Mr ROTH

Compte rendu TP6

14/02/2024

PRTG – Supervision - Monitoring

TEWES Arnaud
BTS SIO SISR 1ÈRE ANNÉE

1. Introduction

PRTG (Paessler Router Traffic Grapher) est un outil de supervision et de surveillance puissant, utilisé notamment en entreprise. Il permet de surveiller et de superviser la qualité de service en installant des capteurs (ou sondes) sur des équipements (serveurs, ordinateurs, routeurs, switchs, etc.), en collectant des données réseau et en générant des alertes en cas de problème.

Cet outil permet de vérifier en temps réel que l'ensemble des équipements de notre réseau fonctionne correctement. Il intègre un système d'alarme intégré personnalisable comme nous le souhaitons, qui permet de nous avertir par courriel, notification push ou SMS de différentes erreurs, défaillances système ou réseau, ou lorsqu'un équipement aura atteint un seuil défini (exemple : espace disque libre inférieur à 10% -> alerte).

PRTG utilise principalement les technologies WMI et SNMP :

- SNMP (Simple Network Management Protocol) : SNMP est un protocole de surveillance largement utilisé qui permet de superviser et de gérer une grande variété d'équipements sur les réseaux TCP/IP (tels que des switchs réseau, routeurs, pare-feu, imprimantes, etc.). Cette technologie est moins gourmande que WMI.

- WMI (Windows Management Instrumentation) : WMI est la technologie de base de Microsoft pour la surveillance et la gestion des systèmes Windows. PRTG l'utilise pour accéder aux données de divers paramètres de configuration Windows et à des valeurs d'état système.

PRTG peut également créer des sondes en se servant d'autres protocoles comme :

- ICMP (Internet Control Message Protocol) : Plus connu sous le nom de Ping, pour vérifier la disponibilité des appareils sur le réseau.

- Packet Sniffing : Cette méthode permet à PRTG d'analyser le trafic réseau en détail.

- Compteurs de performance : PRTG peut utiliser des compteurs de performance pour surveiller les systèmes Windows. L'avantage de PRTG est qu'il est gratuit jusqu'à 100 capteurs (un capteur étant une sonde qu'on installe pour surveiller un point précis).

Dans mon entreprise, nous utilisons PRTG sur les serveurs de nos clients principalement grâce à la technologie « iLo » des serveurs. Ce dernier est affiché sur un écran dans le helpdesk et nous permet de surveiller les serveurs et autres équipements en temps réel d'un simple coup d'œil. Nous avons bien évidemment des notifications lorsque ce dernier recense une erreur.

Prérequis :

- Système d'exploitation : Windows Server 2022, Windows Server 2019, Windows Server 2016, Windows 11 ou Windows 10.

- RAM : Environ 150 KB de RAM par capteur. En général, il est recommandé au moins 1 cœur de CPU supplémentaire et 1 Go de RAM pour chaque 1 000 capteurs supplémentaires.

- Espace disque : Environ 200 KB d'espace disque par capteur par jour.

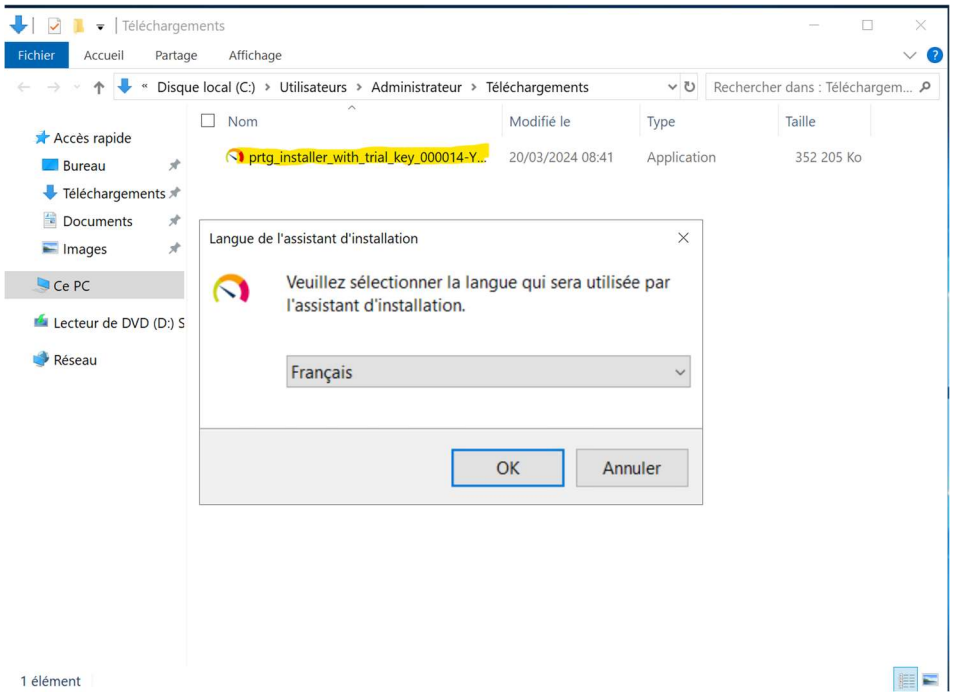
- Des équipements compatibles SNMP ou WMI.

En fonction du nombre de capteurs que vous prévoyez d'utiliser, voici les recommandations pour l'installation du serveur central PRTG : Jusqu'à 500 capteurs : 4 cœurs de processeur, 4 Go de RAM, 100 Go d'espace disque. Jusqu'à 1 000 capteurs : 6 cœurs de processeur, 6 Go de RAM, 500 Go d'espace disque. Jusqu'à 2 500 capteurs : 8 cœurs de processeur, 8 Go de RAM, 750 Go d'espace disque. Jusqu'à 5 000 capteurs : 8 cœurs de processeur, 12 Go de RAM, 1 000 Go d'espace disque. Jusqu'à 10 000 capteurs : 10-12 cœurs de processeur, 16 Go de RAM, 1 500 Go d'espace disque.

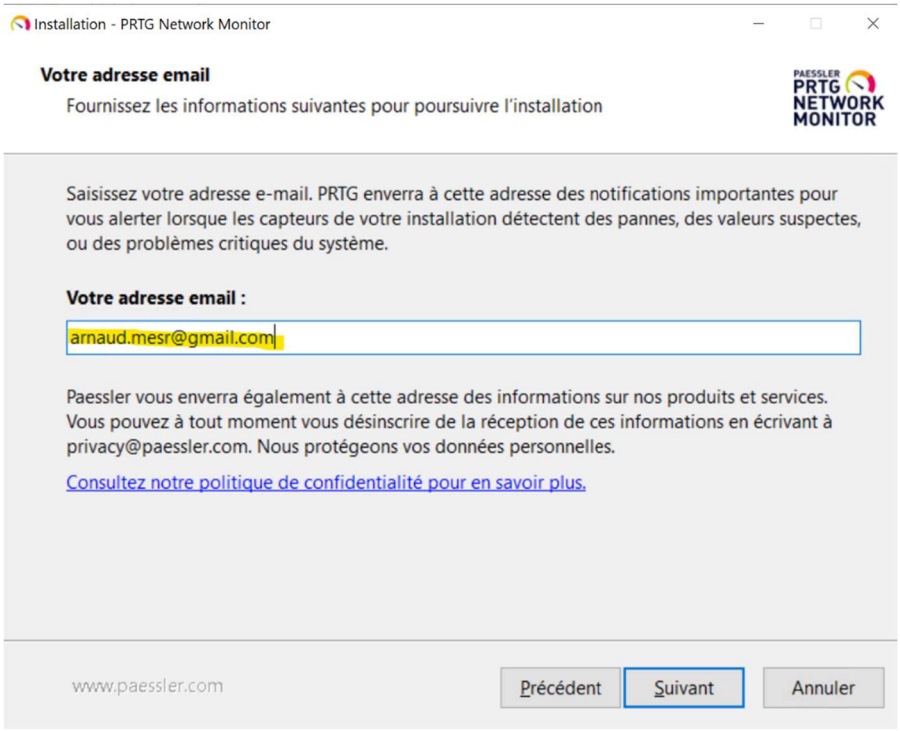
Dans ce TP, j'ai procédé à l'installation de PRTG, et à la mise en place de sondes WMI et ICMP sur notre serveur Active Directory (étant en labo de test pour ma formation, je n'ai pas d'équipements SNMP disponibles pour créer des sondes sur ce dernier).

2. Installation et procédé pas à pas

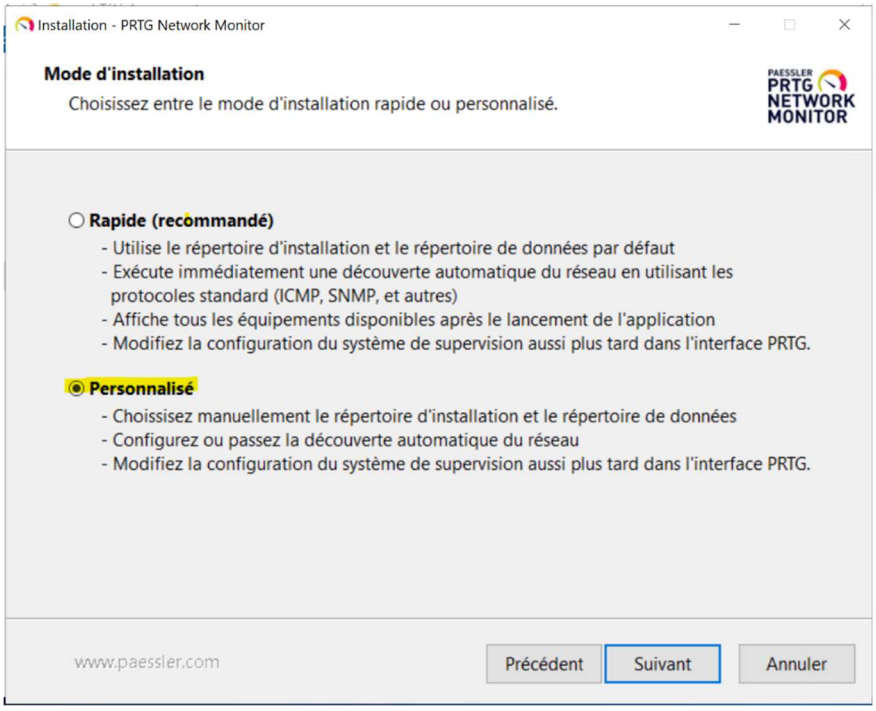
Dans un premier temps, il faudra télécharger l'exécutable d'installation de PRTG sur le site officiel et commencer l'installation. PRTG nous fournit une clé de licence gratuite directement intégré à l'exécutable pour nos 100 capteurs gratuits



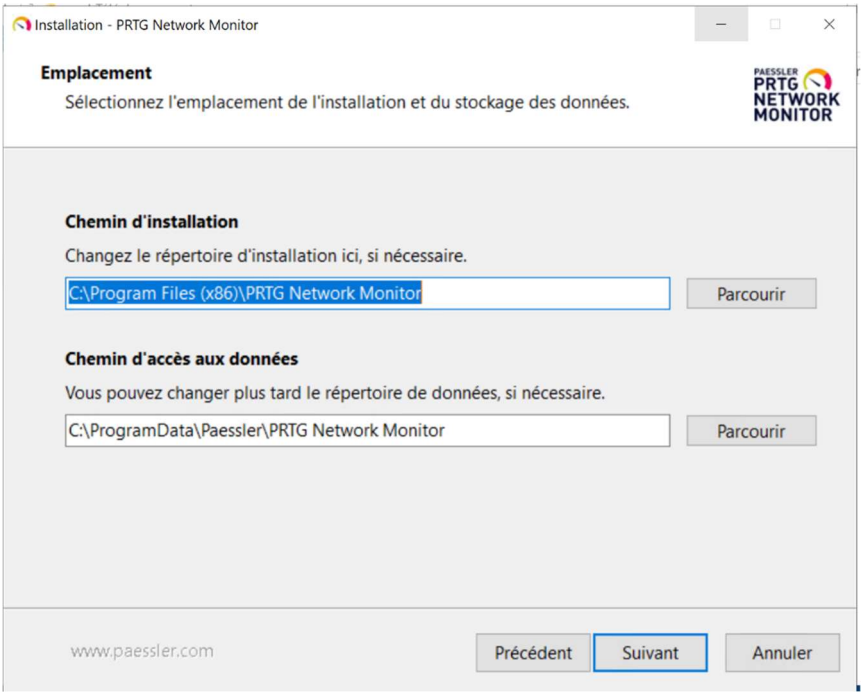
Ensuite, il faut indiquer sur quelle adresse mail nous voulons recevoir les notifications et alertes importantes



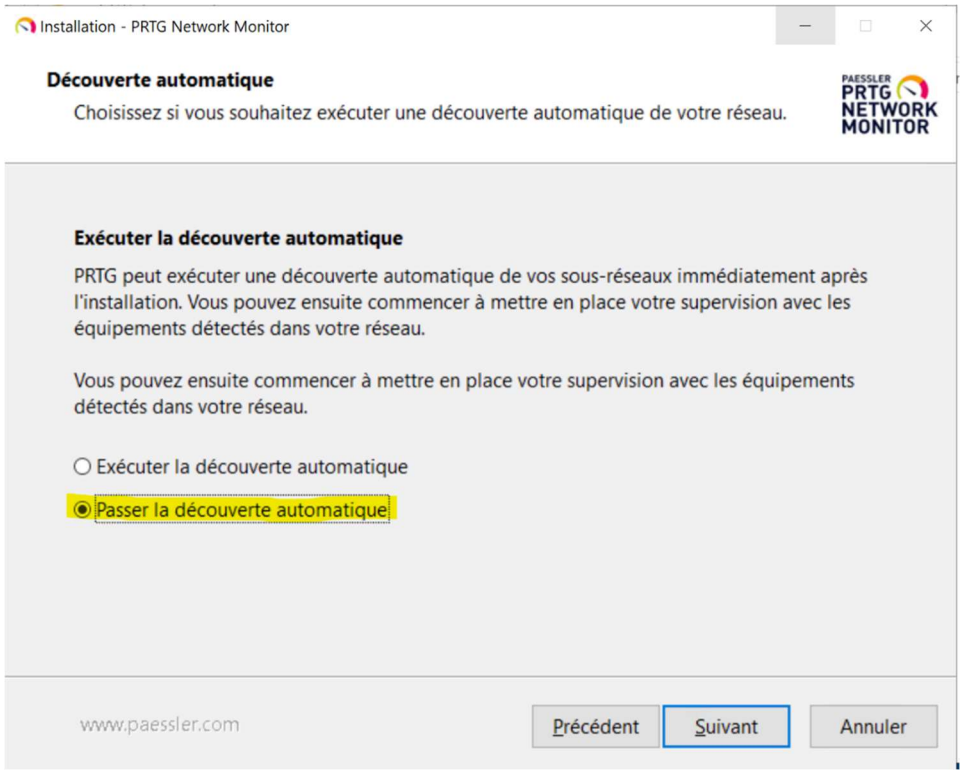
Dans mon cas, j'utilise l'installation personnalisée pour pouvoir configurer comme je le souhaite mes préférences d'installation



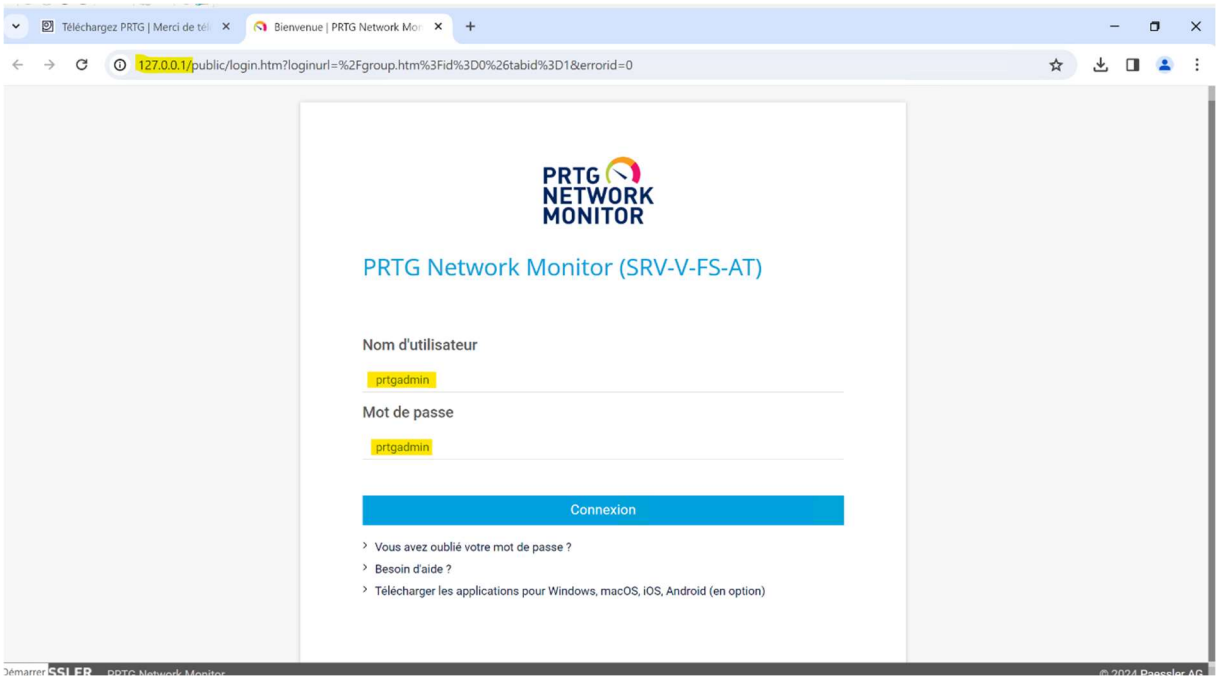
Il faudra maintenant indiquer dans quel répertoire nous voulons installer PRTG (les chemins par défaut sont très bien si aucun besoins particulier)



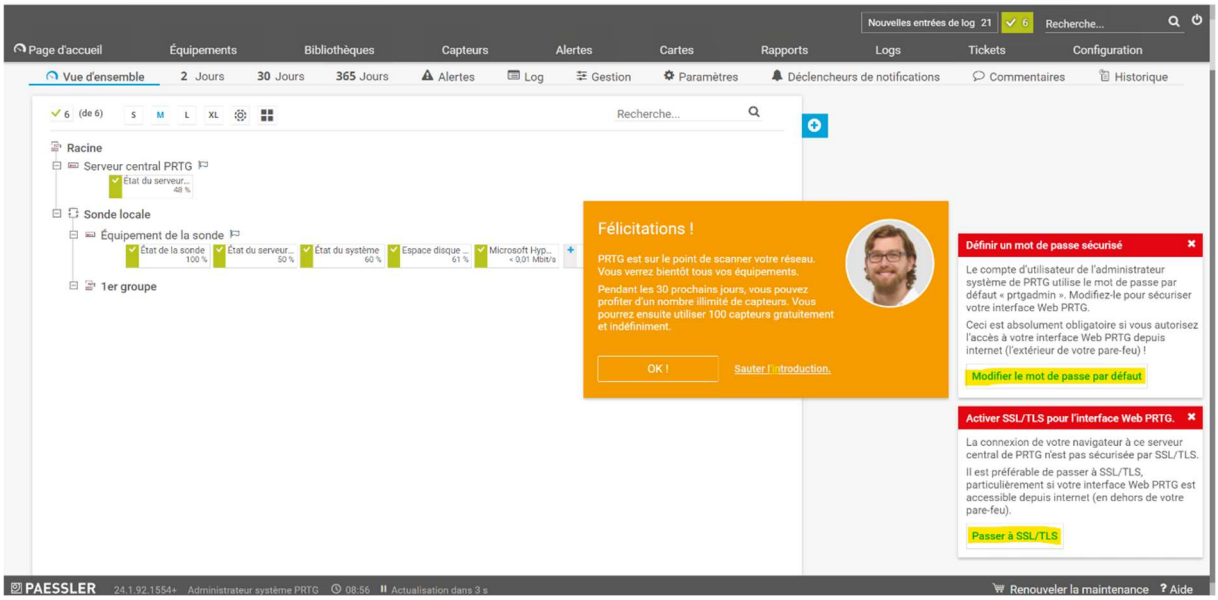
Il faut ensuite choisir si nous voulons une découverte automatique de nos équipements sur notre réseau. Étant sur la version d'essai et n'ayant que 100 capteurs, c'est déconseillé. Nous ajouterons nos capteurs manuellement



L'installation se lance ensuite et à la fin de cette dernière, un navigateur se lance directement sur la page de gestion de PRTG (le nom d'utilisateur et le mot de passe sont : prtgadmin – prtgadmin par défaut. À modifier impérativement)

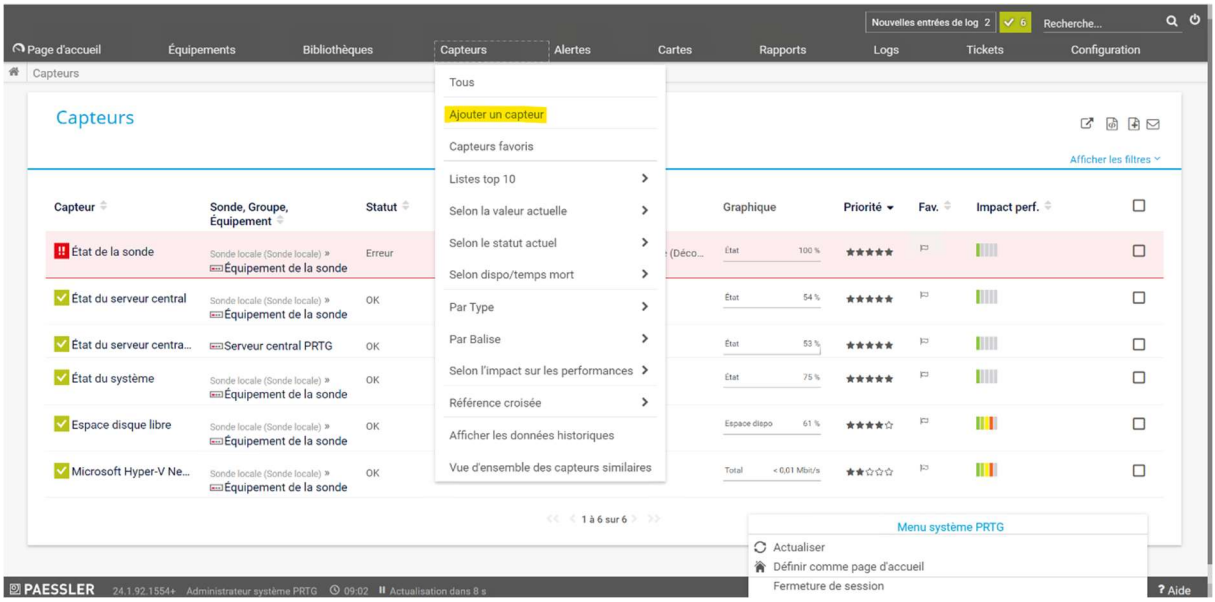


Nous arrivons sur la page d'accueil de PRTG. Par défaut, nous aurons déjà une sondé locale installé, celle de notre serveur central (ou est installé PRTG)

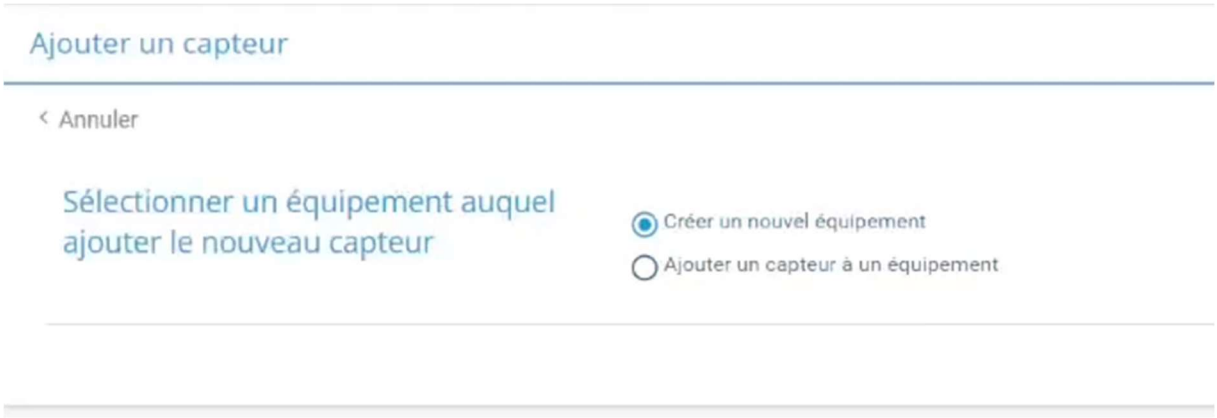


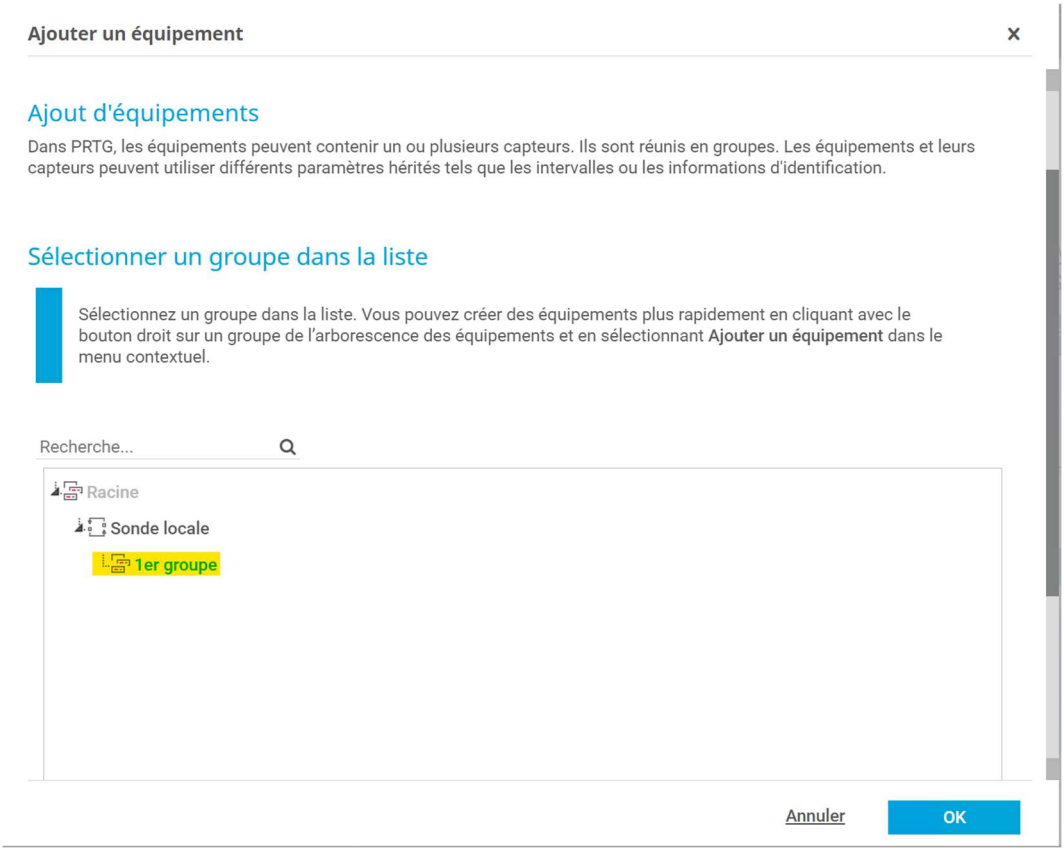
Il faudra dans un premier temps modifier le mot de passe administrateur de PRTG, et activer SSL pour la connexion à PRTG (pour que les échanges entre les différents clients et le serveur PRTG soit chiffrer)

Cela fait, il faudra maintenant ajouter un nouveau capteur. Cliquez en haut de la page sur « capteur », et sur « ajouter un capteur ».

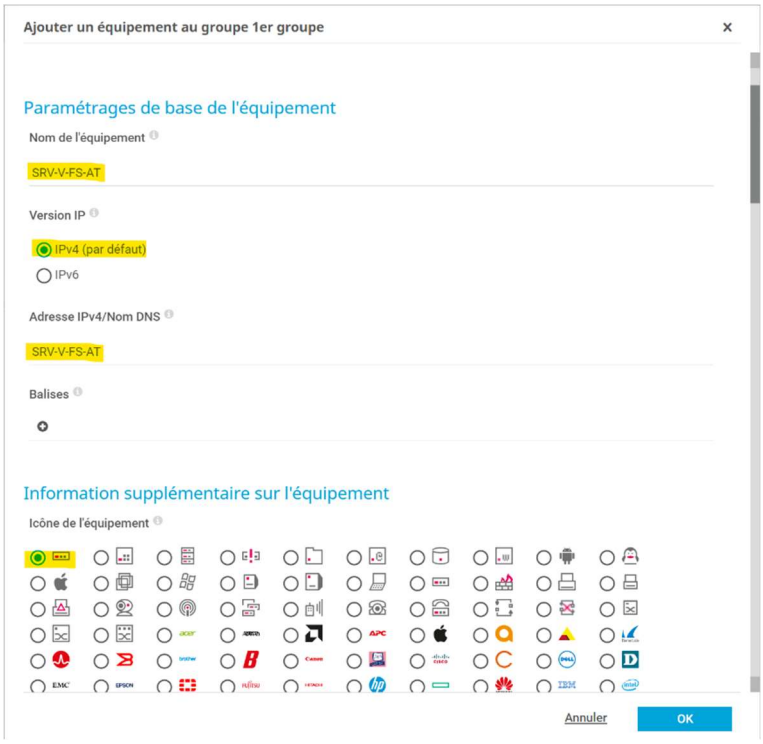


On va maintenant nous demander si l'équipement existe déjà. Etant donné que c'est une nouvelle installation, il faudra cliquer sur « créer un nouvel équipement » pour créer le nouvel équipement que l'on veut surveiller

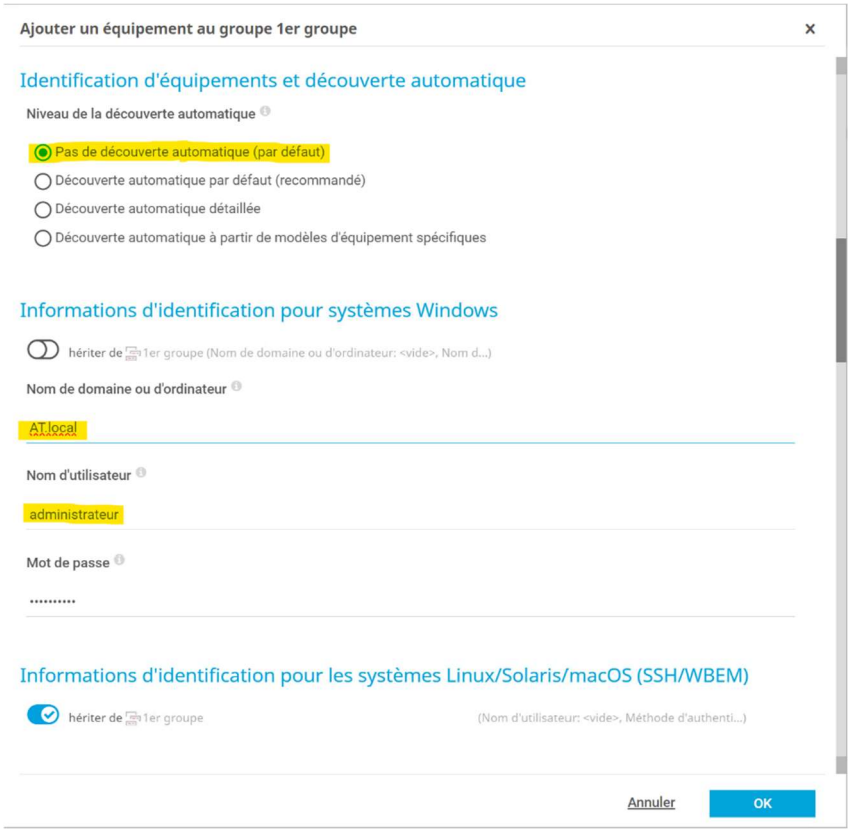




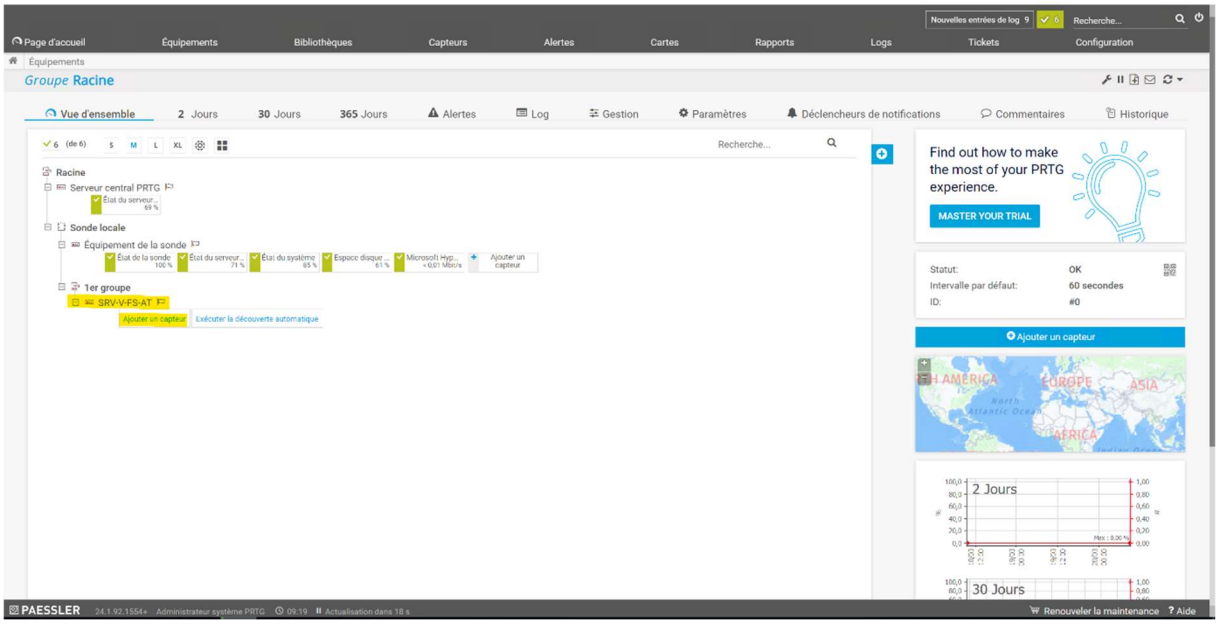
Cela fait, il faudra configurer notre nouvel équipement en lui mettant un nom, en indiquant son adresse IP (si elle n'est pas fixe, nous pouvons le configurer avec son nom DNS) et lui choisir une icône pour mieux le retrouver.



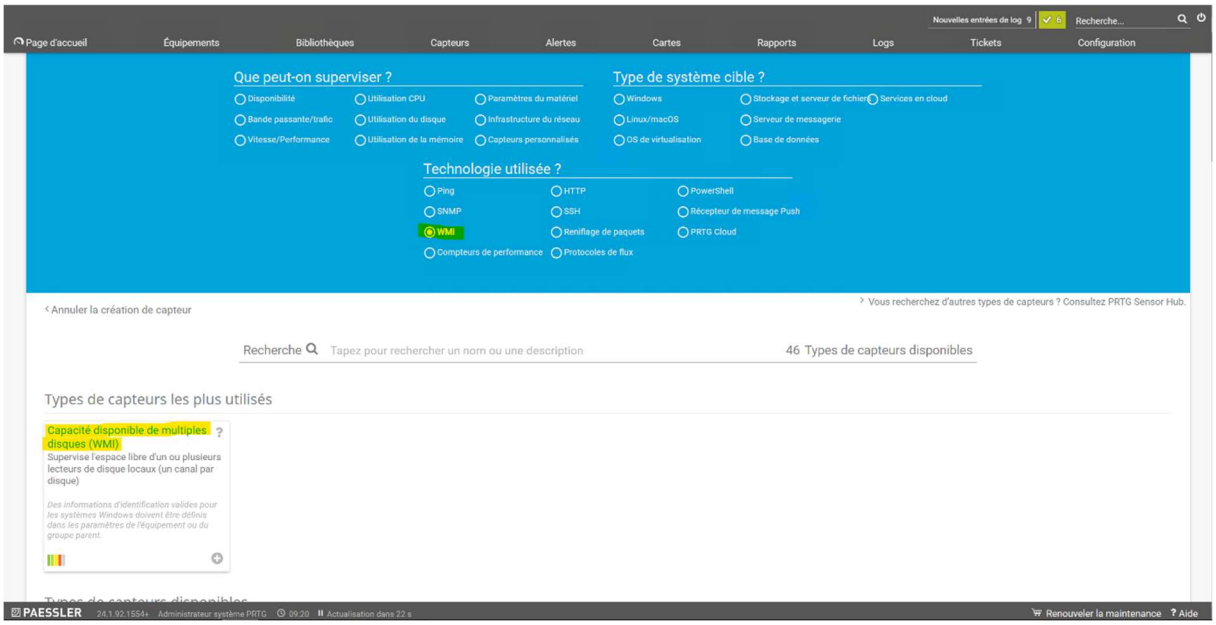
Nous laissons toujours la découverte automatique désactivée car nous sommes sur la version gratuite et n'avons que 100 capteurs disponibles. Cela évite d'avoir des capteurs non voulus. Nous allons également devoir nous authentifier étant donné que nous travaillons sur un système Windows.



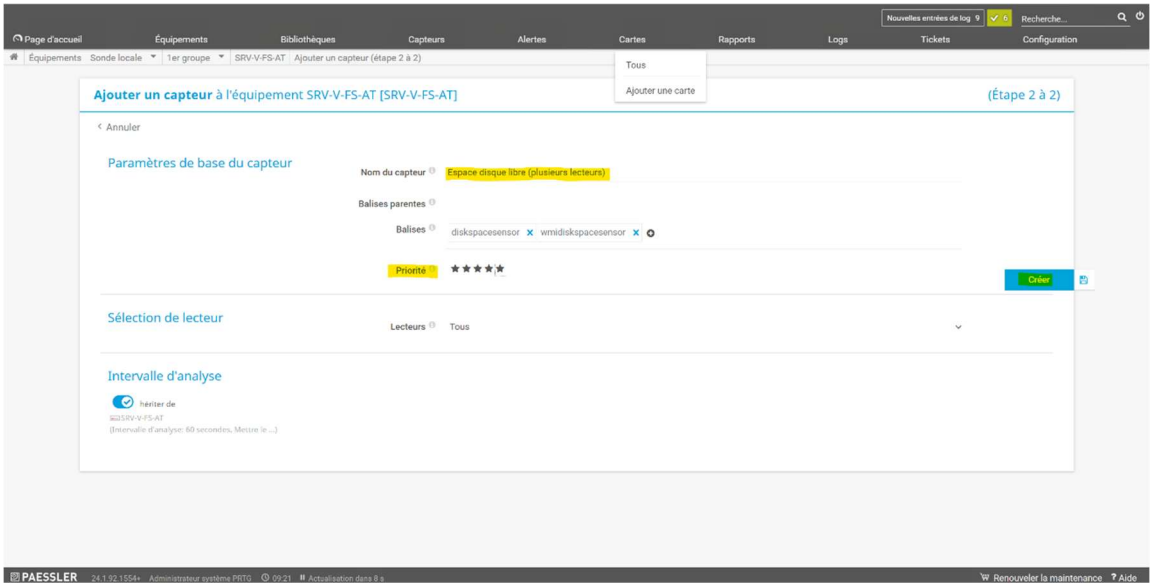
Nous voyons apparaître notre serveur sur la page de PRTG, et en cliquant sur ajouter un capteur, nous allons pouvoir choisir dans la liste le protocole WMI (ayant ajouté un serveur Windows à surveiller)



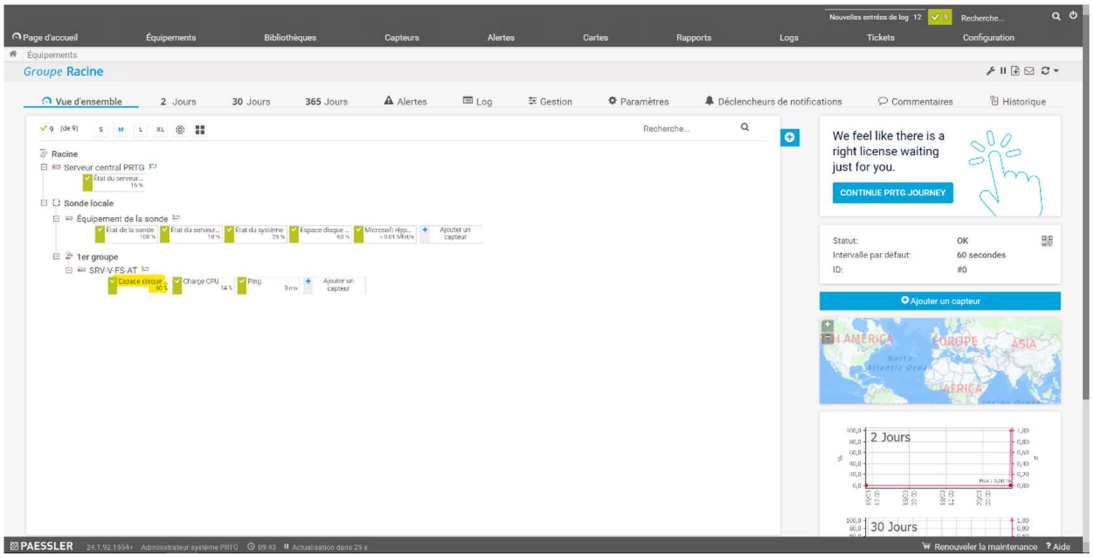
Nous sélectionnons également quel capteur nous voulons installer

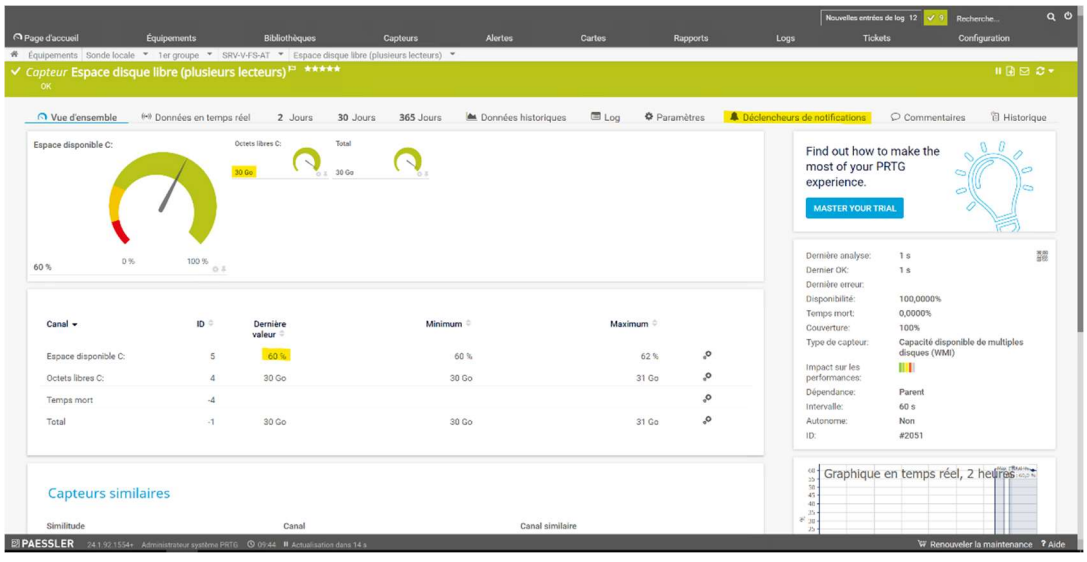


Nous pouvons laisser le paramétrage par défaut qui convient parfaitement et cliquer sur créer

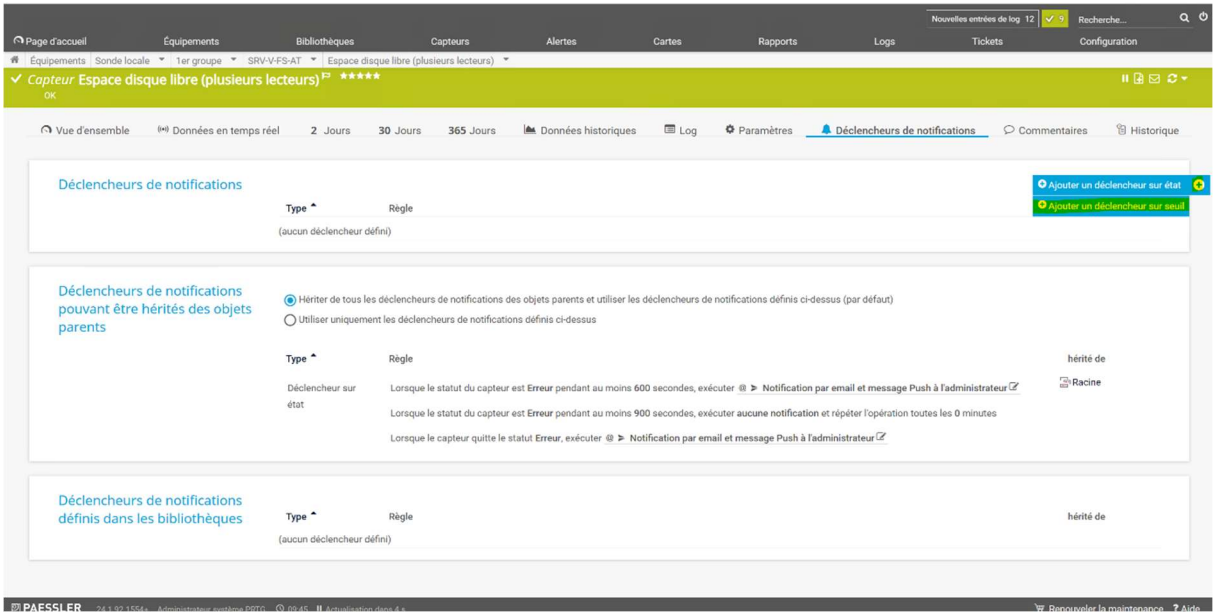


Nous pouvons maintenant vérifier l'espace disque en cliquant sur le capteur que nous venons de créer dans notre liste.

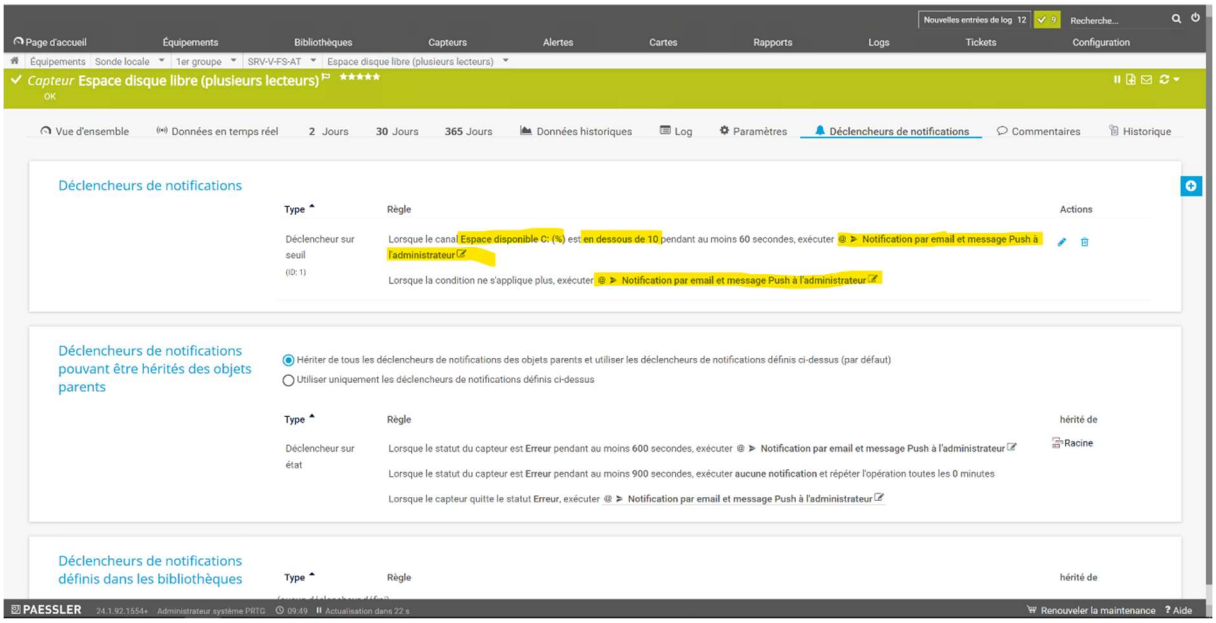




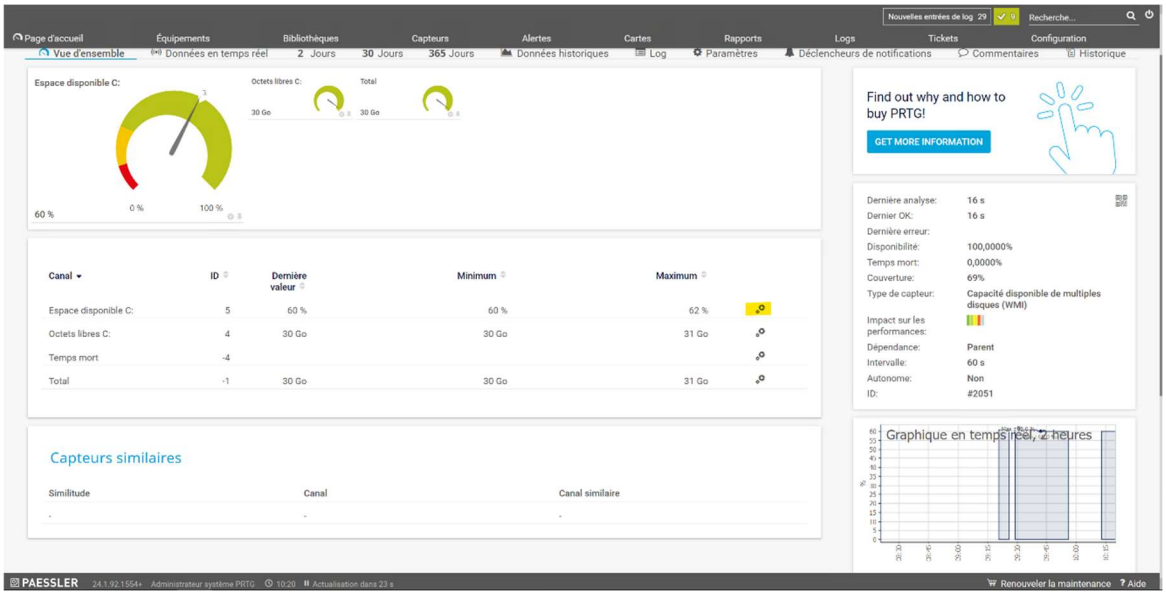
Nous allons pouvoir également mettre en place un déclencheur de notifications, pour éviter de devoir surveiller en temps réel tous nos capteurs. L'idée étant d'être prévenu en amont si nous avons un souci sur une de nos machines.
Dans notre cas, nous allons installer un déclencheur sur seuil (nous avons aussi la possibilité d'en activer un sur état). Il faudra cliquer sur « ajouter un déclencheur sur seuil » à droite de cette même page.

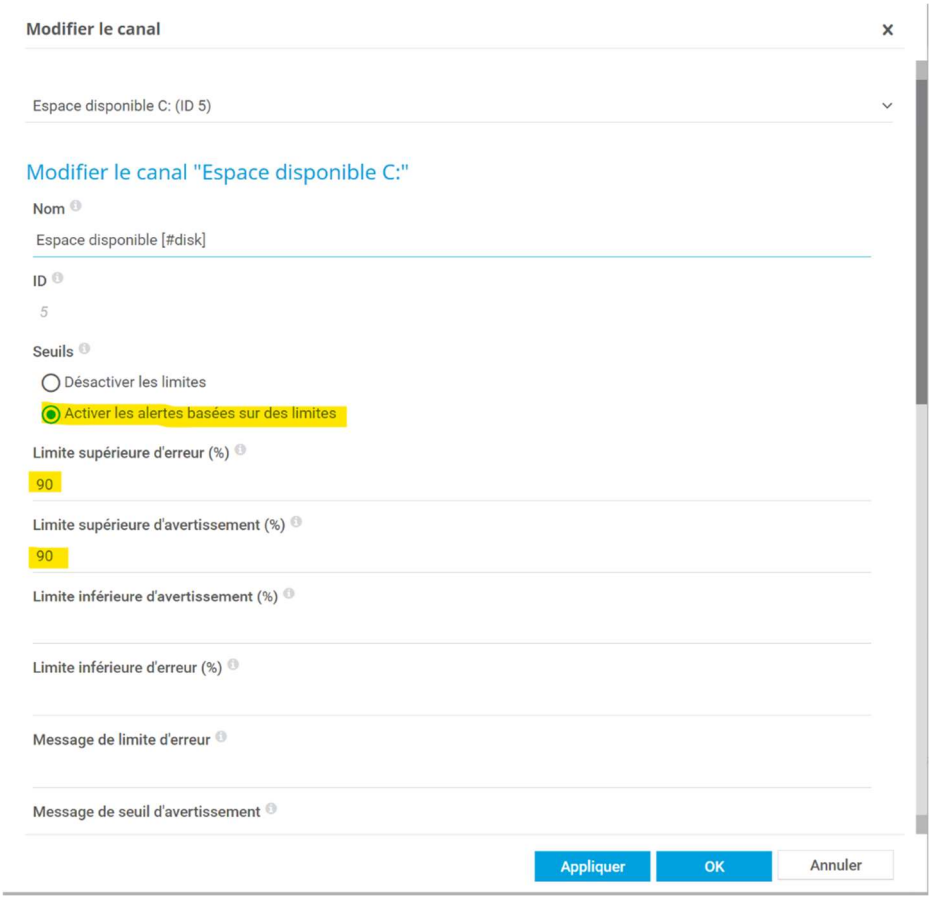


Nous avons la possibilité de choisir le cas où le déclencheur de notifications s'active. Dans mon cas, étant en labo de test, j'ai choisi de déclencher une notification lorsque le canal espace disponible en % est en dessous de 10% (car 10% d'espace libre est un seuil important à ne pas dépasser sur un serveur Windows) par e-mail et notification push.
Nous pouvons ensuite choisir d'envoyer une notification lorsque le problème est résolu

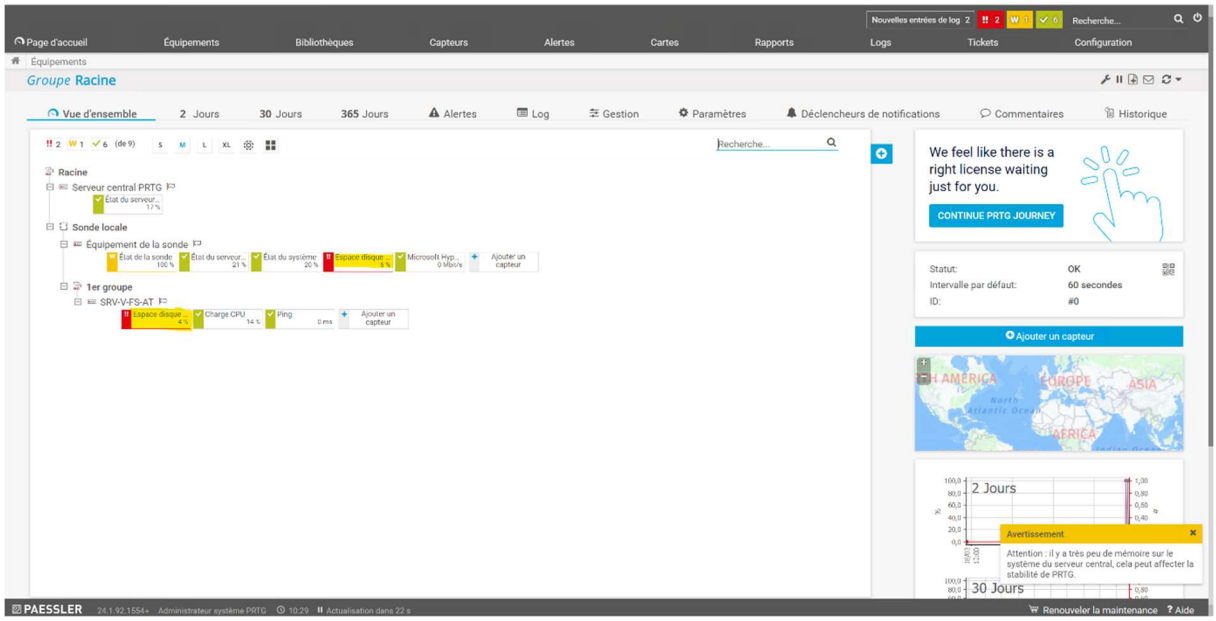


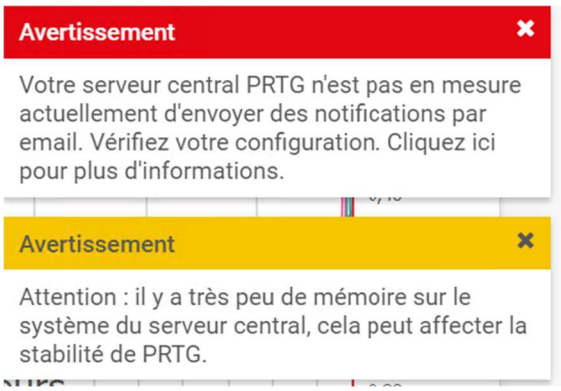
Pour que cela crée une erreur et que mon capteur s'affiche en rouge sur la page d'accueil de PRTG, je peux également indiquer à partir de quelle limite PRTG me remonte une erreur. Il faudra cliquer sur le capteur désiré, et cliquer sur la petite roue crantée à droite du point que l'on veut surveiller. Nous pouvons ensuite choisir les limites voulues

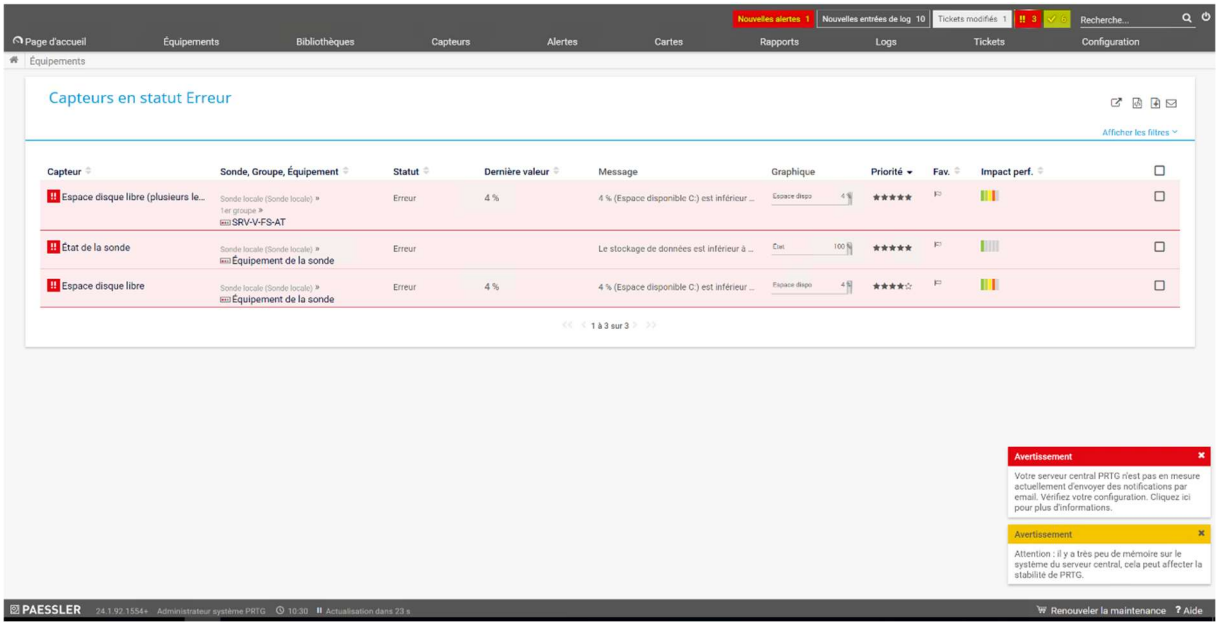




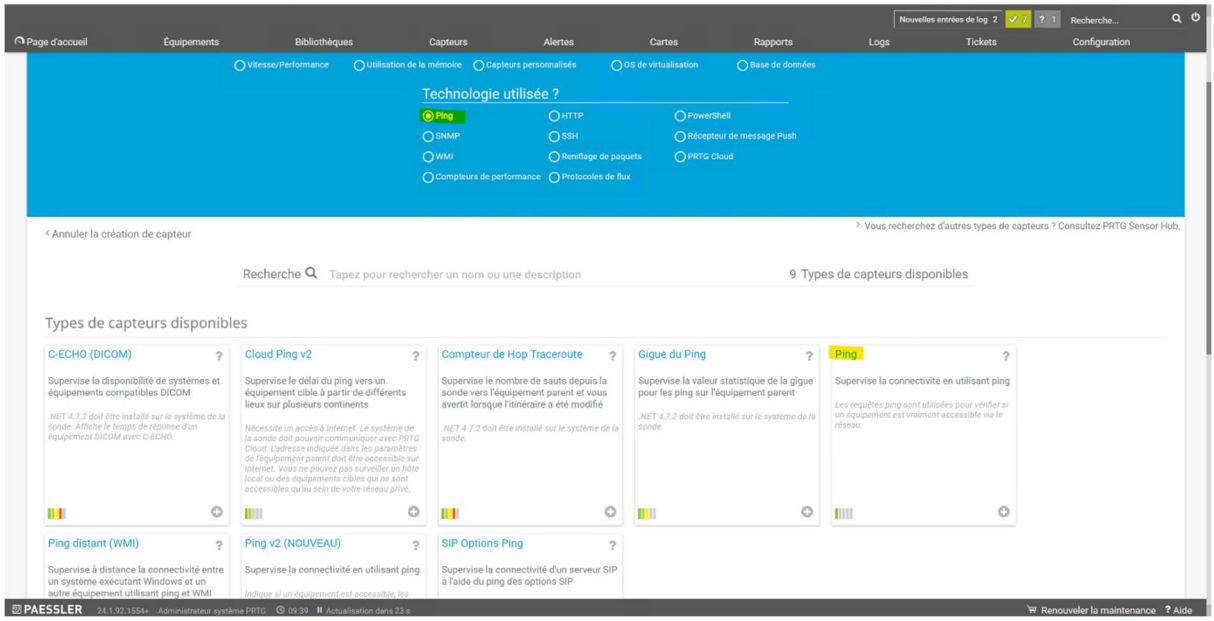
Dans mon cas, j'ai fait en sorte de créer une erreur en réduisant la partition C : de mon serveur Active Directory pour vérifier que l'erreur remonte correctement et que je reçois donc bien les alertes créer précédemment (mon serveur central PRTG étant également mon serveur Active Directory, l'alerte s'active sur les deux équipements)



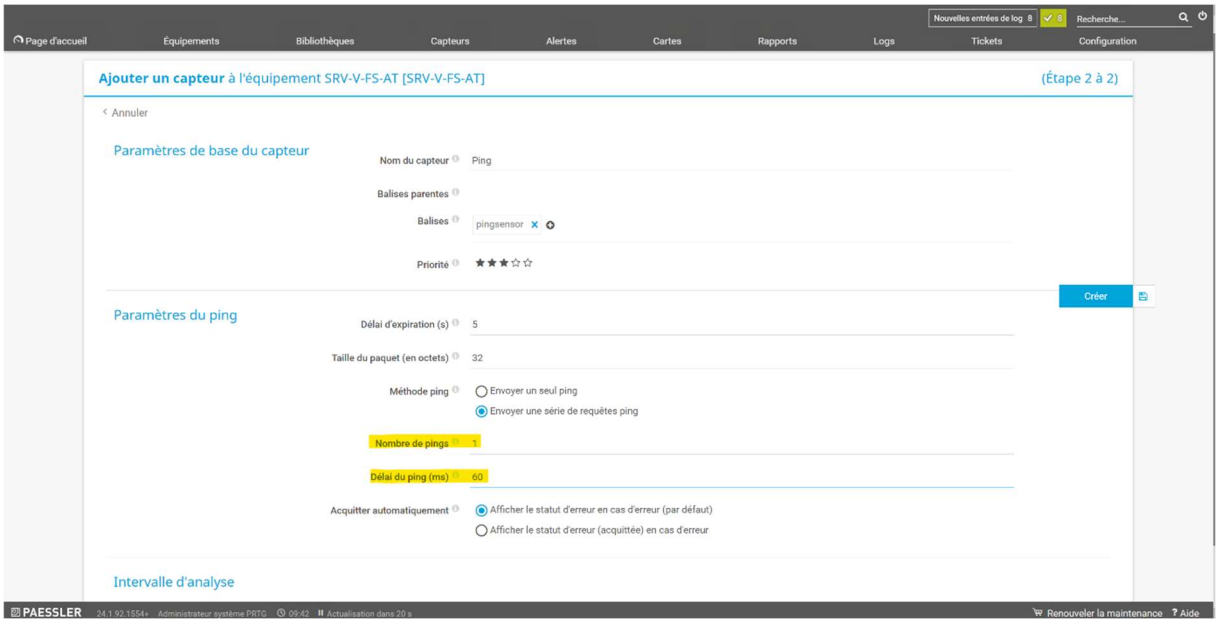




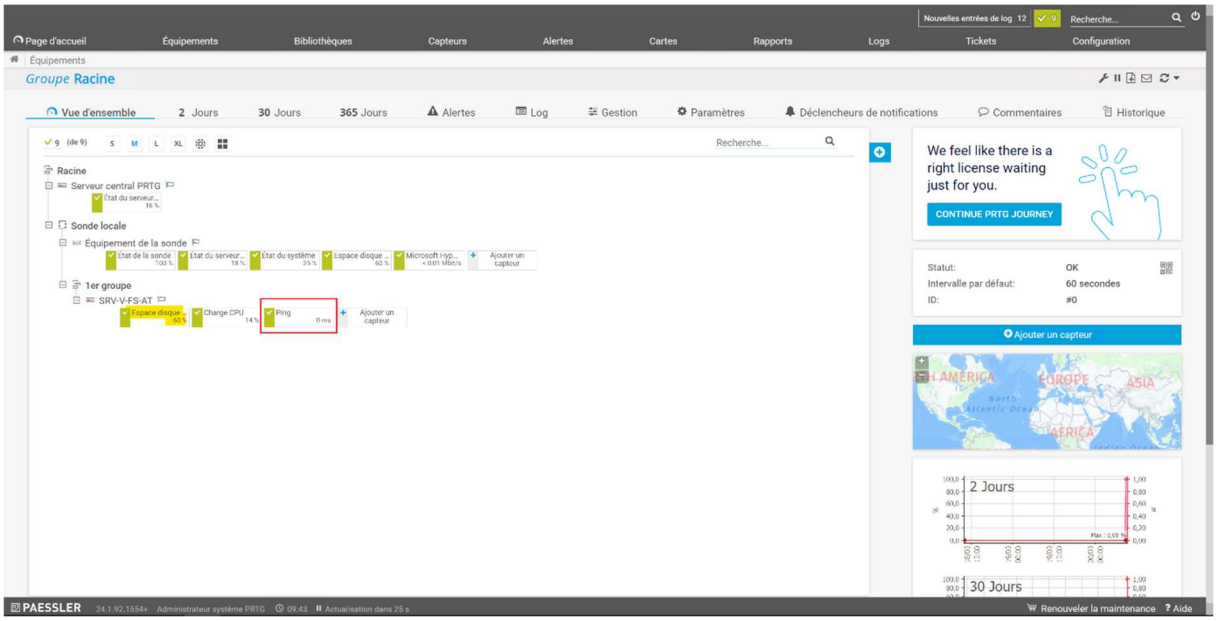
Je vais maintenant créer une sonde ICMP (ou Ping) pour vérifier que mon serveur répond bien sur le réseau. Pour se faire, il faut ajouter un nouveau capteur sur l'équipement souhaité, et choisir « ping » dans technologie utilisé et choisir le capteur « ping » dans la liste.



Il faut maintenant régler la fréquence de ces dernières et lui mettre un nom



Et voilà, nous avons installé un capteur ping qui envoie une requête ICMP toutes les 60 secondes à notre serveur pour vérifier sa disponibilité sur le réseau. PRTG nous indique également le temps de réponse en ms.



3. Conclusion

Et voilà, nous avons procédé à l'installation du logiciel PRTG, avons configuré deux sondes sur notre serveur Active Directory (donc en WMI car je n'avais pas d'équipement SNMP disponible) et avons mis en place un déclencheur de notifications sur seuil qui nous prévient par mail dès lors que le seuil que nous avons défini est atteint/dépassé.

Il n'y a pas de problème particulier quant à cette installation, c'est un logiciel très simple d'utilisation, qui utilise des technologies avancées de surveillance et qui permet aux administrateurs de vérifier leurs équipements informatiques beaucoup plus simplement.

Points de vigilance et conseils de sécurité :

- Bien évidemment, comme pour tout rôle Windows, on essaie au maximum d'isoler et de créer des serveurs dédiés à chaque rôle que nous installons.

- Comme toujours depuis le début de nos TP, bien modifier le mot de passe administrateur de PRTG par un mot de passe fort et sécurisé qui respecte les normes.

- Pour des raisons de sécurité, on crée un utilisateur dédié à SNMP ou WMI pour la connexion d'un équipement avec PRTG. Cela est bien plus propre.

- Attention lors de l'installation de PRTG ou lors de l'ajout d'un nouvel équipement, de bien décocher la découverte automatique de sonde car nous n'avons que 100 capteurs disponibles en version gratuite.

- Bien activer SSL pour la connexion à PRTG pour que les échanges entre les différents clients et le serveur soient chiffrés.

- Lors de l'ajout d'un équipement, si le serveur que l'on paramètre n'est pas en IP fixe, il est possible de mettre son nom DNS sur le réseau au cas où il serait amené à changer d'IP.

- Lors de la mise en place du déclencheur de notification, ne pas oublier de préciser à PRTG une adresse mail et une configuration SMTP pour qu'il puisse nous envoyer des notifications lorsque le seuil du déclencheur de notification est atteint.

- L'idée du déclencheur de notification est d'être prévenu en amont d'un souci sur une de nos machines sans avoir à vérifier tous nos équipements un par un.