http://WWW.CABARE.NET ©

Prtg Paessler network monitor - tutoriel -

Monitoring et Supervision Réseau

Michel Cabaré – Ver 1.1 – Mai 2016-

Prtg Paessler
Network monitor

Michel Cabaré – Ver 1.1 – Mai 2016

www.cabare.net ©

TABLE DES MATIÈRES

PRTG TELECHARGEMENT

Source et 100 capteurs illimités:

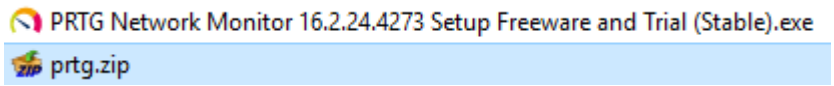
Tout se passe via le site web **https://www.fr.paessler.com/**

Avec

Téléchargement	Logiciel de surveillance réseau pour Windows – Version 16.2.24.4273 (June 8th, 2016)
Langues disponibles	Anglais, Allemand, Espagnol, Français, Portugais, Néerlandais, Tchèque, Japonais, et Chinois Simplifié
Prix	Gratuit jusqu'à 100 capteurs (Liste de prix)

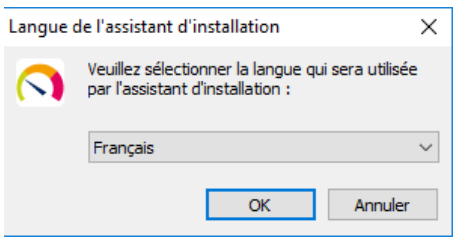
Installer Prtg Monitor 16.2.24.4273:

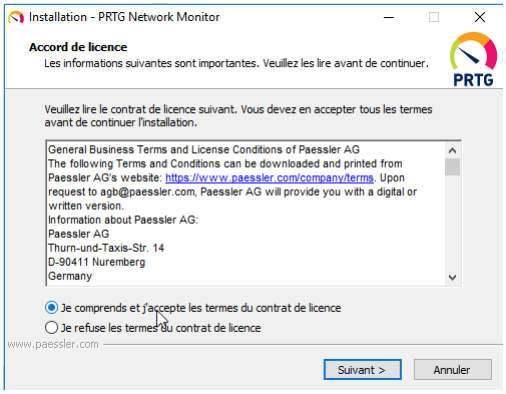
Il faut désarchiver le fichier récupéré..



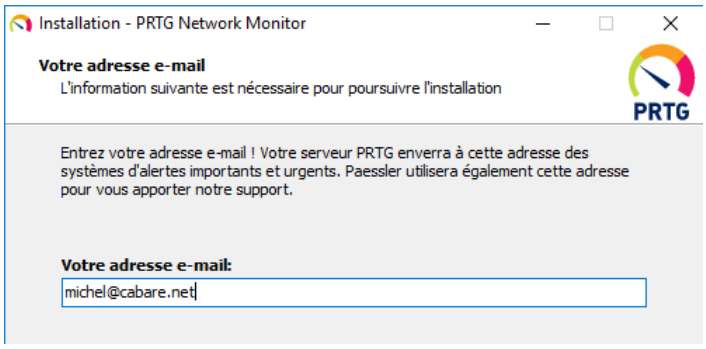
Qui fait environ 180Mo

Cela déclanche un assistant, un accord de licence…

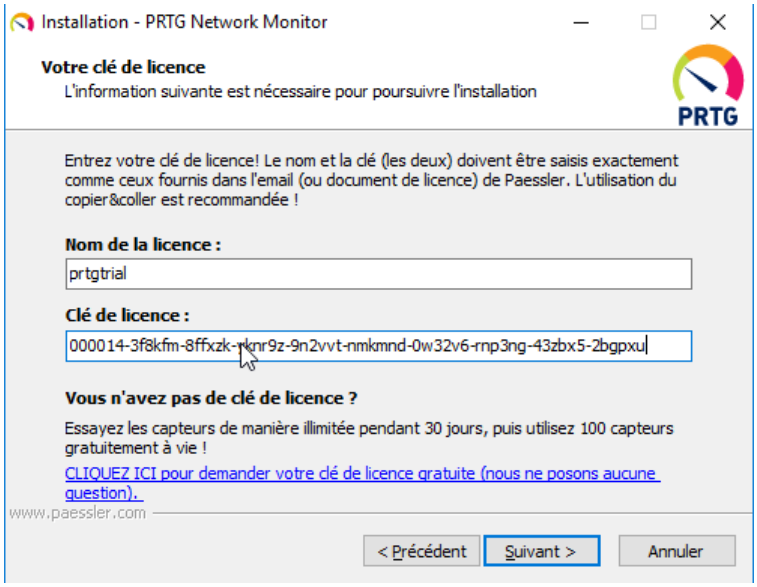




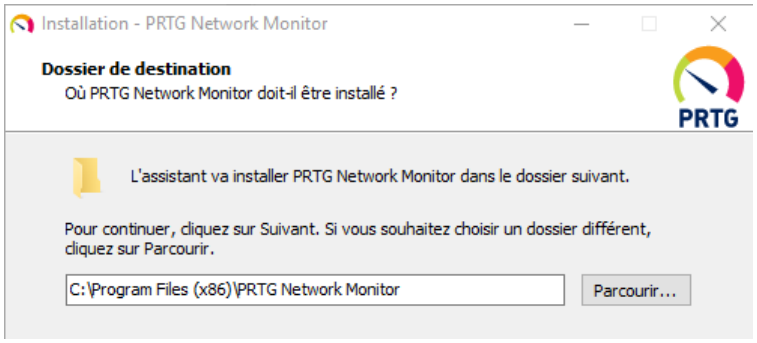
Il faut rentrer une adresse mail

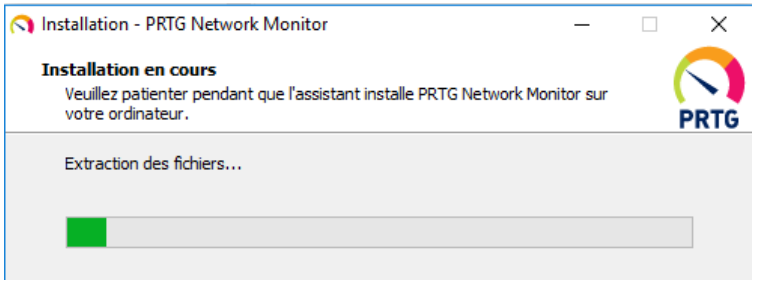


Entrer une clé

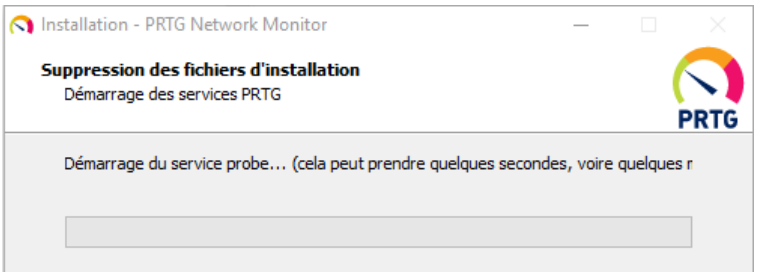


Choisir un dossier (enriron 800 mo de requis)





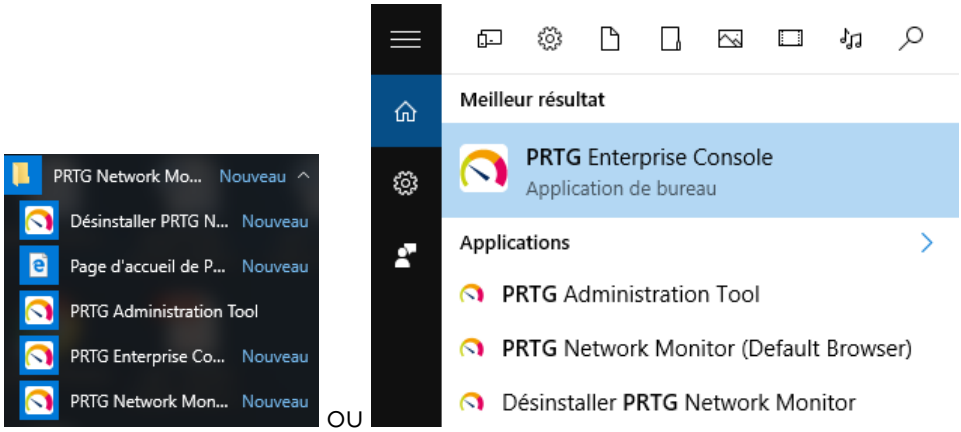
Ensuite les 2 services **probe** et **serveur** démarrent



Et on tombe directement sur

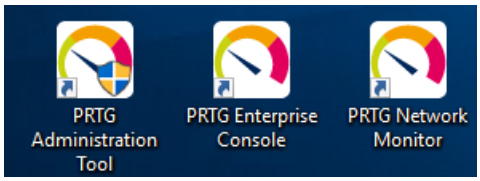
Résultat d'installation

Cela crée un groupe PRTG dans lequel on voit les 3 entrées



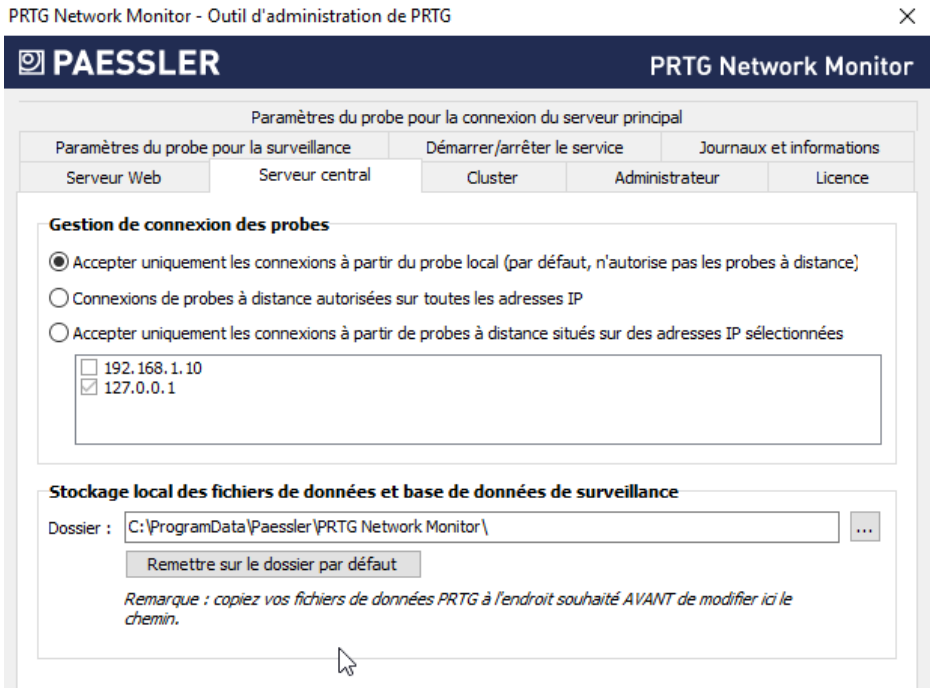
Il y a l'installation de PRTG "core" proprement dit dans la machine, administrable via **PRTG administration Tool**

Et deux clients : un client lourd **PRTG Enterprise Console** et un client léger **PRTG Network Monitor**

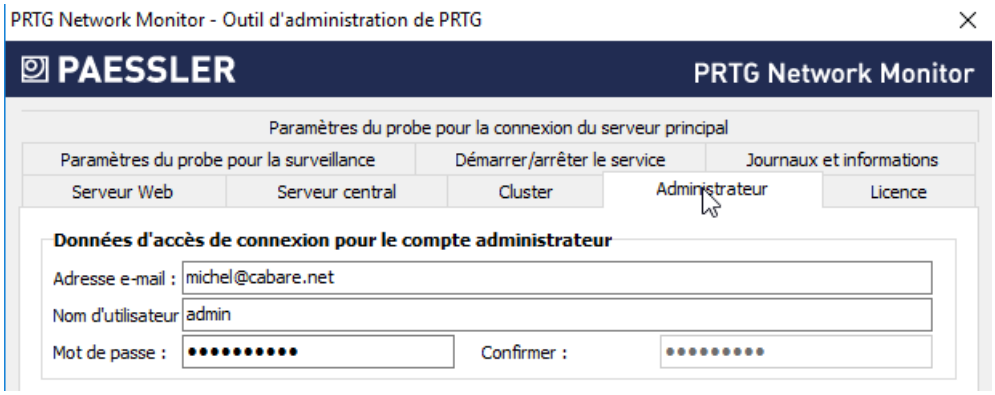


PRTG Administration Tool

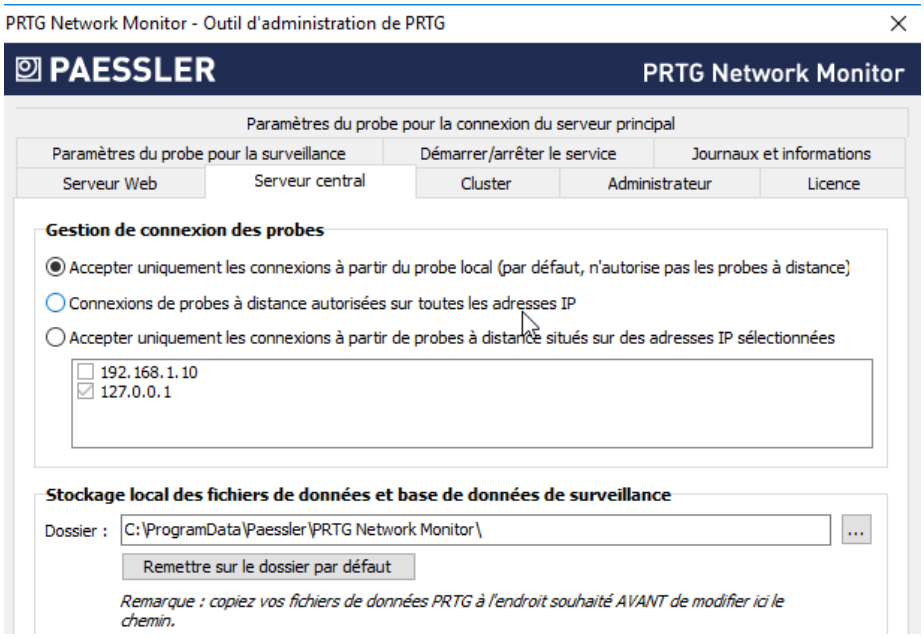
Il y a l'installation de PRTG "core" proprement dit dans la machine, administrable via **PRTG administration Tool**



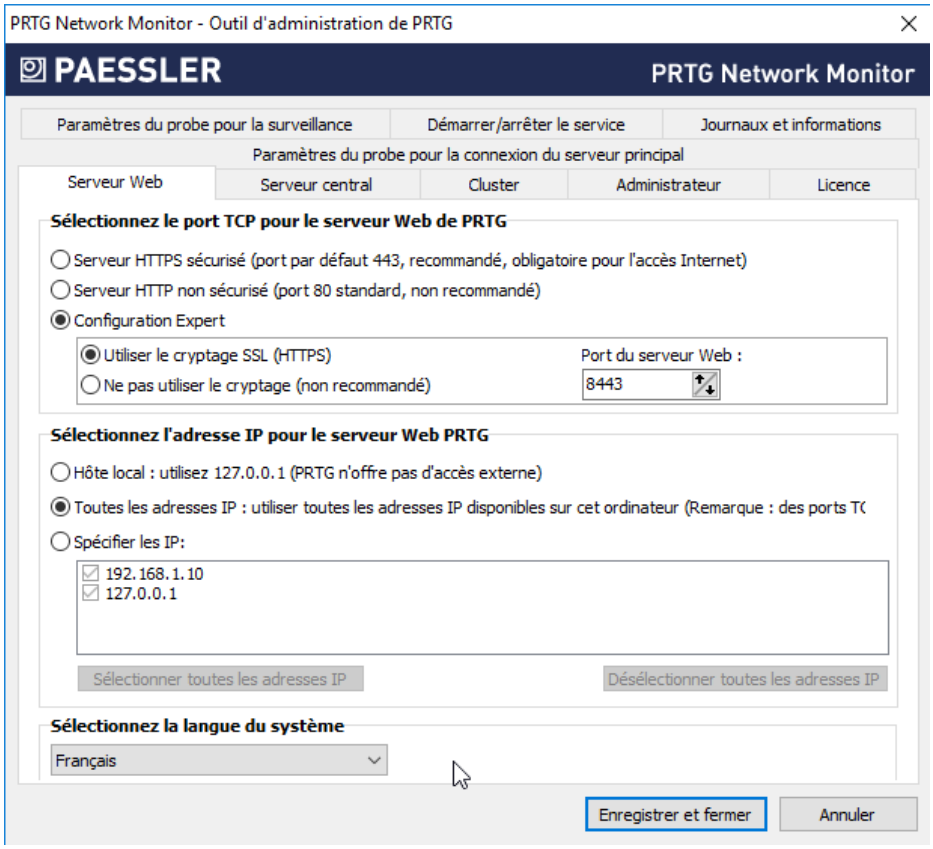
On y retrouve tous les réglages important, onglet **Administrateur**



onglet **Serveur central**



onglet **Serveur Web**



Changer l'endroit de stockage des données

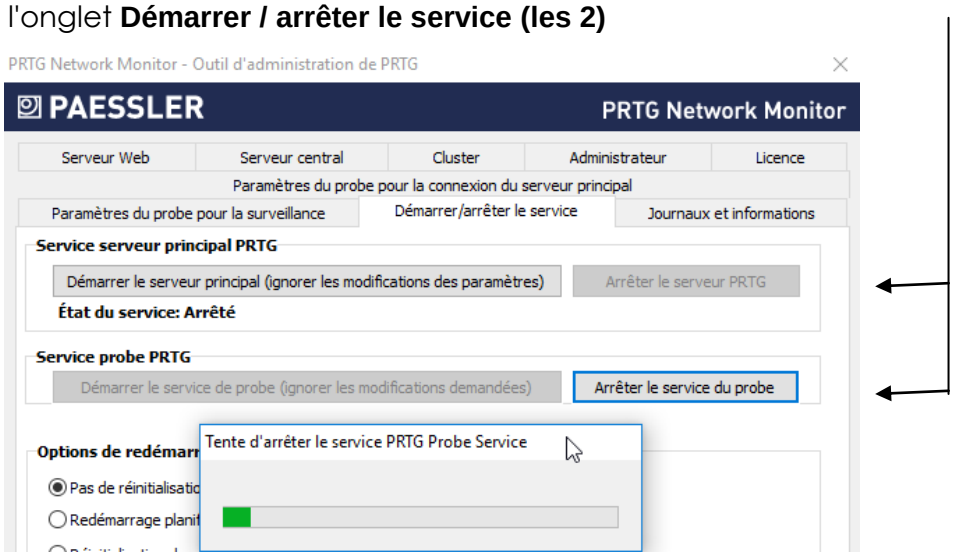
Les données par défaut étant dans **programData\Paessler\PrtgNetwork**

On veut les placer en ***C:\data-prtg*** Il faut effectuer la séquence suivante :

- Arrêter PRTG, service principal, et probe
- Déplacer les données
- Re-démarrer PRTG

Arrêt PRTG

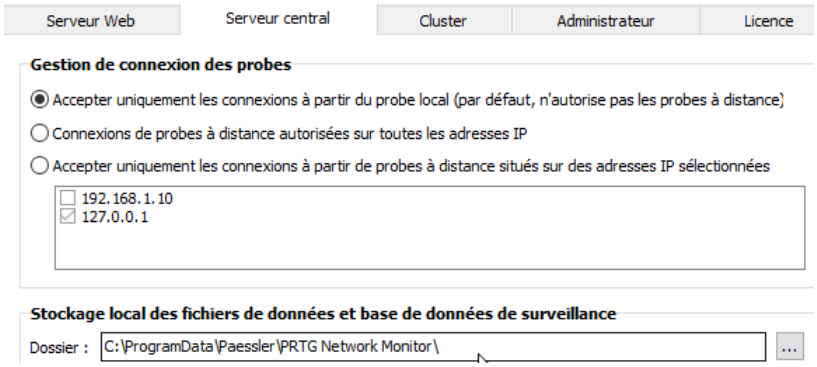
Dans l'onglet **Démarrer / arrêter le service (les 2)**



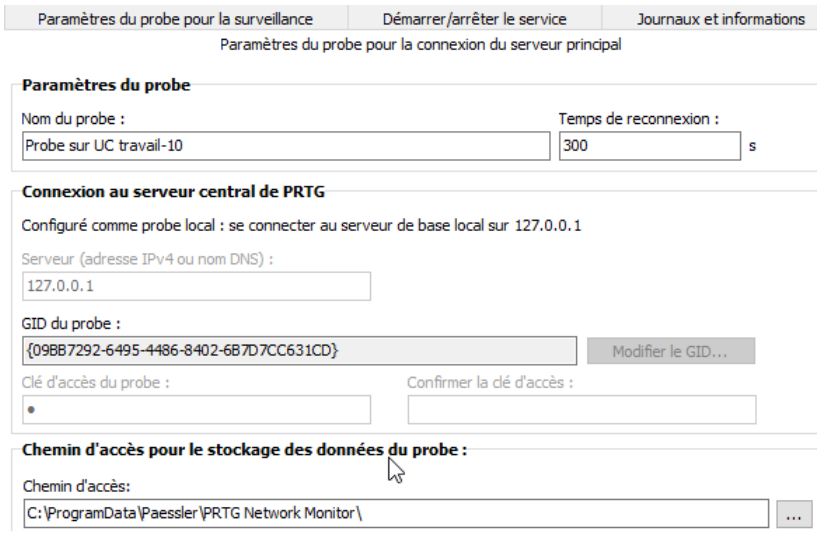
Déplacer les données

Il faut vérifier 2 paramètres (normallement identiques) indiquant les fichiers de stockage utilisés, repectivement

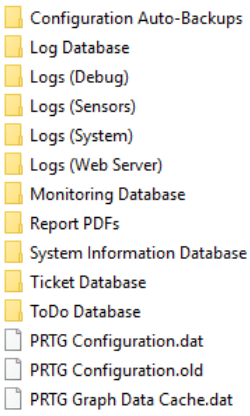
Onglet **Serveur central**, puis **Stockage local des fichiers de données et base de données de surveillance**

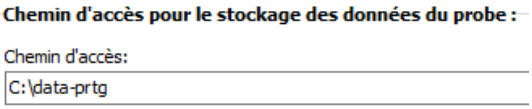


Onglet **Paramètres du probe pour la connexion du serveur principal**, puis **Chemin d'accès pour le stockage des données du probe**



On va donc copier tout ce qui s'y trouve dans notre nouvel emplacement





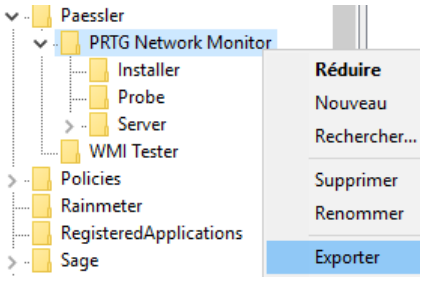
Redémarrer le probe

Déplacer le Core system de PRTG sur une autre machine

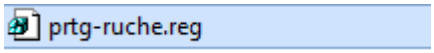
C'est possible, mais la procédure est un peu.. laborieuse, imaginons devoir transférer notre installation de poste-A à un poste-B

- Installer un version sur le système cible poste-A
- Placer les données dans un dossier équivallent (s'il a été modifié sur le poste A) sur le poste B
- Arrêter sur les 2 postes les services PRTG
- Copier tous le dosssier data du poste-A dans le dossier data du poste-B
- Déplacer en Exportant une branche de la base de registre du système d'origine-A

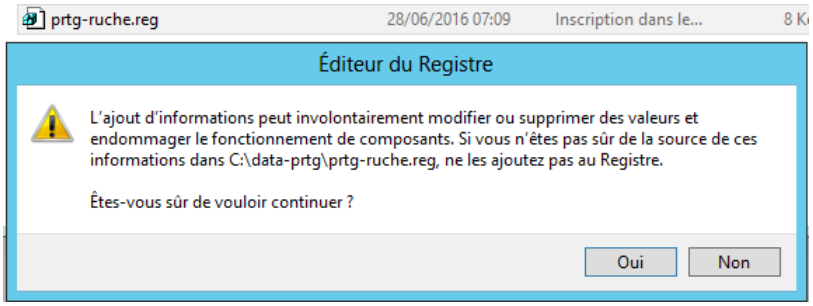
  HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432 Node\Paessler\PRTG Network Monitor



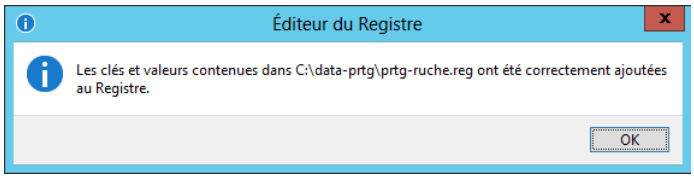
On obtient un fichier **.reg**



Copier ce fichier sur le Poste-B et l'importer dans la base de registre en double cliquant dessus

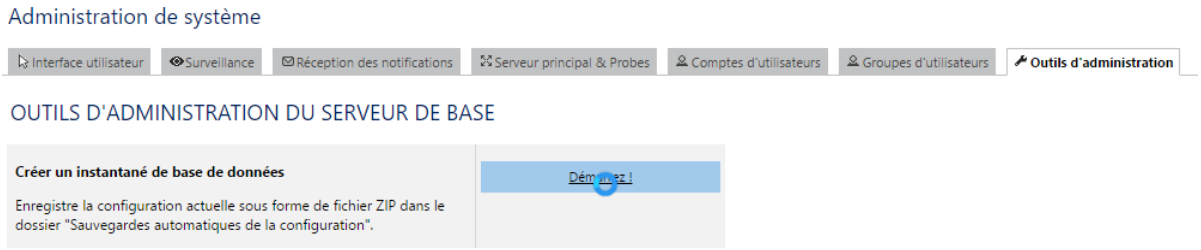


On a une confirmation

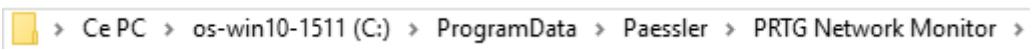


Effectuer une sauvegarde :

Dans **Administration de système – Outils d'administration – Créer un instantané de base de donnée**



Les fichiers se trouvent dans **programData\Paessler\PrtgNetwork**



Port utilisés :

Webserver

Port User	Port Number	Remarks
Webserver	TCP 80 (HTTP), 443 (HTTPS) **Fallbacks**: 8443 and 32000+ (HTTPS), 8080 (HTTP)	You can change the TCP port or define a custom one in the webGUI in the **User Interface** settings, section **Web Server**. The Enterprise Console also uses this port to connect to the server, as well as mobile apps.
Reports	8085 (PDF reports)	This port is only opened and blocked on the local PRTG server (localhost). For HTML reports, the configured webserver port is used. If necessary, you can change this in the registry.
Auto-update and activation	443	See this article for details.
Update check and download	80	See this article for details.
Active Directory integration	TCP and UDP 389 (non-secure), TCP 636 (SSL)	LDAP port for AD integration

Note: If the PRTG web server always uses a fallback port after a server restart, check for programs that use the same port as PRTG on startup. For example, the integrated Microsoft IIS web server uses the port 80 (443 for SSL) by default and starts before PRTG so that the port is not available for PRTG. Please define a different port for IIS or disable it. You can also disable the **World Wide Web Publishing Service** on startup to get the same effect.

Notifications

Notification	Port Number	Remarks
Push	TCP 443	Target URL: https://api.prtgcloud.com:443 *Note:* In PRTG versions previous to 15.4.20 push notifications used port 8443 (https://push.prtgcloud.net:8443)
SMTP	TCP 25	-
SNMP Trap	UDP 162	-
Syslog	TCP 514	-

Cluster

Port User	Port Number	Remarks
Communication between cluster nodes	23570	All communication between cluster nodes is directed through this TCP port.

Monitoring

PRTG sensors use various monitoring technologies to query the desired data. For this purpose, the particularly used technologies need open ports for the communication between the PRTG core server and the monitored devices in the network.

Technology	Port Number (default)
Cloud (Ping and HTTP)	TCP 443 (8443 before PRTG version 15.4.20)
HTTP (proxy)	TCP 8080
IMAP	TCP 143 (non-secure), 993 (SSL)
LDAP	TCP/UDP 389 (non-secure), TCP 636 (SSL)
MSSQL	TCP 1433
MySQL	TCP 3306
Oracle	TCP 1521
POP3	TCP 110 (non-secure), 995 (SSL)
PostgreSQL	TCP 5432
SMTP	TCP 25 (non-secure), 465 (SSL), 587 (SSL)
SNMP	UDP 161
SNMP Trap	UDP 162
SSH	TCP 22
Syslog	TCP 514
WBEM	TCP 5988 (non-secure), 5989 (SSL)
WMI	TCP 135 (*)

Note: This list might not be complete. The used ports can be different depending on your configuration. Usually, you can change the default ports in PRTG in the particular device and/or senso settings.

(*) WMI needs not only the open port 135. Please refer to this article for details.

Remote Probes

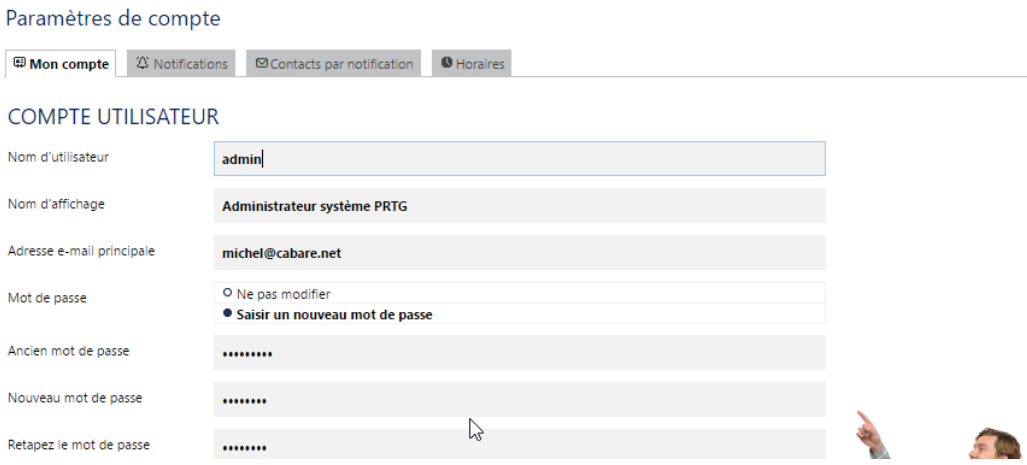
Port User	Port Number	Remarks
Connections between remote probes and core and vice-versa	23560	Usually, it is sufficient to open or forward this TCP port on the core server only. Please see this article if you need to change it.

Changer le mot de passe d'accès à prtg:

Dans **Configuration – Paramètres de compte – Mon compte**

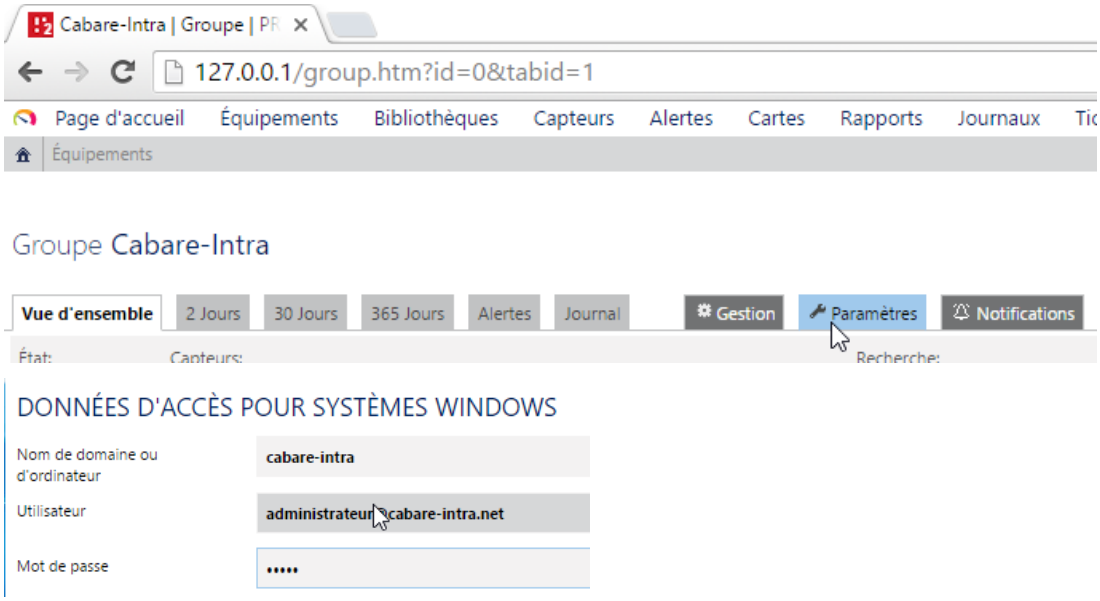
Et on donne login:***admin*** password:***Prtgzk28***

Par défaut login:***prtgadmin*** password:***Prtgadmin***



Paramètres identifiants windows:

Dans **Equipement – Paramètres**



Vue d'ensemble = Equipement:

Dans **Equipement**

Vocabulaire prtg - :

Core server : application principale

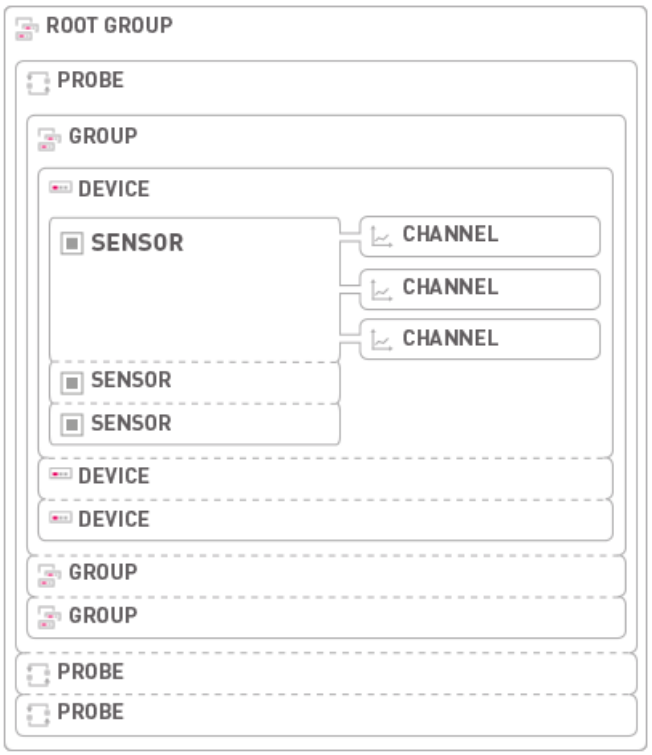
Probe : unité d'administration pour laquelle lorsque l'on effectue des réglages, ceux-ci s'appliquent par héritage à tous son contenu (groupes et device)

Group : unité logique

Device : équipements accessible via une adresse IP

Sensor : capteur

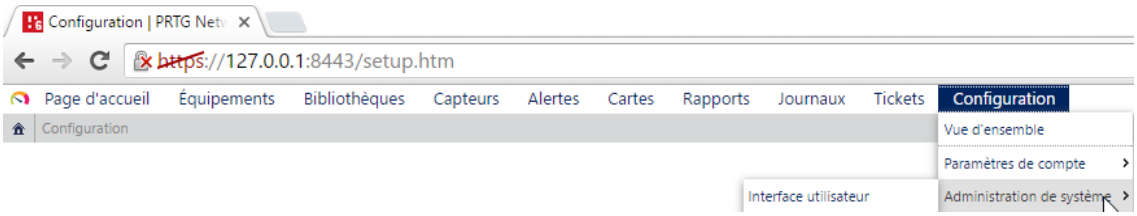
Channel : voie de communication



PRTG ET ROOT GROUP

Paramétrage administration Prtg:

Accessible depuis l'accueil via **Configuration / Administration de système**



Paramétrage Groupe de Base:

L'arborescence se présente ainsi **Root Group** Cabare-intra, **Probe** 127.0.0.1

On se place sur le groupe, et on demande **Paramètres**

Plusieurs choses sont intéressantes, notamment

DONNÉES D'ACCÈS POUR SYSTÈMES WINDOWS

Nom de domaine ou d'ordinateur	**cabare-intra**
Utilisateur	**administrateur@cabare-intra.net**
Mot de passe	•••••••••

INTERVALLE DE BALAYAGE

Intervalle de balayage	**60 secondes**
Lorsqu'un capteur signale une erreur	**Régler le capteur afin qu'il envoie un avertissement après 1 intervalle, puis le régler sur "non fo**

Lorsqu'un capteur signale une erreur, PRTG peut essayer d'atteindre et vérifier de nouveau l'équipement concerné au cours de l'intervalle de balayage suivant, avant que le capteur ne soit affiché comme 'non fonctionnel'. Cela peut éviter de recevoir de fausses alertes si votre appareil rencontre uniquement des problèmes temporaires.

Remarque : les capteurs WMI utilisent toujours au moins 1 intervalle. Les limites des erreurs de

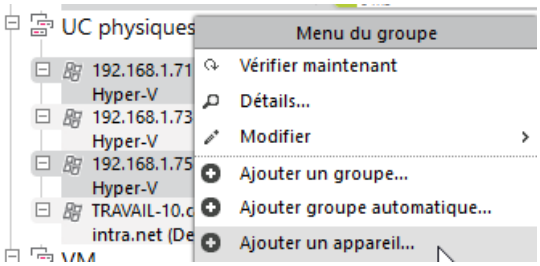
DONNÉES D'ACCÈS POUR LES ÉQUIPEMENTS SNMP

Version SNMP	○ v1 ● **v2c (recommandée)** ○ v3
Chaîne de communauté	**public**
Port SNMP	**161**
Délai d'expiration SNMP (s)	**5**

AJOUTER UN EQUIPEMENT

1 équipement – 1 @ ip:

On se place sur un groupe, et on demande via clic droit **Ajouter un appareil**

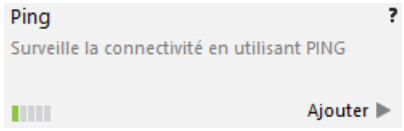


Et soit on donne une @ ip soit un nom DNS, et on indique le type de découverte (cela peut donner une idée des possibilités)

Ajouter un capteur Ping:

Un fois que l'on a un équipement, il faut au minimum lui ajouter un capteur,

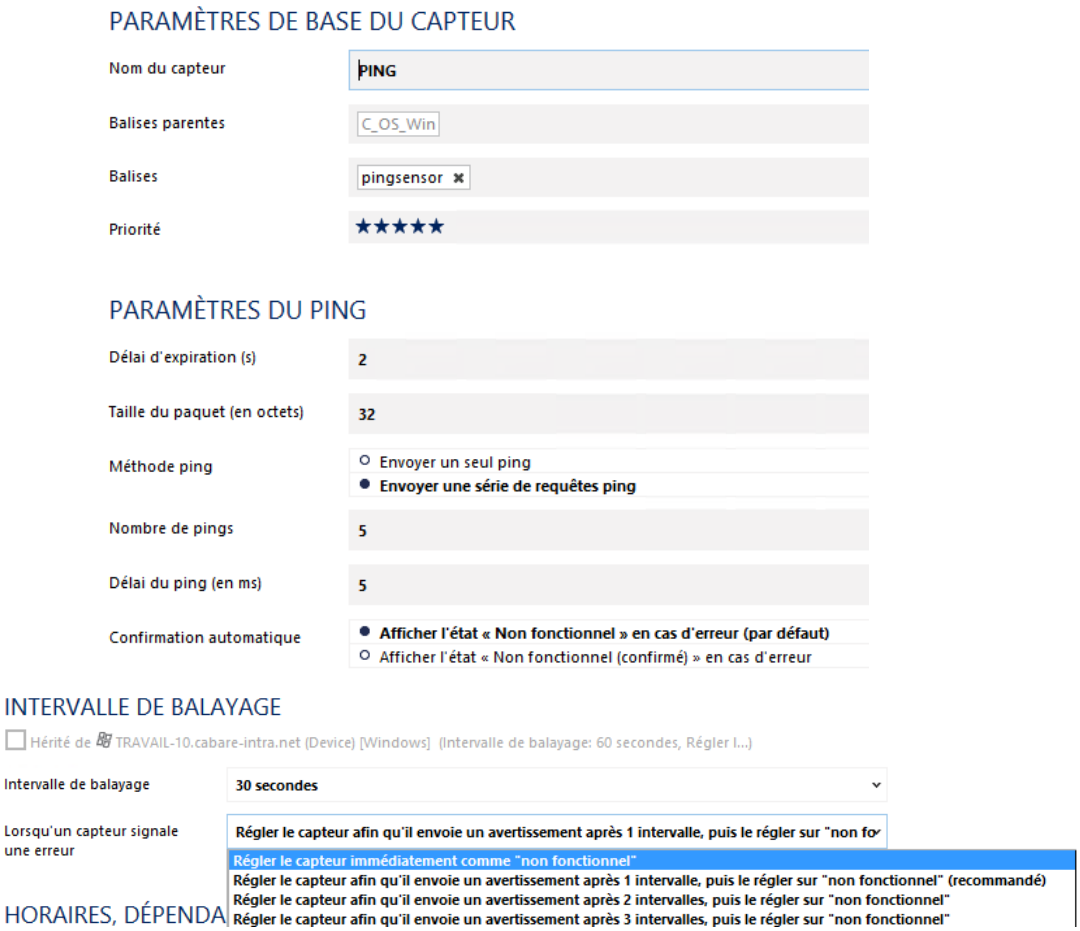
Le capteur de Base peut être un capteur ping



Donnant, avec un historique facilement accessible

On peut bien sur effectuer quelques réglages, notamment

- Délais du ping
- au bout de combien de ping on déclare que le ping ne réponds pas…

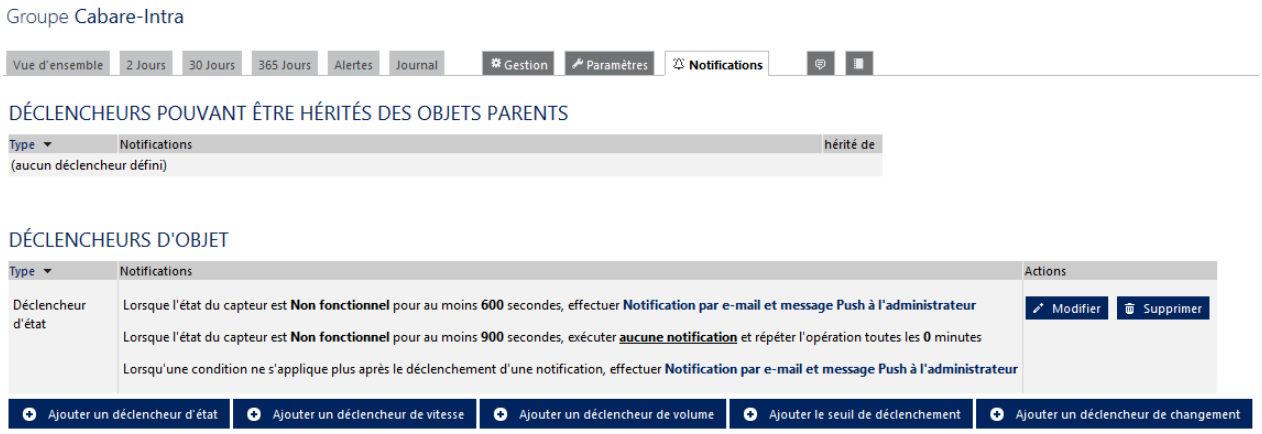


NOTIFICATION

Principe de notification:

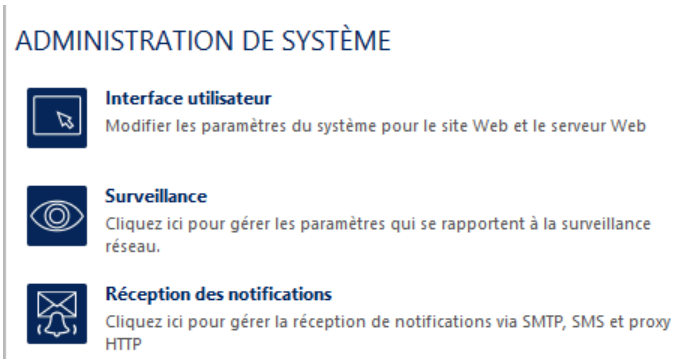
Au niveau du probe, on définit un principe de notification, qui sera ensuite hérité par tous les équipements et tous les capteurs

On se place sur le **Groupe principal**, et on demande **Notifications**

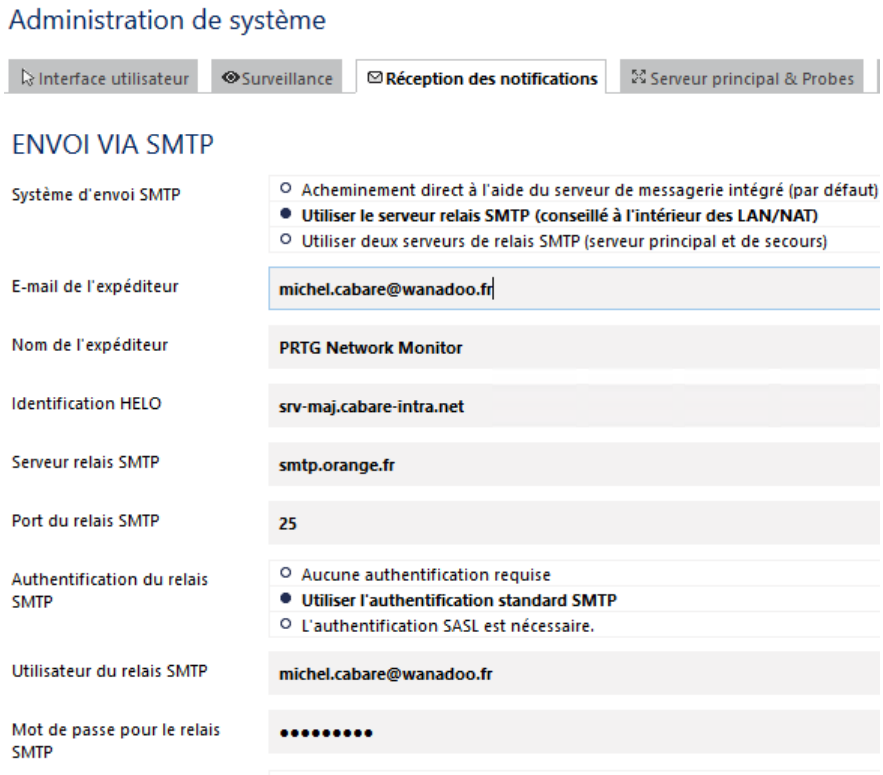


Paramétrage système smtp:

Dans **Configuration**, via **Administration de système** puis **Réception des notifications**

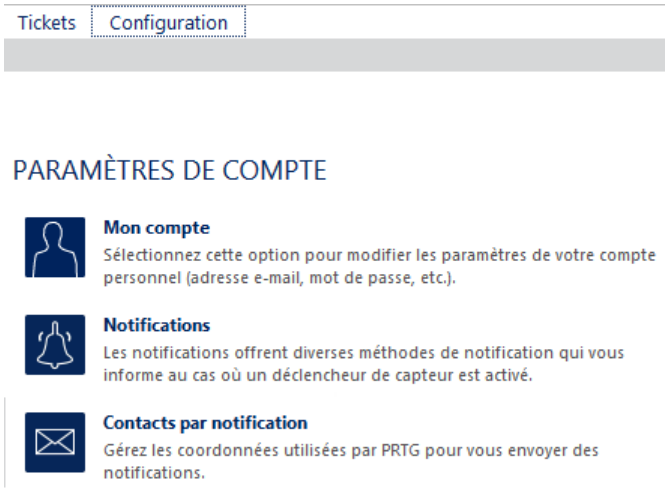


On peut donner les informations pour une connection smpt

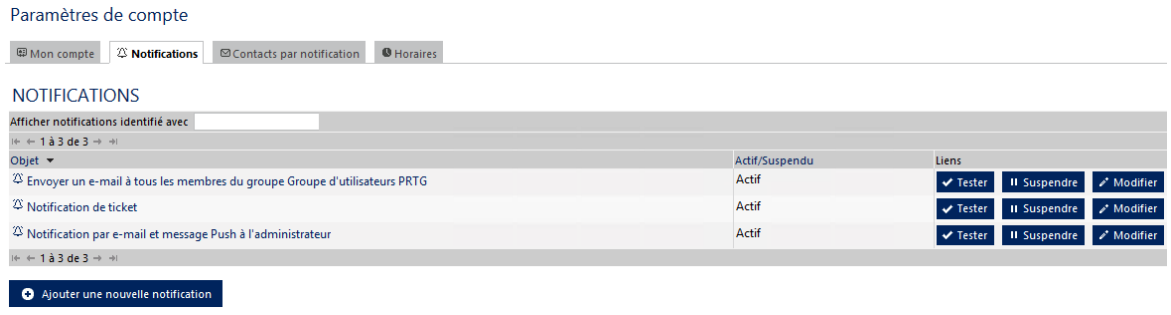


Paramètrage de base de la notification:

Dans **Configuration**, via **paramètres de compte** puis **Notifications**



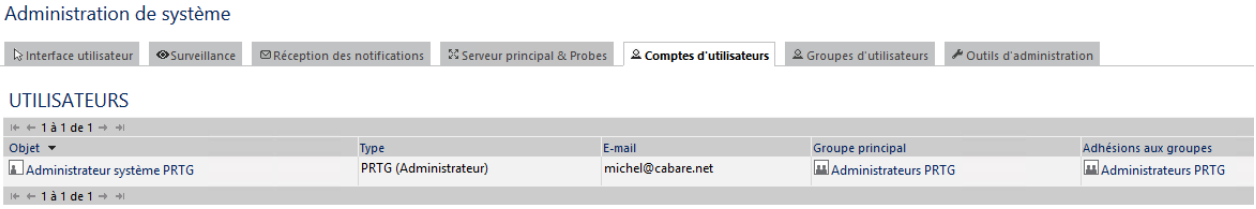
On obtient



Ne pas confondre le compte **Administrateur Système PRTG**, et le groupe des **Administrateurs Prtg** et le groupe **Groupe d'utilisateurs PRTG**

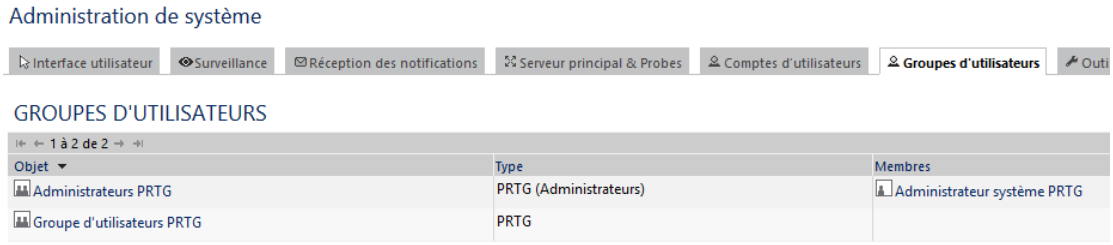
Dans les comptes,

On a le compte **Administrateur Système PRTG**

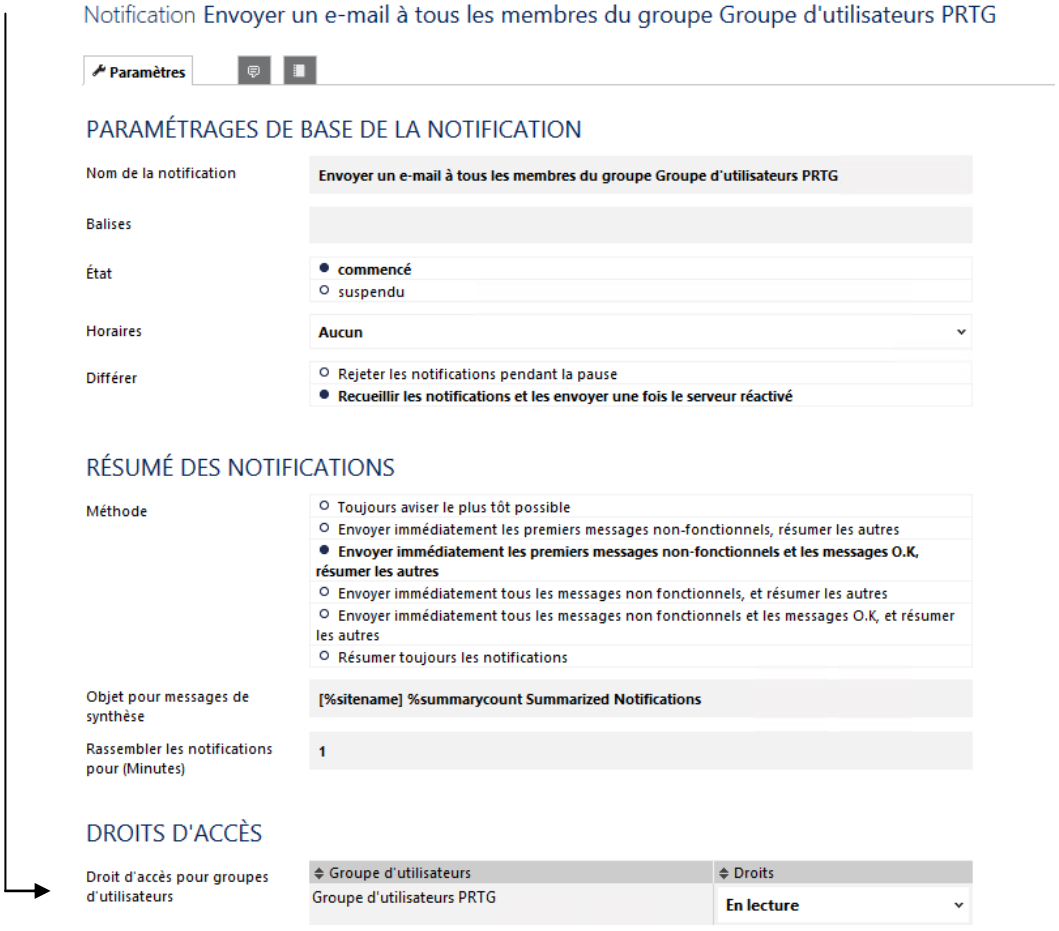


Dans les groupes

On a les groupes **Administrateurs PRTG** et le groupe **Groupe d'utilisateurs PRTG**

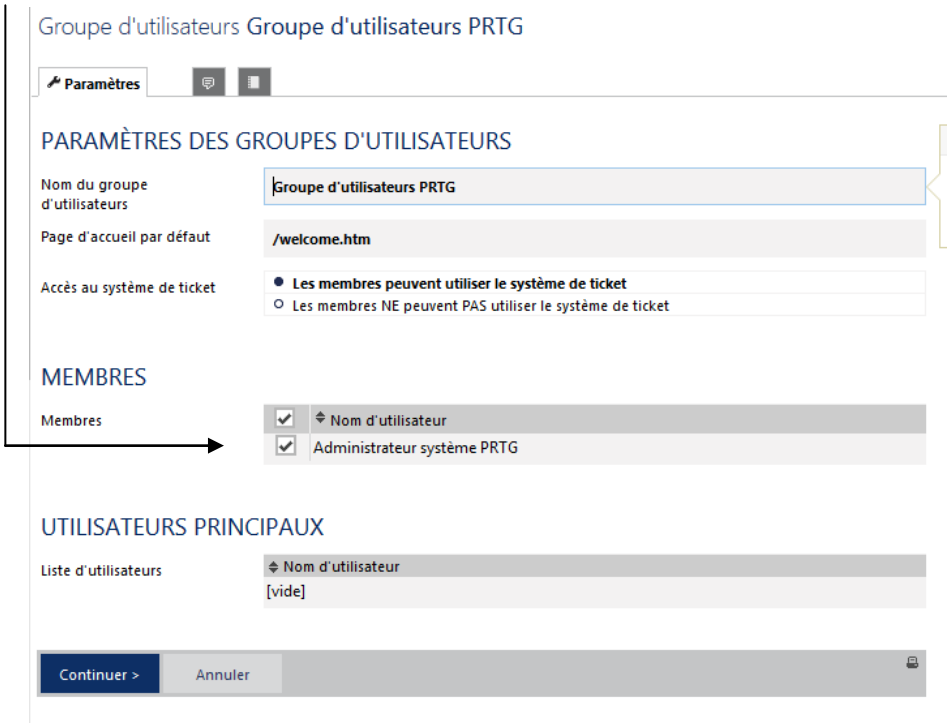


De base, la notification est envoyée à tous les membres du groupe **Groupe des utilisateurs PRTG** qui est vide !

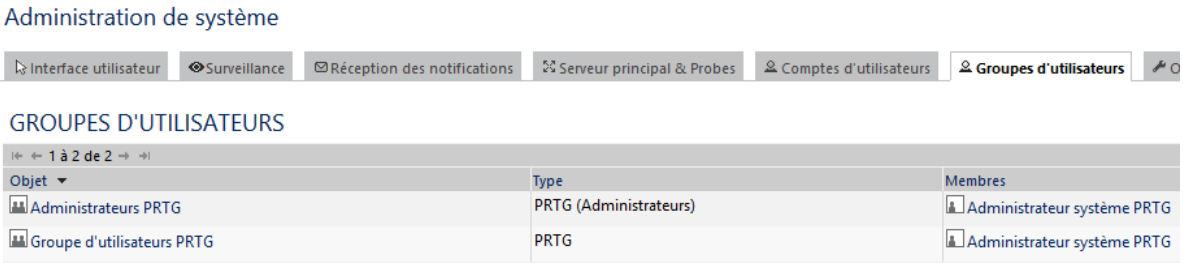


Au plus simple, il suffit de mettre le compte **Administrateur système PRTG** dans le groupe **Groupe d'utilisateurs PRTG**

Dans **Configuration Administration** puis **Système**, **Groupes d'Utilisateurs**



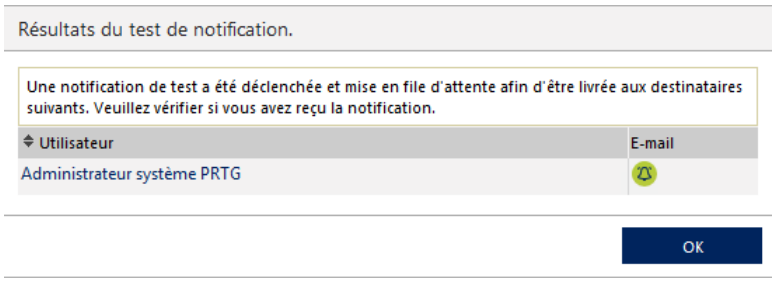
Pour avoir



Test de la notification:

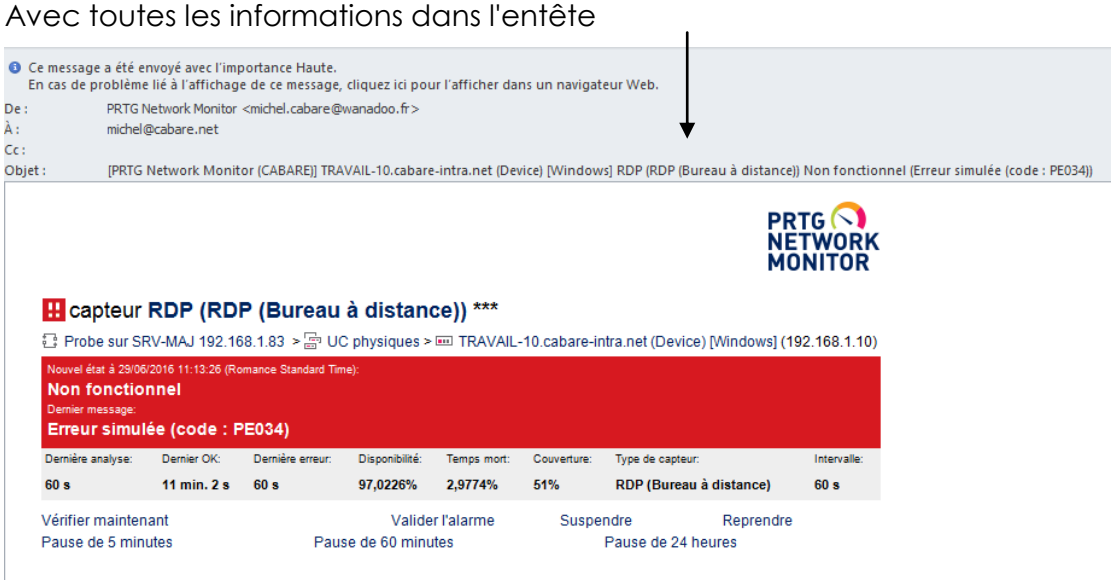
Du coup il est possible de tester, via **Configuration, Paramètres de compte notification**, avec **tester**

Qui donne un message

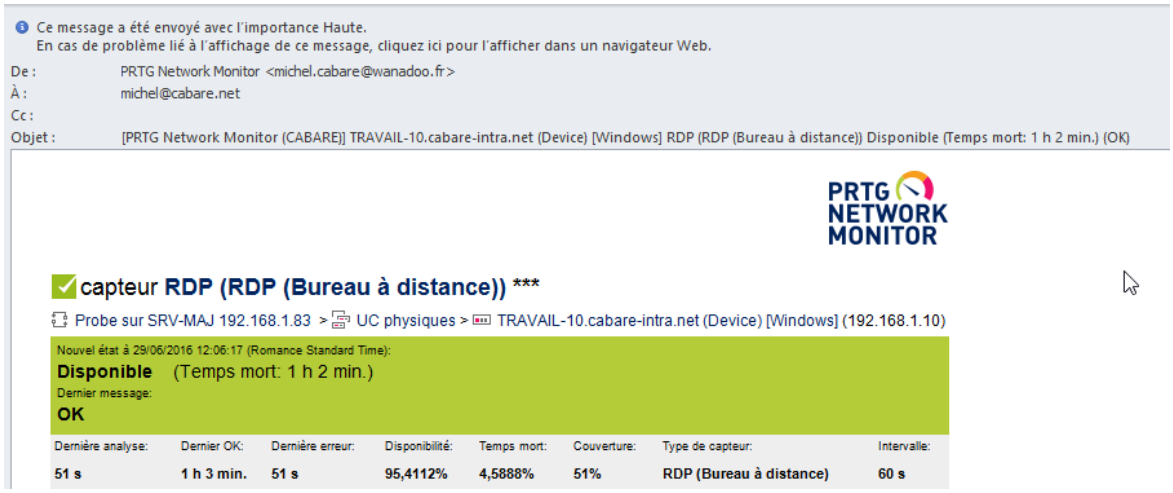


Et pour le destinataire la réception d'un mail

Avec toutes les informations dans l'entête



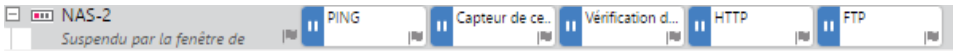
Et lorsque la situation revient normale



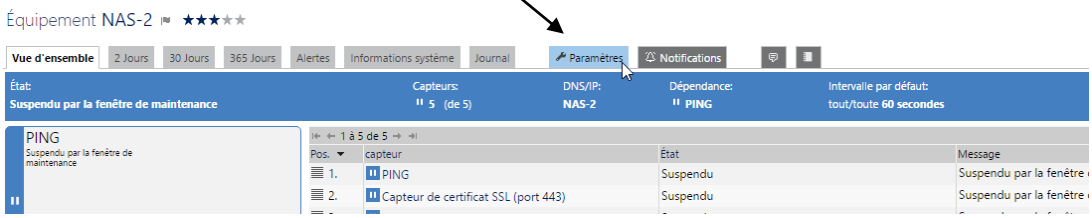
PLANIFICATION SURVEILLANCE CAPTEUR

Utiliser une planification par défaut:

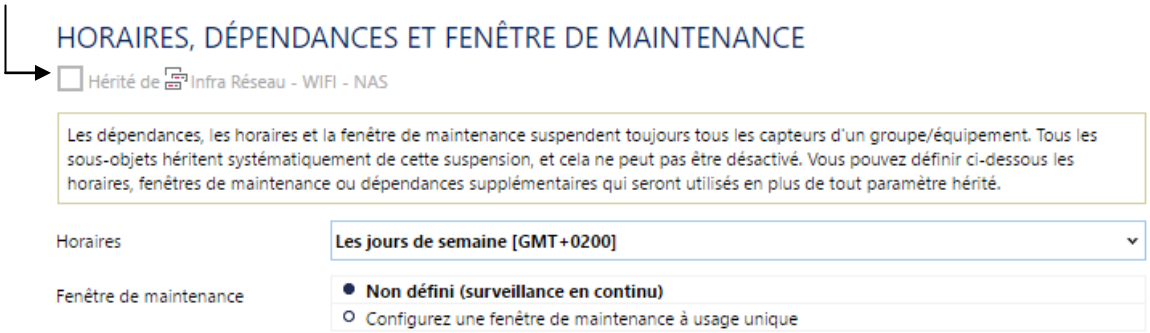
On veut qu'un capteur ne soit armé que pendant une plage horaire, par exemple de 8h du matin à 20h le soir.. C'est le cas de ce ***NAS-2***



Dans les **paramètres**, il faut



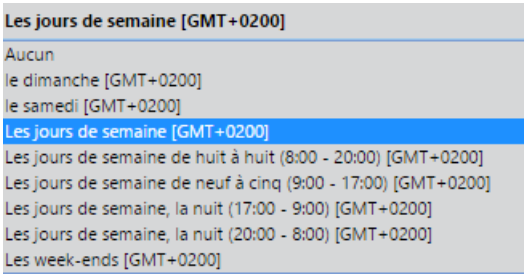
Il faut aller dans la section **Horaires dépendances et fenêtre de maintenance** on décoche l'héritage , et on configure comme on le souhaite



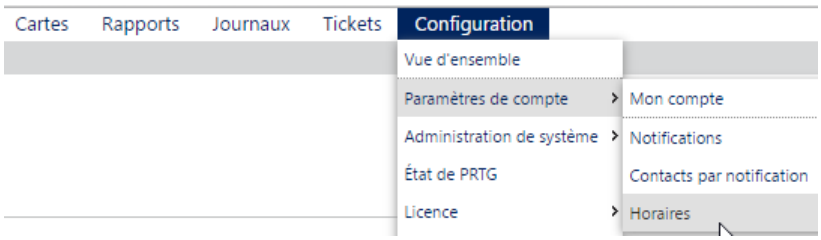
Créer sa planification:

Si les planifications par défaut ne nous conviennent pas,

Par exemple on veut tous les jours de la semaine, y compris le week-end



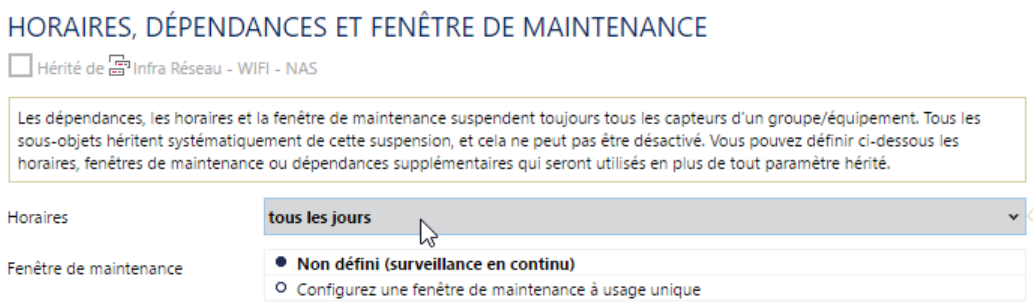
On peut se créer des plages personnalisées dans **Configuration / paramètres de compte / horaires**



On obtient une fenetre dans laquelle on demande **Ajouter un nouvel horaire**,

Et on crée la planification voulue, en la nomant, ici par exemple ***tous les jours***

Elle sera désormais disponible pour notre capteur



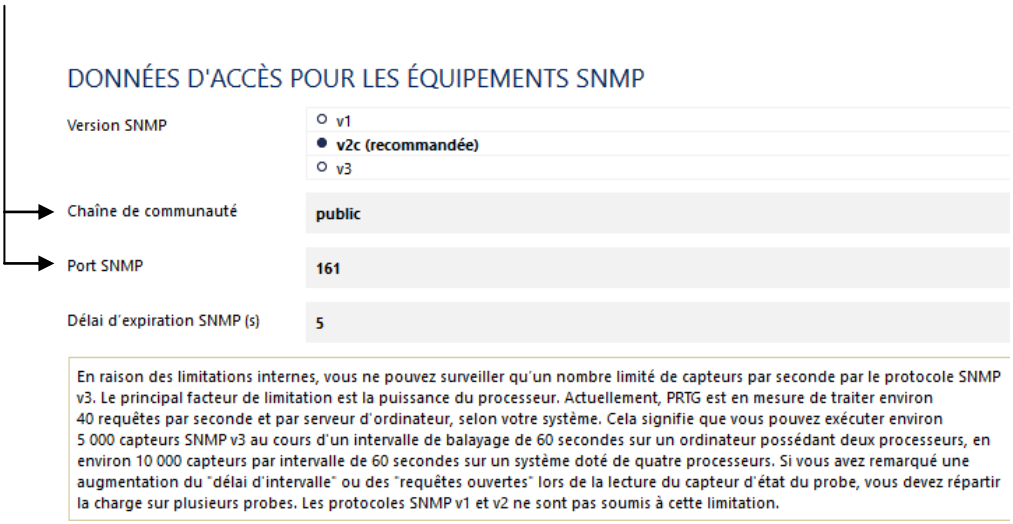
CAPTEUR SNMP

Paramètres snmp de PRTG:

Dans le **groupe principal**, Dans Paramètres, on trouve une section **Données d'accès pour les équipements SNMP**

Avec notamment le nom **de chaine de communauté** ici ***public***

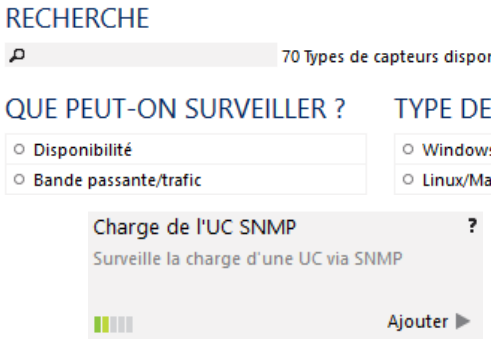
Et le **port SNMP** utilisé par défaut ici ***161***



Ce qui entrainera au cas où cela sera nécessaire que sur un Pare-Feu on laisse passer le **Port UDP** en **161**

70 capteur SNMP (13 windows):

Sur un équipement, on ajoute un capteur SNMP parmis les 70

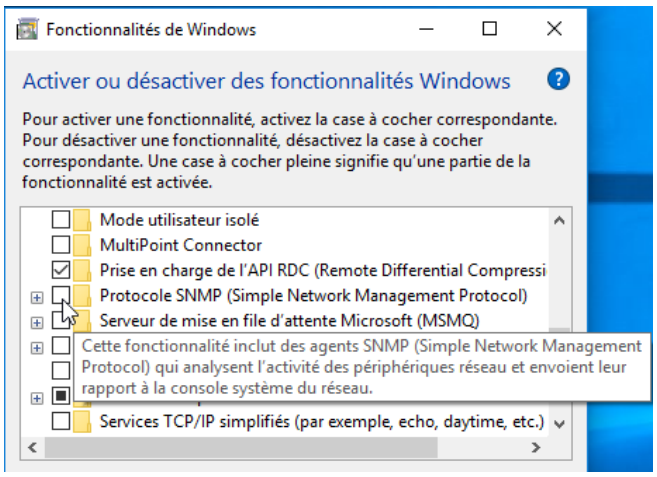


Mais ce capteur peut poser soucis

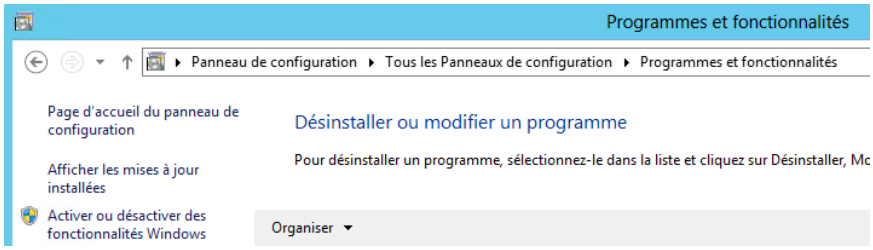
Installer service SNMP sur Windows:

Sur un équipement Windows, le service SNMP n'est pas forcément installé.

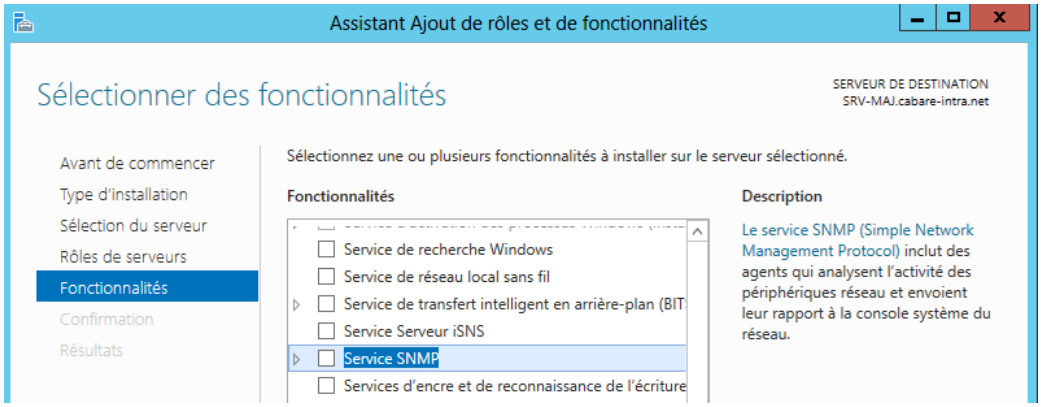
Sur un client Windows on y remédie soit via le panneau de configuration, **programmes et fonctionnalité**s, et on demande dans **Activer ou désactiver des fonctionnalités Windows**



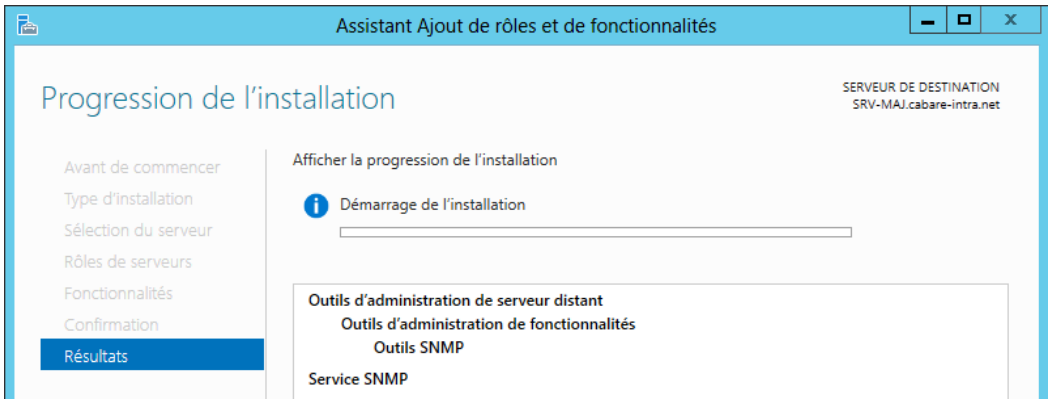
Sur un serveur Windows via le **gestionnaire de serveur en demandant ajouter des rôles et des fonctionnalités**



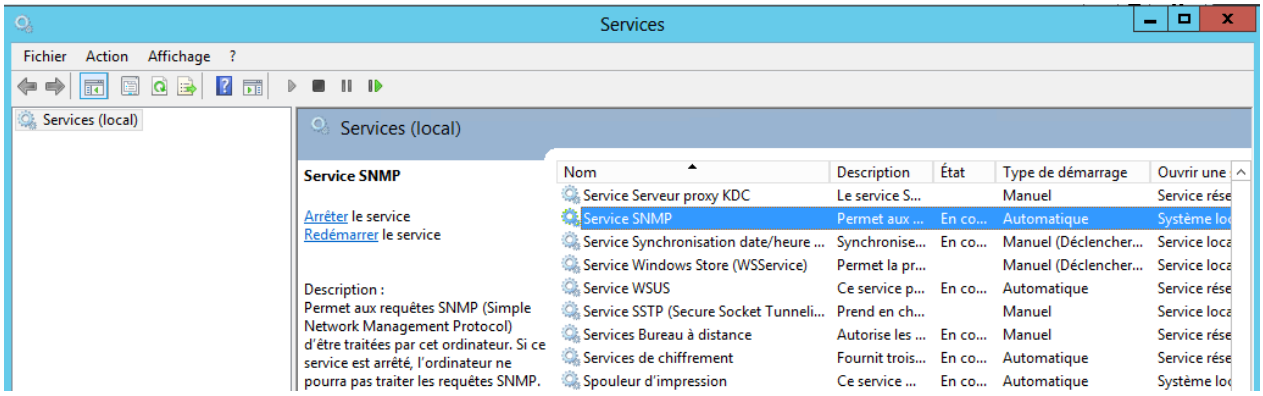
On demande d'ajouter le **service SNMP** (pas confondre avec Serveur SNMP)



et tout ce qui est coché par défaut



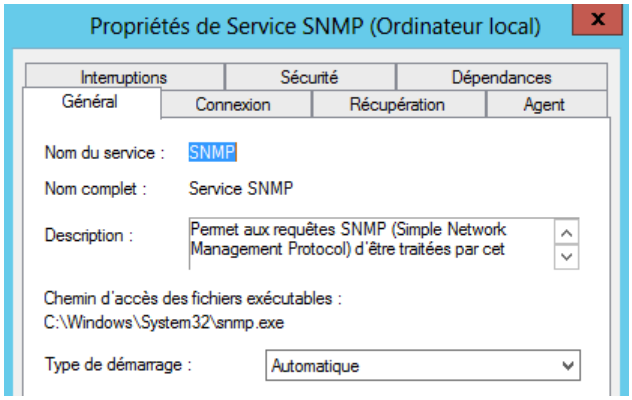
On peut désormais ouvrir le **Service SNMP**



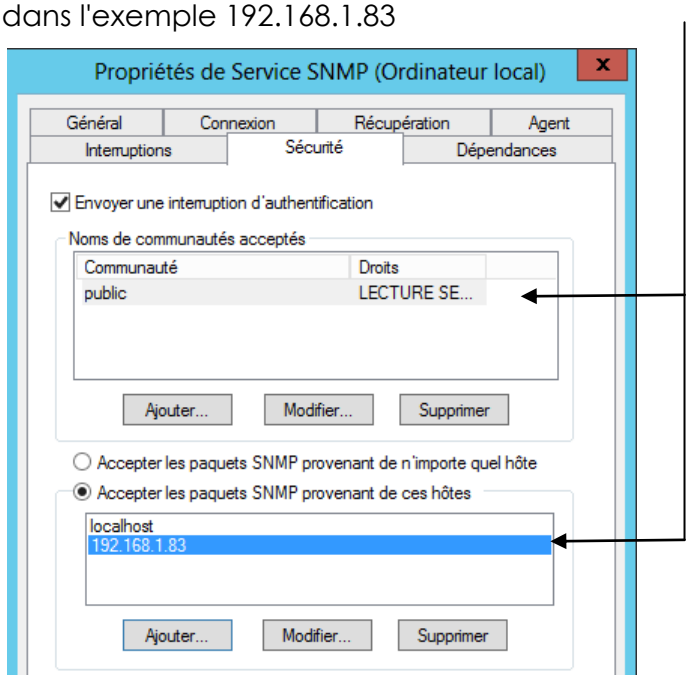
Paramétrer le service SNMP sur Windows:

Dans les **propriétés du service SNMP**,

onglet **Général** on demande un **type de démarrage automatique**



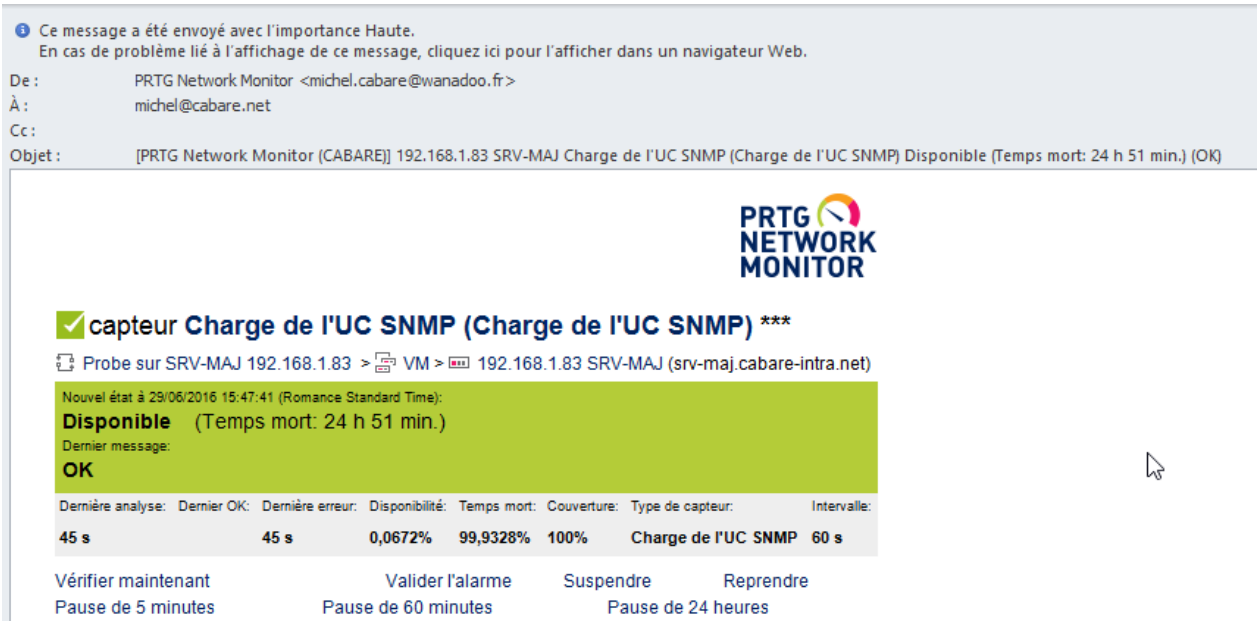
onglet **Sécurité** on saisit le **nom de communauté** , dans l'exemple ***public*** et l'adresse IP de l'agent SNMP autorisé, c'est à dire de la machine qui hébèrge **PRTG** dans l'exemple 192.168.1.83



onglet **Agent** on coche tout

Et on redémmare le service SNMP

On recevra un mail confirmant

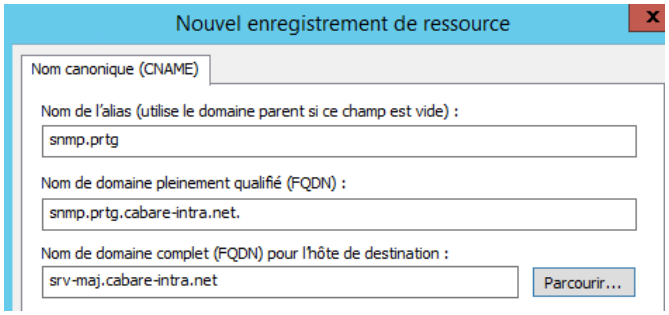


Cas Windows 2012

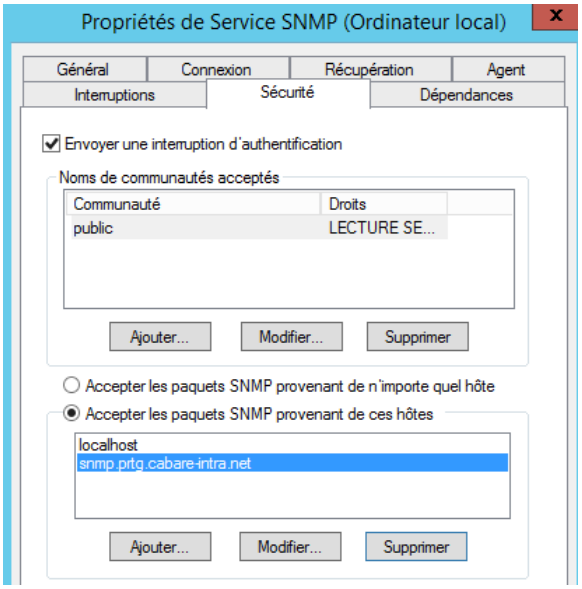
Note: On Windows Server 2012, you might encounter missing Security, Agent, and Traps tabs in SNMP service properties. Please see this article on joshancel.wordpress.com for a workaround. You can also find information about this issue in this Knowledge Base article.

Alias DNS pour hôte serveur snmp

Pour éviter que ne cas de changement d'hebergement sur service snmp, on peut créer un alias dans le DNS, par exemple ***snmp.prtg***



que l'on utilisera dans le paramétrage du service SNMP à la place de l'adresse IP

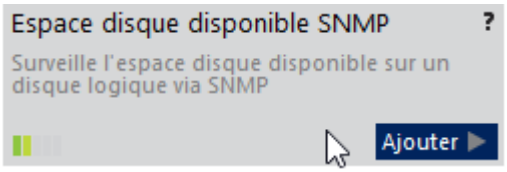


Exemples capteur SNMP disque – mémoire – charge Uc

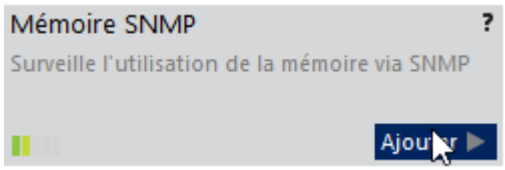
Parmis tous les capteurs PRTG on peut noter

Espace disque disponible SNMP

Attention, tout changement de label, implique une reconstruction du capteur

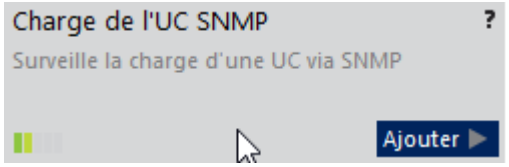


Mémoire SNMP



Il existe un contrôlle identique WMI

Charge UC



Dans les **propriétés du service SNMP**,

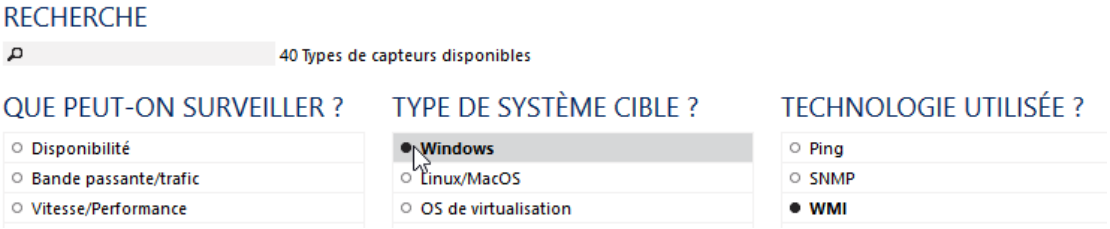
CAPTEUR WMI

Paramètres wmi de PRTG:

Dans le **groupe principal**, Dans Paramètres, on trouve une section **Données d'accès pour les équipements WMI**

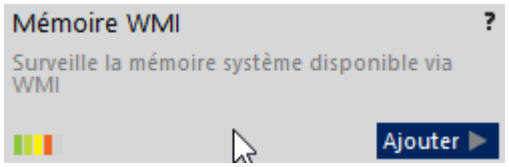
40 capteur WMI disque – mémoire – charge Uc – Hyper-V

Parmis tous les capteurs WMI on peut noter



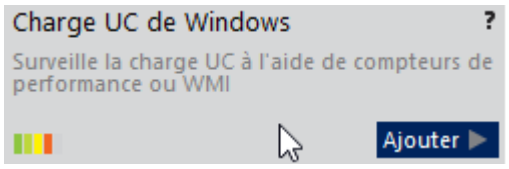
Capacité du disque WMI

Mémoire WMI



Il existe un contrôlle identique WMI

Charge UC



Serveur Hôte Hyper-V et Machine Virtuelle Hyper-V

Erreur accès wmi:

Il se peut qu'un capteur utilisant WMI ai des problèmes

Les messages d'erreurs pouvant être nombreux et variés…, Il faut vérifier:

- Adhésion au domaine et accès avec login administrateur tel que celui définit dans le capteur
- Pas de pare-feu ou de logiciels spécifiques de filtrage réseau
- The **RPC server** used for WMI on the target computer is running on the **port** specified in PRTG (135 by default).
- Vérification du Nom DNS, de l'adresse IP, via nslookup
- Vérification RPC autorisé via la valeur Y de la clé de la base de registre

  HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Ole

  Valeur de la clé nécessaire = **enableDCOM = Y**
- Désactivation de l'UAC pour les accès disques distant. (idem accès partages administratifs). Via la clé de la base de registre

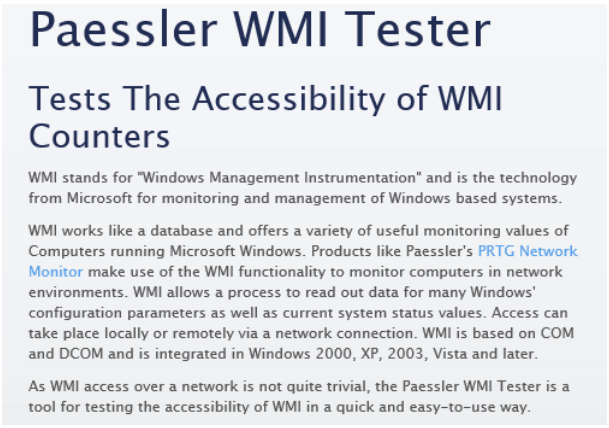
  HKEY_LOCAL_MACHINE
  \SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

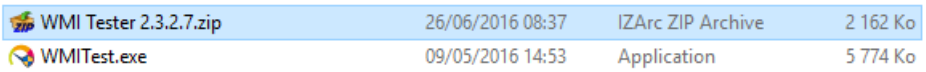
  Ajouter une clé **Dword** nommée **LocalAccountTokenFilterPolicy** Value: **1**

  http://support.microsoft.com/kb/951016

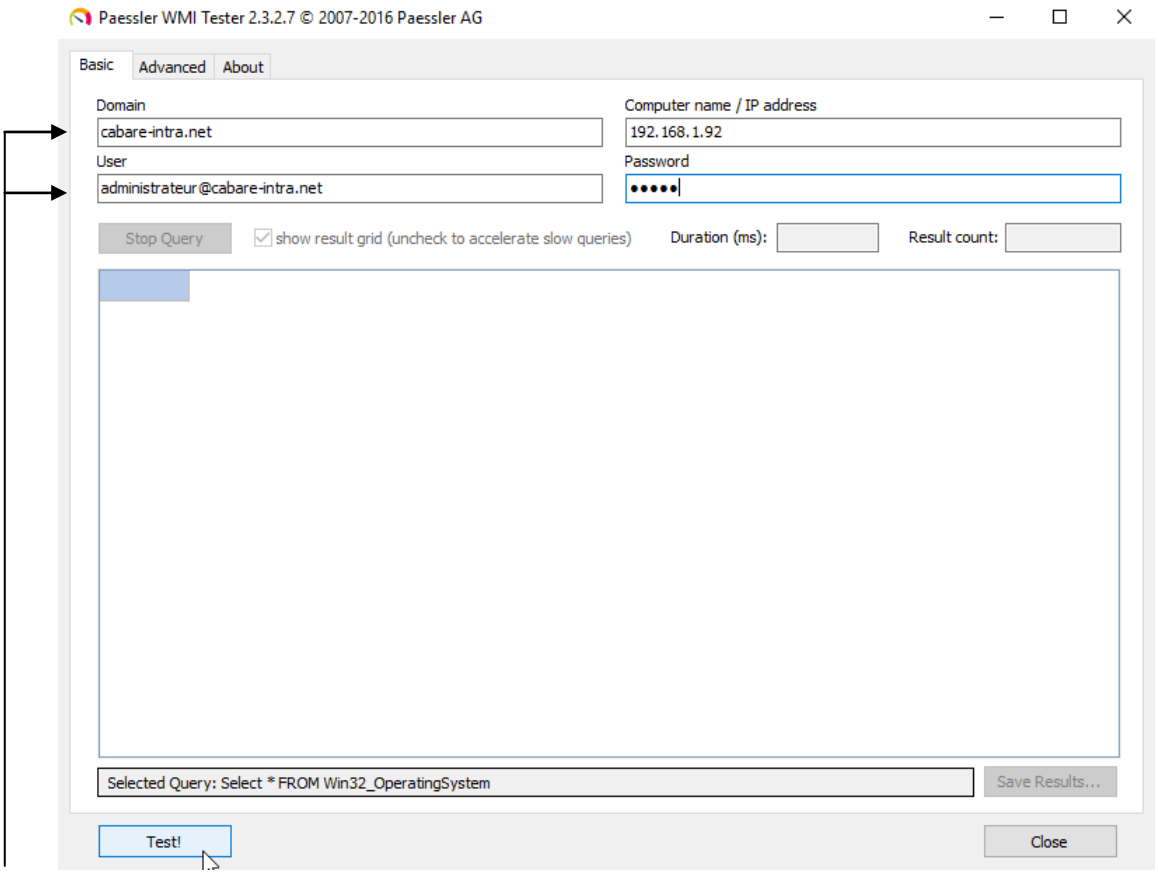
Paessler wmi tester:

On peut récupérer en téléchargement un outil





Lorqu'on le lance, on obtient



Il faut renseigner au minimum

- **Target computer IP address**
- **Domain**: the Windows domain containing the computer you want to test, or the computer name if not running inside of a domain.
- **User**: the name of a user with login credentials for the target machine
- **Password**: the user's password

N.B: Si on teste la machine locale (sur laquelle on est) on laisse les champs vides.

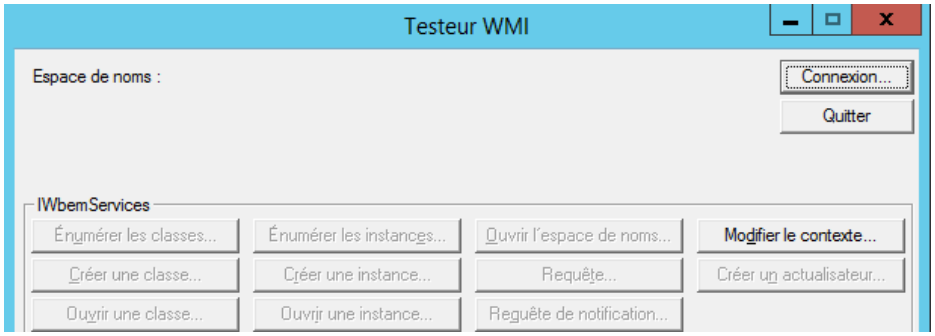
Outil wbemtest windows:

Nativement sur une machine windows on peut lancer un utilitaire de test wmi nommé **wbemtest**

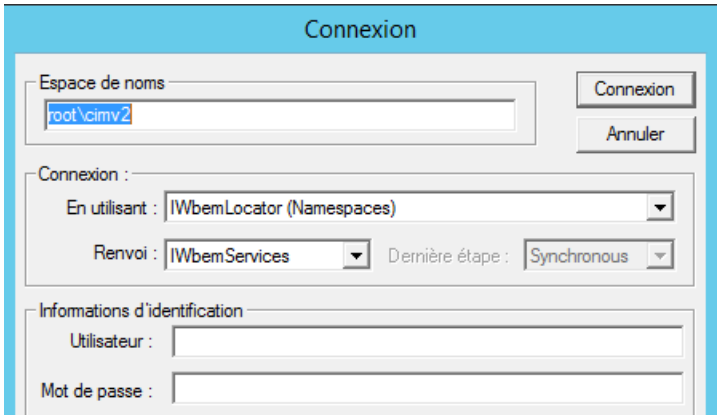
```
C:\Windows\system32>wbemtest
```

WMI sur la machine locale

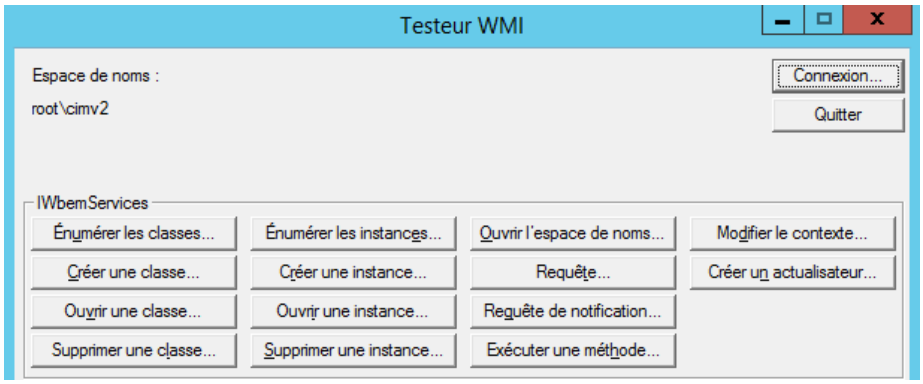
Cela permet de savoir sir WMI est opérationnel sur la machine en question, simplement par une demande de **Connexion…**



Avec les paramètres par défaut



Si cela fonctionne,



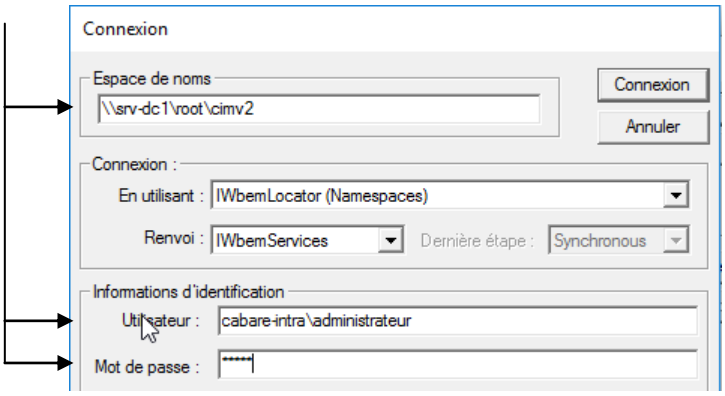
cela veut dire que WMI est opérationnel sur la machine

WMI sur la machine à distance

Pour vérifier l'accès distant aux ressources WMI d'une machine on part d'un poste windows sur lequel on execute **wbemtest**

Sauf que lors de la demande de connexion, on va demander

Le ***nom de la machine distante***, avec un ***login de domaine***



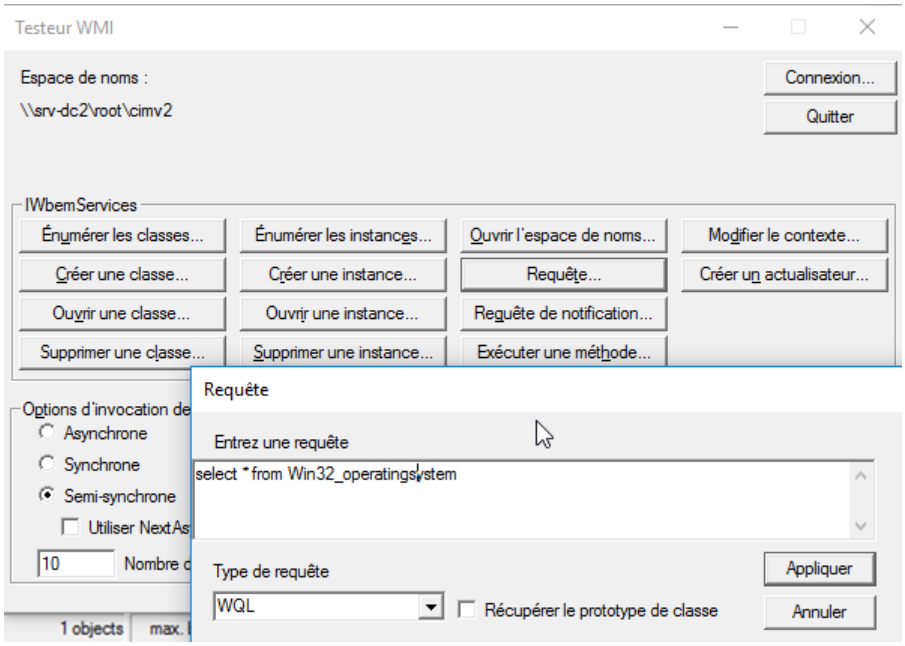
Executer une requête

Il s'agit juste de voir si l'on a accès aux primitives WMI…

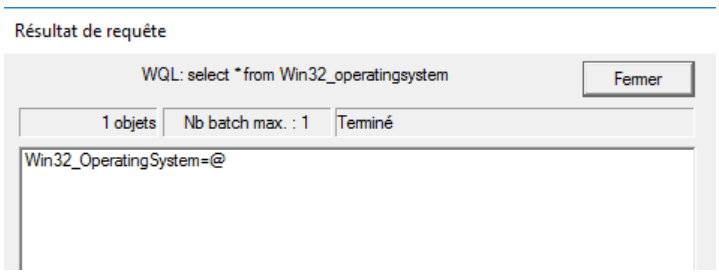
On demande **Requête…** puis on demande une requête du genre

select * from Win32_operatingsystem

comme dans la capture ci dessous



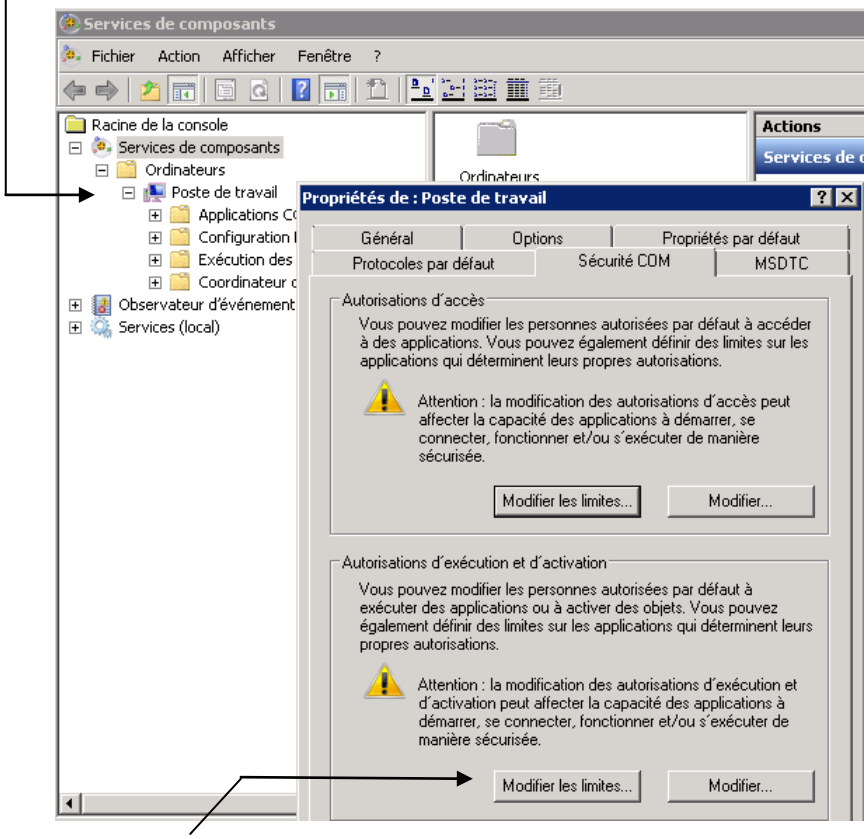
Si on obtient un résultat, et pas un message d'erreur, c'est que l'on a acès à WMI



DCOM sur Contrôleurs de domaine - dcomcnfg:

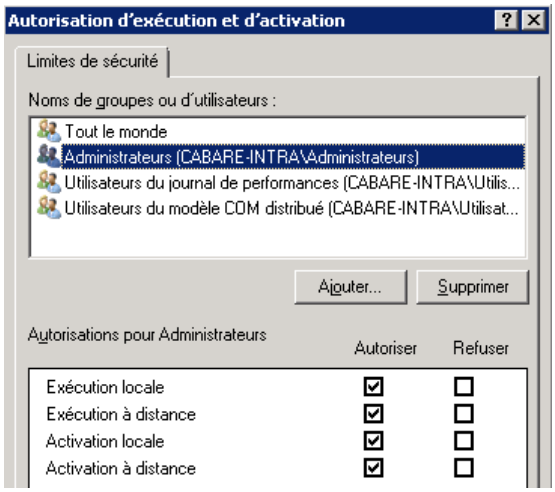
1. Login sur le Domain Controller
2. Executer **dcomcnfg**

   dans **Services de composants** / **Ordinateurs / Poste de travail** on demande les **Propriétés** onglet **Sécurité COM**



Demander **Modifier les limites** dans **Autorisations d'execution et d'activation**

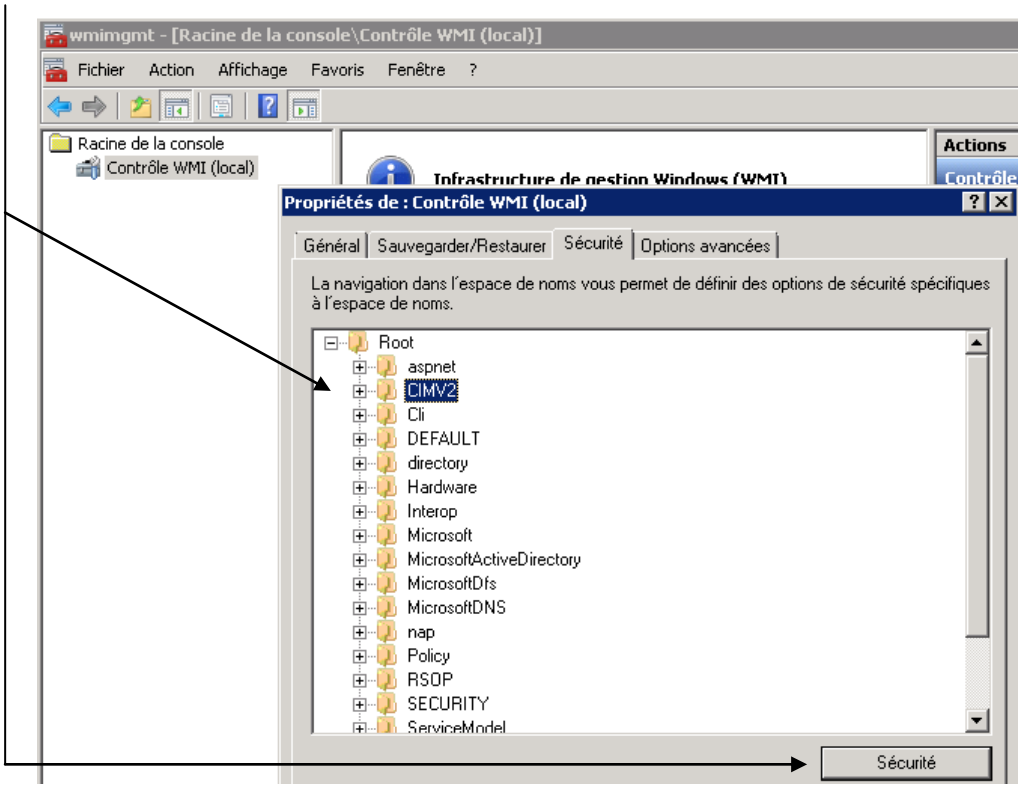
Vérifier que l'on ait bien



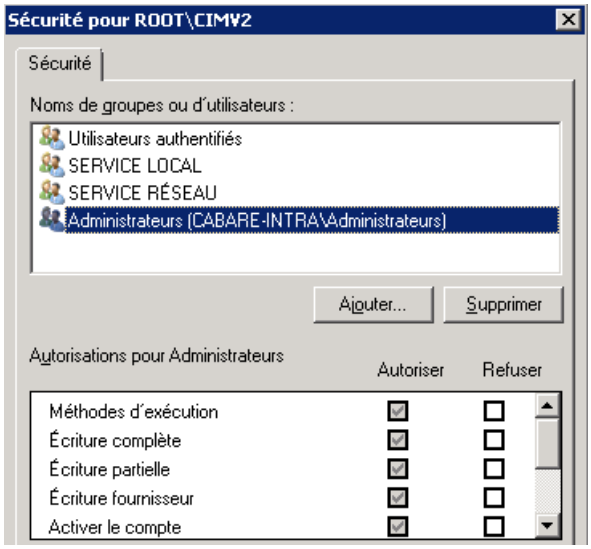
WMI sur Contrôleurs de domaine – wmimgmt.msc:

1. Login sur le Domain Controller
2. Executer **"wmimgmt.msc"**

   dans **Contrôle WMI** on demande les **Propriétés** onglet **Sécurité** on se place sur CIMV2 et on demande **Sécurité**



Vérifier que l'on ait bien



CAPTEUR POWERSHELL

winrmParamètres powershell de PRTG:

Sur le Probe il faut

- FrameWork Net .40 ou plus
- Powershell 2.0 sur le probe
- Remote Powershell Activé
- Authentification Windows

Test client disponibilité Powershell

Démarrer **Windows powershell**

Vérifier si l'exécution des scripts est activée par

get-Executionpolicy

```
PS C:\Users\Administrateur.CABARE-INTRA> get-Executionpolicy
Restricted
```

Le cas échéant activer Windows powershell par

get-Executionpolicy Unrestricted

```
PS C:\Users\Administrateur.CABARE-INTRA> Set-ExecutionPolicy Unrestricted

Modification de la stratégie d'exécution
La stratégie d'exécution permet de vous prémunir contre les scripts que vous
jugez non fiables. En modifiant la stratégie d'exécution, vous vous exposez aux
 risques de sécurité décrits dans la rubrique d'aide about_Execution_Policies.
Voulez-vous modifier la stratégie d'exécution ?
[O] Oui  [N] Non  [S] Suspendre  [?] Aide (la valeur par défaut est « O ») : o
```

Vérifier que le Service WinRm est lancé par

get-service winrm

```
PS C:\Users\Administrateur.CABARE-INTRA> get-service winrm

Status   Name               DisplayName
------   ----               -----------
Running  winrm              Gestion à distance de Windows (Gest..
```

Que la version est la bonne par

$psversiontable

```
PS C:\Users\Administrateur.CABARE-INTRA> $psversiontable

Name                           Value
----                           -----
CLRVersion                     2.0.50727.5485
BuildVersion                   6.1.7601.17514
PSVersion                      2.0
WSManStackVersion              2.0
PSCompatibleVersions           {1.0, 2.0}
SerializationVersion           1.1.0.1
PSRemotingProtocolVersion      2.1
```

Que l'on accepte les connexions à distance par

Enable-PSRemoting –force

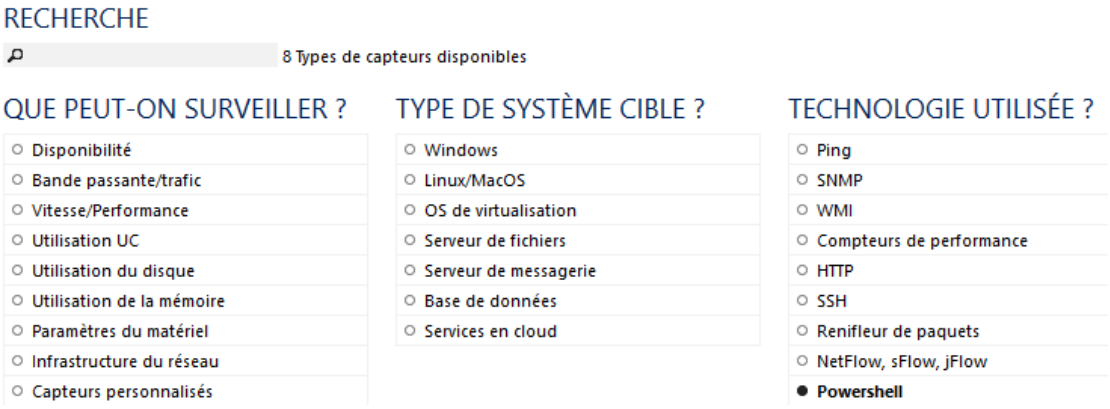
```
PS C:\Users\Administrateur.CABARE-INTRA> enable-PSRemoting -force
WinRM est déjà configuré pour recevoir des demandes sur cet ordinateur.
WinRM a été mis à jour pour la gestion à distance.
écouteur WinRM créé sur HTTP://* pour accepter les demandes de la gestio
e cet ordinateur.
Exception de pare-feu WinRM activée.
```

To enable authentication, you need to add the remote computer to the list of trusted hosts for the local computer in WinRM. To do so, type: **winrm s winrm/config/client '@{TrustedHosts="RemoteComputer"}'** Here, RemoteComputer should be the name of the remote computer, such as:
winrm s winrm/config/client '@{TrustedHosts="CorpServer56"}

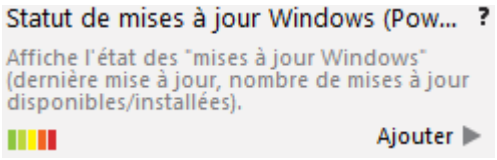
winrm quickconfig

This command analyzes and configures the WinRM service.

8 capteurs powershell - statut des mises à jour



Statut des mises à jour Windows

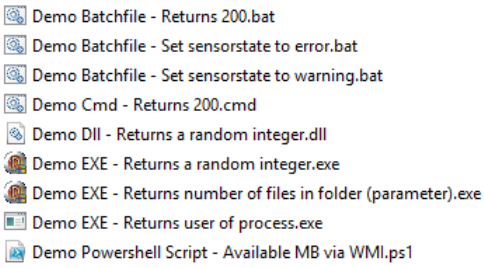


CAPTEUR A BASE DE SCRIPT

Emplacement des capteurs :

Lorsque **Prtg** est installé par défaut, les capteurs sont stockées dans **C:\Program Files (x86)\PRTG Network Monitor\Custom Sensors\EXE**

Et dans le dossier **EXE** il y a un certain nombre de fichier de démo

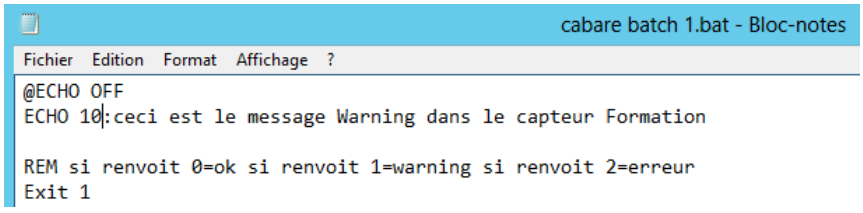


Premier script batch:

On demande de créer un capteur **script/EXE**

Associé à un fichier .batch stocké dans le dossier **C:\Program Files (x86)\PRTG Network Monitor\Custom Sensors\EXE**

Par exemple ***cabare batch 1.bat*** contenant



Les valeurs de retour sont:

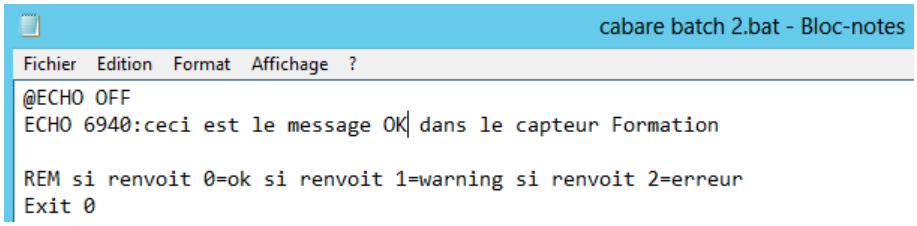
- 0=ok
- 1 = warning
- 2 = erreur

Le message c'est le dernier message envoyé par le script: précédé de la valeur du canal (ici dans l'exemple 10)

Donc

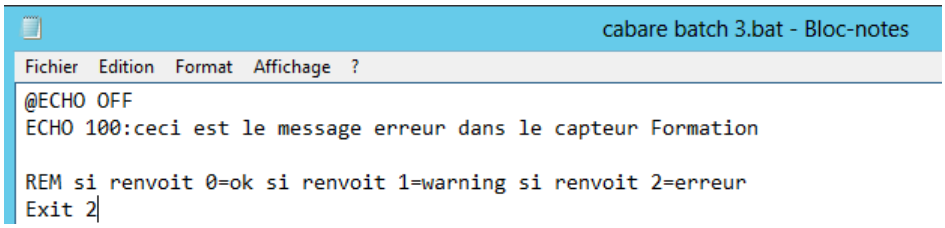
Son execution renvoit bien la valeur **10** et un **warning**…

Et donc



Renverrait

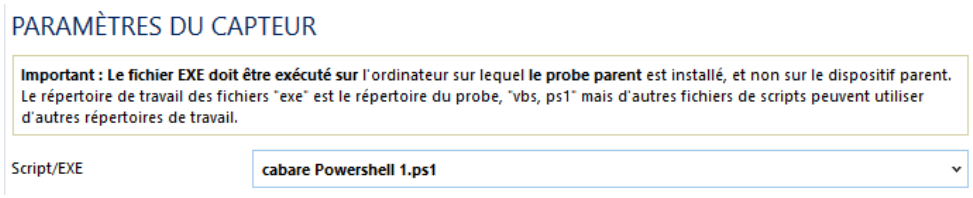
Alors que



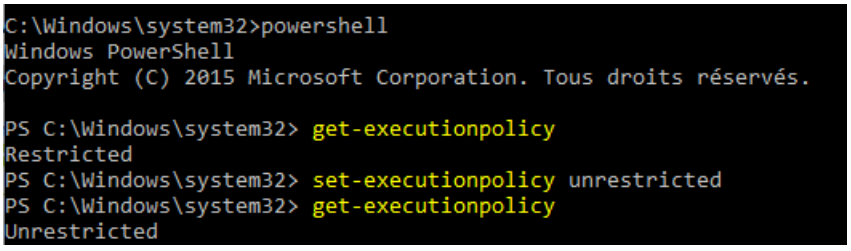
Renvoit

Premier script powershell:

On demande de créer un capteur **script/EXE**

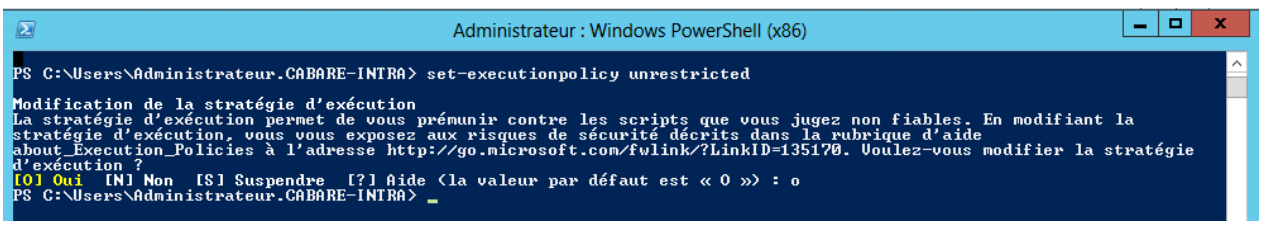


Il faut bien sur autoriser l'execution des scripts sur le poste sur lequel Prtg est installé avec un **Set-executionpolicy unrestricted**



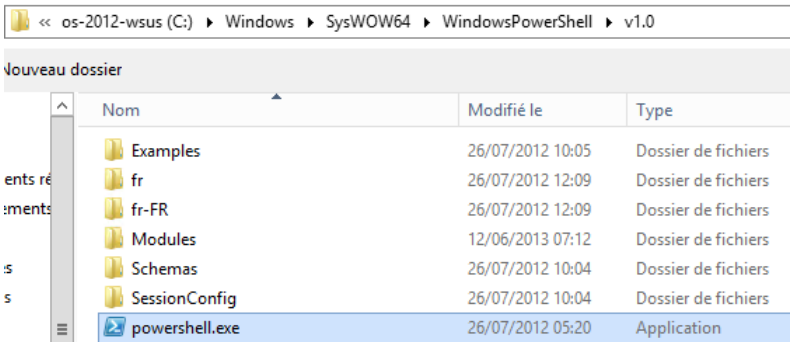
N.B: si on est sur un serveur 64bits, il faut egalement le faire pour le Powershell 32bits, qui est le powershell utilisé par Prtg,

donc dans Windows Powershell (x86) on execute egalement la même commande



N.B: Pour lancer powershell 32bits IE x86 on, peut executer la commande
%SystemRoot%\syswow64\WindowsPowerShell\v1.0\powershell.exe

Correpondant à



En effet

PowerShell Executables File System Locations on 64-bit Windows

The default paths to the executables for PowerShell and PowerShell ISE on relevant **64-bit** Windows operating systems:

32-bit (x86) PowerShell executable	**%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe**
64-bit (x64) Powershell executable	**%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe**
32-bit (x86) Powershell ISE executable	**%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe**
64-bit (x64) Powershell ISE executable	**%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell_ise.exe**

Et

PowerShell Executables File System Locations on 32-bit Windows

The default paths to the executables for PowerShell and PowerShell ISE on relevant **32-bit** Windows operating systems:

32-bit (x86) PowerShell executable	**%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe**
32-bit (x86) Powershell ISE executable	**%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell_ise.exe**

Puis

```
PS C:\Windows\system32> get-service winrm

Status   Name               DisplayName
------   ----               -----------
Stopped  winrm              Gestion à distance de Windows (Gest...
```

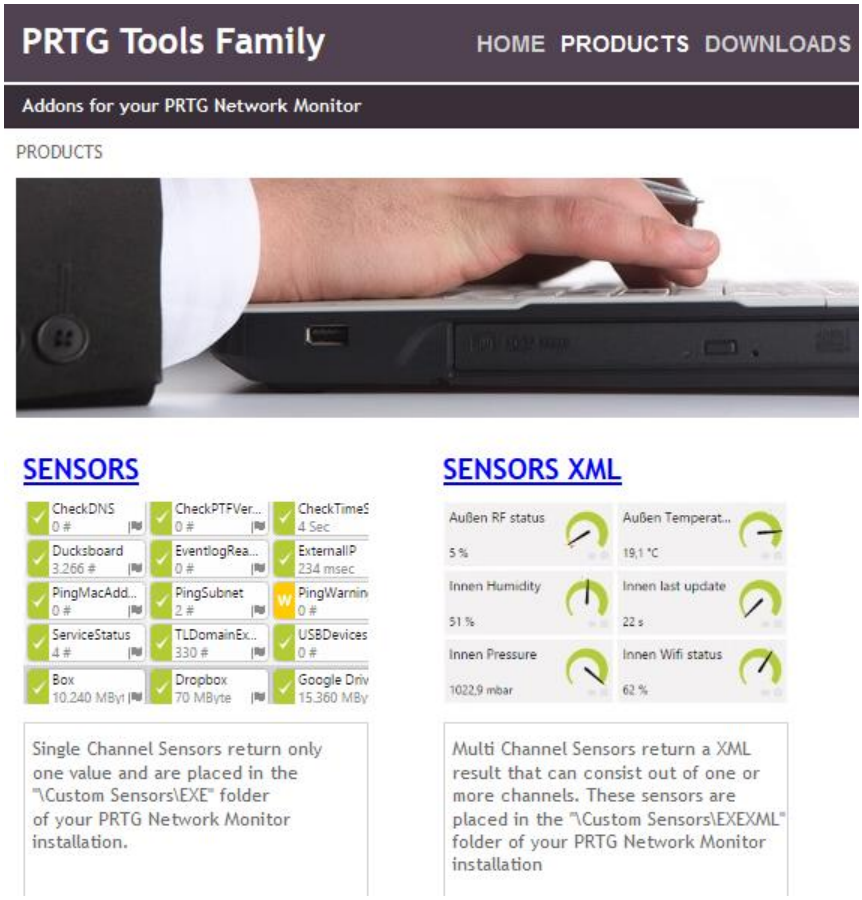
```
PS C:\Windows\system32> enable-psremoting
WinRM a été mis à jour pour recevoir des demandes.
Le type du service WinRM a été correctement modifié.
Le service WinRM a démarré.

WinRM a été mis à jour pour la gestion à distance.
Écouteur WinRM créé sur HTTP://* pour accepter les demandes de la gestion des services Web
 cet ordinateur.
Exception de pare-feu WinRM activée.
```

CAPTEUR SUPPLEMENTAIRE

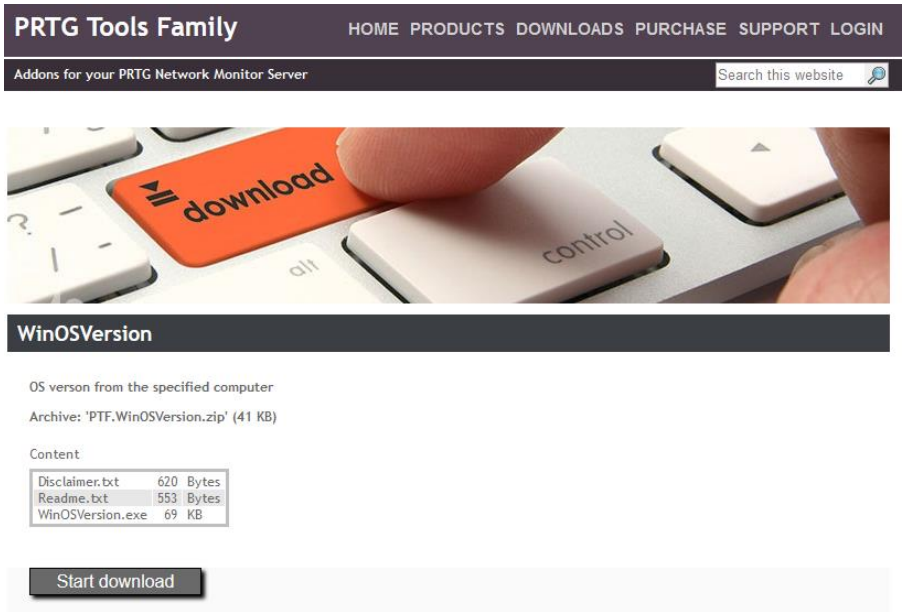
Trouver un capteur :

On a la possibilité de chercher des capteurs supplémentaires,

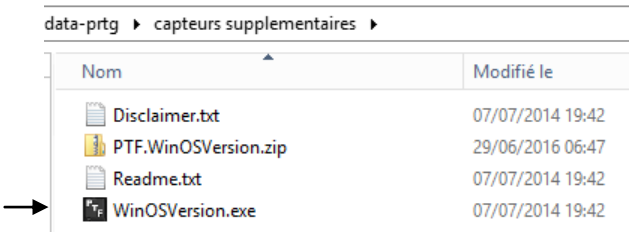


qui pour être utilisés doivent simplement être placés dans le bon dossier

on récupère par exemple un capteur qui donne la version de Windows

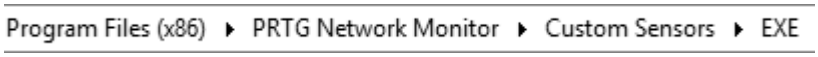


Et on récupère un capteur **WinOSversion.exe**



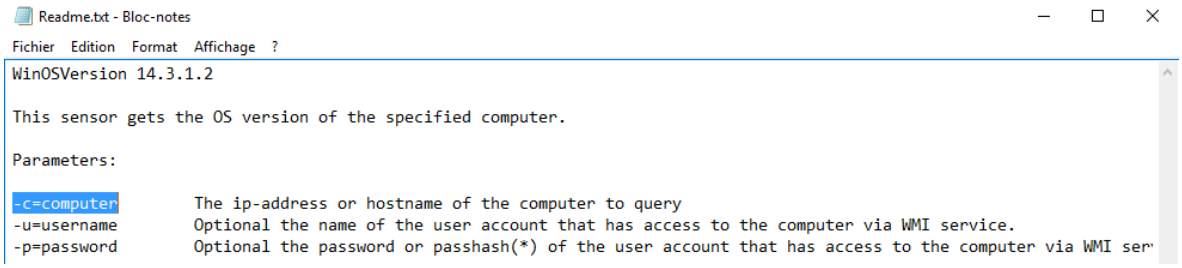
Installer un capteur Script/EXE:

Et on le colle pour celui-ci dans le dossier



Puis on ajoute un capteur de type **Script/EXE**

Dans lequel il faut aller choisir notre executable, et indiquer les paramètres dont il a besoin. Paramètres qui sont indiqués dans le fichier readme.txt livrés avec le capteur, par exemple ici



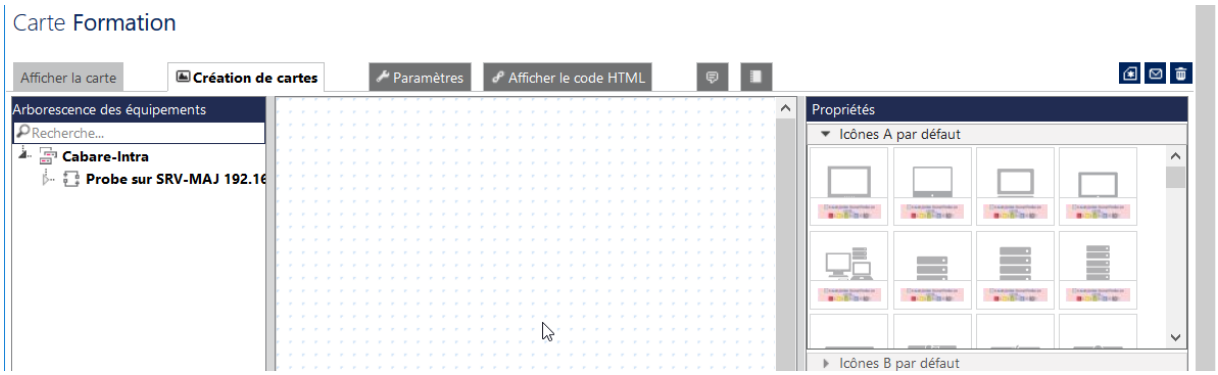
Donc cela donnerait

CARTE

Création d'une carte:

Pour créer une nouvelle carte on demande **carte** un assistant de déclenche, on donne un nom et une taille principalement

Puis avec **Continuer** on obtient



On y trouve :

Les éléments de PRTG des icones

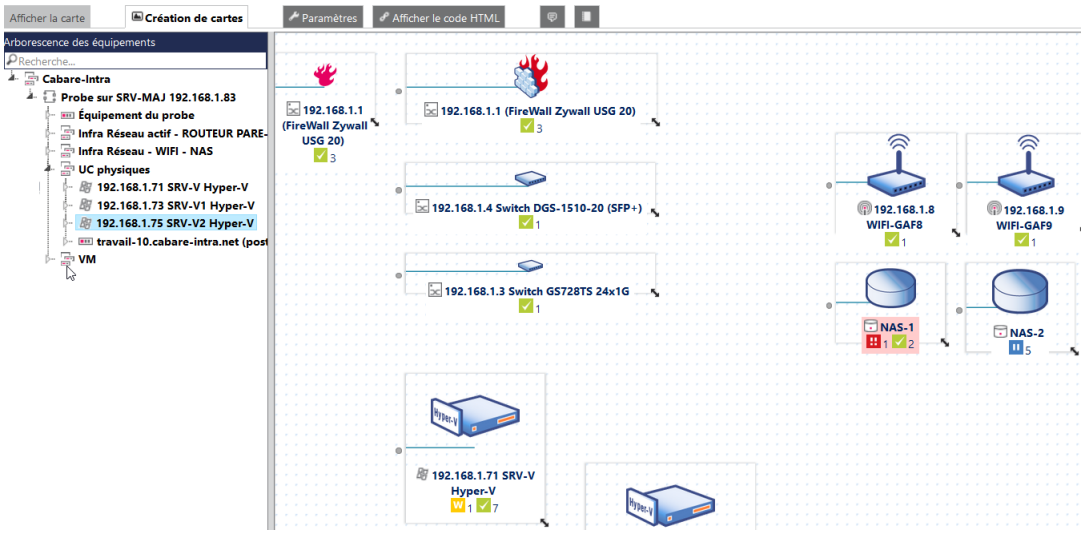
Selon notre configuration soit dynamiques avec capteurs

Soit statiques (illustratives)

Poser des icônes :

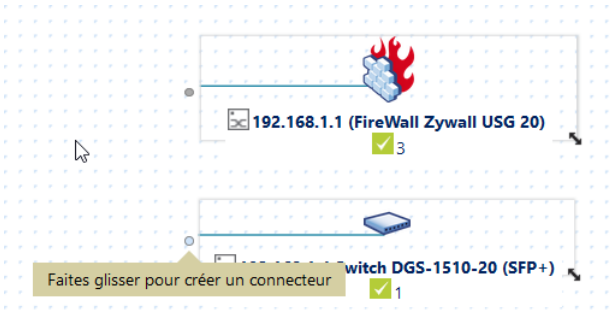
Pour créer une nouvelle carte on demande **carte** un assistant de déclenche, on donne un nom et une taille principalement

On pose les icones dynamique que l'on souhaite de manière à obtenir un graphique général

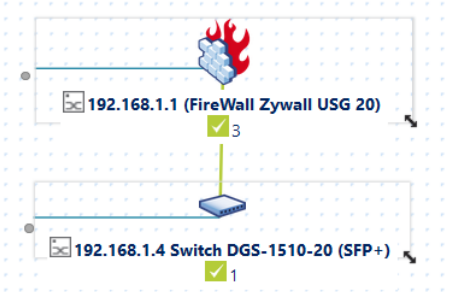


Lier des icônes :

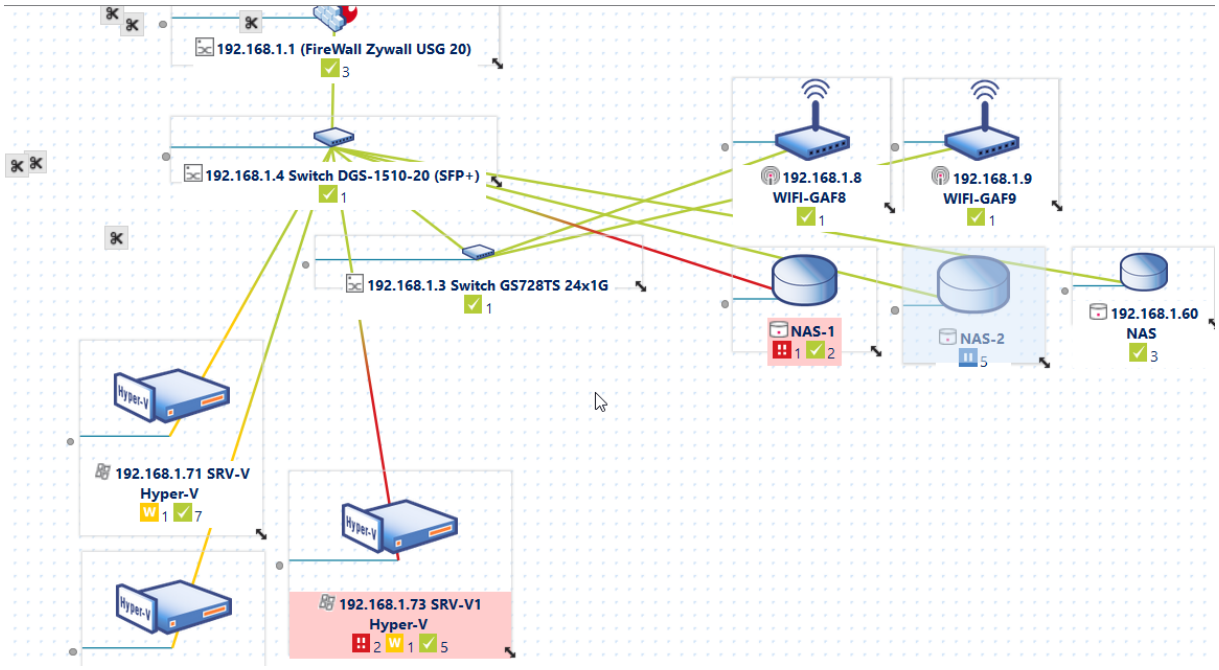
Il suffit avec la souris de faire glisser le point d'ancrage vers l'éléments souhaité



Pour obtenir

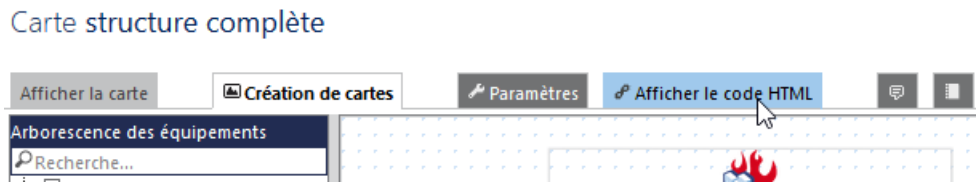


N.B : pour supprimer la liaison il suffira de sélectionner l'icone ciseaux du point d'accroche, et cliquer dessus

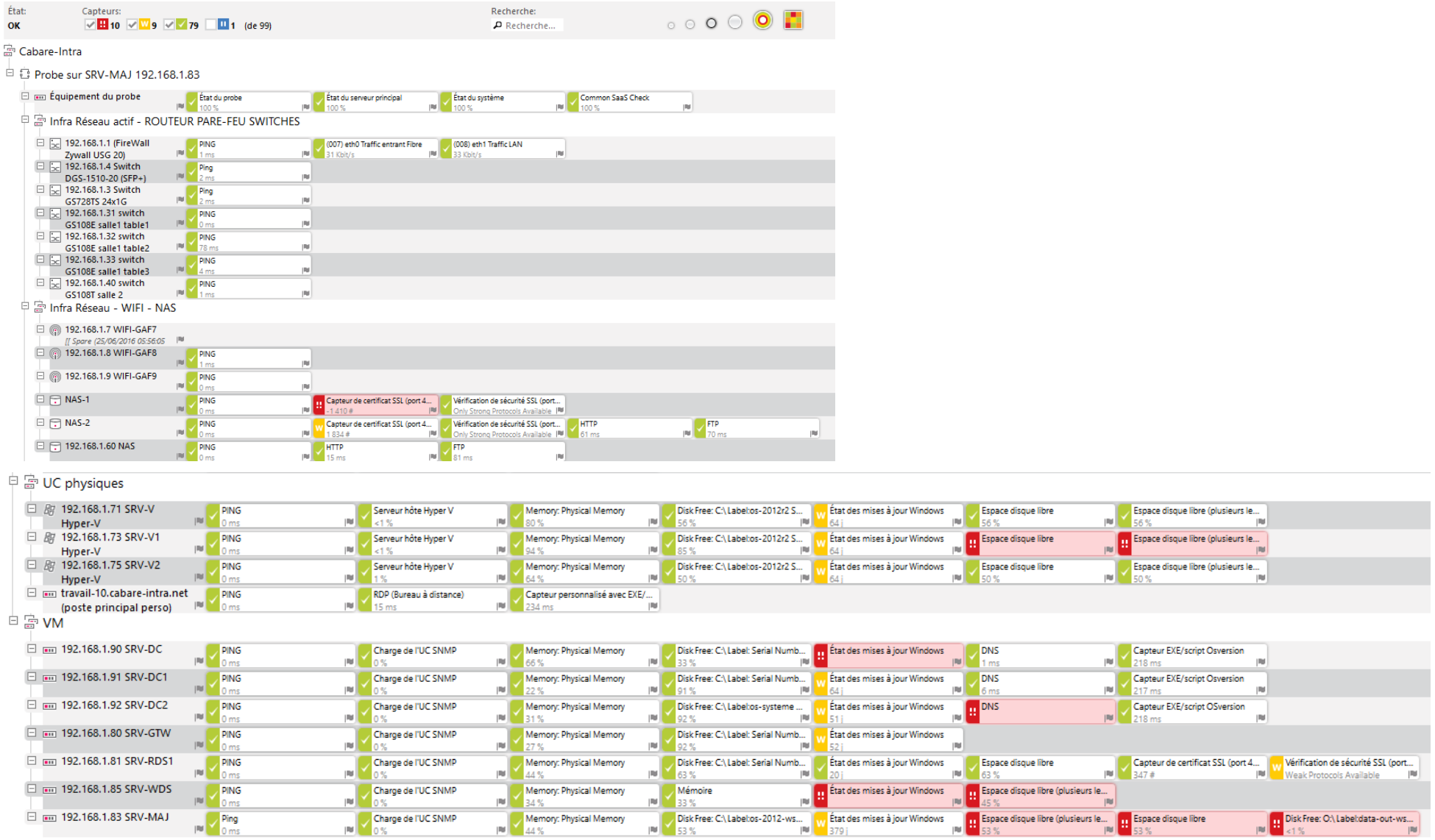


Publier une carte:

Il faut demandr Afficher le code HTML et on choisit



Et on choisit


État:
OK
Capteurs:
10 9 79 1 (de 99)
Recherche:
Recherche...
Cabare-Intra
Probe sur SRV-MAJ 192.168.1.83
Équipement du probe
État du probe 100 %
État du serveur principal 100 %
État du système 100 %
Common SaaS Check 100 %
Infra Réseau actif - ROUTEUR PARE-FEU SWITCHES
192.168.1.1 (FireWall Zywall USG 20)
PING 1 ms
(007) eth0 Traffic entrant Fibre 31 Kbit/s
(008) eth1 Traffic LAN 33 Kbit/s
192.168.1.4 Switch DGS-1510-20 (SFP+)
Ping 2 ms
192.168.1.3 Switch GS728TS 24x1G
Ping 2 ms
192.168.1.31 switch GS108E salle1 table1
PING 0 ms
192.168.1.32 switch GS108E salle1 table2
PING 78 ms
192.168.1.33 switch GS108E salle1 table3
PING 4 ms
192.168.1.40 switch GS108T salle 2
PING 1 ms
Infra Réseau - WIFI - NAS
192.168.1.7 WIFI-GAF7
[[Spare (25/06/2016 05:56:05
192.168.1.8 WIFI-GAF8
PING 1 ms
192.168.1.9 WIFI-GAF9
PING 0 ms
NAS-1
PING 0 ms
Capteur de certificat SSL (port 4... -1 410 #
Vérification de sécurité SSL (port... Only Strong Protocols Available
NAS-2
PING 0 ms
Capteur de certificat SSL (port 4... 1 834 #
Vérification de sécurité SSL (port... Only Strong Protocols Available
HTTP 61 ms
FTP 70 ms
192.168.1.60 NAS
PING 0 ms
HTTP 15 ms
FTP 81 ms
UC physiques
192.168.1.71 SRV-V Hyper-V
PING 0 ms
Serveur hôte Hyper V <1 %
Memory: Physical Memory 80 %
Disk Free: C:\ Label:os-2012r2 S... 56 %
État des mises à jour Windows 64 j
Espace disque libre 56 %
Espace disque libre (plusieurs le... 56 %
192.168.1.73 SRV-V1 Hyper-V
PING 0 ms
Serveur hôte Hyper V <1 %
Memory: Physical Memory 94 %
Disk Free: C:\ Label:os-2012r2 S... 85 %
État des mises à jour Windows 64 j
Espace disque libre
Espace disque libre (plusieurs le...
192.168.1.75 SRV-V2 Hyper-V
PING 0 ms
Serveur hôte Hyper V 1 %
Memory: Physical Memory 64 %
Disk Free: C:\ Label:os-2012r2 S... 50 %
État des mises à jour Windows 64 j
Espace disque libre 50 %
Espace disque libre (plusieurs le... 50 %
travail-10.cabare-intra.net (poste principal perso)
PING 0 ms
RDP (Bureau à distance) 15 ms
Capteur personnalisé avec EXE/... 234 ms
VM
192.168.1.90 SRV-DC
PING 0 ms
Charge de l'UC SNMP 0 %
Memory: Physical Memory 66 %
Disk Free: C:\ Label: Serial Numb... 33 %
État des mises à jour Windows
DNS 1 ms
Capteur EXE/script Osversion 218 ms
192.168.1.91 SRV-DC1
PING 0 ms
Charge de l'UC SNMP 0 %
Memory: Physical Memory 22 %
Disk Free: C:\ Label: Serial Numb... 91 %
État des mises à jour Windows 64 j
DNS 6 ms
Capteur EXE/script Osversion 217 ms
192.168.1.92 SRV-DC2
PING 0 ms
Charge de l'UC SNMP 0 %
Memory: Physical Memory 31 %
Disk Free: C:\ Label:os-systeme ... 92 %
État des mises à jour Windows 51 j
DNS
Capteur EXE/script OSversion 218 ms
192.168.1.80 SRV-GTW
PING 0 ms
Charge de l'UC SNMP 0 %
Memory: Physical Memory 27 %
Disk Free: C:\ Label: Serial Numb... 92 %
État des mises à jour Windows 52 j
192.168.1.81 SRV-RDS1
PING 0 ms
Charge de l'UC SNMP 0 %
Memory: Physical Memory 44 %
Disk Free: C:\ Label: Serial Numb... 63 %
État des mises à jour Windows 20 j
Espace disque libre 63 %
Capteur de certificat SSL (port 4... 347 #
Vérification de sécurité SSL (port... Weak Protocols Available
192.168.1.85 SRV-WDS
PING 0 ms
Charge de l'UC SNMP 0 %
Memory: Physical Memory 34 %
Mémoire 33 %
État des mises à jour Windows
Espace disque libre (plusieurs le... 45 %
192.168.1.83 SRV-MAJ
Ping 0 ms
Charge de l'UC SNMP 0 %
Memory: Physical Memory 44 %
Disk Free: C:\ Label:os-2012-ws... 53 %
État des mises à jour Windows 379 j
Espace disque libre (plusieurs le... 53 %
Espace disque libre 53 %
Disk Free: O:\ Label:data-out-ws... <1 %