



COMPTE RENDU : SUPERVISION AVEC OBSERVIVUM



21 MARS 2025

CFA UTEC
Florian Cesa

Table des matières

Contexte de la situation :	2
Objectif du Projet	2
Ressources utilisées :	2
Présentation d’Observium	3
Installation d’Observium avec TurnKey Linux	3
Étapes principales :	3
Configuration SNMP	3
Sur Linux (Debian 12)	3
Sur Windows	4
Sur un switch Cisco	4
Sur un routeur TP-Link	5
Ajout des Équipements dans Observium	5
Gestion des Alertes Personnalisées	6
Envoi des alertes par E-mail	8
Envoi des alertes sur Discord (Webhook JSON)	10
Étapes de configuration :	10
Exemple de message JSON envoyé :	11
Tests et Résultats	11
Problèmes rencontrés	12
Améliorations envisageables	13
Conclusion	13

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>

```
# Read-only access to everyone to the systemonly view
rocommunity bancb 192.168.30.32 -V systemonly
rocommunity6 bancb 192.168.30.32 -V systemonly
```

4. sysLocation CFA UTEC

```
sysContact floriancesa.snmp@gmail.com
```

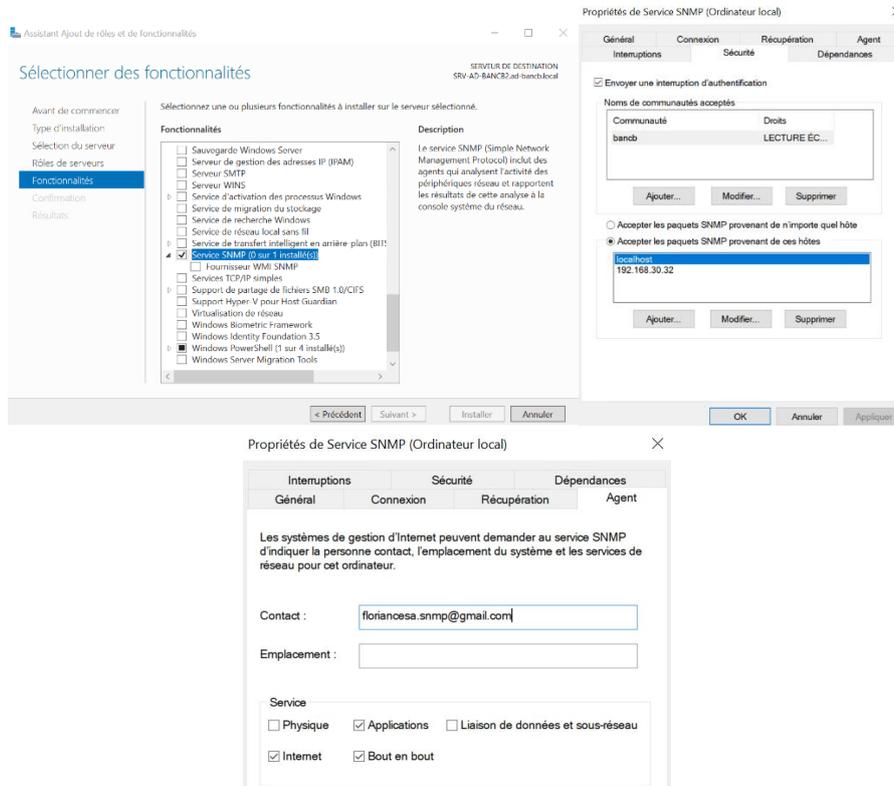
```
# arguments: location_string
sysLocation CFA UTEC
sysContact Me <floriancesa.snmp@gmail.com>
```

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
```

2. Créer la communauté SNMP (lecture seule, nommée par ex. public) :

```
bash
```

Copier

Modifier

```
Switch(config)# snmp-server community public RO
```

⚠ Tu peux changer `public` → mets un nom plus unique pour la sécurité, genre `monchouCREME` .

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.

SNMP

SNMPv1&v2c:	<input checked="" type="checkbox"/> Enable
Contact:	<input type="text" value="floriancesa.snmp@gmail.com"/>
Device Name:	<input type="text" value="ER706W-4G"/>
Location:	<input type="text" value="TP-Link"/>
Get Community:	<input type="text" value="bancb"/>
Get Trusted Host:	<input type="text" value="192.168.30.32"/>
SNMPv3:	<input type="checkbox"/> Enable

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.).

Basic Configuration

Hostname
Skip PING Skip ICMP echo checks
Protocol Version
Transport
Port
Timeout
Retries
Max Repetitions
Ignore existing RRDs Ignore pre-existing RRD directory and files

SNMP v1/v2c Authentication

SNMP Community

Extra Configuration

SNMPable OIDs
SNMP Context

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

Hostname / Domain / Location	Operating System / Hardware Platform	Uptime / sysName
192.168.1.253 Cisco	Cisco IOS 12.1(22)EA9 (ISK2L2Q3) WS-C3550-48	2d 6h 29m 49s switch
192.168.1.254 TP-Link	Linux Generic	28d 4h 57m 7s er706w-4g
192.168.20.3 Sitting on the Dock of the Bay	Linux 6.8.0-55-generic (Ubuntu) Generic x86 [64bit]	6m 56s ubuntu-servbancb
192.168.30.3	Microsoft Windows Server 2022 Datacenter (NT 6.3) (Multiprocessor) Intel (64-bit)	1d 3h 32m 58s windowsserverurb.ad-bancb.local
192.168.30.4 Unknown	Linux 6.1.0-32-amd64 (Debian) Generic x86 [64bit]	11m 21s omv-bancb
192.168.30.5	Microsoft Windows Server 2022 Datacenter (NT 6.3) (Multiprocessor) Intel (64-bit)	4h 53m 10s srv-ad-bancb2.ad-bancb.local
192.168.30.6	Microsoft Windows Server 2022 (NT 6.3) (Multiprocessor) Intel (64-bit)	1h 58m 5s srv-wds-bancb.ad-bancb.local

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).

The screenshot shows the configuration for an alert named "Changement de statut". The criteria are set to "Device" and the test condition is "device_status equals 0". The alert is critical and has 2 notifiers. Below the configuration, there is a table of alert entries:

Device	Entity	Status	Checked	Changed	Alerted
192.168.30.5	192.168.30.5	OK	2m 48s	4h 52m 54s	4h 57m 38s
192.168.30.3	192.168.30.3	OK	2m 46s	8h 47m 53s	Never
192.168.1.254	192.168.1.254	OK	2m 52s	6h 27m 2s	6h 37m 43s
192.168.20.3	192.168.20.3	OK	2m 42s	7m 42s	52m 32s

Below the table, there is an "Entity Association Ruleset" section with a list of rules:

- Device in 192.168.1.254
- Device in 192.168.20.3
- Device in 192.168.30.3
- Device in 192.168.30.5
- Device in 192.168.1.253
- Device in 192.168.30.4
- Device in 192.168.30.6

At the bottom, there are buttons for "Clear Rules", "Restore Rules", and "Save Changes".

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

The screenshot shows the configuration for an alert named "Stockage plein". The criteria are set to "Storage" and the test condition is "storage_perc greater 75". The alert is critical and has 2 notifiers. Below the configuration, there is an "Entity Association Ruleset" section with a list of rules:

- Device in 192.168.20.3
- Device in 192.168.30.3
- Device in 192.168.30.5
- Device in 192.168.30.4

At the bottom, there are buttons for "Clear Rules", "Restore Rules", and "Save Changes".

- 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.

Name	Tests	Device Match / Entity Match	Entities
CPU surchargé Le processeur du serveur est surchargé.	AND (ALL) processor_usage greater than 90	(device.device_id in 4 OR device.device_id in 2 OR device.device_id in 1 OR device.device_id in 7 OR device.device_id in 6 OR device.device_id in 3 OR device.device_id in 5)	15 15 0 0 0 0 2 Notifiers
Changement de status Votre serveur vient de changer de statut	AND (ALL) device_status equals 0	(device.device_id in 3 OR device.device_id in 4 OR device.device_id in 2 OR device.device_id in 1)	4 4 0 0 0 0 2 Notifiers
L'interface réseau est désactiver L'interface réseau est hors service. Causes possibles : Interface désactivée manuellement, Câble réseau débranché, Panne switch, coupure réseau, interface en erreur matérielle.	AND (ALL) ifOperStatus equals down	(device.device_id in 3 OR device.device_id in 4 OR device.device_id in 2 OR device.device_id in 1 OR device.device_id in 7 OR device.device_id in 6 OR device.device_id in 5)	146 50 86 0 0 0 2 Notifiers
Stockage plein Vous venez de dépasser plus de 75% de l'espace de stockage sur votre serveur.	AND (ALL) storage_perc greater 75	(device.device_id in 4 OR device.device_id in 2 OR device.device_id in 1 OR device.device_id in 5)	4 4 0 0 0 0 2 Notifiers
Trop d'erreurs réseau Il y a une pertes ou collisions réseau	AND (ALL) ifnErrors_rate greater than 50	(device.device_id in 3 OR device.device_id in 4 OR device.device_id in 2 OR device.device_id in 1 OR device.device_id in 6 OR device.device_id in 7 OR device.device_id in 5)	146 146 0 0 0 0 2 Notifiers
Trop de trafic entrant Il y a beaucoup de trafic entrant sur le serveur.	AND (ALL) ifnBits_rate greater than 300000000	(device.device_id in 3 OR device.device_id in 4 OR device.device_id in 2 OR device.device_id in 1 OR device.device_id in 6 OR device.device_id in 7 OR device.device_id in 5)	146 146 0 0 0 0 2 Notifiers

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.



Email From: address

Email address used in the from: Field. Default is observium@-localhost-



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.



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)

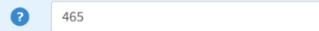
SMTP hostname

Outgoing SMTP server name.



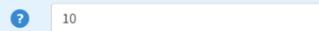
SMTP server port

Port to be used to connect to the SMTP server.



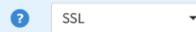
SMTP connection timeout

SMTP server connection timeout in seconds.



SMTP connection encryption

Use SMTP connection encryption (TLS, SSL, or none).



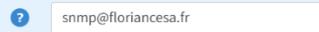
SMTP authentication

Whether or not to use SMTP authentication.



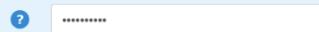
SMTP username

SMTP authentication username.



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

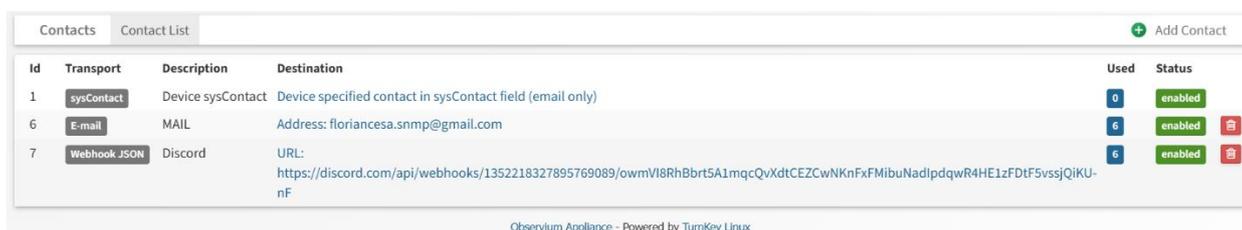
Associate Alert Checker + Associate

Envoi des alertes sur Discord (Webhook JSON)

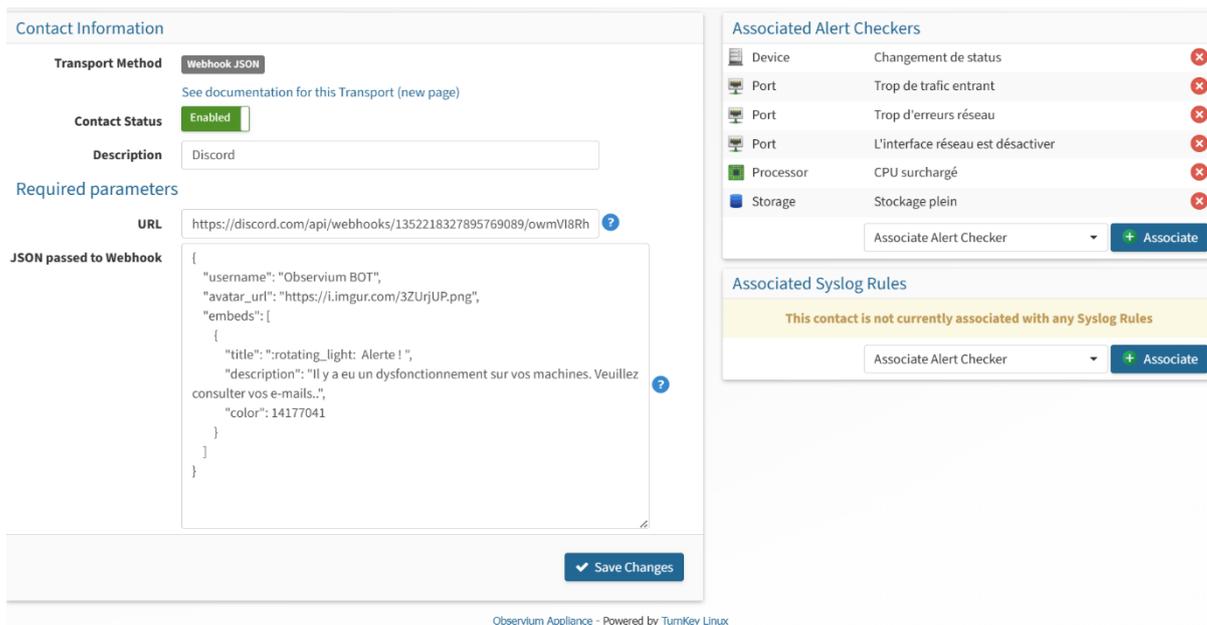
En complément du courriel, les alertes critiques sont envoyées sur un serveur Discord via Webhook, pour un affichage immédiat. Cela permet d'être tenu au courant directement, car Discord est une messagerie instantanée.

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.



Id	Transport	Description	Destination	Used	Status
1	sysContact	Device sysContact	Device specified contact in sysContact field (email only)	0	enabled
6	E-mail	MAIL	Address: floriancesa.snmp@gmail.com	6	enabled
7	Webhook JSON	Discord	URL: https://discord.com/api/webhooks/1352218327895769089/owmVl8RhBbrt5A1mqcQvXdtCEZCwNKnFxFMibuNadlpdqWR4HE1zFDtF5vssjQlKUnF	6	enabled



Contact Information

Transport Method Webhook JSON
See documentation for this Transport (new page)

Contact Status Enabled

Description Discord

Required parameters

URL https://discord.com/api/webhooks/1352218327895769089/owmVl8Rh

JSON passed to Webhook

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

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 Syslog Rule + Associate

Exemple de message JSON envoyé :

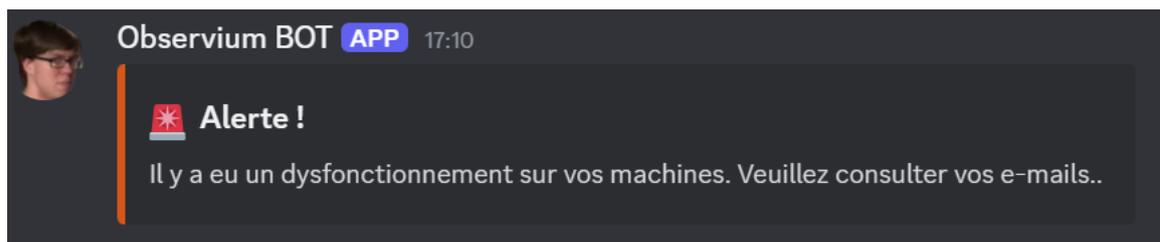
```
{
  "username": "Observium BOT",
  "avatar_url": "https://i.imgur.com/3ZUjrUP.png",
  "embeds": [
    {
      "title": ":rotating_light: Alerte !",
      "description": "Il y a eu un dysfonctionnement sur vos machines. Veuillez consulter vos e-mails..",
      "color": 14177041
    }
  ]
}
```

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

[Translate to English](#) X

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)IEA9 (15K2L2Q3)
Location	
Uptime	2 days, 5h 14m 49s

4:00 PM (1 hour ago) ☆ ☺ ↶ ⋮

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.