

TP Supervision PRTG

Intro :

Aujourd'hui nous allons installer sur notre serveur de fichier un outil de supervision appelé PRTG et on va y superviser notre pare-feu élément important du réseau.

Tout d'abord on va aller télécharger l'installateur sur le site de Paessler en cliquant sur essai gratuit puis on suis les étape et on met de côté la clé fournie avec le logiciel.



Supervisez l'intégralité de votre infrastructure IT avec les outils de supervision Paessler PRTG

- ✓ Une supervision IT professionnelle pour tous les types d'infrastructures
- ✓ Pour les environnements de toutes les tailles : petits, moyens, grands et très grands
- ✓ Sur site ou basé sur le Cloud et hébergé par Paessler
- ✓ Une tarification à votre convenance : abonnement ou licence permanente

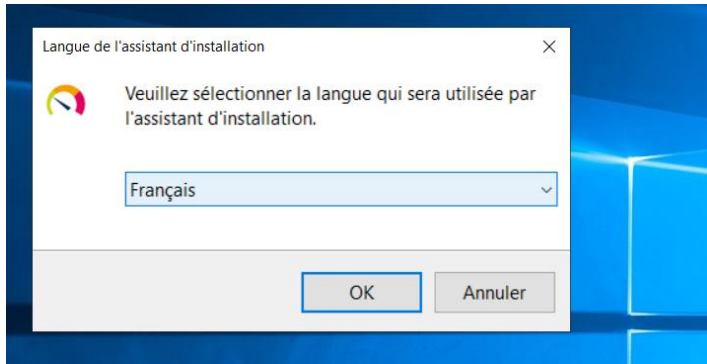
Votre clé de licence

000014-YYRKFM-8FFVHH-JMPE5F-1TNTXQ-
TP3ZTP-74BDTJ-5KHNBj-ERX6ZG-UM8XPR

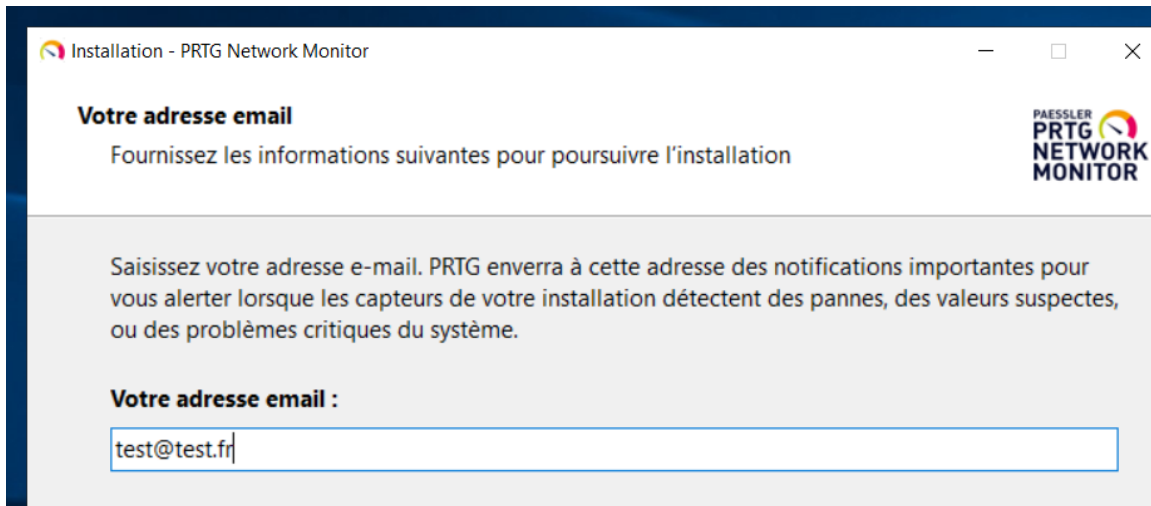
000014-YYRKFM-8FFVHH-JMPE5F-
1TNTXQ-TP3ZTP-74BDTJ-5KHNBj-ERX6ZG-UM8XPR

Prochaine étape on va donc exécuter notre logiciel sur la vm srv fichier.

Et on suit le programme d'installation :



Puis quand on nous demande une adresse mail ici dans le cas d'un labo on mettra n'importe quel mail.



Et on va choisir une installation personnalisé.

Mode d'installation

Choisissez entre le mode d'installation rapide ou personnalisé.



Rapide (recommandé)

- Utilise le répertoire d'installation et le répertoire de données par défaut
- Exécute immédiatement une découverte automatique du réseau en utilisant les protocoles standard (ICMP, SNMP, et autres)
- Affiche tous les équipements disponibles après le lancement de l'application
- Modifiez la configuration du système de supervision aussi plus tard dans l'interface PRTG.

Personnalisé

- Choisissez manuellement le répertoire d'installation et le répertoire de données
- Configurez ou passez la découverte automatique du réseau
- Modifiez la configuration du système de supervision aussi plus tard dans l'interface PRTG.

Et on passera la découverte automatique qui nous ajoute des capteurs que l'on a pas besoin.

Exécuter la découverte automatique

PRTG peut exécuter une découverte automatique de vos sous-réseaux pendant l'installation. Vous pouvez ensuite commencer à mettre en place vos équipements détectés dans votre réseau.

Vous pouvez ensuite commencer à mettre en place votre serveur détectés dans votre réseau.

Exécuter la découverte automatique

Passer la découverte automatique

Puis après la décompression des fichier on va installer google chrome pour plus de simplicité et on va lancer l'interface web.



PRTG Network Monitor (SRV-FICHIERS1)

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)

Les identifiants sont déjà rentrés.

Activer votre licence

Statut de la licence:

Non activé (Failed to establish secure connection Socket Error # 11002)

Vous pouvez commencer à utiliser PRTG une fois votre licence activée.

Choisissez le type d'activation automatique ou manuel, puis vérifiez le nom de votre licence et votre clé.

Remarque : Votre serveur central PRTG a besoin d'une connexion à l'un des domaines de serveur d'activation Paessler. Si votre serveur PRTG ne peut pas se connecter au serveur d'activation Paessler, sélectionnez **Manuelle (activation hors ligne)** sous Type d'activation. Pour obtenir une liste de tous les domaines du serveur d'activation Paessler, consultez la Base de connaissances : <https://kb.paessler.com/en/topic/32513>

ÉTAPE 1 : Choisir le type d'activation

Type d'activation ⓘ

Automatique (activation en ligne avec proxy HTTP facultatif)

Manuelle (activation hors ligne)

ÉTAPE 2 : Vérifier votre licence PRTG

Clé de licence ⓘ

000014-YYRKFM-8FFVHH-JMPESF-1TNTXQ-TP3ZTP-74BDTJ-5KHNBJ-ERX6ZG-UM8XPR

il suffit juste de passer à la suite.

Puis les informations pour activer la licence également

Si la connexion ne passe pas il faudra juste ajouter une règle de pare-feu qui autorise toutes les connexions.

Puis une fois sur l'interface on va activer la connexion ssl

Activer SSL/TLS pour l'interface Web PRTG.✕

La connexion de votre navigateur à ce serveur central de PRTG n'est pas sécurisée par SSL/TLS. Il est préférable de passer à SSL/TLS, particulièrement si votre interface Web PRTG est accessible depuis internet (en dehors de votre pare-feu).

[Passer à SSL/TLS](#)

Premièrement on va ajouter un capteur :

Commençons avec le pfsense. On va créer un nouvel appareil depuis la vue d'ensemble dans le premier groupe on va ajouter un équipement.

Puis on rentre l'ip du pfsense 192.168.0.254

Ajouter un équipement au groupe 1er groupe

Informations d'identification pour les équipements SNMP

hériter de 1er groupe (Version SNMP: v2, Port SNMP: 161, Délai d'exp...)

Version SNMP

SNMP v1

SNMP v2c (par défaut)

SNMP v3

Chaine de communauté

snmp

Port SNMP

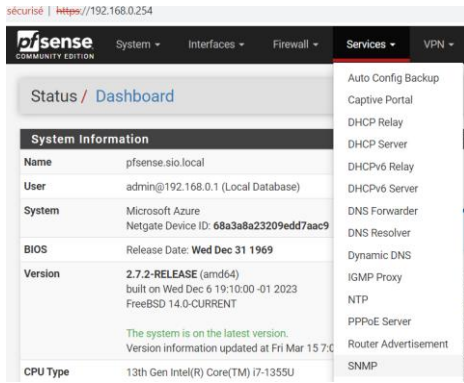
161

Délai d'expiration (s)

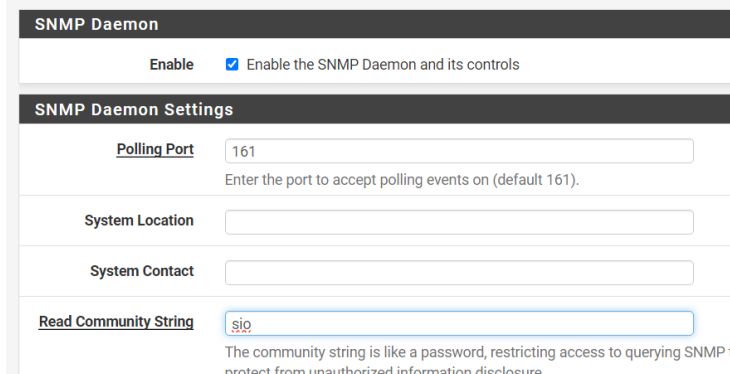
5

Puis on descendant un peu on va décocher la case SNMP pour la configurer

Puis on se rendre sur le pfsense à l'ip 192.168.0.254 et configurer sa partie également.



Donc service en haut puis SNMP.



Il faut donc activer avec la case en haut

vérifier que le port est le même et mettre le même nom de communauté puis sauvegarder.

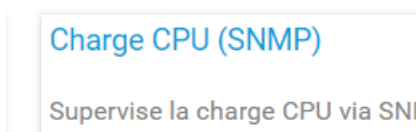
Ensuite on retourne sur le PRTG et sur le pfsense on ajoute un capteur.



En haut on sélectionne SNMP



Par exemple on va essayer avec la charge cpu.



On peut monter la priorité et valider.

Ajouter un capteur à l'équipement pfSense [192.168.0.254] (Étape 2 à 2)

< Annuler

Paramètres de base du capteur

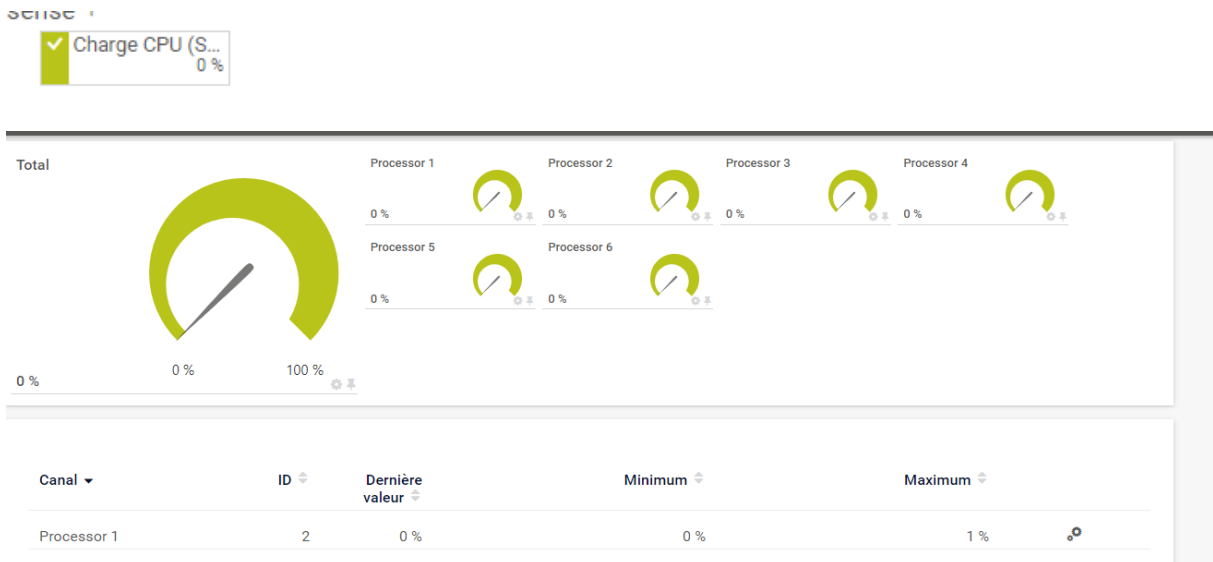
Nom du capteur

Balises parentes

Balises

Priorité

Puis on peut maintenant voir les données de l'équipement.



On va maintenant aussi ajouter un autre capteur intéressant le capteur de trafic internet.

< Annuler la création de capteur

Recherche

Types de capteurs les plus utilisés

Trafic (SNMP) ?

Supervise la bande passante et le trafic sur les serveurs, les ordinateurs, les commutateurs, etc. via SNMP

Pour rechercher les données provenant d'un équipement de sonde (localhost, 127.0.0.1, ou ...), ajoutez cet équipement PRIG avec l'adresse IP qu'il possède dans votre réseau et créez le capteur sur cet équipement.

<input type="checkbox"/>	Nom	État	Débit	Type	64 bits	Nom interne
<input type="checkbox"/>	(001) enc0 Traffic	Non connecté		(not defined)	Oui	enc0
<input type="checkbox"/>	(002) lo0 Traffic	Connecté		Software Loopback	Oui	lo0
<input type="checkbox"/>	(003) pflog0 Traffic	Non connecté		(not defined)	Oui	pflog0
<input type="checkbox"/>	(004) pfsync0 Traffic	Latent		(not defined)	Oui	pfsync0
<input checked="" type="checkbox"/>	(005) hn0 Traffic	Connecté	10 GBit/s	Ethernet	Oui	hn0
<input checked="" type="checkbox"/>	(006) hn1 Traffic	Connecté	10 GBit/s	Ethernet	Oui	hn1
<input checked="" type="checkbox"/>	(007) CARP1 Traffic	Connecté	10 GBit/s	Ethernet	Oui	CARP1

Canaux supplémentaires Erreurs entrantes et sortantes

Rejets entrants et sortants

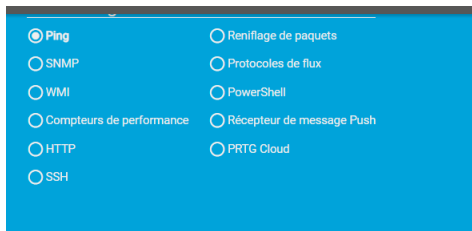
Paquets de monodiffusion entrants et sortants

Paquets non monodiffusion entrants et sortants (32 bits uniquement)

Paquets de multidiffusion entrants et sortants (64 bits uniquement)

On coche donc nos deux carte wan et lan et la carte qui fait la liaison puis on peut rajouter deux notifications pour monitorer.

Et un autre capteur celui de ping qui est intéressant dans un réseau.



> Vous recherchez d'autres types de capteurs ? Consultez PRTG

9 Types de capteurs disponibles



Pas de paramètre spécifique pour celui là on laissera par défaut.

Maintenant on va passer à la supervision des serveur avec le protocole WMI propre à Windows.

Pour cela on fait ajouter un nouveau capteur comme précédemment

Ajouter un équipement



Recherche...



Ensuite on mettra non pas l'ip mais le nom de la

machine au cas où elle changera d'ip.

Paramétrages de base de l'équipement

Nom de l'équipement [?]
SRV-FICHIER

Version IP [?]
 IPv4 (par défaut)
 IPv6

Adresse IPv4/Nom DNS [?]
SRV-FICHIERS1

Balises [?]
•

[Information supplémentaire sur l'équipement](#)

Et en dessous on changera uniquement la première option avec le nom de domaine et un administrateur dédié ou pas.

Informations d'identification pour systèmes Windows

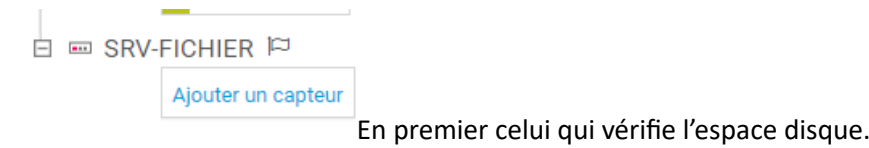
Hériter de **1er groupe** (Nom de domaine ou d'ordinateur: <vide>, Nom d...)

Nom de domaine ou d'ordinateur [?]
sio.local

Nom d'utilisateur [?]
administrateur

Mot de passe [?]
.....

On va alors ajouter un capteur WMI sur celui-ci.



Types de capteurs les plus utilisés

Capacité disponible de multiples disques (WMI)
Supervise l'espace libre d'un ou plusieurs lecteurs de disque locaux (un canal par

Et pareil on laisse les paramètres par

défaut.

On va ajouter un autre capteur concernant la réplique active directory pour vérifier que les connexions se font bien.

Types de capteurs disponibles

Active Directory erreurs de réplique
Vérifie les contrôleurs de domaine Windows pour des erreurs de réplique
.NET 4.7.2 doit être installé sur le système de la sonde. Des informations d'identification Windows valides doivent être définis dans les paramètres de l'équipement ou du domaine.

On laissera aussi par défaut celui-ci.

Notez que ce capteur fonctionne uniquement si vous avez plusieurs active directory dans mon cas ce n'est pas le cas donc on se passera de la présence de ce capteurs.

On va ensuite ajouter un déclencheur de notifications pour les disques pour être prévenu des problèmes.

Capteur Espace disque libre (plusieurs lecteurs) OK

Vue d'ensemble (4) Données en temps réel 2 Jours 30 Jours 365 Jours Données historiques Log Paramètres Déclencheurs de notifications Comm

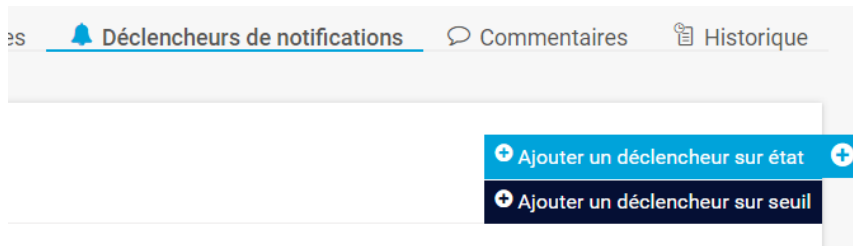
Espace disponible C: 26 Go 26 Go

Octets libres C: 26 Go

Total 26 Go

Find out why and how to buy PRTG!
GET MORE INFORMATION

Dernière analyse: 43 s



On peut alors modifier les

paramètres à notre guise.

IS

Type ^	Règle	Actions
Déclencheur sur seuil	Lorsque le canal Espace disponible C: (%) est en dessous de 10 pendant au moins 60 secondes, exécuter @ Notification par email et message Push à l'administrateur	✓ x
	Lorsque la condition ne s'applique plus, exécuter @ Notification par email et message Push à l'administrateur	

Et valider.

Conclusion :

Dans ce tp on a donc mis en place la supervision PRTG qui permet d'ajouter des capteurs SNMP sur les différents équipement du réseau de et suivre leur état. Et aussi des capteur WMI pour les servers propre à Windows, il existe bien sûr plein de possibilités mais trop de notifications incite à moins les regarder.