



La possibilité de superviser un commutateur et un routeur est également intéressante, surtout si vous pouvez utiliser des capteurs spécifiques (propres au constructeur).

A minima vous pouvez installer des capteurs type « ping » pour vérifier qu'ils sont en ligne, et vérifier la connectivité à Internet le cas échéant.

## Tutoriel – Préparation de la machine

Faire un clone complet.

Modifier la configuration avant redémarrage :

Processeurs : 4 cores, changer également le type en « host »

Carte réseau : Intel E1000E

Machine virtuelle 230097 (dduro-W11-PRTG-ter) sur le nœud pve14		Aucune étiquette
Résumé	Ajouter   Supprimer   Éditer   Action disque   Revenir en arrière	
Console	Mémoire	4.00 Gio
Matériel	Processeurs	4 (1 sockets, 4 cores) [host]
Cloud-Init	BIOS	OVMF (UEFI)
Options	Affichage	Par défaut
Historique des tâches	Machine	pc-q35-10.0
Instantanés	Contrôleur SCSI	VirtIO SCSI single
Pare-feu	Lecteur CD/DVD (ide2)	none,media=cdrom
	Disque dur (scsi0)	datastore-pve14:vm-230097-disk-1,discard=on,iotread=1,size=100G
	Carte réseau (net0)	e1000e=BC:24:11:F9:9A:13,bridge=vlan230,firewall=1
	Disque EFI	datastore-pve14:vm-230097-disk-0,efitype=4m,pre-enrolled-keys=1,size=4M
	État TPM	datastore-pve14:vm-230097-disk-2,size=4M,version=v2.0

Éditer: Carte réseau

Pont (bridge):  Modèle:

Étiquette de VLAN:  Adresse MAC:

Pare-feu:

Aide Avancé  OK

Éditer: Processeurs

Supports de processeur:  Type:

Cœurs:  Total de cœurs: 4

Aide Avancé  OK

Ne pas oublier de sélectionner votre vlan.

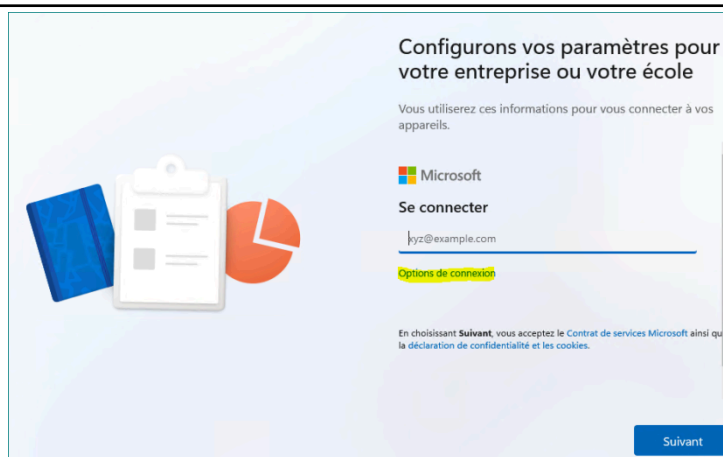
Avant le démarrage de votre machine :

- Vérifier qu'elle est bien connectée à votre vlan personnel.
- Vérifier que votre serveur DHCP (qui distribue une configuration permettant l'accès à Internet) est bien démarré, et seulement celui-là.

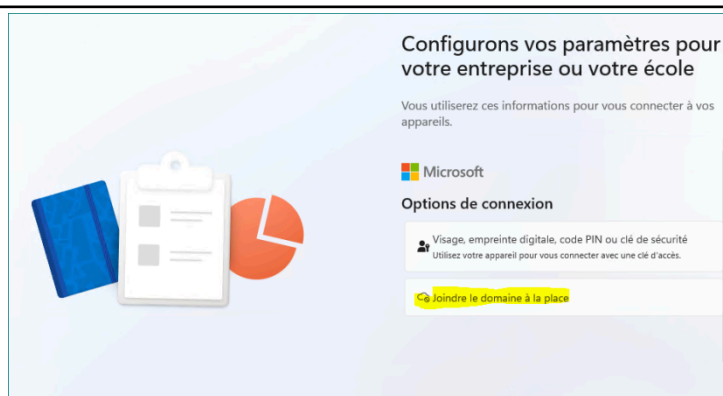
Au démarrage, lors de l'assistant de configuration de la machine :

- Patienter pendant l'activation
- Accepter la licence

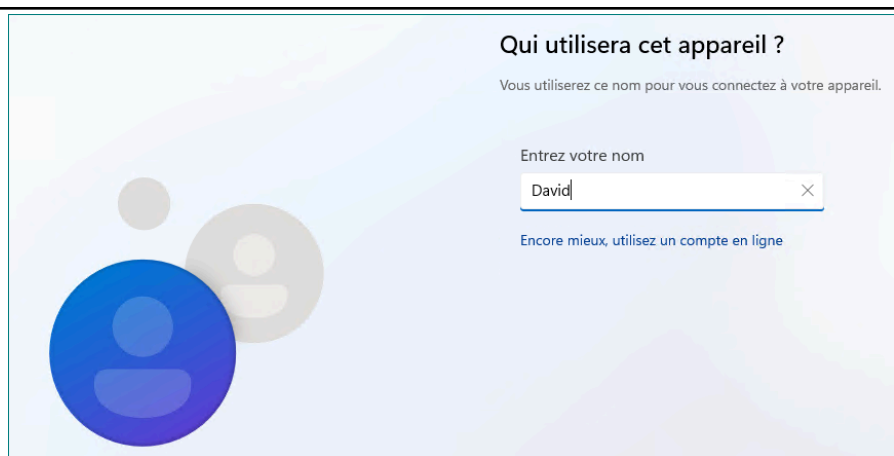
Au moment de l'écran « Se connecter », choisir « Options de connexion » :



Puis puis « Joindre un domaine à la place » pour ne pas avoir besoin d'un compte Microsoft



Indiquer votre prénom comme nouvel administrateur local pour la machine quant la question « Qui utilisera cet appareil » vous est posée :



Indiquer votre mot de passe habituel et confirmer.

Poursuivre l'assistant, en mettant par exemple « lmd » comme réponse aux 3 questions de sécurité

Terminer en mettant les autorisations minimales : Non, Non, Obligatoire uniquement, Non, Non

Patienter pendant la fin de l'installation

Ensuite procéder aux modifications suivantes :

Modifier le nom de votre machine : PRTG-LOGIN(votre login)

**Renommer votre PC**

Vous pouvez utiliser une combinaison de lettres, de traits d'union et de chiffres.

Nom actuel du PC : DESKTOP-V3LL1O9

Suivant Annuler

Attribuer une adresse fixe à votre machine : **172.30.255.50**

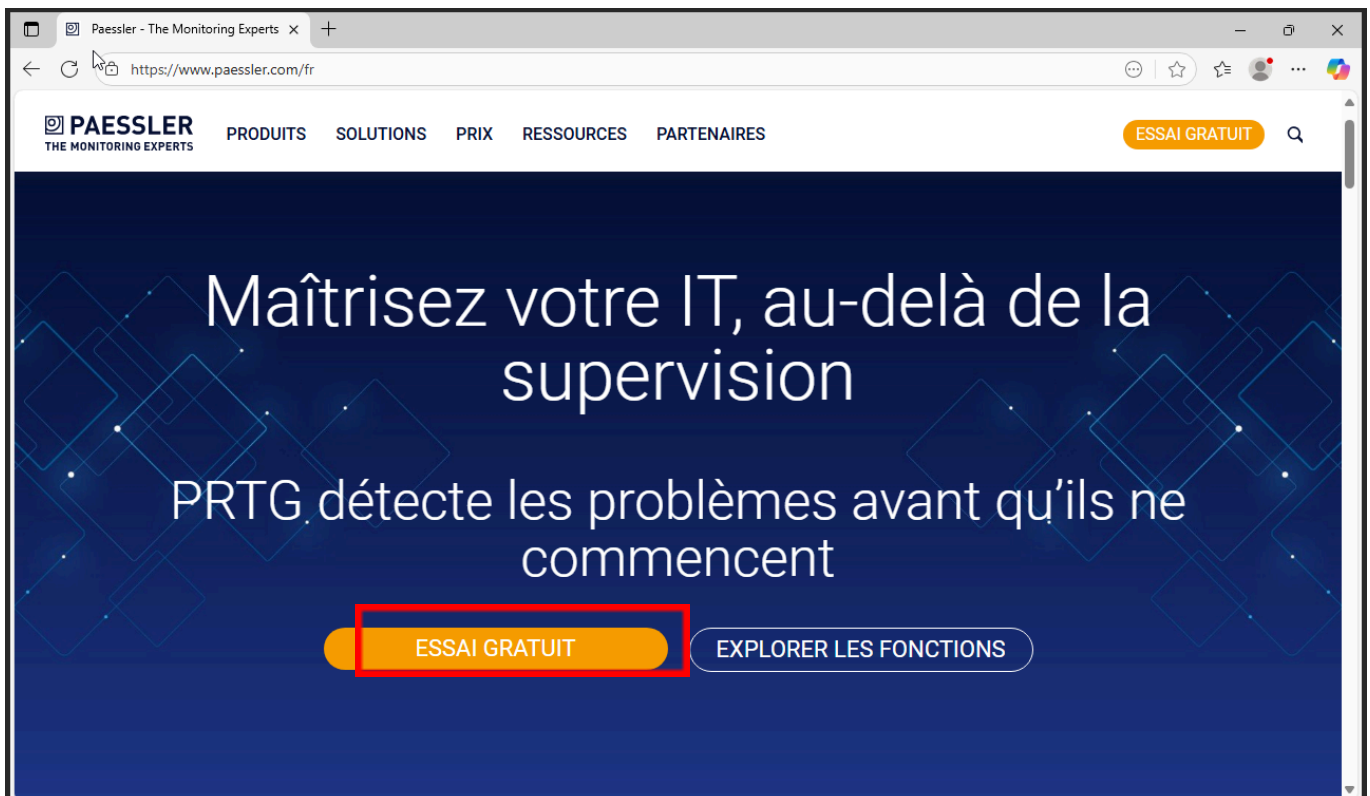
Redémarrer la machine

## Installation de PRTG

Accéder au site de PAESSLER pour télécharger la version d'évaluation de PRTG

<https://www.paessler.com/fr>

Lorsque le site vous demande une adresse mail, utilisez votre adresse **lmdsio.fr**.



## Téléchargez l'installateur PRTG :

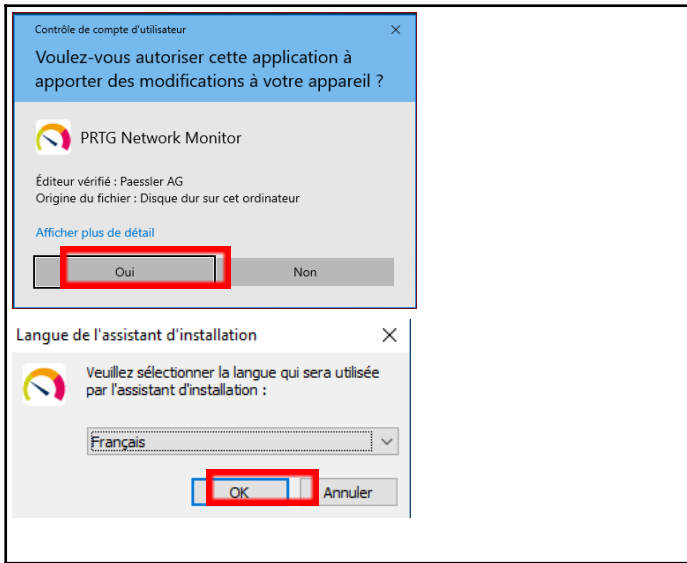
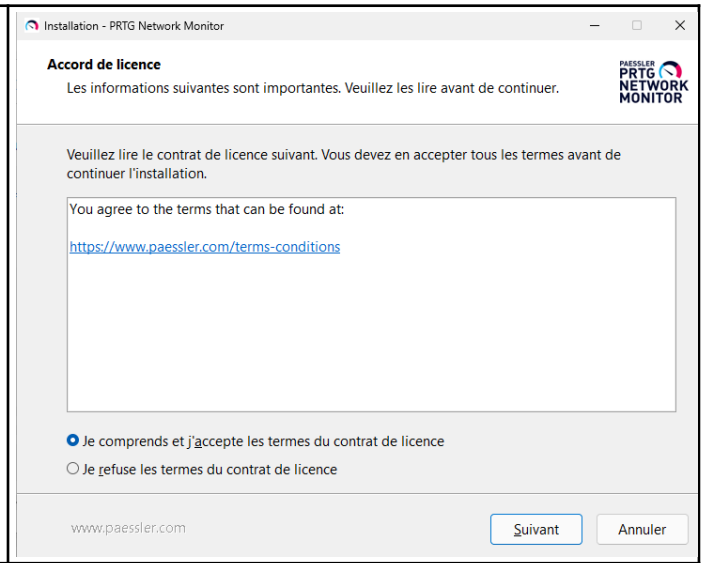
- Si vous utilisez Edge, il faudra «**Conserver** » le téléchargement
- Si vous utilisez Chrome, un avertissement s'affichera lors de l'exécution (voir ci-dessous)

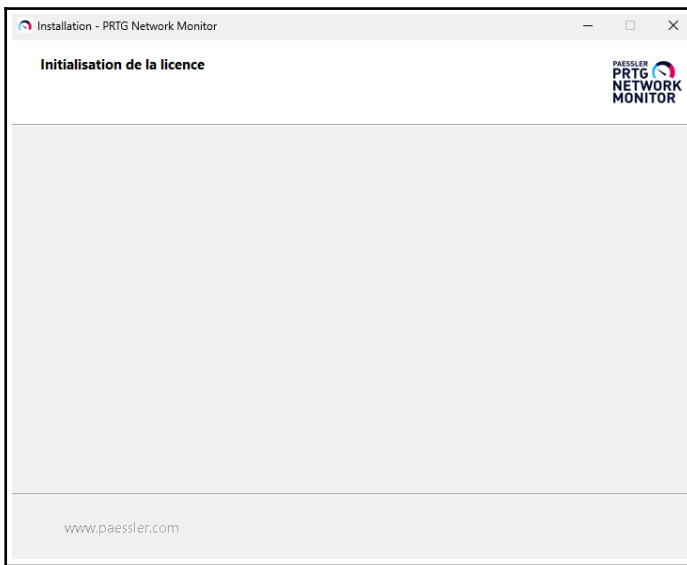
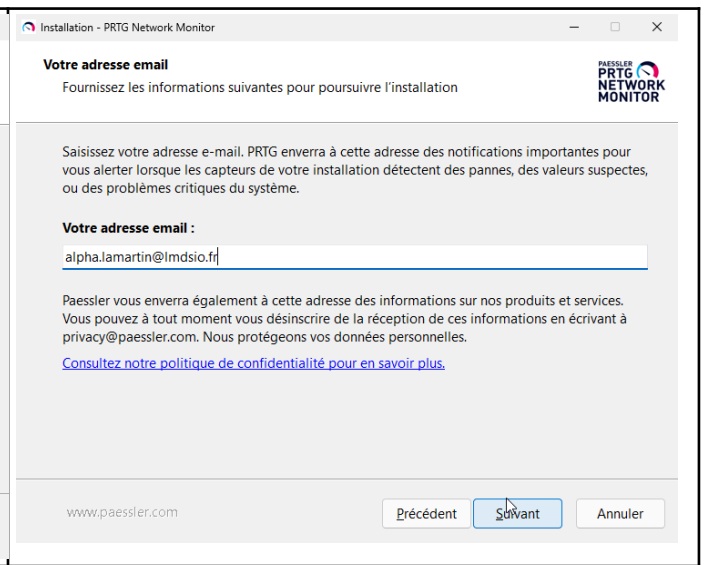
The screenshot shows a web browser window displaying the PRTG download page. The page has a navigation menu with 'PRODUITS', 'SOLUTIONS', 'PRIX', 'RESSOURCES', and 'PARTENAIRES'. The main content is divided into two numbered steps: '1. Le téléchargement a commencé automatiquement. Attendez que le téléchargement soit terminé.' and '2. Lancez l'installation. La clé de licence ci-dessous est déjà incluse dans votre fichier .exe.' Below step 2, the license key is displayed: 'Nom de licence: prtgtrial' and 'Votre clé de licence: 000023-FAKYXJ-MHUOWU-5D5Z65-X5W6PP-24ZUKQ-SEIIZT-EMI7Z4-6IK4ZY-OXEHLV'. A download warning box in the top right corner of the browser reads: 'prtgt\_installer\_with\_trial\_key\_000023-FAKYXJ-MHUOWU-5D5Z65-X5W6PP-24ZUKQ-SEIIZT-EMI7Z4-6IK4ZY-OXEHLV.exe n'est pas fréquemment téléchargé. Assurez-vous que vous faites confiance à prtgt\_installer\_with\_trial\_key\_000023-FAKYXJ-MHUOWU-5D5Z65-X5W6PP-24ZUKQ-SEIIZT-EMI7Z4-6IK4ZY-OXEHLV.exe avant de l'ouvrir.' A callout box at the bottom right states: 'Le n° de licence s'affiche, mais il est aussi inclus dans le nom du fichier téléchargé.'

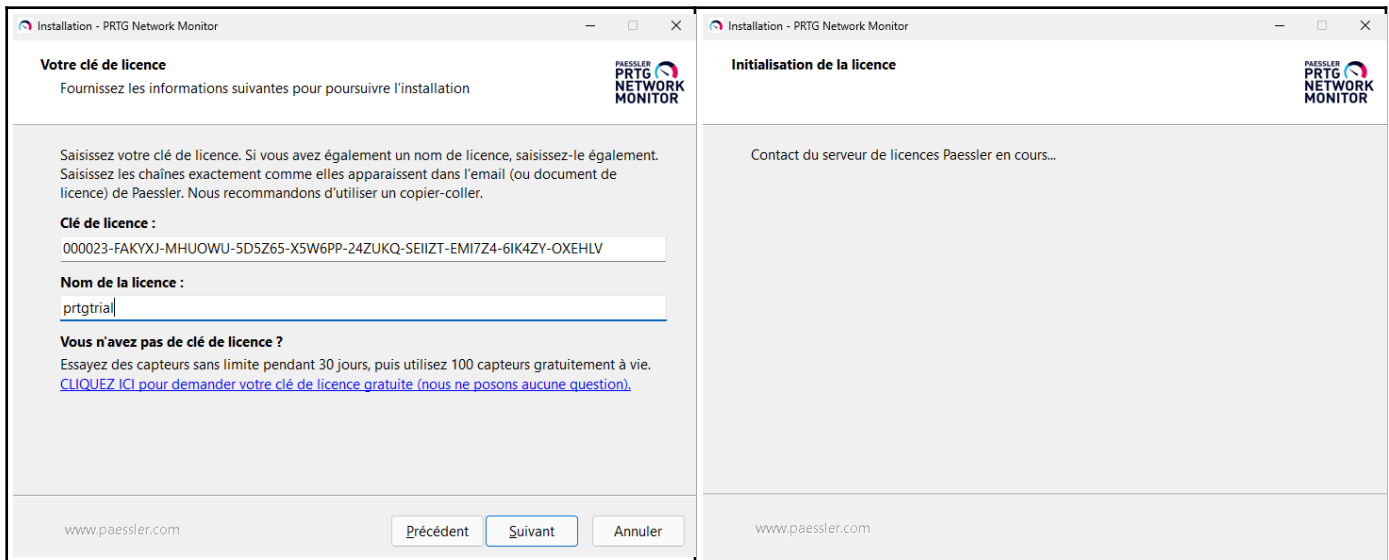
Lancer l'exécutable d'installation, une fois celui-ci téléchargé.

Si un avertissement est affiché :

The image shows two side-by-side Windows SmartScreen warning dialog boxes. The left dialog box has the title 'Windows a protégé votre ordinateur' and the text: 'Microsoft Defender SmartScreen a empêché le démarrage d'une application non reconnue. L'exécution de cette application peut mettre votre ordinateur en danger.' Below the text is a link 'Informations complémentaires' and a button 'Ne pas exécuter'. The right dialog box has the same title and text, but includes additional details: 'Application : prtgt\_installer\_with\_trial\_key\_000023-Z7MBB', 'Application : I-SQZGYE-BEJZK7-B7SUNV-I4ZTSM-CEGEY T-KNYIPR-RYCUDG-FDUJK3.exe', and 'Éditeur : DE, Bavaria, Nürnberg, Paessler GmbH, Paessler GmbH'. It has buttons for 'Exécuter quand même' and 'Ne pas exécuter'. Below each dialog box is a caption: 'Cliquer sur « Informations complémentaires »' and 'Cliquer sur « Exécuter quand même »'.

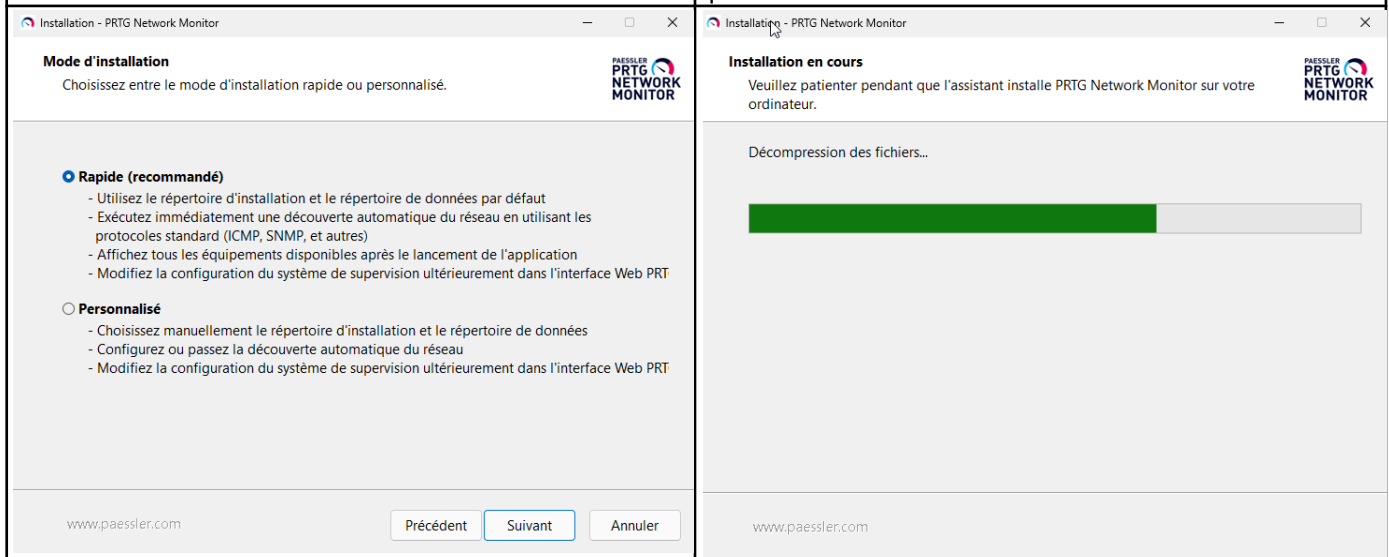
	
<p>Autoriser l'installation de l'application et confirmer la langue</p>	<p>Accepter la licence (si vous le souhaitez, sinon abandonner le TP ;-)</p>

	
<p>Initialisation de la licence (par rapport à la période d'évaluation de 30 jours sans limite de capteur)</p>	<p>Il faut saisir une adresse mail pour les notifications. Si vous mettez votre adresse @lmdsio.fr, vous recevrez réellement les notifications. Pour que le projet aboutisse, il faudra constater la réception des alertes.</p>



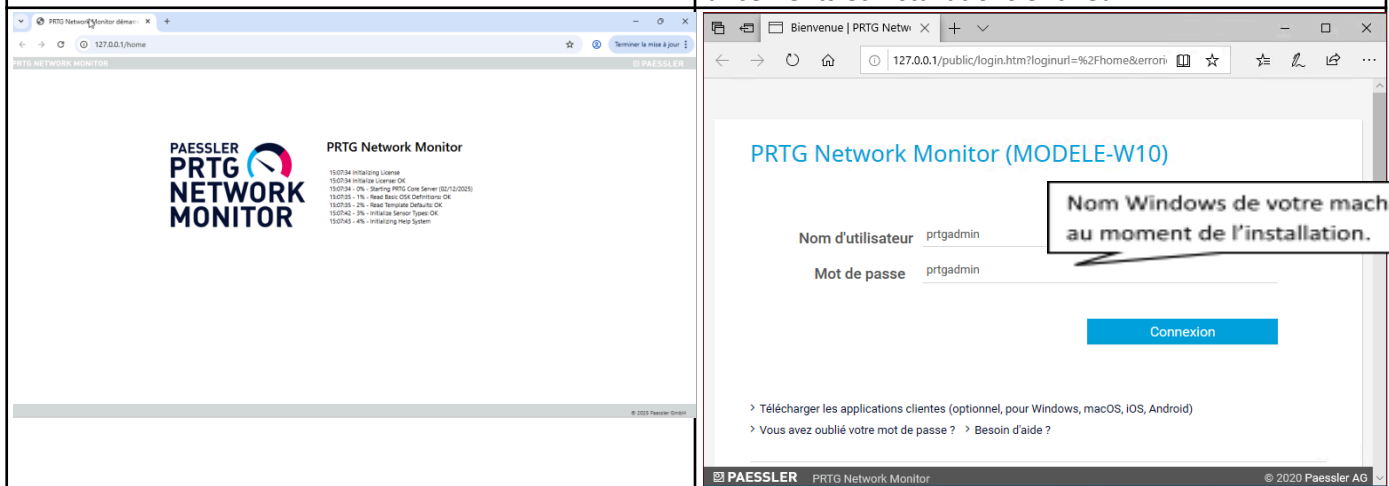
Cette étape ne se présentera pas forcément. Si c'est le cas, la clé et le nom de la licence sont censés être pré-remplis.

Initialisation de la licence. Si le temps s'écoule indéfiniment (au moins plus de 5 minutes), arrêter la tâche, redémarrer la machine et retenter l'exécution de l'installateur en tant qu'administrateur.




Choisir le mode d'installation

Décompression des services. Puis, de multiples lancements et installations ont lieu.



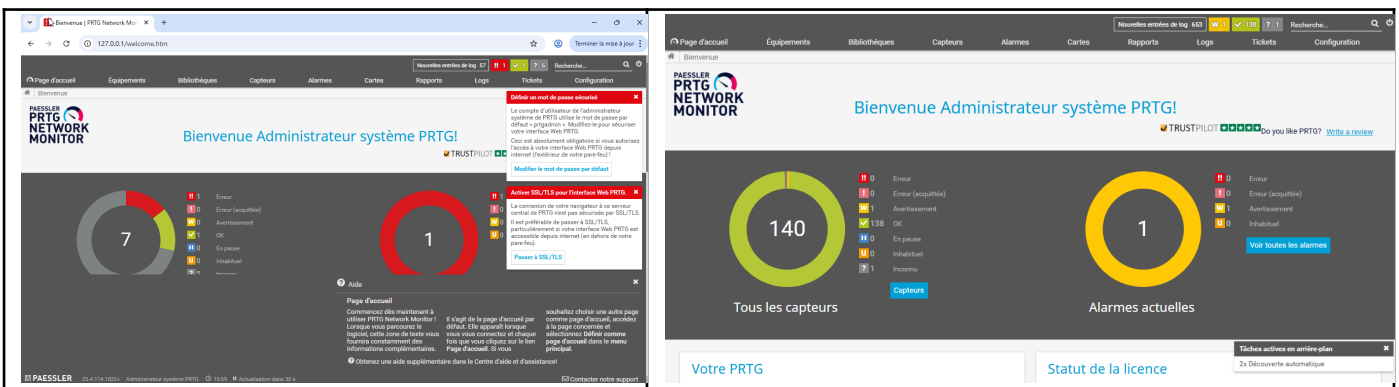
Nom Windows de votre machine au moment de l'installation.

La fin de l'installation s'affiche dans une interface WEB... qui va vous permettre d'administrer les différents capteurs en vous connectant, la 1<sup>ère</sup> fois avec les identifiants de connexion par défaut.



Noter l'icône qui se place sur votre bureau pour lancer l'interface d'administration les fois suivantes.  
NB : Il est conseillé d'utiliser Chrome ou Firefox, car certains menus contextuels et boutons ne fonctionnent pas très bien avec Edge.

Une découverte automatique d'équipements sur le réseau, et de capteurs sur ces équipements, s'est lancée. En fonction du temps que vous attendez, ce nombre d'équipements peut monter à plusieurs dizaines si vous êtes sur un véritable réseau en exploitation :



Ci-dessus le logiciel a découvert 141 capteurs.

Du coup aucun capteur n'est disponible, puisque la licence gratuite autorise 100 capteurs maximum.

NB : La licence gratuite donne droit à un essai de 30 jours en version illimitée. Mais PRTG associe apparemment la licence à une adresse IP publique. Mes premiers tests datant de plus de 30 jours, toute réinstallation qui détecte la même IP publique prend en compte la 1<sup>ère</sup> date d'installation.

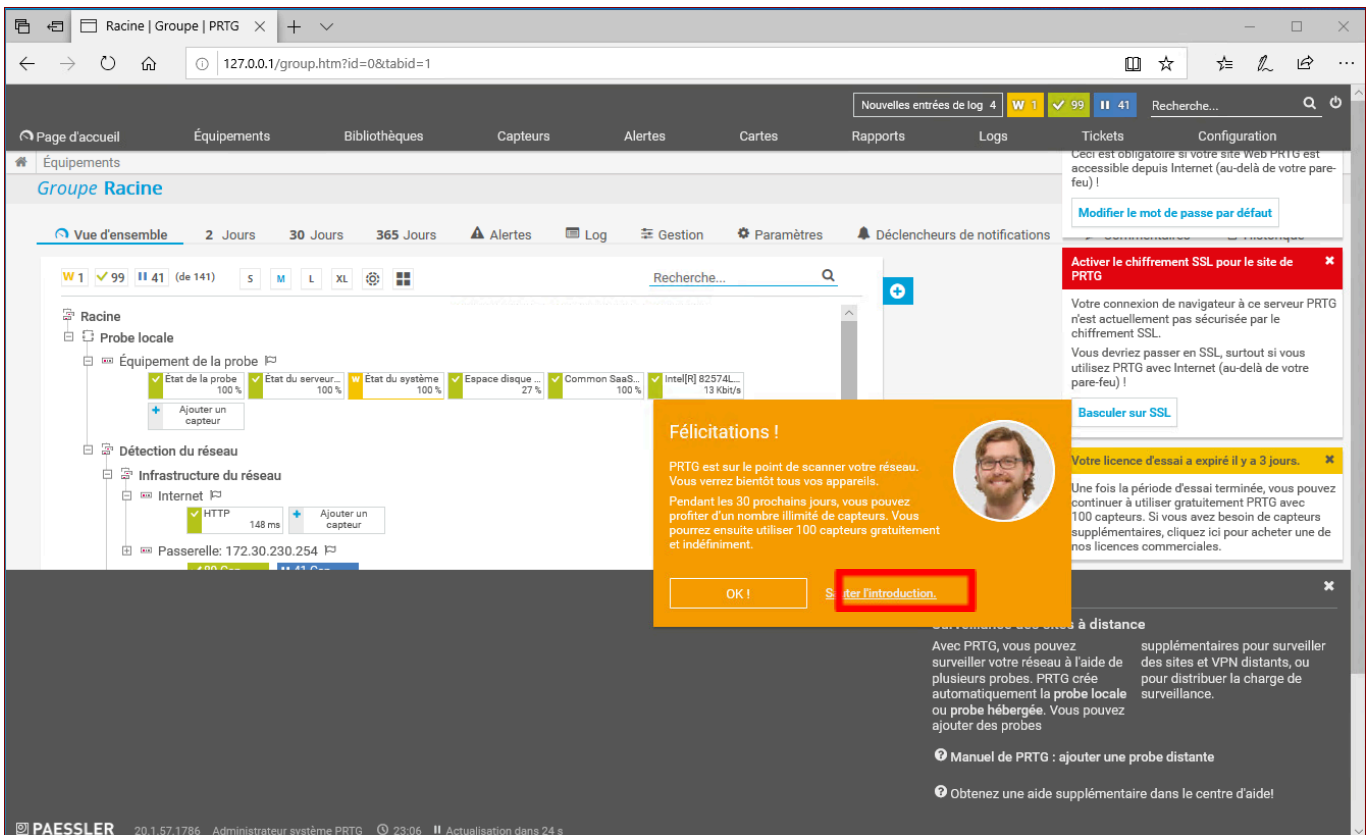
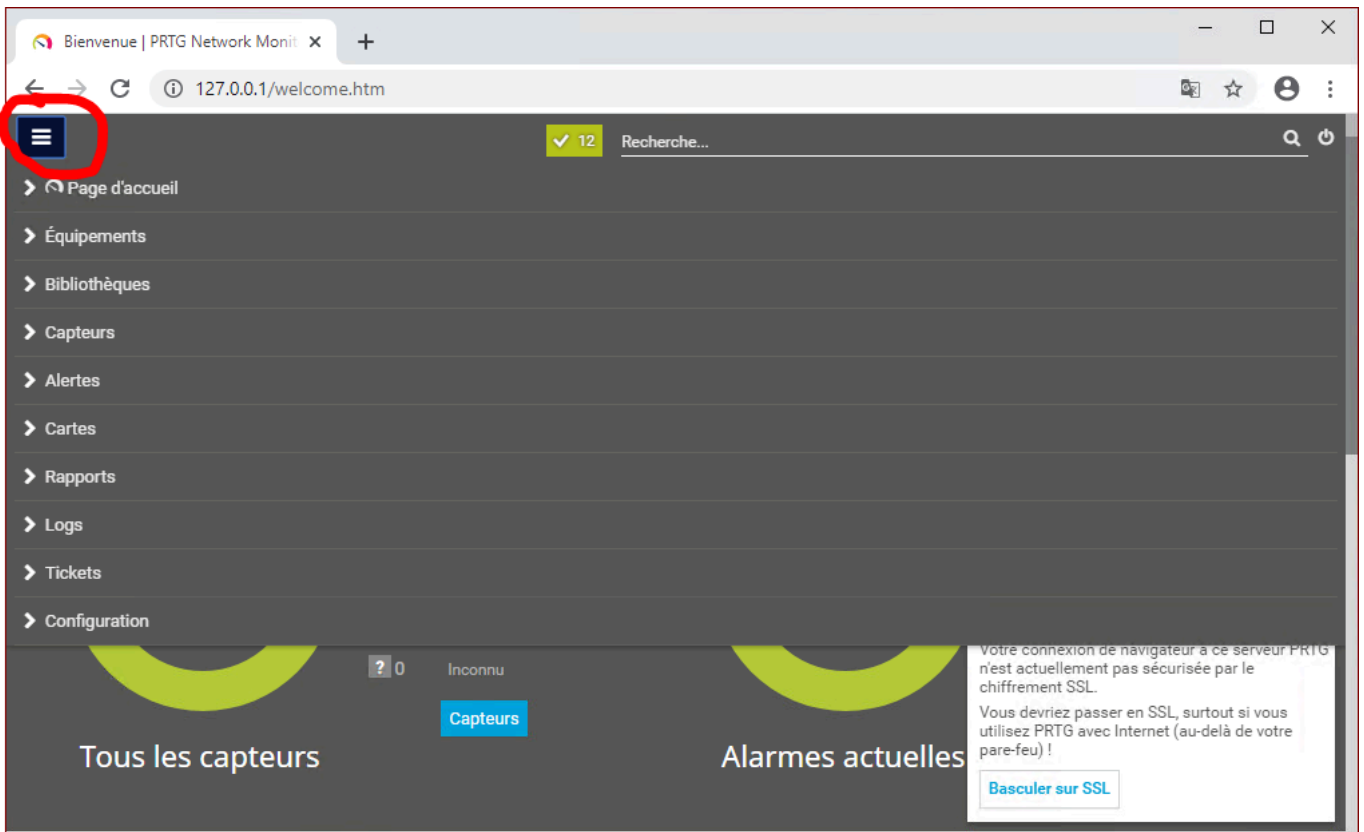
Nous allons voir, dans le cas précis (vlan d'un étudiant) que la découverte automatique a notamment inspecté le commutateur de niveau 3 qui relie les vlan étudiants entre eux et trouvé de nombreux capteurs, en fait 2 par port Ethernet.

Ils ne sont pas utiles pour le TP, vous allez donc commencer par supprimer cet équipement de votre inventaire.

NB : De très bonnes vidéos sont disponibles sur le site de PAESSLER. Ce tutoriel a pour objectif de réaliser rapidement quelques capteurs sur vos équipements, puis de passer en revue quelques options intéressantes. Il n'a pas d'objectif d'exhaustivité.

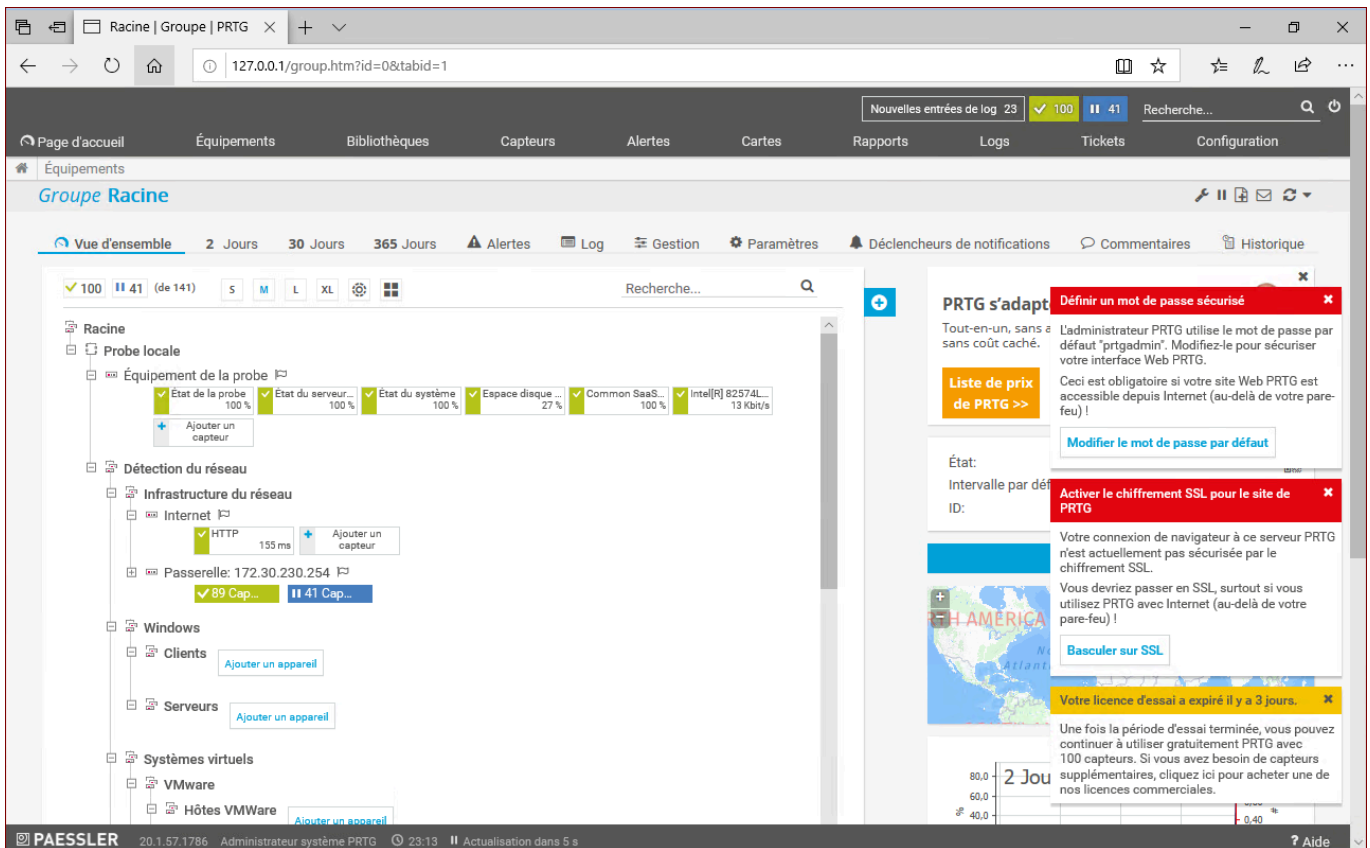
Cliquer sur **Equipements**. Sauter l'introduction pour procéder aux manipulations suivantes.

NB : Si le menu ne s'affiche pas, c'est parce que la fenêtre du navigateur est trop petite ; dans ce cas le menu s'affiche en cliquant sur le petit carré en haut à gauche :



Par défaut PRTG catégorise les équipements dans une arborescence. On distingue très clairement la « Probe locale », c'est-à-dire un système de sondes locales qui interroge des équipements.

Il est possible d'installer plusieurs systèmes similaires répartis, à distance, chargés par exemple d'interroger les équipements de différents sites pour répartir la charge.



La probe locale comprend ensuite deux branches :

- L'équipement de la probe, autrement dit l'équipement sur lequel est installé le système de sondes.
  - On peut remarquer que quelques capteurs ont automatiquement été découverts sur cette machine, notamment :
    - Le pourcentage d'espace disque disponible
    - La charge CPU
- La détection du réseau qui tente de découvrir :
  - L'infrastructure du réseau
  - La présence d'un capteur « Internet » qui vérifie la connectivité du réseau avec Internet
  - La présence de l'équipement « Passerelle » qui totalise plus d'une centaine de capteurs, dont 41 sont suspendus parce qu'on dépasse la limitation de 100 capteurs
  - Les équipements situés sur le même réseau logique, classés de la manière suivante :
    - Machines Physiques Windows
    - Clients
    - Serveurs
    - Systèmes virtuels
    - VMWare

- HyperV
- Machines apparentées Linux / macOS / Unix
- Imprimantes

Si on regarde la liste des capteurs à l'état « disponible », on constate la présence de 2 capteurs par port du commutateur.

capteur	Probe, Groupe, Équipement	État	Dernière valeur	Message	Graphique	Priorité	Fav.	Perf. Impact
✓ Ping	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254	Disponible	0 ms	OK	Temps du ping 0 ms	★★★★★	🔖	🟢
✓ (001) ESXi1 - vmnic0 RMON	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254	Disponible	82 Kbit/s	OK	Transmis 82 Kbit/s	★★★★☆	🔖	🟢
✓ (001) ESXi1 - vmnic0 Traffic	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254	Disponible	77 Kbit/s	OK	Somme 87 Kbit/s	★★★★☆	🔖	🟢
✓ (002) ESXi3 - vmnic0 RMON	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254	Disponible	4,54 Kbit/s	OK	Transmis 4,54 Kbit/s	★★★★☆	🔖	🟢
✓ (002) ESXi3 - vmnic0 Traffic	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254	Disponible	4,70 Kbit/s	OK	Somme 4,81 Kbit/s	★★★★☆	🔖	🟢
✓ (003) ESXi2 - ILO RMON	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254	Disponible	0,11 Kbit/s	OK	Transmis 0,11 Kbit/s	★★★★☆	🔖	🟢
✓ (003) ESXi2 - ILO Traffic	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254	Disponible	0,15 Kbit/s	OK	Somme 0,30 Kbit/s	★★★★☆	🔖	🟢
✓ (004) ESXi4 - ILO RMON	Probe locale (Probe locale) »	Disponible	0,11 Kbit/s	OK	Transmis 0,11 Kbit/s	★★★★☆	🔖	🟢

On remarque l’affichage d’informations qui ont été paramétrées sur le commutateur, qui font qu’on obtient même des informations relativement claires sur l’usage des ports. Peut-être même trop d’informations pour suivant qu’on n’a normalement aucun droit sur cet équipement. En revanche elles sont très utiles pour l’administrateur du réseau.

Ces informations seraient intéressantes, mais vous n’avez pas la charge d’administration de ce commutateur, et vous ne pouvez pas intervenir sur celui-ci pour effectuer des tests.

### Suppression du commutateur pour libérer des capteurs

Nous allons donc, comme évoqué plus haut, supprimer cet équipement pour nous permettre d’installer / configurer d’autres capteurs.

**Groupe Racine**

Vue d'ensemble 2 Jours 30 Jours 365 Jours Alertes Log Gestion Paramètres

100 41 (de 141) S M L XL

Recherche...

Racine

- Probe locale
  - État de la probe 100 %
  - État du r...
  - Détection du réseau
    - Infrastructure du réseau
      - Internet
        - HTTP 121 ms
        - Passerelle: 172.30.230.2
        - 89 Cap...
      - Windows
      - Clients
        - Ajouter un appareil
      - Serveurs
        - Ajouter un appa
      - Systèmes virtuels
        - VMware
          - Hôtes VMWare
            - Ajov

Menu d'équipements

- Démarrer une analyse
- Détails...
- Modifier
- Ajouter un capteur...
- Découverte automatique
- Créer un modèle d'équipement...
- Recommander maintenant
- Trier par ordre alphabétique
- Supprimer...
- Cloner...
- Déplacer
- Suspendre
- Priorité/Favori
- Données historiques
- Outils d'équipement
- Rechercher les duplicatas...
- Envoyer le lien par e-mail
- Ajouter un ticket

Common SaaS... 100 % Intel[R] 82574L... 15 Kbit/s

Ajouter un capteur

Clic droit sur l'équipement Passerelle / Supprimer

Supprimer l'objet Passerelle: 172.30.230.254

Supprimer un objet

Vous avez décidé de supprimer un objet de la base de données. Sur cette page, PRTG affichera systématiquement tous les autres objets de la base de données qui sont éventuellement connectés à l'objet que vous voulez supprimer. Vous devez toujours contrôler attentivement cette liste pour éviter de supprimer par erreur des objets que vous voulez conserver.

Remarque : la suppression des comptes d'utilisateurs affecte les entrées dans les tables du journal et dans les onglets Historique des objets. Les utilisateurs supprimés s'affichent en tant qu'utilisateurs ou objets *inconnus*, pour que les modifications apportées à la configuration de la surveillance ne puissent plus leur être associées.

Important : certains objets connectés comme les cartes, bibliothèques et rapports peuvent ne pas apparaître dans cette liste en fonction de leurs paramètres de Contexte de sécurité.

130 Capteurs utilisent cet objet

Éléments: 50

Objet ▾ Probe, Groupe, Équipement

<input checked="" type="checkbox"/> (001) ESX1 - V...	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254
<input checked="" type="checkbox"/> (001) ESX1 - V...	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254
<input checked="" type="checkbox"/> (002) ESX13 - V...	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254
<input checked="" type="checkbox"/> (002) ESX13 - V...	Probe locale (Probe locale) » Infrastructure du réseau » Passerelle: 172.30.230.254

Annuler Supprimer un objet

Confirmer ensuite la suppression de l'objet et donc des x capteurs.

Une fois l'équipement « Passerelle » supprimé, on obtient un tableau de bord avec seulement 11 capteurs, tous à l'état disponible :

The screenshot shows the PRTG Network Monitor dashboard. At the top, there's a navigation bar with tabs for 'Page d'accueil', 'Équipements', 'Bibliothèques', 'Capteurs', 'Alertes', 'Cartes', 'Rapports', 'Logs', 'Tickets', and 'Configuration'. The main content area features a large green circle with the number '11' and the text 'Tous les capteurs' (All sensors). To its right is another large green circle with the number '0' and the text 'Alarmes actuelles' (Current alarms). Below these are three smaller sections: 'Votre PRTG' with links for 'Voir les résultats', 'Installer l'appi mobile', and 'Installer l'appi desktop'; 'État de la licence' with a green circle showing '89 Capteurs disponibles'; and 'Activités d'hier' showing '0 Analyses de capteurs effectuées' and '0 Modifications de l'état' and '0 Notifications envoyées'. A red banner on the right side prompts the user to 'Définir un mot de passe sécurisé' (Set a secure password).

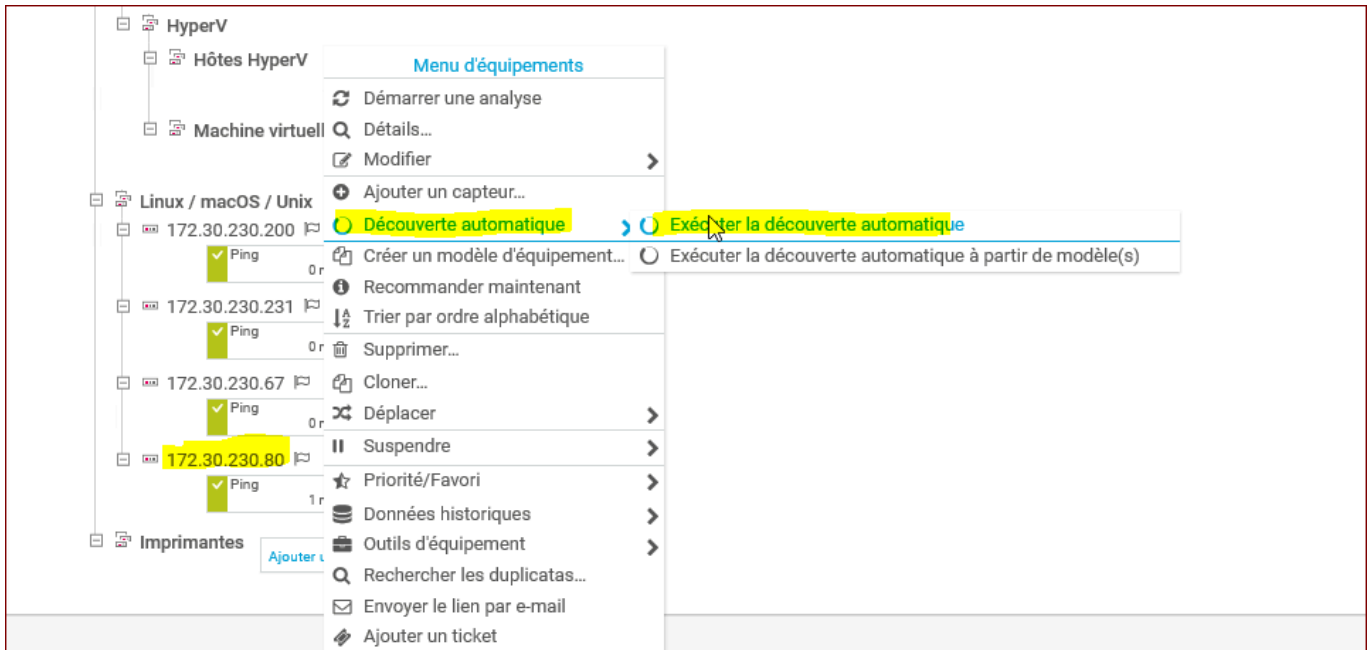
NB : Vous pouvez obtenir, en fonction des machines présentes et en ligne sur votre réseau, un nombre de capteurs différents, surtout si vous disposez de la licence 30 jours sans limite de capteurs.

Si on revient à la vue « Equipements » (clic sur le menu correspondant), dans le cas présent, le système de découverte automatique avait par exemple identifié 4 machines linux :

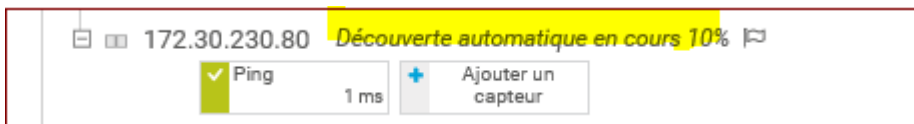
The screenshot shows the 'Equipements' (Devices) view in PRTG. It displays a tree structure under the heading 'Linux / macOS / Unix'. Four devices are listed with their IP addresses: 172.30.230.200, 172.30.230.231, 172.30.230.67, and 172.30.230.80. Each device has a green checkmark and the text 'Ping' followed by a response time (0 ms for the first three, 1 ms for the last). To the right of each device is a button labeled 'Ajouter un capteur' (Add sensor).

Ajout de capteurs grâce à la découverte automatique

Il est possible, maintenant que nous disposons de capteurs supplémentaires, de lancer une découverte sur un équipement :



La découverte automatique progresse :



Un service HTTP (par exemple) est rapidement découvert ...



... puis signalé opérationnel :



La machine concernée ci-dessus héberge d'autres services, mais qui ne peuvent pas être découverts, soit pour des problèmes d'authentification (« credentials »), soit pour d'autres raisons que nous verrons ultérieurement, comme l'absence de fonctionnalités permettant l'interrogation.

Pour les besoins du TP, nous allons :

Créer un groupe d'équipements spécifique au TP : Equipements-TP

Ajouter les machines (virtuelles dans notre cas) qui nous intéressent dans ce groupe

Installer pour chaque équipement à surveiller quelques capteurs intéressants

Vérifier que les alertes fonctionnent

Modifier les valeurs par défaut des capteurs pour répondre à un cahier des charges personnalisé

Installer des capteurs un peu plus poussés comme la vérification d'une base de données

Création d'un groupe d'équipements

Le fonctionnement de PRTG permet un système d'héritage au niveau de l'arborescence des équipements. L'un des intérêts d'un groupe d'équipements repose précisément sur ce système d'héritage : on pourra définir des propriétés par défaut, par exemple des « credentials » d'authentification, des intervalles d'analyse, etc...

Nous allons donc créer un groupe « Equipements-TP » avec 3 sous-groupes :

Mes-Machines-Linux

Mes-Machines-AD

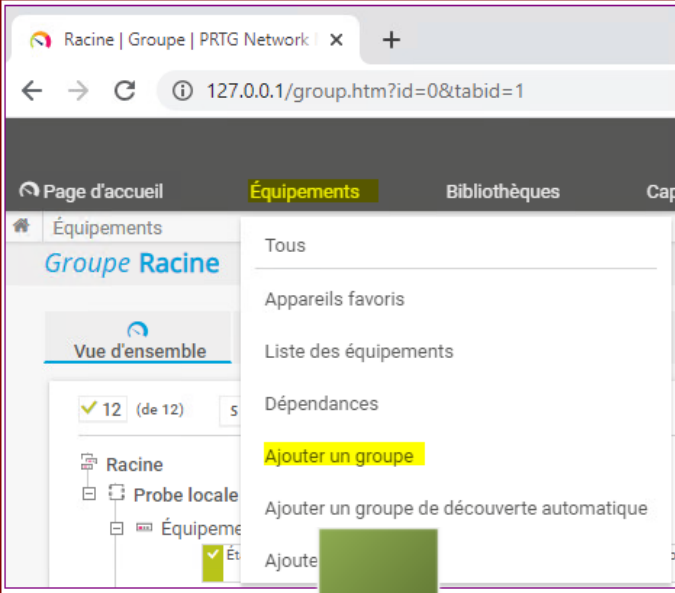
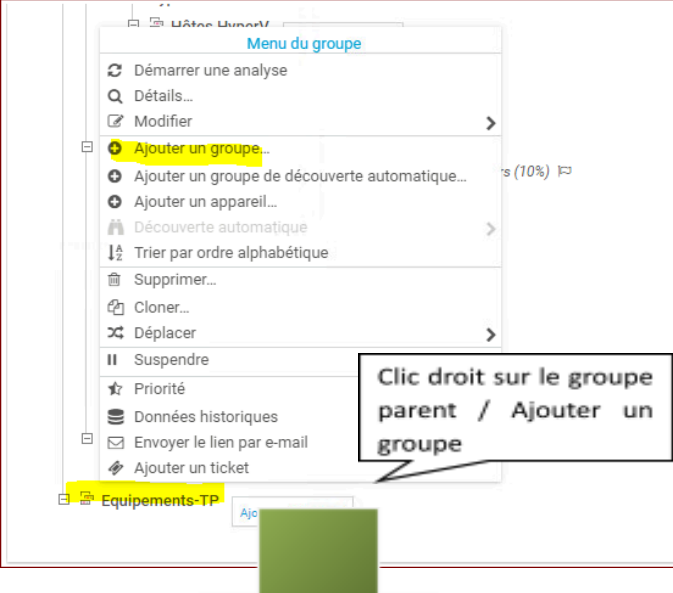


Mes-Machines-Windows-Autonomes

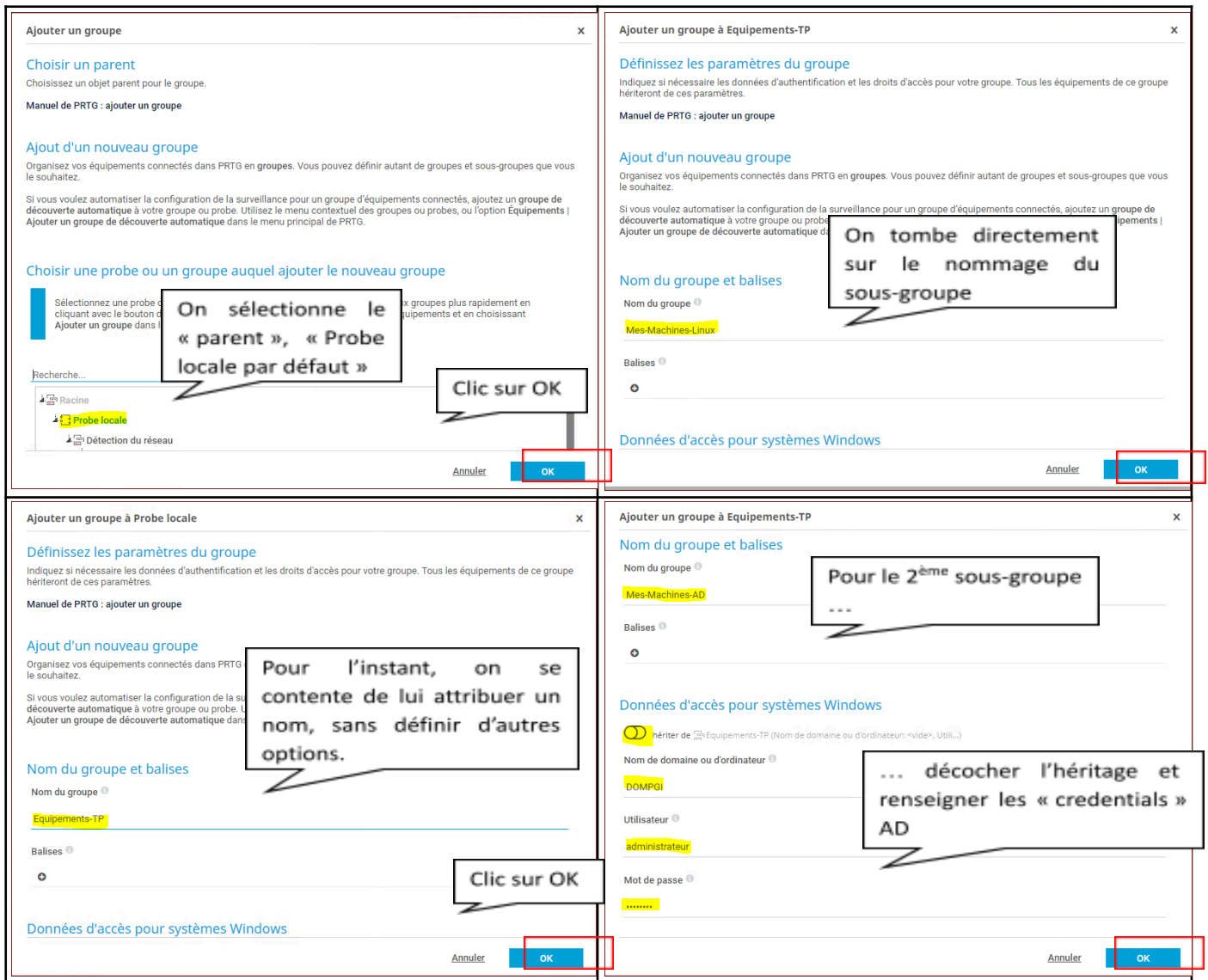
Pour créer un groupe :

Menu Equipements / Ajouter un groupe

Ou bien

Clic droit sur un groupe / Ajouter un groupe (pour ajouter un sous-groupe)

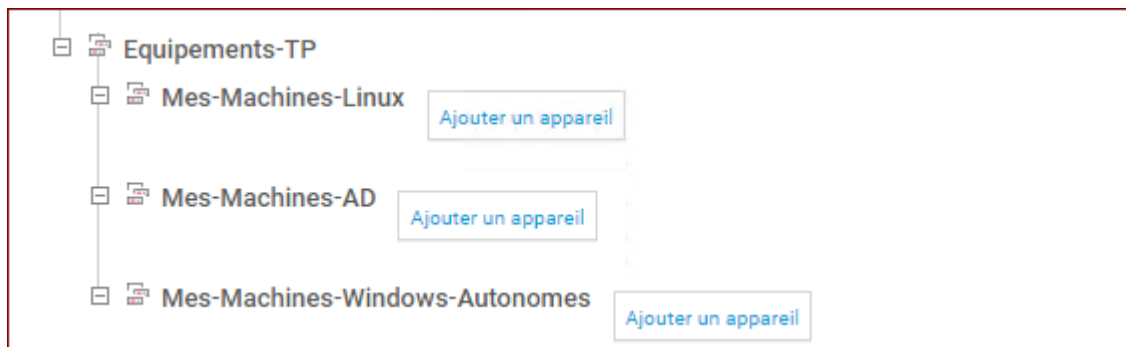
Pour créer le groupe	Pour créer les sous-groupes
 <p>The screenshot shows the PRTG Network Manager interface. The 'Équipements' menu is active, and the 'Ajouter un groupe' button is highlighted in yellow. A green arrow points from this button to the bottom of the column.</p>	 <p>The screenshot shows the context menu for a group. The 'Ajouter un groupe' option is highlighted in yellow. A callout box with the text 'Clic droit sur le groupe parent / Ajouter un groupe' points to this option. A green arrow points from the menu to the bottom of the column.</p>
	



## Créer le groupe et les 3 sous-groupes

Pour le sous-groupe « Mes-Machines-AD », indiquer les crédeniels Windows AD qui permettront de s'authentifier sur le domaine

NB : Dans la réalité, on n'utiliserait pas le compte Administrateur, mais plutôt un compte dédié à l'analyse des capteurs, avec les droits suffisants pour le faire (**à déterminer par vos soins ultérieurement**)



Ajout d'une machine au groupe « Mes-Machines-Linux »

Nous allons déplacer la machine LAMP qui avait été découverte automatiquement vers notre nouveau groupe « Mes-Machines-Linux » :

**Déplacer l'objet 172.30.230.80 vers un autre groupe**

172.30.230.80

Choisissez un groupe cible

Recherche...

Hôtes VMWare  
Serveurs VMWare vCenter  
HyperV  
Hôtes HyperV  
Machine virtuelle HyperV  
Linux / macOS / Unix  
Imprimantes  
Equipements-TP  
**Mes-Machines-Linux**  
Mes-Machines-AD  
Mes-Machines-Windows-Autonomes

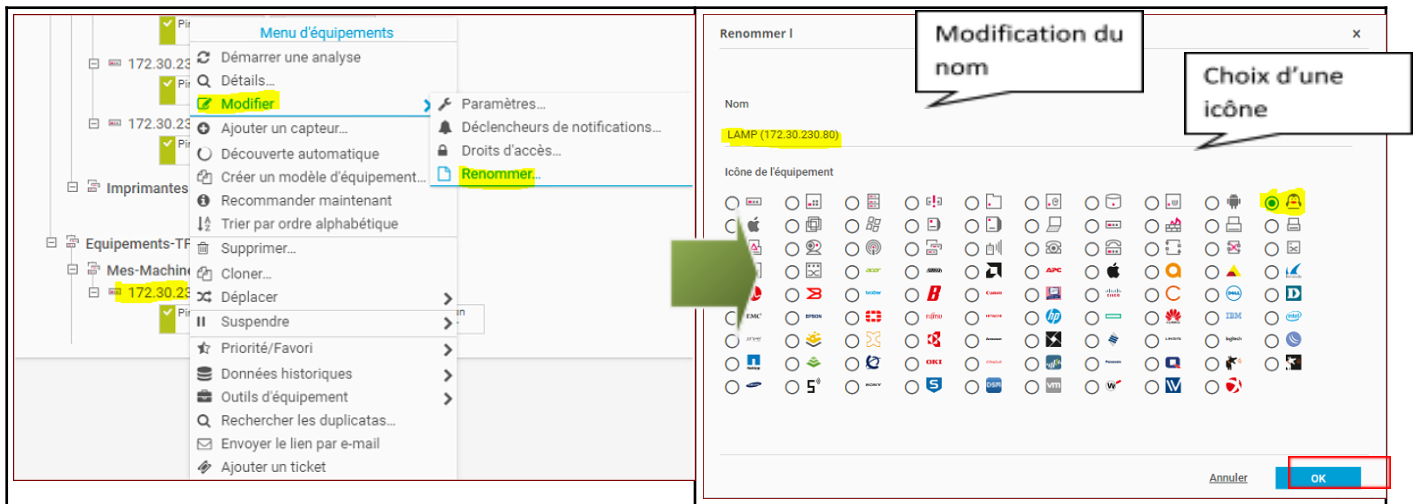
Sélectionner le groupe cible

2 les sous-objets seront également déplacés.

Groupe	Équipement	capteur	État
Linux / macOS / Unix	172.30.230.80	<input checked="" type="checkbox"/> Ping	Disponible
Linux / macOS / Unix	172.30.230.80	<input checked="" type="checkbox"/> HTTP	Disponible

Annuler OK


Nous allons en profiter pour renommer cette machine :

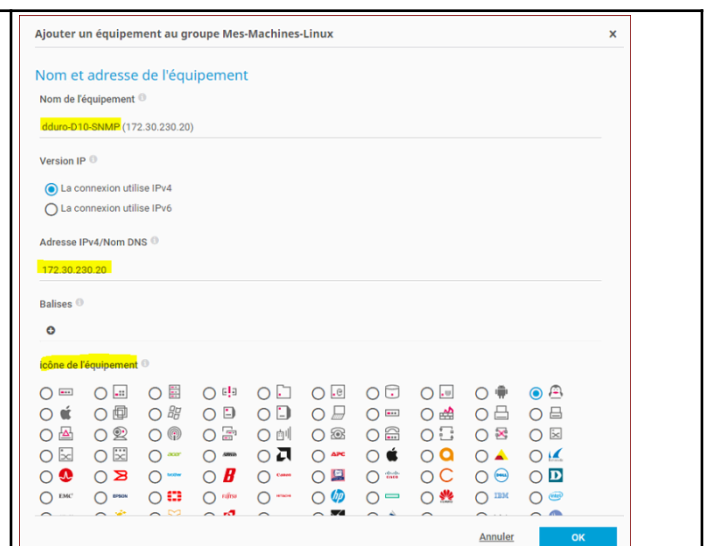
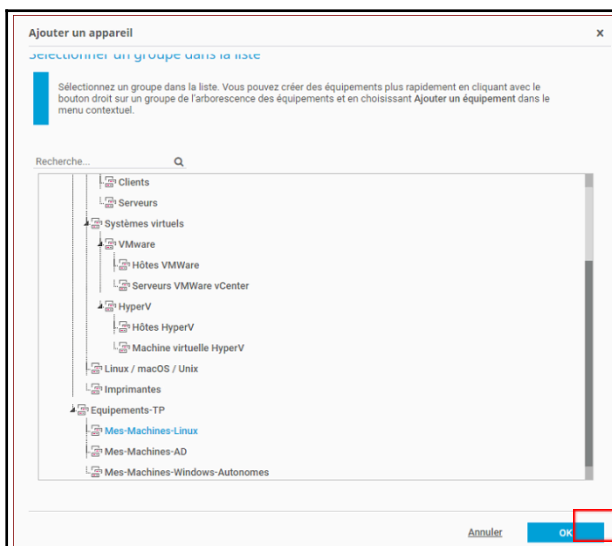
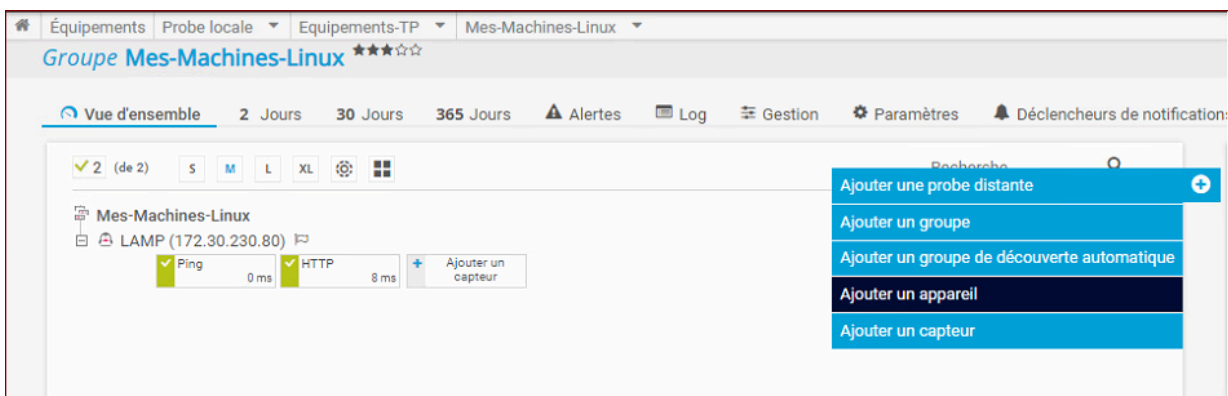


Ajout d'une nouvelle machine à un groupe

Lancer votre MV-LINUX-SNMP si ce n'est pas déjà fait.

On peut ajouter une machine par clic droit sur le groupe « Mes-Machines-Linux » / Ajouter un appareil

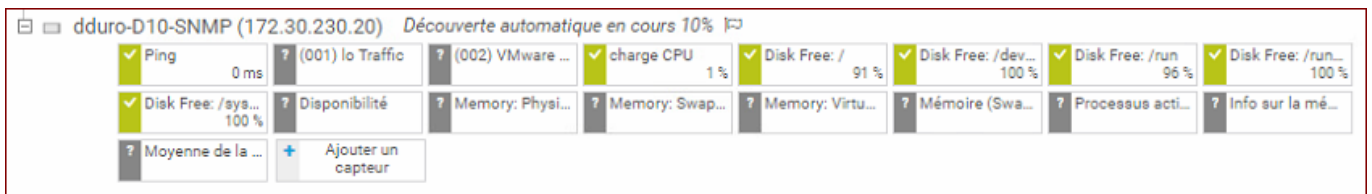
**ou bien** cliquer sur le nom du groupe (« Mes-Machines-Linux »), puis dans l'interface du groupe, cliquer sur le bouton « Ajouter un appareil » : 



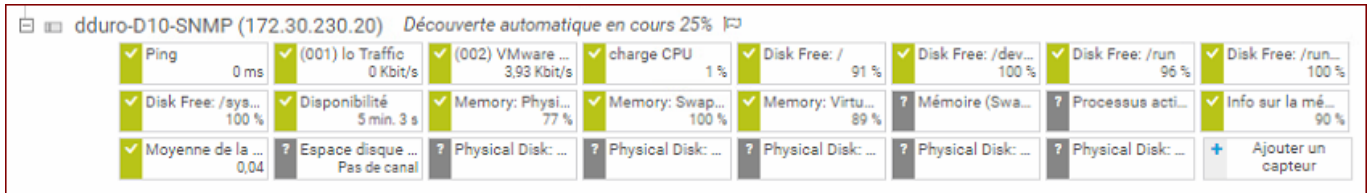
Vérifier que le groupe est bien sélectionné (en bleu)

Attribuer un nom, préciser l'IP et choisir une icône

Lancer une découverte automatique :

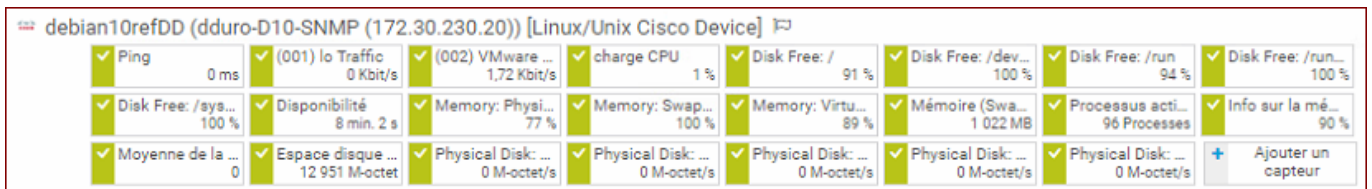


Les capteurs répondent les uns après les autres ; on constate que l'agent SNMP fournit beaucoup de capteurs supplémentaires :



Remarque : la découverte automatique n'est pas forcément la solution, car elle multiplie les capteurs, peut-être inutiles, mais il était intéressant visualiser le résultat obtenu.

A noter que nous obtenons autant de capteurs, parce que nous avons laissé la lecture possible à la communauté publique.



Au final 23 capteurs, et on constate que le nom Linux de la machine est affiché (Le nom manuel est mis entre parenthèses) : ce qui apporte la preuve que même le professeur ne renomme pas toujours ses machines !



Vérification du fonctionnement des alertes

Avant d'aller plus loin dans le paramétrage, vérifions qu'en l'état, bien :



les capteurs détectent

L'arrêt d'un service (par exemple l'arrêt du service APACHE2),

La mise hors service d'une machine.

Arrêter le service Apache sur la machine LAMP :

```

VMRC - dduro-D10-MVLamp - VMware Remote Console
root@debian10lamp:~# service apache2 stop
root@debian10lamp:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: inactive (dead) since Mon 2020-04-06 04:54:51 CEST; 8s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 4097 ExecReload=/usr/sbin/apachectl graceful (code=exited, status=0/SUCCESS)
   Process: 4305 ExecStop=/usr/sbin/apachectl stop (code=exited, status=0/SUCCESS)
   Main PID: 449 (code=exited, status=0/SUCCESS)

avril 03 00:00:29 debian10lamp systemd[1]: Reloaded The Apache HTTP Server.
avril 04 00:00:29 debian10lamp systemd[1]: Reloading The Apache HTTP Server.
avril 04 00:00:29 debian10lamp systemd[1]: Reloaded The Apache HTTP Server.
avril 05 00:00:29 debian10lamp systemd[1]: Reloading The Apache HTTP Server.
avril 05 00:00:29 debian10lamp systemd[1]: Reloaded The Apache HTTP Server.
avril 06 00:00:29 debian10lamp systemd[1]: Reloading The Apache HTTP Server.
avril 06 00:00:29 debian10lamp systemd[1]: Reloaded The Apache HTTP Server.
avril 06 04:54:51 debian10lamp systemd[1]: Stopping The Apache HTTP Server...
avril 06 04:54:51 debian10lamp systemd[1]: apache2.service: Succeeded.
avril 06 04:54:51 debian10lamp systemd[1]: Stopped The Apache HTTP Server.
root@debian10lamp:~#

```

Eteindre complètement la machine SNMP.

Les voyants passent rapidement au orange dans un premier temps :

Puis ils passent au rouge ou au bleu

### Au bleu ?

Le serveur LAMP reste joignable (Ping), mais le service HTTP est bien indisponible

La machine SNMP n'est pas joignable, les capteurs sont donc dans l'état « suspendu » :

Inutile de lancer une analyse de ces capteurs, puisque la machine est injoignable

Il s'agit d'une dépendance évidente : si la machine n'est pas joignable, les capteurs de mémoire ou autre pas plus.

L'administrateur peut également indiquer à PRTG qu'il y a une dépendance (non évidente) entre certains hôtes et un commutateur. Cette indication évitera les alertes en cascade suite à la panne d'un commutateur : une panne de commutateur suspendra les capteurs sur les machines impactées.

Mais on entre là dans des considérations intéressantes mais un peu plus poussées. Revenons à des choses plus simples.

Avant de poursuivre les investigations, vérifions que les capteurs reviennent à la normale en cas de relance du service HTTP et de la machine SNMP.

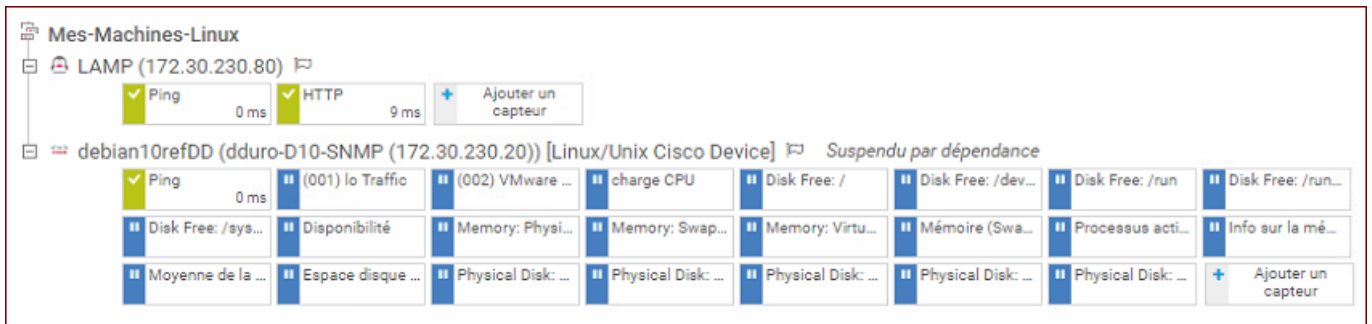
```

root@debian10lamp:~# service apache2 start
root@debian10lamp:~# service apache2 status
● apache2.service - The Apache HTTP Server
   Loaded: loaded (/lib/systemd/system/apache2.service; enabled; vendor preset: enabled)
   Active: active (running) since Mon 2020-04-06 05:11:00 CEST; 3s ago
     Docs: https://httpd.apache.org/docs/2.4/
   Process: 4358 ExecStart=/usr/sbin/apachectl start (code=exited, status=0/SUCCESS)
  Main PID: 4362 (apache2)
    Tasks: 55 (limit: 1149)
   Memory: 10.8M
   CGroup: /system.slice/apache2.service
           └─4362 /usr/sbin/apache2 -k start
             └─4363 /usr/sbin/apache2 -k start
               └─4364 /usr/sbin/apache2 -k start

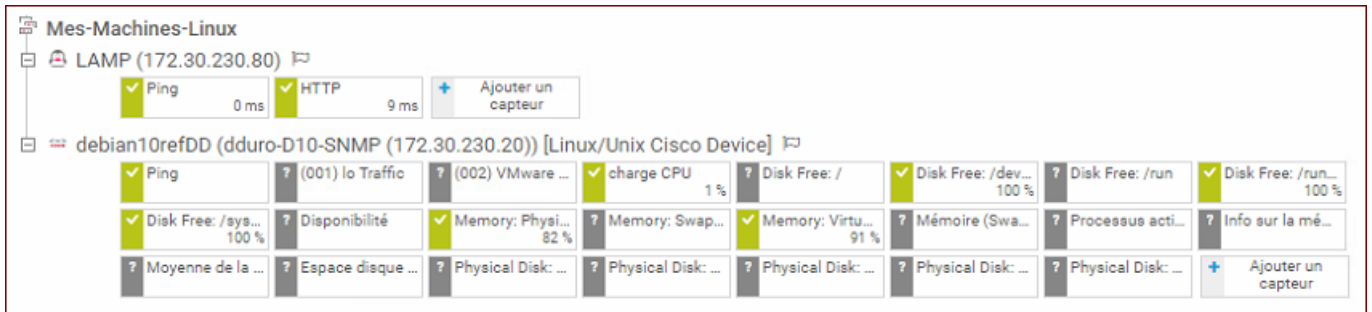
avril 06 05:11:00 debian10lamp systemd[1]: Starting The Apache HTTP Server...
avril 06 05:11:00 debian10lamp systemd[1]: Started The Apache HTTP Server.

```

Dans un premier temps, certains passent au vert (1<sup>er</sup> niveau)



Puis progressivement les analyses aboutissent :



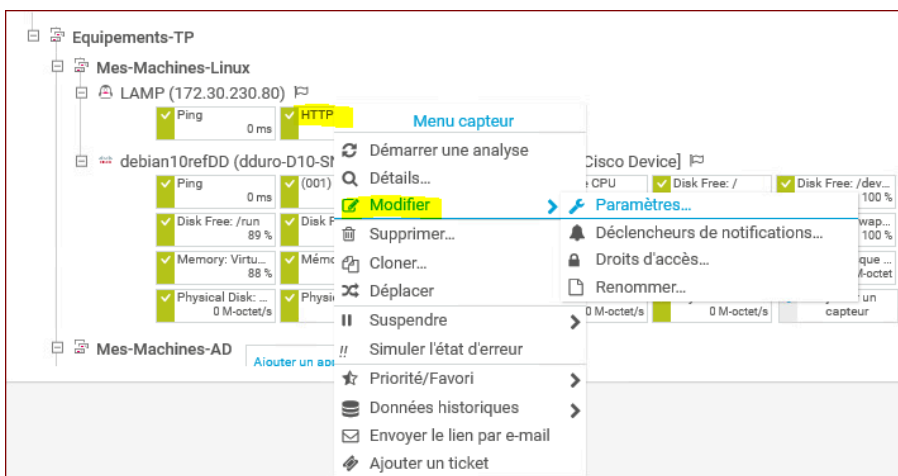
Jusqu'au retour à la « normale » :



Personnalisation des capteurs

Nous allons personnaliser un premier capteur par rapport à sa cible :

Le capteur HTTP test l'accès au répertoire grâce à l'URL « racine » du site comme le montre son paramétrage (clic droit sur le capteur HTTP / Paramètres



Voici les paramètres par défaut d'un capteur HTTP :

Modifier Object HTTP

Paramètres de base du capteur

Nom du capteur

HTTP

Balises parentes

Balises

httpsensor

Priorité

★★★★☆

Paramètres propres au HTTP

Délai d'expiration (s)

60

URL

http://

Annuler OK

N'hésitez pas à fermer les messages d'erreur :

Page d'accueil Équipements Bibliothèques Capteurs Alertes Cartes Rapports Logs Tickets Configuration

Équipements Probe locale Équipements-TP Mes-Machines-Linux LAMP (172.30.230.80) Ajouter un capteur (étape 1 à 2)

Ajouter un capteur à l'équipement LAMP (172.30.230.80) [172.30.230.80] (Étape 1 à 2)

Que peut-on surveiller ?

Utilisation de la mémoire

Type de système cible ?

Technologie utilisée ?

Activer le chiffrement SSL pour le site de PRTG

Votre licence d'essai a expiré il y a 4 jours...

Vous pouvez aussi modifier le mot de passe administrateur (Attention de s'en souvenir !) pour supprimer le 1<sup>er</sup> message (déjà effacé ci-dessus)

Plutôt que de supprimer le capteur, qui nous renseignera sur l'accès à la page web « racine », nous allons en créer un autre, mais en ciblant par exemple un alias ou un sous-répertoire pour faire simple :

Equipements-TP

Mes-Machines-Linux

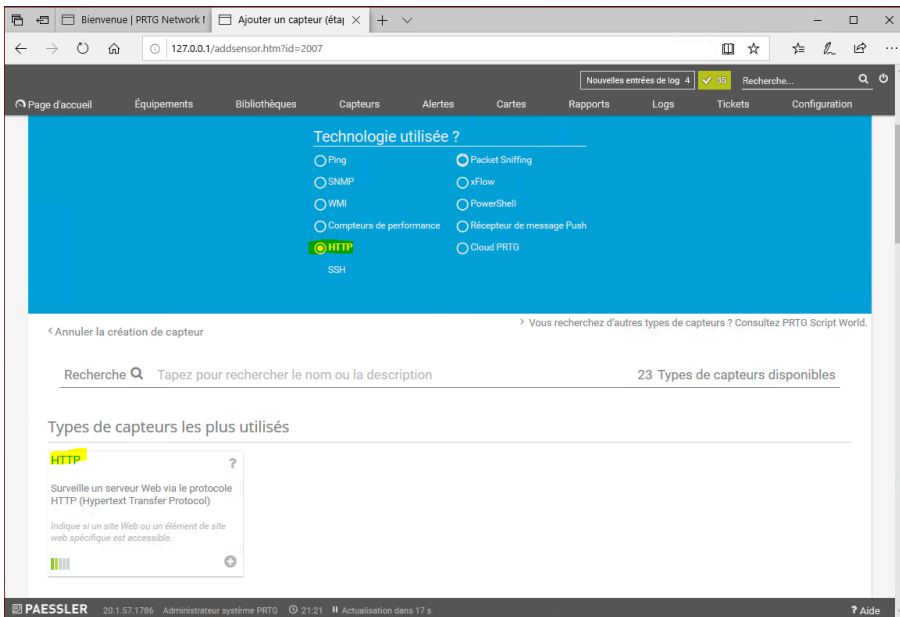
LAMP (172.30.230.80)

Ping 0 ms

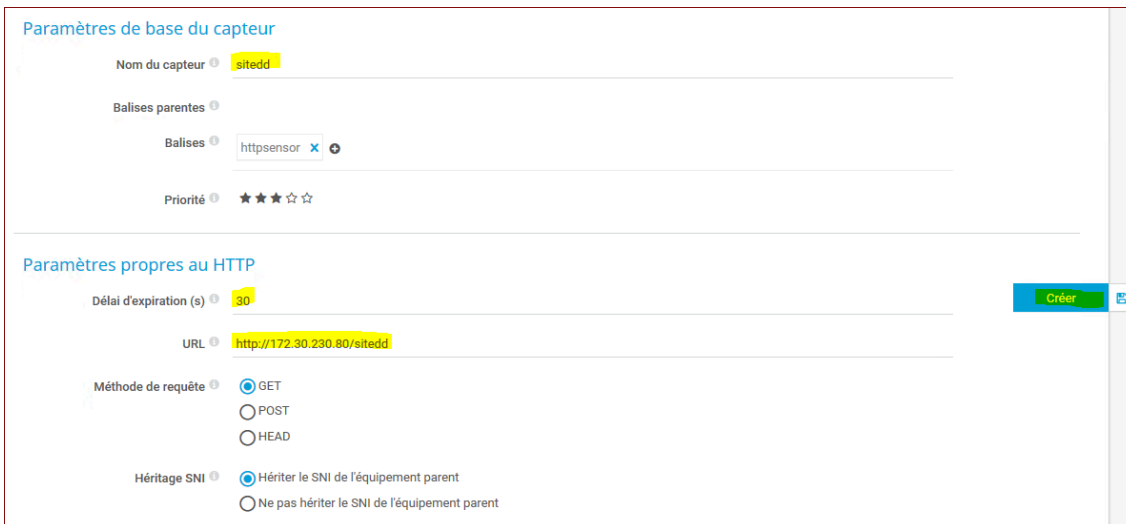
HTTP 9 ms

Ajouter un capteur

Sélectionner la technologie « HTTP » et cliquer sur type de capteur le plus utilisé :



Personnaliser le capteur comme ceci :



Dans un premier temps, le capteur ne reçoit pas de données :

Pos.	capteur	État	Message	Graphique	Priorité
1.	Ping	Disponi...	OK	Temps du pin 0 ms	★★★★★
2.	HTTP	Disponi...	OK	Temps de ch: 11 ms	★★★★☆
3.	sitedd	Inconnu	Pas encore de données	Temps de chPas de donn	★★★★☆

Si on démarre une analyse (pour accélérer le processus : clic droit sur le capteur / Démarrer l'analyse), le voyant est d'abord au jaune, puis au rouge :

Pos.	capteur	État	Message	Graphique	Priorité
1.	Ping	Disponi...	OK	Temps du pin 1 ms	★★★★★
2.	HTTP	Disponi...	OK	Temps de ch: 11 ms	★★★★☆
3.	sitedd	Non fo...	HTTP/1.1 404 Not Found	Temps de chPas de donn	★★★★☆

On va simuler la présence de « sitepn » (remplacer par vos initiales) en créant un sous-répertoire sur le serveur LAMP :

```
root@debian10lamp:~# cd /var/www/html/  
root@debian10lamp:/var/www/html# mkdir sitedd  
root@debian10lamp:/var/www/html# cd sitedd  
root@debian10lamp:/var/www/html/sitedd# touch index.html  
root@debian10lamp:/var/www/html/sitedd#
```

Vous pouvez accélérer la mise à jour du capteur, en démarrant une analyse sur le capteur et en réactualisant la page :

The screenshot shows the PRTG network monitoring interface. The top navigation bar includes 'Page d'accueil', 'Équipements', 'Bibliothèques', 'Capteurs', 'Alertes', 'Cartes', 'Rapports', 'Logs', 'Tickets', and 'Configuration'. The main content area displays a tree view of equipment under 'Groupe Racine'. A red arrow points to the 'sitedd' sensor under the 'LAMP (172.30.230.80)' group. The sensor status is 'OK' with a green checkmark. The right sidebar contains a 'SUPERVISER LES SITES DISTANTS' widget with a status of 'OK' and a default interval of '60 secondes'. Below the main view, a detailed view of the 'capteur sitedd' is shown, featuring a 'Temps de chargement' gauge and a table of sensor statistics.

Metric	Value
Dernière analyse:	30 s
Dernier OK:	30 s
Dernière erreur:	90 s
Disponibilité:	60,0005%
Temps mort:	39,9995%
Couverture:	100%
Type de capteur:	HTTP
Performance Impact:	
Dépendance:	Parent
Intervalle:	60 s
ID:	#2172

## Surveillance d'un serveur W2016

Nous allons maintenant surveiller une machine Windows 2016, plus précisément un AD 2016. Cette machine étant cruciale, nous souhaitons notamment surveiller :

L'espace disque sur ce serveur (en définissant un niveau critique)

La RAM

Le CPU

NB : Plusieurs capteurs sont disponibles, avec des fournisseurs différents. Nous utilisons le fournisseur WMI dans la suite de ce tuto.

Nous allons opérer en 4 étapes :

Vérifier ce que fait une découverte automatique sur un AD 2016 sans configuration spéciale pour la surveillance.

Tenter d'installer les capteurs Windows Espace Disque / RAM / CPU

Installer le Fournisseur WMI SNMP (Fonctionnalité) pour permettre leur mise en place effective.

Mise en place effective et paramétrage du capteur

## Découverte automatique

Ajouter l'équipement Serveur-AD au groupe « Mes-Machines-AD »

The screenshot shows the 'Ajouter un équipement au groupe Mes-Machines-AD' dialog box. The left pane is titled 'Nom et adresse de l'équipement' and contains fields for 'Nom de l'équipement' (ServerAD), 'Version IP' (IPv4 selected), and 'Adresse IPv4/Nom DNS' (172.30.230.53). Below these is a grid of device icons. The right pane is titled 'Identification d'équipements et découverte automatique' and shows 'Niveau de la découverte automatique' with 'Découverte automatique standard (recommandé)' selected. It also shows 'Données d'accès pour systèmes Windows' and 'Données d'accès pour les systèmes Linux/Solaris/Mac OS (SSH/WBEM)'. An 'OK' button is highlighted in yellow at the bottom right.

Une erreur devrait vous être retournée :

The screenshot shows an error dialog box with the title 'Désolé, l'analyse des éléments de surveillance disponibles a échoué...'. The main text reads: 'Impossible de créer le capteur Espace disque disponible SNMP sur l'équipement SERVEURAD (Srv-AD) (172.30.230.53)'. Below this, a red message states: 'No response (check: firewalls, routing, snmp settings of device, IPs, SNMP version, community, passwords etc) (erreur SNMP # -2003)'. At the bottom, there are buttons for '< Sélectionnez un autre type de capteur', 'Aide SNMP', 'Aide WMI', and 'Annuler'.

On sait que pour avoir certaines informations, il faut disposer d'informations supplémentaires comme des « credentials », au niveau du groupe pour en bénéficier plusieurs équipements, ou bien au niveau de l'équipement.

Dans notre scénario, nous avons prévu d'identifier plusieurs machines de la même manière, donc nous le ferons au niveau du groupe :

**Modifier Object Group-MV-AD**

Découverte automatique détaillée  
 Découverte automatique à partir de modèles d'équipement spécifiques

**Localisation**

Hérité de Group-MV-PPE (Localisation (pour Geo Maps): <vide>)

**Données d'accès pour systèmes Windows**

Hérité de Group-MV-PPE (Nom de domaine ou d'ordinateur: <vide>, Utili...)

**Nom de domaine ou d'ordinateur**

DOMPGI

**Utilisateur**

administrateur

**Mot de passe**

.....

**Données d'accès pour les systèmes Linux/Solaris/Mac OS (SSH/WBEM)**

Hérité de Group-MV-PPE (Utilisateur: <vide>, Connexion: 0, Pour le po...)

**Données d'accès pour VMware/XENServer**

Annuler OK

NB : Dans l'idéal, il serait préférable de ne pas utiliser le compte administrateur, mais d'un compte dédié, avec suffisamment de droit pour récupérer les informations. Vous êtes invité dans un 2<sup>ème</sup> temps à affiner ce paramétrage pour trouver les bons droits.

Installation des capteurs

**Ajouter un capteur à l'équipement SERVEURAD (Srv-AD) [172.30.230.53]**

< Annuler

**Paramètres de base du capteur**

Nom du capteur ⓘ Espace disque libre (plusieurs lecteurs)

Balises parentes ⓘ C\_OS\_VMware

Balises ⓘ diskspacesensor x wmidiskspacesensor x +

Priorité ⓘ ★★☆☆☆

---

**Configuration de l'espace disque libre WMI**

Lecteur ⓘ Tous

---

**intervalle**

Hérité de  
SERVEURAD (Srv-AD)  
(intervalle: 60 secondes, Régler le capteur en...)

## Installation du fournisseur WMI SNMP







Sur Windows 10

Ajouter la fonctionnalité facultative :

← Paramètres

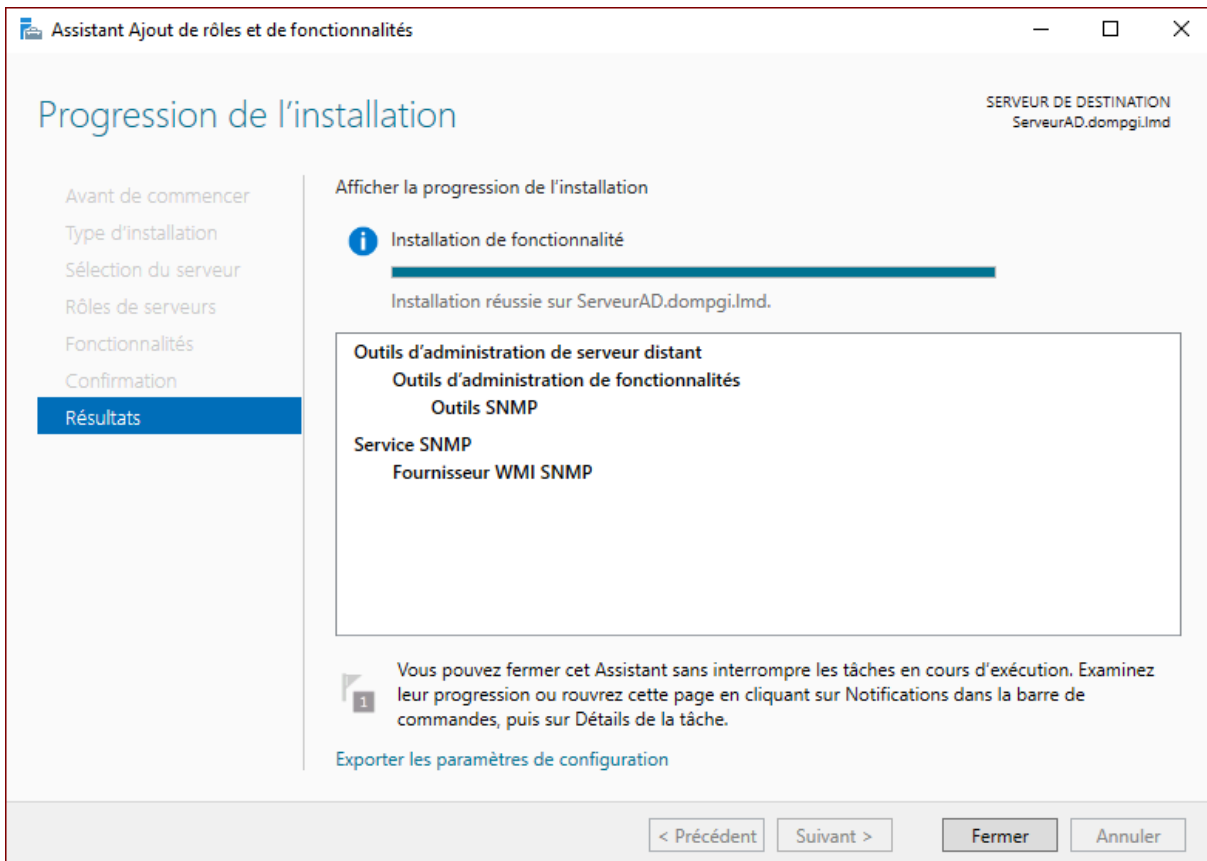
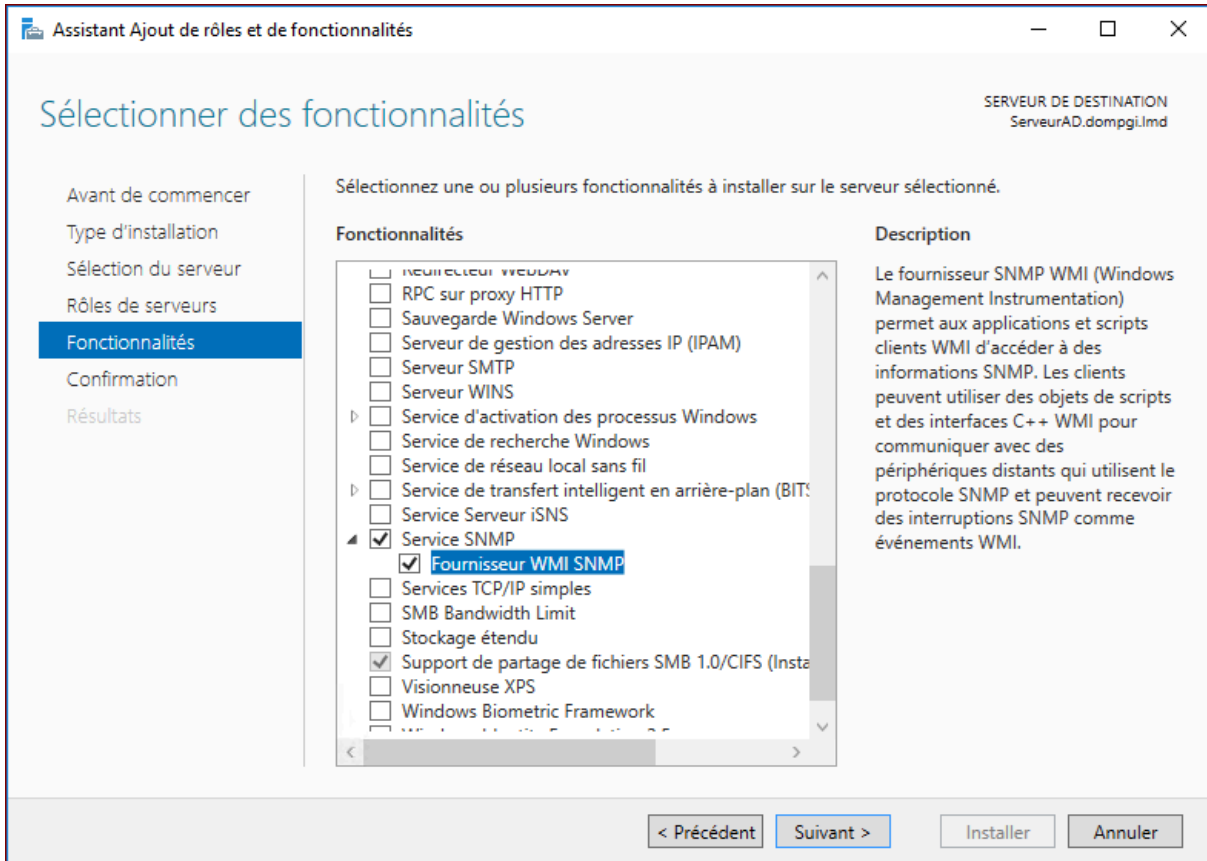
🏠 Ajouter une fonctionnalité

**Fonctionnalités facultatives**

	Fournisseur SNMP WMI	820 Ko
Le fournisseur WMI SNMP permet aux clients WMI d'utiliser des informations SNMP via le modèle CIM tel qu'il a été implémenté par WMI		
<b>Installer</b>		
	Gestion de Windows Storage	5,02 Mo
	Infrarouge IrDA	589 Ko
	Kit d'administration du Gestionnaire des connexions Microsoft (CMAK) RAS	482 Ko
	Lecteur Windows Media	16,5 Mo
	Media Feature Pack	67,5 Mo

Sur Windows 2016

C'est une fonctionnalité qu'on ajoute avec l'assistant « Ajout de rôles et de fonctionnalités »



Mise en place effective et paramétrage du capteur

Nouvelles entrées de log 69 Tickets modifiés 1 10 19 24 Recherche...

Page d'accueil Équipements Bibliothèques Capteurs Alertes Cartes Rapports Logs Tickets Configuration

Équipements Probe locale Group-MV-PPE Group-MV-AD SERVEURAD (Srv-AD) Ajouter un capteur (étape 1 à 2)

### Ajouter un capteur à l'équipement SERVEURAD (Srv-AD) [172.30.230.53] (Étape 1 à 2)

#### Que peut-on surveiller ?

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

#### Type de système cible ?

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

#### Technologie utilisée ?

- Ping
- SNMP
- WMI
- Compteurs de performance
- HTTP
- SSH
- Packet Sniffing
- xFlow
- PowerShell
- Récepteur de message Push

[Définir un mot de passe sécurisé](#)

L'administrateur PRTG utilise le mot de passe par défaut "prtgadmin". Modifiez-le pour sécuriser votre interface Web PRTG.

Ceci est obligatoire si votre site Web PRTG est accessible depuis Internet (au-delà de votre pare-feu) !

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

Recherche Tapez pour rechercher le nom ou la description 17 Types de capteurs disponibles

#### Types de capteurs disponibles

**Disque logique Dell PowerVault MDi**

Surveille l'état d'un disque logique sur votre Dell PowerVault MD3000

Nécessite Dell Modular Disk Storage Manager sur l'ordinateur exécutant la probe PRTG.

**Disque physique Dell PowerVault MDi BETA**

Surveille l'état d'un disque physique sur votre Dell PowerVault MD3000

Nécessite Dell Modular Disk Storage Manager sur l'ordinateur exécutant la probe PRTG.

**Espace disque disponible SNMP**

Surveille l'espace disque disponible sur un disque logique via SNMP

Utilise des valeurs OID plus génériques par rapport au SNMP Linux Disk Free Sensor.

Capteurs nécessitant des informations d'identification valides pour les serveurs Windows.

Pour ajouter ces types de capteurs, saisissez les informations d'identification appropriées sur l'équipement parent ou dans un groupe parent.

[Activer le chiffrement SSL pour le site de PRTG](#)

Votre connexion de navigateur à ce serveur PRTG n'est actuellement pas sécurisée par le chiffrement SSL.

Vous devriez passer en SSL, surtout si vous utilisez PRTG avec Internet (au-delà de votre pare-feu) !

[Basculer sur SSL](#)

[Votre licence d'essai a expiré il y a 1 jours.](#)

Une fois la période d'essai terminée, vous pouvez continuer à utiliser gratuitement PRTG avec 100 capteurs. Si vous avez besoin de capteurs supplémentaires, cliquez ici pour acheter une de nos licences commerciales.

Pas sûr que ce soit ce capteur qui soit proposé.

⇒ WMI plutôt

### Ajouter un capteur à l'équipement SERVEURAD (Srv-AD) [172.30.230.53]

< Annuler

#### Paramètres de base du capteur

**Nom du capteur** Espace disque libre (plusieurs lecteurs)

**Balises parentes** C\_OS\_VMware

**Balises** diskspacesensor wmidiskspacesensor

**Priorité** ★★★★★

---

#### Configuration de l'espace disque libre WMI

**Lecteur** Tous

---

#### Intervalle

Hérité de SERVEURAD (Srv-AD)  
(intervalle: 60 secondes, Régler le capteur en...)

## Modification des valeurs limite par défaut

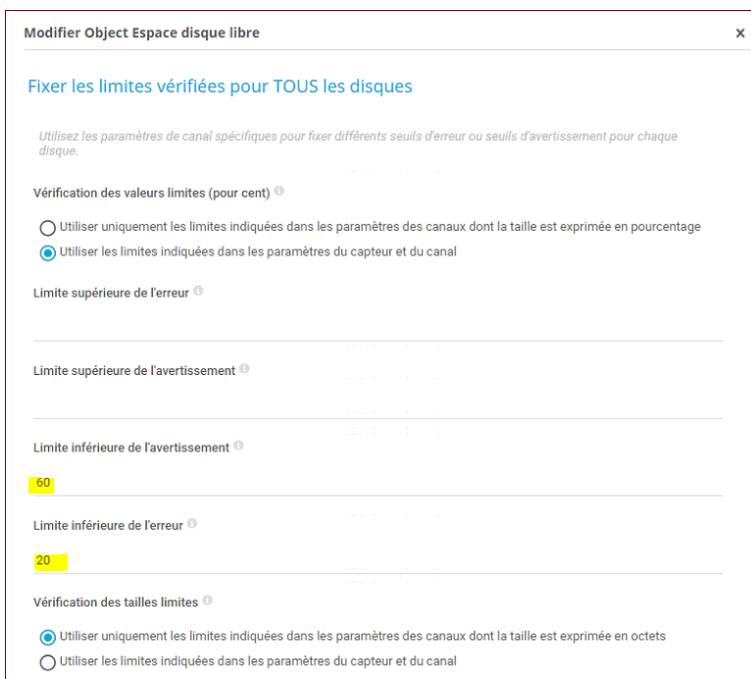
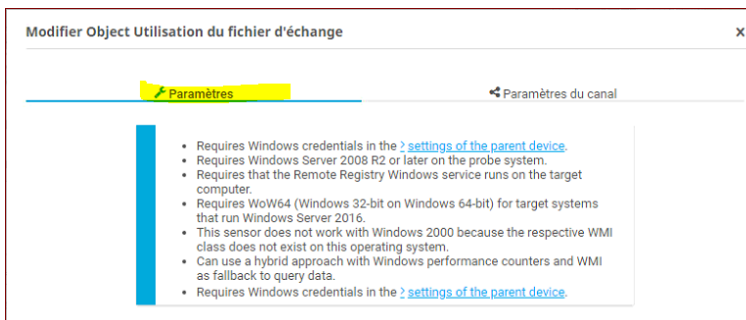
Pour vérifier le bon fonctionnement du capteur, attribuer une valeur critique adaptée à l'espace réel disponible sur votre machine :

Sensor	Value
Ping	0 ms
charge CPU	1 %
Espace disque libre	51 %

Ci-dessus je constate que l'espace disque disponible est de 51%

Je souhaiterais que le capteur passe au « orange » si l'espace disque est inférieur à 60% et au rouge s'il est inférieur à 20%.

Je retourne sur la configuration du capteur et j'accède à l'onglet Paramètres :



A noter que comme il s'agit de l'espace restant, ce sont des valeurs de type **Limite inférieure** que l'on définit !

Après réactualisation, le capteur passe au « orange », comme attendu, puisque l'espace disponible est de 51%, soit moins des 60% souhaités :

✓	Ping	0 ms
✓	charge CPU	0 %
W	Espace disque libre	51 %
✓	Mémoire	64 %

Attention ! Ce capteur n'effectue pas des tests aussi régulièrement que les capteurs que nous avons déjà vu, donc il faut forcer son analyse pour obtenir rapidement le nouvel état :

W capteur État des mises à jour Windows ★★★☆☆


32 j (Temps écoulé depuis la dernière mise à jour) est supérieur au seuil d'avertissement de 30 j dans Temps écoulé depuis la dernière mise à jour. Heure depuis la dernière mise à jour incorrecte

Vue d'ensemble | Données en temps réel | 2 Jours | 30 Jours | 365 Jours | Données historiques | Log | Paramètres | Déclencheurs de notifications | Commentaires | Historique

Dernière analyse: 168 s | Dernier OK: 168 s | Dernière erreur: | Disponibilité: 100,0000% | Temps mort: 0,0000% | Couverture: 7%

Type de capteur: Statut de mises à jour Windows (PowerShell) | Performance Impact: | Dépendance: Parent | Intervalle: 1 h | ID: #2187

Temps écoulé depuis la dernière mise à jour



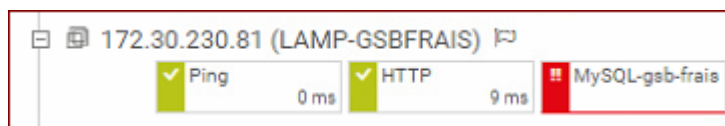
32 j | 0 s | 32 j

Temps écoulé depuis la dernière mise à jour  
ID du canal: 11  
Minimale: 26 j  
Moyenne: 30 j  
Max.: 32 j

Ci	D	Dernière valeur	Minimum	Maximum
Temps écoulé depuis la dernière ...	11	32 j	26 j	32 j
Temps mort	-4			

## Surveillance d'un serveur de bases de données MySQL

Si on tente rapidement de mettre en place un capteur MySQL sur un serveur Debian, on obtient une erreur, due aux nouvelles règles de sécurité par défaut :



En effet par défaut :

Il est impossible de se connecter à distance sur un serveur MySQL pour exécuter une requête.

Le service MySQL, dans sa configuration initiale, n'écoute que sur l'adresse de boucle « hôte local », à savoir 127.0.0.1

Pour rappel, un site web, comme « phpmysql » permet d'accéder aux bases de données parce qu'en fait le serveur LAMP exécute en local la requête SQL, et ne retourne que le résultat dans l'interface WEB.

```
#
# These groups are read by MariaDB server.
# Use it for options that only the server (but not clients) should see
#
# See the examples of server my.cnf files in /usr/share/mysql

# this is read by the standalone daemon and embedded servers
[server]

# this is only for the mysqld standalone daemon
[mysqld]

#
# * Basic Settings
#
user                = mysql
pid-file            = /run/mysqld/mysqld.pid
socket              = /run/mysqld/mysqld.sock
#port               = 3306
basedir             = /usr
datadir             = /var/lib/mysql
tmpdir              = /tmp
lc-messages-dir    = /usr/share/mysql
#skip-external-locking

# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address        = 127.0.0.1

#
# * Fine Tuning
#
#key_buffer_size    = 16M
#max_allowed_packet = 16M
#thread_stack       = 192K
#thread_cache_size  = 8
"/etc/mysql/mariadb.conf.d/50-server.cnf" 133L, 3940C écrit(s) 31,15 Haut
```

Pour s'en assurer, on peut tenter de se connecter à partir d'une autre machine :

```
root@debian10lamp:~# mysql -h 172.30.230.81 -u userGsb -p
Enter password:
ERROR 2002 (HY000): Can't connect to MySQL server on '172.80.230.81' (115)
root@debian10lamp:~#
```

Modification du fichier de configuration pour écouter sur l'adresse réelle :

```
# Instead of skip-networking the default is now to listen only on
# localhost which is more compatible and is not less secure.
bind-address            = 172.30.230.81
```

NB : On peut aussi écrire « 0.0.0.0 » pour toute adresse disponible sur la machine !

Le message n'est plus le même après une nouvelle tentative une fois la modification effectuée pour écouter sur l'adresse réelle IP, et pas seulement en local :

```
root@debian10lamp:~# mysql -h 172.30.230.81 -u userGsb -p
Enter password:
ERROR 1130 (HY000): Host '172.30.230.80' is not allowed to connect to this MariaDB server
root@debian10lamp:~#
```

Il s'agit maintenant d'une problématique de droits. Pour autoriser l'accès depuis une machine externe sur une base de données, on peut le faire, en invite de commande MySQL, avec l'instruction « GRANT » :

```
root@dduro-web1:~# mysql -u root -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 29
Server version: 10.3.15-MariaDB-1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

MariaDB [(none)]> GRANT ALL PRIVILEGES ON gsb_frais.* TO prtguser@172.30.230.91 IDENTIFIED by "secret";
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
MariaDB [(none)]> GRANT ALL PRIVILEGES ON gsb_frais.* TO prtguser@172.30.230.80 IDENTIFIED by "secret";
Query OK, 0 rows affected (0.001 sec)

MariaDB [(none)]>
```

D'après les instructions tapées ci-dessus, désormais l'accès sera possible depuis une autre machine linux (adresse .80) et la machine PRTG (adresse .91)

On note que l'utilisateur **prtguser** est créé s'il n'existe pas (ce qui était le cas ici).

La connexion est possible :

```
root@debian10lamp:~# mysql -h 172.30.230.81 -u prtguser -p
Enter password:
Welcome to the MariaDB monitor.  Commands end with ; or \g.
Your MariaDB connection id is 63
Server version: 10.3.15-MariaDB-1 Debian 10

Copyright (c) 2000, 2018, Oracle, MariaDB Corporation Ab and others.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

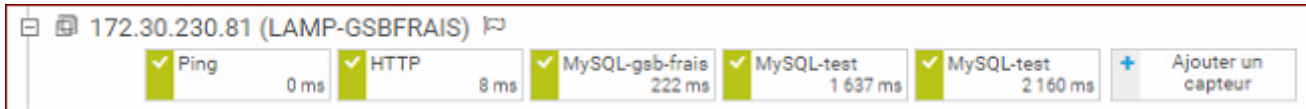
MariaDB [(none)]>
```

On peut obtenir le résultat de la commande SQL que l'on va utiliser dans la suite de ce tutorial :

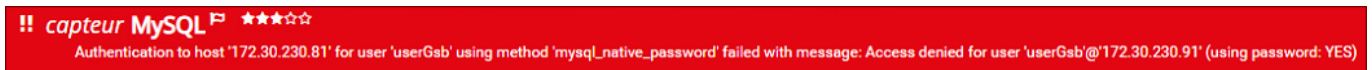
```
MariaDB [(none)]> use gsb_frais
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Database changed
MariaDB [gsb_frais]> select count(*) from Visiteur;
+-----+
| count(*) |
+-----+
|        27 |
+-----+
1 row in set (0.001 sec)

MariaDB [gsb_frais]> _
```

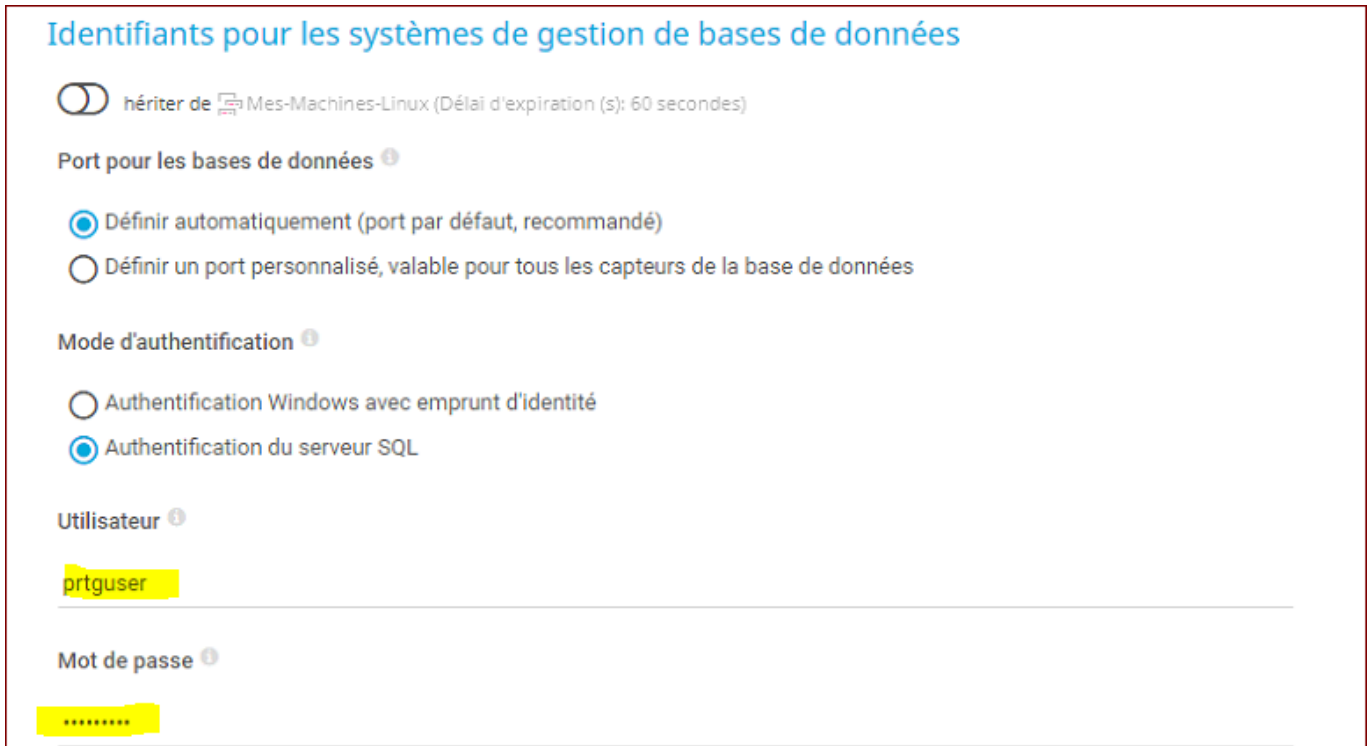


Si le message suivant s'affiche dans les manipulations qui vont suivre, c'est que vous n'avez pas donné les bons « credentials » au niveau de l'équipement, pour l'accès à la base de données, ou bien que l'utilisateur n'a pas les droits suffisants :



Mise en place des « credentials » sur l'équipement serveur MySQL :

Clic droit / modifier les paramètres de l'équipement, descendre dans la liste de paramètres de personnalisation :



Les capteurs sur un serveur de base de données peuvent avoir plusieurs objectifs :

Vérifier le bon fonctionnement du service. Un capteur « classique » sur l'ouverture d'un port peut être suffisant. Vérifier l'existence d'une base de données : la requête proposée par défaut par le capteur MySQL convient très bien.

Vérifier l'existence d'une table ou même récupérer le nombre de lignes d'une table, ou encore récupérer le résultat d'une requête plus complexe (ex : moyenne des commandes, nombre de fiches de frais non traitées, etc ...)

Nous nous proposons de :

Créer un capteur affichant simplement la disponibilité du serveur mysql (port 3306)

Créer un capteur affichant le nombre de visiteurs d'après le nombre de lignes retournées par une requête :

Requête utilisée : `SELECT * FROM Visiteur ;`

Créer un capteur affichant le nombre de visiteurs cette fois-ci d'après le résultat d'une requête :

Requête utilisée : `SELECT Count(*) FROM Visiteur ;`

## Ecoute d'un port

Plusieurs possibilités sont généralement offertes pour surveiller la fonctionnalité d'un équipement. La vérification d'un port peut se faire par un capteur dédié, que l'on peut repérer en faisant une recherche sur « port TCP » :

The screenshot shows the PRTG sensor creation wizard for the device 172.30.230.81. The search term 'port TCP' has been entered, resulting in four sensor options:

- Bibliothèque SNMP**: Surveille un équipement à l'aide du SNMP et de fichiers MIB compilés ("bibliothèques SNMP (oidlib)").
- Plage de port**: Surveille un service réseau en se connectant à différents ports TCP/IP. Description: "Essaie de se connecter aux ports TCP/IP spécifiés d'un équipement et attend que la demande soit acceptée."
- Port**: Vérifie la disponibilité d'un service de réseau en se connectant à son port TCP / IP. Description: "Tente de se connecter au port TCP/IP d'un équipement et attend l'acceptation de la requête."
- Vérification de sécurité SSL**: Surveille la connectivité SSL d'un port TCP/IP. Description: "Tente de se connecter au numéro de port TCP/IP spécifié avec différents protocoles SSL."

Page d'accueil Équipements Bibliothèques Capteurs Alertes Cartes Rapports Logs Tickets Configuration

Équipements Probe locale Équipements-TP Mes-Machines-Linux 172.30.230.81 (LAMP-GSBFRAIS) Ajouter un capteur (étape 2 à 2)

### Ajouter un capteur à l'équipement 172.30.230.81 (LAMP-GSBFRAIS) [172.30.230.81] (Étape 2 à 2)

< Annuler

#### Paramètres de base du capteur

Nom du capteur

Balises parentes

Balises

Priorité

#### Paramètres de port

Délai d'expiration (s)

Port

#### Sécurité au niveau du transport

Sécurité  Ne pas utiliser la sécurité au niveau du transport (par défaut)  
 Utiliser la sécurité au niveau du transport

#### Paramétrages avancés du capteur

État désiré  Ouvert

Noter le paramétrage par défaut de l'intervalle :

intervalle

hériter de  172.30.230.81 (LAMP-GSBFRAIS)

(intervalle: 60 secondes, Régler le capteur en...)

intervalle: 60 secondes, Régler le capteur en avertissement pour 1 intervalle, puis en non fonctionnel (recommandé)

Dans un 1<sup>er</sup> temps, le capteur affiche « Pas encore de données » :

Port-3306-MySQL Inconnu Pas encore de données Disponible Pas de donné ★★★★★

Après quelques 60 secondes et un rafraîchissement, le port est bien détecté comme disponible :

Port-3306-MySQL Disponi... OK Disponible 0 ms ★★★★★

Vérifions toutefois qu'en cas d'arrêt du service, le capteur passe bien au rouge :

Arrêt du service

```
root@dduro-web1:~#
root@dduro-web1:~# service mysql stop
root@dduro-web1:~# _
```

Passage au « orange » dans un premier temps, comme prévu par le paramétrage par défaut

Port-3306-MySQL Avertis... Connection refused (erreur de so... Disponible Pas de donné ★★★★★

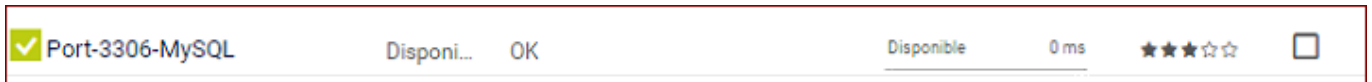
Passage au « rouge »

Port-3306-MySQL Non fo... Connection refused (erreur de so... Disponible Pas de donné ★★★★★

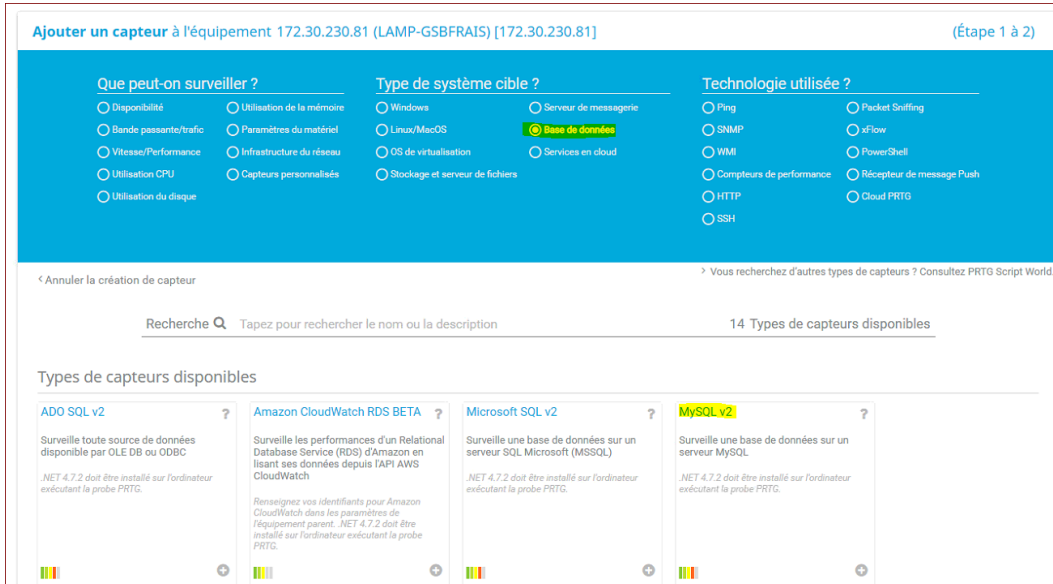
Redémarrage du service

```
root@dduro-web1:~# service mysql start
root@dduro-web1:~# _
```

Au bout de 60 secondes, même sans réactualisation, le capteur repasse au vert :

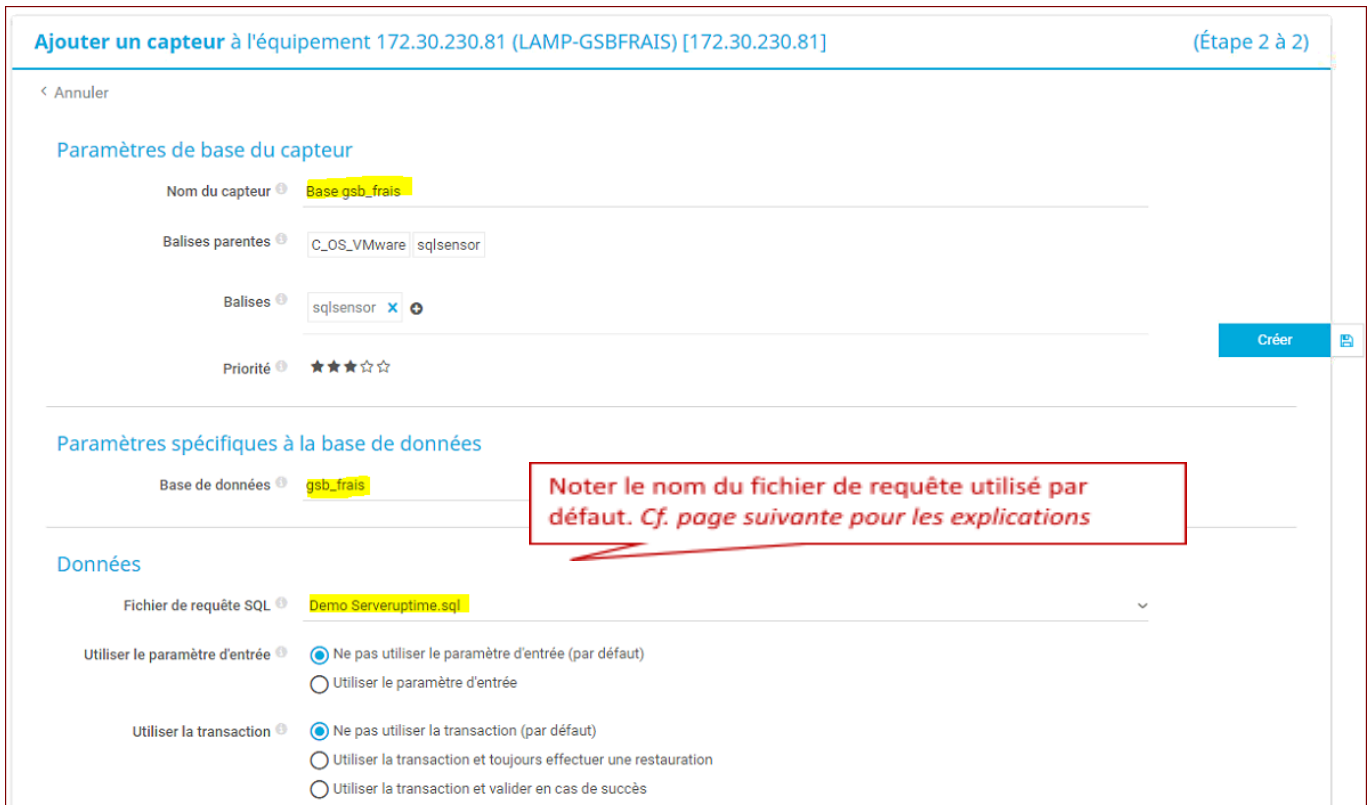


Il est aussi également possible, plutôt que de vérifier simplement l'ouverture d'un port, de vérifier la présence d'une base de données précise sur le serveur MySQL :

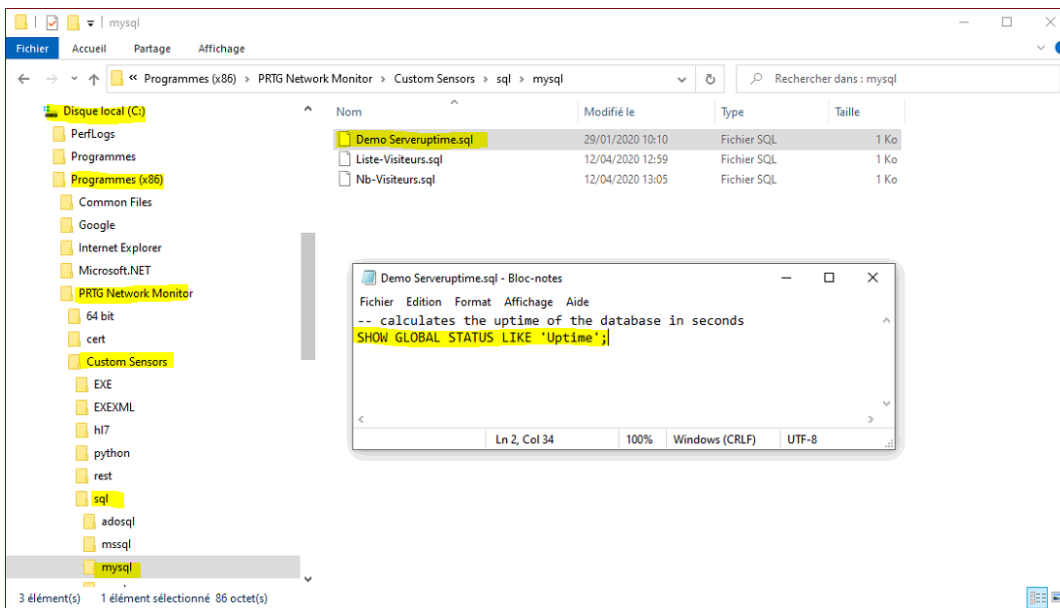


NB : Il est possible aussi de cibler la recherche en indiquant MySQL dans le champ de recherche.

Le paramétrage est alors relativement simple :



NB : On remarque le fichier de requête exécutée par défaut. Dans la documentation PRTG, on trouve l'emplacement des modèles de requêtes :



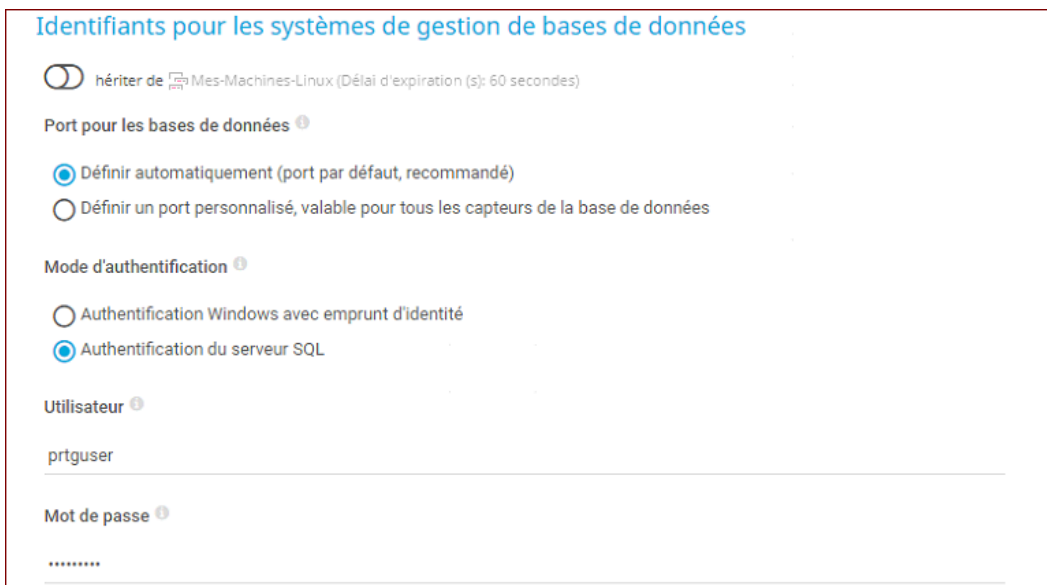
La requête se contente de récupérer l'information concernant la durée de fonctionnement. Pour information, exécution de la requête dans l'invite de commande mysql :

```

MariaDB [gsb_frais]> SHOW GLOBAL STATUS LIKE 'Uptime';
+-----+-----+
| Variable_name | Value |
+-----+-----+
| Uptime        | 1719  |
+-----+-----+
1 row in set (0.002 sec)
MariaDB [gsb_frais]> _

```

Rappel : Pour que le capteur soit opérationnel et passe au vert, il faut bien entendu 2 conditions : avoir autorisé l'accès au service MySQL depuis la machine hébergeant PRTG (ou depuis son réseau) avoir renseigné les identifiants permettant l'accès au SGBD au niveau de l'équipement :



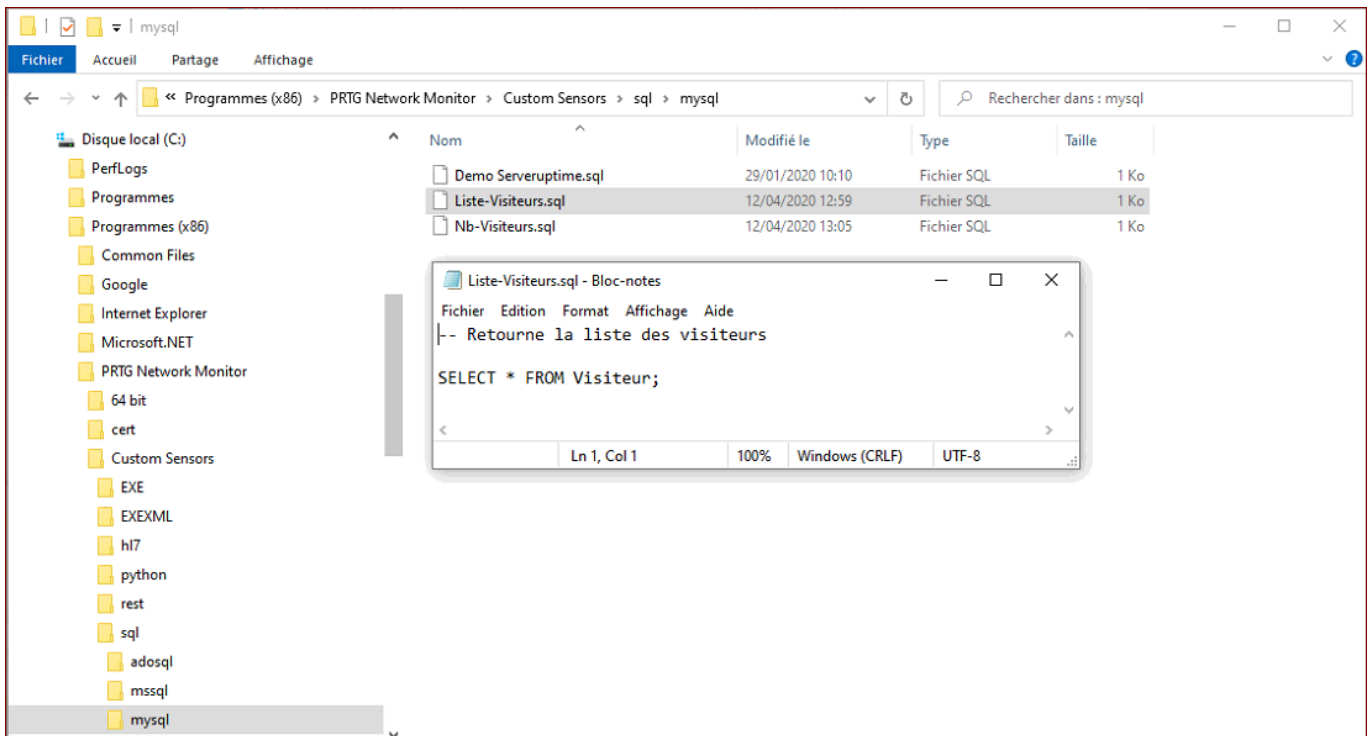
Le capteur devient rapidement opérationnel :



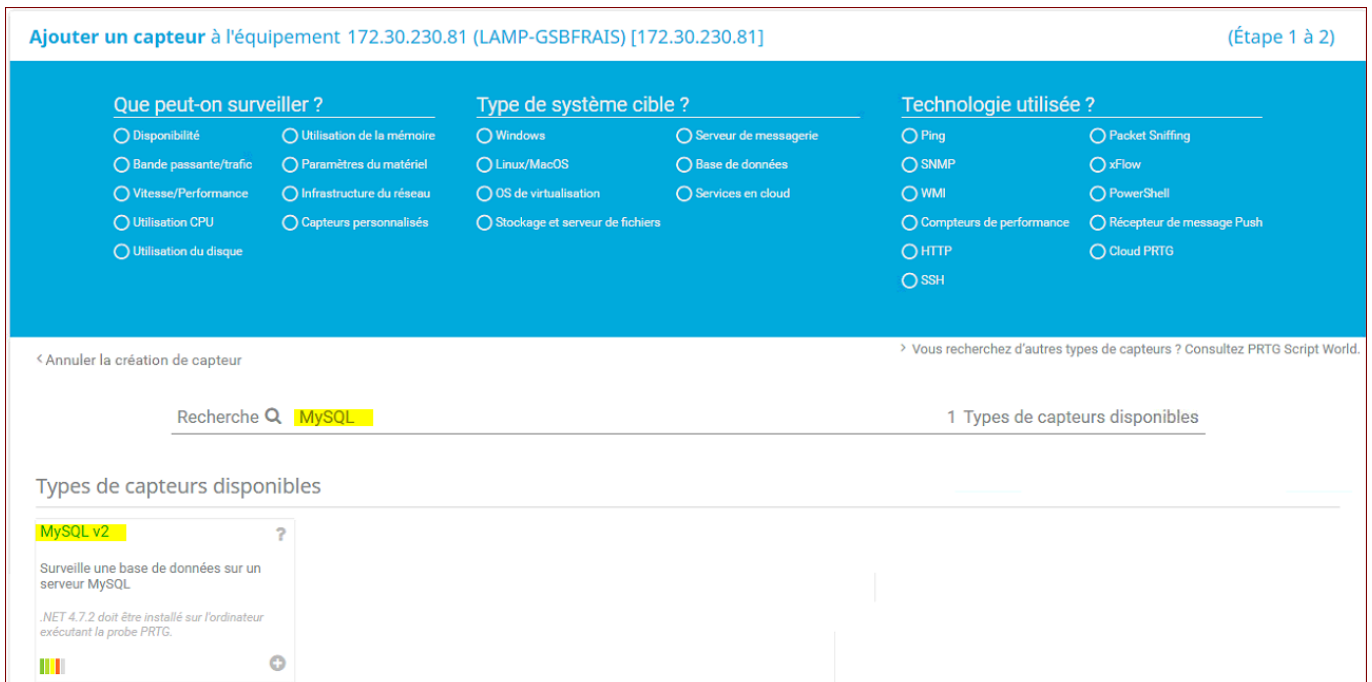
### Capteur indiquant le nombre de lignes retournées par une requête :

On ajoute d'abord la requête souhaitée dans le dossier mysql des « Custom Sensors » :

Attention ! Ces fichiers se trouvent d'un sous-répertoire de c:\Programme(x86) il faut des droits administrateur pour sauvegarder le fichier. ⇒ Lancer Notepad **en tant qu'administrateur** pour pouvoir l'enregistrer :



On ajoute un nouveau capteur MySQL :



**Ajouter un capteur** à l'équipement 172.30.230.81 (LAMP-GSBFRAIS) [172.30.230.81] (Étape 2 à 2)

< Annuler

### Paramètres de base du capteur

Nom du capteur

Balises parentes

Balises

Priorité

---

### Paramètres spécifiques à la base de données

Base de données

---

### Données

Fichier de requête SQL

Utiliser le paramètre d'entrée

Utiliser le paramètre d'entrée

Choisir la requête que vous avez créée dans la liste

Ne pas oublier de changer l'option de Traitement des données avant de valider la création du capteur ; on souhaite compter les lignes retournées :

### Données

Fichier de requête SQL

Utiliser le paramètre d'entrée  Ne pas utiliser le paramètre d'entrée (par défaut)  Utiliser le paramètre d'entrée

Utiliser la transaction  Ne pas utiliser la transaction (par défaut)  Utiliser la transaction et toujours effectuer une restauration  Utiliser la transaction et valider en cas de succès

Traitement des données  Exécuter simplement la requête  Compter les lignes du tableau  Traiter le tableau de données

Après réactualisation du capteur, si on regarde le détail, on retrouve la valeur correspondant au nombre de visiteurs présents dans la table **Visiteur** :

<input checked="" type="checkbox"/> Nb-Lignes-Table-Visiteur (gsb_frais)	Disponible	Ok	Temps d'exéc	265 ms	★★★★☆	<input type="checkbox"/>
--	------------	----	--------------	--------	-------	--------------------------

Le résultat complet se trouve dans détail du capteur (accéder aux détails du capteur) :

capteur Nb-Lignes-Table-Visiteur (gsb\_frais) ★★★★☆ Ok

Vue d'ensemble | Données en temps réel | 2 Jours | 30 Jours | 365 Jours | Données historiques | Log | Paramètres | Déclencheurs de notifications | Commentaires | Historique

Dernière analyse: 56 s | Dernier OK: 56 s | Dernière erreur: 5 min. 26 s | Disponibilité: 68,5243% | Temps mort: 31,4757% | Couverture: 100%

Type de capteur: MySQL v2 | Performance Impact: ■■■ | Dépendance: Parent | Intervalle: 60 s | ID: #2206

Temps d'exécution: 265 ms | Lignes affectées: 27 # | Temps d'exécution de la requête: 56 ms

**La table Visiteur comporte précisément 27 lignes.**

Canal	ID	Dernière valeur	Minimum	Maximum
Lignes affectées	2	27 #	27 #	27 #
Temps d'exécution	0	265 ms	263 ms	283 ms
Temps d'exécution de la requête	1	56 ms	56 ms	66 ms
Temps mort	-4			

Si le message suivant s'affiche, c'est que les droits ne sont pas suffisants pour exécuter la requête, ou bien que vous n'avez pas renseigné correctement les « credentials » de l'utilisateur MySQL :

!! capteur Nb-Lignes-Table-Visiteur (gsb\_frais) ★★★★☆

Authentication to host '172.30.230.81' for user 'prtguser' using method 'mysql\_native\_password' failed with message: Access denied for user 'prtguser'@'172.30.230.91' to database 'gsb\_grais'

Ci-dessus on avait fait une erreur dans le nom de la base de données : « gsb\_grais » au lieu de « gsb\_frais ».

Vérifions la mise à jour du capteur en cas d'ajout des visiteurs :

Ajout de 2 visiteurs :

The screenshot shows the phpMyAdmin interface for the 'Visiteur' table in the 'gsb\_frais' database. The table structure is defined with the following columns and values:

Colonne	Type	Fonction	Null	Valeur
id	char(4)		d10	
nom	char(30)		DURON	
prenom	char(30)		David	
login	char(20)		dduron	
mdp	char(20)		rtyu10	
adresse	char(30)		300 Avenue Sakharov	
cp	char(5)		69009	
ville	char(30)		LYON	
dateEmbauche	date		2020-04-13	

Colonne	Type	Fonction	Null	Valeur
id	char(4)		c20	
nom	char(30)		CHEKARI	
prenom	char(30)		Karim	
login	char(20)		kchekari	
mdp	char(20)		kckr20	
adresse	char(30)		1 rue de Crouy	
cp	char(5)		01000	
ville	char(30)		BOURG-EN-BRESSE	
dateEmbauche	date		2020-04-13	

La table comporte bien 29 lignes désormais :

The screenshot shows the phpMyAdmin interface displaying the 'Visiteur' table with 29 rows of data. A green status bar at the top indicates 'Affichage des lignes 0 - 2 (total de 29, traitement en 0.0003 seconde(s))', with the number '29' circled in red. The table structure and data are as follows:

Options	id	nom	prenom	login	mdp	adresse	cp	ville	dateEmbauche
Éditer Copier Supprimer	a131	Villechalane	Louis	lvillachane	jux7g	8 rue des Charmes	46000	Cahors	2005-12-21
Éditer Copier Supprimer	a17	Andre	David	dandre	oppg5	1 rue Petit	46200	Lalbenque	1998-11-23
Éditer Copier Supprimer	a55	Bedos	Christian	cbedos	gmhxd	1 rue Peranud	46250	Montcuq	1995-01-12
Éditer Copier Supprimer	a93	Tusseau	Louis	ltusseau	ktp3s	22 rue des Ternes	46123	Gramat	2000-05-01

Vérification du nouvel état du capteur :

The screenshot shows the PRTG Network Monitor interface for a sensor named 'capteur Nb-Lignes-Table-Visiteur (gsb\_frais)'. The interface includes a navigation bar with options like 'Vue d'ensemble', 'Données en temps réel', and 'Données historiques'. Below this, there are several performance metrics and gauges:

- Statistiques :** Dernière analyse: 46 s, Dernier OK: 46 s, Dernière erreur: 22 min. 16 s, Disponibilité: 90,6825%, Temps mort: 9,3175%, Couverture: 100%.
- Configuration :** Type de capteur: MySQL v2, Performance Impact: (indicated by a bar chart), Dépendance: Parent, Intervalle: 60 s, ID: #2206.
- Temps d'exécution :** A large gauge shows a current value of 267 ms, with a range from 0 ms to 311 ms.
- Lignes affectées :** A gauge shows 29 lines affected, with a range from 27 # to 29 #.
- Temps d'exécution de la requête :** A gauge shows 62 ms, with a range from 56 ms to 84 ms.

At the bottom, a table provides a detailed breakdown of the sensor's performance:

Canal	ID	Dernière valeur	Minimum	Maximum
Lignes affectées	2	29 #	27 #	29 #
Temps d'exécution	0	267 ms	250 ms	311 ms
Temps d'exécution de la requête	1	62 ms	56 ms	84 ms
Temps mort	-4			

### Capteur récupérant le résultat d'une requête SQL :

La requête est légèrement différente de la précédente ; elle ne retournera qu'une ligne et qu'une valeur :

The screenshot shows a Windows File Explorer window displaying the 'mysql' folder. The folder contains three SQL files: 'Demo Serveruptime.sql', 'Liste-Visiteurs.sql', and 'Nb-Visiteurs.sql'. A Notepad window titled 'Nb-Visiteurs.sql - Bloc-notes' is open, showing the following SQL query:

```
SELECT count(*) FROM Visiteur;
```

The Notepad window also shows the file's encoding as UTF-8 and the line/column position as Ln 1, Col 1.

[< Annuler](#)

## Paramètres de base du capteur

Nom du capteur Balises parentes  Balises   Priorité     

Créer



## Paramètres spécifiques à la base de données

Base de données 

## Données

Fichier de requête SQL Utiliser le paramètre d'entrée  Ne pas utiliser le paramètre d'entrée (par défaut)  
 Utiliser le paramètre d'entréeUtiliser la transaction  Ne pas utiliser la transaction (par défaut)  
 Utiliser la transaction et toujours effectuer une restauration  
 Utiliser la transaction et valider en cas de succèsTraitement des données  Exécuter simplement la requête  
 Compter les lignes du tableau  
 Traiter le tableau de donnéesTraiter DBNull dans les valeurs de canal  
comme  Erreur  
 Chiffre 0Sélectionner la valeur de canal par  Numéro de colonne  
 Nom de la colonne  
 Numéro de ligne  
 Paire clé-valeurNom du canal de capteur #1 Numéro de colonne du canal de capteur #1 

Créer



La requête ne renvoie qu'une colonne correspondant au « count(\*) »

 Compte-Nb-Visiteurs (gsb\_frais)

Disponible

Ok

Temps d'exéc 1 052 ms

Le détail du compteur retourne bien la valeur 29, comme le capteur précédent :

**capteur Compte-Nb-Visiteurs (gsb\_frais)** ★★☆☆☆

Ok

Vue d'ensemble | Données en temps réel | 2 Jours | 30 Jours | 365 Jours | Données historiques | Log | Paramètres | Déclencheurs de notifications | Commentaires | Historique

Dernière analyse: 58 s | Dernier OK: 58 s | Dernière erreur: | Disponibilité: 100,0000% | Temps mort: 0,0000% | Couverture: 100%

Type de capteur: MySQL v2 | Performance Impact: | Dépendance: Parent | Intervalle: 60 s | ID: #2207

**Temps d'exécution**

Lignes affectées: 1 # | Nb-Visiteurs-GSB: 29 # | Temps d'exécution de la requête: 58 ms

261 ms | 0 ms | 1 052 ms

Canal	ID	Dernière valeur	Minimum	Maximum
Lignes affectées	2	1 #	1 #	1 #
Nb-Visiteurs-GSB	3	29 #	29 #	29 #
Temps d'exécution	0	261 ms	261 ms	1 052 ms
Temps d'exécution de la requête	1	58 ms	58 ms	94 ms
Temps mort	-4			

On note que le capteur n'a jamais détectée de valeur < 29