

## TP SUPERVISION PRTG

### /Introduction/

En informatique et pour n'importe quelle entreprise la supervision des équipements est cruciale pour avoir un retour efficace et rapide, savoir s'ils sont en panne, s'ils surchauffent ou encore si leurs utilisations sont anormales, un débit de bande passante trop haut pourrait signifier une attaque informatique.

Peu importe la situation il faut pouvoir recevoir l'information le plus vite possible pour réagir en conséquence, nous allons donc voir comment nous pouvons superviser nos équipements avec le logiciel PRTG et avec le protocole SNMP (simple network management protocol) et quelques autres outils.

### 1/ Installation de PRTG

PRTG est un logiciel de monitoring d'équipement, il suffit d'aller sur leur site internet pour le télécharger, puis lancer l'installation.

Quelques informations seront demandées, adresse mail, chemin d'installation, etc. Après ces quelques informations et plusieurs clics sur le bouton suivant on pourra lancer PRTG.

Installation - PRTG Network Monitor

**Votre adresse e-mail**  
Fournissez les informations suivantes pour poursuivre l'installation

Saisissez votre adresse e-mail. PRTG enverra à cette adresse des notifications importantes pour vous alerter lorsque les capteurs de votre installation détectent des pannes, des valeurs suspectes, ou des problèmes critiques du système.

**Votre adresse e-mail:**

Paessler vous enverra également à cette adresse des informations sur nos produits et services. Vous pouvez à tout moment vous désinscrire de la réception de ces informations en écrivant à [privacy@paessler.com](mailto:privacy@paessler.com). Nous protégeons vos données personnelles.  
[Consultez notre politique de confidentialité pour en savoir plus.](#)

[www.paessler.com](http://www.paessler.com)

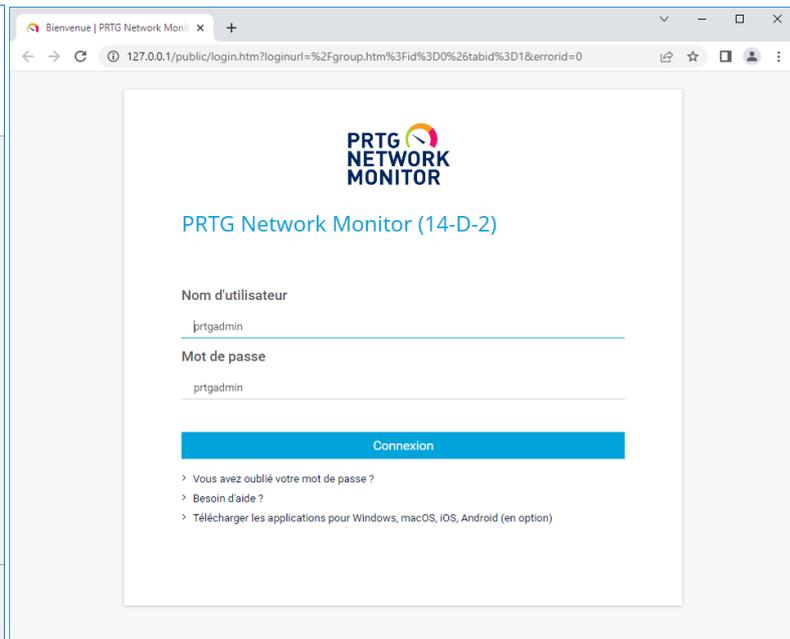
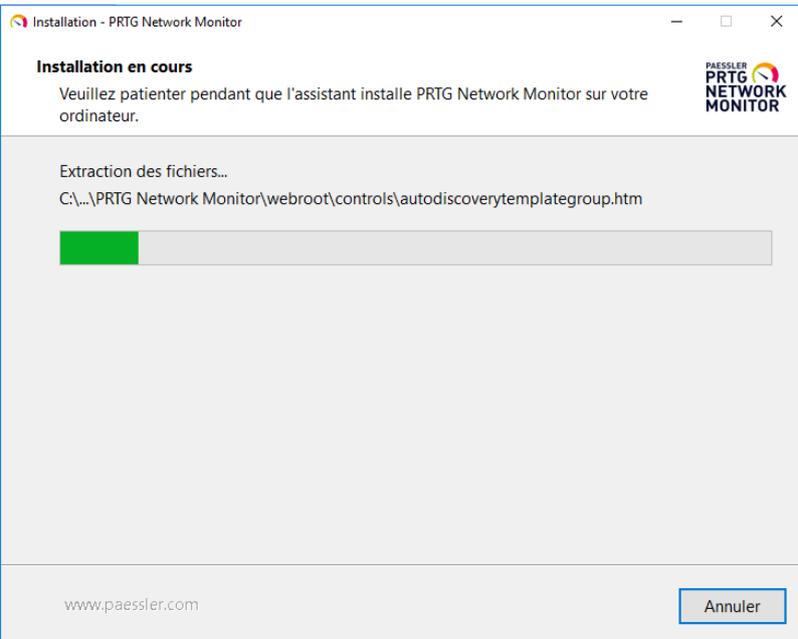
Installation - PRTG Network Monitor

**Emplacement**  
Sélectionnez l'emplacement de l'installation et du stockage des données.

**Répertoire d'installation**  
Changez le répertoire d'installation ici, si nécessaire.

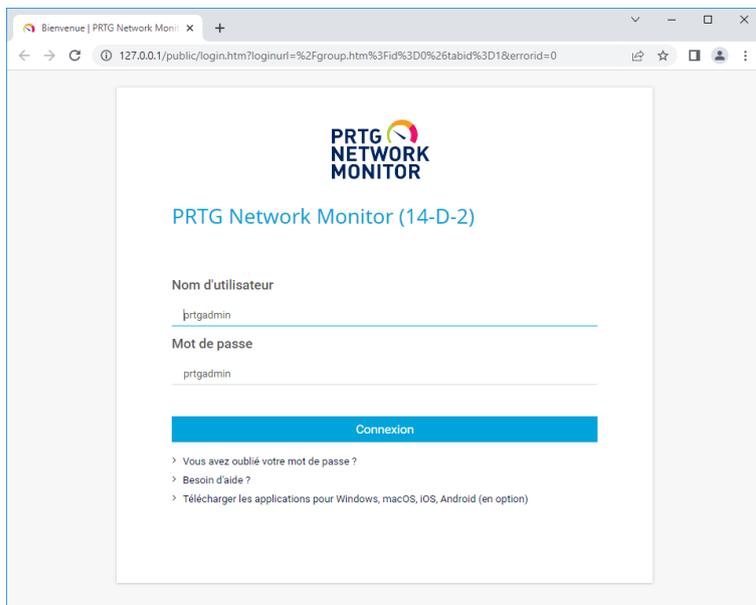
**Répertoire de données**  
Vous pouvez changer plus tard le répertoire de données, si nécessaire.

[www.paessler.com](http://www.paessler.com)



## 2/ Configuration et création d'équipements

Une fois l'installation terminée on pourra lancer PRTG via la petite icône sera apparue sur le bureau.



On arrive sur cette page de connexion avec des identifiants de base, après s'être connecté on voit directement deux messages qui concerne le mot de passe et le SSL, nous allons donc modifier notre mot de passe pour le sécuriser et activer SSL.

### Définir un mot de passe sécurisé ✕

Le compte d'utilisateur de l'administrateur système de PRTG utilise le mot de passe par défaut « prtgadmin ». Modifiez-le pour sécuriser votre interface Web PRTG.

Ceci est absolument obligatoire si vous autorisez l'accès à votre interface Web PRTG depuis internet (l'extérieur de votre pare-feu) !

[Modifier le mot de passe par défaut](#)

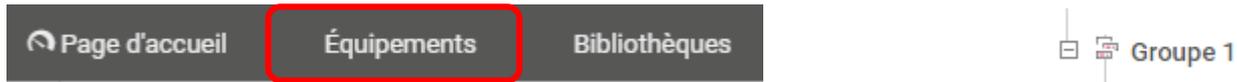
### Activer SSL/TLS pour l'interface Web PRTG. ✕

La connexion de votre navigateur à ce serveur central de PRTG n'est pas sécurisée par SSL/TLS.

Il est préférable de passer à SSL/TLS, particulièrement si votre interface Web PRTG est accessible depuis internet (en dehors de votre pare-feu).

[Passer à SSL/TLS](#)

Dans l'onglet en haut de page on va cliquer sur « équipements », puis sur « Groupe 1 ».



Ensuite sur le « + » on va pouvoir créer un groupe puis dans ce groupe un premier équipement.



Dans un premier temps on va superviser notre pc client, on va donc l'ajouter.

Ajouter un équipement au groupe 1er Groupe

< Annuler la création de l'équipement

Nom et adresse de l'équipement

Nom de l'équipement

Version IP  IPv4  IPv6

Adresse IPv4/Nom DNS

Balises

Icône de l'équipement

Identification d'équipements et découverte automatique

Niveau de la découverte automatique  Pas de découverte automatique  
 Découverte automatique standard (recommandé)  
 Découverte automatique détaillée  
 Découverte automatique à partir de modèles d'équipement spécifiques

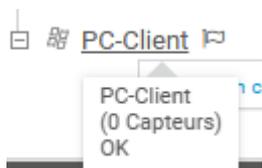
Informations d'identification pour systèmes Windows

Hériter de 1er Groupe (Nom de domaine ou d'ordinateur: «vide», Nom d...)

Nom de domaine ou d'ordinateur

Nom d'utilisateur

Mot de passe



On va également ajouter notre serveur, on s'en servira plus tard. (Indiquez le nom que vous souhaitez voir affiché ainsi que l'adresse IP de l'équipement, et pour le SNMP indiquez la communauté voulue)

## Nom et adresse de l'équipement

### Nom de l'équipement ⓘ

WIN-SRV-PC

### Version IP ⓘ

IPv4

IPv6

### Adresse IPv4/Nom DNS ⓘ

192.168.1.100

### Informations d'identification pour les équipements SNMP

hériter de 1er Groupe (Version SNMP: V2, Port SNMP: 161, Délai d'exp...)

#### Version SNMP ⓘ

SNMP v1

SNMP v2c (recommandé)

SNMP v3

#### Chaîne de communauté ⓘ

pc|

#### Port SNMP ⓘ

161

#### Délai d'expiration (s) ⓘ

5

## Informations d'identification pour systèmes Windows

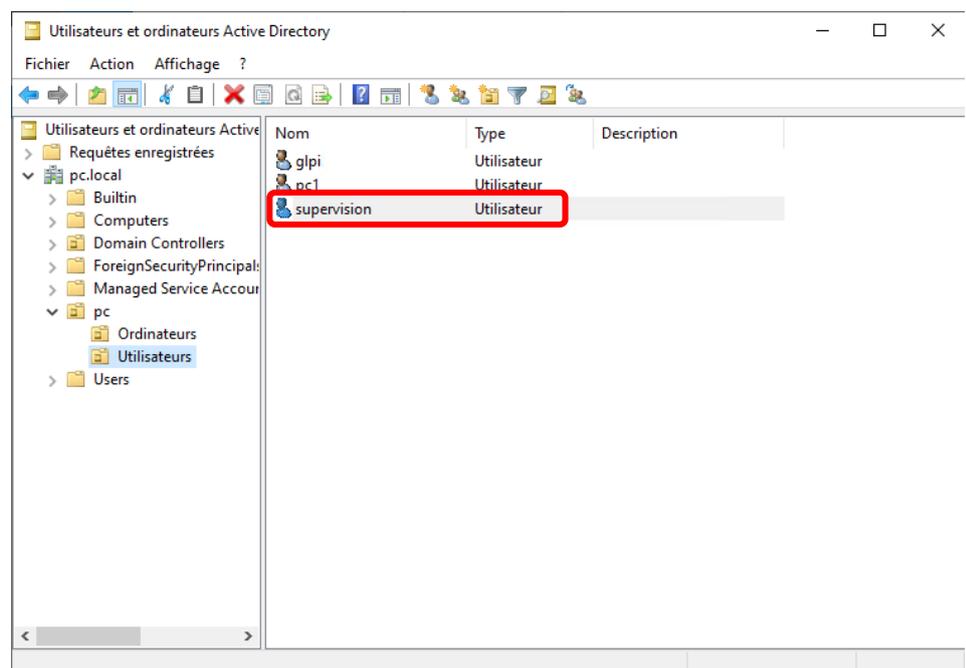
hériter de 1er Groupe (Nom de domaine ou d'ordinateur: <vide>, Nom d...)

Nom de domaine ou d'ordinateur ⓘ pc.local

Nom d'utilisateur ⓘ supervision

Mot de passe ⓘ .....

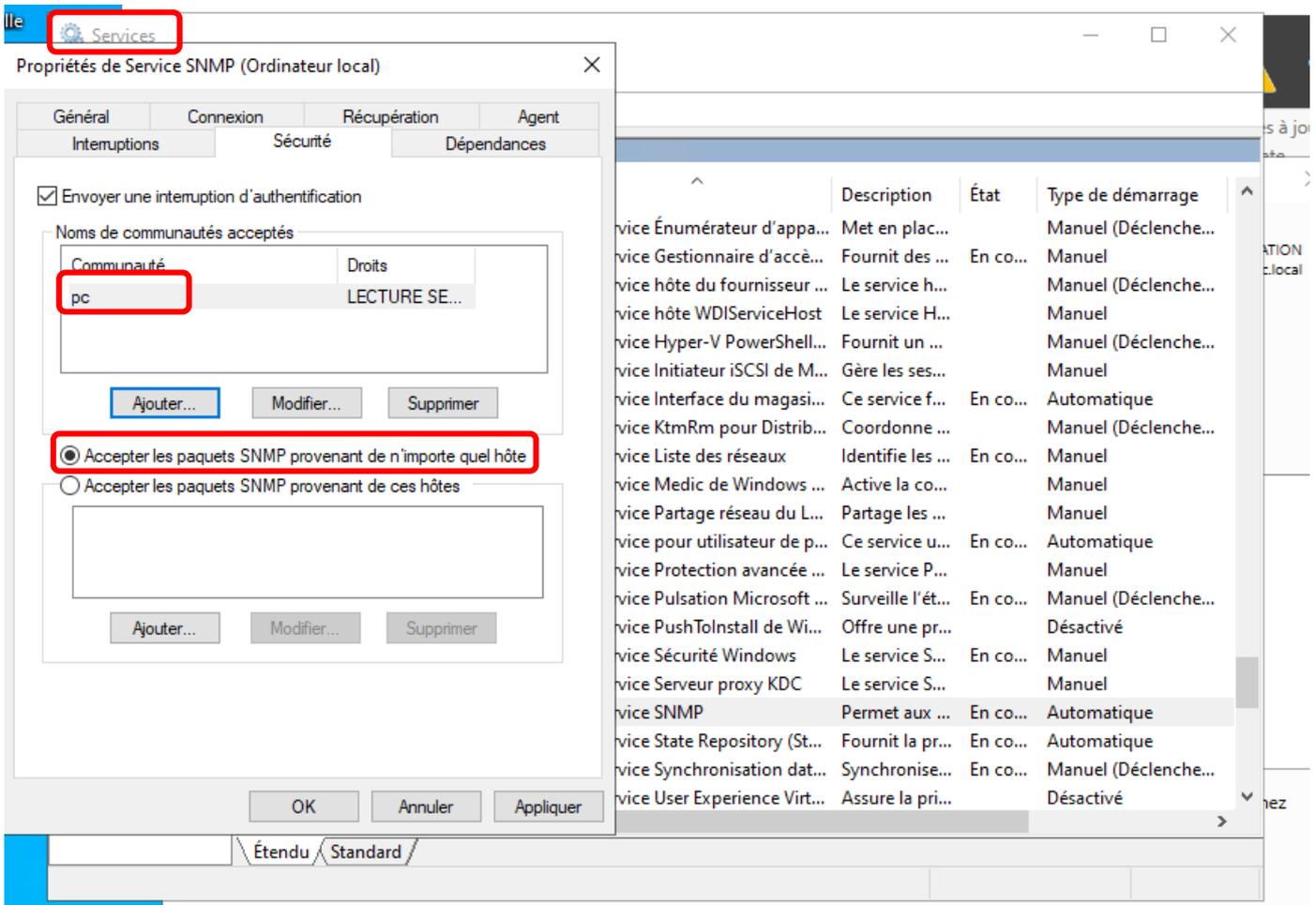
On a ajouté un utilisateur pour notre équipement « serveur » sur prtg on va donc également créer sur notre serveur cet utilisateur « supervision » dédié à cette tâche.



### 3/ SNMP et capteurs

Le protocole SNMP va nous être très utile pour récolter les données de nos équipements, à l'aide de différents OID (Object Identifier) il va pouvoir remonter énormément d'informations venant d'un switch, d'un routeur ou encore de caméras de surveillances. Une fois les informations récoltées elles sont envoyées dans une base de données puis redirigées vers un superviseur, ici PRTG, le protocole SMTP (simple mail transfer protocol) est également utile pour pouvoir configurer des alertes automatiques vers une adresse mail donnée.

Revenons à notre serveur, dans les services on va chercher « service SNMP » et dans propriétés puis sécurité on ajoutera notre communauté et on cochera également « Accepter les paquets SNMP provenant de n'importe quel hôte ». (Si SNMP n'est pas installé il faudra l'installer sur le serveur local)



Pour des premiers tests j'ai installé deux capteurs « Ping » et WMI « espace disque » sur mon pc client on peut voir qu'ils sont bien actifs et fonctionnels.



On va maintenant créer plusieurs capteurs sur notre équipement serveur.

Ajouter un capteur à l'équipement WIN-SRV-PC [192.168.1.100]

**Que peut-on superviser ?**

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

**Type de système cible ?**

Windows     Stockage et serveur de fichier     Services en cloud  
 Linux/macOS     Serveur de messagerie  
 OS de virtualisation     Base de données

**Technologie utilisée ?**

Ping     HTTP     PowerShell  
 SNMP     SSH     Récepteur de message Push  
 WMI     Renflage de paquets     Cloud PRTO  
 Compteurs de performance     Protocoles de flux

< Annuler la création de capteur > Vous recherchez d'autres types de c...

Recherche 🔍 Tapez pour rechercher un nom ou une description 40 Types de capteurs disponibles

Types de capteurs les plus utilisés

**AWS Alarm v2 (NOUVEAU)** ?

Monitors the status of an AWS alarm by reading its data from Amazon CloudWatch

Requires credentials for AWS. Shows the status and other metrics of an AWS alarm. Every sensor scan can generate costs in your AWS account based on the number of API calls.

**Cloud HTTP v2** ?

Monitors a web server and shows the loading time from different locations on a number of continents

Requires access to the internet. The probe system must be able to communicate with the PRTO Cloud. The address in the parent device settings must be reachable over the internet. You cannot monitor localhost or target devices that are only reachable within your private network.

**HTTP** ?

Supervise un serveur web en utilisant HTTP

Indique si un site Web ou un élément de site web spécifique est accessible.

Ajouter un capteur à l'équipement WIN-SRV-PC [192.168.1.100]

(Étape 2 à 2)

< Annuler Créer

**Paramètres de base du capteur**

Nom du capteur ⓘ HTTP

Balises parentes ⓘ

Balises ⓘ httpsensor x

Priorité ⓘ ★★☆☆☆

---

**Paramètres propres au HTTP**

Délai d'expiration (s) ⓘ 60

URL ⓘ http://192.168.1.35

Méthode de requête ⓘ  GET  
 POST  
 HEAD

Héritage SNI ⓘ  Hériter le SNI de l'équipement parent  
 Ne pas hériter le SNI de l'équipement parent

---

**Paramètres proxy pour capteurs HTTP**

hériter de

WIN-SRV-PC  
(Adresse IP/Nom DNS: <vide>, Port: 8080, Nom d...)

J'ai ajouté dans un premier temps un capteur CPU (via SNMP) pour voir la charge cpu actuelle, un capteur Ethernet qui renvoie la bande passante (via SNMP) et un capteur HTTP qui m'indique si mon serveur web est actif (serveur web GLPI également utilisé dans un autre tp).

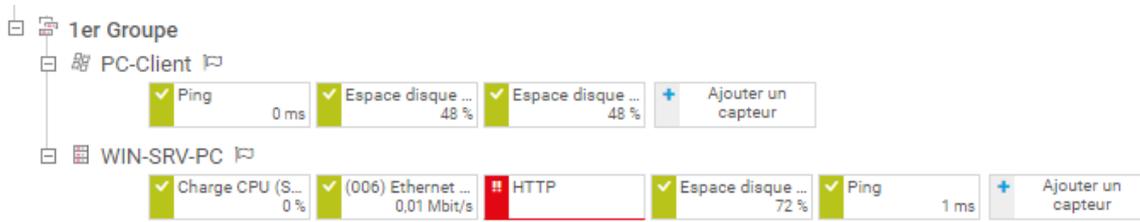
PC-Client

- ✓ Ping 0 ms
- ✓ Espace disque ... 48 %
- + Ajouter un capteur

WIN-SRV-PC

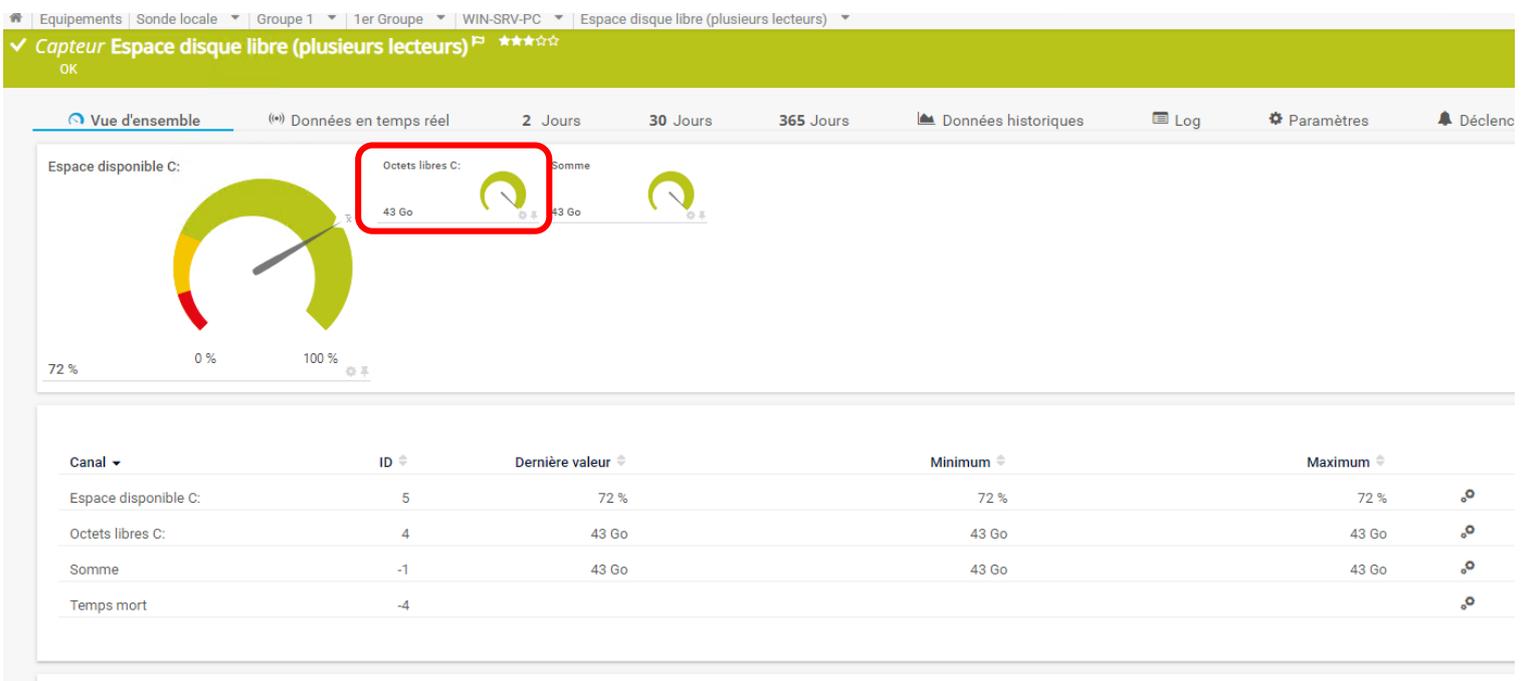
- ✓ Charge CPU (S... 0 %
- ✓ (006) Ethernet ... 0,02 Mbit/s
- ✓ HTTP 22 ms
- + Ajouter un capteur

J'ai ensuite ajouté un capteur ping pour voir la disponibilité de mon serveur en direct et un capteur WMI comme pour le pc client, ils sont tous deux fonctionnels et on peut également voir que le capteur HTTP renvoie une alerte, en effet je l'ai éteint et le retour se fait correctement.



**!! Capteur HTTP** ★★☆☆☆  
 Connection timed out Socket Error # 10060 Connection timed out. (erreur de socket # 10060)

Si on clique sur le capteur « espace disque » on arrive sur cette page et on peut voir en direct le stockage disponible sur le serveur (43Go libres), ce qui peut s'avérer très utile car manquer de stockage sur un serveur peut vite être problématique.



Une autre fonctionnalité intéressante sera les alertes, elles peuvent être mise en place pour tous types de capteurs et nous allons voir notre capteur WMI sur notre serveur comment en configurer une.

Rien de bien compliqué il suffira sur la page ci-dessus de cliquer sur « Déclencheurs de notifications » une fois sur cette page cliquer sur « + » et ajouter une alerte sur seuil ou état selon le besoin, ici je vais choisir alerte sur seuil pour définir un seuil critique d'espace disque restant.

The screenshot shows the PRTG monitoring interface for a device named 'Capteur Espace disque libre (plusieurs lecteurs)'. The breadcrumb navigation at the top includes: Équipements > Sonde locale > Groupe 1 > 1er Groupe > WIN-SRV-PC > Espace disque libre (plusieurs lecteurs). The main navigation bar contains: Vue d'ensemble, Données en temps réel, 2 Jours, 30 Jours, 365 Jours, Données historiques, Log, Paramètres, and Déclencheurs de notifications (highlighted with a red box). Below the navigation, there are three sections for notification triggers:

- Déclencheurs de notifications:** A table with columns 'Type', 'Règle', and 'Actions'. It lists two triggers for 'Déclencheur sur seuil (ID: 1)'. The first rule is 'Lorsque le canal Espace disponible C: (%) est en dessous de 10 pendant au moins 60 secondes, exécuter @ Envoyer un email à tous les membres du groupe Groupe d'utilisateurs PRTG'. The second rule is 'Lorsque la condition ne s'applique plus, exécuter @ Envoyer un email à tous les membres du groupe Groupe d'utilisateurs PRTG'. An 'Enregistrer le déclencheur' button is visible.
- Déclencheurs pouvant être hérités des objets parents:** Radio buttons for 'Hériter de tous les déclencheurs des objets parents et utiliser les déclencheurs définis ci-dessus' (selected) and 'Utiliser uniquement les déclencheurs définis ci-dessus'. Below is a table with columns 'Type', 'Règle', and 'hérité de'. It lists two triggers for 'Déclencheur sur état'. The first rule is 'Lorsque le statut du capteur est Erreur pendant au moins 600 secondes, exécuter @ Notification par email et message Push à l'administrateur'. The second rule is 'Lorsque le statut du capteur est Erreur pendant au moins 900 secondes, exécuter aucune notification et répéter l'opération toutes les 0 minutes'. The 'hérité de' column shows 'Racine'.
- Déclencheurs définis dans les bibliothèques:** A table with columns 'Type', 'Règle', and 'hérité de'. It lists one trigger for '(aucun déclencheur défini)'.

Notre alerte est bien configurée et fonctionnelle.

## /Conclusion/

Nous avons vu comment installer et configurer PRTG ainsi que plusieurs capteurs à l'aide de SNMP sur notre pc client et notre serveur et activer une alerte sur un de ces capteurs.

Notre outil de supervision est opérationnel, attention toutefois à ne pas surcharger l'interface de supervision au risque de s'y perdre, cela serait contreproductif. Utilisez des capteurs essentiels pour les machines importantes de votre réseau tel que vos serveurs, firewall ou caméras de surveillances.