29/05/2024

PETTE Benjamin

Installation de PRTG

Supervision avec le logiciel PRTG – Ping – SNMP – WMI - Projet

**Projet :** Installation de PRTG et supervision avec cet outil

**Date :** 29/05/2024

**Réalisé par :** PETTE Benjamin

Introduction :

Dans ce projet, nous allons installer et configurer PRTG (Paessler Router Traffic Grapher) pour la supervision réseau. PRTG utilise diverses technologies comme Ping, SNMP (Simple Network Management Protocol) et WMI (Windows Management Instrumentation) pour surveiller les performances et la disponibilité des infrastructures informatiques en temps réel.

Nous détaillerons les étapes d'installation de PRTG, suivies de l'utilisation de :

* **Ping** : Pour vérifier la disponibilité des appareils réseau.
* **SNMP** : Pour collecter des données sur les équipements réseau.
* **WMI** : Pour superviser les systèmes Windows.

Ce projet vise à fournir une méthode pratique pour améliorer la gestion et la réactivité de l'infrastructure informatique grâce à une supervision efficace et proactive.

Commencer par choisir la langue :

Une image contenant texte, capture d’écran, logiciel, Système d’exploitation

Description générée automatiquement

Continuer ensuite par accepter les termes du contrat de licence :

Une image contenant texte, capture d’écran, logiciel, affichage

Description générée automatiquement

Renseigner votre adresse mail d’entreprise pour recevoir les alertes lier a PRTG :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Pour les modes d’installation choisissez l’installation Personnalisé :

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Par la suite renseignez le chemin qui vous convient pour finaliser l’installation de PRTG

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

Ici, cocher « passer la découverte automatique »

Une image contenant texte, Appareils électroniques, capture d’écran, logiciel

Description générée automatiquement

A la fin de l’installation une fenêtre web s’ouvre automatiquement avec des identifiant connectez-vous directement :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Une fois arriver sur l’interface cliquer sur « Modifier le mot de passe par défaut » en bas à droite :

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Une fois arriver ici, cocher la case « spécifier un nouveau mot de passe » et mettez-y un mot de passe propre à vous.

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Une fois le mot de passe définis nous allons passer à la deuxième alerte qui se situe toujours en bas a droites « Activer SSL/TLS »

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

Et confirmer donc ensuite le passage à SSL/TLS :

Une image contenant texte, capture d’écran, logiciel, Police

Description générée automatiquement

Une fois redémarrer la page web vous affichera un message disant que votre connexion n’est pas sécurisée pour ignorer ce message cliquer sur « Avancé » et cliquer ensuite sur « Continuer vers … »

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Connecter vous ensuite à votre session avec votre nouveau mot de passe :

Une image contenant texte, capture d’écran, logiciel, Page web

Description générée automatiquement

Aller ensuite dans le menu déroulant « Capteur » et cliquer sur Ajouter un capteur

Une image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

En premier cocher « Créer un nouvelle équipement » et une fois ca fait cliquer sur 1er groupe en dessous de Sonde locale et continuer à nouveau sur la case de Continuer :

Une image contenant texte, logiciel, Icône d’ordinateur, Page web

Description générée automatiquement

Par la suite recopier cette configuration

Une image contenant texte, capture d’écran, nombre, Police

Description générée automatiquement

Ensuite descendez un peu et chercher cette capsule, décoché la et recopier la configuration en changeant par votre chaine de communauté en mettant les initiales ou nom que vous pouvez choisir :

Une image contenant texte, capture d’écran, Police

Description générée automatiquement

Ensuite accédez à votre serveur psSense sur votre navigateur et dans l’onglet « Service » et « SNMP »

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquement

Remplacer le “Read Community String” par votre nom de communauté renseigner précédemment par la suite sur le pfSense cliquer sur « Ajouter un capteur »

Une image contenant texte, capture d’écran

Description générée automatiquement

Choisissez donc SNMP

Vous pouvez ajouter comme capteur la charge CPU Une image contenant texte, capture d’écran, ligne

Description générée automatiquement

Une image contenant capture d’écran, texte, ligne

Description générée automatiquementEt comme vous pouvez le voir la charge CPU s’affiche correctement :

Une image contenant texte, Police, capture d’écran

Description générée automatiquementUn autre capteur qui pourrait être intéressant, cliquer sur ajouter un capteur et rechercher snmp :

Celui-ci va superviser le trafic de la bande passante sur les serveurs.

Quand vous arriver dans la configuration du capteur veillez a bien activé vos différentes interface :

Une image contenant texte, capture d’écran, Police, nombre

Description générée automatiquement

En plus de ça vous pouvez ajouter des canaux supplémentaires comme :

Une image contenant texte, capture d’écran, Police, algèbre

Description générée automatiquement

Après l’avoir créé vous pourrez apercevoir 3 nouveaux capteurs

En plus de ces 4 capteurs nous allons rajouter un capteur de ping qui permet de savoir si le serveur répond en temps réel

Une image contenant texte, logiciel, nombre, Page web

Description générée automatiquement

Une fois créer vous pourrez apercevoir vos 4 capteurs qui s’affiche en vert sur la vue d’ensemble :

Une image contenant texte, capture d’écran, Police, ligne

Description générée automatiquement

Dès à présent nous allons mettre en place un WMI pour les serveurs Windows pour vérifier l’état d’un service ou d’un serveur Windows, commençons par créer un nouvel équipement qui va donc être notre serveur Active Directory

Une image contenant texte, capture d’écran, logiciel, nombre

Description générée automatiquementUne image contenant texte, capture d’écran, logiciel, Icône d’ordinateur

Description générée automatiquement

En premier lieu nommer votre équipement par le nom que vous avez attribué à votre AD de même pour votre Nom DNS, pour ce qui est de l’icone c’est propre a votre choix, pour la découverte automatique nous allons skipper en cochant « Pas de découverte automatique »

Pour ce qui est de la configuration de l’identification pour système Windows renseignez votre nom de domaine, et les identifiants Administrateur avec le mot de passe puis valider.

Après avoir fait ça vous pourrais apercevoir votre serveur sur lequel vous allez ajouter un capteur WMI en cochant WMI

Une image contenant texte, capture d’écran, logiciel

Description générée automatiquement

Nous allons donc choisir ce capteur qui va nous permettre de vérifier l’espace libre pour éviter qu’il sature, laisser les paramètres par défauts et créer le. En patientant qu’il récupère l’espace libre, nous allons donc ajouter un nouveau capteur WMI en recherchant cette fois ci « Active Directory »

Une image contenant texte, logiciel, Page web, Site web

Description générée automatiquement

La réplication AD va nous permettre qu’un ou plusieurs AD communique entre eux et synchronise toutes les données.

En rentrant dans la configuration du capteur il repère directement que notre voisin de republication est bien le nom de notre AD en laissant tous par défaut vous pouvez le créer.

Une image contenant texte, logiciel, Page web, capture d’écran

Description générée automatiquement

Par la suite en allant sur mon capteur d’espace disque vous pourrez apercevoir que l’espace à été calculé et vous montre combien de pourcentage de stockage libre il vous reste. Pour être prévenu d’un éventuel souci nous allons ajouter un « Déclencheur de notification » pour cela cliquer sur le petit plus et « Ajouter un déclencheur sur seuil »

Une image contenant texte, capture d’écran

Description générée automatiquement



Reprenez la configuration de ce déclencheur qui si vous le comprenez va vous envoyer une notification (seulement admin), si l’espace disponible est inferieur a 10%.

**Conclusion :**

En conclusion, l'installation et la configuration de PRTG offrent de nombreux avantages pour la supervision réseau. PRTG permet une surveillance en temps réel des performances et de la disponibilité des infrastructures informatiques, ce qui améliore la réactivité et la gestion des ressources critiques. L'utilisation de technologies comme Ping, SNMP et WMI permet de collecter des données précises et de détecter rapidement les problèmes potentiels.

Pour vérifier le bon fonctionnement de PRTG, assurez-vous que :

* Le tableau de bord PRTG affiche des données en temps réel.
* Les alertes et notifications sont correctement configurées et fonctionnelles.
* Les capteurs Ping, SNMP et WMI collectent des données et génèrent des rapports précis.

Les points de vigilance incluent :

**Mises à jour régulières** : Assurez-vous que PRTG et ses composants sont à jour pour bénéficier des dernières fonctionnalités et corrections de sécurité.

**Sauvegardes** : Effectuez des sauvegardes régulières de la configuration de PRTG et des données collectées.

**Surveillance des performances** : Suivez les performances du serveur PRTG pour anticiper les problèmes de charge.

Conseils de sécurité :

* Utiliser des connexions **SSL/TLS** pour sécuriser les communications.
* Configurer des **mots de passe forts** et des politiques de rotation régulières.
* Limiter l'accès à l'interface PRTG aux adresses IP autorisées et utiliser des **pares-feux** pour protéger le réseau.

En suivant ces recommandations, vous garantirez une supervision réseau efficace et sécurisée avec PRTG.