Status       MacAddress             LinkSpeed
----                      --------------------                ------- ------       ----------             ---------
Ethernet 2                Mellanox ConnectX-2 Ethernet Adapter       5 Up           00-02-C9-4E-7D-12      10 Gbps
Ethernet                  Atheros AR8121/AR8113/AR8114 PCI-E E...    4 Disconnected 00-22-15-56-35-71       0 bps
```

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

```
PS C:\Users\Administrateur> Get-NetAdapter | format-list Name, IfIndex, LinkSpeed


Name      : Ethernet 2
ifIndex   : 5
LinkSpeed : 10 Gbps

Name      : Ethernet
ifIndex   : 4
LinkSpeed : 0 bps
```

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

```
PS C:\Windows\system32> New-NetIPAddress -InterfaceIndex 4 -IPAddress 192.168.

IPAddress         : 192.168.1.254
InterfaceIndex    : 4
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Tentative
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : ActiveStore

IPAddress         : 192.168.1.254
InterfaceIndex    : 4
InterfaceAlias    : Ethernet
AddressFamily     : IPv4
Type              : Unicast
PrefixLength      : 24
PrefixOrigin      : Manual
SuffixOrigin      : Manual
AddressState      : Invalid
ValidLifetime     : Infinite ([TimeSpan]::MaxValue)
PreferredLifetime : Infinite ([TimeSpan]::MaxValue)
SkipAsSource      : False
PolicyStore       : PersistentStore
```

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

```
PS C:\Windows\system32> Set-DnsClientServerAddress -InterfaceIndex 4 -ServerAddresses 8.8.8.8
PS C:\Windows\system32>
```

Pour la vérification :

Get-DnsClientServerAddress -InterfaceIndex 4

```
PS C:\Windows\system32> Get-DnsClientServerAddress -InterfaceIndex 4

InterfaceAlias               Interface Address ServerAddresses
                             Index     Family
---------------              --------- ------- ---------------
Ethernet                             4 IPv4    {8.8.8.8}
Ethernet                             4 IPv6    {}
```

Vérif configuration - Get-NetIPConfiguration

donne

```
PS C:\Windows\system32> Get-NetIPConfiguration


InterfaceAlias        : Ethernet
InterfaceIndex        : 4
InterfaceDescription  : Atheros AR8121/AR8113/AR8114 PCI-E Ethernet Controller
NetProfile.Name       : cabare-intra.net
IPv4Address           : 192.168.1.254
IPv4DefaultGateway    : 192.168.1.1
DNSServer             : 8.8.8.8

InterfaceAlias        : Ethernet 2
InterfaceIndex        : 5
InterfaceDescription  : Mellanox ConnectX-2 Ethernet Adapter
NetProfile.Name       : cabare-intra.net
IPv4Address           : 192.168.1.10
IPv6DefaultGateway    :
IPv4DefaultGateway    : 192.168.1.1
DNSServer             : 192.168.1.90
                        192.168.1.91
```

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}

```
PS C:\Windows\system32> Set-NetIPInterface -InterfaceIndex 4 -Dhcp Enabled
PS C:\Windows\system32> _
```

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 ».