

PRTG



SEYOT Lucas

UFA R.Schuman

12/06/2024

## Table des matières

Introduction : .....	2
Installation PRTG .....	3
Conclusion : .....	12

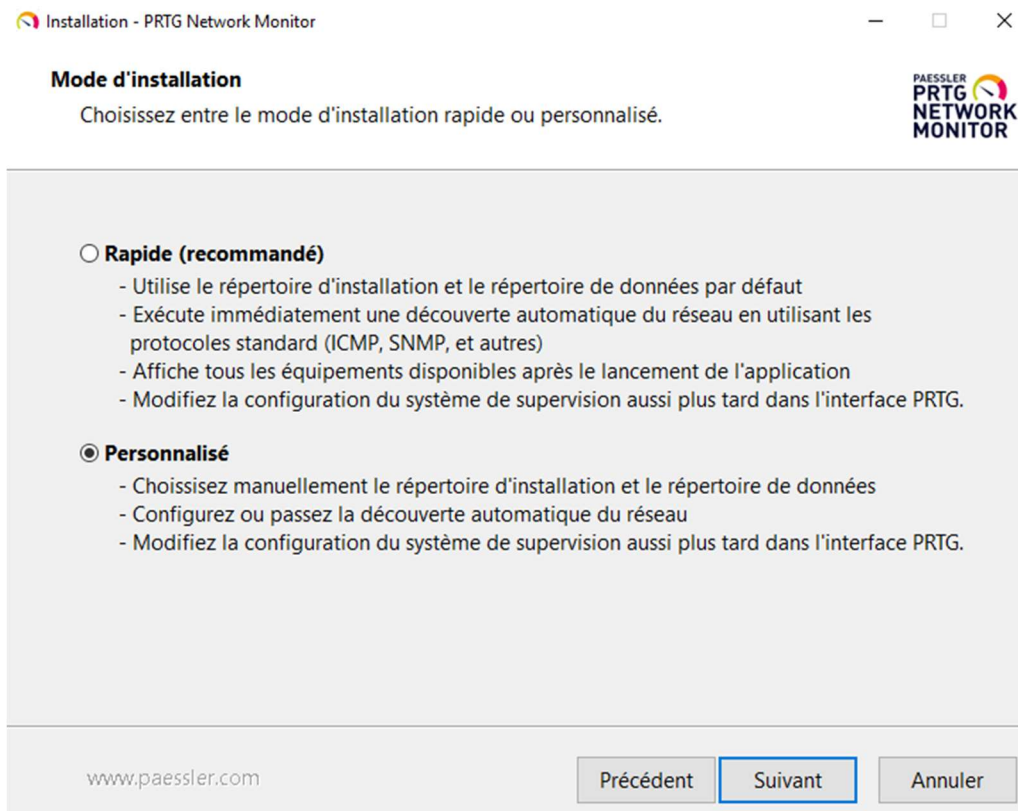
# Introduction :

Dans ce document, nous allons procéder à l'installation de PRTG afin de suivre l'installation de LAMPHP8.2 et de GLPI.

Le PRTG a pour objectif de nous offrir une vision d'ensemble de notre équipement. À partir de là, nous pouvons mettre en place des sondes (Node en anglais) pour évaluer l'état du matériel, y établir des règles de priorité et suivre l'équipement. Dans notre situation, nous le connecterons à notre serveur Active Directory afin de vérifier son état de santé, de fonctionnement et de connectivité.

# Installation PRTG

On dépose le documents PRTG installeur sur le Windows server et on le lance.

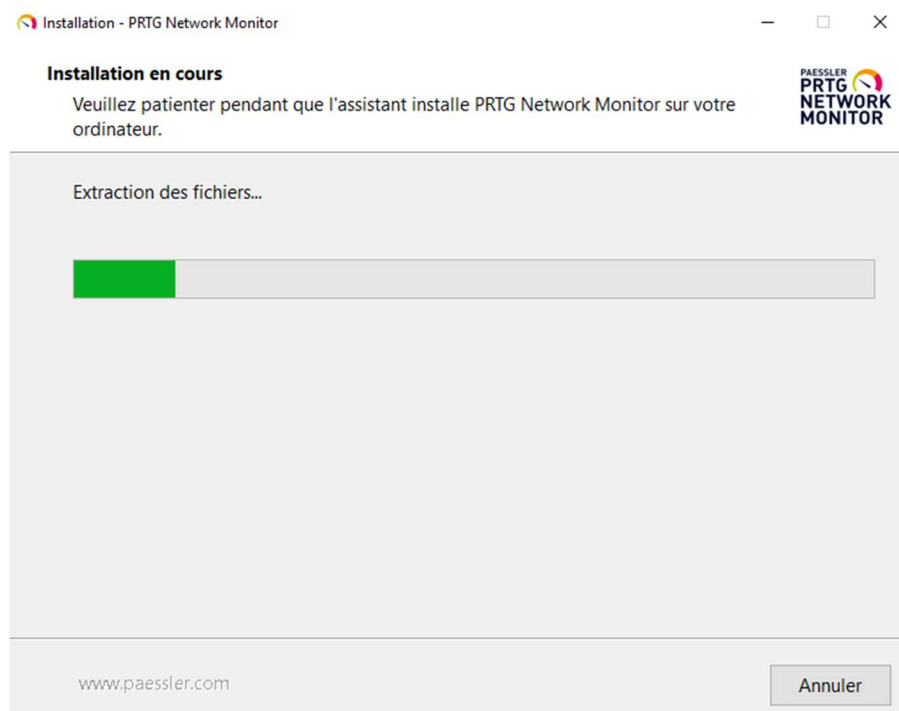


Il est nécessaire d'accepter le règlement dans les premières étapes, puis d'initialiser l'adresse électronique. La troisième étape est plus cruciale car elle nous permettra de personnaliser notre configuration :

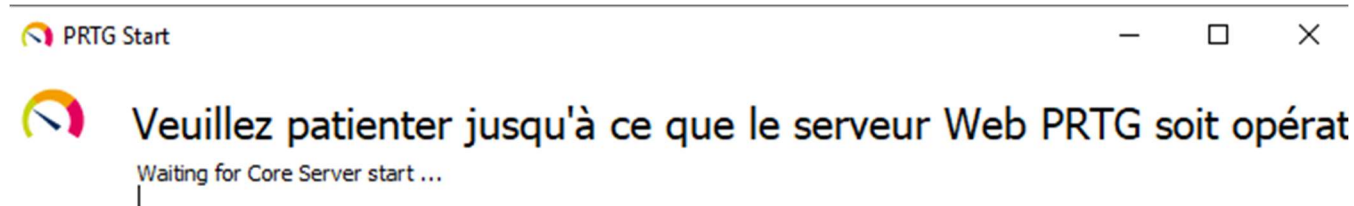
Ensuite le choix du fichier d'installation qui reste inchangé.

L'étape qui suis est un de découverte automatique, on n'en a pas besoin car notre bon professeur nous suit dans les étapes.

## Et ensuite on attend sagement l'installation :



## Ce n'est pas fini car après installation il a besoin de s'initialiser :



Une fois fini nous avons une page qui s'ouvre automatique qui est :



## PRTG Network Monitor (SRV-V-AD1-GA)

Nom d'utilisateur

prtgadmin

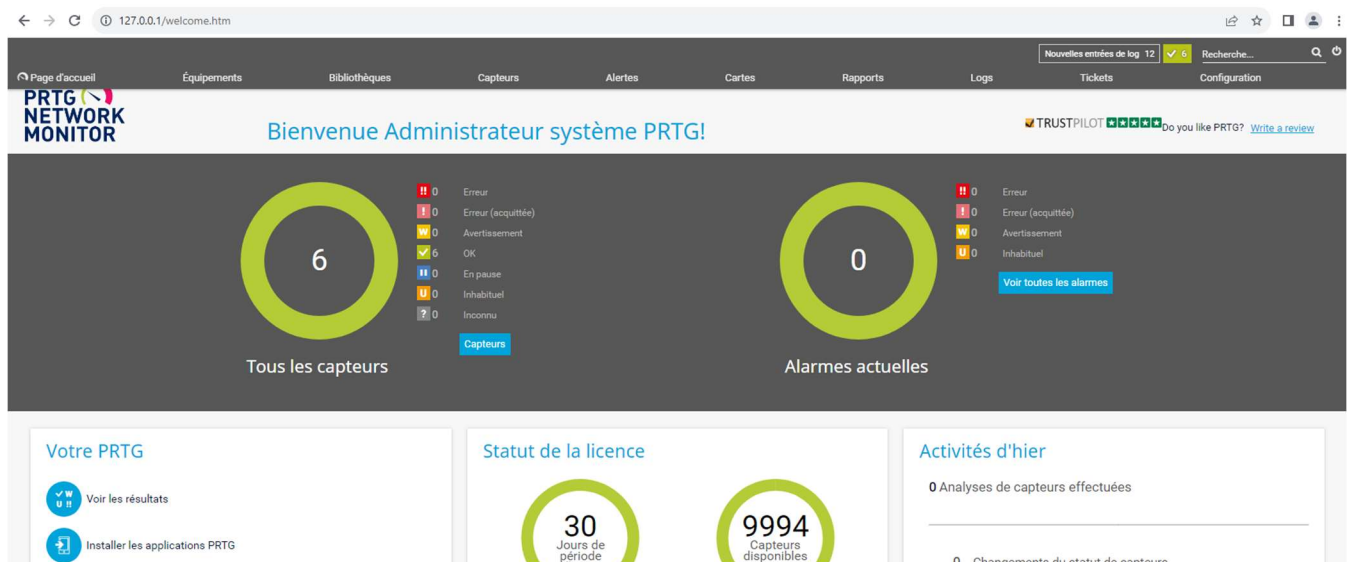
Mot de passe

prtgadmin

Connexion

- > Vous avez oublié votre mot de passe ?
- > Besoin d'aide ?
- > Télécharger les applications pour Windows, macOS, iOS, Android (en option)

On se connecte et on tombe sur cette belle interface :



## On va ajouter une sonde pour la WMI en allant dans capteur > Ajouter un capteur > créer un nouvel équipement.

### Ajouter un équipement

< Annuler

Choisissez un groupe pour l'ajout du nouvel équipement

- ☐ Créer un nouveau groupe  
☒ Ajouter un équipement à un groupe déjà existant

Sélectionner un groupe dans la liste

Sélectionnez un groupe dans la liste. Vous pouvez créer des équipements plus rapidement en cliquant avec le bouton droit sur un groupe de l'arborescence des équipements et en sélectionnant Ajouter un équipement dans le menu contextuel.

Continuer

Recherche...



Racine  
Sonde locale  
1er groupe

## On va le paramétrer maintenant en faisant continuer.

Paramétrages de base de l'équipement

Nom de l'équipement <sup>?</sup> pfSense01

Version IP <sup>?</sup> ☒ IPv4 (par défaut)  
☐ IPv6

Adresse IPv4/Nom DNS <sup>?</sup> 192.168.10.1

Balises <sup>?</sup>

Information supplémentaire sur l'équipement

Icône de l'équipement <sup>?</sup>

Ajouter

Identification d'équipements et découverte automatique

Niveau de la découverte automatique <sup>?</sup> ☒ Pas de découverte automatique (par défaut)  
☐ -

Informations d'identification pour les équipements SNMP

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

Version SNMP <sup>?</sup> ☐ SNMP v1  
☒ SNMP v2c (par défaut)  
☐ SNMP v3

Chaine de communauté <sup>?</sup> ga

Port SNMP <sup>?</sup> 161

Délai d'expiration (s) <sup>?</sup> 5

Ajouter

(Ceci est juste un exemple car nous n'avons pas de firewall installé)  
Nous allons donc ajouter)

On va maintenant ajouter une sonde sur notre serveur pour cela on retourne dans notre équipement afin de créer un nouveau groupe comme ceci :

Ajouter un équipement au groupe 1er groupe

Ajout d'équipements

Indiquez le nom et l'adresse IP d'un équipement, les options de découverte automatique et si nécessaire les paramètres d'authentification pour Windows, Linux, VMware/XenServer, SNMP et des fournisseurs spécifiques.

Manuel de PRTG : ajouter un équipement

Paramétrages de base de l'équipement

Nom de l'équipement ⓘ

SRV-V-AD1-GA

Version IP ⓘ

☒ IPv4 (par défaut)

☐ IPv6

Adresse IPv4/Nom DNS ⓘ

SRV-V-AD1-GA

Balises ⓘ

Et on lui ensuite les règles d'identification pour le système Windows :

#### Informations d'identification pour systèmes Windows

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

Nom de domaine ou d'ordinateur ⓘ

GA.local

Nom d'utilisateur ⓘ

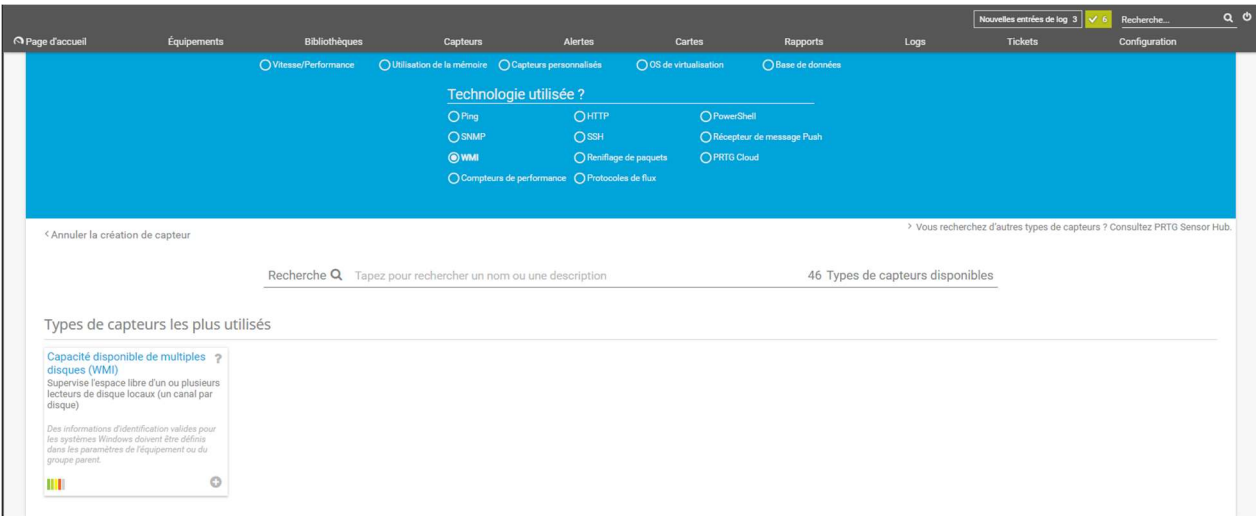
Florent

Mot de passe ⓘ

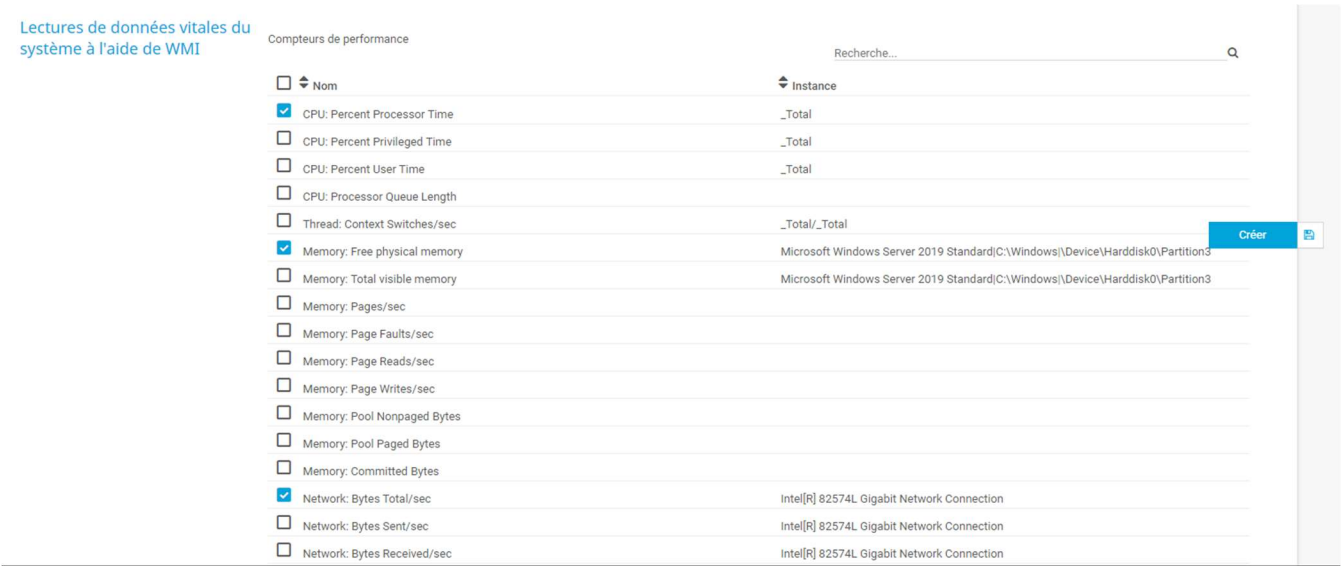
\*\*\*\*\*



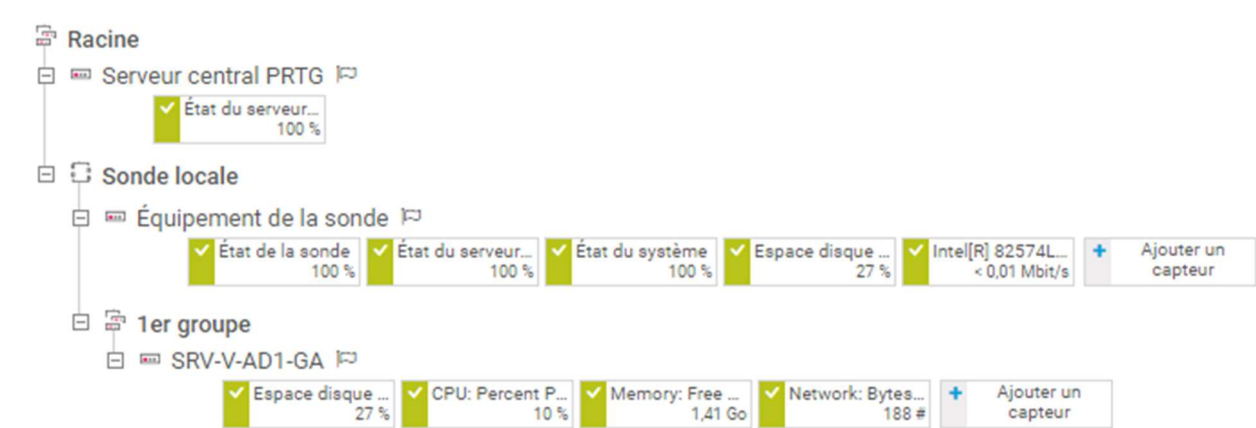
Après cela on le voit bien le nouveau groupe apparaitre, on aura juste à ajouter des capteurs et les configurer comme cela :



Après chargement du capteur on le valide et il sera ajouté au groupe. Le temps que le capteur s'initialise, on va aller ajouter un autre capteur en retournant dans équipement > ajouter un capteur. Nous prenons la technologie pour voir la charge cpu et nous avons la configuration :



Le temps que la charge CPU s'initialise voici à quoi ressemble déjà nos sondes :



On se rendra ensuite sur notre groupe « SRV-V-AD1-GA » afin d'aller s'occuper des déclencheurs d'évènement on ira sur cet onglet :

Équipement SRV-V-AD1-GA

Vue d'ensemble 2 Jours 30 Jours 365 Jours Alertes Informations système Log Paramètres **Déclencheurs de notifications** Commentaires Historique

Déclencheurs de notifications

Type	Règle	Actions
(aucun déclencheur défini)		

Déclencheurs de notifications pouvant être hérités des objets parents

☒ Hériter de tous les déclencheurs de notifications des objets parents et utiliser les déclencheurs de notifications définis ci-dessus (par défaut)  
☐ Utiliser uniquement les déclencheurs de notifications définis ci-dessus

Type	Règle	hérité de
Déclencheur sur état	Lorsque le statut du capteur est Erreur pendant au moins 600 secondes, exécuter @ ➤ Notification par email et message Push à l'administrateur	Racine
	Lorsque le statut du capteur est Erreur pendant au moins 900 secondes, exécuter aucune notification et répéter l'opération toutes les 0 minutes	
	Lorsque le capteur quitte le statut Erreur, exécuter @ ➤ Notification par email et message Push à l'administrateur	

Une fois ici on va ajouter un nouveau déclencheur (le + à droite) et on ajoute un déclencheur sur seuil comme cela :

Déclencheurs de notifications

Type	Règle	Actions
Déclencheur sur seuil	Lorsque le canal Espace disponible C: (%) est en dessous de 25 pendant au moins 60 secondes, exécuter ➤ Notification de ticket	
Déclencheur sur seuil (ID: 1)	Lorsque la condition ne s'applique plus, exécuter ➤ Notification de ticket	

Enregistrer le déclencheur

On va ensuite paramétrer les tickets qui sont créés lors d'une erreur en cliquant sur « notification de ticket »

Modifier un modèle de notification

Envoyer un email

☒ Ajouter une entrée au journal des événements

Fichier journal ⓘ

☒ Application  
☐ PRTG Network Monitor

Source d'événement ⓘ

PRTG Network Monitor

Type d'événement ⓘ

Erreur

Message ⓘ

[%sitename] %device %name %status %down (%message)

Envoyer un message SMS/Pager

Annuler Enregistrer

## Et aussi :

Modifier un modèle de notification

Attribuer un ticket

Attribuer à un groupe d'utilisateurs ou à un utilisateur

☒ À un groupe d'utilisateurs

☐ À un utilisateur

Groupe d'utilisateurs

Administrateurs PRTG

Objet

%device %name %status %down (%message)

Contenu

Capteur: %name  
Statut: %status %down  
Date/Heure: %datetime (%timezone)

Lorsque la condition ne s'applique plus

☒ Fermer le ticket de notification (recommandé)

☐ Ne pas fermer le ticket de notification

Annuler

Enregistrer

Et ensuite on répète l'étapes sur les autres sondes.

✓ Capteur CPU: Percent Processor Time \_Total

Vue d'ensemble

Données en temps réel

2 Jours

30 Jours

365 Jours

Données historiques

Log

Paramètres

Déclencheurs de notifications

Commentaires

Historique

Déclencheurs de notifications

Type	Règle	Actions
Déclencheur sur seuil	Lorsque le canal Processor Time (%) est au-dessus de 65 pendant au moins 60 secondes, exécuter	Notification de ticket
	Lorsque la condition ne s'applique plus, exécuter	Notification de ticket

✓ Capteur Memory: Free physical memory Microsoft Windows Server 2019 Standard|C:\Windo...

Vue d'ensemble

Données en temps réel

2 Jours

30 Jours

365 Jours

Données historiques

Log

Paramètres

Déclencheurs de notifications

Commentaires

Historique

Déclencheurs de notifications

Type	Règle	Actions
Déclencheur sur seuil	Lorsque le canal Free physical memory (Octet) est en dessous de 0.5 pendant au moins 60 secondes, exécuter	Notification de ticket
	Lorsque la condition ne s'applique plus, exécuter	Notification de ticket

✓ Capteur Network: Bytes Total/sec Intel[R] 82574L Gigabit Network Connection

Vue d'ensemble

Données en temps réel

2 Jours

30 Jours

365 Jours

Données historiques

Log

Paramètres

Déclencheurs de notifications

Commentaires

Historique

Déclencheurs de notifications

Type	Règle	Actions
Déclencheur sur seuil	Lorsque le canal Bytes Total/sec (#) est en dessous de 0.5 pendant au moins 60 secondes, exécuter	Notification de ticket
	Lorsque la condition ne s'applique plus, exécuter	Notification de ticket

On peut voir ici les logs disponibles avec plusieurs informations :

Entrées log

Éléments: 50

Afficher les filtres

Date et heure	Parent	Type	Objet	Statut	Message
20/03/2024 09:34:59	SRV-V-AD1-GA	Données système vitales v2 (WMI)	Network: Bytes Total/sec Intel[R] 82574L Gigabit Net...	Sous-nœuds créés	[ Déclencheur sur seuil ID:1/Canal: Bytes Total/sec
20/03/2024 09:33:59	SRV-V-AD1-GA	Données système vitales v2 (WMI)	Memory: Free physical memory Microsoft Windows S...	Sous-nœuds créés	[ Déclencheur sur seuil ID:1/Canal: Free physical m...
20/03/2024 09:33:13	SRV-V-AD1-GA	Données système vitales v2 (WMI)	CPU: Percent Processor Time _Total	Sous-nœuds créés	[ Déclencheur sur seuil ID:1/Canal: Processor Time
20/03/2024 09:31:29	Aucun	Modèle de notifications	Notification de ticket	Modifié	Consultez l'historique de l'objet pour plus de détails
20/03/2024 09:31:29	Aucun	Modèle de notifications	Notification de ticket	Sous-nœuds modi...	Consultez l'historique de l'objet pour plus de détails
20/03/2024 09:31:29	Aucun	Modèle de notifications	Notification de ticket	Sous-nœuds modi...	Consultez l'historique de l'objet pour plus de détails
20/03/2024 09:31:29	Aucun	Modèle de notifications	Notification de ticket	Sous-nœuds modi...	Consultez l'historique de l'objet pour plus de détails
20/03/2024 09:29:08	SRV-V-AD1-GA	Capacité disponible de multiples di...	Espace disque libre (plusieurs lecteurs)	Sous-nœuds modi...	Consultez l'historique de l'objet pour plus de détails
20/03/2024 09:27:44	SRV-V-AD1-GA	Capacité disponible de multiples di...	Espace disque libre (plusieurs lecteurs)	Sous-nœuds modi...	Consultez l'historique de l'objet pour plus de détails
20/03/2024 09:26:52	SRV-V-AD1-GA	Capacité disponible de multiples di...	Espace disque libre (plusieurs lecteurs)	Sous-nœuds créés	[ Déclencheur sur seuil ID:1/Canal: Espace disponi...
20/03/2024 09:24:25	SRV-V-AD1-GA	Données système vitales v2 (WMI)	CPU: Percent Processor Time _Total	OK	10 %
20/03/2024 09:24:15	SRV-V-AD1-GA	Données système vitales v2 (WMI)	Network: Bytes Total/sec Intel[R] 82574L Gigabit Net...	OK	188 #
20/03/2024 09:23:20	SRV-V-AD1-GA	Données système vitales v2 (WMI)	Memory: Free physical memory Microsoft Windows S...	OK	1,40 Go
20/03/2024 09:22:55	1er groupe	Device	SRV-V-AD1-GA	Objet enfant créé	Capteur « CPU: Percent Processor Time _Total »
20/03/2024 09:22:55	SRV-V-AD1-GA	Données système vitales v2 (WMI)	CPU: Percent Processor Time _Total	Inconnu	Veuillez patienter. Plusieurs minutes peuvent être n...
20/03/2024 09:22:55	SRV-V-AD1-GA	Données système vitales v2 (WMI)	CPU: Percent Processor Time _Total	Inconnu	Consultez l'historique de l'objet pour plus de détails

Capteurs en statut OK

Afficher les filtres

Capteur	Sonde, Groupe, Équipement	Statut	Dernière valeur	Message	Graphique	Priorité	Fav	Impact perf.	
✓ État de la sonde	Sonde locale (Sonde locale) » Équipement de la sonde	OK	100 %	OK	État 100 %	★★★★★ P2			
✓ État du serveur central	Sonde locale (Sonde locale) » Équipement de la sonde	OK	100 %	OK	État 100 %	★★★★★ P2			
✓ État du serveur central (autonome)	Serveur central PRTG	OK	100 %	OK	État 100 %	★★★★★ P2			
✓ État du système	Sonde locale (Sonde locale) » Équipement de la sonde	OK	100 %	OK	État 100 %	★★★★★ P2			
✓ Espace disque libre	Sonde locale (Sonde locale) » Équipement de la sonde	OK	27 %	OK	Espace dispo 27 %	★★★★☆ P2			
✓ CPU: Percent Processor Time _Tot...	Sonde locale (Sonde locale) » 1er groupe » SRV-V-AD1-GA	OK	8 %	OK	Processor Tir 8 %	★★★★☆ P2			
✓ Espace disque libre (plusieurs lect...	Sonde locale (Sonde locale) » 1er groupe » SRV-V-AD1-GA	OK	27 %	OK	Espace dispo 27 %	★★★★☆ P2			
✓ Memory: Free physical memory MI...	Sonde locale (Sonde locale) » 1er groupe » SRV-V-AD1-GA	OK	1,47 Go	OK	Free physical 1,47 Go	★★★★☆ P2			
✓ Network: Bytes Total/sec Intel[R] 8...	Sonde locale (Sonde locale) » 1er groupe » SRV-V-AD1-GA	OK	108 #	OK	Bytes Total/s 108 #	★★★★☆ P2			

# Conclusion :

Après installation et configuration de nos sondes sur nos divers équipements, on peut se rendre compte que ce " logiciel " nous est bénéfique grâce à son système de suivis et de logs car en cas de pannes, on peut y retrouver les informations nécessaires quand les règles et les déclencheurs sont bien paramétré, dans cas on peut voir la connective du serveur, sont états de santé matériel et son états de charge matériel.

Il faut donc vérifié :

- Surveillance des capteurs : S'assurer que tous les capteurs configurés dans PRTG fonctionnent correctement en vérifiant régulièrement les données collectées.
- Alertes et notifications : Configurer des alertes et des notifications dans PRTG pour être informé en temps réel des problèmes potentiels.
- Analyse des tendances : Utiliser les fonctionnalités d'analyse et de génération de rapports de PRTG pour suivre les tendances de performance sur le long terme.

Et faire attention à :

- Accès sécurisé : Limitez l'accès à l'interface de gestion de PRTG aux utilisateurs autorisés en utilisant des méthodes d'authentification forte telles que l'authentification à deux facteurs.
- Mises à jour régulières : Verifié si PRTG est à jour avec les dernières versions et correctifs de sécurité.
- Sauvegardes régulières : Faires des sauvegardes régulières des configurations de PRTG et des données collectées pour éviter toute perte de données en cas de panne ou de corruption.
- Surveillance de la sécurité réseau : Utilisez PRTG pour surveiller les activités réseau suspectes.