

ADRAR FORMATION

Mis en place de la Supervision



MARAVAL Liam
07/10/2024

Ce document sera décomposé en plusieurs chapitres :

1. Contexte : Définition des besoins ainsi que le choix des solutions en réponse à la demande client.
2. Configuration technique : Procédure technique de mise en place des solutions
3. Conclusion du projet

Table des matières

1.	Contexte	2
1.1	Demandes du client.....	2
1.2	Evolution de l'infrastructure	2
1.3	Choix de la solution	3
1.4	Sécurisation des accès.....	4
2.	Configuration technique.....	4
2.1	Supervision d'un hôte Windows	5
2.2	Supervision d'un serveur Linux	18
2.3	Supervision d'un Switch Cisco	26
3.	Conclusion	31
4.	Annexes	32

1. Contexte

1.1 Demandes du client

Nous sommes contactés par l'ADRAR afin de mettre en place une solution de supervision.

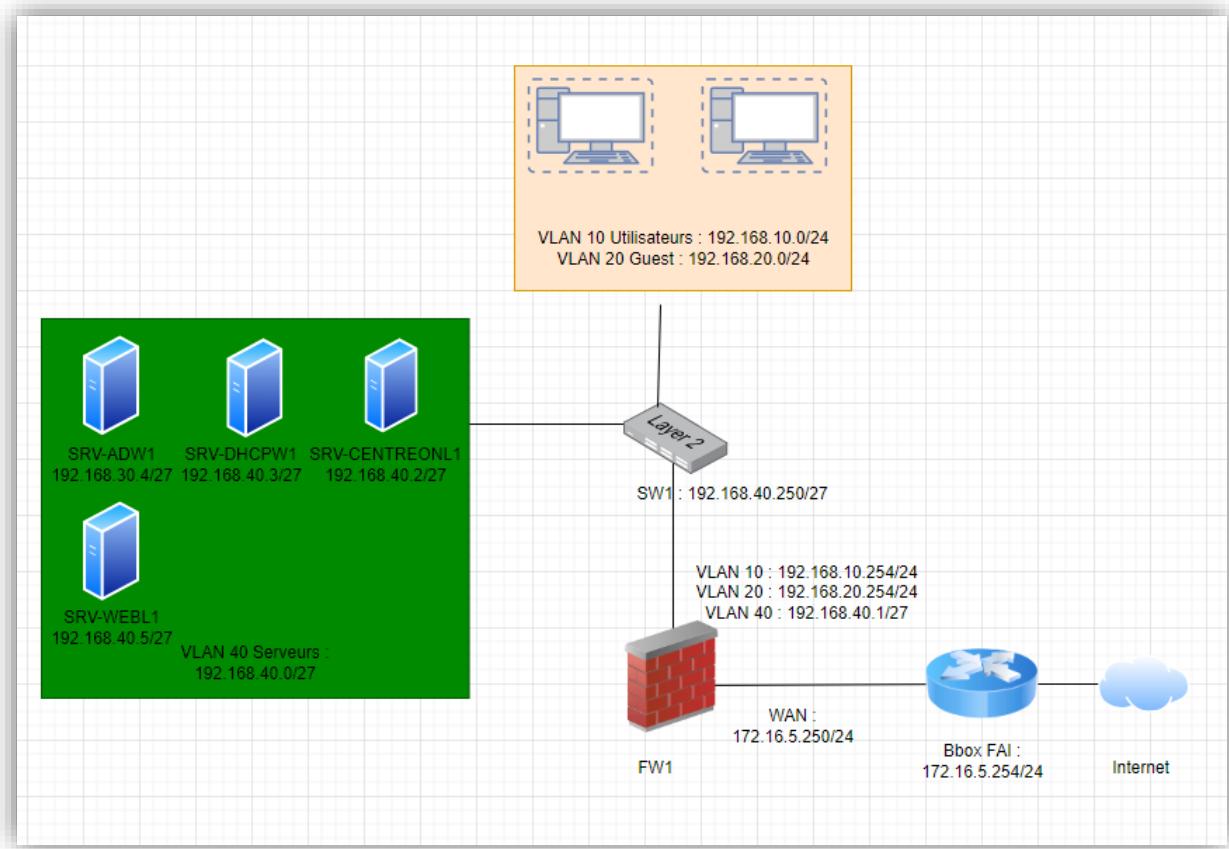
L'ADRAR a pour objectif d'implémenter ce système afin de garantir le bon fonctionnement de ses équipements et services, tout en recevant des alertes en cas de dysfonctionnement.

Voici les éléments à examiner :

- Que les équipements soient joignables par Ping
- Vérifier le RAM (avertissement si RAM restant entre 20% et 10%, critique en dessous de 10%)
- Espace disque (avertissement si espace disque restant entre 20% et 10%, critique en dessous de 10%)
- Utilisation CPU (avertissement si CPU restant entre 20% et 10%, critique en dessous de 10%)
- Service MariaDB sur un serveur Debian 12
- Service DHCP sur un Windows Server
- Les équipements actifs type switch, routeurs

1.2 Evolution de l'infrastructure

Pour mieux comprendre la mise en place de la nouvelle infrastructure, veuillez-vous référer au nouveau schéma effectué :



Afin de répondre à la demande de l'ADRAR, nous allons ajouter un serveur de supervision. Celui-ci sera en charge d'envoyer des requêtes SNMP aux différents serveurs afin de s'assurer des bons fonctionnements de la partie hardware des équipements (RAM, CPU, disques etc...) mais aussi des services qui sont hébergés sur les serveurs (MariaDB, DHCP etc...)

Pour cela, nous allons configurer des agents SNMP sur nos différents serveurs avec les informations essentielles au bon fonctionnement de la solution.

1.3 Choix de la solution

Nous avons opté pour une solution de supervision via Centreon. Voici les raisons qui ont motivé notre choix :

- Solution complète et modulaire
- Interface graphique intuitive
- Grande communauté et support actif
- Large documentation
- Flexible et évolutive
- Adapté aux environnements On-Prem et Cloud

Concernant les couts, Centreon propose une version gratuite jusqu'à 100 équipements sans limite dans le temps, ce qui suffit pour les besoins actuels.

Si des évolutions arrivent sur l'infrastructure, il est possible de demander un devis totalement

modulable à l'éditeur pour superviser le nombre d'équipements voulu (150,200...) et les fonctionnalités à ajouter.

En ce qui concerne le cout de main d'œuvre il est estimé à quatre jours de travail.

1.4 Sécurisation des accès

Afin de sécuriser notre solution, il va falloir définir la version utilisée par SNMP.

Les recommandations ANSSI nous conseillent l'utilisation de SNMPv3 dès que possible cependant les contraintes techniques des OS Windows serveur nous imposent d'utiliser du SNMPv2.

En effet, la V3 n'est pas supportée nativement par les Windows Serveurs.

Il serait possible d'installer des agents sur les serveurs Windows pour faire du SNMP over TLS mais ceux-ci sont encore en phase expérimentale sur Centreon.

Nous avons donc opté pour le SNMP natif à Windows qui est le SNMPv2c.

La version 2 de SNMP fonctionnant avec un système de communauté, celles-ci seront bien évidemment en Read Only pour des raisons de sécurité.

Afin d'essayer de répondre au maximum aux recommandations ANSSI, les hôtes Linux et les Switch/Routeurs seront configurés en SNMPv3.

Le mode choisi pour SNMPv3 est « **AuthPriv** » car ce mode, contrairement aux deux autres (AuthNoPriv et noAuthNoPriv), permet d'assurer de l'authentification via SHA 256 et du chiffrement via AES 256 dans notre cas.

Les agents configurés sur nos différents hôtes n'accepteront les requêtes SNMP venant uniquement de notre serveur Centreon via un filtrage IP dans leurs configurations.

Nous allons également créer un compte de service dédié pour la supervision sur le serveur Centreon, comme le recommande l'ANSSI.

2. Configuration technique

Dans cette procédure, nous ne reviendrons pas sur la partie installation de Centreon.

Voici la documentation officielle de Centreon concernant l'installation (via package Debian/CentOS ou par des VM prêtées à l'emploi) : <https://docs.centreon.com/docs/category/installation-of-a-central-server/>

Notions :

Pour rappel, voici quelques termes à connaitre afin de mieux comprendre la mise en place de notre solution :

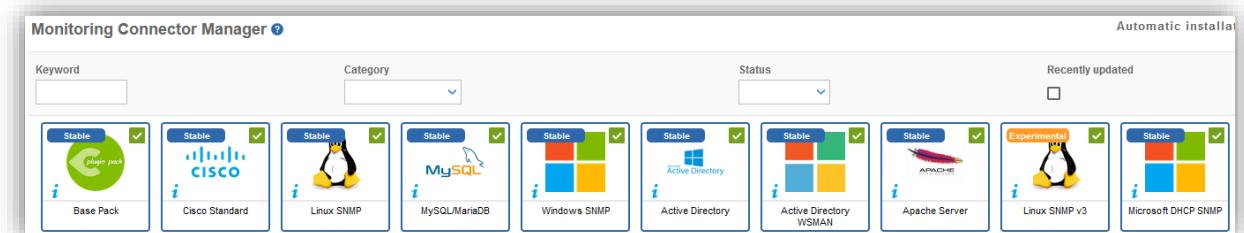
- Pooler : C'est le serveur de supervision
- Hôte : C'est un équipement supervisé (Switch, Serveurs, AP ect...)
- Service : C'est une ressource supervisée, cela peut être le rôle d'un serveur, par exemple (DHCP, Mariadb, http ect...) ou encore une ressource matérielle comme la RAM, le CPU ect...

- Plugins : C'est un module à installer qui permet de collecter les informations d'un service via les templates qui lui sont associés

Prérequis :

Comme vu ci-dessus, il va falloir installer différents plugins pour superviser nos hôtes.

Voici la liste complète à installer pour notre infrastructure (Ceux-ci peuvent être installés dans le menu « Configuration » puis « Monitoring Connector Manager ») :

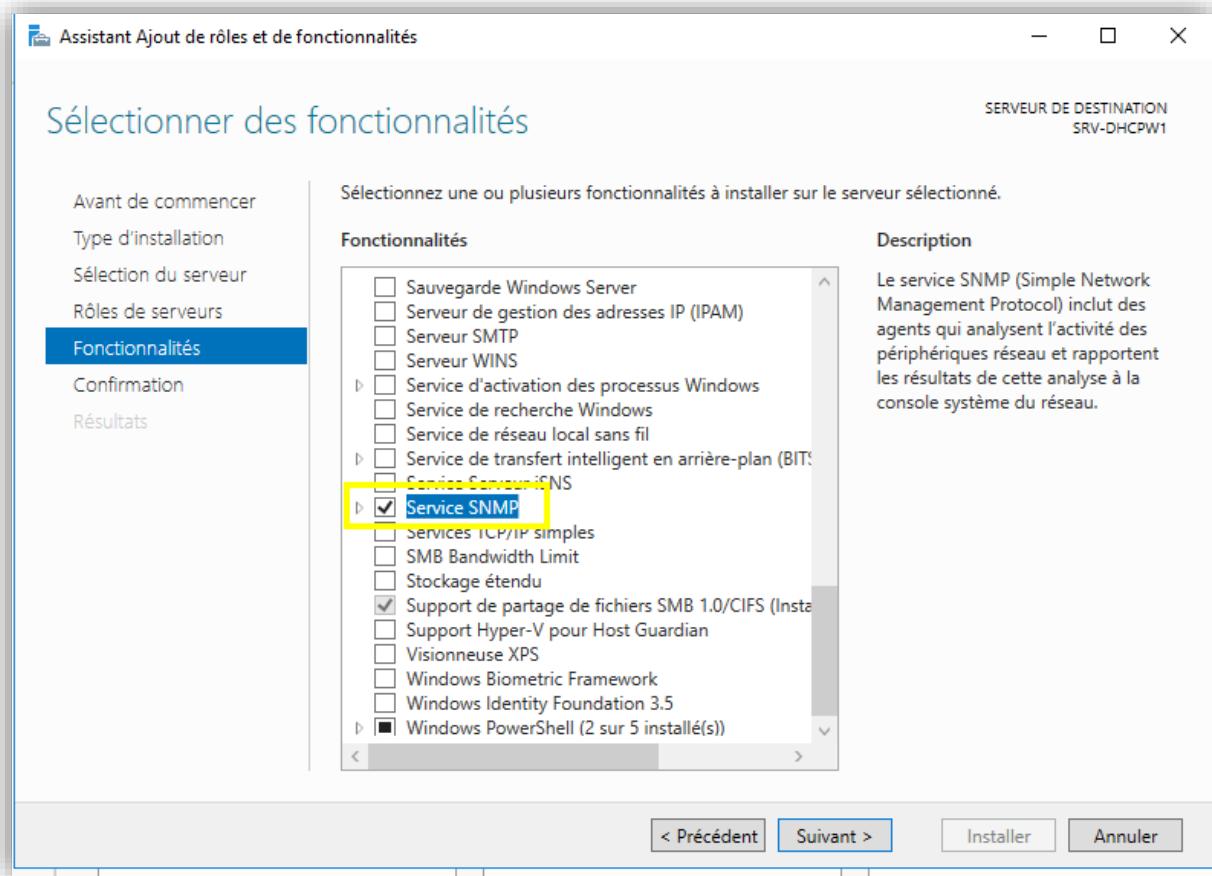


2.1 Supervision d'un hôte Windows

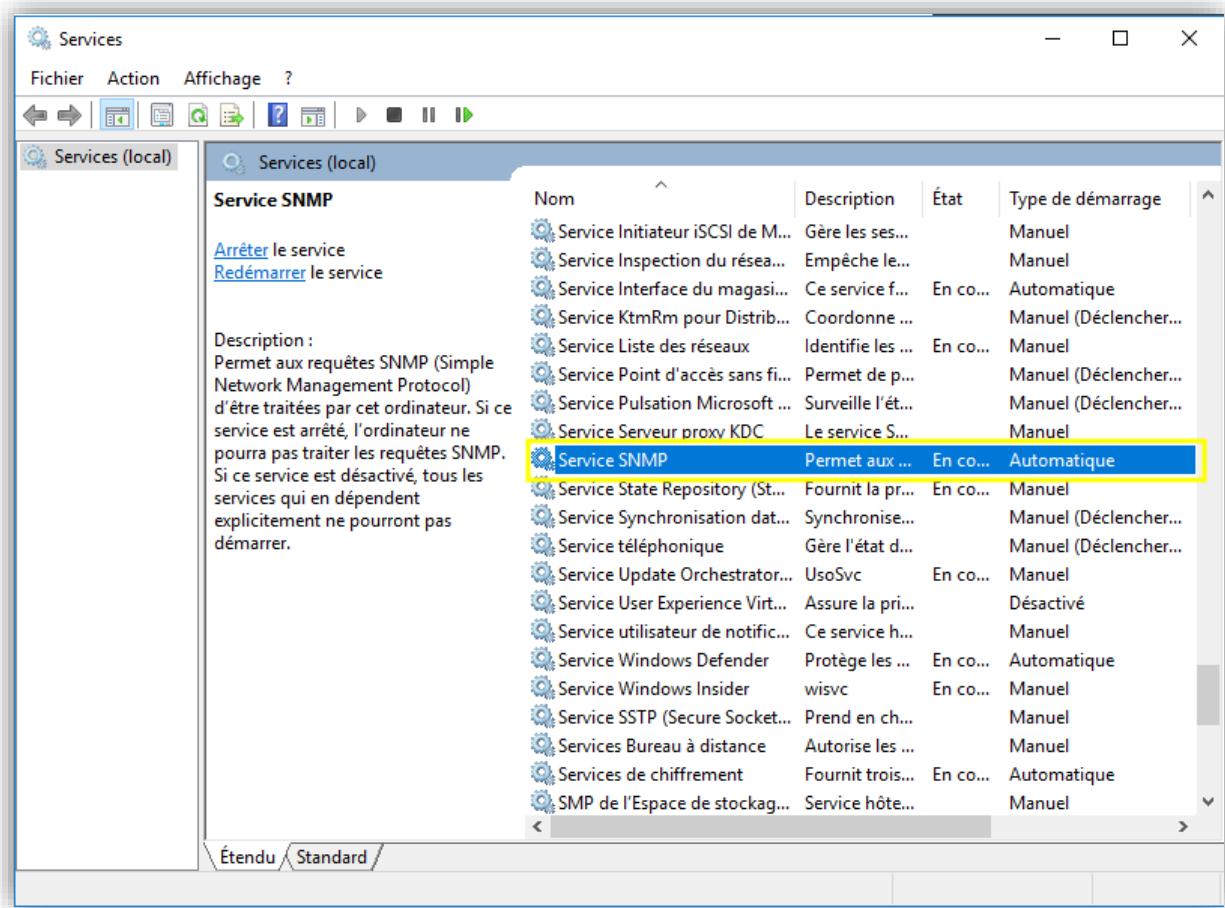
Nous commençons par superviser le serveur DHCP « **SRV-DHCPW1** », ensuite nous ajouterons le serveur AD nommé « **SRV-ADW1** ».

Avant de configurer notre hôte sur le Pooler, nous allons installer l'agent SNMP sur le serveur Windows.

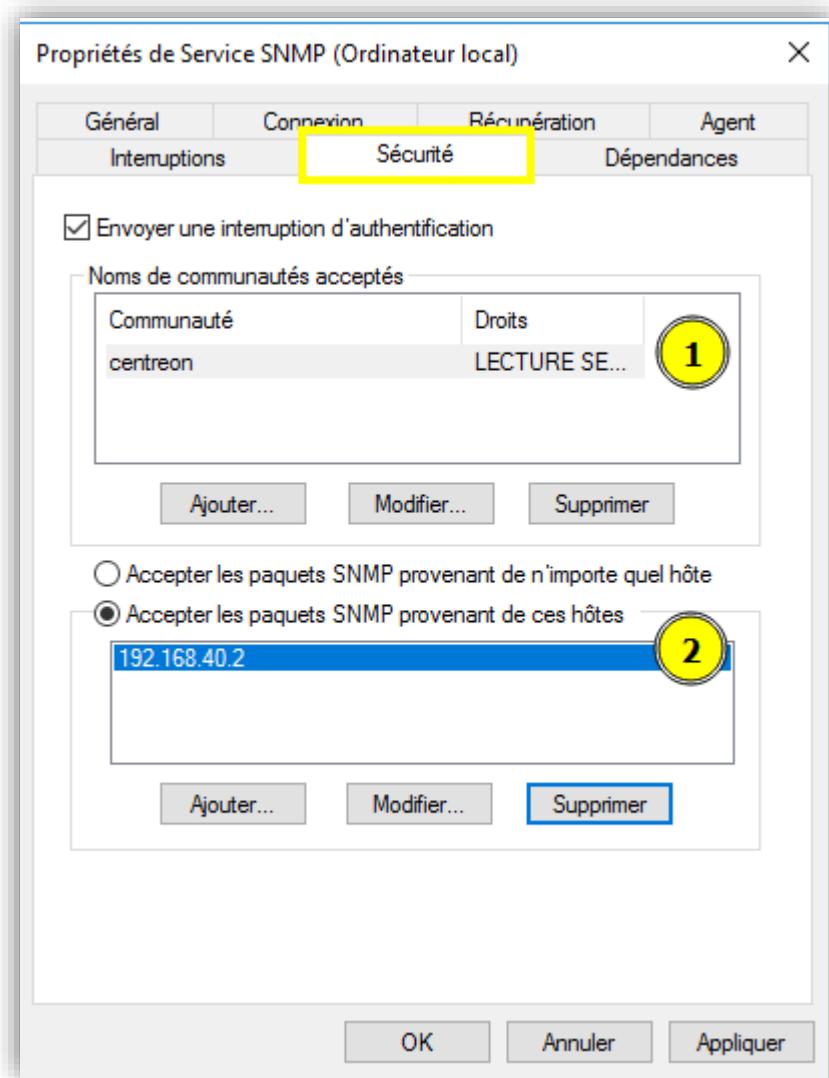
Pour cela, il faut se rendre dans le menu d'installation des rôles et fonctionnalités et cocher la fonctionnalité suivante :



Une fois cela fait, nous allons nous rendre dans les services du serveur puis faire un clic droit « Propriété » sur « Service SNMP » pour configurer l'agent :



Nous allons nous rendre dans l'onglet « Sécurité » et définir les options nécessaires :



1. Nom de la communauté en RO
2. Accepte les requêtes uniquement depuis l'IP de notre Pooler

Maintenant que cela est fait, nous allons pouvoir déclarer notre hôte sur notre Pooler.
Pour cela, nous allons dans le menu « Configuration » puis « Hosts »

The screenshot shows the Centreon web interface. At the top, there's a navigation bar with icons for Pollers (0/0/1/0), Services (0/0/1/0), and Hosts (1/0). Below the navigation bar is a left sidebar with links: Home, Monitoring, Reporting, Configuration (which is expanded to show Hosts, Services, Users, Commands, Notifications, SNMP Traps, Pollers, Additional Connector Configurations, and Knowledge Base), Administration, and Help. The main content area is titled "Configuration > Hosts". It has fields for "Name" and "Hostgroup". A table lists "Hosts" under "Hosts". The "Hosts" row is highlighted with a yellow box. To the right of the table are links for Host Groups, Templates, Categories, and Discovery.

Nous cliquons sur « Add » pour ajouter un nouvel hôte et définissons les paramètres suivants :

The screenshot shows the 'Host Configuration' page for creating a new host. The fields and their values are:

- Name ***: SRV-DHCPW1 (highlighted by yellow circle 1)
- Address ***: 192.168.40.3 (highlighted by yellow circle 2)
- SNMP Community & Version**: centreon (highlighted by yellow circle 3)
- Monitoring server**: Central (highlighted by yellow circle 4)
- Timezone**: Europe/Paris (highlighted by yellow circle 4)
- Templates**: OS-Windows-SNMP-custom (highlighted by yellow circle 5)
- Create Services linked to the Template too**: Yes (highlighted by yellow circle 6)

1. Nom du serveur
2. IP du serveur
3. Communauté et version SNMP utilisée (nom de communauté pouvant être modifié pour en mettre une plus complexe)
4. Zone de temps
5. Template utilisé pour la création de services
6. Créer les services associés à cet hôte via le template

Dans le menu « **Notification** », il est possible de lier des contacts pour avoir des alertes par mail quand l'hôte passe « **Down** ».

Dans notre cas, nous avons renseigné « **Admin Adrar** » créé pendant l'installation :

The 'Notification' tab is selected. The configuration includes:

- Notification Enabled**: Yes (highlighted by yellow box)
- Linked Contacts**: Admin Adrar (highlighted by yellow box)
- Notification options**:
 - Notification Options**: Down, Unreachable, Recovery, Flapping, Downtime Scheduled, None
 - Notification Interval**: * 60 seconds
 - Notification Period**: Notification Period
 - First notification delay**: * 60 seconds
 - Recovery notification delay**: * 60 seconds

Une fois l'hôte créé, il est nécessaire de redémarrer le service Centreon.

Pour cela, nous allons dans le menu « Configuration » puis « Poolers ».

Nous voyons que la configuration a changé ,il faut donc sélectionner le serveur et cliquer sur « Export Configuration » :

Name	IP Address	Server type	Is running ?	Conf Changed *	PID	Uptime	Last Update	Version	Default	Status	Actions	Options	
Central	127.0.0.1	Central	YES	YES	782	53 minutes 30 seconds	January 2, 2025 10:50:33 AM	Centreon Engine 24.10.2	Yes	ENABLED			1

Une fois cela fait, nous cochons les 4 premières cases afin de charger la nouvelle configuration et redémarrer le service :

Configuration > Pollers > Export configuration

Configuration Files Export

Polling instances

② Pollers • Central

Actions

- ② Generate Configuration Files
- ② Run monitoring engine debug (-v)
- ② Move Export Files
- ② Restart Monitoring Engine
- ② Post generation command

Method: Reload

Export

Maintenant, dans le menu « Hosts » nous voyons notre serveur « up »

Monitoring > Resources Status

Hosts

Status	Count
Down	0/0
Unreachable	0/0
Up	2/2
Pending	0/0

Display view: All

Status: Up

SRV-DHCPW1

Nous allons ensuite nous rendre dans le menu « Services » et retrouvons tous les services supervisés, comme l'utilisation de la RAM, du CPU ect...

Monitoring > Services

Hosts

Status	Count
Critical	0/0
Warning	0/0
Unknown	1/1
OK	11/12
Pending	0/0

Display view: All

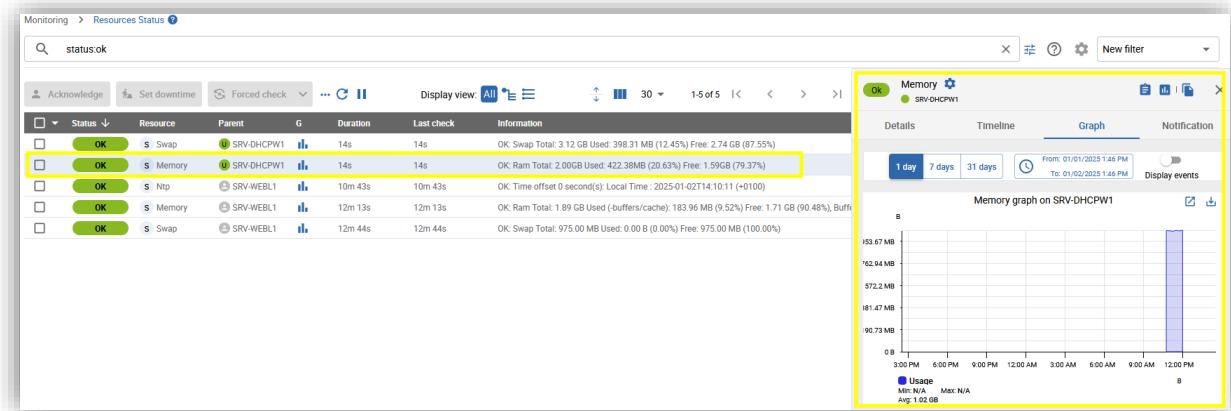
Status: Up

SRV-DHCPW1

OK Swap Total: 3.12 GB Used: 398.31 MB (12.45%) Free: 2.74 GB (87.55%)

Host	Service	Scheduling	Template	Status	Options
SRV-DHCPW1	Cpu	5 min / 1 min	OS-Windows-Cpu-SNMP-custom -> OS-Windows-Cpu-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	<input checked="" type="checkbox"/>
	Memory	15 min / 1 min	OS-Windows-Memory-SNMP-custom -> OS-Windows-Memory-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	<input checked="" type="checkbox"/>
	Ping	5 min / 1 min	Base-Ping-LAN-custom -> Base-Ping-LAN -> generic-active-service-custom -> generic-active-service	ENABLED	<input checked="" type="checkbox"/>
	Swap	15 min / 1 min	OS-Windows-Swap-SNMP-custom -> OS-Windows-Swap-SNMP -> generic-active-service-custom -> generic-active-service	ENABLED	<input checked="" type="checkbox"/>

En cliquant sur le service, nous avons également la possibilité d'avoir plus de détails, voici un exemple pour des graphiques d'utilisation de la RAM :



Nous pouvons également rajouter des services rattachés à l'hôte manuellement.
Nous allons donc ajouter un check sur l'espace disque du serveur.

Pour cela, nous allons dans le « Configuration » ; « Services » puis « Services by host » et cliquons sur « Add ».

Nous arrivons sur cette page et renseignons les différents champs :

Service Basic Information	
① Name	Check_Disk 1
② Hosts	SRV-DHCPW1 2
③ Template	OS-Windows-Disk-Global-SNMP-custom 3
Service Check Options	
④ Check Command	Check Command 4
Custom macros	Name: FILTER Value: * Password: <input type="password"/> Name: TRANSFORMSRC Value: ^(..)* Password: <input type="password"/> Name: TRANSFORMDST Value: \$1 Password: <input type="password"/> Name: WARNING Value: 80 Password: <input type="password"/> Name: CRITICAL Value: 90 Password: <input type="password"/> Name: EXTRAOPTIONS Value: --verbose --filter-perfdata='stor' Password: <input type="password"/>
Args	No argument found for this command

1. Nom du service à ajouter
2. Hôte rattaché à ce service

3. Template utilisé pour la vérification du service
4. Option de configuration des vérifications effectuées, comme les seuils pour les alertes de type « **Warning** », « **Critical** » ect...

Une fois ajouté, nous redémarrons le pooler, comme vu précédemment, puis nous retournons dans le menu « **Services** ».

Nous constatons notre nouveau service avec les informations d'utilisation du disque :

	Status	Resource	Parent	G	Duration	Last check	Information	Tries
□	OK	\$: Memory	SRV-DHCPW1	■	14s	14s	OK: Ram Total: 2.00GB Used: 1.14GB (57.18%) Free: 876.62MB (42.82%)	1/3 (H)
□	OK	\$: Check_Disk	SRV-DHCPW1	■	1m 41s	1m 41s	OK: Storage C:\Label: Serial Number beeef6ea7 Usage Total: 59.45 GB Used: 10.64 GB (17.90%) Free: 48.80 GB (82.10%)	1/3 (H)
□	OK	\$: Cpu	SRV-DHCPW1	■	2m 44s	2m 44s	OK: 2 CPU(s) average usage is 0.00 %	1/3 (H)
□	OK	\$: Ping	SRV-DHCPW1	■	5m 14s	14s	OK - 192.168.40.3: rta 0.399ms, lost 0%	1/3 (H)

Afin de s'assurer du bon fonctionnement de la supervision, nous allons effectuer un test d'arrêt du serveur.

Nous voyons que celui-ci passe bien en état « **Down** » :

Status	Resource	Parent	G	Duration	Last check	Information
Down	SRV-DHCPW1		■	26m 26s	31s	CRITICAL - 192.168.40.3: Host unreachable @ 192.168.40.2. rta nan, lost 100%

Status information
 CRITICAL - 192.168.40.3: Host unreachable @ 192.168.40.2. rta nan, lost 100%

FQDN / Address
192.168.40.3

Alias
SRV-DHCPW1

Monitoring server
Central

Timezone
Europe/Paris

Current status duration
26m 27s - 1/3(H)

Last status change
01/02/2025 1:46 PM

Last check
01/02/2025 2:12 PM

Next check
01/02/2025 2:17 PM

Check duration
3 2642379999999998 s

Latency
0.145 s

Status change percentage
5 328947368421053%

Current notification number
19

Performance data

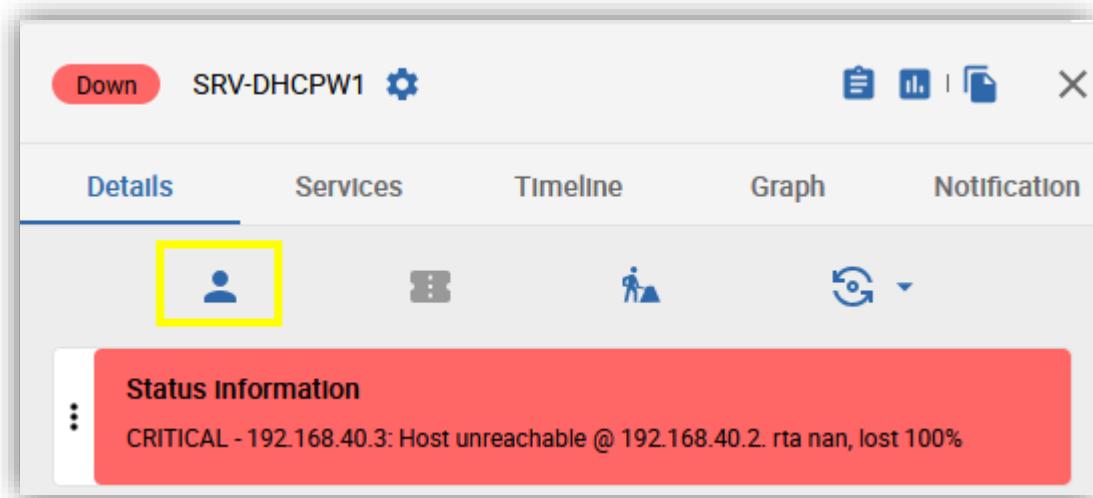
Dans le menu « **Timeline** » nous avons l'historique des états UP/DOWN :

The screenshot shows the 'Timeline' view for the service 'SRV-DHCPW1'. The 'Timeline' tab is highlighted with a yellow box. The timeline displays historical events from January 2, 2025, at 1:47 PM to January 2, 2025, at 10:20 AM. The events are categorized by status: 'Down' (red) and 'Up' (green). The 'OK' status is shown in black. The events are as follows:

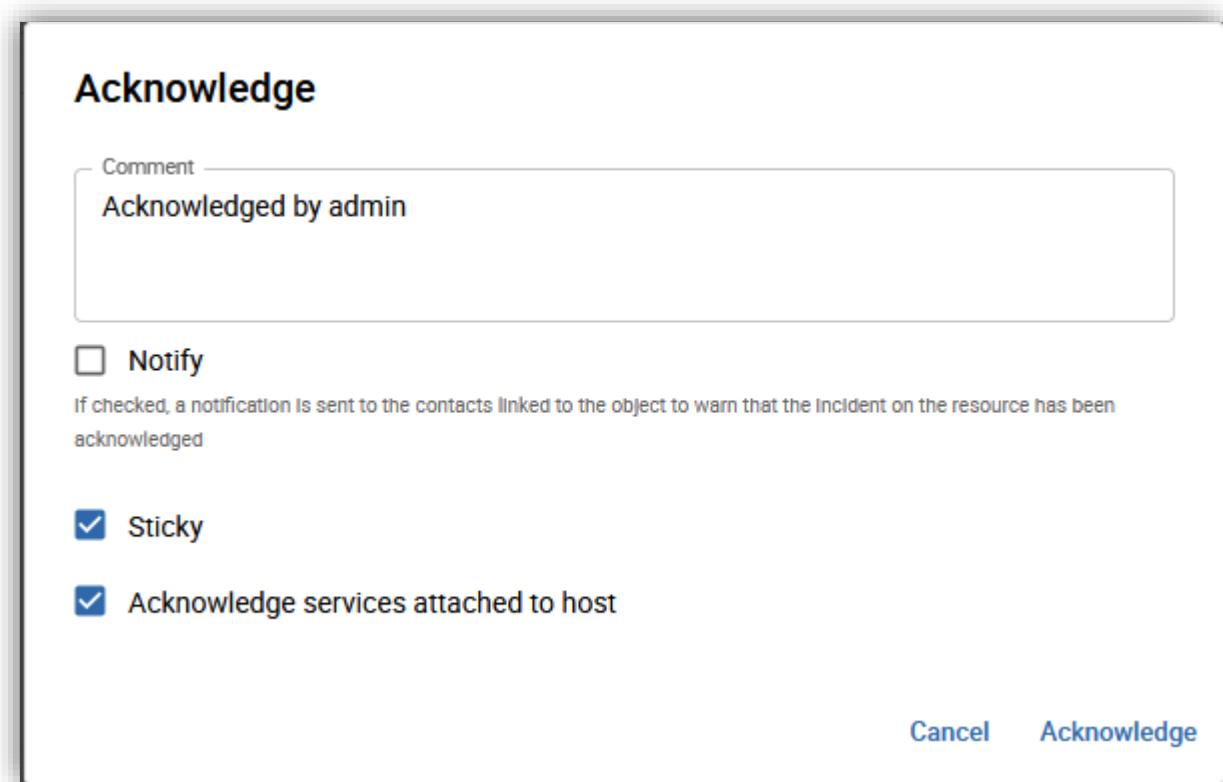
- Thursday, January 2, 2025 1:47 PM: Down (Red) - CRITICAL - 192.168.40.3: Host unreachable @ 192.168.40.2. rta nan, lost 100%
- Thursday, January 2, 2025 1:46 PM: Down (Red) - CRITICAL - 192.168.40.3: Host unreachable @ 192.168.40.2. rta nan, lost 100%
- Thursday, January 2, 2025 1:45 PM: Down (Red) - CRITICAL - 192.168.40.3: Host unreachable @ 192.168.40.2. rta nan, lost 100%
- Thursday, January 2, 2025 1:42 PM: Up (Green) - OK - 192.168.40.3: rta 0,582ms, lost 0%
- Thursday, January 2, 2025 10:20 AM: Up (Green) - OK - 192.168.40.3: rta 0,421ms, lost 0%

Si un serveur est « **Down** » pour des raisons de maintenance ou autre, il est possible d'« **Acknowledge** » celui-ci temporairement afin qu'il ne remonte pas dans les alertes de la supervision.

Pour cela, il faut que rendre sur l'hôte et cliquer sur le bouton « Acknowledge » :



Une fenêtre apparaît demandant confirmation avec la possibilité d'ajouter une note :



Ni notre hôte ni les services n'apparaitront dans les alertes désormais.

Dès la maintenance fini, il suffit de rechercher le serveur via le Menu « Host » puis « All » et cliquer

sur le bouton « **Disascknowledge** » pour qu'il remonte dans la supervision :

Maintenant, nous allons superviser le service DHCP du serveur ce qui nous permettra d'avoir des informations sur nos pools IP.

Nous allons donc dans le menu « **Services by Host** » afin d'ajouter un service à notre hôte, comme vu précédemment :

1. Hôte rattaché au service
2. Template pour la supervision du service DHCP
3. Filtre sur le pool IP du VLAN 10
4. Warning à 80% d'utilisation des IP du pool
5. Alerte critique à 90% d'utilisation des IP du pool

Nous retournons dans le menu « **Services** » afin de retrouver notre service ainsi que les informations concernant le pool DHCP supervisé :

Status	Resource	Parent	G	Duration	Last check	Information
OK	Check_Disk	SRV-DHCPW1		12m 48s	2m 48s	OK: Subnet '192.168.10.0' status: enabled, addresses usage total: 141 used: 0 (0.00%) free: 141 (100.00%) pending of
OK	Check_Disk	SRV-DHCPW1		13m 41s	13m 41s	OK: Storage 'C:' Usage Total: 59.45 GB Used: 10.67 GB (17.95%) Free: 48.77 GB (82.05%)
OK	Cpu	SRV-DHCPW1		11m 20s	1m 20s	OK: 2 CPU(s) average usage is 0.00 %
OK	Memory	SRV-DHCPW1		10m 10s	10m 10s	OK: Ram Total: 2.00GB Used: 838.94MB (40.98%) Free: 1.18GB (59.02%)
OK	Ping	SRV-DHCPW1		12m 31s	2m 31s	OK - 192.168.40.3 rta 0.795ms, lost 0%
OK	Swap	SRV-DHCPW1		8m 59s	8m 59s	OK: Swap Total: 3.12 GB Used: 991.44 MB (30.99%) Free: 2.16 GB (69.01%)

Status information
 OK: Subnet '192.168.10.0' status: enabled, addresses usage total: 141 used: 0 (0.00%) free: 141 (100.00%) pending offers: 0
 Subnet '192.168.10.0' status: enabled, addresses usage total: 141 used: 0 (0.00%) free: 141 (100.00%) pending offers: 0

Monitoring server: Central | Current status duration: 12m 48s - 1/3(H)
 Last status change: 01/03/2025 1:44 PM | Last check: 01/03/2025 1:54 PM
 Next check: 01/03/2025 1:59 PM | Check duration: 0.367707 s
 Latency: 0.421 s | Status change percentage: 0%
 Current notification number: 0

Performance data
 '192.168.10.0@subnet.addresses.usage.count'=0;0:141
 '192.168.10.0@subnet.addresses.free.count'=141;0:141
 '192.168.10.0@subnet.addresses.usage.percentage'=0.00%;0:100
 '192.168.10.0@subnet.pending.offers.count'=0;0;

Nous voyons ci-dessus les informations concernant le Pool (pourcentages IP utilisées, IP libres ect...)

Nous allons effectuer les mêmes étapes que précédemment pour notre serveur AD que nous retrouvons ici :

Status	Resource	Parent	G	Duration	Last check	Information
Up	SRV-ADW1			19m 33s	1m 8s	OK - 192.168.40.5: rta 0.461ms, lost 0%
Up	SRV-DHCPW1			50m 47s	52s	OK - 192.168.40.3: rta 0.527ms, lost 0%

Status information
 OK - 192.168.40.5: rta 0.461ms, lost 0%

FQDN / Address: 192.168.40.5
 Alias: SRV-ADW1 | Monitoring server: Central
 Timezone: Europe/Paris | Current status duration: 19m 34s - 1/3(H)
 Last status change: 01/03/2025 2:12 PM | Last check: 01/03/2025 2:31 PM
 Next check: 01/03/2025 2:36 PM | Check duration: 0.096044 s
 Latency: 0.062 s | Status change percentage: 0%
 Current notification number: 0

Performance data

Et nous voyons également les services associés :

Status	Resource	Parent	Duration	Last check	Information
OK	Swap	SRV-ADW1	2m 18s	2m 18s	OK: Swap Total: 3.20 GB Used: 1.82 GB (57.0%) Free: 1.37 GB (42.94%)
OK	Check_Disk	SRV-ADW1	2m 18s	2m 18s	OK: Storage 'C': Usage Total: 59.45 GB Used: 11.25 GB (18.92%) Free: 48.20 GB (81.08%)
OK	Memory	SRV-ADW1	3m 19s	3m 19s	OK: Ram Total: 2.00GB Used: 1.40GB (70.25%) Free: 608.94MB (29.75%)
OK	Cpu	SRV-ADW1	4m 39s	4m 39s	OK: 2 CPU(s) average usage is 15.00 %
OK	Ping	SRV-ADW1	5m 59s	59s	OK - 192.168.40.5: rta 0.384ms, lost 0%
OK	Swap	SRV-DHCPW1	45m 44s	44s	OK: Swap Total: 3.12 GB Used: 1.04 GB (33.45%) Free: 2.08 GB (66.55%)
OK	Memory	SRV-DHCPW1	46m 55s	1m 55s	OK: Ram Total: 2.00GB Used: 903.88MB (44.16%) Free: 1.12GB (55.84%)
OK	Cpu	SRV-DHCPW1	48m 5s	3m 5s	OK: 2 CPU(s) average usage is 0.00 %
OK	Check_DHCP	SRV-DHCPW1	49m 16s	4m 16s	OK - 192.168.40.3: rta 0.296ms, lost 0%
OK	Check_Disk	SRV-DHCPW1	49m 33s	4m 33s	OK: Subnet 192.168.10.0 status: enabled, addresses usage total: 141 used: 0 (0.0%) free: 141 (100.0%), pending of 0
OK	Swap	SRV-DHCPW1	50m 26s	20m 26s	OK: Storage 'C': Usage Total: 59.45 GB Used: 10.71 GB (18.01%) Free: 48.74 GB (81.99%)

Memory SRV-ADW1

Details	Timeline
Monitoring server Central	Current status duration 3m 22s - 1/30
Last status change 01/03/2025 2:30 PM	Last check 01/03/2025 2:30 PM
Next check 01/03/2025 2:45 PM	Check duration 0.165993 s
Latency 0.487 s	Status change percentage 0%
Current notification number 0	
Performance data \used=15079178240.0.1717148057.0.1931791564.0.2146435072	
Command /usr/lib/centreon/plugins/centreon_windows_snmp.pl -plugin=windows:snmp -plugin=memory	

2.2 Supervision d'un serveur Linux

Nous allons maintenant superviser notre serveur Debian 12 nommé « **SRV-WEBL1** » qui comporte une base de donnée MariaDB ainsi qu'un serveur Web Apache2.

Nous commençons par nous rendre sur notre serveur et installer l'agent SNMP :

```
apt install snmpd snmp
```

Une fois cela fait, nous allons créer un utilisateur pour l'utilisation de SNMPv3 (Les passphrases utilisées pour l'authentification du compte n'apparaitront pas en clair dans cette procédure)

```
net-snmp-create-v3-user -ro -A '*****' -X '*****' -a SHA -x AES snmpuser
```

Cette commande sert à :

- Créer un utilisateur « **snmpuser** »
- L'option **-X** correspond à la Passphrase utilisée avec AES (par défaut, le plugin utilisera AES 256) pour chiffrer les données
- L'option **-A** correspond à la Passphrase utilisée avec SHA (par défaut, le plugin utilisera SHA256) pour l'authentification

La commande retournera cela :

```
adding the following line to /var/lib/snmp/snmpd.conf:
  createUser snmpuser SHA "██████████" AES "██████████"
adding the following line to /etc/snmp/snmpd.conf:
  rouser snmpuser
```

Une fois cela fait, nous allons dans le fichier de configuration du service et l'éditons pour ajouter l'interface et le port d'écoute de notre agent :

```
#Port d'écoute de l'agent SNMP local
agentAddress udp :161
```

Nous démarrons et vérifions le statut du service :

```
root@SRV-WEBL1:~# systemctl status snmpd.service
● snmpd.service - Simple Network Management Protocol (SNMP) Daemon.
   Loaded: loaded (/lib/systemd/system/snmpd.service; enabled; preset: enabled)
   Active: active (running) since Thu 2025-01-02 14:07:54 CET; 41s ago
     Main PID: 894 (snmpd)
        Tasks: 1 (limit: 2273)
       Memory: 3.4M
          CPU: 62ms
        CGroup: /system.slice/snmpd.service
           └─894 /usr/sbin/snmpd -L0w -u Debian-snmp -g Debian-snmp -I -smux mteTrigger mteTriggerConf -f
```

Sur notre serveur Centreon nous allons créer un nouvel hôte de la même manière que précédemment.

Nous allons uniquement modifier le template pour utiliser du SNMPv3 pour Linux :

The screenshot shows the 'Modify a Host' interface in Centreon. The 'Host basic information' section includes fields for Name (SRV-WEBL1), Alias, Address (192.168.40.4), Monitoring server (Central), and Timezone (Europe/Paris). In the 'Templates' section, a dropdown menu lists 'OS-Linux-SNMPv3-custom', which is highlighted with a yellow border. A note below the dropdown states: 'A host or host template can have several templates. See help for more details.' At the bottom, there's a question about creating services linked to the template, with 'Yes' selected.

Plus bas dans la page, nous configurons les options pour SNMPv3 :

Host check options

Check Command: Check Command

Args:

+ Add a new entry

Name: SNMPV3USERNAME	Value: snmpuser	Password: <input type="password"/>	1
Name: SNMPV3AUTHPASSPHRASE	Value: [REDACTED]	Password: <input type="password"/>	2
Name: SNMPV3AUTHPROTOCOL	Value: SHA	Password: <input type="password"/>	3
Name: SNMPV3PRIVPASSPHRASE	Value: [REDACTED]	Password: <input type="password"/>	4
Name: SNMPV3PRIVPROTOCOL	Value: AES	Password: <input type="password"/>	5
Name: SNMPEXTRAOPTIONS	Value: [REDACTED]	Password: <input type="password"/>	

1. Utilisateur créé précédemment pour l'utilisation de SNMPv3
2. Passphrase d'authentification
3. Protocole de hachage (Le plugin utilise SHA 256 par défaut)
4. Passphrase privée
5. Protocole de chiffrement (Le plugin utilise AES 256 par défaut)

Nous pouvons maintenant redémarrer le pooler, puis nous rendre dans le menu « hôtes » afin d'en vérifier le bon fonctionnement :

Status	Resource	Parent	G	Duration	Last check	Information
Up	SRV-DHCWP1			31m 50s	1m 48s	OK - 192.168.40.3: rta 0,533ms, lost 0%
Up	SRV-WEBL1			39s		OK - 192.168.40.4: rta 2,359ms, lost 0%

SRV-WEBL1

Details Services Timeline Graph Notification

Status information
OK - 192.168.40.4

FQDN / Address
192.168.40.4

Alias
SRV-WEBL1

Monitoring server
Central

Timezone
Europe/Paris

Last check
01/02/2025 10:51 AM

Next check
01/02/2025 10:56 AM

Latency
0.914 s

Check duration
0.0855503 s

Status change percentage
0%

Current notification number
0

Performance data
rta=2,359ms;3000,000;5000,000; pi=0%;80;100; rttmax=2,359ms;; rttmin=2,359ms;;

Nous allons maintenant vérifier les services pour cet hôte :

Status	Resource	Parent	G	Duration	Last check	Information
OK	Memory	SRV-WEBL1		6s	6s	OK: Ram Total: 1.89 GB Used (buffers/cache): 197.01 MB (10.20%) Free: 1.69 GB (89.80%), Buffer: 15.84 MB, Cached: 14.95 MB
OK	Load	SRV-WEBL1		26s	26s	OK: Load average: 0.00, 0.00, 0.00
OK	Cpu	SRV-WEBL1		26s	26s	OK: 2 CPU(s) average usage is 1.00%
OK	Ping	SRV-WEBL1		26s	26s	OK - 192.168.40.4: rta 0.230ms, lost 0%
OK	Swap	SRV-WEBL1		36s	36s	OK: Swap Total: 975.00 MB Used: 0.00 B (0.00%) Free: 975.00 MB (100.00%)
OK	CPU Usage	SRV-WEBL1		37s	37s	OK: CPU Usage: 0.00% CPU Used: 0.00% CPU Shared: 0.00% CPU Shared: 0.00%

Memory

SRV-WEBL1

Details Timeline Graph Notification

Status information
OK: Ram Total: 1.89 GB Used (buffers/cache): 197.01 MB (10.20%) Free: 1.69 GB (89.80%), Buffer: 15.84 MB, Cached: 14.95 MB

Nous constatons également que c'est bien la version 3 utilisée par SNMP

The screenshot shows the Centreon monitoring interface with the search bar set to "status.ok". The main pane displays a tree view of monitored resources under "SRV-WEBL1" and "SRV-DHCPW1", all of which are currently "OK". The columns in the table include Status, Resource, Parent, G, Duration, Last check, and Information. The "Information" column provides detailed system statistics for each resource.

SRV-WEBL1 Information:

- Memory: OK. Ram Total: 1.89 GB Used: (buffers/cache): 209.99 MB (10.87%) Free: 1.68 GB (89.13%) Buffer: 16.83 MB Cached: 15s
- Load: OK. Load average: 0.02, 0.01, 0.00
- Uptime: OK. System uptime is: 36m 52s
- Swap: OK. Swap Total: 975.00 MB Used: 0.00 B (0.00%) Free: 975.00 MB (100.00%)
- Ntp: OK. Time offset 0 second(s). Local Time : 2025-01-02T11:37:35 (+0100)
- Ping: OK. Ping to 192.168.40.3: rta 0.327ms, lost 0%
- Swap: OK. Swap Total: 3.12 GB Used: 1.14 GB (36.51%) Free: 1.98 GB (63.49%)
- Memory: OK. Ram Total: 2.00GB Used: 1.02GB (51.04%) Free: 1002.25MB (48.96%)
- Check_Disk: OK. Storage 'C': Usage Total: 59.45 GB Used: 10.65 GB (17.91%) Free: 48.80 GB (82.09%)
- Cpu: OK. 2 CPU(s) average usage is 0.50 %
- Ping: OK. Ping to 192.168.40.3: rta 0.292ms, lost 0%

SRV-DHCPW1 Information:

- Memory: OK. Ram Total: 1.89 GB Used: (buffers/cache): 209.99 MB (10.87%) Free: 1.68 GB (89.13%) Buffer: 16.83 MB Cached: 1h 14m
- Swap: OK. Swap Total: 975.00 MB Used: 0.00 B (0.00%) Free: 975.00 MB (100.00%)
- Memory: OK. Ram Total: 2.00GB Used: 1.02GB (51.04%) Free: 1002.25MB (48.96%)
- Check_Disk: OK. Storage 'C': Usage Total: 59.45 GB Used: 10.65 GB (17.91%) Free: 48.80 GB (82.09%)
- Cpu: OK. 2 CPU(s) average usage is 0.50 %
- Ping: OK. Ping to 192.168.40.3: rta 0.292ms, lost 0%

Details Tab (SRV-WEBL1):

- 1/02/2025 11:48 AM
- 01/02/2025 11:48 AM
- Next check: 01/02/2025 12:03 PM
- Check duration: 0.280928 s
- Latency: 6.218 s
- Status change percentage: 21.710528315789473%
- Current notification number: 0

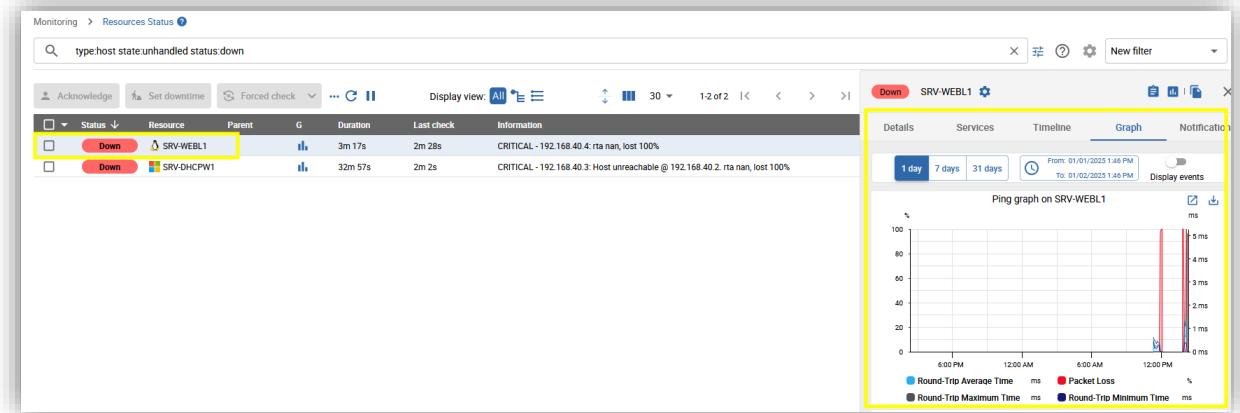
Performance data (SRV-WEBL1):

```
Command /usr/lib/centreon/plugins/centreon_linux_snmp.pl
--plugin=ios_snmp::snmp_plugin
--mode=memory
--hostname=192.168.40.4
--snmp-version 3
--snmp-community public
--authpassword="public"
--authprotocol=SHA
--privpassword="public"
--privprotocol=AES
--oid=1.3.6.1.4.1.1.2.1.1.1
--oid=1.3.6.1.4.1.1.2.1.1.1
--critical-usage="90"
--force-64bit-counters
```

Performance data (SRV-DHCPW1):

```
Command /usr/lib/centreon/plugins/centreon_linux_snmp.pl
--plugin=ios_snmp::snmp_plugin
--mode=memory
--hostname=192.168.40.4
--snmp-version 3
--snmp-community public
--authpassword="public"
--authprotocol=SHA
--privpassword="public"
--privprotocol=AES
--oid=1.3.6.1.4.1.1.2.1.1.1
--oid=1.3.6.1.4.1.1.2.1.1.1
--critical-usage="90"
--force-64bit-counters
```

Maintenant que tout est fonctionnel, nous effectuons un test d'arrêt du serveur pour constater qu'il passe « **Down** » :



Ci-dessus, nous constatons que la supervision est fonctionnel et voyons également un graphique des pertes de ping.

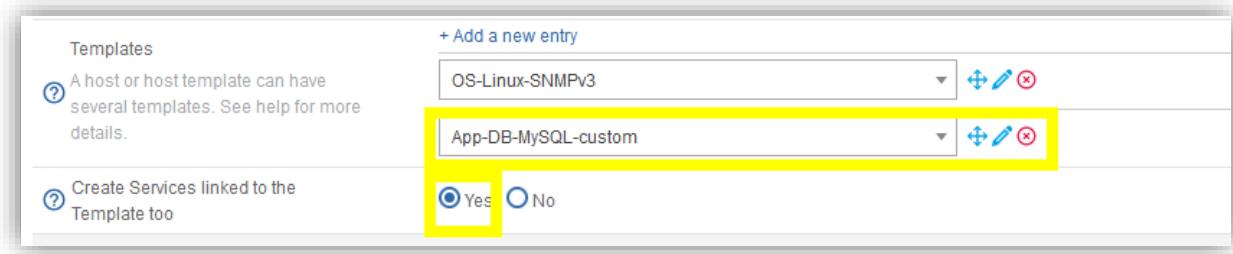
Maintenant que la partie hardware est supervisée nous allons faire la même chose pour un service hébergé sur le serveur.

Une base de données MariaDB étant présente pour le site Web nous allons donc la superviser.

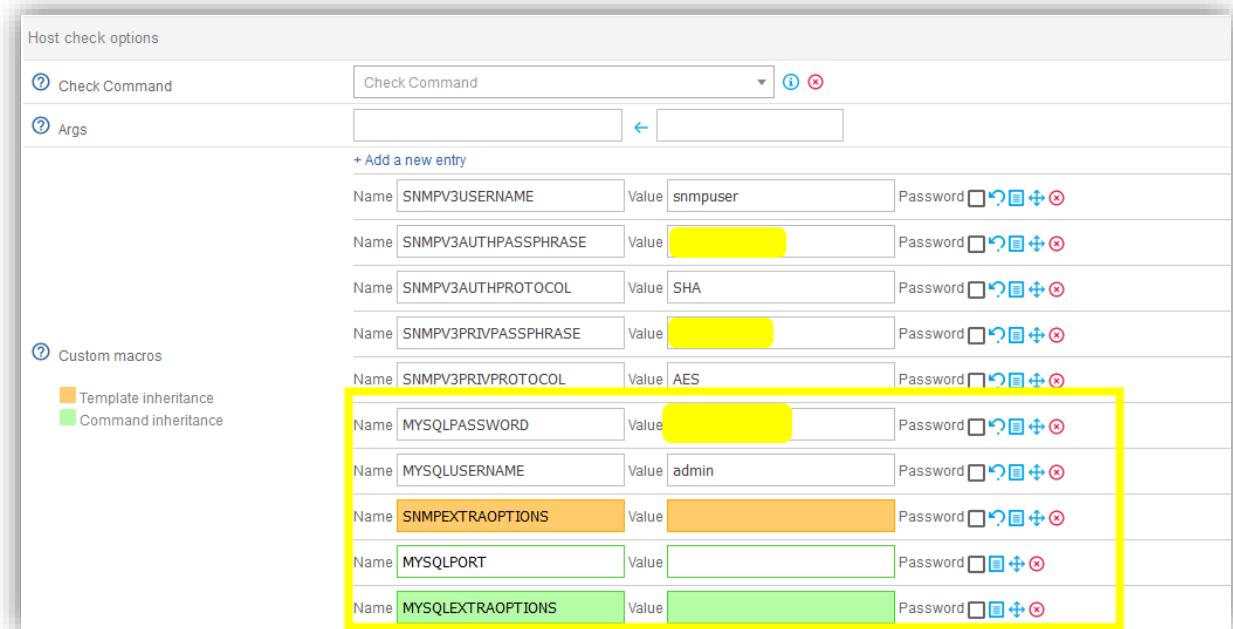
Nous allons nous rendre dans le menu « **Configuration** » - « **Host** » et sélectionner notre serveur.

Dans la partie « **Template** » nous sélectionnons « **Add a new entry** » :

Nous choisissons donc le template associé à « **Mysql** » et créons les services associés :



Plus bas dans la page, nous voyons des macros qui se sont rajoutées pour configurer les options de connexions aux bases de données (le port est laissé vide car le plugin utilise le port par défaut 3306) :



Nous sauvegardons la configuration et redémarrons le pooler.

Plusieurs nouveaux services sont maintenant rattachés à notre hôte :

	Status	Resource	Parent	G	Duration	Last check	Information
<input type="checkbox"/>	OK	\$ Database-Size	(SRV-WEBL1)		11m 28s	1m 13s	OK: Database 'bd1' Used: 16.00 KB, Free: 0.00 B - Table 'utilisateurs' Used: 16.00 KB, Free: 0.00 B, Fragmentation: 0.00 %
<input type="checkbox"/>	OK	\$ Connection-Time	(SRV-WEBL1)		23m 4s	3m 4s	OK: Connection established in 0.016s.
<input type="checkbox"/>	OK	\$ Slowqueries	(SRV-WEBL1)		25m 4s	4s	OK: 0 slow queries since last check.
<input type="checkbox"/>	OK	\$ Connections-Number	(SRV-WEBL1)		25m 4s	4s	OK: Client connected threads total: 151 used: 3 (1.99%) free: 148 (98.01%)
<input type="checkbox"/>	OK	\$ Querles	(SRV-WEBL1)		25m 8s	8s	OK: Requests Total : 0
<input type="checkbox"/>	OK	\$ Open-Files	(SRV-WEBL1)		25m 8s	8s	OK: 0.18% of the open files limit reached (59 of max. 32184)
<input type="checkbox"/>	OK	\$ Myisam-Keycache	(SRV-WEBL1)		25m 8s	8s	OK: myisam keycache hitrate at 100.00%

Beaucoup de paramétrages sont possibles pour affiner les données ressorties par le serveur Centreon, nous allons voir un exemple avec le check du temps de connexion au serveur.

Pour cela, il faut se rendre dans la configuration du service et renseigner les options suivantes :

The screenshot shows the 'Modify a Service' configuration page in Nagios. The tabs at the top are General Information, Notifications, Relations, Data Processing, and Extended Info. The General Information tab is selected.

Service Basic Information:

- Name: Connection-Time
- Hosts: SRV-WEBL1
- Template: App-DB-MySQL-Connection-Time-custom

Service Check Options:

- Check Command: Check Command
- Custom macros:
 - Name: WARNING Value: 200
 - Name: CRITICAL Value: 500
 - Name: EXTRAOPTIONS Value: (empty)
- Args: Argument No argument found for this command

Service Scheduling Options:

1. Warning à partir de 200ms de temps de connexion au serveur
2. Alerte Critique à partir de 500ms de temps de connexion au serveur

Maintenant, nous allons nous rendre dans le menu « **Services** » pour regarder cela plus en détail :

Connection-Time

SRV-WEBL1

Status Information

OK: Connection established in 0.016s.

Monitoring server Central	Current status duration 56m 11s - 1/3(H)
Last status change 01/03/2025 11:53 AM	Last check 01/03/2025 12:48 PM
Next check 01/03/2025 12:53 PM	Check duration 0.371845 s
Latency 0.296 s	Status change percentage 9.473684210526317%
Current notification number 0	
Performance data	
'connection.timemilliseconds'=16ms;;0;	
Command <pre>/usr/lib/centreon/plugins//centreon_mysql.pl --plugin=database::mysql::plugin --host=192.168.40.4</pre>	

Ici nous voyons le temps de connexion au serveur.

Afin de ne pas alourdir cette documentation, nous ne reviendrons pas sur chaque paramétrage cependant la documentation officielle du plugin de Centreon présente dans la partie Annexe permet d'avoir les options de configuration pour chacun des services.

2.3 Supervision d'un Switch Cisco

Nous allons maintenant mettre en place la supervision de notre Switch nommé « **SW1** ».

Nous allons commencer par les configurations sur le Switch pour l'agent SNMP.

Nous déclarons notre utilisateur ainsi que les passphrases associées, comme pour le serveur Linux vu dans le chapitre précédent :

```
enable
conf t
snmp-server group ADMIN v3 priv
snmp-server user snmpuser groupel v3 auth sha ***** priv aes 256 *****
```

Ici nous avons créé un groupe « **ADMIN** » qui contient le « **snmpuser** » qui servira à l'authentification de SNMPv3.

Nous allons maintenant restreindre les autorisations de requêtes SNMP à notre Pooler ainsi qu'à l'utilisateur créé précédemment :

```
snmp-server host 192.168.40.2 version 3 priv snmpuser
```

Une fois cela fait, nous allons pouvoir créer notre hôte sur le serveur Centreon de la même manière que dans les exemples précédents.

Nous allons modifier l'IP, le template et ajouter les options nécessaires pour le SNMPv3 :

Name	Value	Options
SNMPEXTRAOPTIONS	--authprotocol sha --snmp-user	*****

1. Nom du template pour les équipements Cisco

2. Options à ajouter pour l'utilisation de SNMPv3.

Voici les paramètres complets : « **--authprotocol sha --snmp-username snmpuser --authpassphrase ***** --privprotocol aes --privpassphrase ******* »

Cela permet d'indiquer les options de hachage, chiffrement, l'utilisateurs et les passphrases associées à celui-ci.

Dans notre menu « **host** » nous voyons désormais notre switch :

Puis nous allons vérifier les services associés à celui-ci :

Nous constatons bien l'utilisation de SNMPv3 :

The screenshot shows the Centreon monitoring interface for a host named "SW1". The top navigation bar includes tabs for "Details", "Timeline", "Graph", and "Notification". The "Details" tab is currently active, showing the following information:

- Current notification number:** 0
- Performance data:**

```
'total_cpu_5s_avg'=4.00%;0;100 'total_cpu_1m_avg'=5.00%;0;100
'total_cpu_5m_avg'=5.00%;0;100 'cpu_5s'=4.00%;0;100 'cpu_1m'=5.00%;0;100
'cpu_5m'=5.00%;0;90;0;95;0;100
```
- Command:**

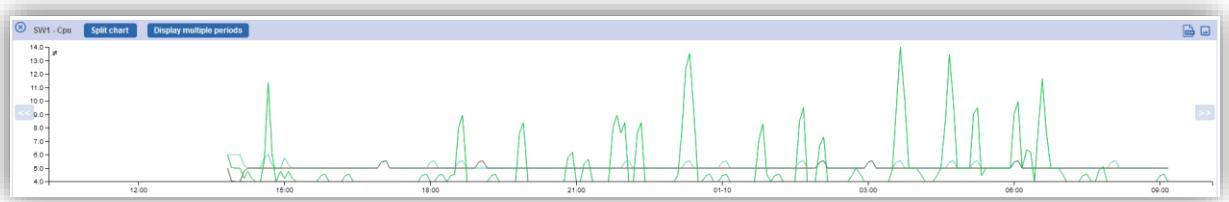
```
/usr/lib/centreon/plugins//centreon_cisco_standard_snmp.pl
--plugin=network::cisco::standard::snmp::plugin
--mode=cpu
--hostname=192.168.40.250
--snmp-version='3'
--snmp-community='public'
--authprotocol sha
--snmp-username snmpuser
--authpassphrase [REDACTED]
--privprotocol aes
--privpassphrase [REDACTED]
--warning-core-5s="
--critical-core-5s="
--warning-core-1m="
--critical-core-1m="
--warning-core-5m='90'
--critical-core-5m='95'
--warning-average-5s="
--critical-average-5s="
--warning-average-1m="
--critical-average-1m="
--warning-average-5m="
--critical-average-5m="
```

(Activé Windows)

Cliquez aux paramètres pour activer Windows.

-verbose

Comme vu précédemment, nous pouvons également avoir des graphiques d'utilisation des services (Voici un exemple pour le CPU) :



Nous allons maintenant pouvoir ajouter un nouveau service à notre hôte via le menu « **Services By Host** » comme vu précédemment.

Dans notre cas, nous allons superviser les interfaces de notre switch :

1. Service attaché à notre hôte SW1
2. Template de supervision des interfaces Cisco
3. Filtre sur l'interface Fa1/0/1. **Attention à la syntaxe à respecter à l'identique** pour le filtre sur une interface (si le paramètre est vide Centreon va checker toutes les interfaces par défaut)

Dans le menu « **Services** », nous constatons que celui-ci fonctionne correctement :

The screenshot shows the Zabbix 'Resources Status' page. The main table lists resources: SW-Interfaces, Environment, Memory, Cpu, and Ping, all in 'OK' status. The 'Status information' panel for 'SW-Interfaces' provides detailed traffic and error statistics. The bottom right corner shows performance data for the Fa1/0/1 interface.

Dans la capture ci-dessus, nous voyons que l'interface est up ainsi que toutes les informations concernant le trafic, les paquets en erreurs ect...

Nous allons maintenant superviser une interface supplémentaire la « **Fa1/0/2** ».

Pour cela, nous allons dans la configuration du service et ajoutons notre interface dans l'option « **Interface Name** » en respectant la syntaxe suivante :

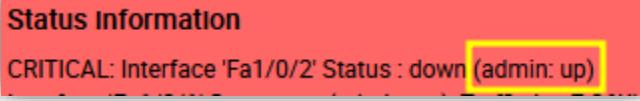
The screenshot shows the 'Check Command' configuration screen. It includes fields for 'Name' (containing 'INTERFACENAME'), 'Value' (containing '^Fa1/0/1\$|^Fa1/0/2\$'), and 'Password'.

L'interface **Fa1/0/2** n'ayant pas d'équipement raccordé sur celle-ci le service devrait passer en alerte « **Critical** » ce que nous vérifions :

The screenshot shows the Centreon Monitoring interface under the 'Resources Status' tab. A search bar at the top left contains the query 'state:unhandled status:critical'. Below the search bar is a toolbar with buttons for 'Acknowledge', 'Set downtime', 'Forced check', and 'Display view' (set to 'All'). The main area displays a table of resources with columns: Status, Resource, Parent, G, Duration, Last check, and Information. Five resources are listed as 'Critical': SWI-Interfaces, SRV-DHCPW1, SRV-ADW1, SRV-WEBL1, and SRV-WEBL1. The 'Information' column for SWI-Interfaces shows the error: 'CRITICAL: Interface Fa1/0/2 Status : down (admin: up)'. To the right of the table is a detailed view for the selected resource, 'SWI-Interfaces'. This view includes tabs for 'Details', 'Timeline', 'Graph', and 'Notification'. The 'Details' tab is active and contains sections for 'Monitoring server', 'Last status change', 'Last check with OK status', 'Check duration', 'Status change percentage', and 'Performance data'. The 'Status information' section is highlighted with a yellow box and contains the critical message: 'CRITICAL: Interface 'Fa1/0/2' Status : down (admin: up)'. The full message is: 'CRITICAL: Interface 'Fa1/0/2' Status : down (admin: up)'. Interface Fa1/0/1 Status : up (admin: up), Traffic In : 7.066kb/s, 0.0100000000. Interface Fa1/0/1 Status : up (admin: up), Traffic In : 982.27b/s (0.0%), Packets In Discard : 0.00% (0 on 276), Packets In Error : 0.00% (0 on 276). Interface Fa1/0/1 Status : up (admin: up), Traffic Out : 7.066kb/s, 0.0100000000. Interface Fa1/0/1 Status : up (admin: up), Packets Out Error : 0.00% (0 on 44), Packets In Err : 0.00% (0 on 276), Packets In Fcserrr : 0.00% (0 on 276). Interface Fa1/0/2 Status : down (admin: up)'. The 'Performance data' section lists several metrics for Fa1/0/1 and Fa1/0/2.

Ci-dessus nous constatons que le port Fa1/0/2 est en état « **Down** ».

Pour rappel : une interface « **administratively down** » ne remonterait pas en alerte, dans notre cas elle remonte car celle-ci est « **administratively up** » comme l'indique le message suivant :



3. Conclusion

En conclusion, ce projet de mise en place d'une solution de supervision pour l'ADRAR répond aux exigences de contrôle et de performance nécessaires à une infrastructure moderne.

La supervision centralisée via Centreon permet de garantir la disponibilité des équipements et services critiques, avec des seuils d'alerte adaptés pour la RAM, le CPU, l'espace disque ect..

L'utilisation de SNMPv3 pour les systèmes Linux et équipements réseau, et de SNMPv2c pour Windows, assure un bon niveau de sécurité tout en prenant en compte les contraintes techniques. Cette solution modulaire, évolutive et sécurisée constitue une base solide pour le suivi et l'optimisation de l'infrastructure, tout en restant adaptée aux besoins futurs de l'établissement.

La supervision étant un sujet complexe et vaste nous sommes restés à l'essentielle via de la supervissons d'équipements et services dans cette procédure. Cependant, beaucoup d'autres améliorations et fonctionnalités pourraient être configurées à l'avenir comme la découverte d'équipement automatique, la mise en place de Dashboard personnalisé pour avoir une vue plus intuitive ect...

4. Annexes

Installation de Centreon : <https://archives-docs.centreon.com/20.10/fr/docs/getting-started/installation-first-steps>

Installation des plugins : <https://docs.centreon.com/docs/22.10/monitoring/pluginpacks/>

Supervision d'un hôte Windows : <https://docs.centreon.com/docs/getting-started/monitor-windows-server-with-snmp/>

Supervision d'un hôte Linux : <https://docs.centreon.com/docs/getting-started/monitor-linux-server-with-snmp/>

Supervision d'un hôte Cisco : <https://docs.centreon.com/docs/getting-started/monitor-cisco-router-with-snmp/>

Configuration du plugin MariaDb : <https://docs.centreon.com/pp/integrations/plugin-packs/procedures/applications-databases-mysql/>

Configuration du plugin DHCP : <https://docs.centreon.com/pp/integrations/plugin-packs/procedures/applications-microsoft-dhcp-snmp/>

Recommandation ANSSI supervision (Chapitre 6.1 Supervision des évènements) :
https://cyber.gouv.fr/sites/default/files/2022/02/ansi-guide-recommandations_configuration_commutateurs_pare-feux_hirschmann.pdf