Guastamacchia Livio

TP PRTG :

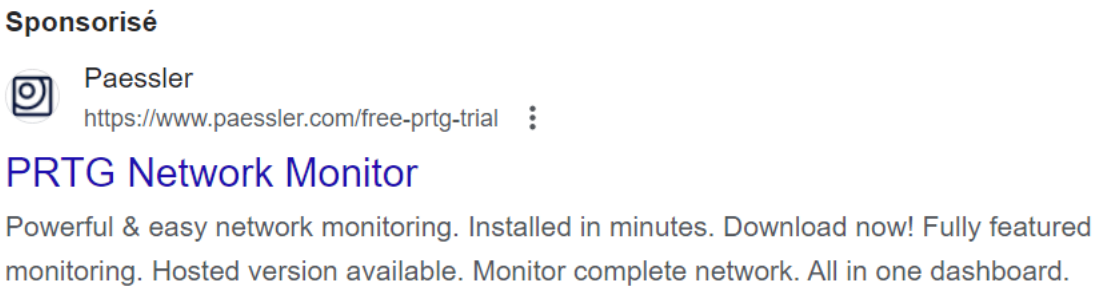
introduction :

Dans ce TP nous allons apprendre a superviser un Serveur Windows via le logiciel PRTG gratuit jusque 100 capteur. Cela nous permettras de vérifier en temps réel si l'ensemble du serveur fonctionne bien ou a une anomalie

---

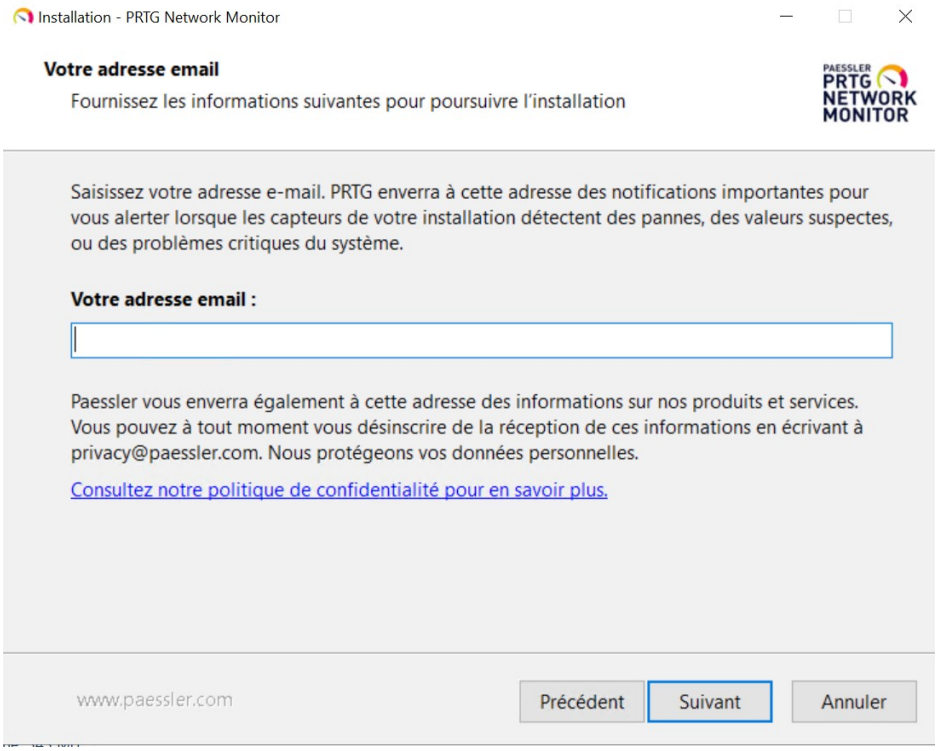
Pour commencer ce tp, il faudra installer le logicile PRTG

il faudra aller sur le site

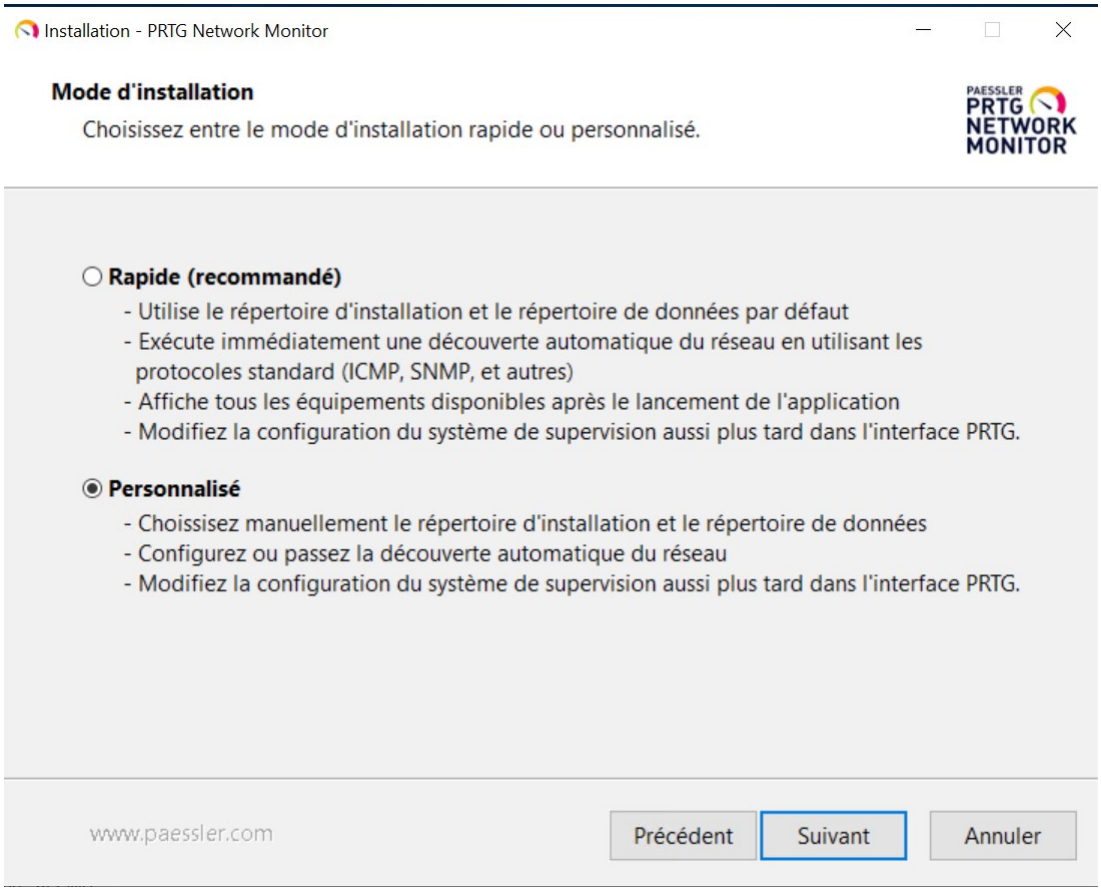


ensuite nous lançons l'installateur, choisissons la langue du logiciel et acceptons les termes de la licence.

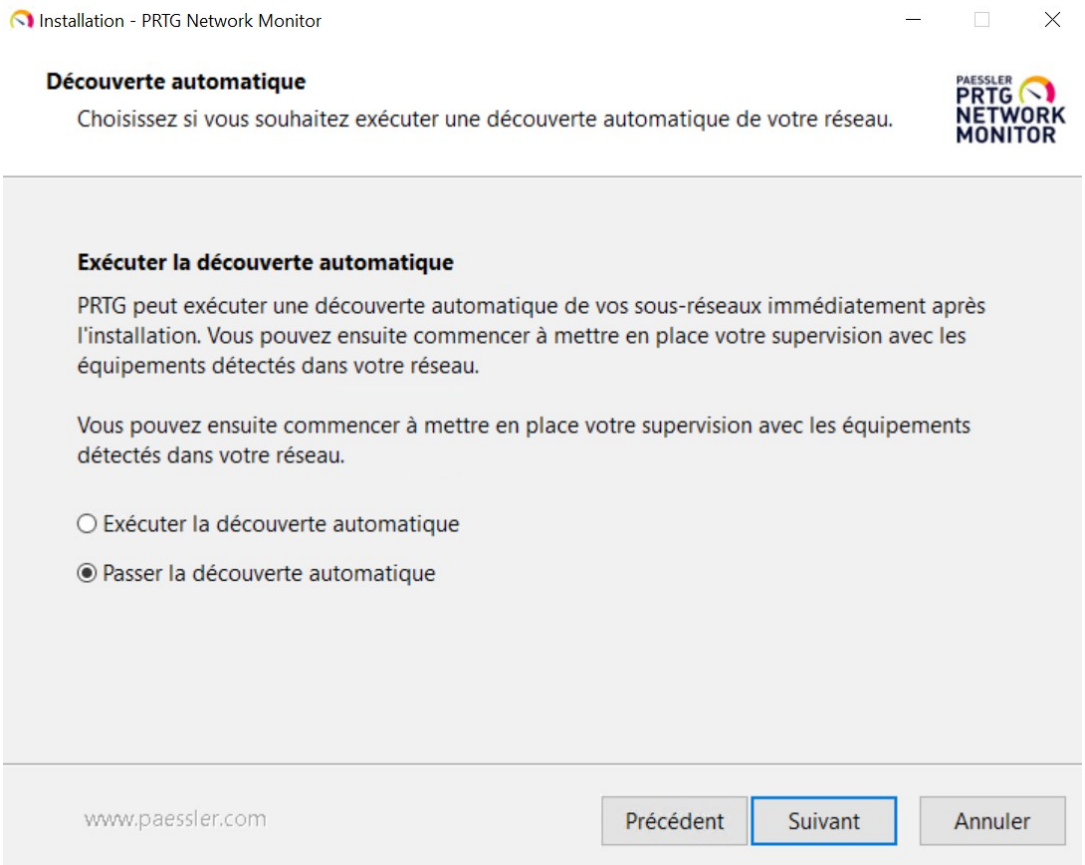
Nous devons maintenant renseigner une adresse mail qui nous permettras de récupérer les alertes lancer par PRTG



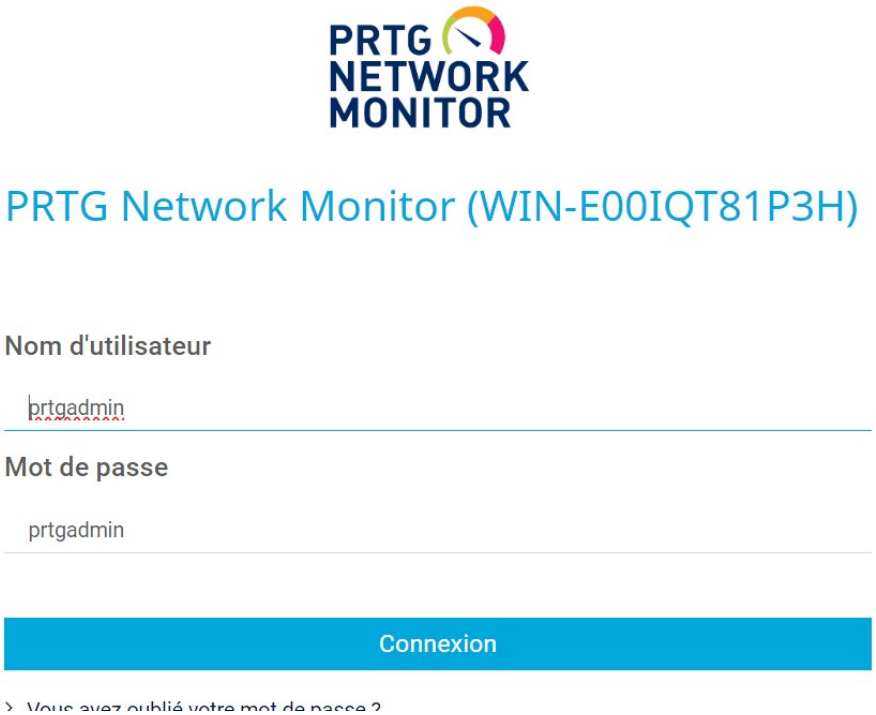
nous choisirons le mode d'installation personnalisé pour pouvoir effectuer nos propre modification



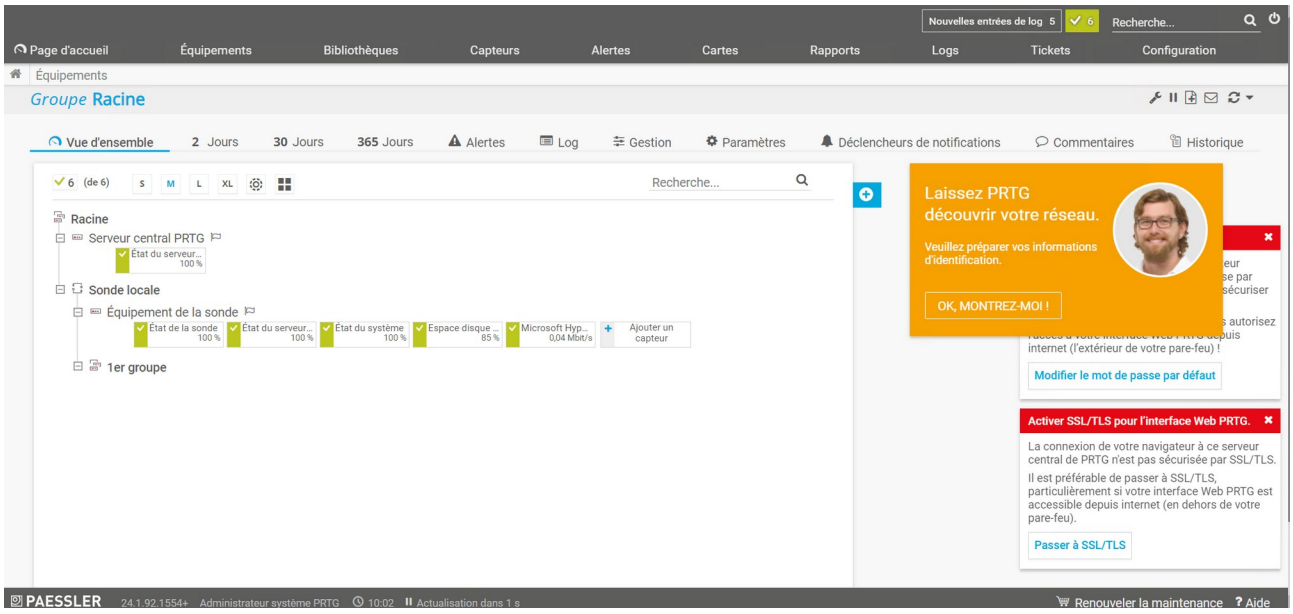
nous ne prendrons pas la découverte automatique car elle rajoute des capteurs pas spécialement utile sachant que nous sommes déjà limité en capteur avec la version gratuite



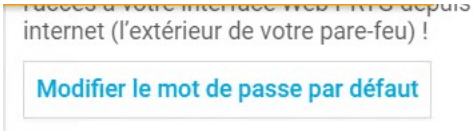
nous nous connectons



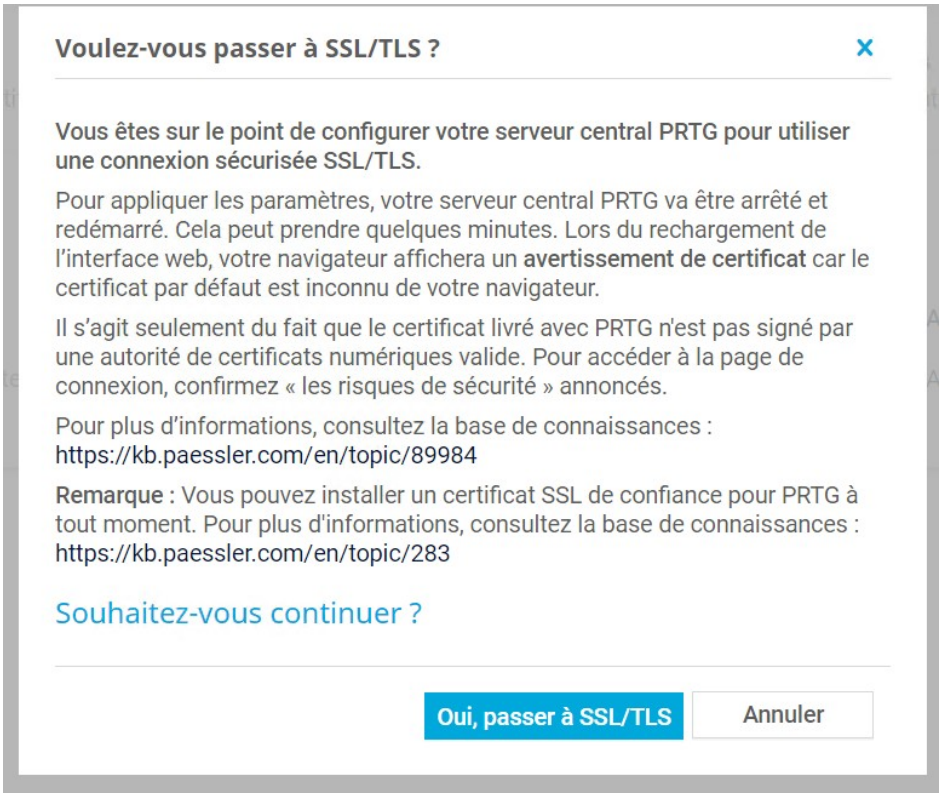
nous arrivons dans l'accueille de PRTG qui nous montre la sonde local qui analyse notre réseaux



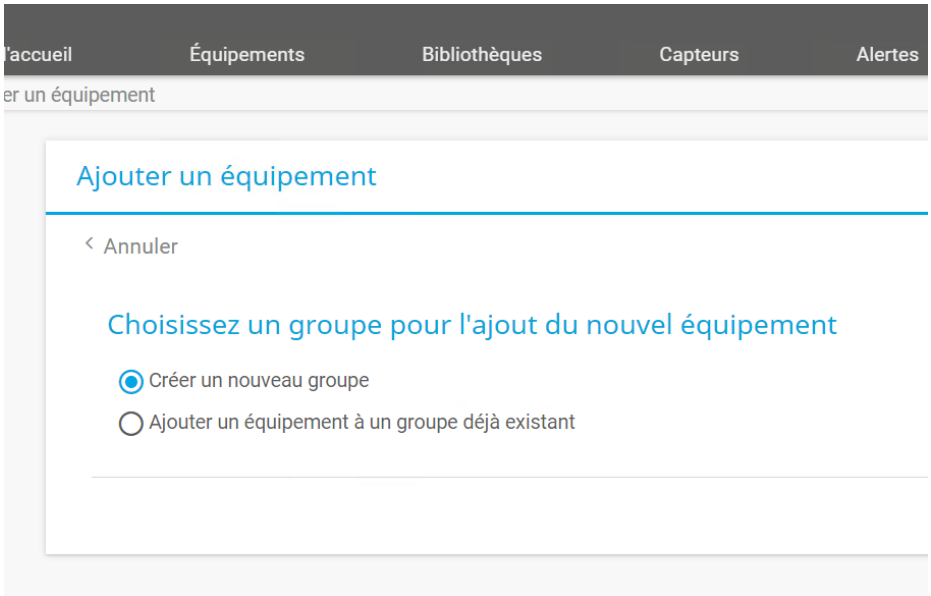
nous allons maintenant sécurise le serveur en modifiant le mdp (Azerty1234)



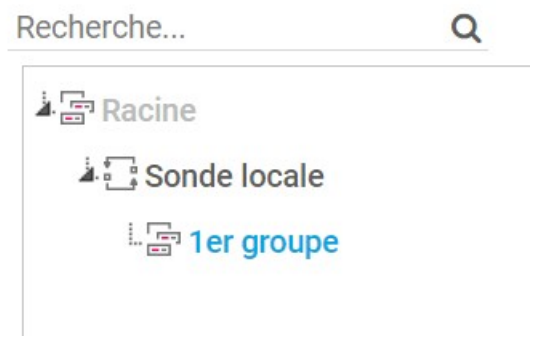
ensuite nous allons activer le SSL/TLS qui nous permettra de chiffre les connexion client et le serveur.



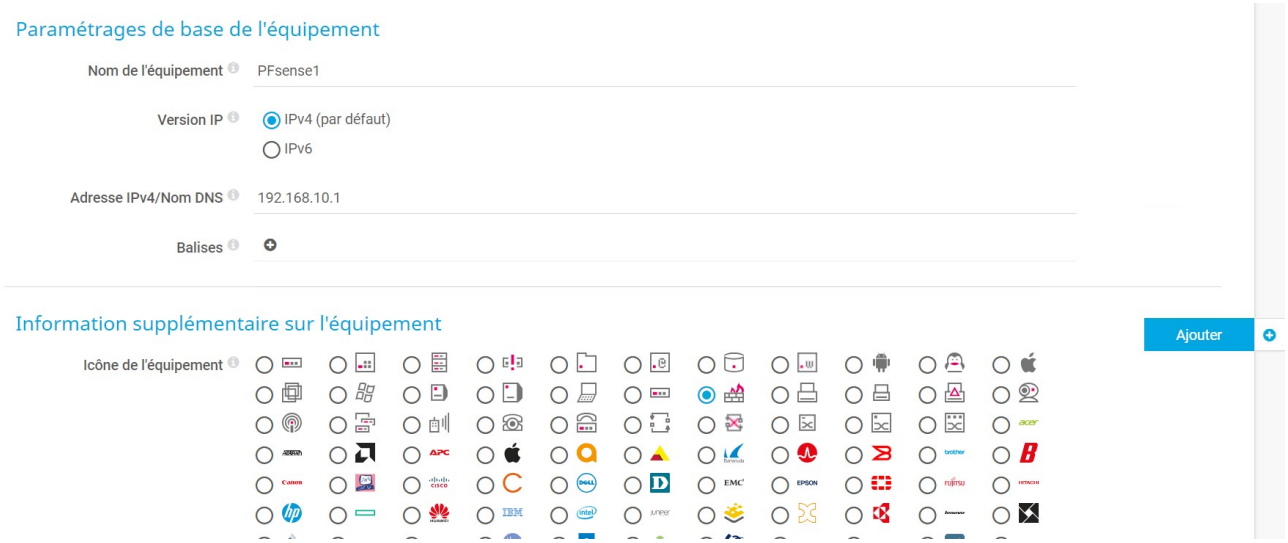
pour créer un nouveau capteur nous allons aller dans l'onglet « capteur » puis « ajouter un nouveau capteur »
nous sélectionnons « créer un nouvel équipement »



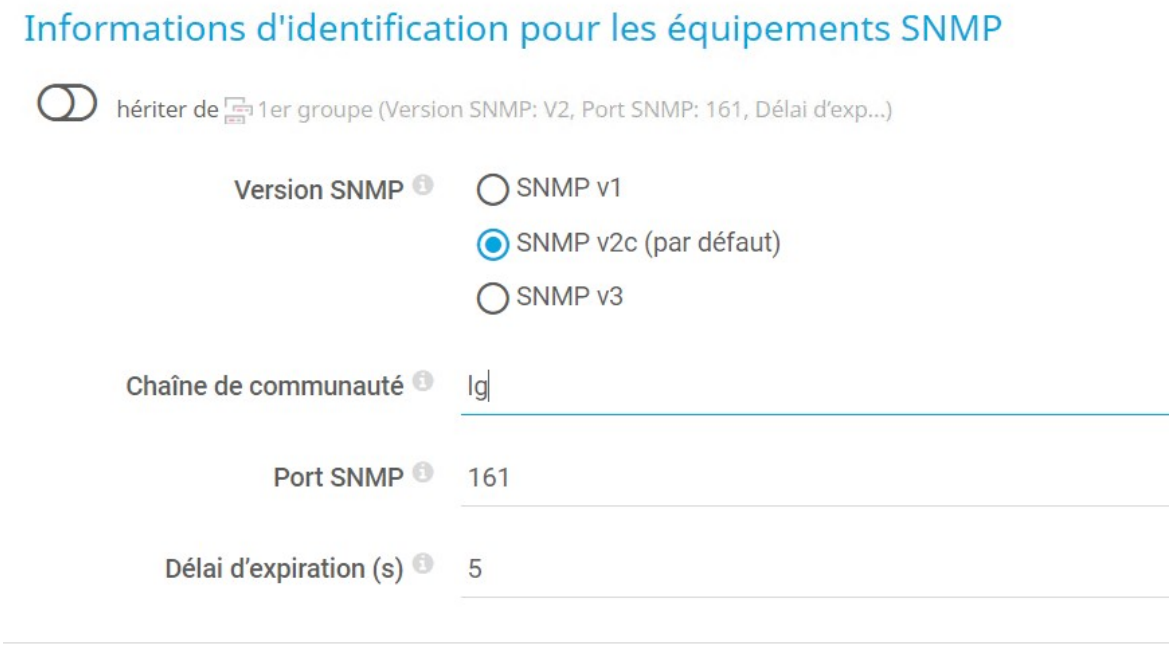
on le laisseras dans le groupe par défaut



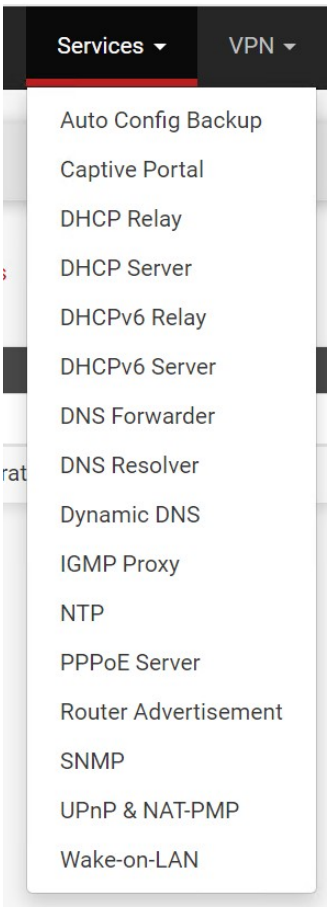
nous nommerons cet équipement « PFsense1 » et nous rentrerons l'adresse IP de notre Pfsense.



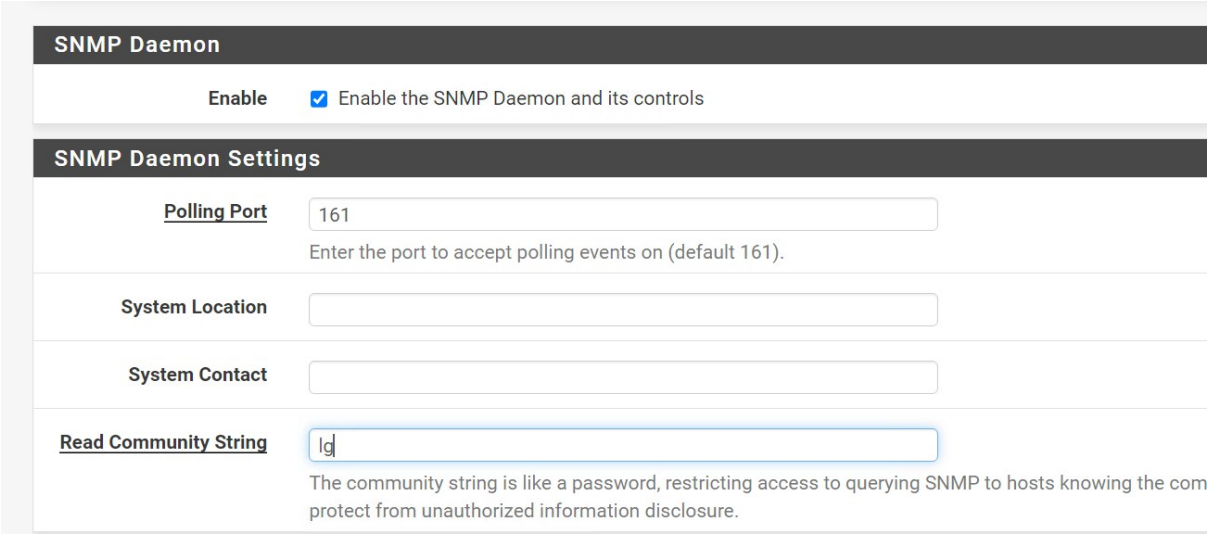
Nous allons fonctionner en protocole SNMP qui est le protocole de supervision. Nous sélectionnerons donc la version v2c de SNMP et changer le nom de communauté par lg qui apparaîtra dans le PRTG ainsi que le serveur.



Parallèlement nous allons lancer l'interface web de notre pfsense et lancer le menu SNMP se trouvant dans l'onglet « service »



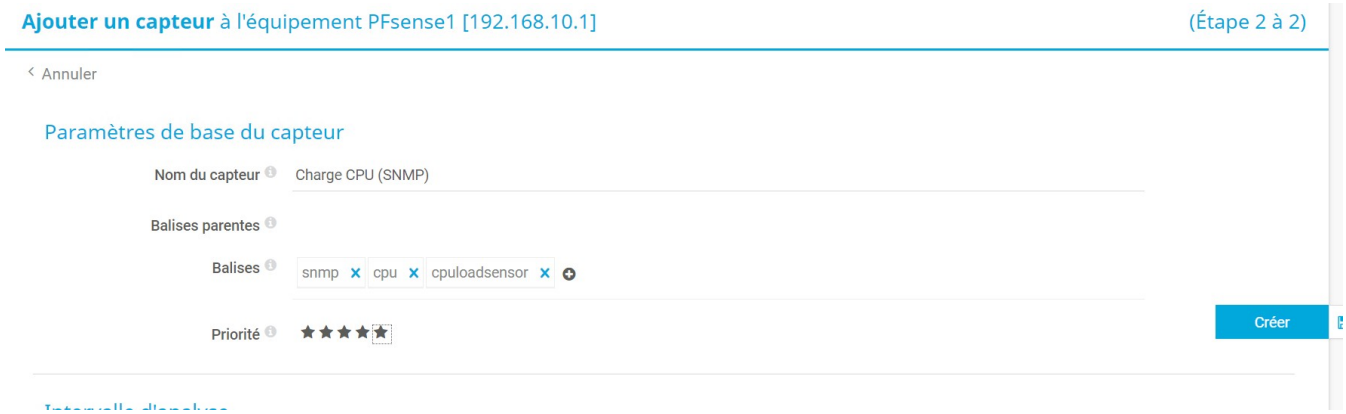
nous activerons le SNMP daemon et nous rentrons le nom de communauté que l'on a rentrer sur PRTG



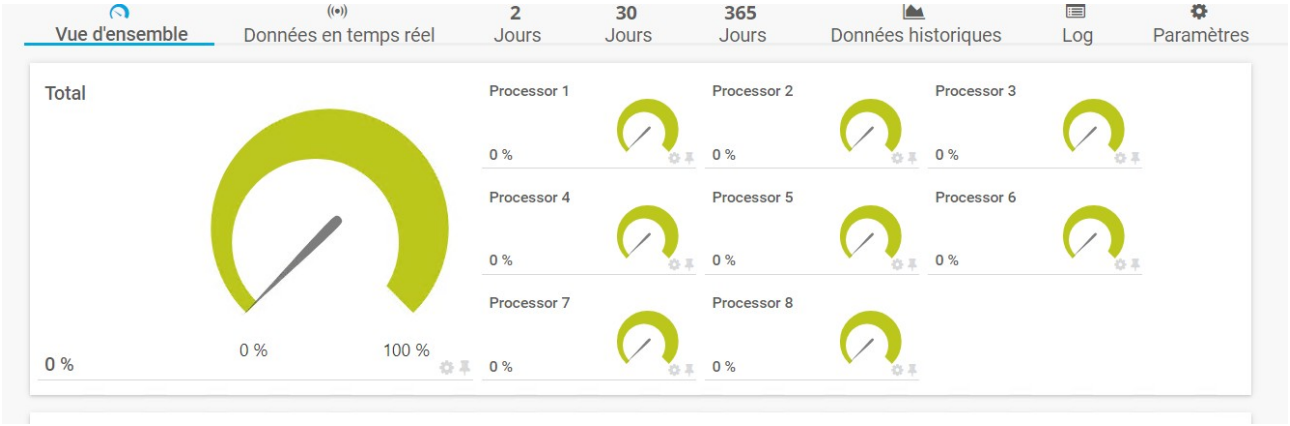
notre équipement a bien été créer nous allons maintenant lui ajouter un capteur précis

nous choisissons la technologie SNMP

nous choisirons par exemple la charge cpu comme capteur et nous lui mettrons la priorité maximal pour qu'il soit afficher en haut

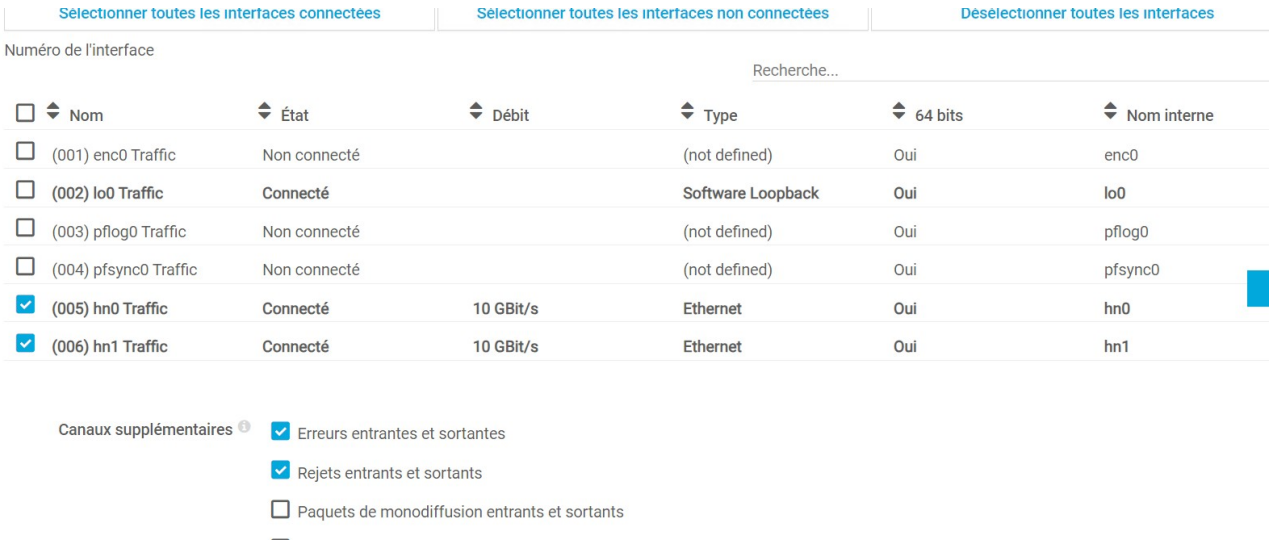


après avoir créer une règle de parefeu pour le protocole SNMP nous voyons bien que le capteur fonctionne

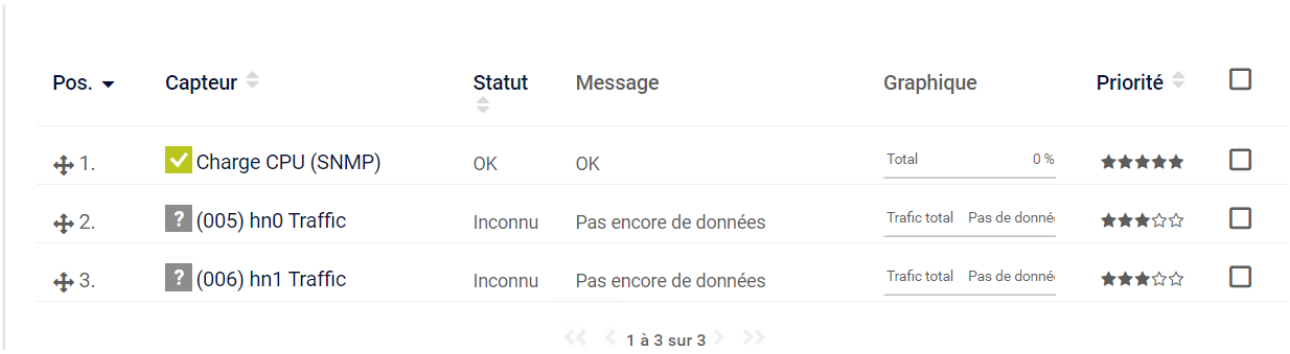


ensuite nous allons voir le trafic SNMP pour cela nous ajoutons un capteur et cherchons SNMP, nous voyons que le trafic SNMP est proposer

nous rajoutons « hn0 » notre carte LAN et « hn1 » notre carte wan, nous allons demander à ce que l'on voit les erreurs et rejets entrant et sortant

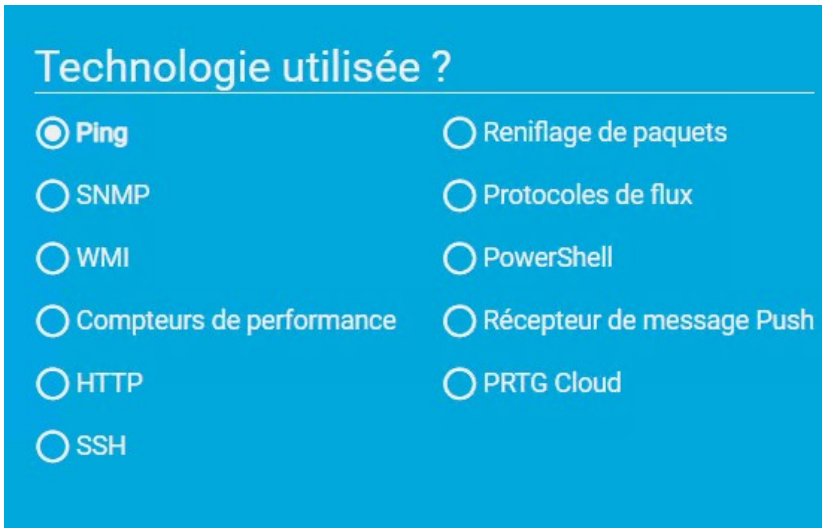


nous voyons que nos capteur ont été ajouté

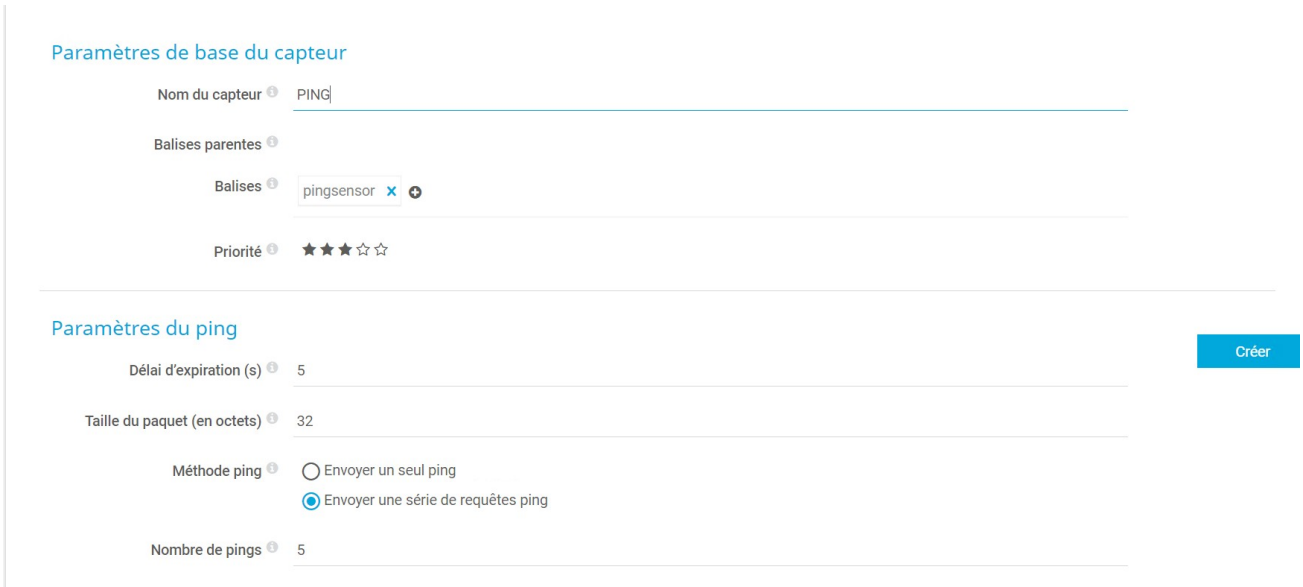


maintenant nous allons ajouter un capteur de ping qui nous permettra de voir si le serveur répond

on va choisir la technologie de ping et on sélectionne ping



nous pouvons changer le nombre de ping et le délais de ping mais cela reste à changer selon le besoin de chacun pour notre cas on le laisseras de base

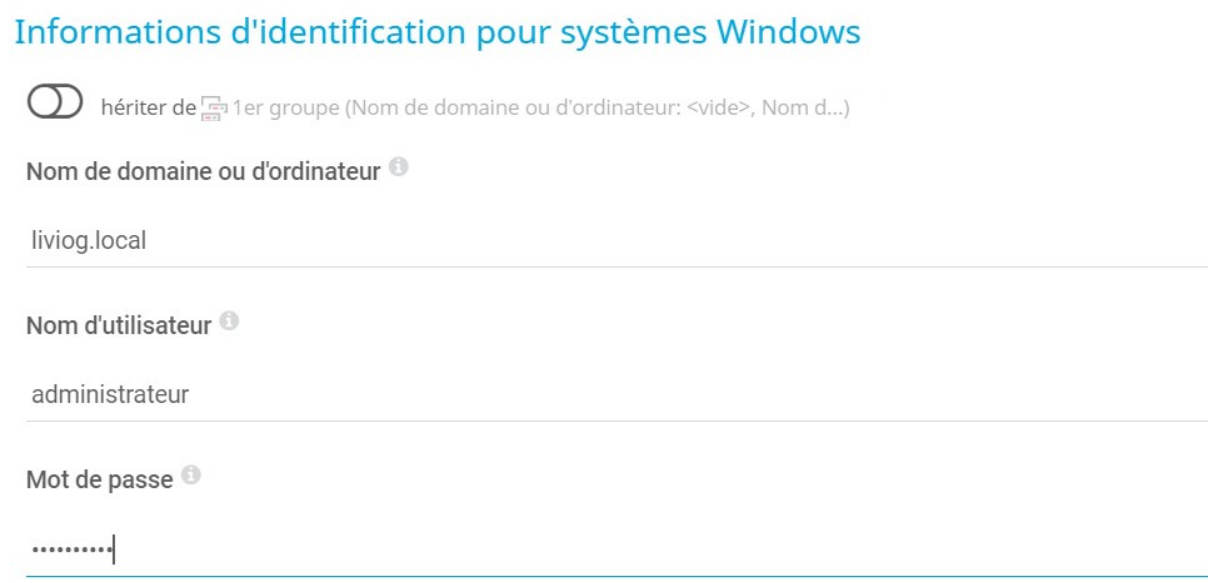


capteur wmi :

nous allons a nouveau créer un nouvelle équipement qui seras notre serveur ad

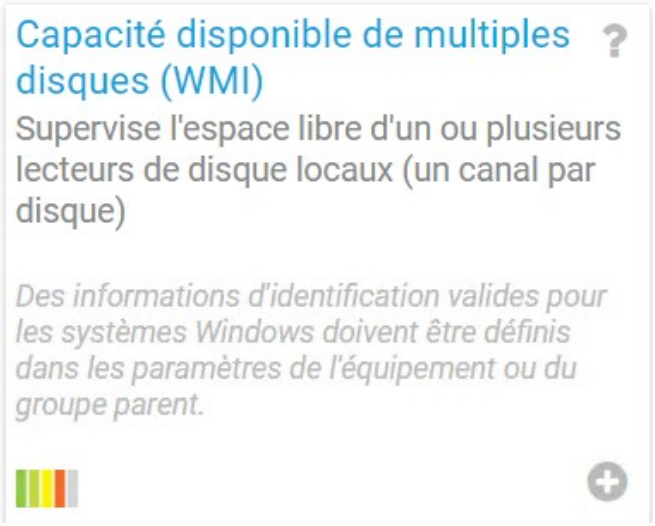
on lui donne un nom et donne le nom de notre serveur

nous nous identifierons pour le cas de windows

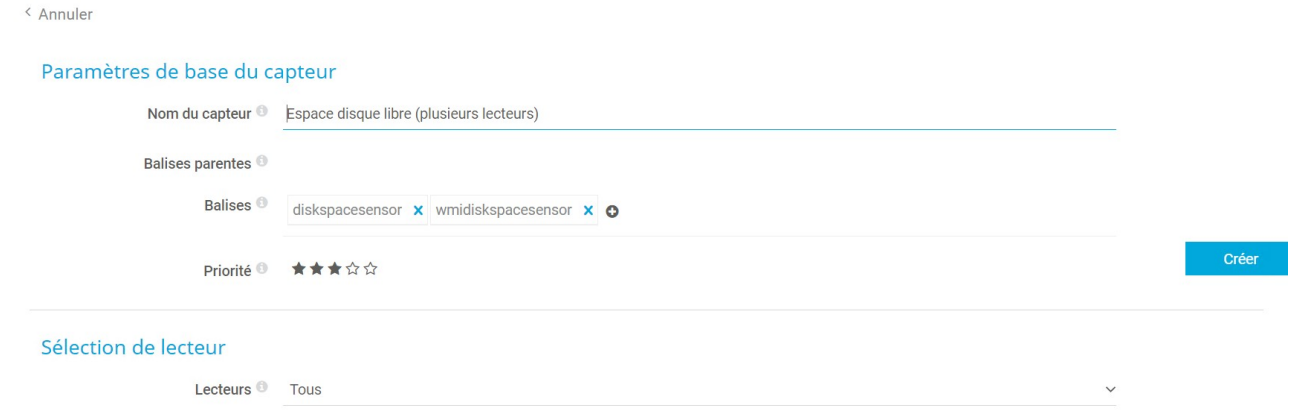


notre équipement est maintenant créer nous allons passer a l'ajout du capteur wmi

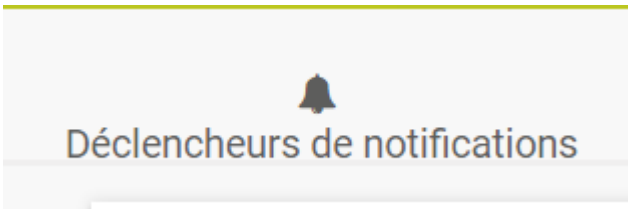
pour cela nous sélectionnons le protocole wmi puis l'important sur les serveur est de vérifier l'espace disponible des disques donc nous sélectionnerons le capteur de « capacité disponible de multiple disques »



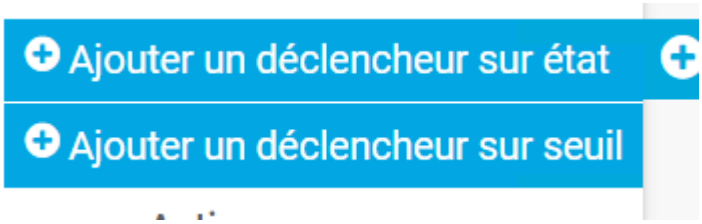
nous pouvons garder le paramétrage par défaut



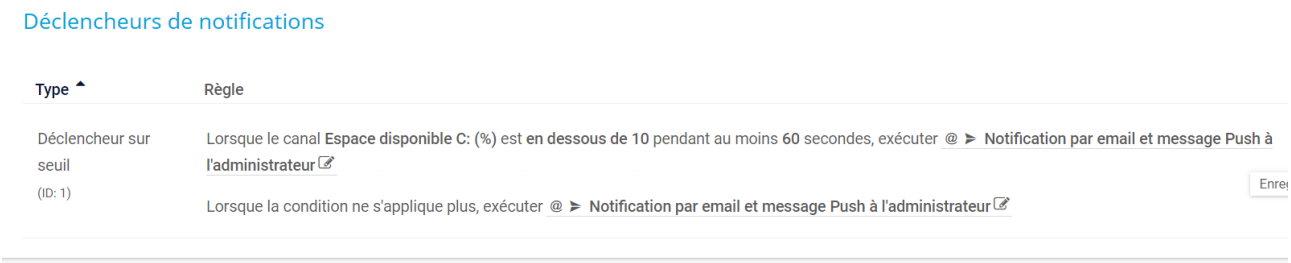
nous pouvons activer un déclencheur qui nous donnera des notifications



nous ajouterons un déclencheur sur seuil



nous rentrons que l'on souhaite une notifications a l'administrateur lorsque le serveur est en dessous de 10 % d'espace de stockage libre et nous souhaitons une deuxième notification lorsque le problème est réglé



conclusion :

TP relativement facile à reproduire sauf pour la réplication ad que je n'ai pas réussis à faire car il ne trouvait pas mon serveur automatiquement