



PRTG

S U P E R V I S I O N

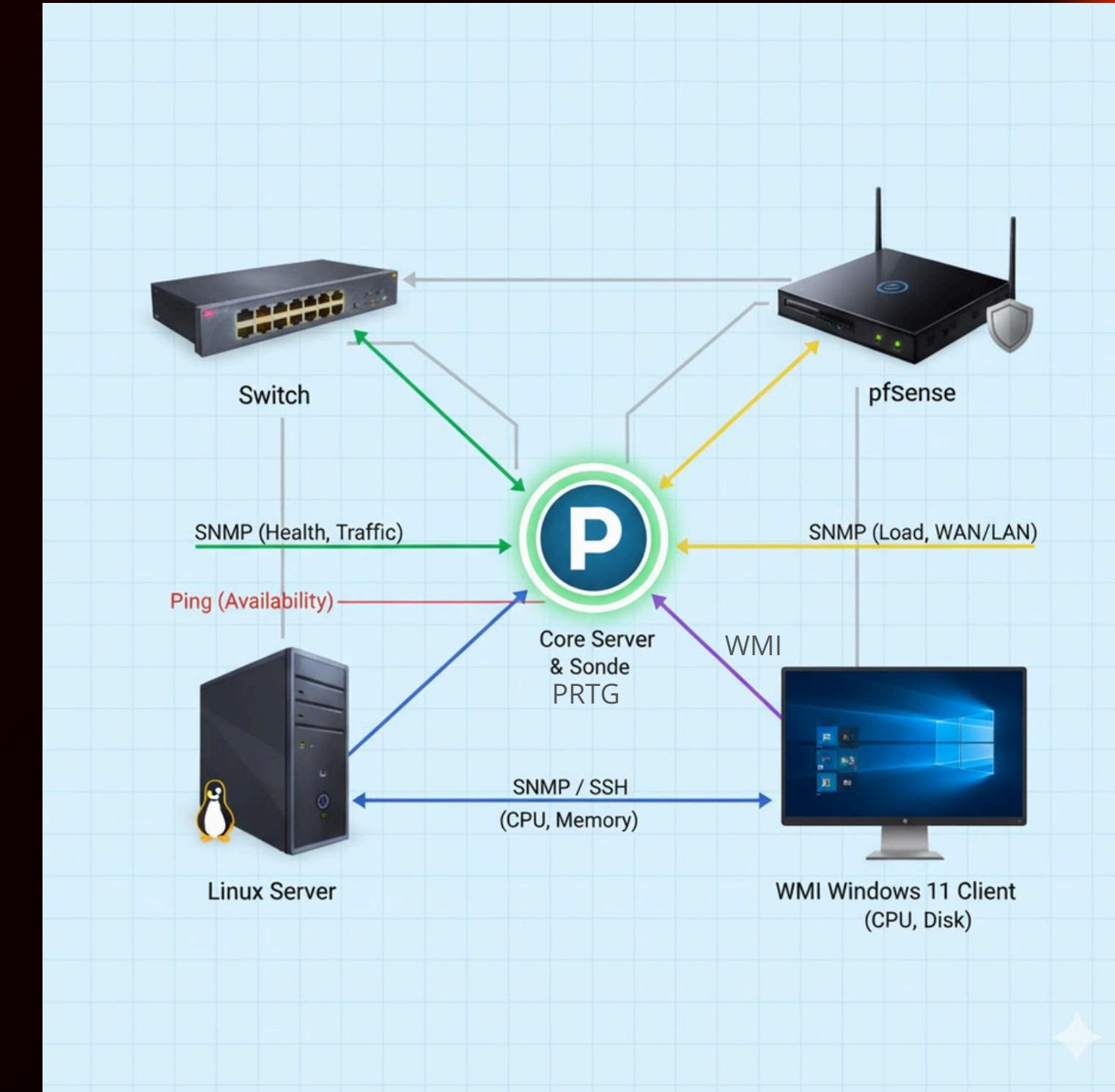


SOMMAIRE

- SCHEMA
- PRTG
- INSTALLATION
- INTERFACE
- SUPERVISER
- SUPERVISION D'UN SWITCH
- SUPERVISION D'UN POST LINUX
- SUPERVISION D'UN POST WINDOWS
- SUPERVISION D'UN PFSENSE
- NOTIFICATION



SCHEMA



PRTG

01

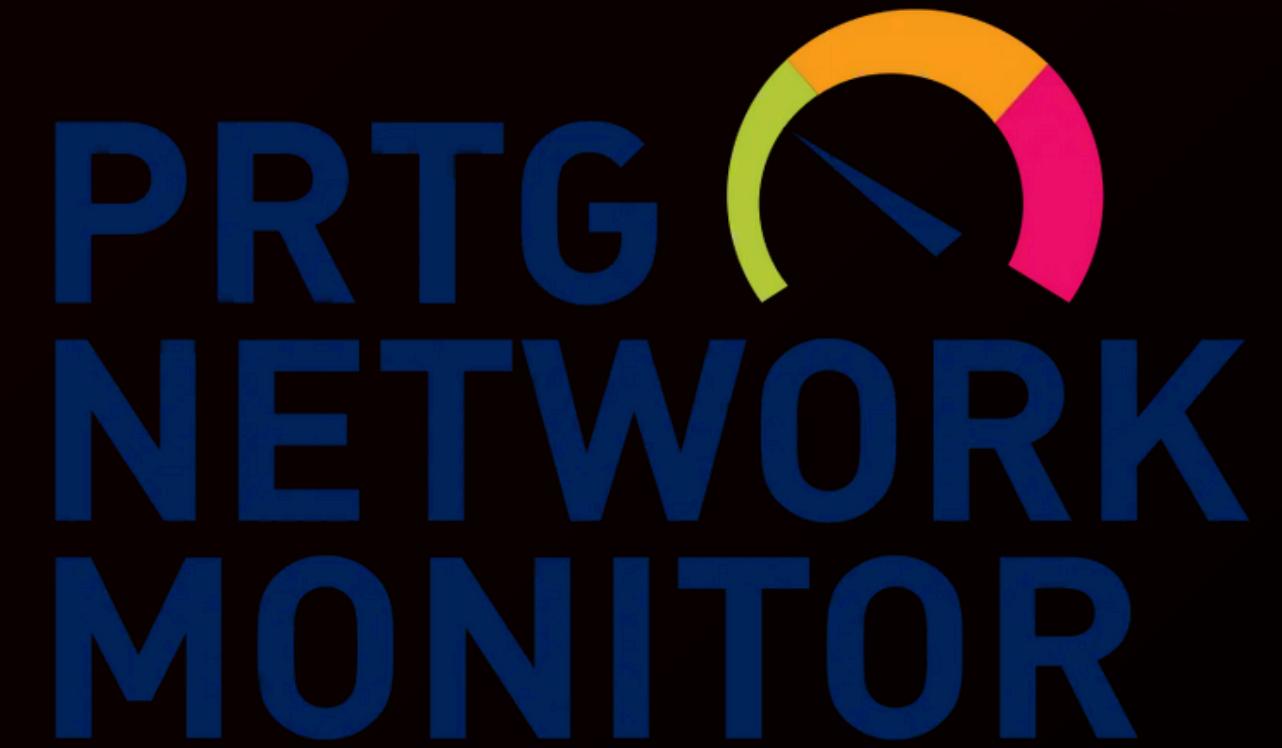
Simplicité et Déploiement Rapide

L'installation de PRTG est très rapide. La fonction de « découverte automatique » scanne le réseau et propose des capteurs précis (dans le sens où vous choisissez ce que vous voulez superviser, pas comme Zabbix, qui lui, avec un seul capteur, remonte toutes les informations liées à la machine, parfois des infos inutiles).

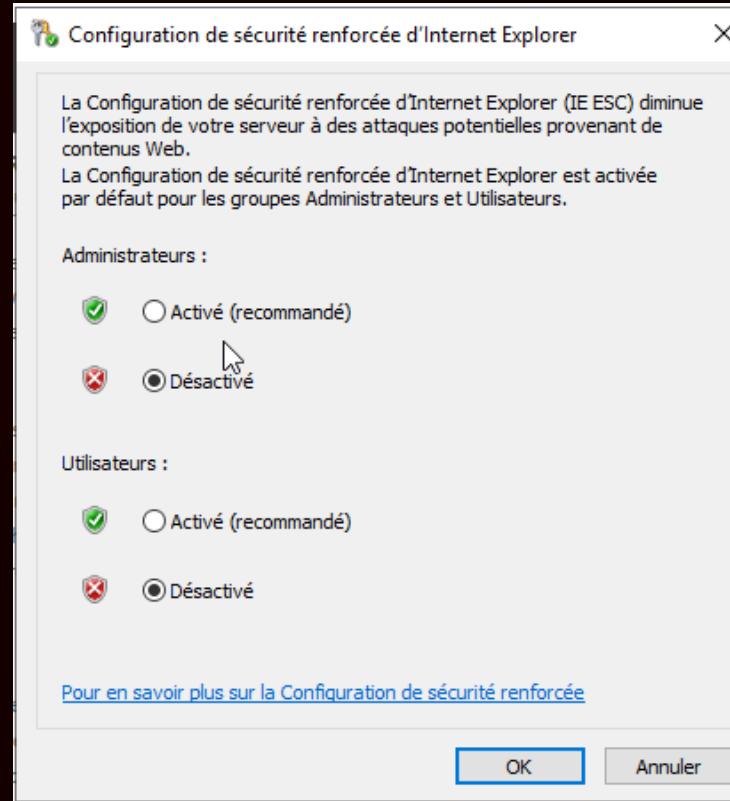
02

Tout-en-un

Contrairement à Zabbix, PRTG n'est pas un logiciel libre (open source). Seuls les 100 premiers capteurs sont gratuits, ce qui n'est malheureusement ni représentatif ni utile pour des entreprises où, parfois, deux ou trois services utilisent à eux seuls plus de 100 capteurs. Là où PRTG tire sa force, c'est dans sa simplicité d'utilisation, que nous verrons lors de cette démonstration.



04



Votre adresse email
Fournissez les informations suivantes pour poursuivre l'installation

PAESSLER
PRTG
NETWORK MONITOR

Saisissez votre adresse e-mail. PRTG enverra à cette adresse des notifications importantes pour vous alerter lorsque les capteurs de votre installation détectent des pannes, des valeurs suspectes, ou des problèmes critiques du système.

Votre adresse email :
test@test.fr

Paessler vous enverra également à cette adresse des informations sur nos produits et services. Vous pouvez à tout moment vous désinscrire de la réception de ces informations en écrivant à privacy@paessler.com. Nous protégeons vos données personnelles.
[Consultez notre politique de confidentialité pour en savoir plus.](#)

www.paessler.com [Précédent](#) [Suivant](#) [Annuler](#)

INSTALLATION

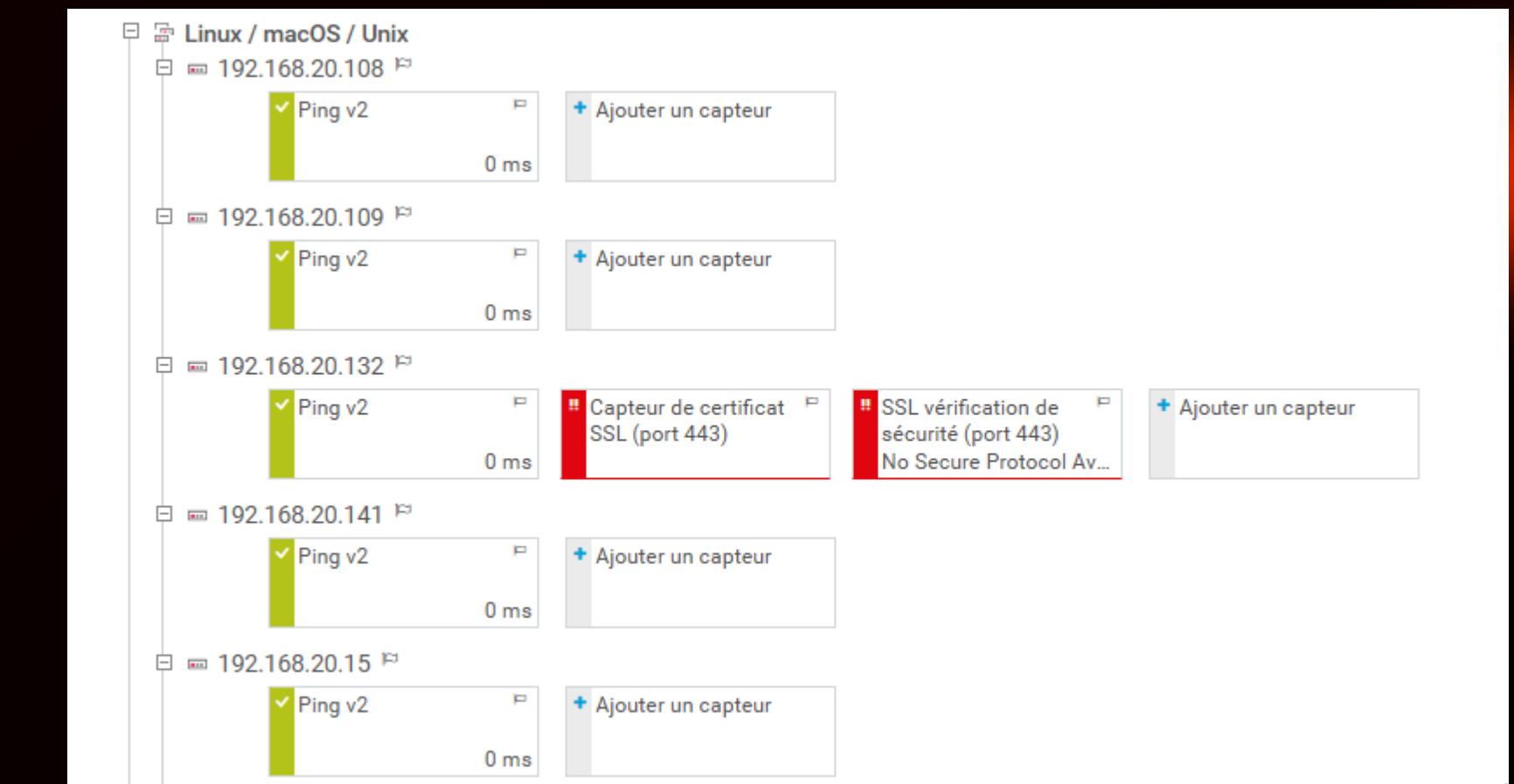
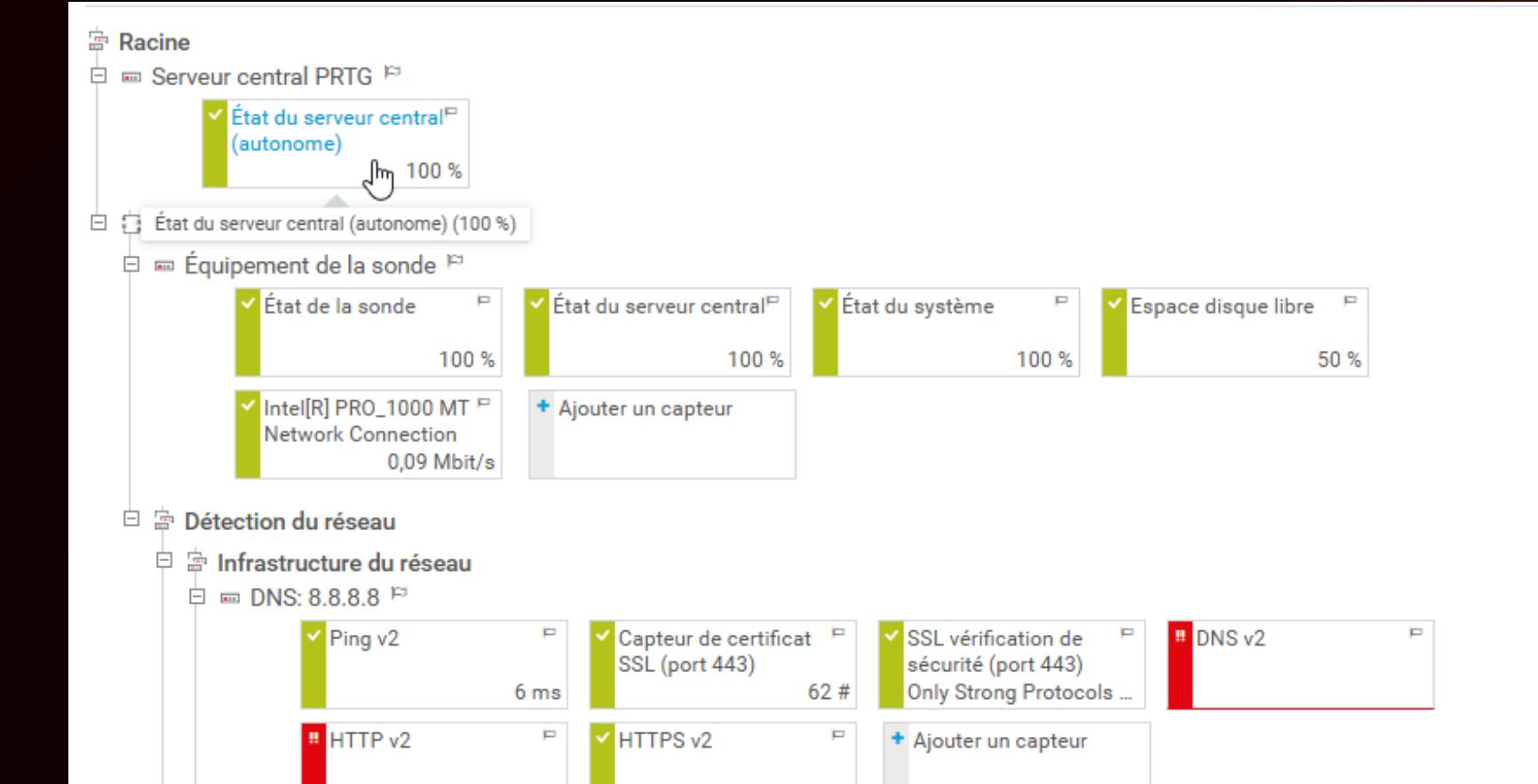
Contrairement à Zabbix, PRTG n'est pas vraiment open source, car seuls les 100 premiers capteurs sont gratuits. Malheureusement, ce n'est pas représentatif ni utile pour des entreprises où parfois deux ou trois services utilisent à eux seuls 100 capteurs. Là où PRTG tire sa force, c'est dans sa simplicité d'utilisation, que nous verrons lors de cette démonstration.

Ensuite, rendez-vous sur la page de PRTG, puis installez-le. Rentrez votre adresse mail, puis vous aurez une redirection web pour obtenir votre licence, qui dure 180 jours.

INTERFACE

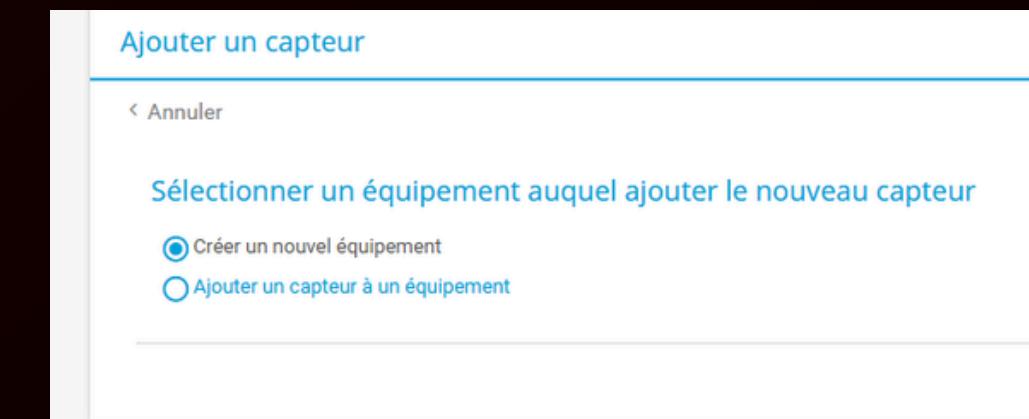
Une fois tout installé, vous allez pouvoir avoir accès à votre supervision. Ici, PRTG scanne tout le réseau, et quand je dis tout le réseau, c'est vraiment tous les composants du réseau qui répondent au ping de PRTG.

Cet outil de supervision va frapper à la porte de tous les PC, switchs et imprimantes du réseau. Si le ping envoyé est reçu, alors PRTG l'intègre sur votre interface de supervision.

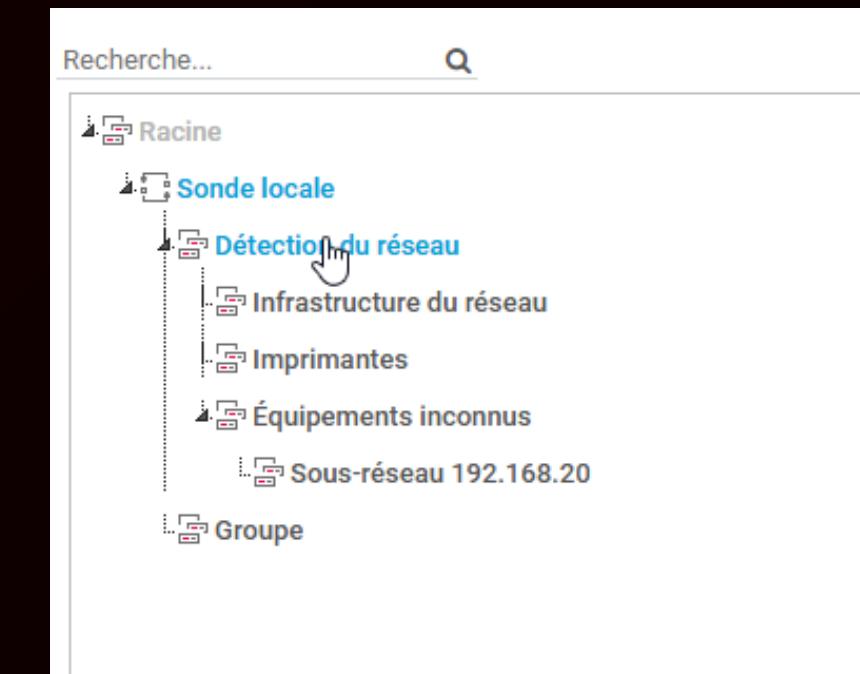


SUPERVISER

Ici, j'effectue une démonstration applicable à tout autre type de machine (Linux, Windows, etc., que l'on verra par la suite).



Premièrement, dans l'onglet Capteur de votre interface PRTG, cliquez sur Ajouter un capteur, sélectionnez « Créer un nouvel équipement ».



Puis sélectionnez la sonde (ou la zone) dans laquelle vous pourrez superviser votre switch.

Ajouter un équipement au groupe Sonde locale

Annuler la création de l'équipement

Paramétrages de base de l'équipement

Nom de l'équipement	Switch 1
Version IP	<input checked="" type="radio"/> IPv4 (par défaut) <input type="radio"/> IPv6
Adresse IPv4/Nom DNS	192.168.50.200
Balises	<input type="button" value="+"/>

Ajouter

Et enfin, donnez-lui un nom, puis rentrez l'adresse IP du switch.

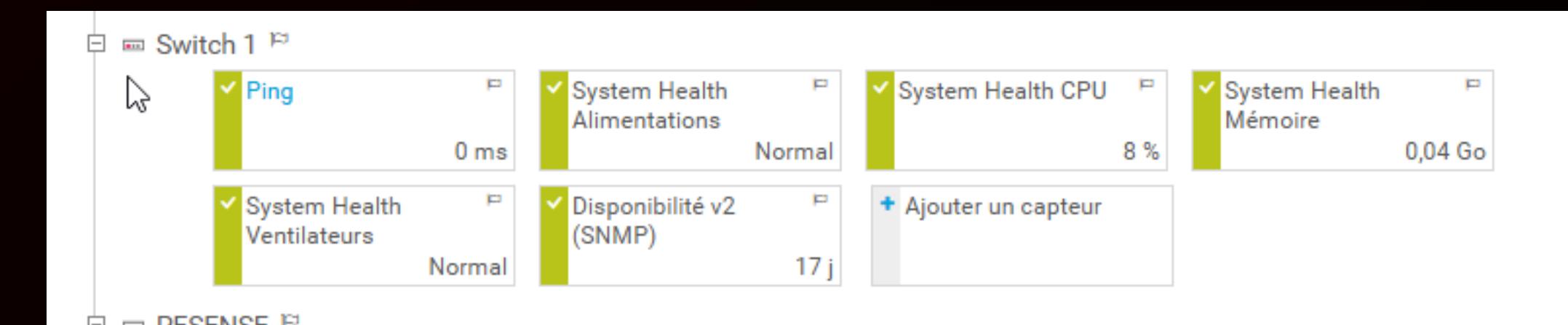
SUPERVISION D'UN SWITCH

Pour la supervision d'un switch rien de plus simple

Il faut bien entendu activer le snmp sur notre machine

snmp-server community Prive ro

Ici est mon nom (mot de passe) de la communauté



LES CAPTEURS D'UN SWITCH

Capteur	Protocole Typique	Utilité et Surveillance	Utilité
Disponibilité (Temps de fonctionnement / Uptime)	SNMP	Mesure la durée écoulée depuis le dernier démarrage de l'équipement. Indispensable pour détecter un redémarrage non planifié ou une instabilité.	Utilisation du processeur et détails des cœurs.
System Health Alimentations	SNMP (ou WMI/Propriétaire)	Surveille l'état du bloc d'alimentation (PSU). Alerte en cas de panne, de mode dégradé, ou de perte de redondance (si plusieurs alimentations).	Utilisation de la mémoire physique et du fichier d'échange (pagefile).
System Health CPU	SNMP (ou WMI/SSH)	Mesure le taux d'utilisation du processeur. Déetecte la saturation (charge élevée) qui pourrait affecter les performances de traitement du réseau.	Surveillance de l'espace disque libre (pour C:, D:, etc.).
System Health Mémoire	SNMP (ou WMI/SSH)	Surveille l'utilisation de la mémoire vive (RAM). Alerte si la mémoire est pleine, ce qui peut entraîner des problèmes de stabilité du système d'exploitation du switch/serveur.	Surveille l'état critique des services Windows (Ex: Spouleur d'impression, SQL Server).
System Health Ventilateurs	SNMP (ou WMI/Propriétaire)	Vérifie la vitesse et l'état des ventilateurs de refroidissement. Indique un risque de surchauffe ou une panne de ventilateur, souvent précurseur d'une panne matérielle.	Surveille l'état des ventilateurs, des alimentations et de la température (si le matériel est compatible WMI).

SUPERVISION D'UN POST LINUX

On utilise le protocole SSH pour une machine Linux.

Il faut bien entendu activer le SSH sur notre machine.

apt install openssh-server

Dans ma situation, j'utilise le compte root pour me connecter en SSH. Cependant, dans un environnement réel d'entreprise, il est crucial de créer un utilisateur dédié pour le partage entre PRTG et la machine surveillée (par exemple, prtg_moniteur ou ssh_admin, peu importe le nom). Cette pratique est une question de sécurité fondamentale.

J'ai donc autorisé les connexions root.

nano /etc/ssh/sshd.config

PermitRootLogin Yes

TRES IMPORTANT

Sur PRTG, une fois dans la configuration de l'équipement LINUX

The screenshot shows the PRTG Network Monitor interface. In the top navigation bar, 'Équipements' is selected. Below it, 'Linux' is chosen from a dropdown menu. The main area is titled 'Équipement Linux'. It features a 'Vue d'ensemble' tab which is currently active, along with tabs for '2 Jours', '30 Jours', and '365 Jours'. There are also buttons for 'Alarmes', 'Informations système', 'Log', 'Paramètres', and 'Déclencheur'. A search bar at the bottom right contains the text 'Find out how to make the ...'.

This screenshot shows the 'Informations d'identification pour les systèmes Linux/Solaris/macOS (SSH/WBEM)' configuration dialog. It includes fields for 'Nom d'utilisateur' (root), 'Méthode d'authentification' (Mot de passe (par défaut)), 'Mot de passe' (redacted), 'Protocole WBEM' (HTTPS), and 'Port WBEM' (Par défaut).

The screenshot displays a list of sensors for a 'Linux' device. The sensors listed are: Ping, Espace disque disponible (SSH), Charge moyenne v2 (SSH), and Information mémoire v2 (SSH). Each sensor has a green status icon and a value displayed next to it: 0 ms, 23 Go, 0,08, and 73 % respectively. A button at the bottom left says '+ Ajouter un capteur'.

Et il ne reste plus qu'à ajouter les capteurs que l'on désire.

LES CAPTEURS LINUX

Catégorie	Capteur Recommandé	Protocole Typique	Utilité et Surveillance
Disponibilité	Ping	ICMP	Vérifie l'accessibilité et la latence du serveur en temps réel.
Stockage	Espace Disque Disponible	SNMP ou SSH	Critique : Mesure l'espace libre sur les points de montage (/, /var, /home) pour éviter la saturation du système.
Performance CPU	Charge Moyenne (Load Average)	SNMP ou SSH	Surveille l'état d'occupation du processeur et des processus en attente d'exécution sur 1, 5 et 15 minutes.
Mémoire	Informations Mémoire	SNMP ou SSH	Mesure la RAM libre et utilisée, ainsi que l'utilisation de l'espace d'échange (Swap).

SUPERVISION D'UN POST WINDOWS

Pour un post Windows, nous devons utiliser le Protocole WMI,

TRES IMPORTANT

Sur PRTG, une fois dans la configuration de l'équipement Windows



Vous pouvez avoir un client sur un domaine ou non, par contre si vous n'arrivez pas à ajouter de capteur car ils sont grisés, c'est que PRTG n'arrive pas à récupérer les informations, optez pour un client avec un domaine

Informations d'identification pour systèmes Windows

hériter de Sonde locale (Nom de domaine ou d'ordinateur: <vide>, Nom d...)

Nom de domaine ou d'ordinateur

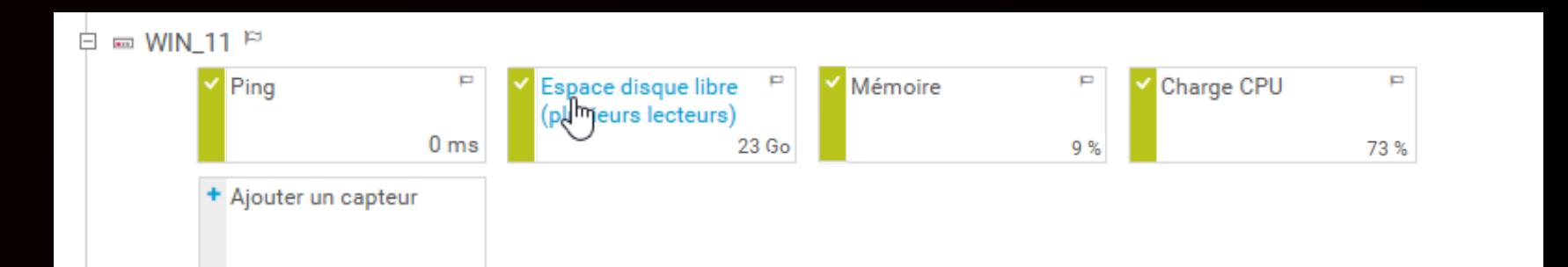
Nom d'utilisateur Administrateur

Mot de passe

Enregistrer

```
C:\Windows\System32>netsh advfirewall firewall add rule name="WMI TCP 135" dir=in action=allow protocol=TCP localport=135 remoteip=192.168.50.40
Ok.
```

Il faut autoriser le port 135 (port du WMI) depuis le Firewall sur la machine cliente, celle que l'on va superviser



LES CAPTEURS WINDOWS

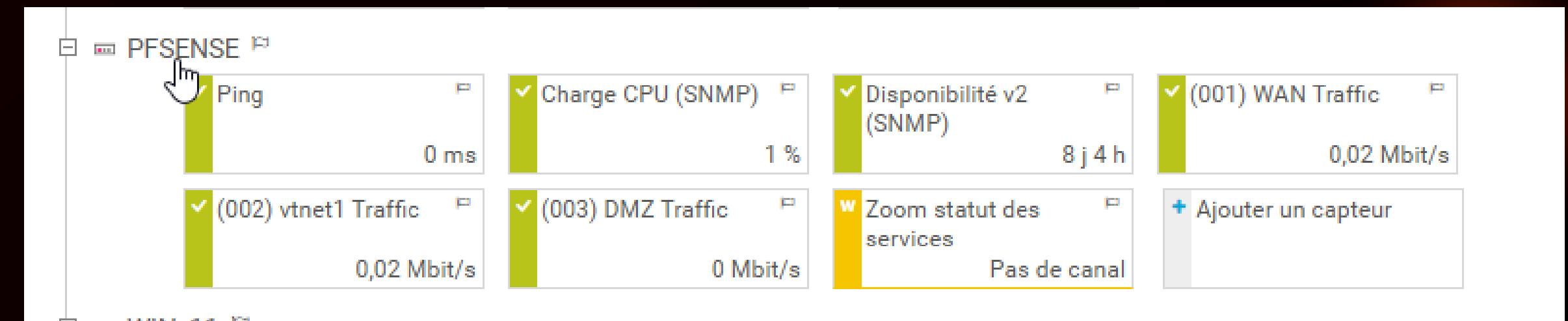
Catégorie	Capteur Recommandé	Protocole Typique	Utilité et Surveillance
Disponibilité	Ping	ICMP	Vérifie l'accessibilité et la latence du serveur en temps réel.
Stockage	Espace Disque Libre	WMI (ou SNMP)	Critique : Mesure l'espace restant sur les partitions (C:, D:).
Mémoire	Mémoire Windows (ou Mémoire Physique)	WMI (ou SNMP)	Mesure la RAM libre et utilisée, et vérifie l'utilisation du fichier d'échange (pagefile).
Performance CPU	Info CPU Windows	WMI (ou SNMP)	Mesure le taux d'utilisation du processeur. Déetecte la saturation qui peut ralentir toutes les applications.

SUPERVISION D'UN PFSENSE

Ici on utilise le protocole SNMP, comme pour le switch

Sur l'interface web du pfsense, vous devez "enable" le snmp, pour que le prtg puisse recuperer les informations

Avec Pfsense on ne s'embete pas avec des users ou domain comme avec Windows ou le ssh de linux



LES CAPTEURS PFSENSE

Capteur	Protocole Typique	Utilité et Surveillance	Utilité
Charge CPU	SNMP (ou SSH)	Mesure la charge de travail du processeur du pare-feu. Une charge élevée peut indiquer une saturation due au filtrage du trafic ou aux services VPN/Proxy.	Utilisation du processeur et détails des cœurs.
Disponibilité (Uptime)	SNMP	Mesure la durée écoulée depuis le dernier démarrage de pfSense, indiquant sa stabilité.	Utilisation de la mémoire physique et du fichier d'échange (pagefile).
Traffic Interfaces (WAN/LAN/D MZ)	Capteur Bande Passante SNMP	Mesure le débit (In/Out) sur les interfaces réseau critiques. Indispensable pour détecter la saturation de la connexion Internet (WAN) ou des liens internes.	Surveillance de l'espace disque libre (pour C:, D:, etc.).
État des Services	SNMP (ou Script)	Vérifie si les services cruciaux de pfSense sont opérationnels (Ex: DHCP, DNS Resolver, OpenVPN, etc.). S'assure que le pare-feu remplit ses fonctions.	Surveille l'état critique des services Windows (Ex: Spouleur d'impression, SQL Server).



NOTIFICATION

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
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
	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

Par défaut, il y a des notifications qui préviennent par mail ou par message push (sur l'interface) l'administrateur, mais on peut aussi personnaliser cette fonctionnalité.

Déclencheurs de notifications

Type	Règle	Actions
Déclencheur sur seuil	Lorsque le canal Free Space / (%) est égal à 10 pendant au moins 60 secondes, exécuter @ ➤ Notification par email et message Push à l'administrateur	<input checked="" type="checkbox"/> <input type="button" value="X"/>
	Lorsque la condition ne s'applique plus, exécuter @ ➤ Notification par email et message Push à l'administrateur	

Je peux ajouter, par exemple, un « seuil » pour un disque : lorsque l'espace restant atteint 10 Go pendant au moins une minute, ceci lance alors une alerte et une notification par mail est envoyée à l'administrateur.