COMPTE RENDU : SUPERVISION AVEC OBSERVIUM

21 MARS 2025

CFA UTEC
Florian Cesa

Table des matières

Compte Rendu Technique : Supervision avec Observium

Contexte de la situation :

Dans le cadre de mes missions au sein de l'entreprise **FIXIT**, il m'a été demandé de mettre en place une solution de supervision réseau centralisée. L'objectif était d'assurer un **suivi en temps réel de l'état des équipements** (serveurs, switchs, routeurs), afin d'anticiper les pannes, de garantir la **continuité de service**, et de réagir rapidement en cas d'incident.

Objectif du Projet

Mettre en place une solution de supervision réseau efficace et centralisée à l'aide d'**Observium Community Edition**, permettant le suivi en temps réel de l'état des serveurs, des périphériques réseaux et des services critiques. L'objectif est de détecter préventivement les pannes, d'optimiser la réactivité et d'automatiser les alertes afin de garantir une continuité de service optimale.

Ressources utilisées :

- **Outil de supervision** : Observium (Community Edition).
- **Environnement virtualisé** : VM sur Proxmox / VirtualBox.
- **Système** : TurnKey Linux – Observium Appliance.
- **Équipements supervisés** : 3 machines Windows, 2 machines Linux, 1 switch Cisco, 1 routeur TP-Link.
- **Protocoles utilisés** : SNMP, SMTP, Webhook JSON.
- **Utilitaires Linux** : snmpd, snmpwalk.

Présentation d'Observium

- **Type** : Outil de supervision réseau open-source.
- **Fonctionnalités** : Supervision SNMP, découverte automatique des équipements, affichage graphique via RRDTool, alertes personnalisables (e-mail, Discord).
- **Équipements compatibles** : Routeurs, switchs, serveurs (Linux, Windows), NAS, pare-feux, etc.

Installation d'Observium avec TurnKey Linux

L'installation d'Observium a été réalisée via l'image préconfigurée **TurnKey Linux - Observium Appliance**. Cette solution permet une mise en place rapide avec tous les composants requis (Apache, MySQL/MariaDB, PHP, SNMP, RRDTool) déjà intégrés.

Étapes principales :

1. **Téléchargement de l'image TurnKey Observium** depuis le site officiel.
2. **Déploiement** dans une machine virtuelle (type Proxmox, VirtualBox ou VMware).
3. **Configuration réseau** : affectation d'une IP statique.
4. **Accès à l'interface web** via l'URL : http://IP/
5. **Création du compte administrateur Observium** via la console ou le script intégré.

Configuration SNMP

Afin que les équipements soient surveillés par Observium, le protocole SNMP doit être activé sur chacun d'eux avec la communauté **bancb**.

Sur Linux (Debian 12)

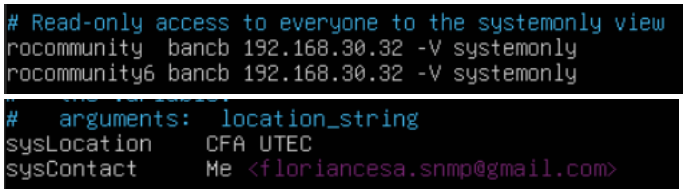
Pour permettre la supervision d'un serveur Linux, il est nécessaire d'installer les paquets SNMP, puis de configurer l'agent :

1. Installation de SNMP :

apt install snmpd snmp

2. Modification du fichier /etc/snmp/snmpd.conf :
3. rocommunity bancb <ip>
4. sysLocation CFA UTEC

   sysContact floriancesa.snmp@gmail.com

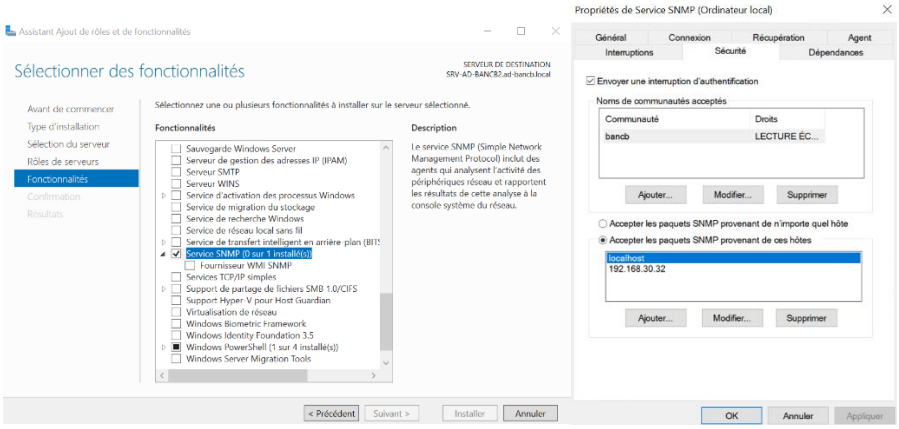


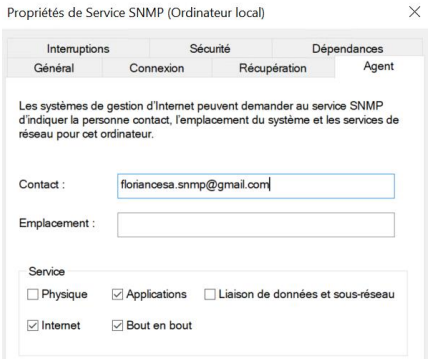
5. Redémarrage du service SNMP pour appliquer la configuration :

systemctl restart snmpd

Sur Windows

Il faut activer le service SNMP via les fonctionnalités Windows, configurer la communauté **bancb**, puis autoriser l'adresse IP du serveur Observium dans la section « hôtes acceptés ».





Sur un switch Cisco

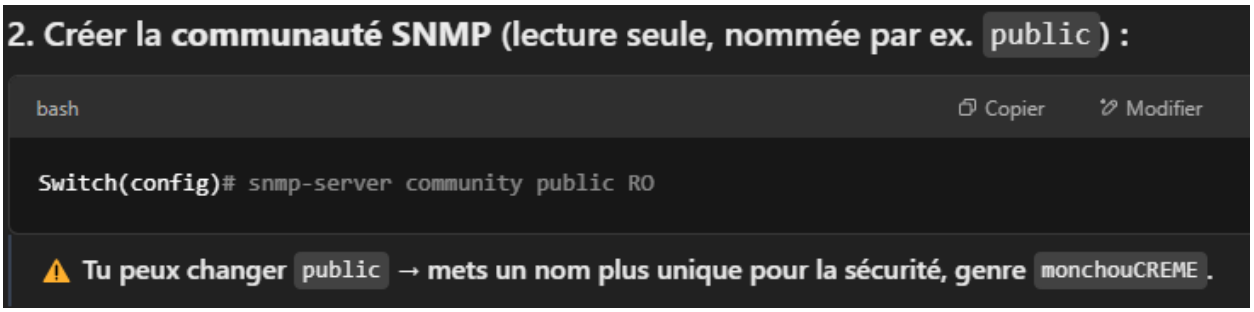
Sur un équipement Cisco, la commande suivante permet d'activer SNMP en lecture seule :

conf t

snmp-server community bancb RO

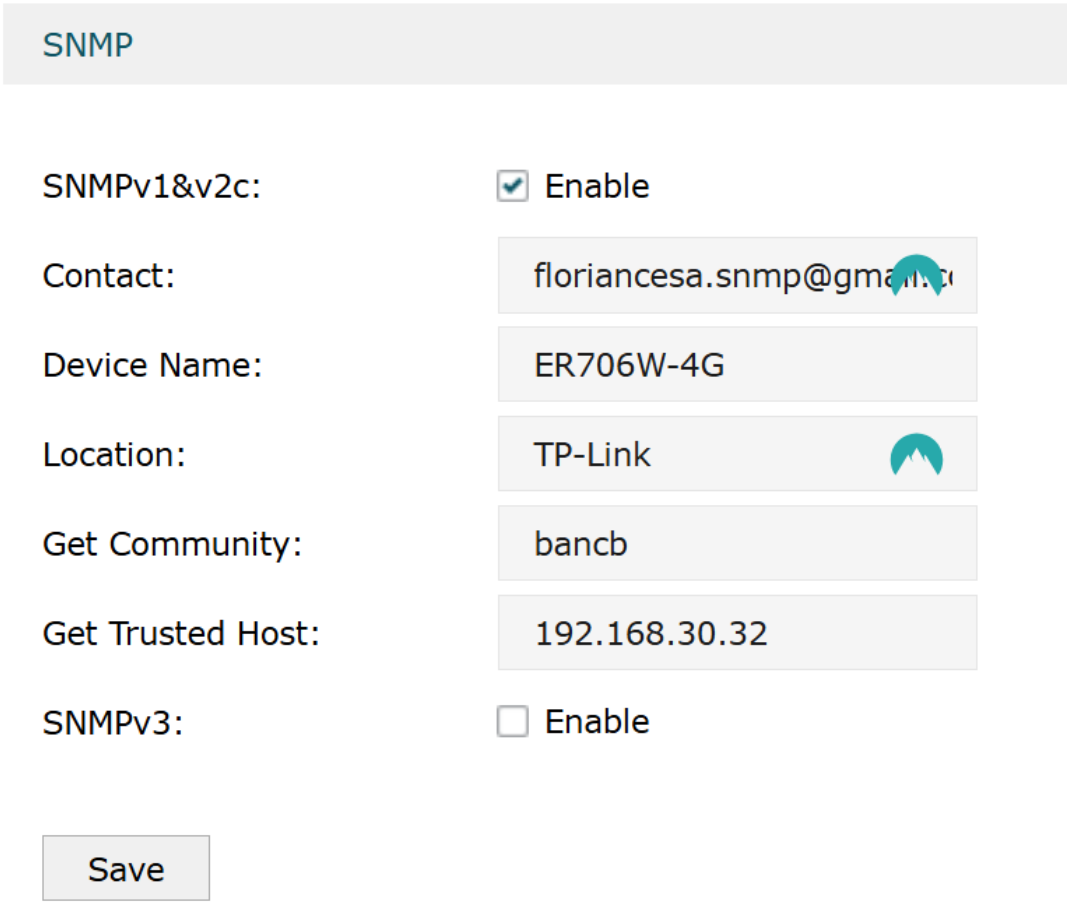
snmp-server location CFA UTEC

snmp-server contact floriancesa.snmp@gmail.com



Sur un routeur TP-Link

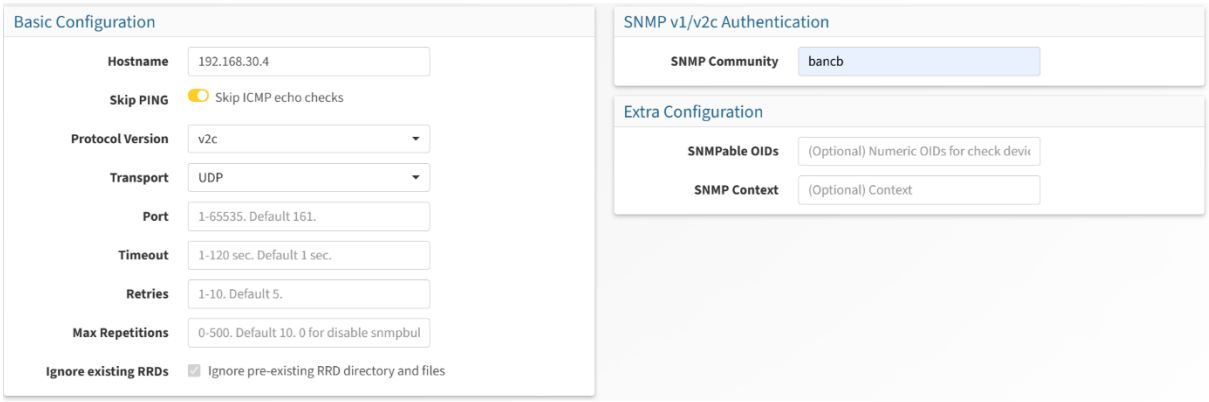
Depuis l'interface web du routeur TP-Link, il suffit d'activer le service SNMP, puis de définir la communauté **bancb** dans les paramètres appropriés.



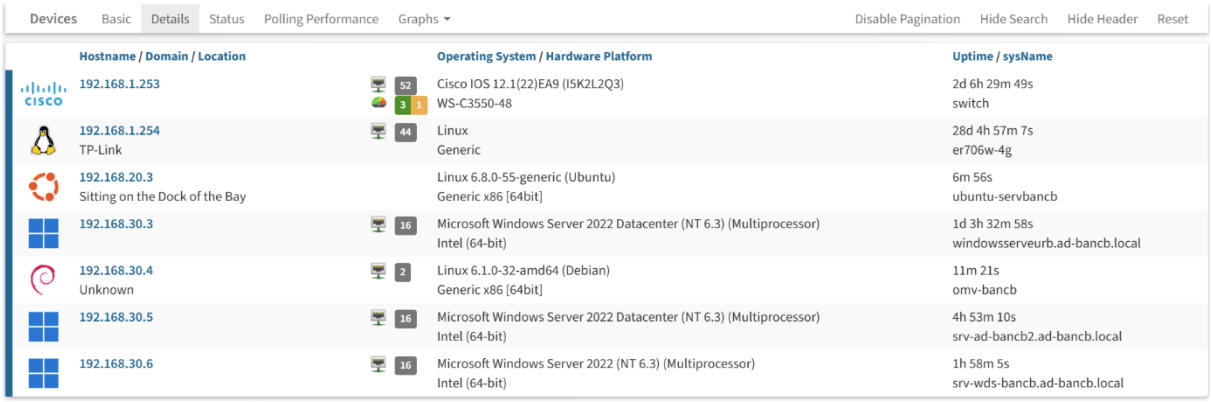
Ajout des Équipements dans Observium

L'ajout des périphériques à superviser se fait directement via l'interface web :

1. Accéder au menu **Devices > Add Device**.
2. Renseigner l'adresse IP du périphérique et la communauté SNMP (**bancb**).
3. Valider l'ajout : Observium découvre automatiquement l'équipement et récupère les informations disponibles (CPU, RAM, stockage, uptime, interfaces réseau, etc.).



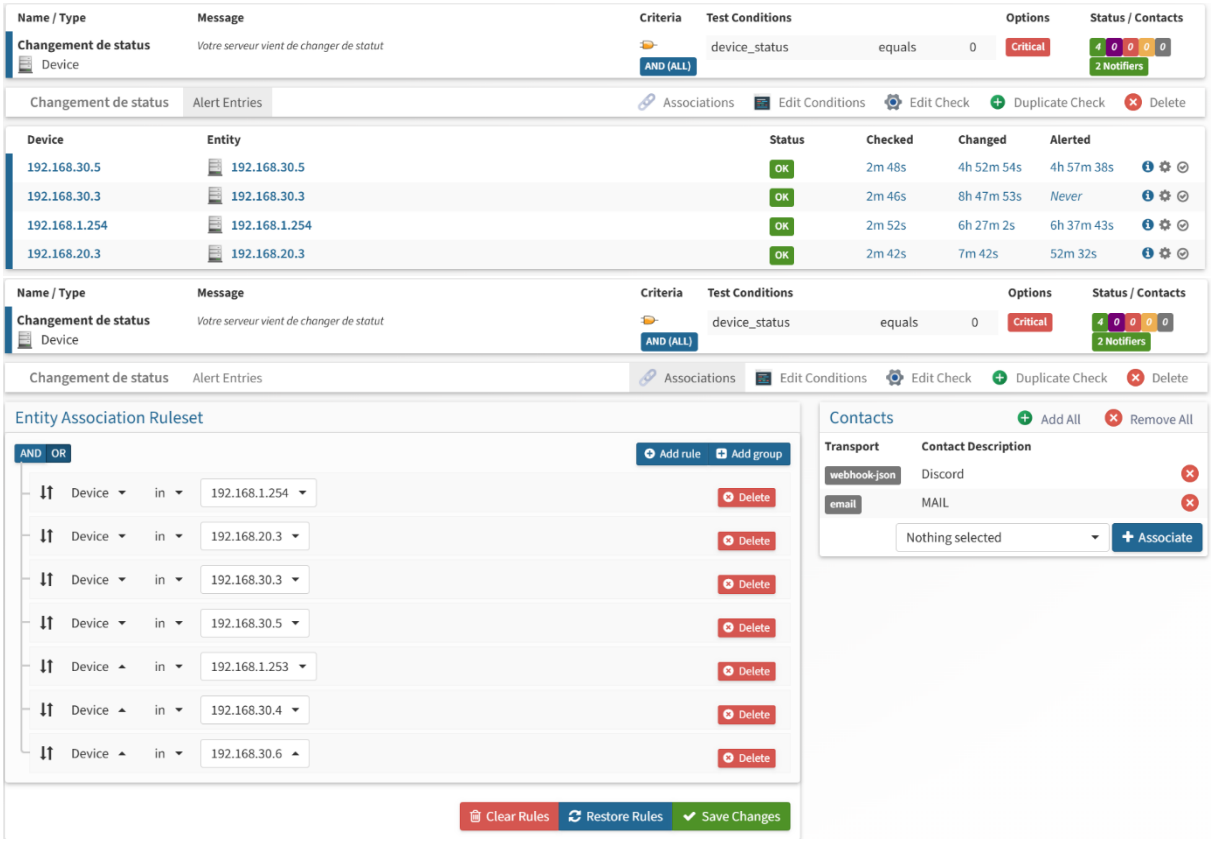
4. Ici, on peut voir que j'ai ajouté 7 machines sur Observium, 3 Windows, 2 linux. 1 TP-Link et 1 switch cisco.



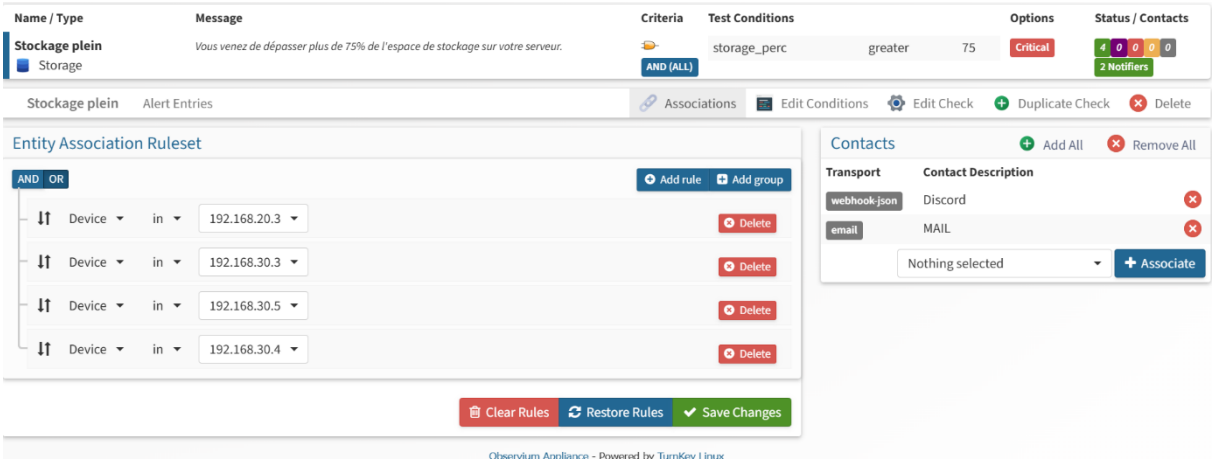
Gestion des Alertes Personnalisées

Observium permet de définir des alertes conditionnelles sur les équipements, afin d'être notifié en cas de dépassement de seuil ou de dysfonctionnement. Voici les principales alertes configurées :

- Une alerte est déclenchée lorsque **le serveur devient injoignable**, ce qui signifie que le statut de l'équipement est égal à 0 (device_status = 0).

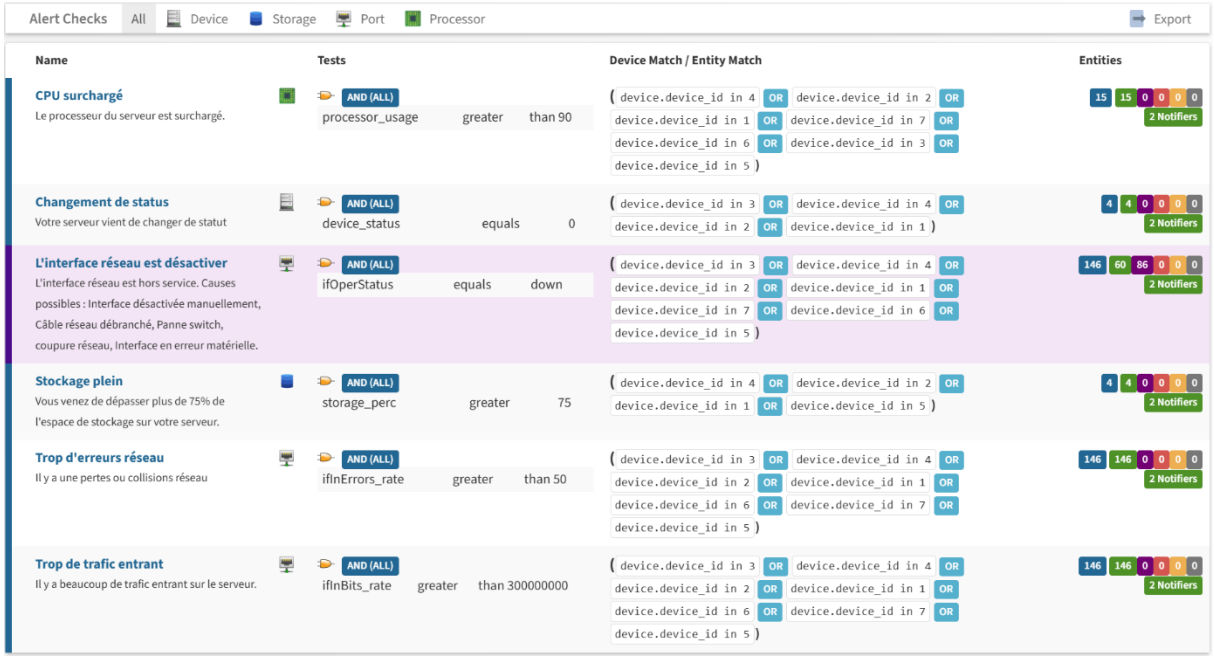


- Une autre alerte prévient lorsque **l'espace disque dépasse 75% d'utilisation** sur un serveur, grâce à la métrique storage_perc > 75%.



- Afin de surveiller le trafic, une alerte est générée si **le débit entrant dépasse 3 Gbps**, ce qui correspond à la condition ifInBits_rate > 3000000000.
- Une alerte est également prévue pour détecter si **une interface réseau est désactivée**, via la condition ifOperStatus = down.
- Concernant les performances, une alerte est levée si **l'utilisation CPU dépasse 90%**, à l'aide de la métrique processor_usage > 90%.
- Enfin, une alerte signale la présence d'**erreurs réseau** dès que plus de 50 erreurs par seconde sont détectées sur une interface, selon la condition ifInErrors_rate > 50.

- Voici tous les alertes que j'ai créer sur Observium, avec l'association des machines.

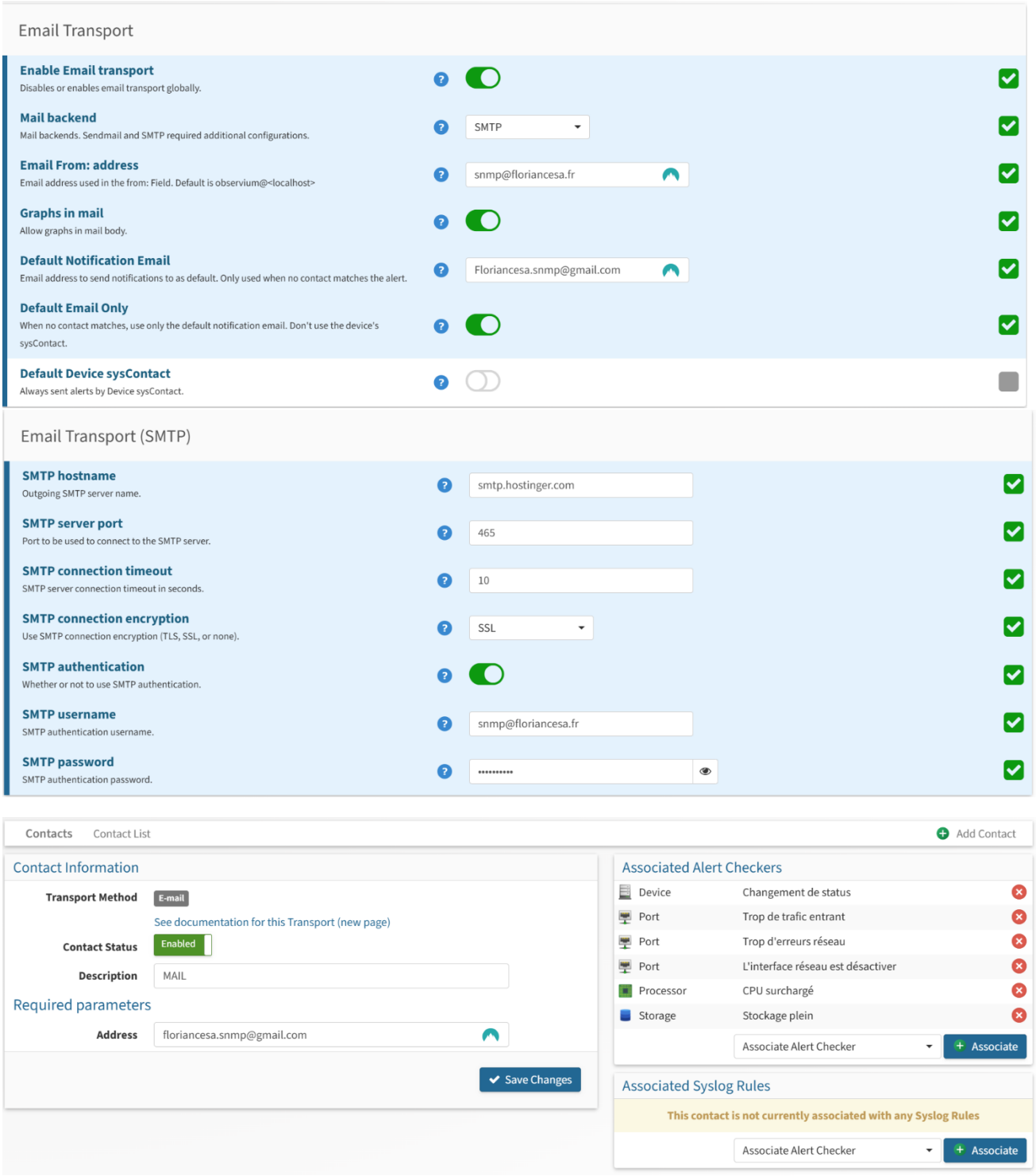


Envoi des alertes par E-mail

Pour recevoir les alertes par courrier électronique, Observium a été configuré pour utiliser un serveur SMTP externe fourni par Hostinger.

- **Serveur SMTP** : smtp.hostinger.com
- **Port utilisé** : 465 avec chiffrement SSL
- **Authentification** : activée avec l'adresse snmp@floriancesa.fr
- **Adresse de réception par défaut** : floriancesa.snmp@gmail.com

Chaque alerte est envoyée sous forme d'e-mail détaillé, incluant l'adresse IP du périphérique, la métrique concernée, la durée de l'alerte et l'état actuel de l'équipement.

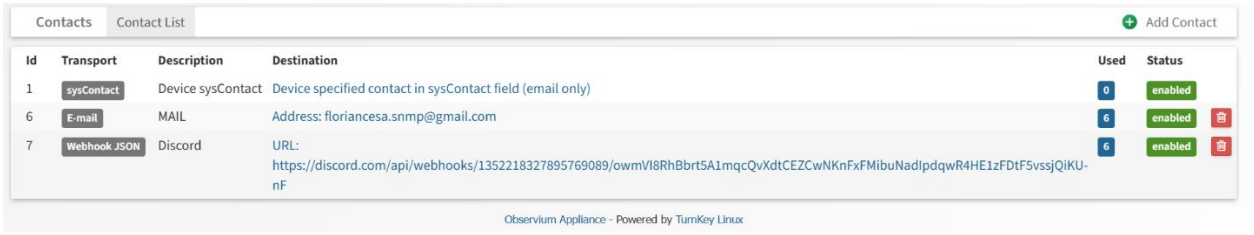

Email Transport
Enable Email transport
Disables or enables email transport globally.
Mail backend
Mail backends. Sendmail and SMTP required additional configurations.
SMTP
Email From: address
Email address used in the from: Field. Default is observium@<localhost>
snmp@floriancesa.fr
Graphs in mail
Allow graphs in mail body.
Default Notification Email
Email address to send notifications to as default. Only used when no contact matches the alert.
Floriancesa.snmp@gmail.com
Default Email Only
When no contact matches, use only the default notification email. Don't use the device's sysContact.
Default Device sysContact
Always sent alerts by Device sysContact.
Email Transport (SMTP)
SMTP hostname
Outgoing SMTP server name.
smtp.hostinger.com
SMTP server port
Port to be used to connect to the SMTP server.
465
SMTP connection timeout
SMTP server connection timeout in seconds.
10
SMTP connection encryption
Use SMTP connection encryption (TLS, SSL, or none).
SSL
SMTP authentication
Whether or not to use SMTP authentication.
SMTP username
SMTP authentication username.
snmp@floriancesa.fr
SMTP password
SMTP authentication password.
Contacts
Contact List
Add Contact
Contact Information
Transport Method
E-mail
See documentation for this Transport (new page)
Contact Status
Enabled
Description
MAIL
Required parameters
Address
floriancesa.snmp@gmail.com
Save Changes
Associated Alert Checkers
Device
Changement de status
Port
Trop de trafic entrant
Port
Trop d'erreurs réseau
Port
L'interface réseau est désactiver
Processor
CPU surchargé
Storage
Stockage plein
Associate Alert Checker
Associate
Associated Syslog Rules
This contact is not currently associated with any Syslog Rules
Associate Alert Checker
Associate

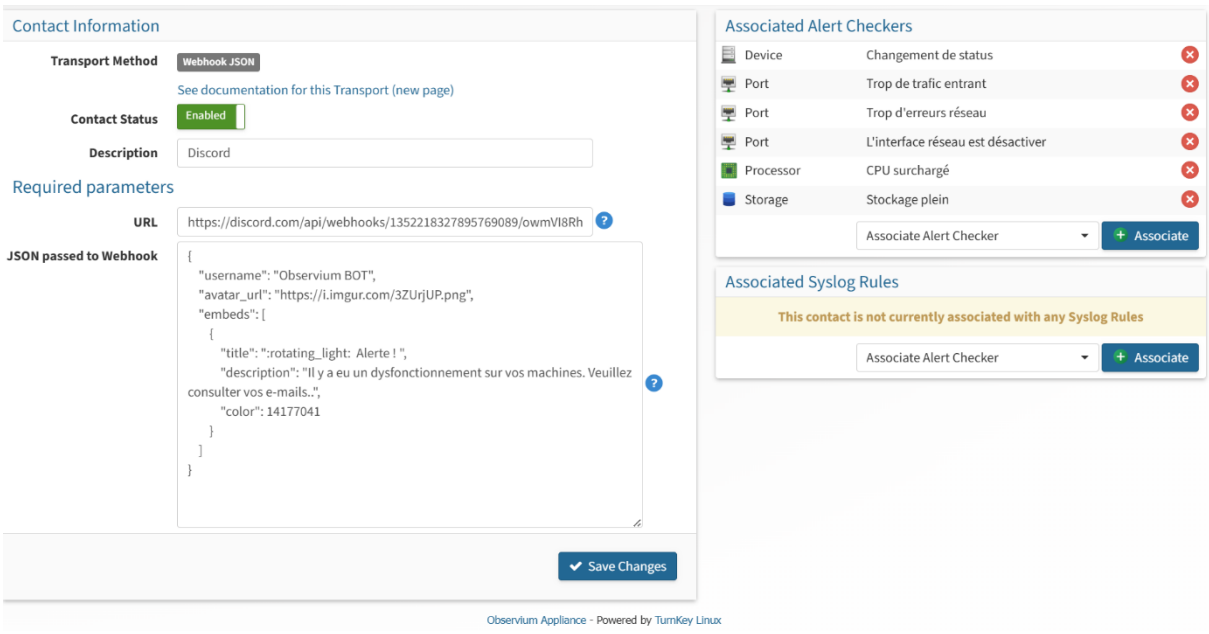
Envoi des alertes sur Discord (Webhook JSON)

En complément du courriel, les alertes critiques sont envoyées sur un serveur Discord via Webhook, pour un affichage immédiat. Cela permet d'être tenu au courant directement, car Discord est une messagerie instantanée.

Étapes de configuration :

1. Création d'un webhook dans un salon Discord, récupération de l'URL.
2. Ajout dans Observium d'un **contact de type Webhook JSON** avec cette URL.
3. Personnalisation du message en JSON avec un embed visuel.





Exemple de message JSON envoyé :

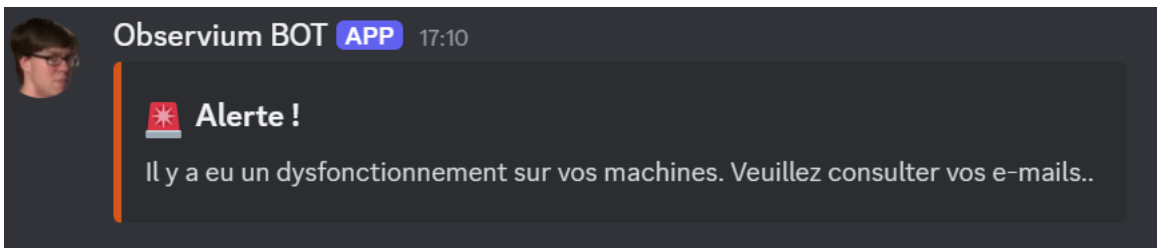

```
{
 "username": "Observium BOT",
 "avatar_url": "https://i.imgur.com/3ZUrjUP.png",
 "embeds": [
  {
   "title": ":rotating_light: Alerte !",
   "description": "Il y a eu un dysfonctionnement sur vos machines. Veuillez consulter vos e-mails..",
   "color": 14177041
  }
 ]
}
```

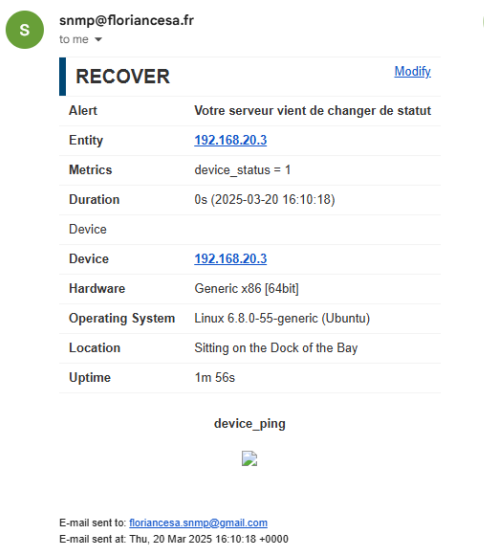

Ce message est reçu instantanément sur Discord sous forme d'alerte visuelle.

Tests et Résultats

Des tests ont été effectués pour valider la réception des alertes sur les deux canaux :

- Les **e-mails d'alerte** ont été reçus avec succès, détaillant les informations critiques.
- Les **notifications Discord** ont bien été transmises sous forme d'embed, assurant une visibilité rapide.
- Les **graphes** générés pour chaque périphérique permettent une surveillance efficace des ressources et du trafic.
- La supervision SNMP a été validée pour l'ensemble des équipements grâce à la commande snmpwalk.





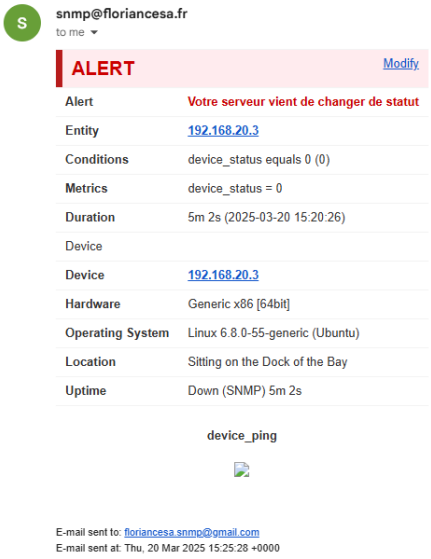
snmp@floriancesa.fr
to me

RECOVER Modify

Alert	Votre serveur vient de changer de statut
Entity	192.168.20.3
Metrics	device_status = 1
Duration	0s (2025-03-20 16:10:18)
Device	
Device	192.168.20.3
Hardware	Generic x86 [64bit]
Operating System	Linux 6.8.0-55-generic (Ubuntu)
Location	Sitting on the Dock of the Bay
Uptime	1m 56s

device_ping

E-mail sent to: floriancesa.snmp@gmail.com
E-mail sent at: Thu, 20 Mar 2025 16:10:18 +0000



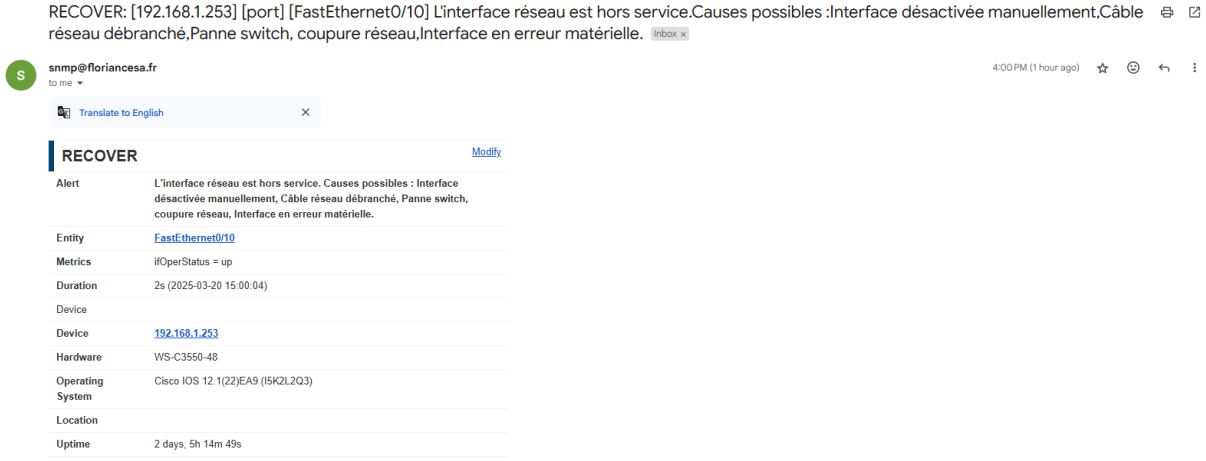
snmp@floriancesa.fr
to me

ALERT Modify

Alert	Votre serveur vient de changer de statut
Entity	192.168.20.3
Conditions	device_status equals 0 (0)
Metrics	device_status = 0
Duration	5m 2s (2025-03-20 15:20:26)
Device	
Device	192.168.20.3
Hardware	Generic x86 [64bit]
Operating System	Linux 6.8.0-55-generic (Ubuntu)
Location	Sitting on the Dock of the Bay
Uptime	Down (SNMP) 5m 2s

device_ping

E-mail sent to: floriancesa.snmp@gmail.com
E-mail sent at: Thu, 20 Mar 2025 15:25:28 +0000



RECOVER: [192.168.1.253] [port] [FastEthernet0/10] L'interface réseau est hors service.Causes possibles :Interface désactivée manuellement,Câble réseau débranché,Panne switch, coupure réseau,Interface en erreur matérielle. Inbox ×

snmp@floriancesa.fr
to me
4:00 PM (1 hour ago)

Translate to English

RECOVER Modify

Alert	L'interface réseau est hors service. Causes possibles : Interface désactivée manuellement, Câble réseau débranché, Panne switch, coupure réseau, Interface en erreur matérielle.
Entity	FastEthernet0/10
Metrics	ifOperStatus = up
Duration	2s (2025-03-20 15:00:04)
Device	
Device	192.168.1.253
Hardware	WS-C3550-48
Operating System	Cisco IOS 12.1(22)EA9 (I5K2L2Q3)
Location	
Uptime	2 days, 5h 14m 49s

Problèmes rencontrés

- Les **variables dynamiques** d'Observium (comme %title%, %message%) ne sont **pas compatibles** avec les messages de type Webhook JSON ➜ un message générique a été mis en place.
- **Blocage SNMP** initial causé par le pare-feu ➜ une règle a été ajoutée pour autoriser le trafic SNMP (UDP 161).

Améliorations envisageables

- Mettre en place une **redondance de la supervision** avec une seconde instance Observium et synchronisation régulière (via rsync ou backup VM).
- Étendre la supervision à l'hyperviseur **Proxmox** avec alertes spécifiques sur les ressources des machines virtuelles.
- Adapter les seuils d'alerte selon les plages horaires pour éviter les faux positifs (ex : trafic élevé aux heures de pointe).

Conclusion

Observium s'est avéré être une solution robuste et simple pour la supervision réseau. Son installation via TurnKey Linux a facilité la mise en œuvre rapide de la plateforme. Grâce à SNMP, l'état des serveurs et équipements est surveillé efficacement, avec des alertes envoyées automatiquement par e-mail et Discord.

Ce projet a permis de maîtriser l'ensemble du cycle de supervision : installation, configuration SNMP, création d'alertes personnalisées, et envoi multi-canaux des notifications.

Résultat final : 100% opérationnel.