



<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 Téléchargement | 4 |
| Source et 100 capteurs illimités:..... | 4 |
| Installer Prtg Monitor 16.2.24.4273:..... | 4 |
| Résultat d'installation | 6 |
| PRTG Administration Tool..... | 7 |
| Changer l'endroit de stockage des données | 8 |
| Déplacer le Core system de PRTG sur une autre machine | 10 |
| Effectuer une sauvegarde :..... | 10 |
| Port utilisés : | 11 |
| Smart setup | 14 |
| Changer le mot de passe d'accès à prtg: | 14 |
| Paramètres identifiants windows: | 14 |
| Vue d'ensemble = Equipement: | 15 |
| Vocabulaire prtg - : | 15 |
| Prtg et Root Group | 16 |
| Paramétrage administration Prtg: | 16 |
| Paramétrage Groupe de Base: | 16 |
| Ajouter un équipement | 18 |
| 1 équipement – 1 @ ip:..... | 18 |
| Ajouter un capteur Ping:..... | 19 |
| Notification | 20 |
| Principe de notification:..... | 20 |
| Paramétrage système smtp: | 20 |
| Paramétrage de base de la notification: | 21 |
| Test de la notification: | 23 |
| Planification surveillance capteur | 25 |
| Utiliser une planification par défaut:..... | 25 |
| Créer sa planification:..... | 25 |
| Capteur Snmp | 27 |
| Paramètres snmp de PRTG: | 27 |
| 70 capteur SNMP (13 windows): | 27 |
| Installer service SNMP sur Windows: | 28 |
| Paramétrer le service SNMP sur Windows:..... | 29 |
| Alias DNS pour hôte serveur snmp | 31 |
| Exemples capteur SNMP disque – mémoire – charge Uc..... | 31 |
| Paramétrer le service SNMP sur un switch | 32 |
| Capteur WMI | 33 |
| Paramètres wmi de PRTG:..... | 33 |
| 40 capteur WMI disque – mémoire – charge Uc – Hyper-V | 33 |
| Erreur accès wmi:..... | 34 |
| Paessler wmi tester:..... | 34 |
| Outil wbemtest windows:..... | 36 |

| | |
|---|----|
| DCOM sur Contrôleurs de domaine - dcomcnfg: | 38 |
| WMI sur Contrôleurs de domaine – wimimgmt.msc: | 39 |
| Capteur powershell..... | 40 |
| winrmParamètres powershell de PRTG: | 40 |
| 8 capteurs powershell - statut des mises à jour | 41 |
| Capteur à base de script | 42 |
| Emplacement des capteurs :..... | 42 |
| Premier script batch: | 42 |
| Capteur supplémentaire | 46 |
| Trouver un capteur : | 46 |
| Installer un capteur Script/EXE: | 47 |
| Carte..... | 48 |
| Création d'une carte: | 48 |
| Poser des icônes :..... | 49 |
| Lier des icônes : | 49 |
| Publier une carte:..... | 50 |

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) |

Bravo! Voici votre clé de licence gratuite pour PRTG Network Monitor



Détails de la licence

Titulaire de la licence :
prtgtrial

Clé de licence :
000014-3F8KFM-8FFH3Q-0KNWE3-V43MPU-WQP9CA-7W5T2G-VUU0XP-G8K7MV-QPN816

Veillez enregistrer cette clé de licence dont vous aurez besoin lors de l'installation du logiciel.

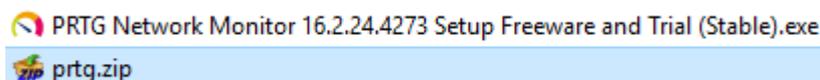
Logiciel à télécharger gratuitement

Si vous ne l'avez pas déjà fait, veuillez télécharger PRTG Network Monitor maintenant.

TÉLÉCHARGEZ ICI >>

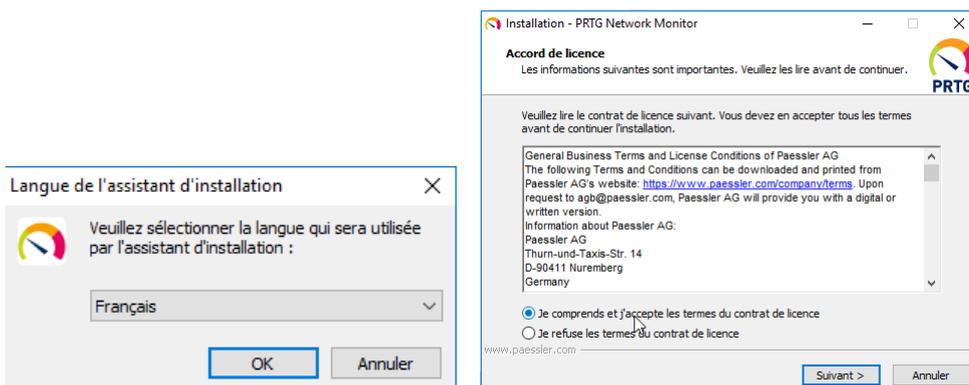
Installer Prtg Monitor 16.2.24.4273:

Il faut désarchiver le fichier récupéré..

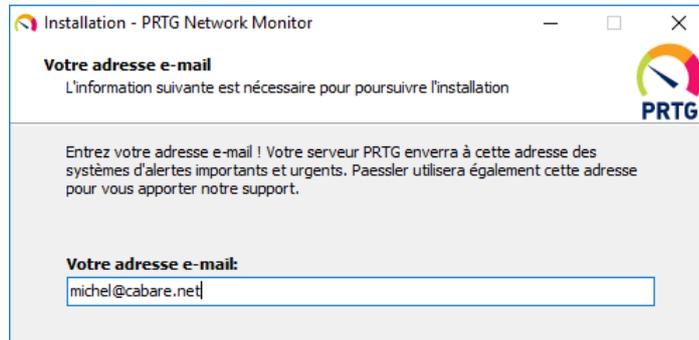


Qui fait environ 180Mo

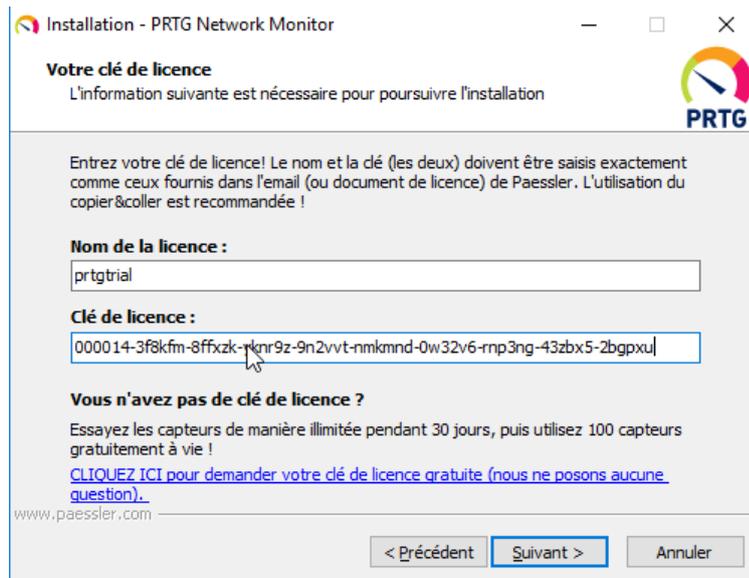
Cela déclenche un assistant, un accord de licence...



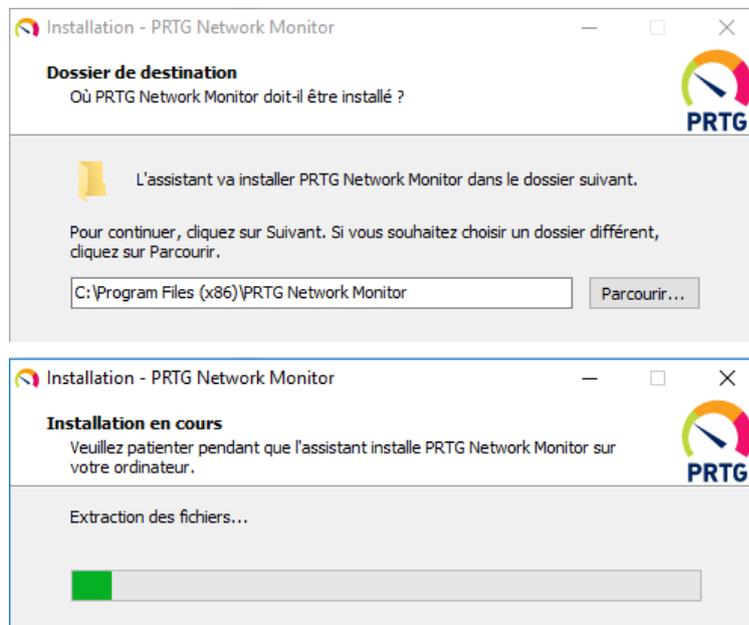
Il faut rentrer une adresse mail



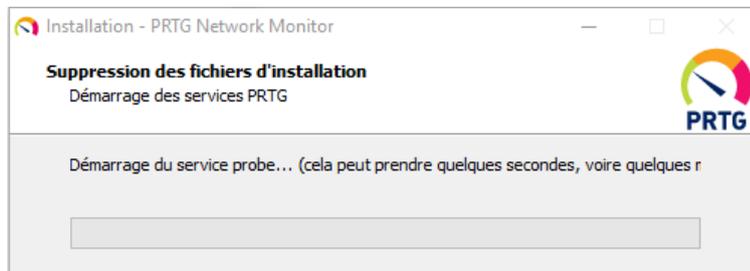
Entrer une clé



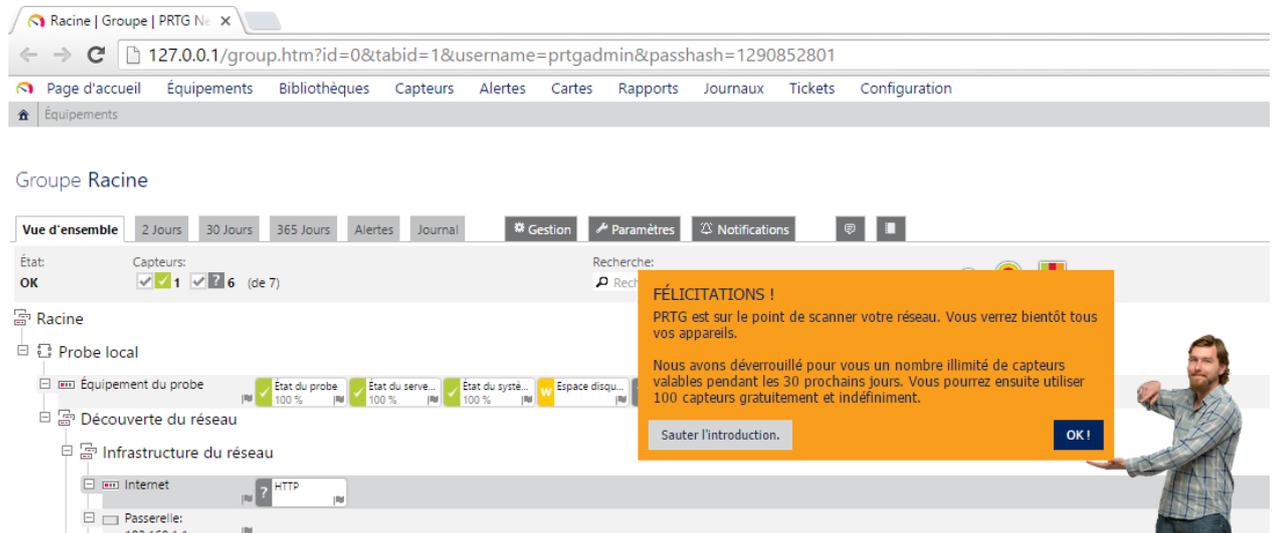
Choisir un dossier (environ 800 mo de requis)



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

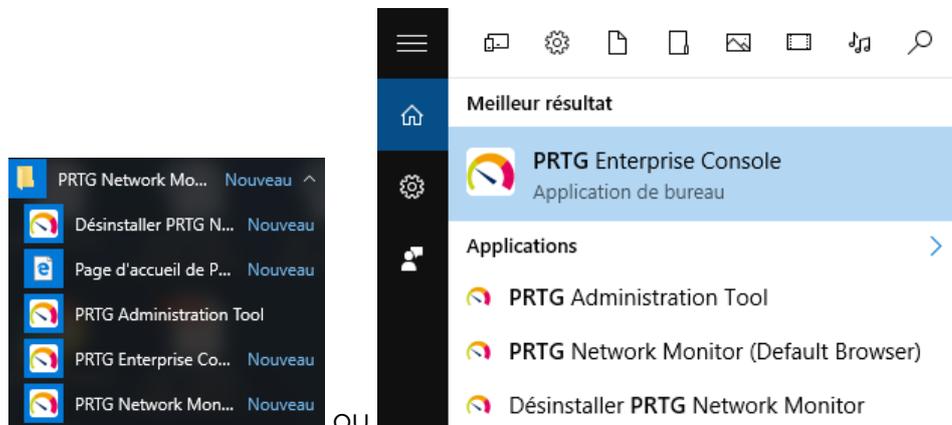


Et on tombe directement sur



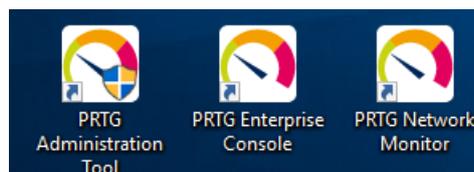
Résultat d'installation

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



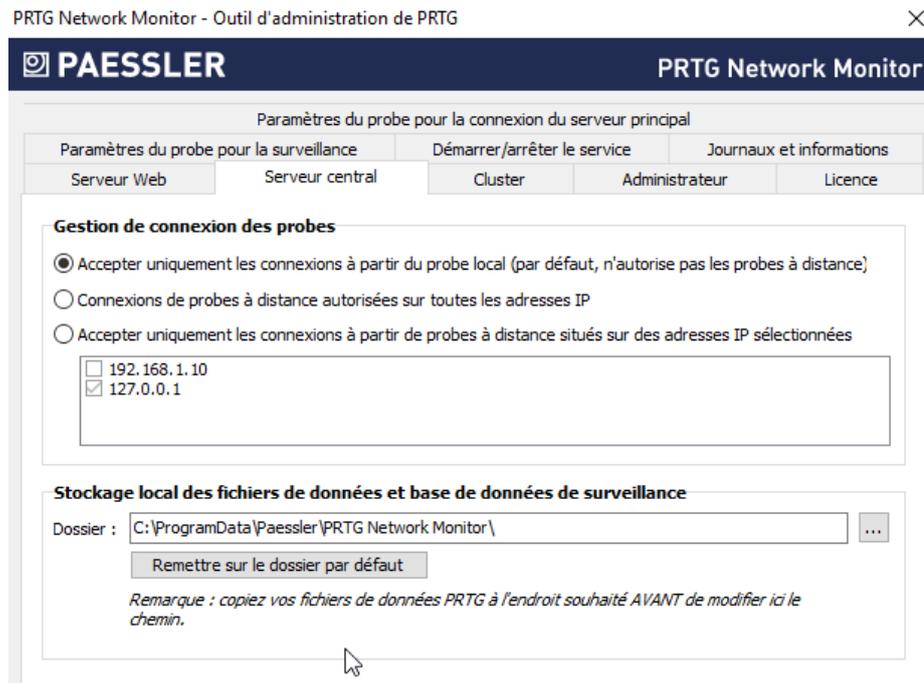
Il y a l'installation de PRTG "core" proprement dit dans la machine, administrable via **PRTG administration Tool**

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

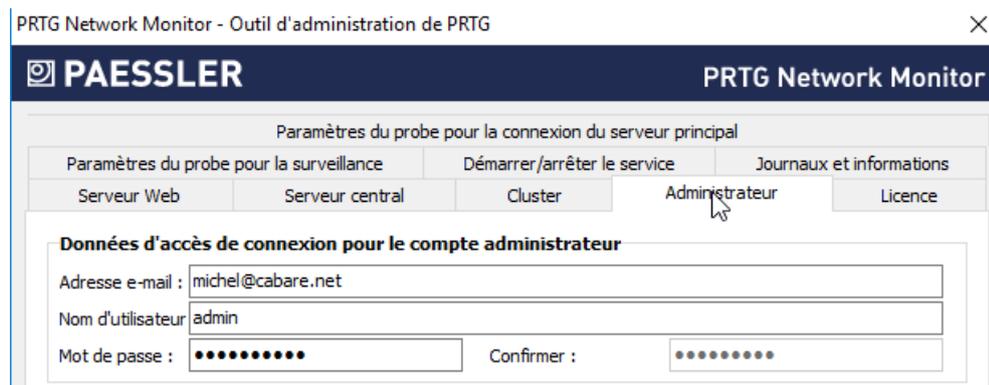


PRTG Administration Tool

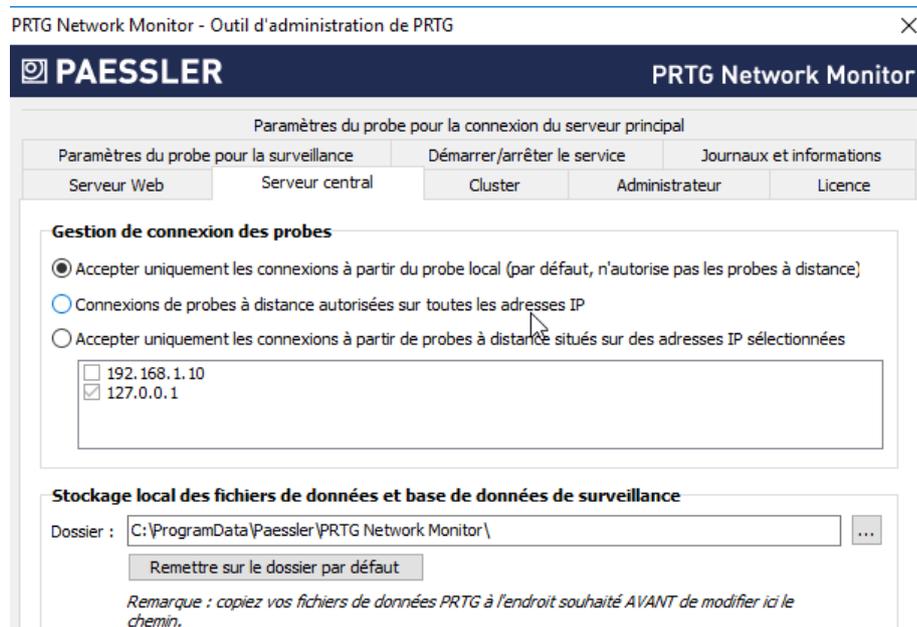
Il y a l'installation de PRTG "core" proprement dit dans la machine, administrable via **PRTG administration Tool**



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



onglet **Serveur central**



onglet **Serveur Web**

PRTG Network Monitor - Outil d'administration de PRTG

PAESSLER PRTG Network Monitor

Paramètres du probe pour la surveillance Démarrer/arrêter le service Journaux et informations

Paramètres du probe pour la connexion du serveur principal

Serveur Web Serveur central Cluster Administrateur Licence

Sélectionnez le port TCP pour le serveur Web de PRTG

Serveur HTTPS sécurisé (port par défaut 443, recommandé, obligatoire pour l'accès Internet)

Serveur HTTP non sécurisé (port 80 standard, non recommandé)

Configuration Expert

Utiliser le cryptage SSL (HTTPS) Ne pas utiliser le cryptage (non recommandé)

Port du serveur Web : 8443

Sélectionnez l'adresse IP pour le serveur Web PRTG

Hôte local : utilisez 127.0.0.1 (PRTG n'offre pas d'accès externe)

Toutes les adresses IP : utiliser toutes les adresses IP disponibles sur cet ordinateur (Remarque : des ports TC

Spécifier les IP:

192.168.1.10
 127.0.0.1

Sélectionner toutes les adresses IP Désélectionner toutes les adresses IP

Sélectionnez la langue du système

Français

Enregistrer et fermer Annuler

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)**

PRTG Network Monitor - Outil d'administration de PRTG

PAESSLER PRTG Network Monitor

Serveur Web Serveur central Cluster Administrateur Licence

Paramètres du probe pour la connexion du serveur principal

Paramètres du probe pour la surveillance Démarrer/arrêter le service Journaux et informations

Service serveur principal PRTG

Démarrer le serveur principal (ignorer les modifications des paramètres) Arrêter le serveur PRTG

État du service: Arrêté

Service probe PRTG

Démarrer le service de probe (ignorer les modifications demandées) Arrêter le service du probe

Options de redémarrage

Pas de réinitialisation Redémarrage planifié

Tente d'arrêter le service PRTG Probe Service

Déplacer les données

Il faut vérifier 2 paramètres (normalement identiques) indiquant les fichiers de stockage utilisés, respectivement

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

The screenshot shows the 'Gestion de connexion des probes' section with three radio button options: 'Accepter uniquement les connexions à partir du probe local (par défaut, n'autorise pas les probes à distance)', 'Connexions de probes à distance autorisées sur toutes les adresses IP', and 'Accepter uniquement les connexions à partir de probes à distance situés sur des adresses IP sélectionnées'. The third option is selected, and a list of IP addresses is shown with '127.0.0.1' checked. Below this is the 'Stockage local des fichiers de données et base de données de surveillance' section with a text field for the file path: 'C:\ProgramData\Paessler\PRTG Network Monitor\'. Navigation tabs at the top include 'Serveur Web', 'Serveur central', 'Cluster', 'Administrateur', and 'Licence'.

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

The screenshot shows the 'Paramètres du probe pour la connexion du serveur principal' settings. It includes fields for 'Nom du probe' (Probe sur UC travail-10) and 'Temps de reconnexion' (300 s). The 'Connexion au serveur central de PRTG' section is configured as a local probe connecting to 127.0.0.1. It shows the 'Serveur (adresse IPv4 ou nom DNS)' as 127.0.0.1, the 'GID du probe' as {09BB7292-6495-4486-8402-6B7D7CC631CD}, and a 'Clé d'accès du probe' field. The 'Chemin d'accès pour le stockage des données du probe' section has a text field with the path 'C:\ProgramData\Paessler\PRTG Network Monitor\'. Navigation tabs at the top include 'Paramètres du probe pour la surveillance', 'Démarrer/arrêter le service', and 'Journaux et informations'.

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

- Configuration Auto-Backups
- Log Database
- Logs (Debug)
- Logs (Sensors)
- Logs (System)
- Logs (Web Server)
- Monitoring Database
- Report PDFs
- System Information Database
- Ticket Database
- ToDo Database
- PRTG Configuration.dat
- PRTG Configuration.old
- PRTG Graph Data Cache.dat

Chemin d'accès pour le stockage des données du probe :

Chemin d'accès:
C:\data-prtg

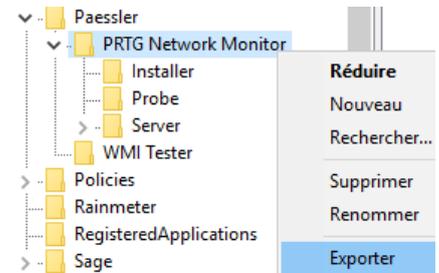
Redémarrer le probe

Déplacer le Core system de PRTG sur une autre machine

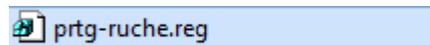
C'est possible, mais la procédure est un peu.. laborieuse, imaginons devoir transférer notre installation de poste-A à un poste-B

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

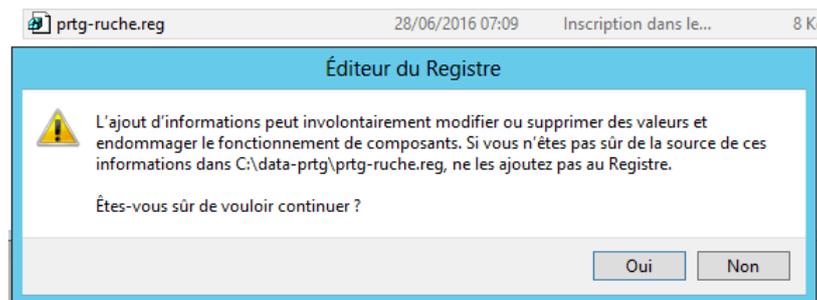
**HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432
Node\Paessler\PRTG Network Monitor**



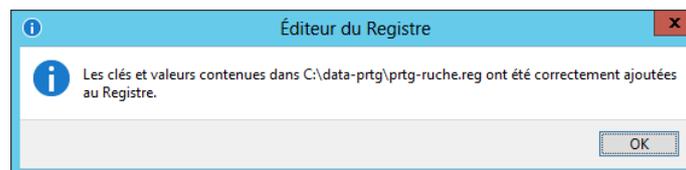
On obtient un fichier .reg



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**

Administration de système



OUTILS D'ADMINISTRATION DU SERVEUR DE BASE



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 <i>Note:</i> 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 sensor settings.

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

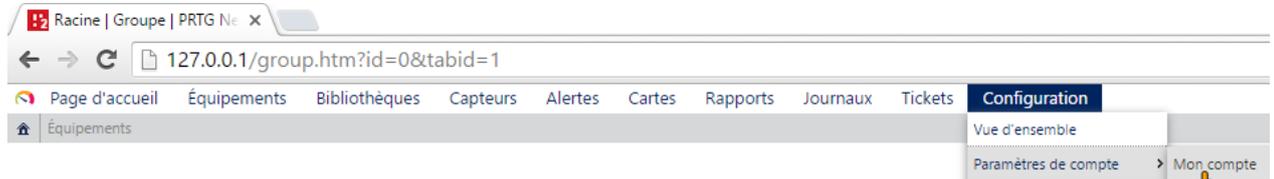
Remote Probes

| 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. |

SMART SETUP

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 de compte

Mon compte Notifications Contacts par notification Horaires

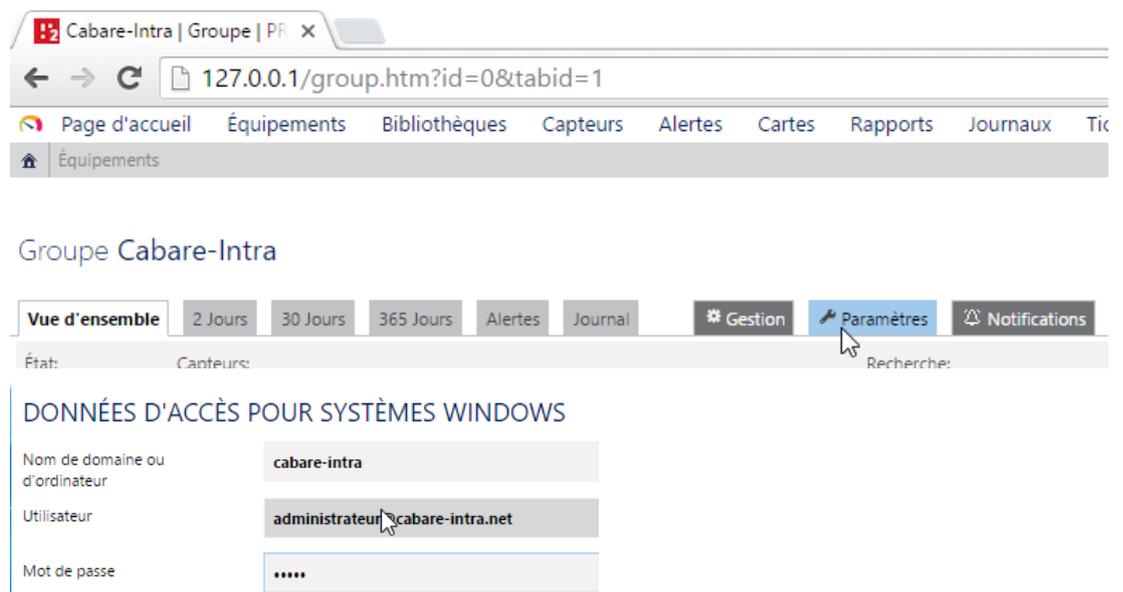
COMPTE UTILISATEUR

| | |
|---------------------------|--|
| Nom d'utilisateur | admin |
| Nom d'affichage | Administrateur système PRTG |
| Adresse e-mail principale | michel@cabare.net |
| Mot de passe | <input type="radio"/> Ne pas modifier <input checked="" type="radio"/> Saisir un nouveau mot de passe |
| Ancien mot de passe | |
| Nouveau mot de passe | |
| Retapez le mot de passe | |



Paramètres identifiants windows:

Dans **Equipement – Paramètres**



Cabare-Intra | Groupe | Paramètres

127.0.0.1/group.htm?id=0&tabid=1

Page d'accueil Équipements Bibliothèques Capteurs Alertes Cartes Rapports Journaux Tickets

Équipements

Groupe Cabare-Intra

Vue d'ensemble 2 Jours 30 Jours 365 Jours Alertes Journal Gestion Paramètres Notifications

État: Capteurs Recherche:

DONNÉES D'ACCÈS POUR SYSTÈMES WINDOWS

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

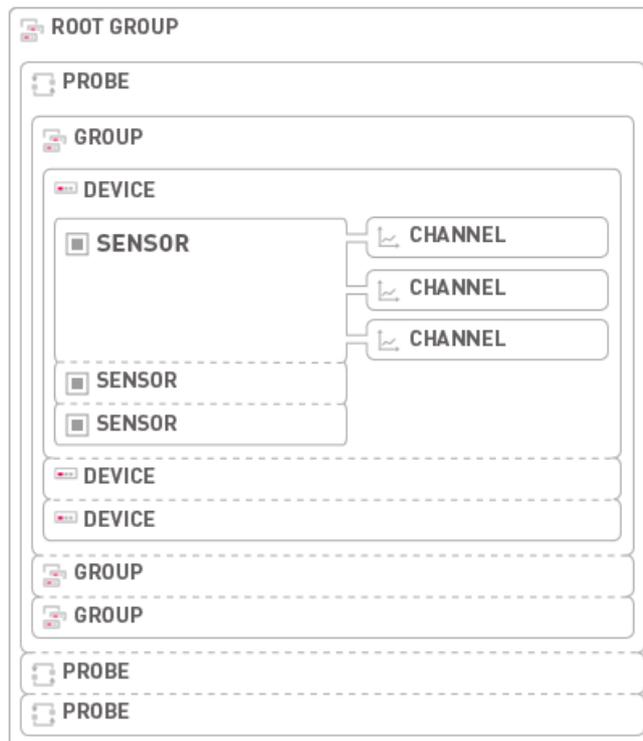
Vue d'ensemble = Equipement:

Dans **Equipement**

The screenshot shows the PRTG Network Monitor web interface. The browser address bar displays '127.0.0.1/group.htm?id=0&tabid=1'. The navigation menu includes 'Page d'accueil', 'Équipements', 'Bibliothèques', 'Capteurs', 'Alertes', 'Cartes', 'Rapports', 'Journaux', 'Tickets', and 'Configuration'. The 'Équipements' tab is active. Below the navigation, the 'Groupe Racine' is displayed. The 'Vue d'ensemble' (Overview) tab is selected, showing a summary of the group's status: 'État: OK', 'Capteurs: 2', 'Alertes: 3', and '141 (de 146)'. A search bar is also visible. The main content area shows a tree view of the group's structure: 'Racine' (expanded) contains 'Probe local' (expanded), which includes 'Équipement du probe' (expanded), 'Découverte du réseau' (expanded), and 'Infrastructure du réseau' (expanded). Under 'Équipement du probe', there are several sensors: 'État du probe' (100%), 'État du serve...' (100%), 'État du systè...' (100%), 'Espace disqu...' (100%), 'Common Saa...' (100%), and 'Atheros AR81...' (41 Kbit/s). Under 'Infrastructure du réseau', there are 'Internet' (HTTP 306 ms) and 'Passerelle: 192.168.1.1' (PING 0 ms, (001) lo Traffic 0.49 Kbit/s, (003) eth_bas... 66 Kbit/s, (007) eth0 Tra... 28 Kbit/s, (008) eth1 Tra... 26 Kbit/s, (009) eth2 Tra... 0 Kbit/s, (010) et... 0 Kbit/s).

Vocabulaire prtg - :

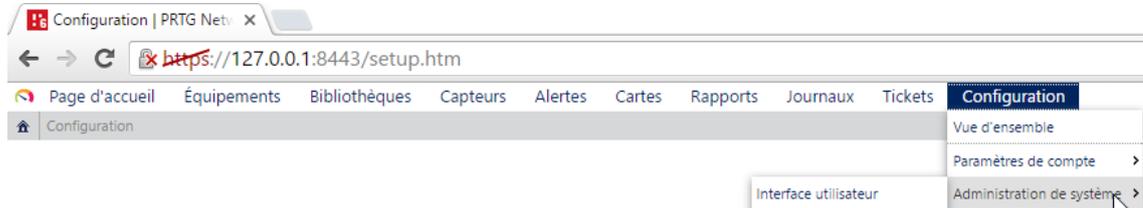
- Core server :** application principale
- Probe :** unité d'administration pour laquelle lorsque l'on effectue des réglages, ceux-ci s'appliquent par héritage à tous son contenu (groupes et device)
- Group :** unité logique
- Device :** équipements accessible via une adresse IP
- Sensor :** capteur
- Channel :** voie de communication



PRTG ET ROOT GROUP

Paramétrage administration Prtg:

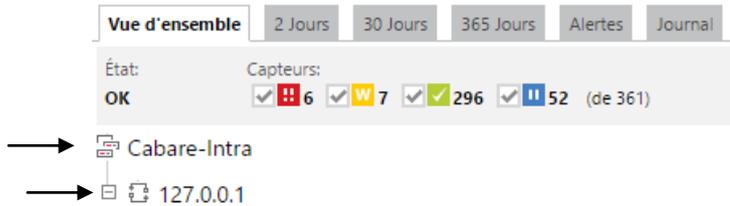
Accessible depuis l'accueil via **Configuration / Administration de système**



Paramétrage Groupe de Base:

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

Groupe Cabare-Intra



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

Groupe Cabare-Intra (automatique)



Plusieurs choses sont intéressantes, notamment



DONNÉES D'ACCÈS POUR SYSTÈMES WINDOWS

| | |
|--------------------------------|--|
| Nom de domaine ou d'ordinateur | <input type="text" value="cabare-intra"/> |
| Utilisateur | <input type="text" value="administrateur@cabare-intra.net"/> |
| Mot de passe | <input type="password" value="*****"/> |

INTERVALLE DE BALAYAGE

| | |
|--------------------------------------|--|
| Intervalle de balayage | <input type="text" value="60 secondes"/> |
| Lorsqu'un capteur signale une erreur | <input type="text" value="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

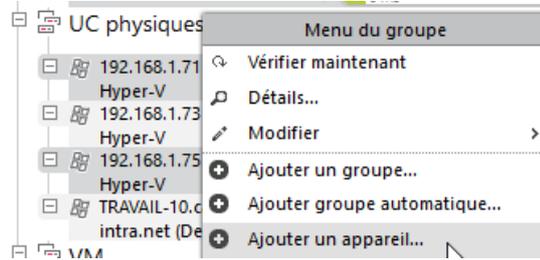
DONNÉES D'ACCÈS POUR LES ÉQUIPEMENTS SNMP

| | |
|-----------------------------|--|
| Version SNMP | <input type="radio"/> v1 <input checked="" type="radio"/> v2c (recommandée) <input type="radio"/> v3 |
| Chaîne de communauté | <input type="text" value="public"/> |
| Port SNMP | <input type="text" value="161"/> |
| Délai d'expiration SNMP (s) | <input type="text" value="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 équipement au groupe UC physiques

AJOUT D'ÉQUIPEMENTS

Si nécessaire, définissez un nom et une adresse d'équipement, les options d'exploration automatique et les paramètres des données d'accès pour Windows, Linux, VMware/XEN et SNMP.

Aide : ajouter un équipement

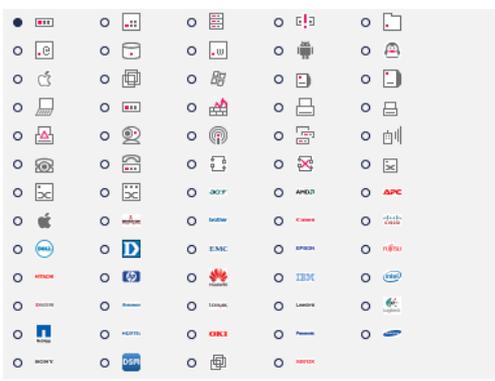
NOM ET ADRESSE DE L'ÉQUIPEMENT

Nom de l'équipement:

Version IP:
 La connexion utilise IPv4
 La connexion utilise IPv6

Adresse IPv4/Nom DNS:

Balises:

icône de l'équipement: 

TYPE D'ÉQUIPEMENT

Gestion du capteur:
 Manuel (pas d'exploration automatique)
 Exploration automatique d'équipement (standard, conseillée)
 Exploration automatique d'équipement (détaillée, peut créer de nombreux capteurs)
 Création automatique de capteurs à partir de modèle(s) d'équipement spécifique(s)

Planification des horaires pour l'exploration automatique:

[Continuer >](#) [Annuler](#)

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...

PARAMÈTRES DE BASE DU CAPTEUR

| | |
|------------------|------------|
| Nom du capteur | PING |
| Balises parentes | C_OS_Win |
| Balises | pingsensor |
| Priorité | ★★★★★ |

PARAMÈTRES DU PING

| | |
|------------------------------|---|
| Délai d'expiration (s) | 2 |
| Taille du paquet (en octets) | 32 |
| Méthode ping | <input type="radio"/> Envoyer un seul ping <input checked="" type="radio"/> Envoyer une série de requêtes ping |
| Nombre de pings | 5 |
| Délai du ping (en ms) | 5 |
| Confirmation automatique | <input checked="" type="radio"/> Afficher l'état « Non fonctionnel » en cas d'erreur (par défaut) <input type="radio"/> Afficher l'état « Non fonctionnel (confirmé) » en cas d'erreur |

INTERVALLE DE BALAYAGE

Hérité de TRAVAIL-10.cabare-intra.net (Device) [Windows] (Intervalle de balayage: 60 secondes, Régler...)

Intervalle de balayage: 30 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...
- Régler le capteur immédiatement comme "non fonctionnel"
- Régler le capteur afin qu'il envoie un avertissement après 1 intervalle, puis le régler sur "non fonctionnel" (recommandé)
- Régler le capteur afin qu'il envoie un avertissement après 2 intervalles, puis le régler sur "non fonctionnel"
- Régler le capteur afin qu'il envoie un avertissement après 3 intervalles, puis le régler sur "non fonctionnel"

HORAIRES, DÉPENDA...

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**

Groupe Cabare-Intra

Vue d'ensemble 2 Jours 30 Jours 365 Jours Alertes Journal # Gestion Paramètres Notifications

DÉCLENCHEURS POUVANT ÊTRE HÉRITÉS DES OBJETS PARENTS

| Type | Notifications | hérité de |
|------|----------------------------|-----------|
| | (aucun déclencheur défini) | |

DÉCLENCHEURS D'OBJET

| Type | Notifications | Actions |
|--------------------|---|--------------------|
| Déclencheur d'état | Lorsque l'état du capteur est Non fonctionnel pour au moins 600 secondes, effectuer Notification par e-mail et message Push à l'administrateur Lorsque l'état du capteur est Non fonctionnel pour au moins 900 secondes, exécuter aucune notification et répéter l'opération toutes les 0 minutes Lorsqu'une condition ne s'applique plus après le déclenchement d'une notification, effectuer Notification par e-mail et message Push à l'administrateur | Modifier Supprimer |

Ajouter un déclencheur d'état Ajouter un déclencheur de vitesse Ajouter un déclencheur de volume Ajouter le seuil de déclenchement Ajouter un déclencheur de changement

Paramétrage système smtp:

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

ADMINISTRATION DE SYSTÈME



Interface utilisateur

Modifier les paramètres du système pour le site Web et le serveur Web



Surveillance

Cliquez ici pour gérer les paramètres qui se rapportent à la surveillance réseau.



Réception des notifications

Cliquez ici pour gérer la réception de notifications via SMTP, SMS et proxy HTTP

On peut donner les informations pour une connexion smtp

ENVOI VIA SMTP

| | |
|----------------------------------|--|
| Système d'envoi SMTP | <input type="radio"/> Acheminement direct à l'aide du serveur de messagerie intégré (par défaut) <input checked="" type="radio"/> Utiliser le serveur relais SMTP (conseillé à l'intérieur des LAN/NAT) <input type="radio"/> Utiliser deux serveurs de relais SMTP (serveur principal et de secours) |
| E-mail de l'expéditeur | <input type="text" value="michel.cabare@wanadoo.fr"/> |
| Nom de l'expéditeur | <input type="text" value="PRTG Network Monitor"/> |
| Identification HELO | <input type="text" value="srv-maj.cabare-intra.net"/> |
| Serveur relais SMTP | <input type="text" value="smtp.orange.fr"/> |
| Port du relais SMTP | <input type="text" value="25"/> |
| Authentification du relais SMTP | <input type="radio"/> Aucune authentification requise <input checked="" type="radio"/> Utiliser l'authentification standard SMTP <input type="radio"/> L'authentification SASL est nécessaire. |
| Utilisateur du relais SMTP | <input type="text" value="michel.cabare@wanadoo.fr"/> |
| Mot de passe pour le relais SMTP | <input type="password" value="••••••••"/> |

Paramétrage de base de la notification:

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

Tickets **Configuration**

PARAMÈTRES DE COMPTE

**Mon compte**

Sélectionnez cette option pour modifier les paramètres de votre compte personnel (adresse e-mail, mot de passe, etc.).

**Notifications**

Les notifications offrent diverses méthodes de notification qui vous informe au cas où un déclencheur de capteur est activé.

**Contacts par notification**

Gérez les coordonnées utilisées par PRTG pour vous envoyer des notifications.

On obtient

Paramètres de compte

Mon compte **Notifications** Contacts par notification Horaires

NOTIFICATIONS

Afficher notifications identifié avec

1 à 3 de 3

| Objet | Actif/Suspendu | Liens |
|---|----------------|--|
| Envoyer un e-mail à tous les membres du groupe Groupe d'utilisateurs PRTG | Actif | <input checked="" type="checkbox"/> Tester <input type="checkbox"/> Suspendre <input checked="" type="checkbox"/> Modifier |
| Notification de ticket | Actif | <input checked="" type="checkbox"/> Tester <input type="checkbox"/> Suspendre <input checked="" type="checkbox"/> Modifier |
| Notification par e-mail et message Push à l'administrateur | Actif | <input checked="" type="checkbox"/> Tester <input type="checkbox"/> Suspendre <input checked="" type="checkbox"/> Modifier |

1 à 3 de 3

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**

Administration de système

Interface utilisateur | Surveillance | Réception des notifications | Serveur principal & Probes | **Comptes d'utilisateurs** | Groupes d'utilisateurs | Outils d'administration

UTILISATEURS

1 à 1 de 1

| Objet | Type | E-mail | Groupe principal | Adhésions aux groupes |
|-----------------------------|-----------------------|-------------------|----------------------|-----------------------|
| Administrateur système PRTG | PRTG (Administrateur) | michel@cabare.net | Administrateurs PRTG | Administrateurs PRTG |

Dans les groupes

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

Administration de système

Interface utilisateur | Surveillance | Réception des notifications | Serveur principal & Probes | Comptes d'utilisateurs | **Groupes d'utilisateurs** | Outil

GROUPES D'UTILISATEURS

1 à 2 de 2

| Objet | Type | Membres |
|----------------------------|------------------------|-----------------------------|
| Administrateurs PRTG | PRTG (Administrateurs) | Administrateur système PRTG |
| Groupe d'utilisateurs PRTG | PRTG | |

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

Notification Envoyer un e-mail à tous les membres du groupe Groupe d'utilisateurs PRTG

Paramètres

PARAMÉTRAGES DE BASE DE LA NOTIFICATION

Nom de la notification: Envoyer un e-mail à tous les membres du groupe Groupe d'utilisateurs PRTG

Balises: []

État:

- commencé
- suspendu

Horaires: Aucun

Différer:

- Rejeter les notifications pendant la pause
- Recueillir les notifications et les envoyer une fois le serveur réactivé

RÉSUMÉ DES NOTIFICATIONS

Méthode:

- Toujours aviser le plus tôt possible
- Envoyer immédiatement les premiers messages non-fonctionnels, résumer les autres
- Envoyer immédiatement les premiers messages non-fonctionnels et les messages O.K, résumer les autres
- Envoyer immédiatement tous les messages non fonctionnels, et résumer les autres
- Envoyer immédiatement tous les messages non fonctionnels et les messages O.K, et résumer les autres
- Résumer toujours les notifications

Objet pour messages de synthèse: [%sitename] %summarycount Summarized Notifications

Rassembler les notifications pour (Minutes): 1

DROITS D'ACCÈS

| Droit d'accès pour groupes d'utilisateurs | Droits |
|---|------------|
| Groupes d'utilisateurs | |
| Groupes d'utilisateurs PRTG | En lecture |

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**

Groupe d'utilisateurs Groupe d'utilisateurs PRTG

Paramètres

PARAMÈTRES DES GROUPES D'UTILISATEURS

Nom du groupe d'utilisateurs:

Page d'accueil par défaut:

Accès au système de ticket:

- Les membres peuvent utiliser le système de ticket
- Les membres NE peuvent PAS utiliser le système de ticket

MEMBRES

Membres:

- Nom d'utilisateur
- Administrateur système PRTG

UTILISATEURS PRINCIPAUX

Liste d'utilisateurs:

Continuer > Annuler

Pour avoir

Administration de système

| Objet | Type | Membres |
|----------------------------|------------------------|-----------------------------|
| Administrateurs PRTG | PRTG (Administrateurs) | Administrateur système PRTG |
| Groupe d'utilisateurs PRTG | PRTG | Administrateur système PRTG |

Test de la notification:

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

Paramètres de compte

Mon compte Notifications Contacts par notification Horaires

NOTIFICATIONS

Afficher notifications identifié avec

| Objet | Actif/Suspendu | Liens |
|---|----------------|---|
| Envoyer un e-mail à tous les membres du groupe Groupe d'utilisateurs PRTG | Actif | <input checked="" type="button" value="Tester"/> <input type="button" value="Suspendre"/> |
| Notification de ticket | Actif | <input checked="" type="button" value="Tester"/> <input type="button" value="Suspendre"/> |
| Notification par e-mail et message Push à l'administrateur | Actif | <input checked="" type="button" value="Tester"/> <input type="button" value="Suspendre"/> |

Qui donne un message

Résultats du test de notification.

Une notification de test a été déclenchée et mise en file d'attente afin d'être livrée aux destinataires suivants. Veuillez vérifier si vous avez reçu la notification.

| Utilisateur | E-mail |
|-----------------------------|--------|
| Administrateur système PRTG | |

OK

Et pour le destinataire la réception d'un mail
Avec toutes les informations dans l'entête

! Ce message a été envoyé avec l'importance Haute.
En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur Web.

De : PRTG Network Monitor <michel.cabare@wanadoo.fr>
À : michel@cabare.net
Cc :
Objet : [PRTG Network Monitor (CABARE)] TRAVAIL-10.cabare-intra.net (Device) [Windows] RDP (RDP (Bureau à distance)) Non fonctionnel (Erreur simulée (code : PE034))

PRTG NETWORK MONITOR

!! capteur RDP (RDP (Bureau à distance)) ***

Probe sur SRV-MAJ 192.168.1.83 > UC physiques > TRAVAIL-10.cabare-intra.net (Device) [Windows] (192.168.1.10)

Nouvel état à 29/06/2016 11:13:26 (Romance Standard Time):
Non fonctionnel
Dernier message:
Erreur simulée (code : PE034)

| Dernière analyse: | Dernier OK: | Dernière erreur: | Disponibilité: | Temps mort: | Couverture: | Type de capteur: | Intervalle: |
|-------------------|-------------|------------------|----------------|-------------|-------------|-------------------------|-------------|
| 60 s | 11 min. 2 s | 60 s | 97,0226% | 2,9774% | 51% | RDP (Bureau à distance) | 60 s |

Vérifier maintenant Valider l'alarme Suspendre Reprendre
Pause de 5 minutes Pause de 60 minutes Pause de 24 heures

Et lorsque la situation revient normale

! Ce message a été envoyé avec l'importance Haute.
En cas de problème lié à l'affichage de ce message, cliquez ici pour l'afficher dans un navigateur Web.

De : PRTG Network Monitor <michel.cabare@wanadoo.fr>
À : michel@cabare.net
Cc :
Objet : [PRTG Network Monitor (CABARE)] TRAVAIL-10.cabare-intra.net (Device) [Windows] RDP (RDP (Bureau à distance)) Disponible (Temps mort: 1 h 2 min.) (OK)

PRTG NETWORK MONITOR

✓ capteur RDP (RDP (Bureau à distance)) ***

Probe sur SRV-MAJ 192.168.1.83 > UC physiques > TRAVAIL-10.cabare-intra.net (Device) [Windows] (192.168.1.10)

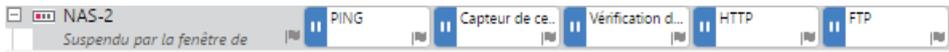
Nouvel état à 29/06/2016 12:06:17 (Romance Standard Time):
Disponible (Temps mort: 1 h 2 min.)
Dernier message:
OK

| Dernière analyse: | Dernier OK: | Dernière erreur: | Disponibilité: | Temps mort: | Couverture: | Type de capteur: | Intervalle: |
|-------------------|-------------|------------------|----------------|-------------|-------------|-------------------------|-------------|
| 51 s | 1 h 3 min. | 51 s | 95,4112% | 4,5888% | 51% | RDP (Bureau à distance) | 60 s |

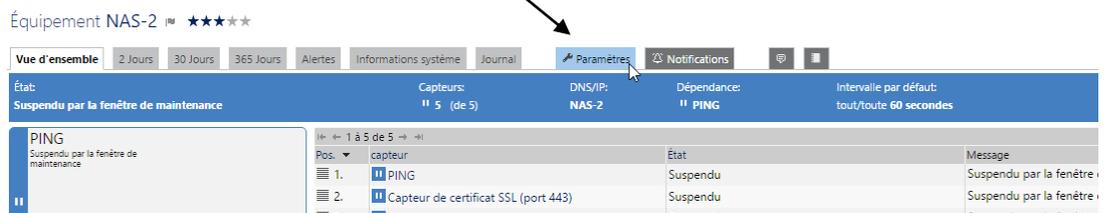
PLANIFICATION SURVEILLANCE CAPTEUR

Utiliser une planification par défaut:

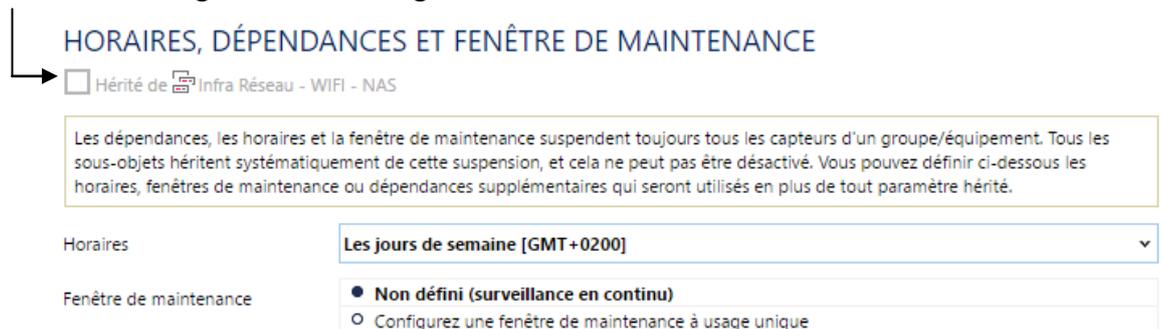
On veut qu'un capteur ne soit armé que pendant une plage horaire, par exemple de 8h du matin à 20h le soir.. C'est le cas de ce **NAS-2**



Dans les **paramètres**, il faut



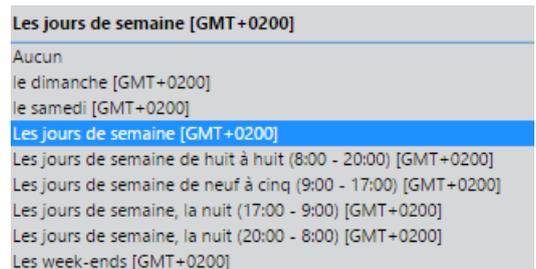
Il faut aller dans la section **Horaires dépendances et fenêtre de maintenance** on décoche l'héritage, et on configure comme on le souhaite



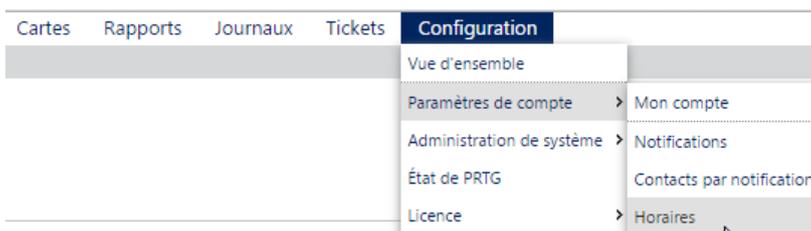
Créer sa planification:

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**

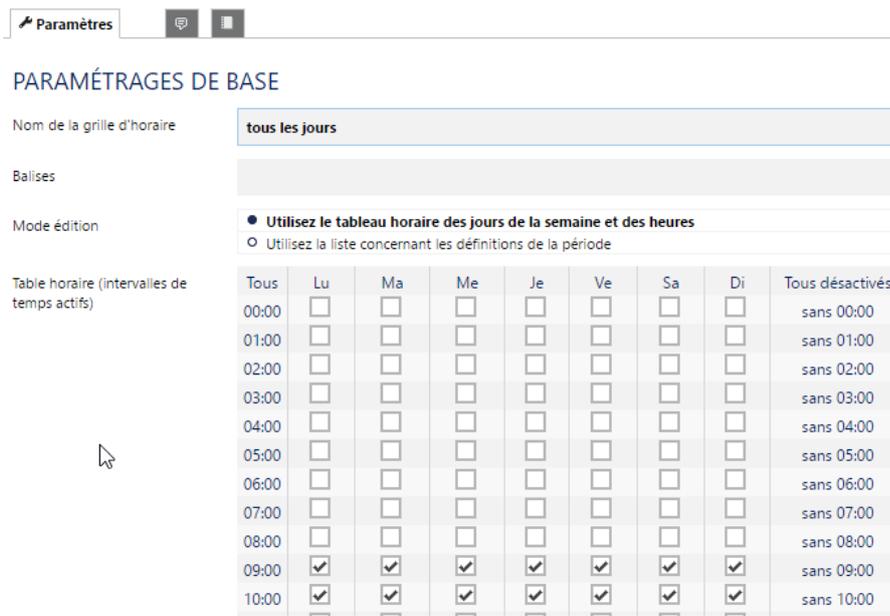


On obtient une fenetre dans laquelle on demande **Ajouter un nouvel horaire**,



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

Horaires tous les jours



Elle sera désormais disponible pour notre capteur

HORAIRES, DÉPENDANCES ET FENÊTRE DE MAINTENANCE

Hérité de **Infra Réseau - WIFI - NAS**

Les dépendances, les horaires et la fenêtre de maintenance suspendent toujours tous les capteurs d'un groupe/équipement. Tous les sous-objets héritent systématiquement de cette suspension, et cela ne peut pas être désactivé. Vous pouvez définir ci-dessous les horaires, fenêtres de maintenance ou dépendances supplémentaires qui seront utilisés en plus de tout paramètre hérité.

Horaires

tous les jours

Fenêtre de maintenance

Non défini (surveillance en continu)

Configurez une fenêtre de maintenance à usage unique

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**

DONNÉES D'ACCÈS POUR LES ÉQUIPEMENTS SNMP

| | |
|-----------------------------|--|
| Version SNMP | <input type="radio"/> v1 <input checked="" type="radio"/> v2c (recommandée) <input type="radio"/> v3 |
| Chaîne de communauté | public |
| Port SNMP | 161 |
| Délai d'expiration SNMP (s) | 5 |

En raison des limitations internes, vous ne pouvez surveiller qu'un nombre limité de capteurs par seconde par le protocole SNMP v3. Le principal facteur de limitation est la puissance du processeur. Actuellement, PRTG est en mesure de traiter environ 40 requêtes par seconde et par serveur d'ordinateur, selon votre système. Cela signifie que vous pouvez exécuter environ 5 000 capteurs SNMP v3 au cours d'un intervalle de balayage de 60 secondes sur un ordinateur possédant deux processeurs, en environ 10 000 capteurs par intervalle de 60 secondes sur un système doté de quatre processeurs. Si vous avez remarqué une augmentation du "délai d'intervalle" ou des "requêtes ouvertes" lors de la lecture du capteur d'état du probe, vous devez répartir la charge sur plusieurs probes. Les protocoles SNMP v1 et v2 ne sont pas soumis à cette limitation.

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 parmi les 70

RECHERCHE

70 Types de capteurs disponibles

QUE PEUT-ON SURVEILLER ?

- Disponibilité
- Bande passante/trafic

TYPE DE SYSTÈME CIBLE ?

- Windows
- Linux/MacOS

TECHNOLOGIE UTILISÉE ?

- Ping
- SNMP

Charge de l'UC SNMP ?
Surveille la charge d'une UC via SNMP

Ajouter ►

Mais ce capteur peut poser soucis

!!! capteur Charge de l'UC SNMP ★★★★★

Vue d'ensemble Données en temps réel 2 Jours 30 Jours 365 Jours Données historiques Journal Paramètres Notifications Canaux

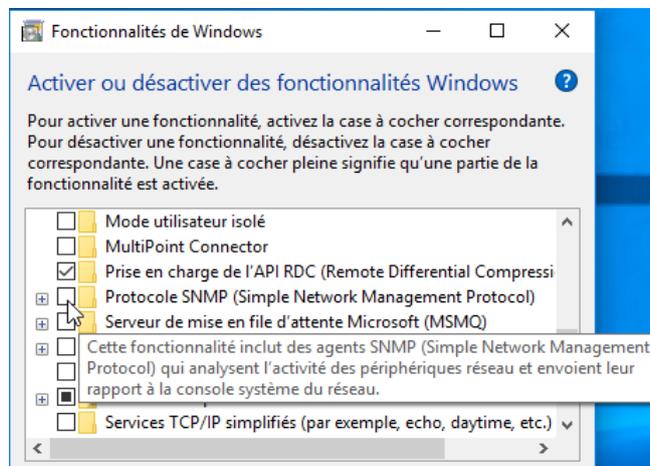
Dernier message :
No response (check: firewalls, routing, snmp settings of device, IPs, SNMP version, community, passwords etc) (erreur SNMP # -2003)

| | | | | | | |
|---------------------------|------------|--------------------------|---------------------------|-------------------------|---------------------|---|
| Dernière analyse: 21 s | Dernier OK | Dernière erreur: 21 s | Disponibilité: 0,0927% | Temps mort: 99,9073% | Couverture: 100% | Type de capteur: Charge de l'UC SNMP |
| Somme | Canal | ID | Dernière valeur | Minimum | Maximum | |

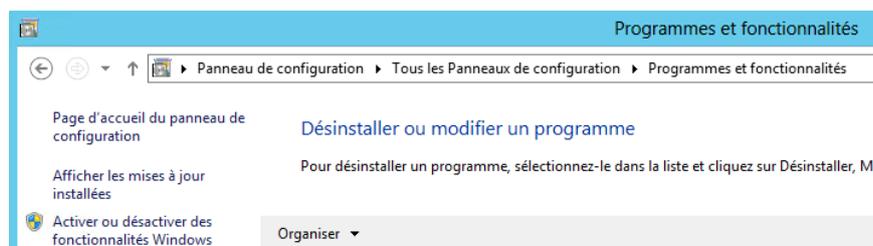
Installer service SNMP sur Windows:

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

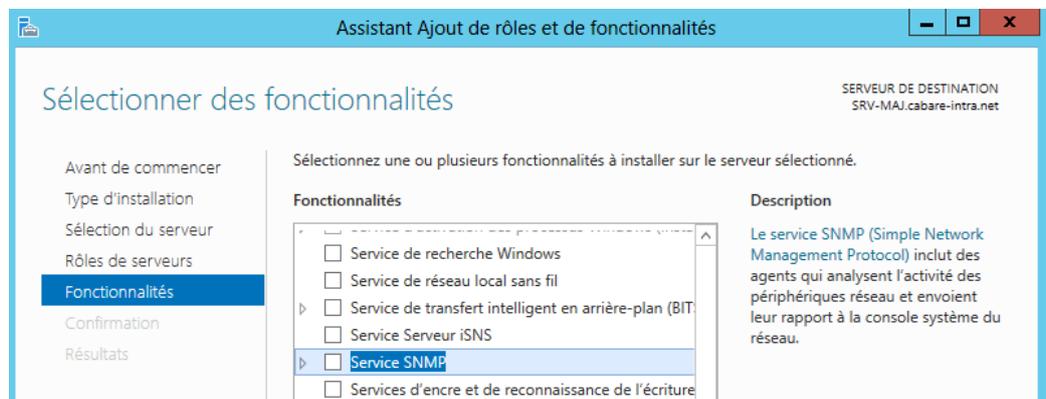
Sur un client Windows on y remédie soit via le panneau de configuration, **programmes et fonctionnalités**, et on demande dans **Activer ou désactiver des fonctionnalités Windows**



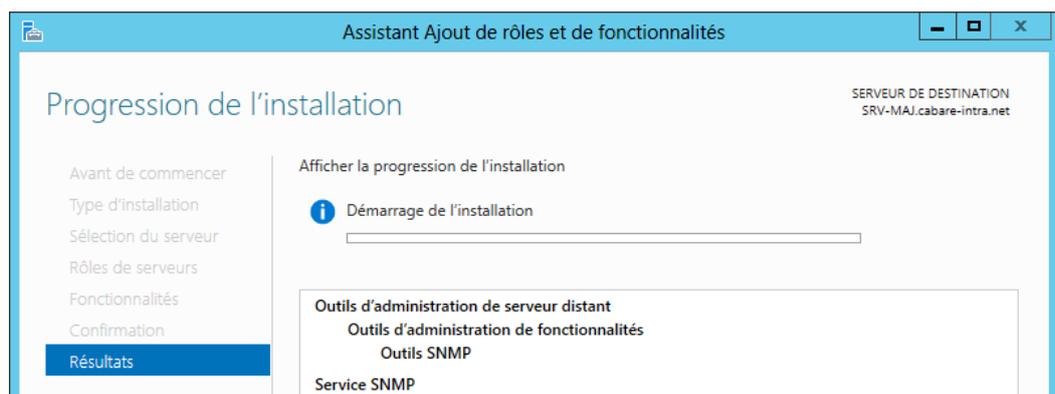
Sur un serveur Windows via le **gestionnaire de serveur en demandant ajouter des rôles et des fonctionnalités**



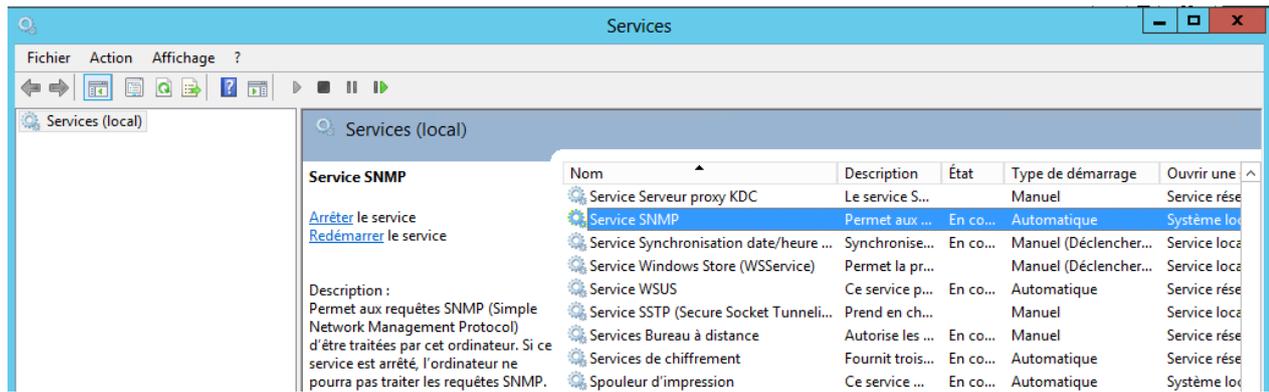
On demande d'ajouter le **service SNMP** (pas confondre avec Serveur SNMP)



et tout ce qui est coché par défaut



On peut désormais ouvrir le **Service SNMP**



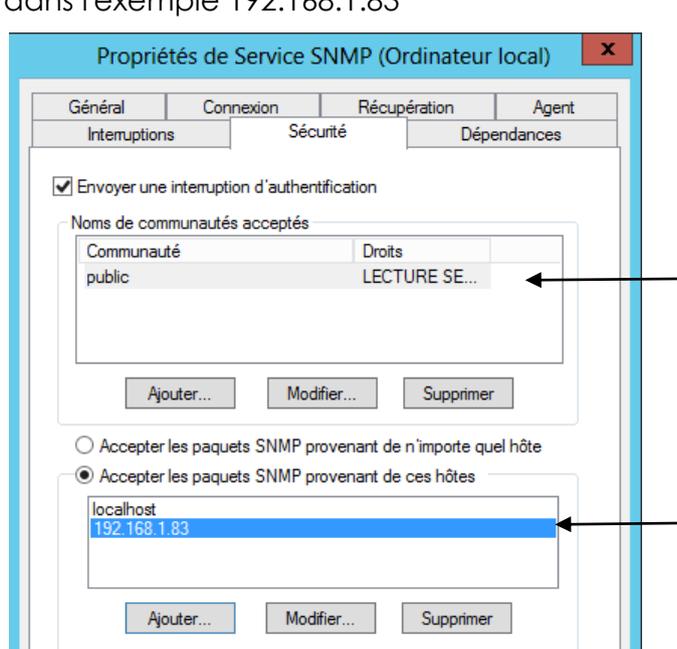
Paramétrer le service SNMP sur Windows:

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 héberge **PRTG** dans l'exemple 192.168.1.83

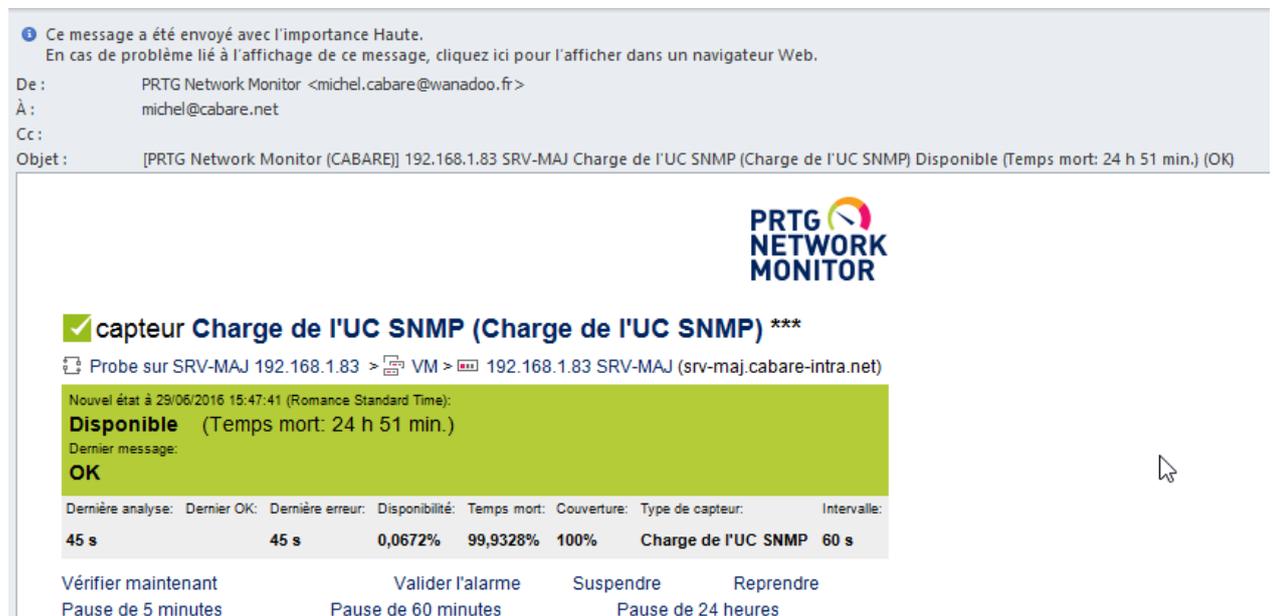


onglet **Agent** on coche tout



Et on redémarrage le service SNMP

On recevra un mail confirmant

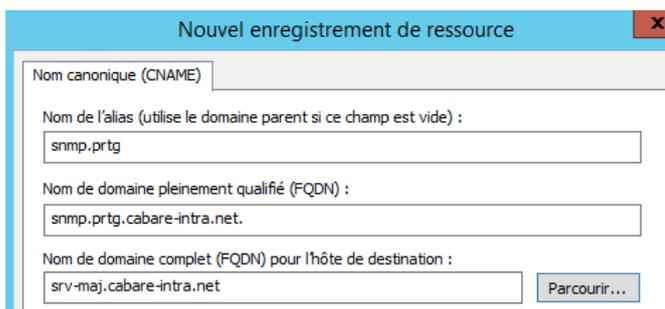


Cas Windows 2012

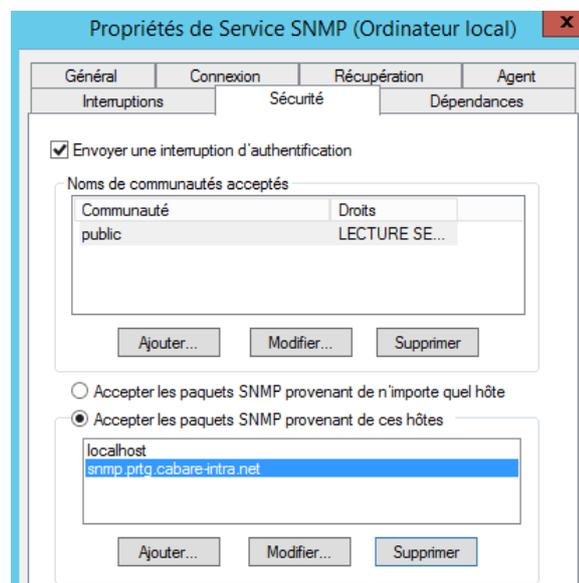
Note: On Windows Server 2012, you might encounter missing Security, Agent, and Traps tabs in SNMP service properties. Please see [this article on joshancel.wordpress.com](http://joshancel.wordpress.com) for a workaround. You can also find information about this issue in [this Knowledge Base article](#).

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

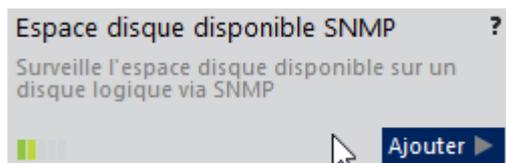


Exemples capteur SNMP disque – mémoire – charge Uc

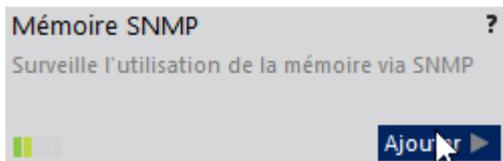
Parmi tous les capteurs PRTG on peut noter

Espace disque disponible SNMP

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

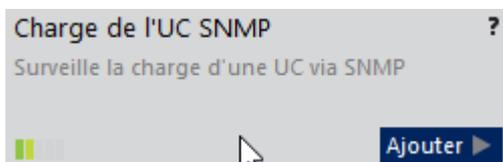


Mémoire SNMP



Il existe un contrôle identique WMI

Charge UC



Paramétrer le service SNMP sur un switch

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

Parmi tous les capteurs WMI on peut noter

RECHERCHE

40 Types de capteurs disponibles

QUE PEUT-ON SURVEILLER ?

- Disponibilité
- Bande passante/trafic
- Vitesse/Performance

TYPE DE SYSTÈME CIBLE ?

- Windows
- Linux/MacOS
- OS de virtualisation

TECHNOLOGIE UTILISÉE ?

- Ping
- SNMP
- WMI

Capacité du disque WMI

Capacité du disque WMI (plusieurs fo... ?
Surveille l'espace libre d'un ou plusieurs lecteurs de disque local (un canal par lecteur)



Ajouter ►

Mémoire WMI

Mémoire WMI ?
Surveille la mémoire système disponible via WMI



Ajouter ►

Il existe un contrôle identique WMI

Charge UC

Charge UC de Windows ?
Surveille la charge UC à l'aide de compteurs de performance ou WMI



Ajouter ►

Serveur Hôte Hyper-V et Machine Virtuelle Hyper-V

| | |
|--|--|
| <p>Serveur hôte Hyper V ? Surveille un serveur hôte Hyper-V</p>  <p>Ajouter ►</p> | <p>Machine virtuelle Hyper-V ? Surveille une machine virtuelle sur un serveur Hyper-V</p>  <p>Ajouter ►</p> |
|--|--|

Erreur accès wmi:

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

!!! capteur Charge de l'UC ★★★★★

Vue d'ensemble | Données en temps réel | 2 Jours | 30 Jours | 365 Jours | Données historiques | Journal | Paramètres | Notifications | Canaux

Dernier message:
WMI: 80070005: Accès refusé- Remarque : la version du système d'exploitation de l'ordinateur n'a pas pu être identifiée, n the system. (erreur de compteur de performance 0xC000BB8)

!!! capteur Espace disque libre (plusieurs lecteurs) ★★★★★

Vue d'ensemble | Données en temps réel | 2 Jours | 30 Jours | 365 Jours | Données historiques | Journal | Paramètres | Notifications | Canaux

Dernier message:
Impossible d'établir la connexion (800706BA: Le serveur RPC n'est pas disponible - Host: srv-v1.cabare-intra.net, User: administrateur@cabare-intra.net, Password: ***, Domain: ntldomain:cabare-intra.net) (code : PE015). Il semble que vous rencontriez des difficultés avec WMI ou les zones associées. Pour plus d'informations, consultez notre base de connaissances : <http://kb.paessler.com/en/topic/60153>**

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

Paessler WMI Tester

Tests The Accessibility of WMI Counters

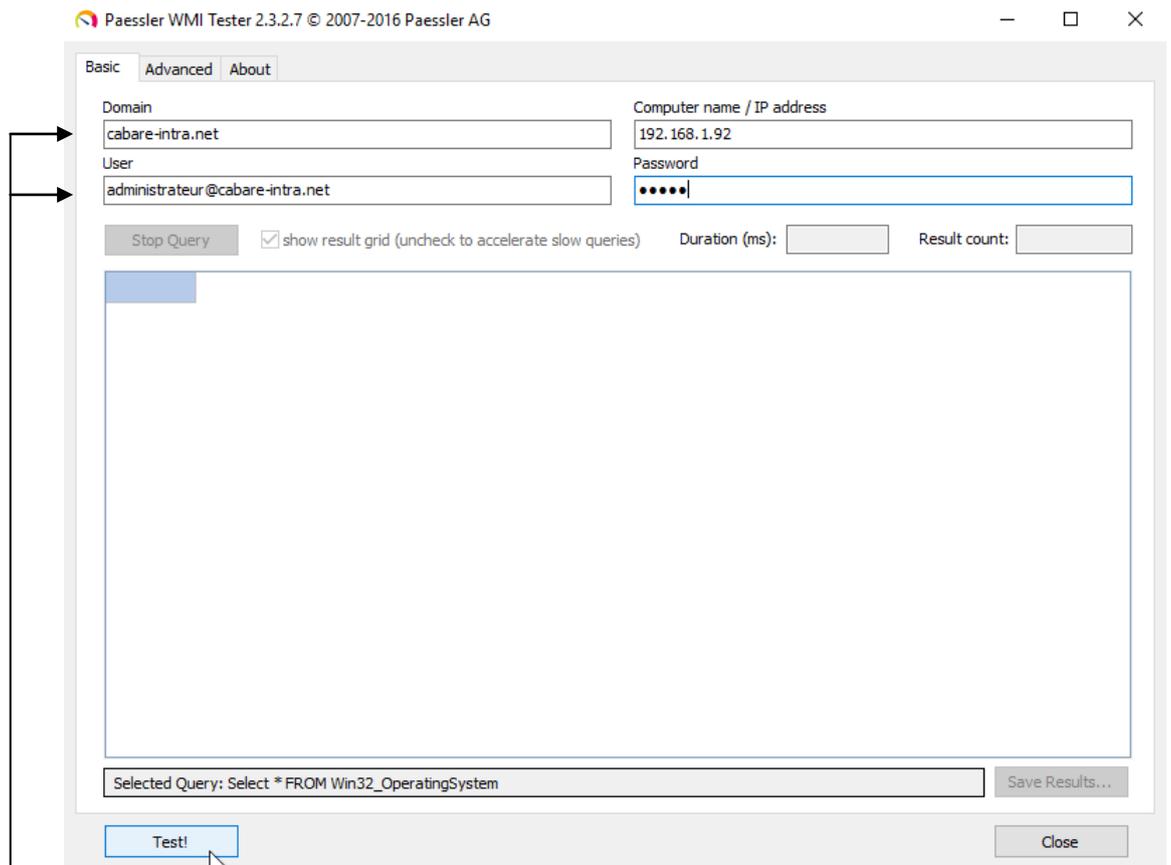
WMI stands for "Windows Management Instrumentation" and is the technology from Microsoft for monitoring and management of Windows based systems.

WMI works like a database and offers a variety of useful monitoring values of Computers running Microsoft Windows. Products like Paessler's [PRTG Network Monitor](#) make use of the WMI functionality to monitor computers in network environments. WMI allows a process to read out data for many Windows' configuration parameters as well as current system status values. Access can take place locally or remotely via a network connection. WMI is based on COM and DCOM and is integrated in Windows 2000, XP, 2003, Vista and later.

As WMI access over a network is not quite trivial, the Paessler WMI Tester is a tool for testing the accessibility of WMI in a quick and easy-to-use way.

| | | | |
|------------------------|------------------|-------------------|----------|
| WMI Tester 2.3.2.7.zip | 26/06/2016 08:37 | IZArc ZIP Archive | 2 162 Ko |
| WMITest.exe | 09/05/2016 14:53 | Application | 5 774 Ko |

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**

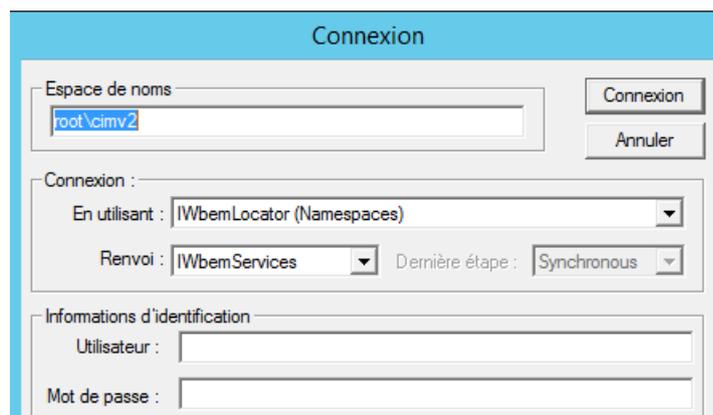
```
C:\Windows\system32>wbemtest
```

WMI sur la machine locale

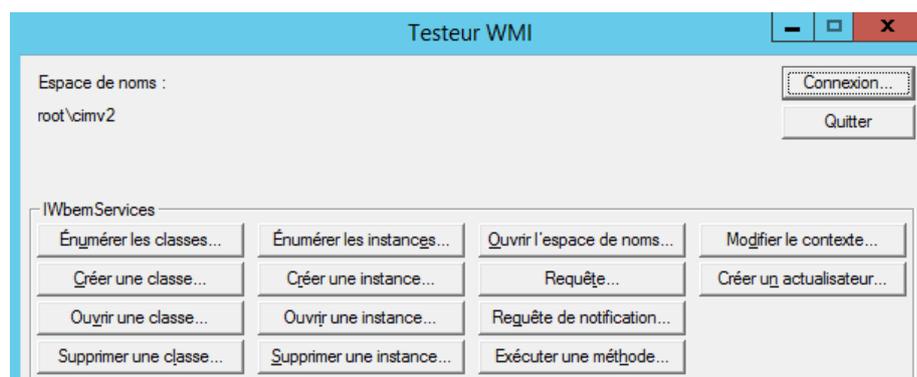
Cela permet de savoir si WMI est opérationnel sur la machine en question, simplement par une demande de **Connexion...**



Avec les paramètres par défaut



Si cela fonctionne,



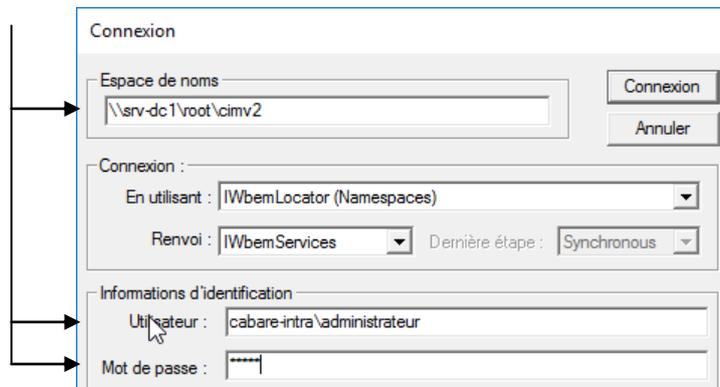
cela veut dire que WMI est opérationnel sur la machine

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 exécute **wbemtest**

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

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



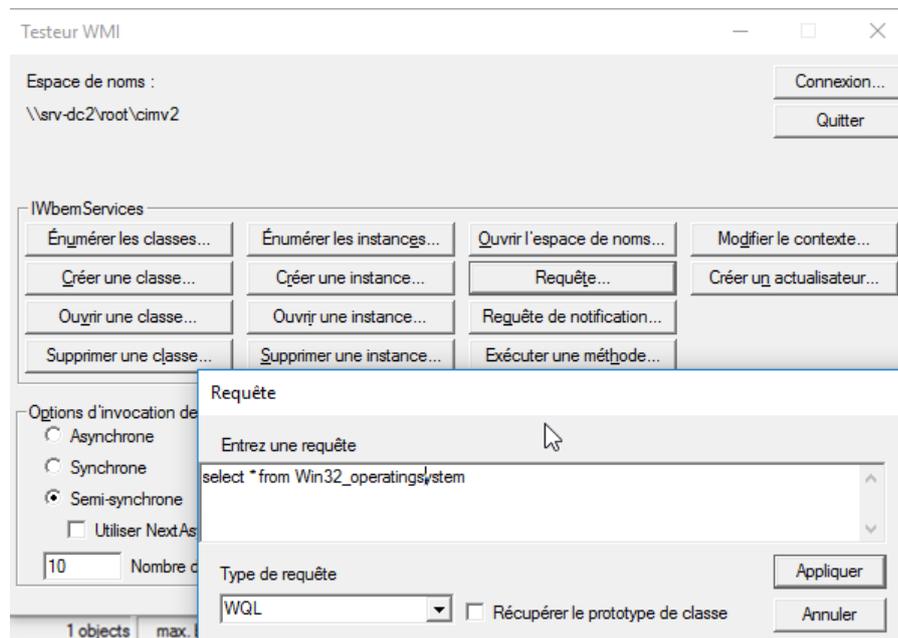
Executer une requête

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

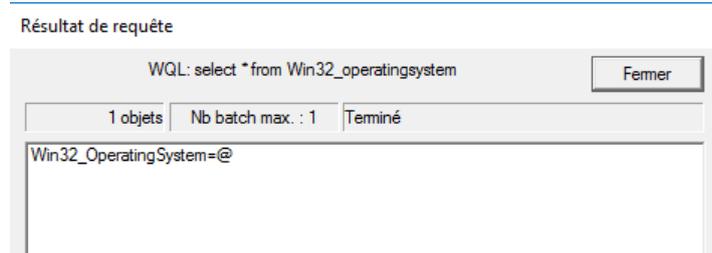
On demande **Requête...** puis on demande une requête du genre

select * from Win32_operatingsystem

comme dans la capture ci dessous



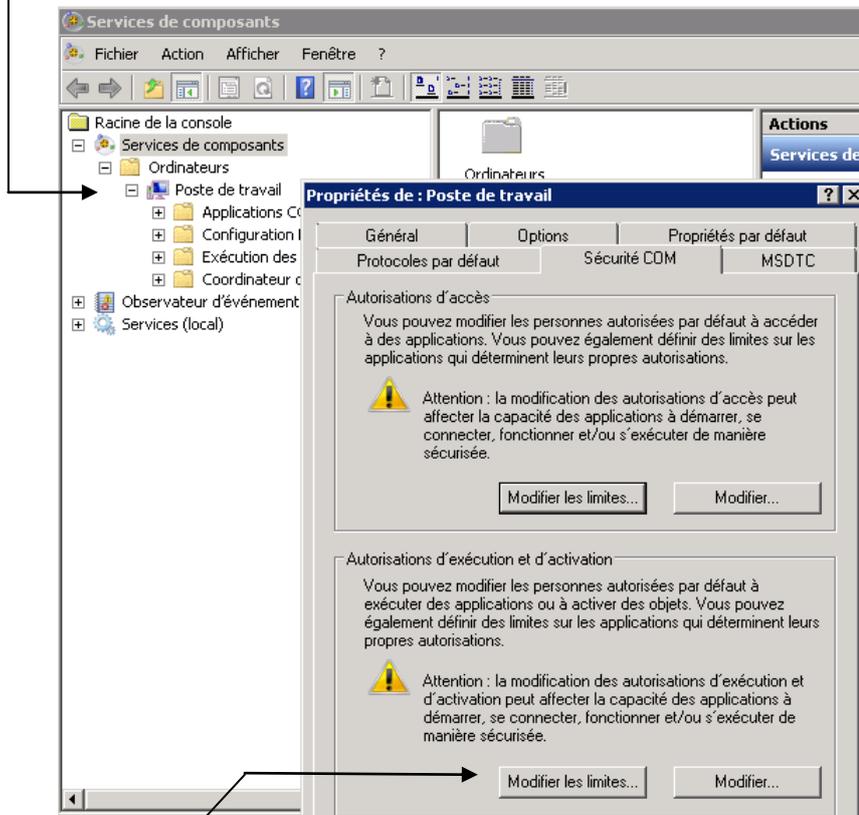
Si on obtient un résultat, et pas un message d'erreur, c'est que l'on a accès à WMI



DCOM sur Contrôleurs de domaine - dcomcnfg:

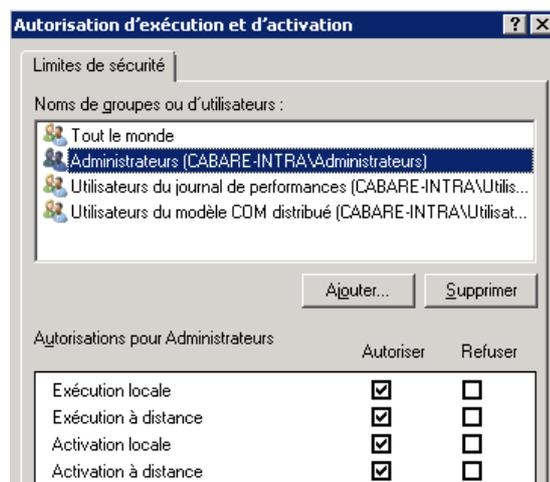
1. Login sur le Domain Controller
2. Executer **dcomcnfg**

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



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

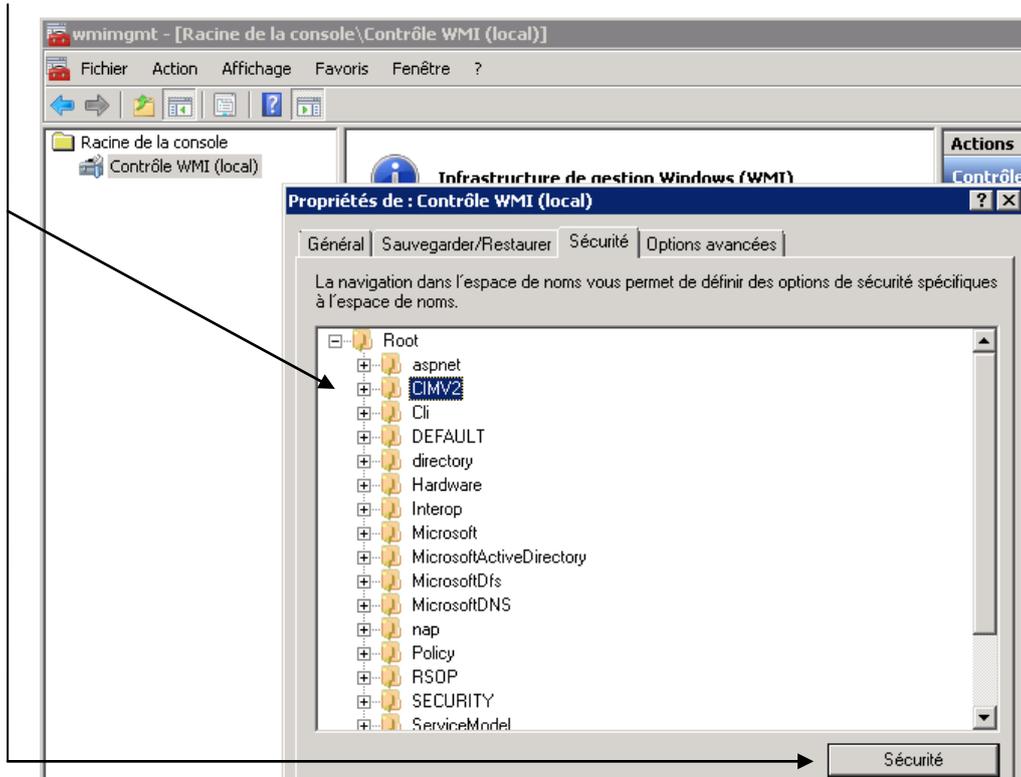
Vérifier que l'on ait bien



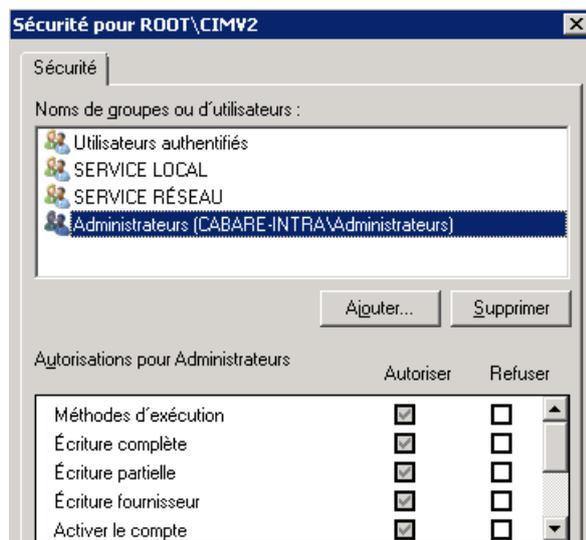
WMI sur Contrôleurs de domaine – wmicmgmt.msc:

1. Login sur le Domain Controller
2. Executer "**wmicmgmt.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

winrm Paramètres 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 « 0 ») : 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 gestion
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

RECHERCHE

8 Types de capteurs disponibles

QUE PEUT-ON SURVEILLER ?

- Disponibilité
- Bande passante/trafic
- Vitesse/Performance
- Utilisation UC
- Utilisation du disque
- Utilisation de la mémoire
- Paramètres du matériel
- Infrastructure du réseau
- Capteurs personnalisés

TYPE DE SYSTÈME CIBLE ?

- Windows
- Linux/MacOS
- OS de virtualisation
- Serveur de fichiers
- Serveur de messagerie
- Base de données
- Services en cloud

TECHNOLOGIE UTILISÉE ?

- Ping
- SNMP
- WMI
- Compteurs de performance
- HTTP
- SSH
- Renifleur de paquets
- NetFlow, sFlow, jFlow
- Powershell

Statut des mises à jour Windows

Statut de mises à jour Windows (Pow... ?

Affiche l'état des "mises à jour Windows" (dernière mise à jour, nombre de mises à jour disponibles/installées).

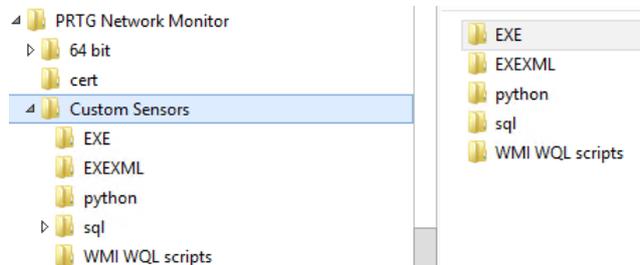


Ajouter ►

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



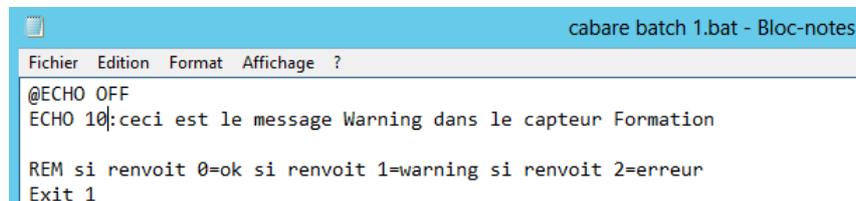
Premier script batch:

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

PARAMÈTRES DE BASE DU CAPTEUR

| | |
|------------------|--------------------------------------|
| Nom du capteur | Capteur personnalisé avec EXE/script |
| Balises parentes | |
| Balises | exesensor ✕ |
| Priorité | ★★★★★ |

PARAMÈTRES DU CAPTEUR

Important : Le fichier EXE doit être exécuté sur l'ordinateur sur lequel le probe parent est installé, et non sur le dispositif parent. Le répertoire de travail des fichiers "exe" est le répertoire du probe, "vbs, ps1" mais d'autres fichiers de scripts peuvent utiliser d'autres répertoires de travail.

| | |
|------------|--------------------|
| Script/EXE | cabare batch 1.bat |
|------------|--------------------|

Son execution renvoie bien la valeur **10** et un **warning**...

W capteur Capteur personnalisé avec EXE/script ★★★★★

Vue d'ensemble Données en temps réel 2 Jours 30 Jours 365 Jours Données historiques Journal Paramètres Notifications Canaux

Dernier message : ceci est le message Warning dans le capteur Formation

Dernière analyse: 6 s Dernière OK: 6 s Dernière erreur: 91 s Disponibilité: 44,6197% Temps mort: 55,3803% Couverture: 100%

| Valeur | Temps d'exécution | Canal | ID | Dernière valeur |
|--------|-------------------|-------------------|----|-----------------|
| | 46 ms | Temps d'exécution | 1 | 46 ms |
| | | Temps mort | -4 | |
| | | Valeur | 2 | 10 # |

10 # 0 10 #

Et donc

```
cabare batch 2.bat - Bloc-notes
Fichier Edition Format Affichage ?
@ECHO OFF
ECHO 6940:ceci est le message OK dans le capteur Formation
REM si renvoie 0=ok si renvoie 1=warning si renvoie 2=erreur
Exit 0
```

Renverrait

✓ capteur Capteur personnalisé avec EXE/script ★★★★★

Vue d'ensemble Données en temps réel 2 Jours 30 Jours 365 Jours Données historiques Journal Paramètres Notifications Canaux

Dernier message : ceci est le message OK dans le capteur Formation

Dernière analyse: 46 s Dernière OK: 46 s Dernière erreur: Disponibilité: 100,0000% Temps mort: 0,0000% Couverture: 100%

| Valeur | Temps d'exécution | Canal | ID | Dernière valeur |
|--------|-------------------|-------------------|----|-----------------|
| | 61 ms | Temps d'exécution | 1 | 61 ms |
| | | Temps mort | -4 | |
| | | Valeur | 2 | 6 940 # |

6 940 # 0 6 940 #

Alors que

```
cabare batch 3.bat - Bloc-notes
Fichier Edition Format Affichage ?
@ECHO OFF
ECHO 100:ceci est le message erreur dans le capteur Formation

REM si renvoie 0=ok si renvoie 1=warning si renvoie 2=erreur
Exit 2
```

Renvoie

capteur Capteur personnalisé avec EXE/script ★★★★★

Vue d'ensemble Données en temps réel 2 Jours 30 Jours 365 Jours Données historiques Journal Paramètres Notifications Canaux

Dernier message :
Erreur de système : ceci est le message erreur dans le capteur Formation (code : PE022)

| Dernière analyse: 45 s | Dernier OK: 165 s | Dernière erreur: 45 s | Disponibilité: 76,3562% | Temps mort: 23,6438% | Couverture: 100% |
|---------------------------|----------------------|--------------------------|----------------------------|-------------------------|---------------------|
| Valeur | Temps d'exécution | Canal | ID | Dernière valeur | Minimum |
| | Pas de données | Temps d'exécution | 1 | | Pas de données |
| | | Temps mort | -4 | | |
| | | Valeur | 2 | | Pas de données |

Premier script powershell:

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

PARAMÈTRES DU CAPTEUR

Important : Le fichier EXE doit être exécuté sur l'ordinateur sur lequel le probe parent est installé, et non sur le dispositif parent. Le répertoire de travail des fichiers "exe" est le répertoire du probe, "vbs, ps1" mais d'autres fichiers de scripts peuvent utiliser d'autres répertoires de travail.

Script/EXE:

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

```
C:\Windows\system32>powershell
Windows PowerShell
Copyright (C) 2015 Microsoft Corporation. Tous droits réservés.

PS C:\Windows\system32> get-executionpolicy
Restricted
PS C:\Windows\system32> set-executionpolicy unrestricted
PS C:\Windows\system32> get-executionpolicy
Unrestricted
```

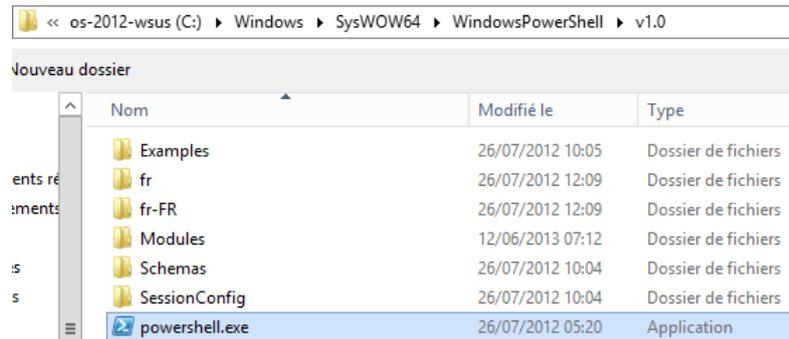
N.B: si on est sur un serveur 64bits, il faut également le faire pour le Powershell 32bits, qui est le powershell utilisé par Prtg,

donc dans Windows PowerShell (x86) on exécute également la même commande

```
Administrateur : Windows PowerShell (x86)
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 à l'adresse http://go.microsoft.com/fwlink/?LinkID=135170. Voulez-vous modifier la stratégie
d'exécution ?
[O] Oui [N] Non [S] Suspendre [?] Aide (la valeur par défaut est « 0 ») : o
PS C:\Users\Administrateur.CABARE-INTRA> _
```

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

Correspondant 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 | <code>%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell.exe</code> |
| 64-bit (x64) Powershell executable | <code>%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe</code> |
| 32-bit (x86) Powershell ISE executable | <code>%SystemRoot%\SysWOW64\WindowsPowerShell\v1.0\powershell_ise.exe</code> |
| 64-bit (x64) Powershell ISE executable | <code>%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell_ise.exe</code> |

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 | <code>%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell.exe</code> |
| 32-bit (x86) Powershell ISE executable | <code>%SystemRoot%\system32\WindowsPowerShell\v1.0\powershell_ise.exe</code> |

Puis

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

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

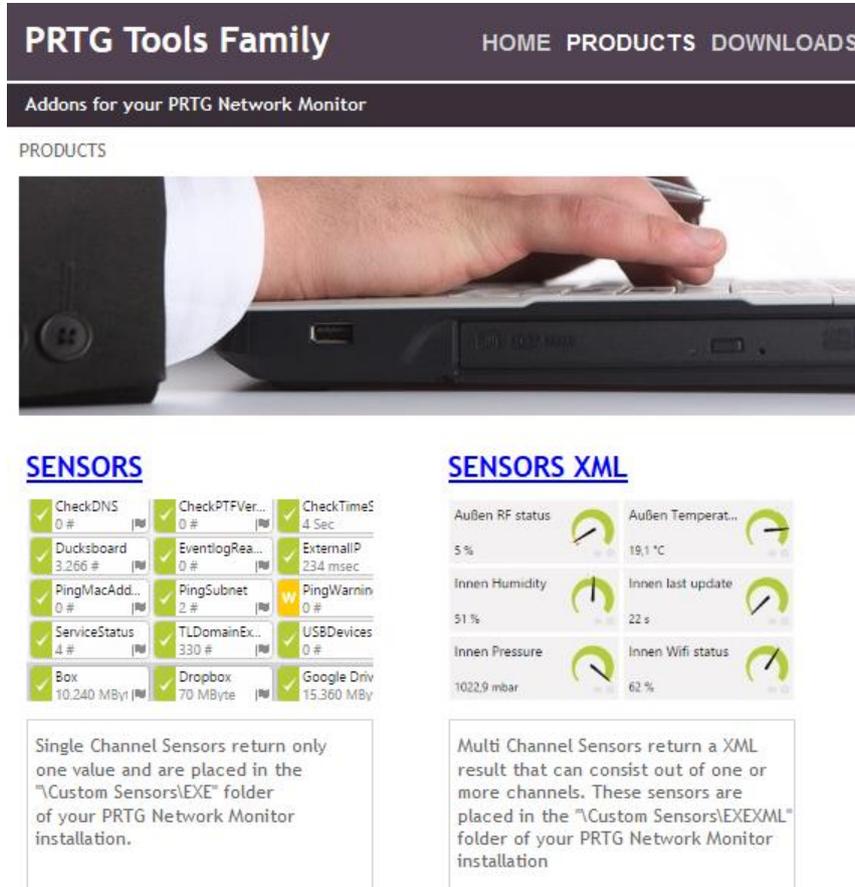
```
PS C:\Windows\system32> enable-psremoting
WinRM a été mis à jour pour recevoir des demandes.
Le type du service WinRM a été correctement modifié.
Le service WinRM a démarré.

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,



PRTG Tools Family HOME PRODUCTS DOWNLOADS

Addons for your PRTG Network Monitor

PRODUCTS



SENSORS

| | | |
|-------------------------|--------------------------|-----------------------------|
| ✓ CheckDNS 0 # | ✓ CheckPTFVer... 0 # | ✓ CheckTimeS 4 Sec |
| ✓ Ducksboard 3.266 # | ✓ EventlogRea... 0 # | ✓ ExternalIP 234 msec |
| ✓ PingMacAdd... 0 # | ✓ PingSubnet 2 # | ✓ PingWarnin 0 # |
| ✓ ServiceStatus 4 # | ✓ TLDomainEx... 330 # | ✓ USBDevices 0 # |
| ✓ Box 10.240 MByte | ✓ Dropbox 70 MByte | ✓ Google Driv 15.360 MBy |

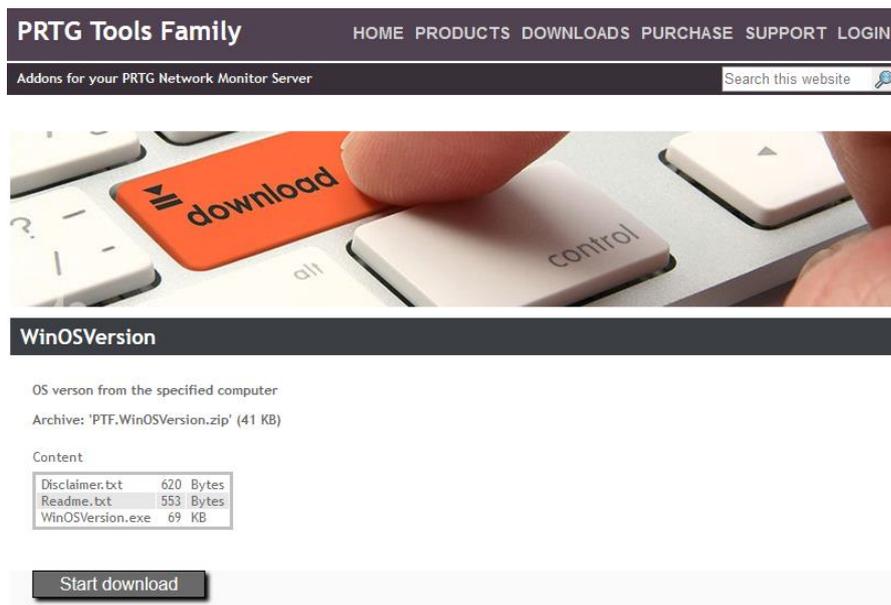
Single Channel Sensors return only one value and are placed in the "\Custom Sensors\EXE" folder of your PRTG Network Monitor installation.

SENSORS XML

| | |
|-------------------------------|------------------------------|
| Außen RF status 5 % | Außen Temperat... 19,1 °C |
| Innen Humidity 51 % | Innen last update 22 s |
| Innen Pressure 1022,9 mbar | Innen Wifi status 62 % |

Multi Channel Sensors return a XML result that can consist out of one or more channels. These sensors are placed in the "\Custom Sensors\EXEXML" folder of your PRTG Network Monitor installation

qui pour être utilisés doivent simplement être placés dans le bon dossier **on récupère par exemple un capteur qui donne la version de Windows**



PRTG Tools Family HOME PRODUCTS DOWNLOADS PURCHASE SUPPORT LOGIN

Addons for your PRTG Network Monitor Server

Search this website



WinOSVersion

OS version from the specified computer

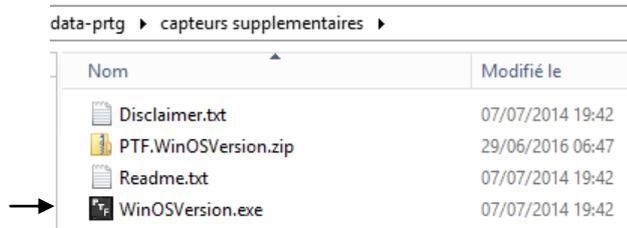
Archive: 'PTF.WinOSVersion.zip' (41 KB)

Content

| | |
|------------------|-----------|
| Disclaimer.txt | 620 Bytes |
| Readme.txt | 553 Bytes |
| WinOSVersion.exe | 69 KB |

Start download

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



Installer un capteur Script/EXE:

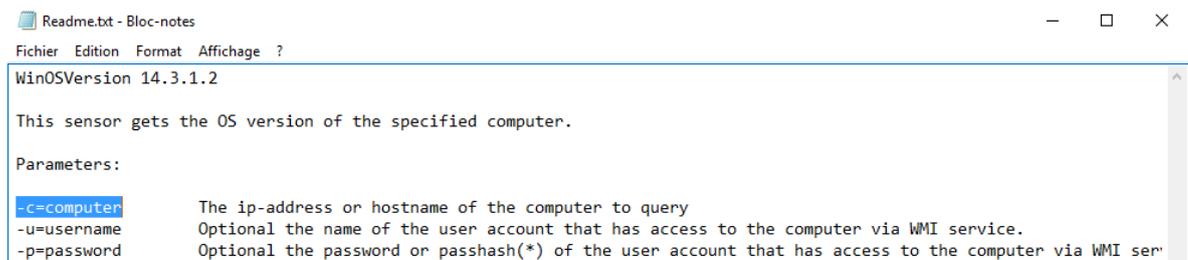
Et on le colle pour celui-ci dans le dossier

Program Files (x86) > PRTG Network Monitor > Custom Sensors > EXE

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 livré avec le capteur, par exemple ici



Donc cela donnerait

PARAMÈTRES DE BASE DU CAPTEUR

| | |
|------------------|--------------------------------------|
| Nom du capteur | Capteur personnalisé avec EXE/script |
| Balises parentes | |
| Balises | exesensor x |
| Priorité | ★★★★ |

PARAMÈTRES DU CAPTEUR

Important : Le fichier EXE doit être exécuté sur l'ordinateur sur lequel le probe parent est installé, et non sur le dispositif parent. Le répertoire de travail des fichiers 'exe' est le répertoire du probe, 'vbs, ps1' mais d'autres fichiers de scripts peuvent utiliser d'autres répertoires de travail.

| | |
|----------------------|---|
| Script/EXE | WinOSVersion.exe |
| Paramètres | -c=192.168.1.10 |
| Environnement | <input checked="" type="radio"/> Environnement par défaut <input type="radio"/> Utilisez les paramètres fictifs comme variables d'environnement |
| Contexte de sécurité | <input type="radio"/> Utiliser le contexte de sécurité du service du probe <input checked="" type="radio"/> Utiliser les données d'accès Windows des équipements parents |

Création d'une carte:

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

Ajouter une carte (Étape 1 sur 2)

NOM DE LA CARTE

Nom de la carte

DISPOSITION DE LA CARTE

Largeur de la carte

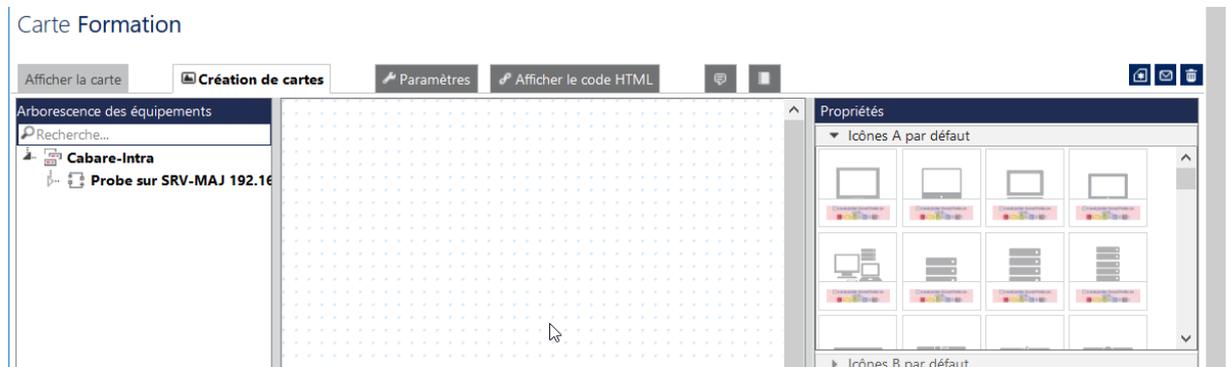
Hauteur de la carte

Image en arrière-plan (en option) **Aucun fichier sélectionné.**

ACCÈS PUBLIC

Autoriser l'accès public **Aucun accès public (la carte ne peut pas être consultée sans nom d'utilisateur)** Autoriser l'accès public (la carte peut être consultée grâce à une simple URL)

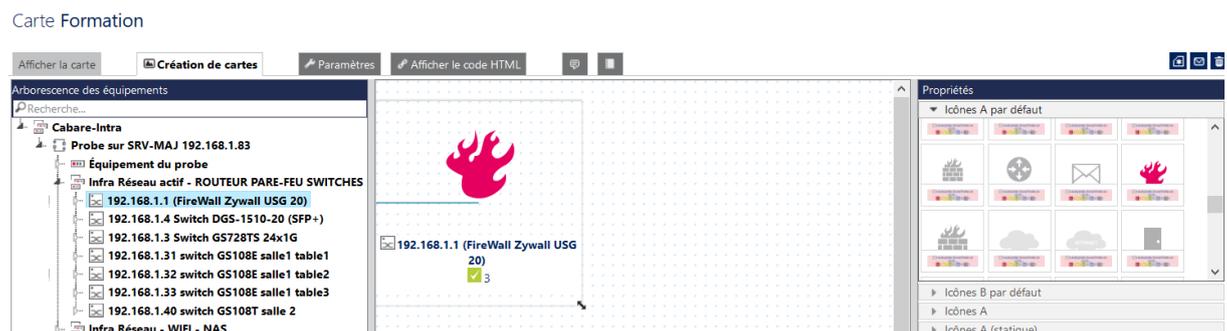
Puis avec **Continuer** on obtient



On y trouve :

Les éléments de PRTG
Selon notre configuration

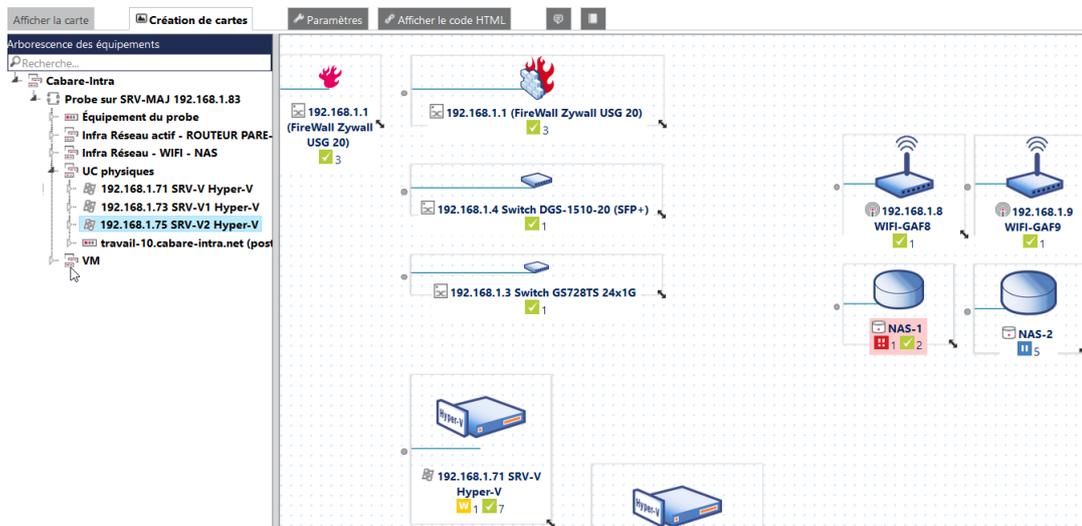
des icones
soit dynamiques avec capteurs
Soit statiques (illustratives)



Poser des icônes :

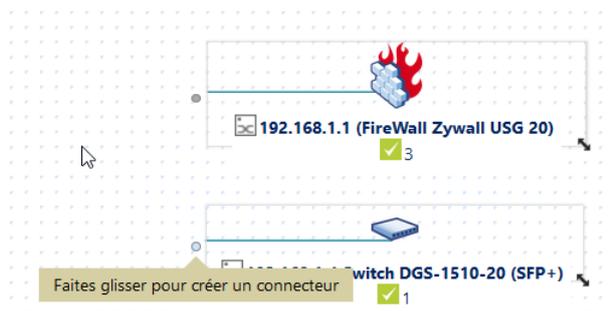
Pour créer une nouvelle carte on demande **carte** un assistant de déclenche, on donne un nom et une taille principalement

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

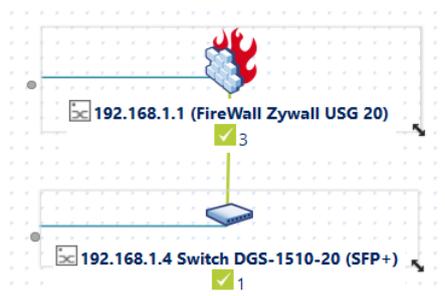


Lier des icônes :

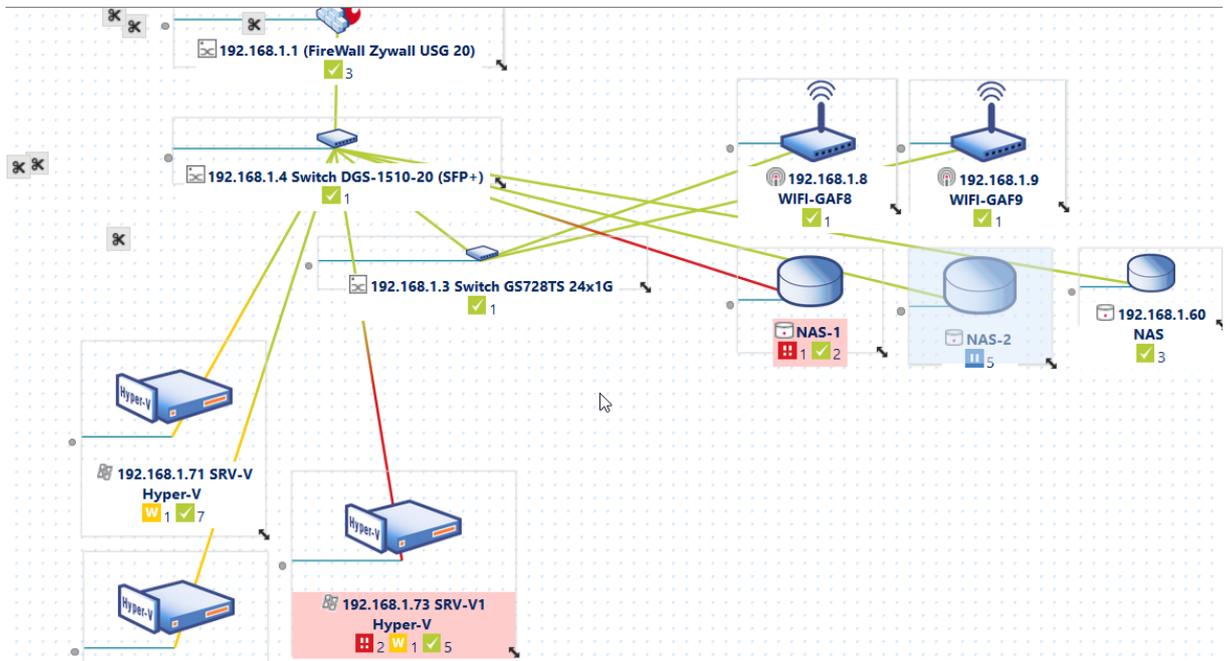
Il suffit avec la souris de faire glisser le point d'ancrage vers l'éléments souhaité



Pour obtenir



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



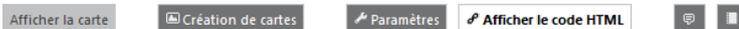
Publier une carte:

Il faut demandr Afficher le code HTML et on choisit

Carte structure complète



Et on choisit



PRTG Network Monitor vous facilite le travail d'intégration des résultats de surveillance dans d'autres pages Web :

OPTION 1 : CRÉER UN LIEN VERS UNE PAGE WEB AVEC UNE CARTE EXIGEANT LES DONNÉES D'ACCÈS DU NOM D'UTILISATEUR.

Créer un lien vers le ou les adresses URL suivantes et il sera demandé à l'utilisateur de fournir les données d'accès de son nom d'utilisateur pour afficher la carte :

<http://srv-maj.cabare-intra.net:8080/mapshow.htm?id=2842>

OPTION 2 : CRÉER UN LIEN VERS UNE PAGE WEB QUI AFFICHE LA CARTE SANS NOM D'UTILISATEUR

Utilisez une URL avec "mapid-password" (définissez le paramètre "Accès public" de la carte sur "Autoriser l'accès public"):

<http://srv-maj.cabare-intra.net:8080/public/mapshow.htm?id=2842&mapid=D18696EC-FFF2-4395-B55E-172D6D381523>

OPTION 3 : AFFICHER UNE CARTE DANS D'AUTRES PAGES WEB UTILISANT UNE IFRAME

Collez le code HTML suivant dans votre page Web et réglez le paramètre « Accès public » de la carte sur « Autoriser l'accès public ».

```
<iframe width=1024 height=768 frameborder="1"
src="http://srv-maj.cabare-intra.net:8080/public/mapshow.htm?id=2842&mapid=D18696EC-FFF2-4395-B55E-172D6D381523">
</iframe>
```


Cabare-Intra

Probe sur SRV-MAJ 192.168.1.83

| | | | | | |
|--|------|---------------|---------------------------------------|--|-------------------------|
| Équipement du probe | | État du probe | État du serveur principal | État du système | Common SaaS Check |
| | | 100 % | 100 % | 100 % | 100 % |
| Infra Réseau actif - ROUTEUR PARE-FEU SWITCHES | | | | | |
| 192.168.1.1 (FireWall Zywall USG 20) | PING | 1 ms | (007) eth0 Traffic entrant Fibre | (008) eth1 Traffic LAN | |
| 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 | 0 ms | | | |
| 192.168.1.33 switch GS108E salle1 table3 | PING | 18 ms | | | |
| 192.168.1.40 switch GS108T salle 2 | PING | 4 ms | | | |
| Infra Réseau - WIFI - NAS | | | | | |
| 192.168.1.7 WIFI-GAF7 | | | | | |
| <i>If Spare (25/06/2016 05:56:05)</i> | | | | | |
| 192.168.1.8 WIFI-GAF8 | PING | 0 ms | | | |
| 192.168.1.9 WIFI-GAF9 | PING | 0 ms | | | |
| NAS-1 | PING | 0 ms | Capteur de certificat SSL (port 4...) | Vérification de sécurité SSL (port...) | |
| NAS-2 | PING | 0 ms | Capteur de certificat SSL (port 4...) | Vérification de sécurité SSL (port...) | HTTP 61 ms FTP 70 ms |
| 192.168.1.60 NAS | PING | 0 ms | HTTP 15 ms | FTP 61 ms | |

UC physiques

| | | | | | | | | |
|---|------|------|-------------------------|-----------------------------------|-----------------------------------|-------------------------------|---------------------|---------------------------------------|
| 192.168.1.71 SRV-V Hyper-V | PING | 0 ms | Serveur hôte Hyper V | Memory: Physical Memory | Disk Free: C:\Labelos-2012r2 S... | État des mises à jour Windows | Espace disque libre | Espace disque libre (plusieurs le...) |
| 192.168.1.73 SRV-V1 Hyper-V | PING | 0 ms | Serveur hôte Hyper V | Memory: Physical Memory | Disk Free: C:\Labelos-2012r2 S... | État des mises à jour Windows | Espace disque libre | Espace disque libre (plusieurs le...) |
| 192.168.1.75 SRV-V2 Hyper-V | PING | 0 ms | Serveur hôte Hyper V | Memory: Physical Memory | Disk Free: C:\Labelos-2012r2 S... | État des mises à jour Windows | Espace disque libre | Espace disque libre (plusieurs le...) |
| travail-10.cabare-intra.net (poste principal perso) | PING | 0 ms | RDP (Bureau à distance) | Capteur personnalisé avec EXE/... | | | | |

VM

| | | | | | | | | |
|-----------------------|------|------|---------------------|-------------------------|-------------------------------------|-------------------------------|---------------------------------------|--|
| 192.168.1.90 SRV-DC | PING | 0 ms | Charge de l'UC SNMP | Memory: Physical Memory | Disk Free: C:\Label: Serial Numb... | État des mises à jour Windows | DNS | Capteur EXE/script OsVersion |
| 192.168.1.91 SRV-DC1 | PING | 0 ms | Charge de l'UC SNMP | Memory: Physical Memory | Disk Free: C:\Label: Serial Numb... | État des mises à jour Windows | DNS | Capteur EXE/script OsVersion |
| 192.168.1.92 SRV-DC2 | PING | 0 ms | Charge de l'UC SNMP | Memory: Physical Memory | Disk Free: C:\Labelos-système ... | État des mises à jour Windows | DNS | Capteur EXE/script OsVersion |
| 192.168.1.80 SRV-GTW | PING | 0 ms | Charge de l'UC SNMP | Memory: Physical Memory | Disk Free: C:\Label: Serial Numb... | État des mises à jour Windows | | |
| 192.168.1.81 SRV-RDS1 | PING | 0 ms | Charge de l'UC SNMP | Memory: Physical Memory | Disk Free: C:\Label: Serial Numb... | État des mises à jour Windows | Espace disque libre | Capteur de certificat SSL (port 4...) |
| 192.168.1.85 SRV-WDS | PING | 0 ms | Charge de l'UC SNMP | Memory: Physical Memory | Mémoire | État des mises à jour Windows | Espace disque libre (plusieurs le...) | Vérification de sécurité SSL (port...) |
| 192.168.1.83 SRV-MAJ | Ping | 0 ms | Charge de l'UC SNMP | Memory: Physical Memory | Disk Free: C:\Labelos-2012-ws... | État des mises à jour Windows | Espace disque libre (plusieurs le...) | Espace disque libre |