### 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

Sponsorisé

Paessler

https://www.paessler.com/free-prtg-trial

### **PRTG Network Monitor**

Powerful & easy network monitoring. Installed in minutes. Download now! Fully featured monitoring. Hosted version available. Monitor complete network. All in one dashboard.

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

Ninstallation - PRTG Network Monitor			×
Votre adresse email Fournissez les informations suivantes pour poursuivre l'installation		PAESSLER PRTG NETW MONIT	ORK OR
Saisissez votre adresse e-mail. PRTG enverra à cette adresse des notifications impor vous alerter lorsque les capteurs de votre installation détectent des pannes, des vale ou des problèmes critiques du système.	tante eurs s	es pour suspecte	s,
Votre adresse email : Paessler vous enverra également à cette adresse des informations sur nos produits e Vous pouvez à tout moment vous désinscrire de la réception de ces informations er privacy@paessler.com. Nous protégeons vos données personnelles. <u>Consultez notre politique de confidentialité pour en savoir plus.</u>	et ser écri	vices. vant à	
www.paessler.com Précédent Suivant		Annule	r

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

Installation - PRTG Network Monitor	- 🗆 X
Mode d'installation	
Choisissez entre le mode d'installation rapide ou personnalisé.	NÉTWORK MONITOR
<ul> <li>Rapide (recommandé)</li> <li>Utilise le répertoire d'installation et le répertoire de données par défa Exécute immédiatement une découverte automatique du réseau en ut protocoles standard (ICMP, SNMP, et autres)</li> <li>Affiche tous les équipements disponibles après le lancement de l'app</li> <li>Modifiez la configuration du système de supervision aussi plus tard da</li> <li>Personnalisé</li> <li>Choissisez manuellement le répertoire d'installation et le répertoire de Configurez ou passez la découverte automatique du réseau</li> <li>Modifiez la configuration du système de supervision aussi plus tard da</li> </ul>	aut tilisant les lication ans l'interface PRTG. e données ans l'interface PRTG.
www.paessler.com Précédent Sui	ivant Annuler

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





# PRTG Network Monitor (WIN-E00IQT81P3H)

Nom d'utilisateur		
prtgadmin		
Mot de passe		
prtgadmin		
	Connexion	
	de naces 2	

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)

internet (l'extérieur de votre pare-feu) ! Modifier le mot de passe par défaut

	Spécifier un nouveau mot de passe
Ancien mot de passe	
Nouveau mot de passe	
Confirmer le mot de passe	
Passhash 📵	Afficher le passhash
Passnash U	Afficher le passnash

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

Voulez-vous passer à SSL/	TLS ?
Vous êtes sur le point de config	jurer votre serveur central PRTG pour utiliser
une connexion sécurisée SSL/1	FLS.
Pour appliquer les paramètres,	votre serveur central PRTG va être arrêté et
redémarré. Cela peut prendre qu	uelques minutes. Lors du rechargement de
l'interface web, votre navigateur	r affichera un <b>avertissement de certificat</b> car le
certificat par défaut est inconnu	u de votre navigateur.
Il s'agit seulement du fait que le	e certificat livré avec PRTG n'est pas signé par
une autorité de certificats numé	ériques valide. Pour accéder à la page de
connexion, confirmez « les risqu	Jes de sécurité » annoncés.
Pour plus d'informations, consu	Iltez la base de connaissances :
https://kb.paessler.com/en/top	ic/89984
Remarque : Vous pouvez install	er un certificat SSL de confiance pour PRTG à
tout moment. Pour plus d'inforr	nations, consultez la base de connaissances :
https://kb.paessler.com/en/top	ic/283
Soubaitez-vous continue	er?

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

nous sélectionnons « créer un nouvel équipement »

'accueil	Équipements	Bibliothèques	Capteurs	Alertes
er un éq	uipement			
	Ajouter un équipemen	t		
	< Annuler			
	Choisissez un group	e pour l'ajout du n	ouvel équipeme	nt
	<ul> <li>Greer un houveau groupe</li> <li>Ajouter un équipement à</li> </ul>	e un groupe déjà existant		

### on le laisseras dans le groupe par défaut



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

Paramétrages de base de	e l'équip	pement							
Nom de l'équipement 🖲	PFsense	1							
Version IP 0	<ul><li>IPv4</li><li>IPv6</li></ul>	(par défaut	)						
Adresse IPv4/Nom DNS	192.168.	10.1							
Balises 🔍	0								
Information supplément	aire sur	l'équipe	ement					Ajouter	0
Icône de l'équipement <sup>()</sup>									

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.

Informations d'identification	pour	les équipements S	SNMP
-------------------------------	------	-------------------	------

$\mathcal{D}$	hériter de 📄 1er groupe (Versio	n SNMP: V2, Port SNMP: 161, Délai d'exp)
	Version SNMP 🖲	<ul> <li>SNMP v1</li> <li>SNMP v2c (par défaut)</li> <li>SNMP v3</li> </ul>
	Chaîne de communauté 🖲	Ig
	Port SNMP	161
	Délai d'expiration (s) 🖲	5

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

	Services 🗸	VPN 🗸
	Auto Config Ba	ckup
	Captive Portal	
	DHCP Relay	
5	DHCP Server	
	DHCPv6 Relay	
	DHCPv6 Server	r 📕
	DNS Forwarder	
at	DNS Resolver	
	Dynamic DNS	
	IGMP Proxy	
	NTP	
	PPPoE Server	
	Router Advertis	sement
	SNMP	
	UPnP & NAT-PI	MP
	Wake-on-LAN	

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

SNMP Daemon	
Enable	Enable the SNMP Daemon and its controls
SNMP Daemon Settin	ngs
Polling Port	161 Enter the port to accept polling events on (default 161).
System Location	
System Contact	
Read Community String	Ig The community string is like a password, restricting access to querying SNMP to hosts knowing the com protect from unauthorized information disclosure.

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



⊖ Ping	O Reniflage de paq
SNMP	O Protocoles de flu
О wmi	
O Compteurs de performance	O Récepteur de me
Онттр	O PRTG Cloud
() ssh	

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

Ajouter un capteur à l'équi	pement PFsense1 [192.168.10.1]	(Étape 2 à 2)	
< Annuler			1
Paramètres de base du ca	pteur		
Nom du capteur 🎱	Charge CPU (SNMP)		
Balises parentes 💿			
Balises 🖲	snmp x cpu x cpuloadsensor x		
Priorité <sup>()</sup>	****	Créer	q

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

Vue d'ensemble	(•)) Données en temps réel	2 Jours	<b>30</b> Jours	365 Jours	Données historiques	E Log	Paramètres
Total		Processor 1	0	Processor 2	Processor 3		
		0 %	0.1	0 %	0%	01	E.
		Processor 4		Processor 5	Processor 6		
		0 %	0.1	0 %	0%		<u>F</u>
		Processor 7		Processor 8			
0 %	0 % 100 %	0 %	( ) 0.1	0 %	× •		

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

Recherche **Q** SNMP

### Types de capteurs les plus utilisés



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

Sélectionner toutes les interfaces connectées		Sélectionner toute	es les interfaces non connectées	Désélectionner toutes les interfaces		
Numéro de l'interface			Recherche			
□ ◆ Nom	🗢 État	Débit	🗢 Туре	64 bits	Nom interne	
(001) enc0 Traffic	Non connecté		(not defined)	Oui	enc0	
(002) Io0 Traffic	Connecté		Software Loopback	Oui	lo0	
(003) pflog0 Traffic	Non connecté		(not defined)	Oui	pflog0	
(004) pfsync0 Traffic	Non connecté		(not defined)	Oui	pfsync0	
(005) hn0 Traffic	Connecté	10 GBit/s	Ethernet	Oui	hn0	
(006) hn1 Traffic	Connecté	10 GBit/s	Ethernet	Oui	hn1	

Rejets entrants et sortants

Paquets de monodiffusion entrants et sortants

### nous voyons que nos capteur ont été ajouté

Pos. 🔻	Capteur 🗢	Statut ≑	Message	Graphique	Priorité ≑	
<b>4</b> 1.	✓ Charge CPU (SNMP)	OK	ОК	Total 0 %	*****	
<b>. 4</b> 2.	? (005) hn0 Traffic	Inconnu	Pas encore de données	Trafic total Pas de donné	<b>★★★</b> ☆☆	
<b>4</b> 3.	? (006) hn1 Traffic	Inconnu	Pas encore de données	Trafic total Pas de donné	★★★☆☆	
<ul><li></li></ul>	<ul><li>? (005) hn0 Traffic</li><li>? (006) hn1 Traffic</li></ul>	Inconnu	Pas encore de données Pas encore de données	Trafic total Pas de donné Trafic total Pas de donné	<b>★★★</b> ☆☆ ★★★☆☆	

4 1 à 3 sur 3 > >>

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

O Ping	O Reniflage de paquets
O SNMP	O Protocoles de flux
O WMI	O PowerShell
O Compteurs de performance	O Récepteur de message Push
Онттр	
O SSH	



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

Paramètres de base du ca	apteur		
Nom du capteur 🕚	PING	21	
Balises parentes 🕚			
Balises 🔍	pingsensor X		
Priorité <sup>©</sup>	★★★☆☆		
Paramètres du ping			
Délai d'expiration (s) 🕚	5		Créer
Taille du paquet (en octets) 💿	32		
Méthode ping 🕚	O Envoyer un seul ping		
	Envoyer une série de requêtes ping		
Nombre de pings 💿	5		

### <u>capteur wmi :</u>

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

Paramétrages de base de l'équipement
Nom de l'équipement 🔍
SRV-V-AD-LG
Version IP 🕚
IPv4 (par défaut)
O IPv6
Adresse IPv4/Nom DNS <sup>®</sup>
WIN-JSHAQ697VQS
Balises <sup>®</sup>
0

nous nous identifierons pour le cas de windows

# Informations d'identification pour systèmes Windows

••••••
Mot de passe 💿
administrateur
Nom d'utilisateur 🖲
liviog.local
Nom de domaine ou d'ordinateur 💿
hériter de 🔚 1er groupe (Nom de domaine ou d'ordinateur: <vide>, Nom d)</vide>

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 »

# Technologie utilisée : Ping Renif SNMP Proto WMI Powe Compteurs de performance Récer HTTP PRTG SSH SSH

# Capacité disponible de multiples ? disques (WMI)

Supervise l'espace libre d'un ou plusieurs lecteurs de disque locaux (un canal par disque)

Des informations d'identification valides pour les systèmes Windows doivent être définis dans les paramètres de l'équipement ou du groupe parent.



nous pouvons garder le paramétrage par défaut



0

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

### Déclencheurs de notifications

Туре 🕇	Règle				
Déclencheur sur seuil	Lorsque le canal Espace disponible C: (%) est en dessous de 10 pendant au moins 60 secondes, exécuter @ > Notification par email l'administrateur 🕜	et message Push à			
(ID: 1)	Lorsque la condition ne s'applique plus, exécuter @ > Notification par email et message Push à l'administrateur 🗹				

### 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