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

1.1 Demandes du client

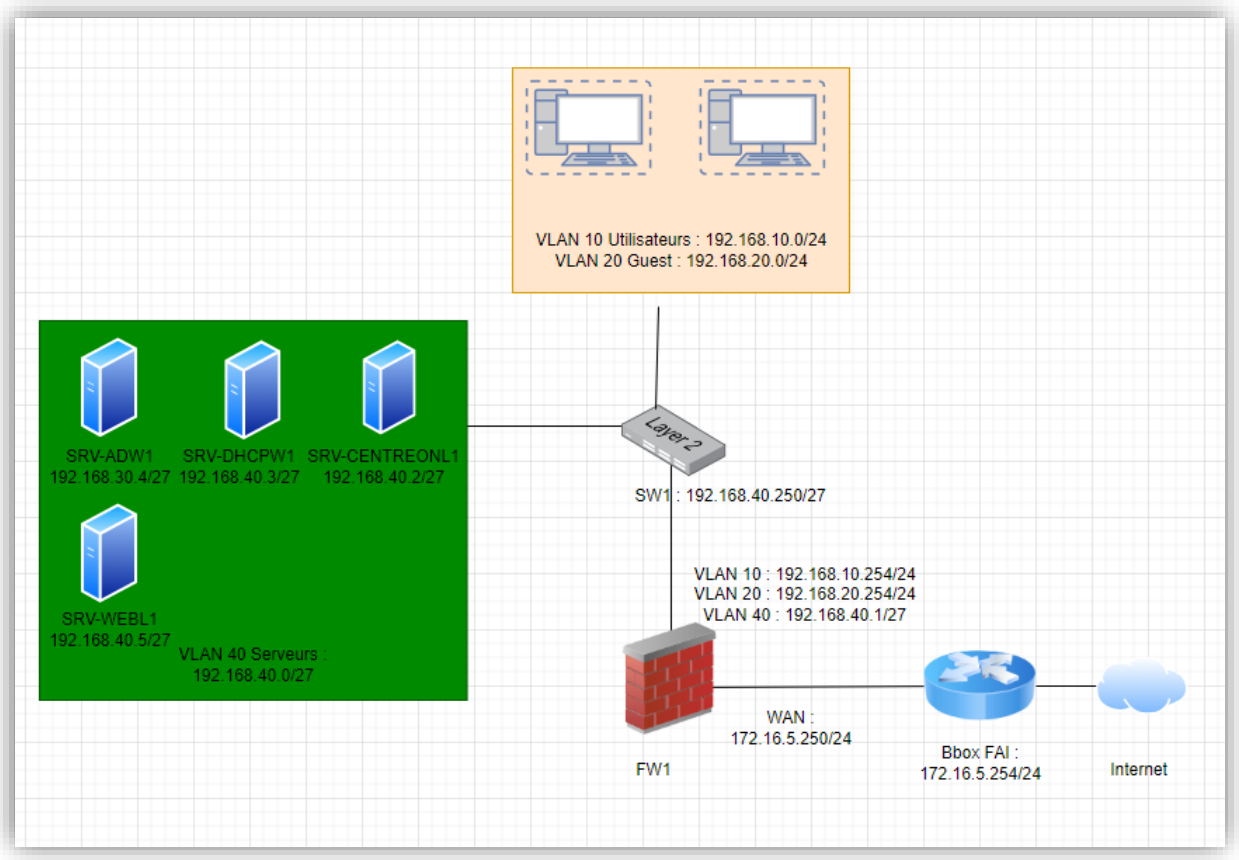
Nous sommes contactés par l'ADRAR afin de mettre en place une solution de supervision.

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 harware des équipements (RAM, CPU, disques ect…) mais aussi des services qui sont hébergés sur les serveurs (MariaDB, DHCP ect…)

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 SNPMv2.
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 prêtes à l'emploi) : https://docs.centreon.com/docs/category/installation-of-a-central-server/

Notions :

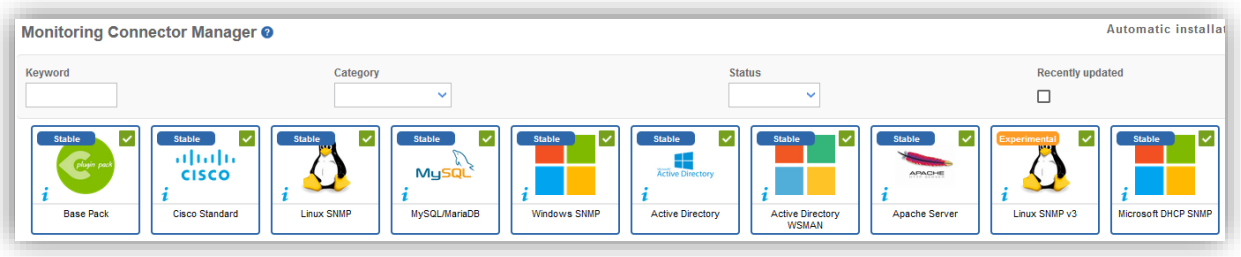
Pour rappel, voici quelques termes à connaitre afin de mieux comprendre la mise en place de notre solution :

- 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 »)** :

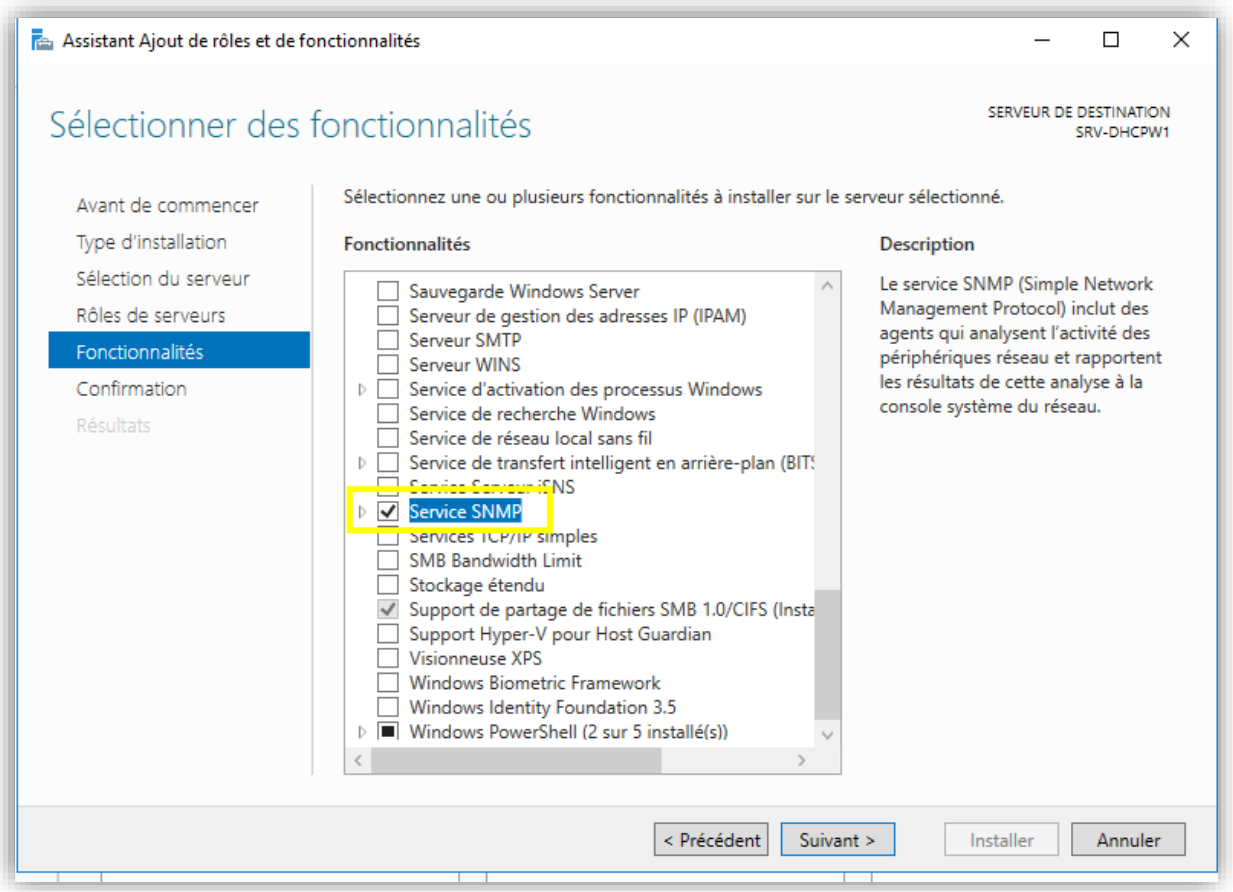


2.1 Supervision d'un hôte Windows

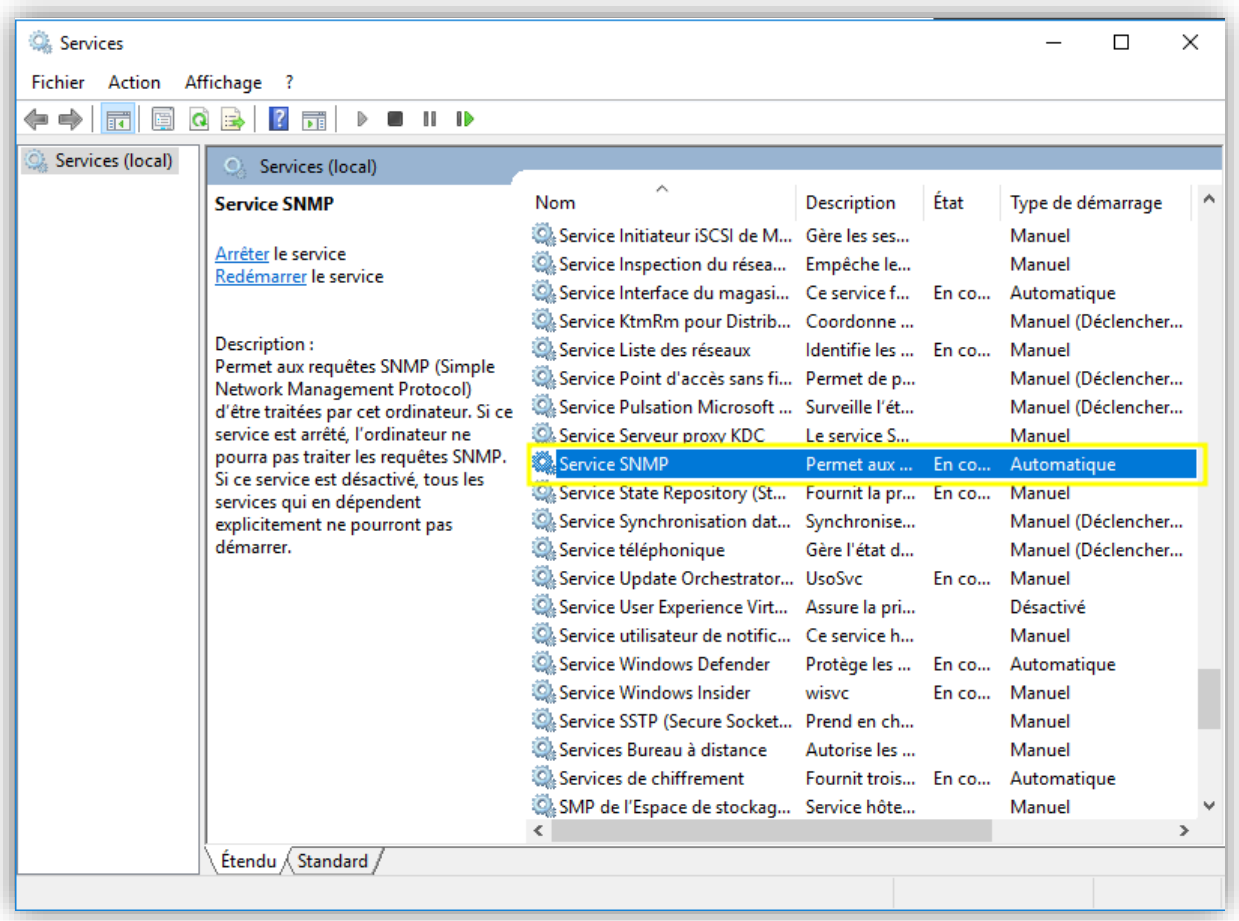
Nous commençons par superviser le serveur DHCP **« SRV-DHCPW1 »,** ensuite nous ajouterons le serveur AD nommé **« SRV-ADW1 ».**

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

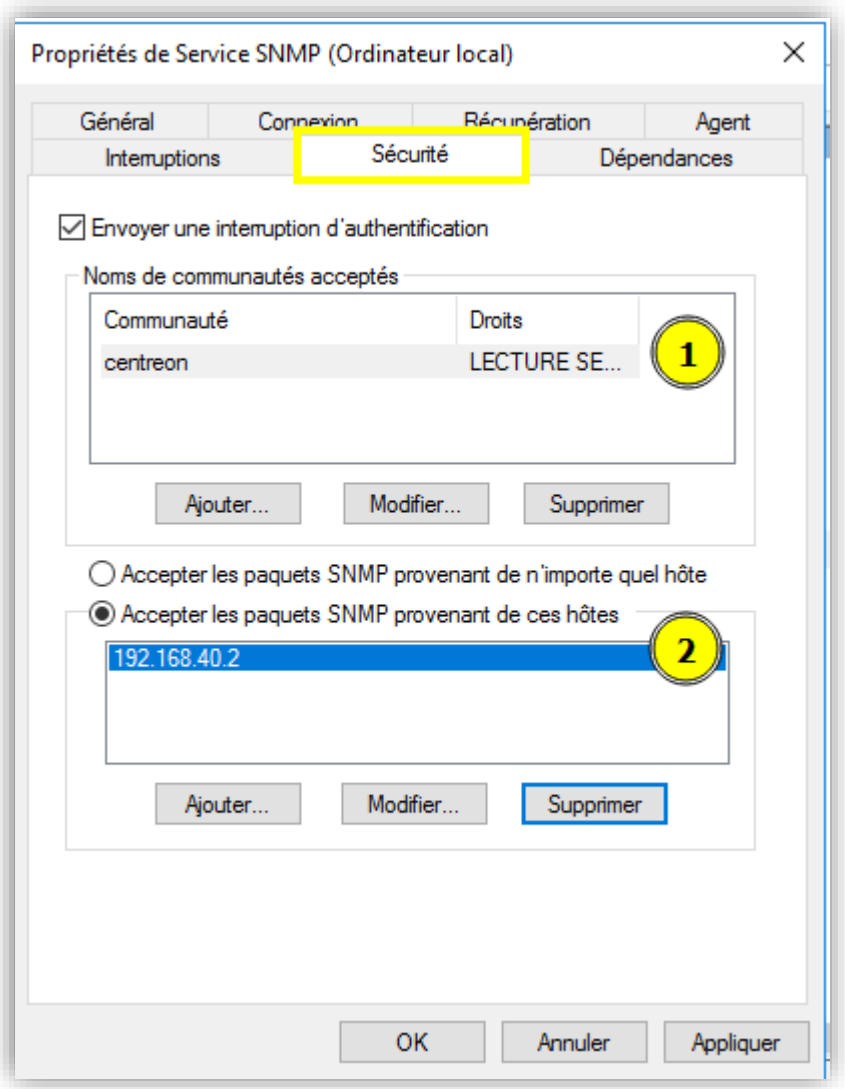
Pour cela, il faut se rendre dans le menu d'installation des rôles et fonctionnalités et cocher la fonctionnalité suivante :



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 :

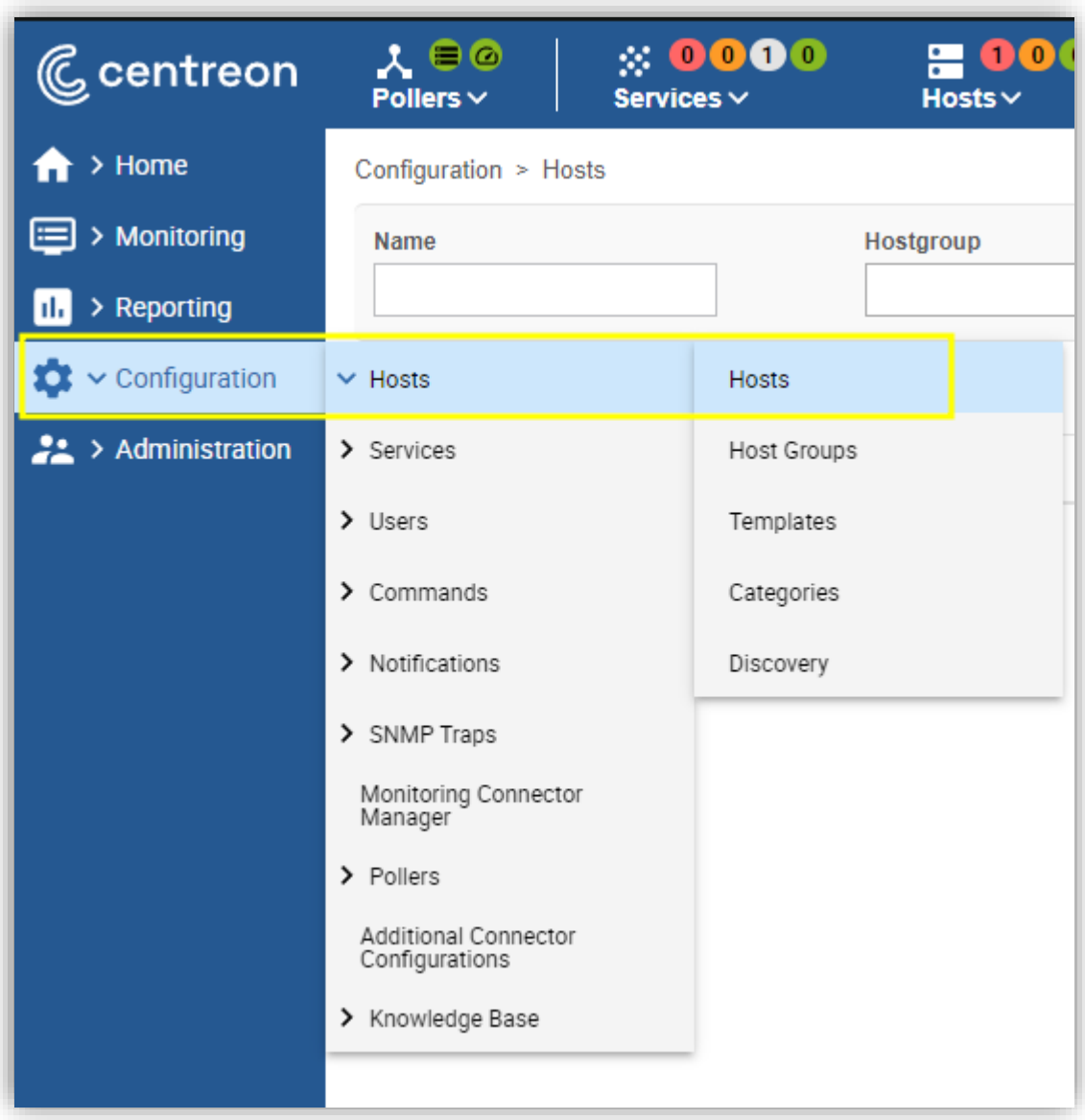


Nous allons nous rendre dans l'onglet **« Sécurité »** et définir les options nécessaires :

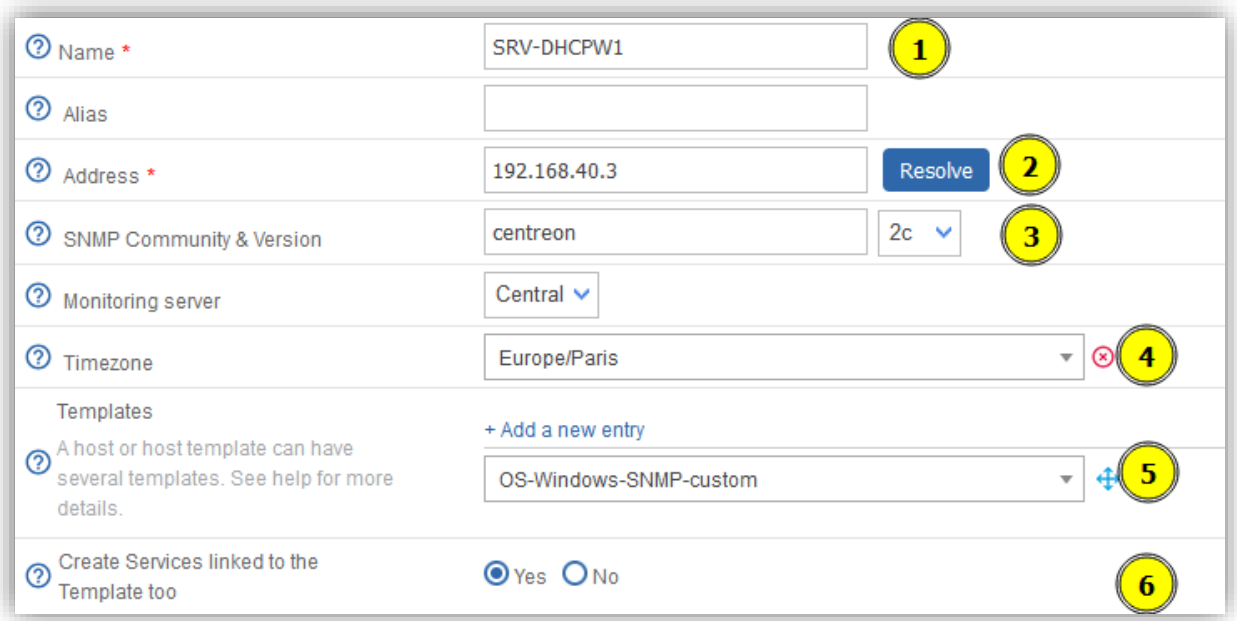


1. Nom de la communauté en RO
2. Accepte les requêtes uniquement depuis l'IP de notre Pooler

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

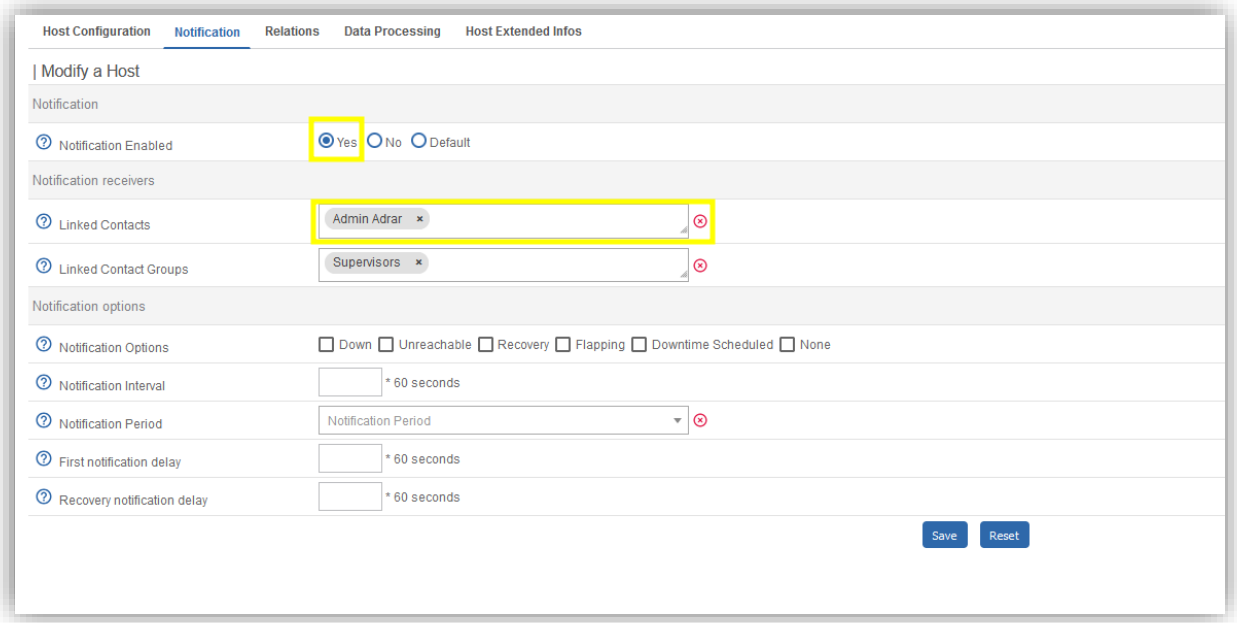


Nous cliquons sur **« Add »** pour ajouter un nouvel hôte et définissons les paramètres suivants :



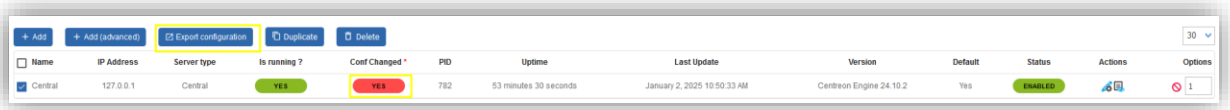
1. Nom du serveur
2. IP du serveur
3. Communauté et version SNMP utilisée (nom de communauté pouvant être modifié pour en mettre une plus complexe)
4. Zone de temps
5. Template utilisé pour la création de services
6. Créer les services associés à cet hôte via le template

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 :

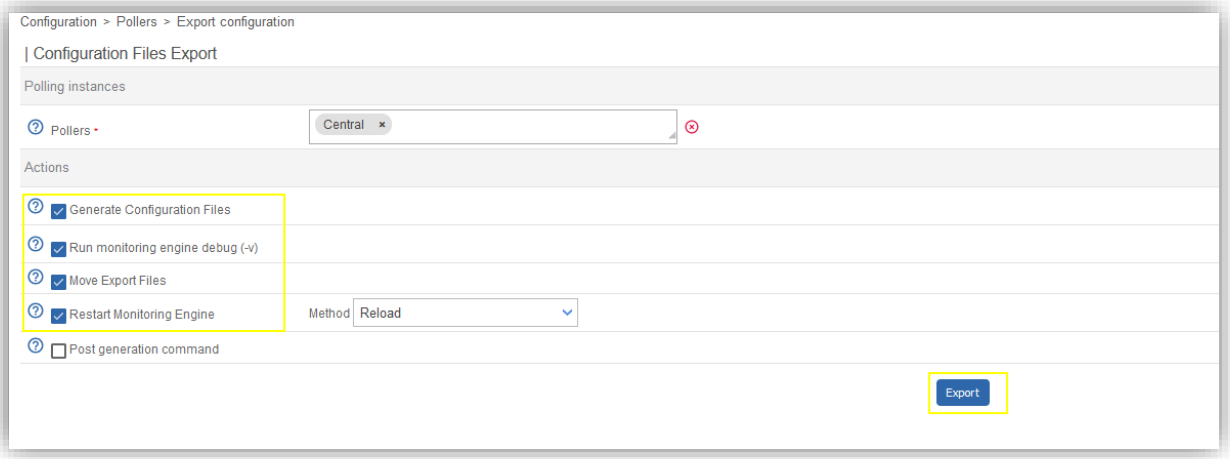


Une fois l'hôte créé, il est nécessaire de redémarrer le service Centreon.

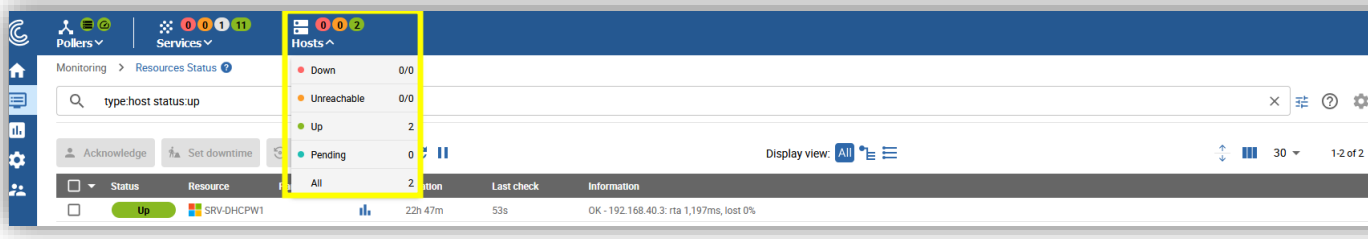
Pour cela, nous allons dans le menu **« Configuration »** puis **« Poolers ».**
Nous voyons que la configuration a changé ,il faut donc sélectionner le serveur et cliquer sur **« Export Configuration »** :



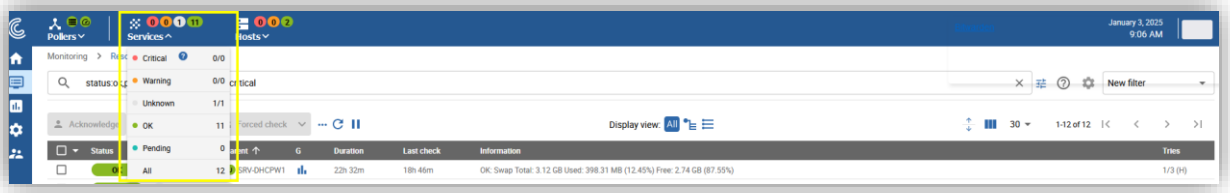
Une fois cela fait, nous cochons les 4 premières cases afin de charger la nouvelle configuration et redémarrer le service :

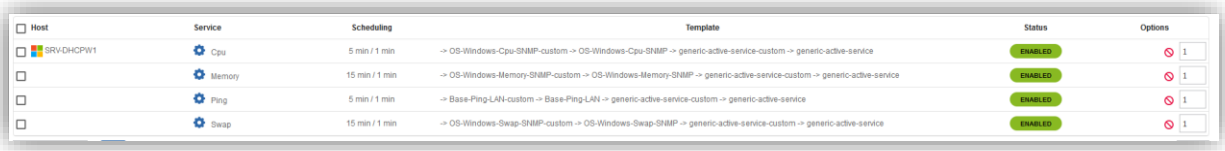


Maintenant, dans le menu **« Hosts »** nous voyons notre serveur **« up »**

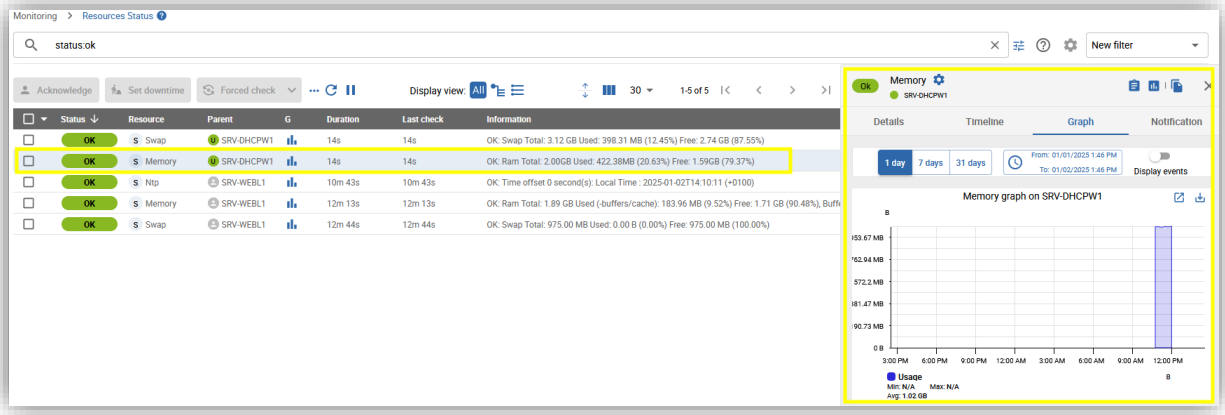


Nous allons ensuite nous rendre dans le menu **« Services »** et retrouvons tous les services supervisés, comme l'utilisation de la RAM, du CPU ect…



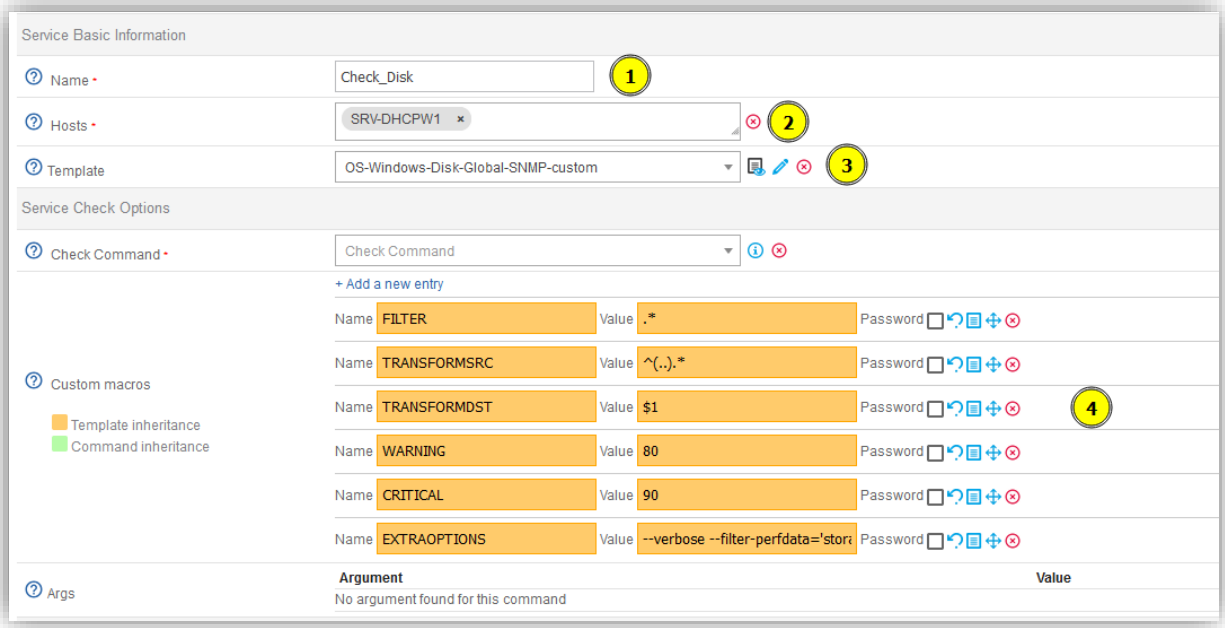


En cliquant sur le service, nous avons également la possibilité d'avoir plus de détails, voici un exemple pour des graphiques d'utilisation de la RAM :



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

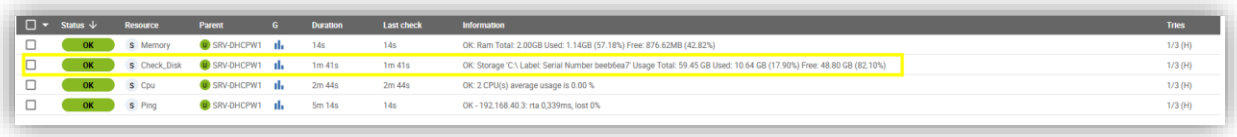
Pour cela, nous allons dans le **« Configuration »** ; **« Services »** puis **« Services by host »** et cliquons sur **« Add ».**
Nous arrivons sur cette page et renseignons les différents champs :



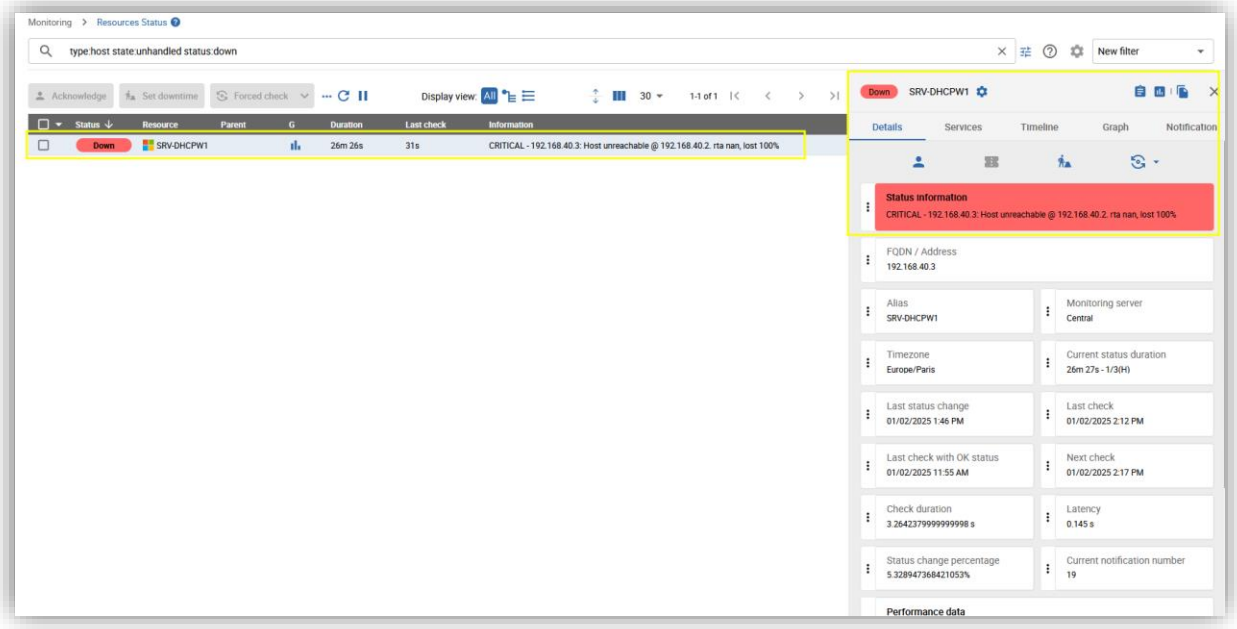
1. Nom du service à ajouter
2. Hôte rattaché à ce service

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…

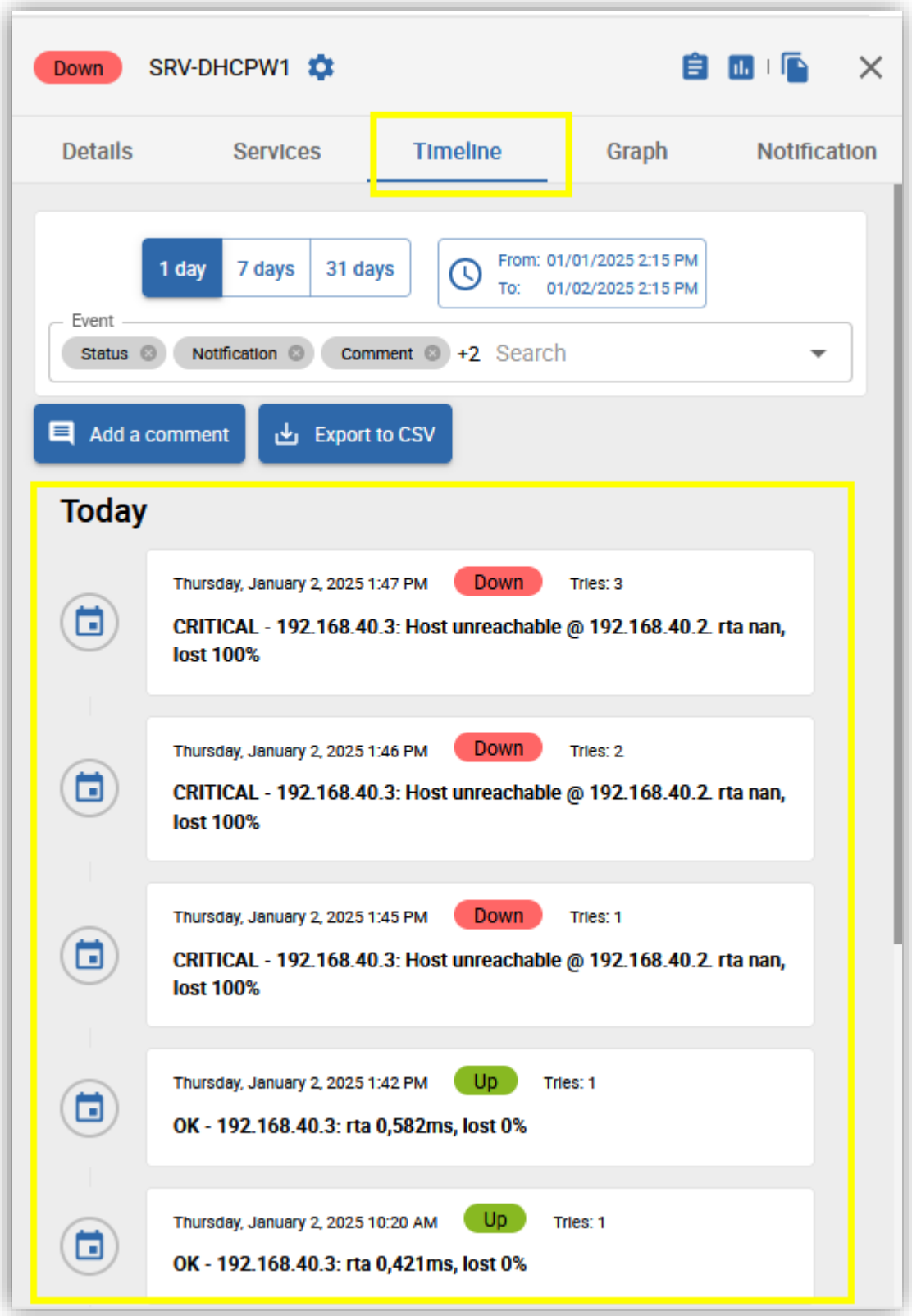
Une fois ajouté, nous redémarrons le pooler, comme vu précédemment, puis nous retournons dans le menu **« Services »**.
Nous constatons notre nouveau service avec les informations d'utilisation du disque :



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 » :**

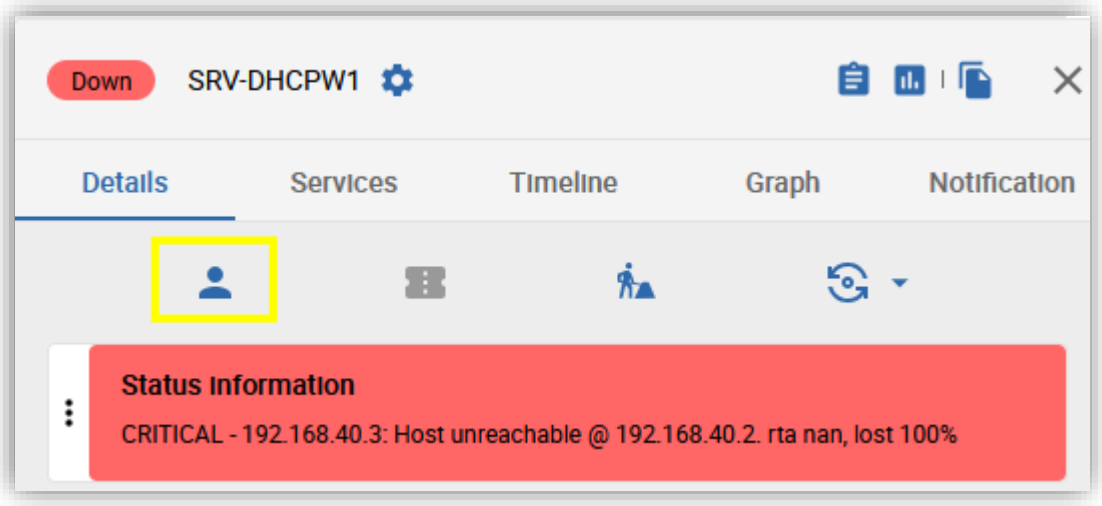


Dans le menu **« Timeline »** nous avons l'historique des états UP/DOWN :

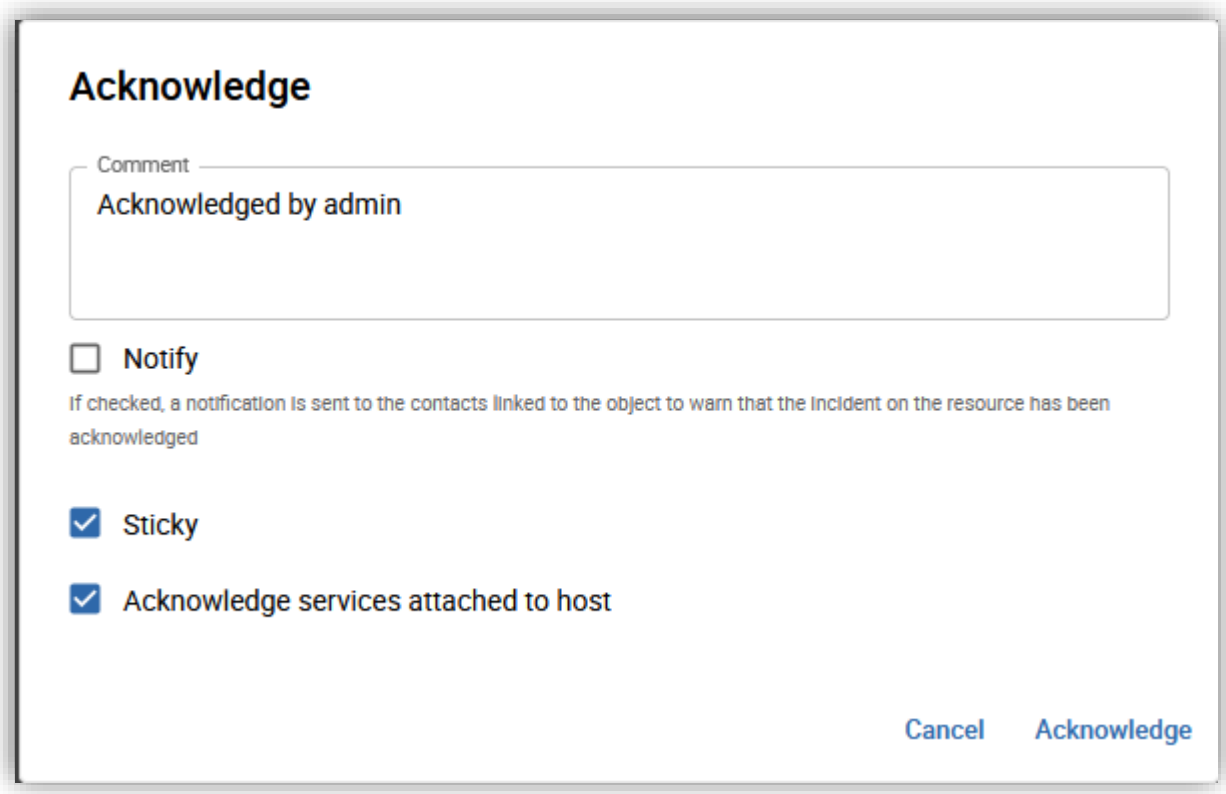


Si un serveur est **« Down »** pour des raison de maintenance ou autre, il est possible d' **« Acknowlegde »** celui-ci temporairement afin qu'il ne remonte pas dans les alertes de la supervision.

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

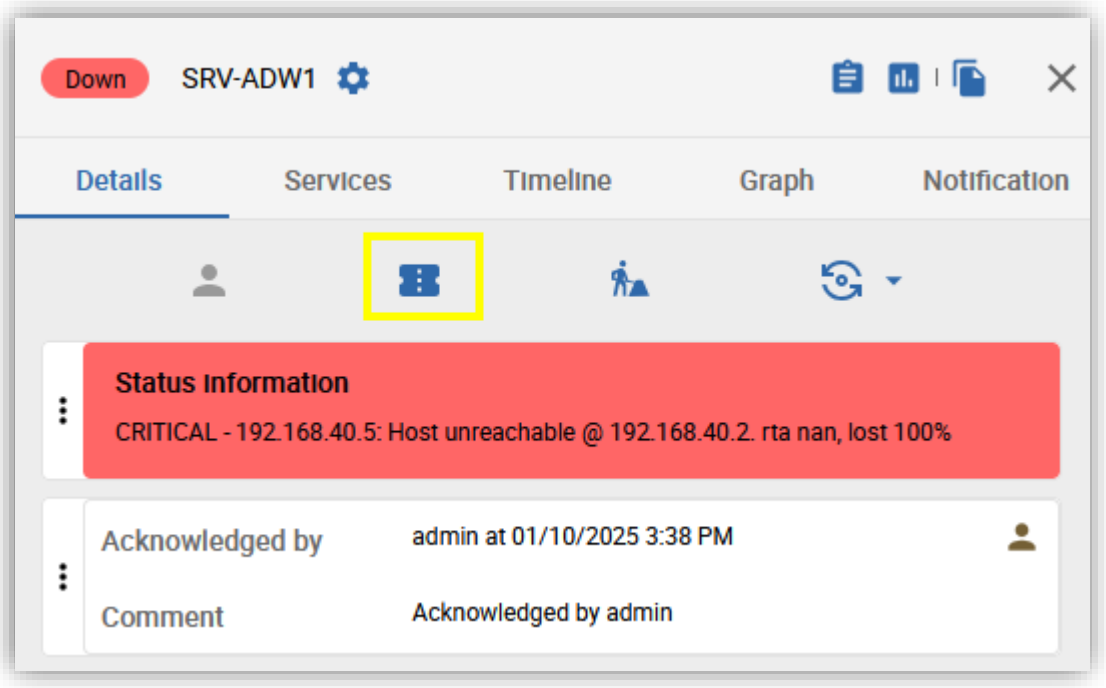


Une fenêtre apparais demandant confirmation avec la possibilité d'ajouter une note :



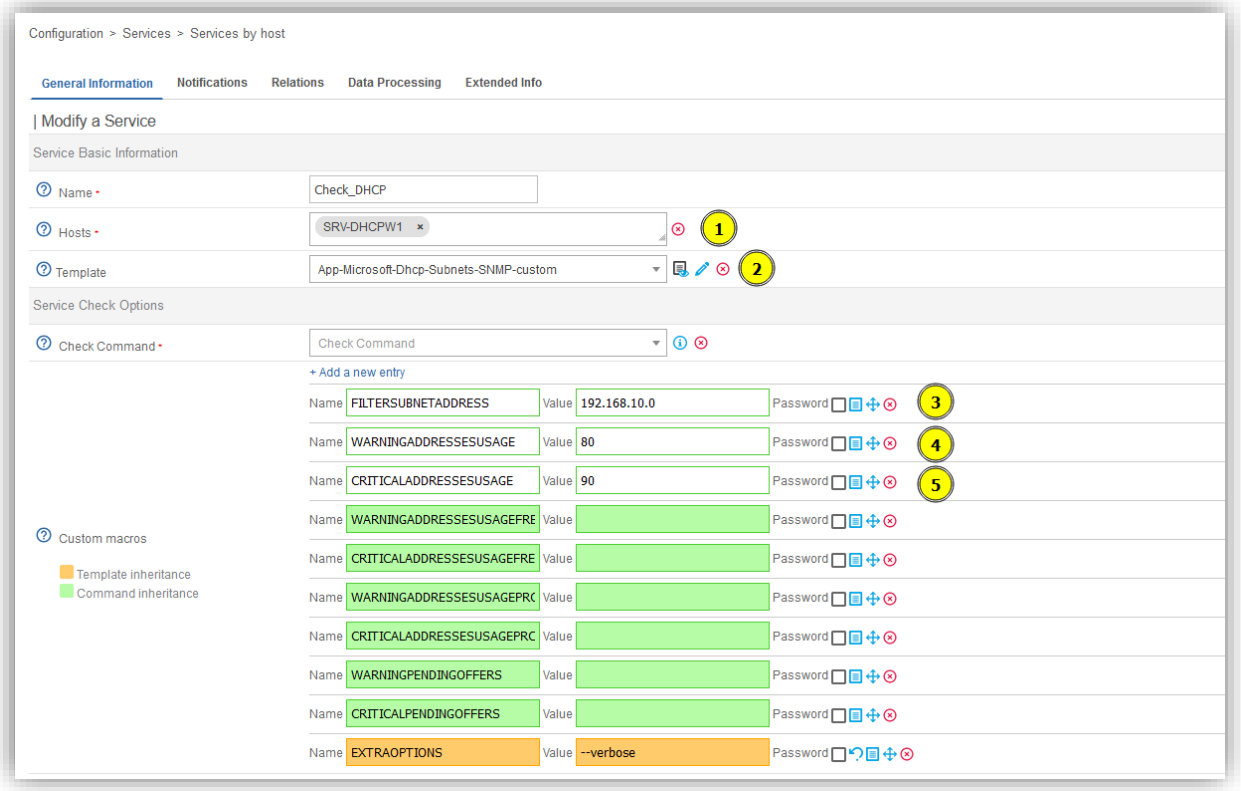
Ni notre hôte ni les services n'apparaitrons dans les alertes désormais.
Dès la maintenance fini, il suffit de rechercher le serveur via le Menu **« Host »** puis **« All »** et cliquer

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



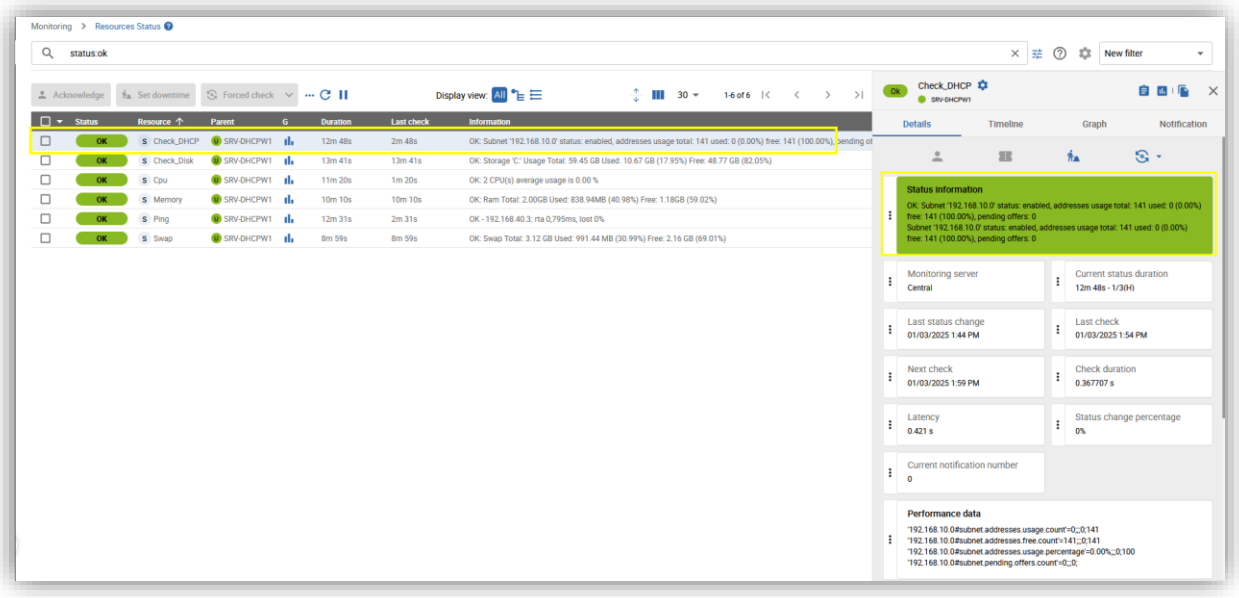
Maintenant, nous allons superviser le service DHCP du serveur ce qui nous permettra d'avoir des informations sur nos pools IP.

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



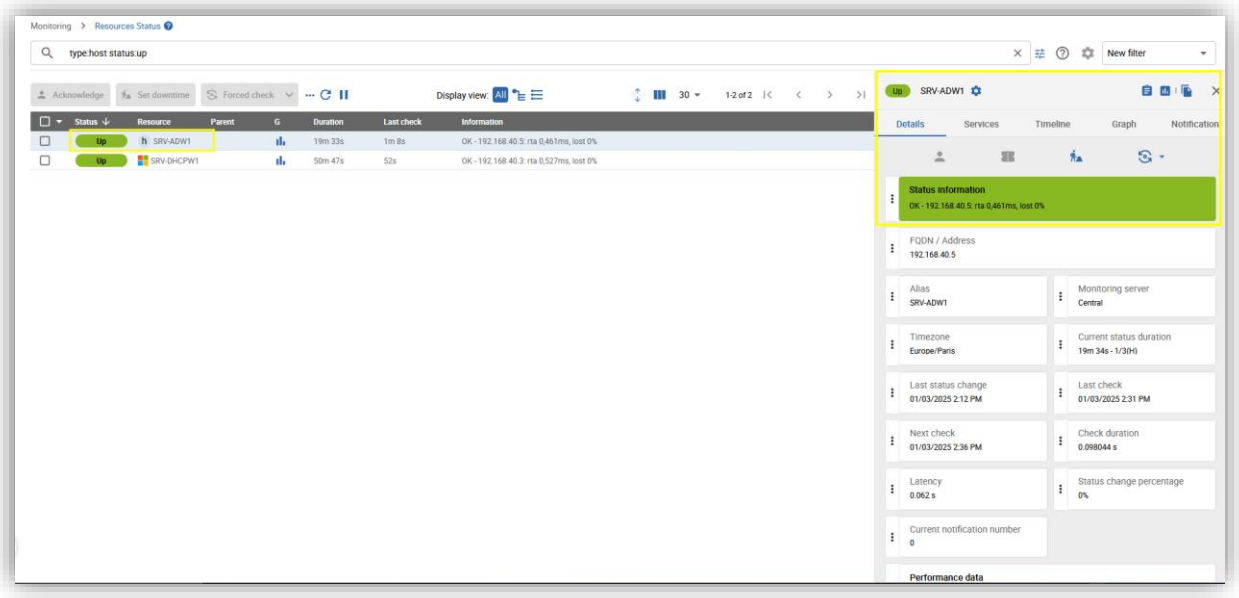
1. Hôte rattaché au service
2. Template pour la supervision du service DHCP
3. Filtre sur le pool IP du VLAN 10
4. Warning à 80% d'utilisation des IP du pool
5. Alerte critique à 90% d'utilisation des IP du pool

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

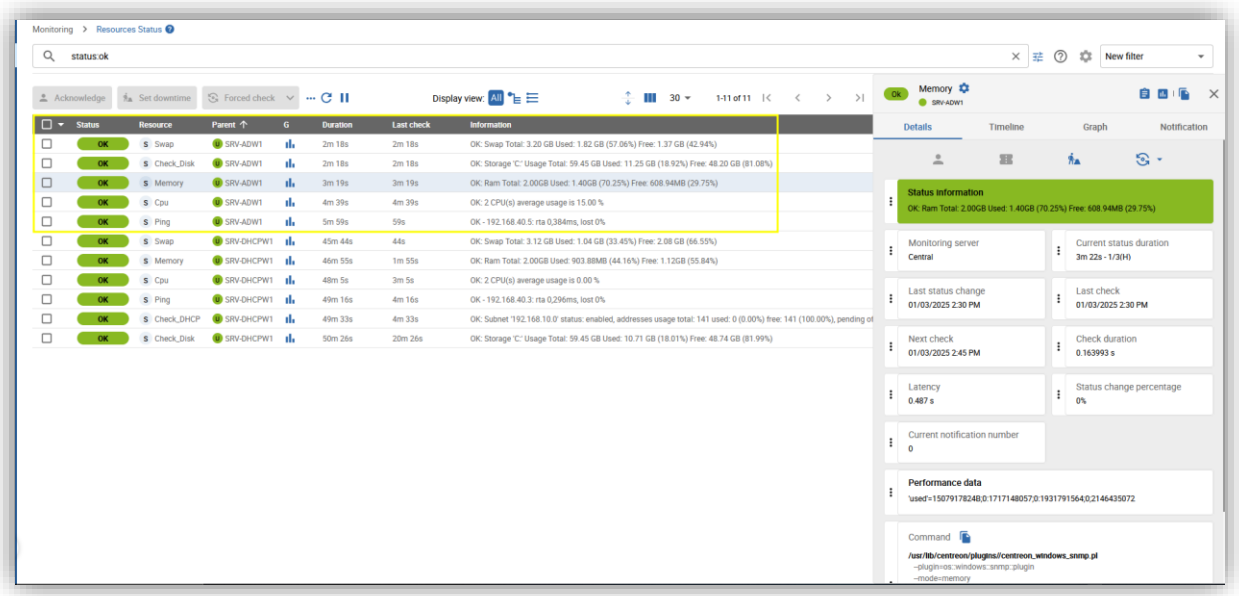


Nous voyons ci-dessus les informations concernant le Pool (pourcentages IP utilisées, IP libres ect…)

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



Et nous voyons également les services associés :



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
```

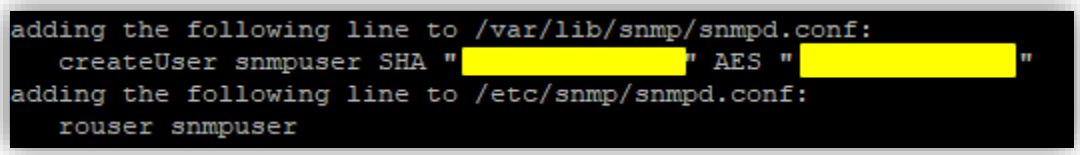
Une fois cela fait, nous allons créer un utilisateur pour l'utilisation de SNMPv3 (Les passphrases utilisées pour l'authentification du compte n'apparaitront pas en clair dans cette procédure)

```
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 :



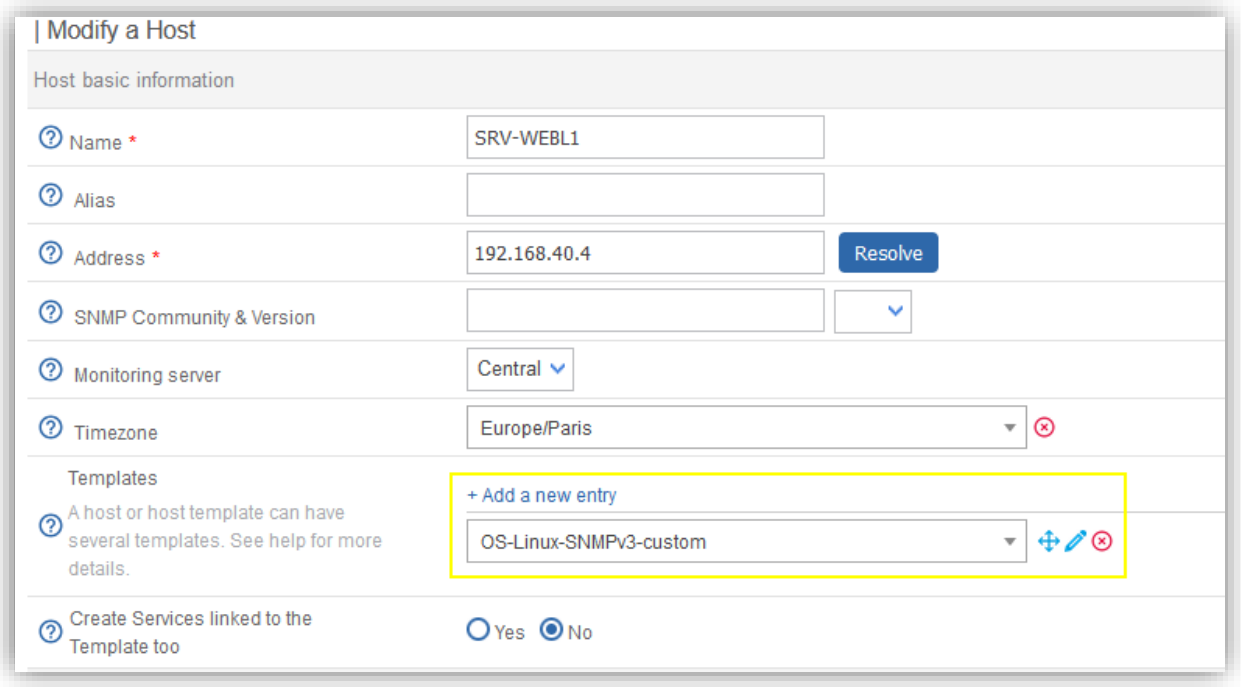
Une fois cela fait, nous allons dans le fichier de configuration du service et l'éditons pour ajouter l'interface et le port d'écoute de notre agent :

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

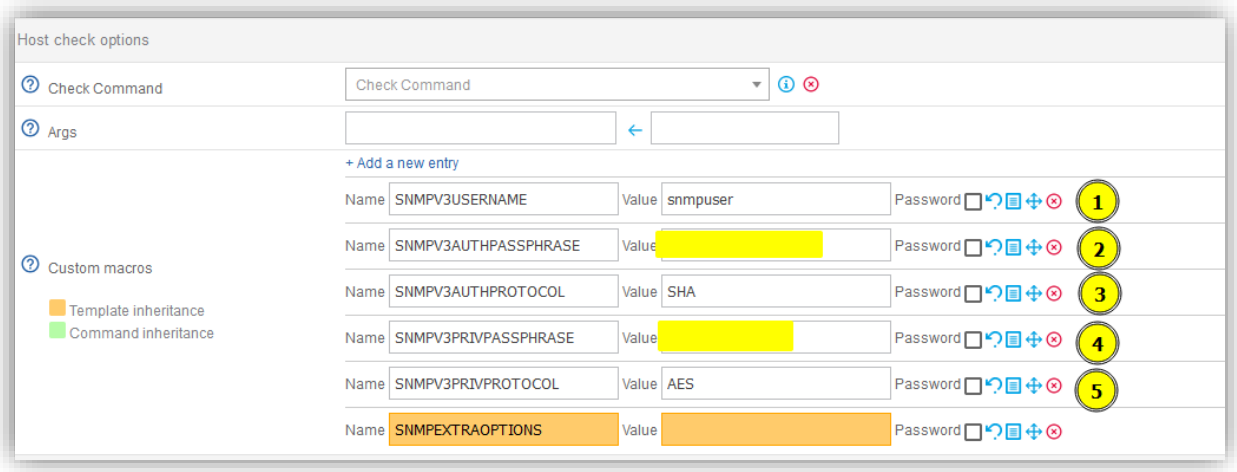
Nous démarrons et vérifions le statut du service :

```
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 -LOw -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 :

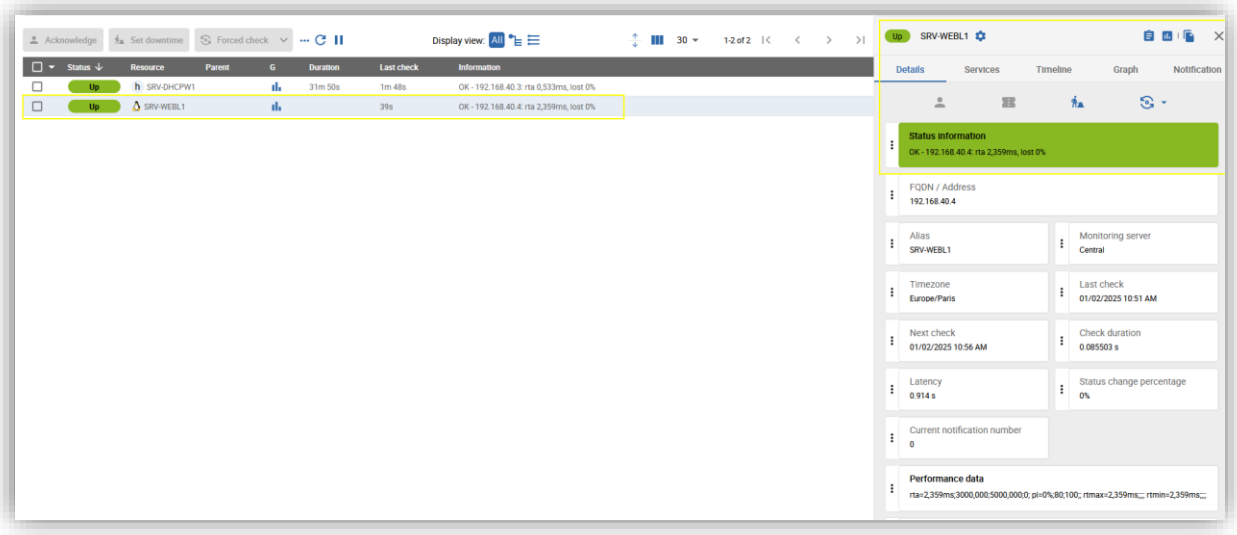


Plus bas dans la page, nous configurons les options pour SNMPv3 :

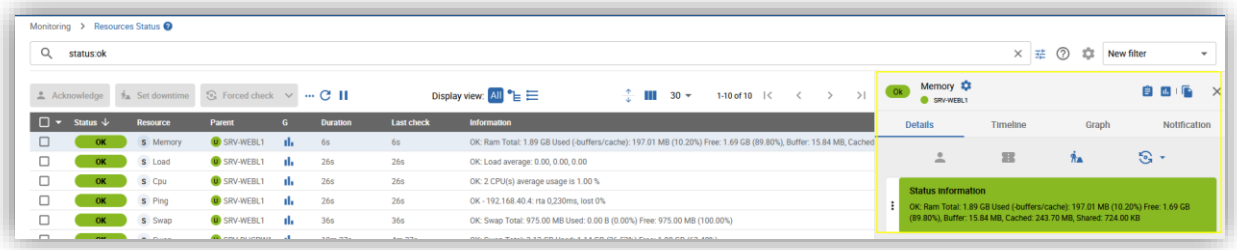


1. Utilisateur créé précédemment pour l'utilisation de SNMPv3
2. Passphrase d'authentification
3. Protocole de hachage (Le plugin utilise SHA 256 par défaut)
4. Passphrase privée
5. Protocole de chiffrement (Le plugin utilise AES 256 par défaut)

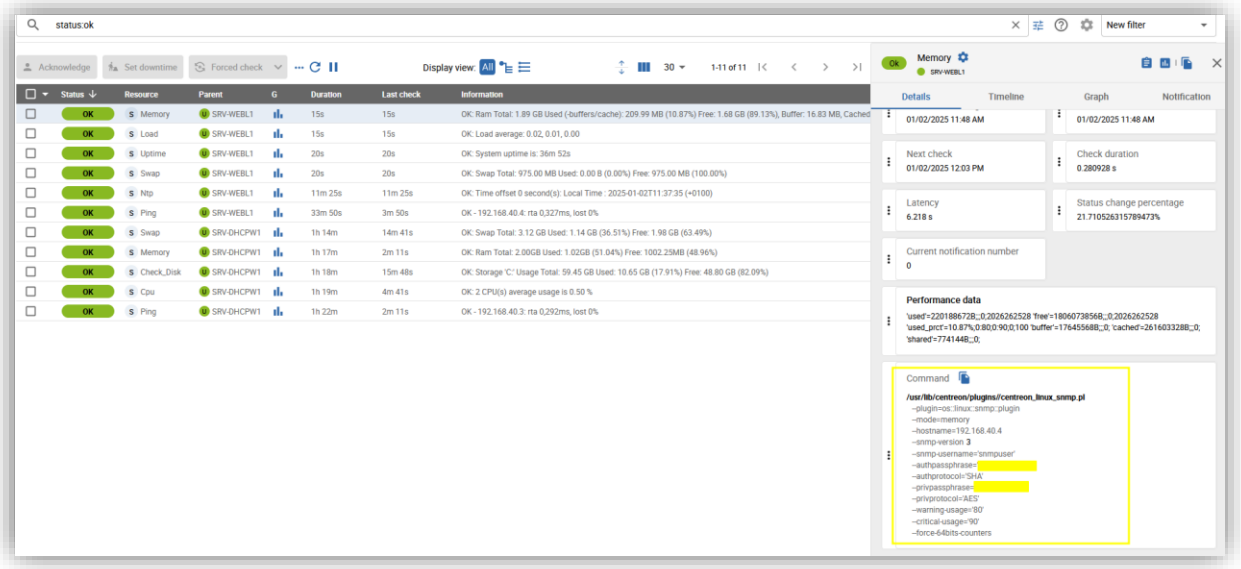
Nous pouvons maintenant redémarrer le pooler, puis nous rendre dans le menu **« hôtes »** afin d'en vérifier le bon fonctionnement :



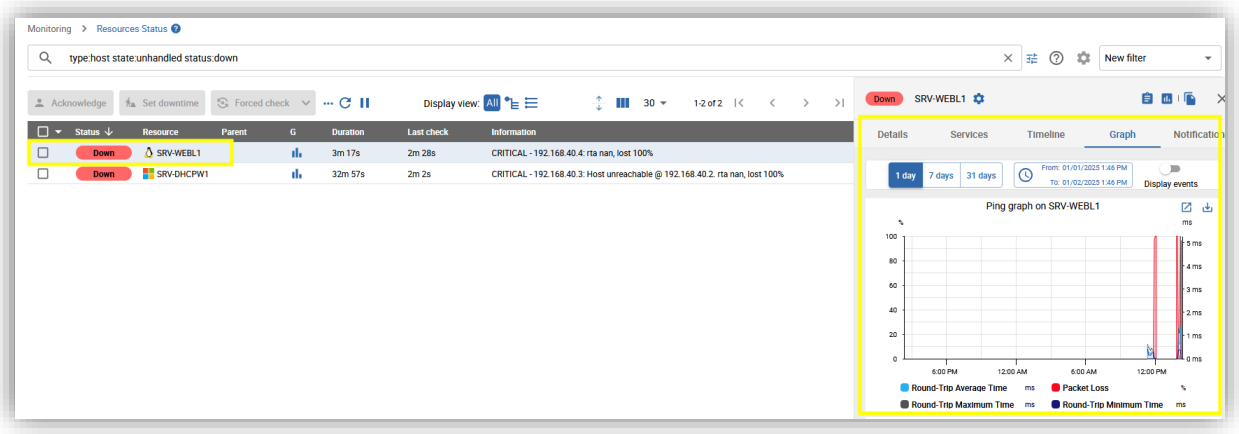
Nous allons maintenant vérifier les services pour cet hôte :



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



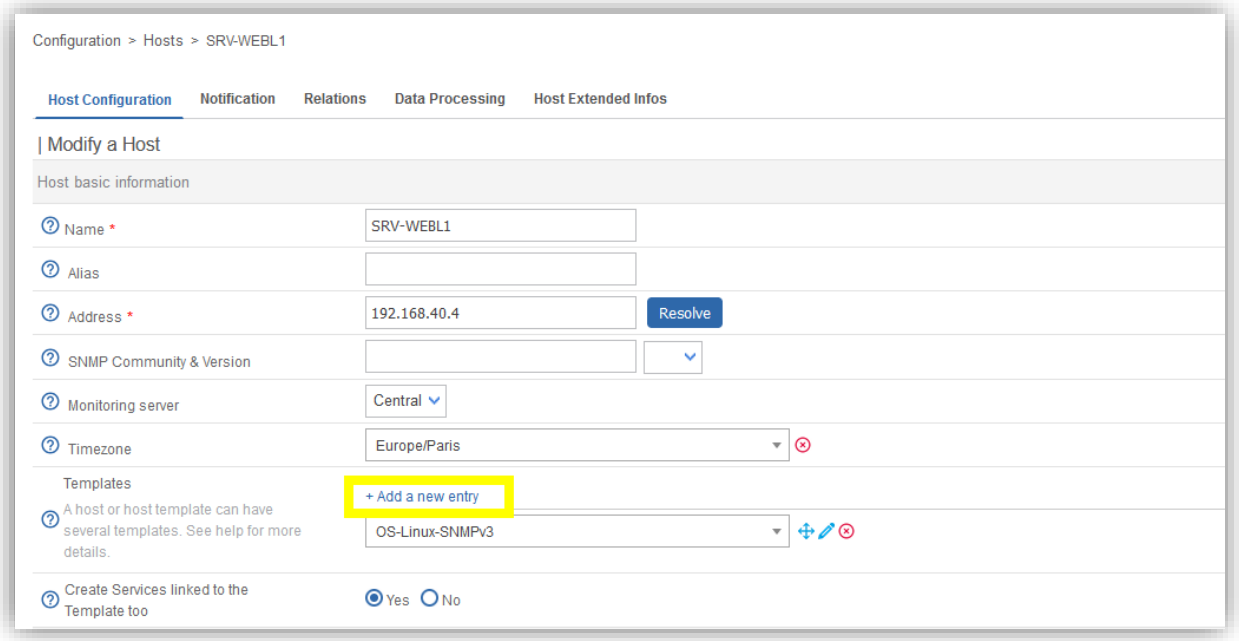
Maintenant que tout est fonctionnel, nous effectuons un test d'arrêt du serveur pour constater qu'il passe **« Down »** :



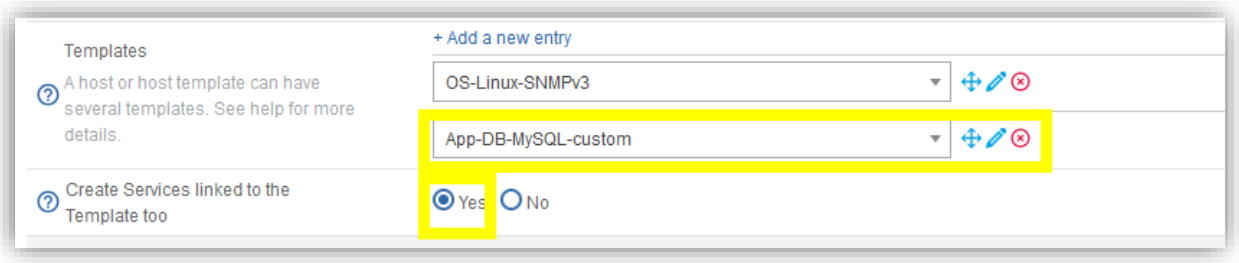
Ci-dessus, nous constatons que la supervision est fonctionnel et voyons également un graphique des pertes de ping.

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.

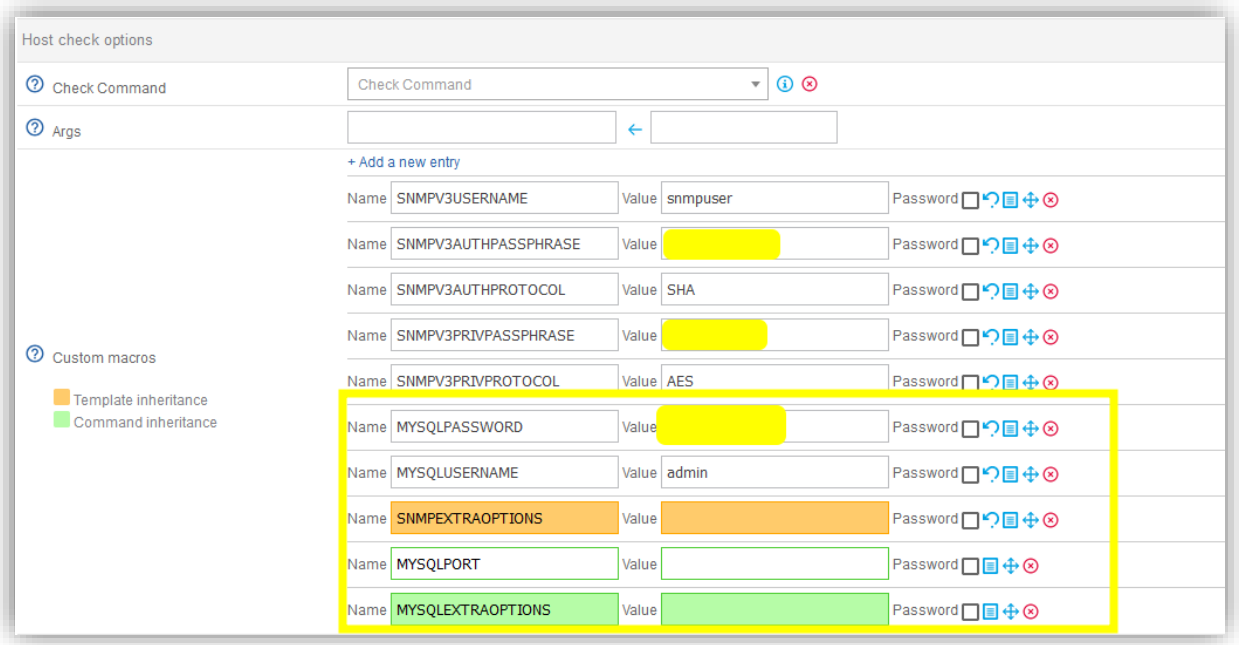
Nous allons nous rendre dans le menu **« Configuration »** - **« Host »** et sélectionner notre serveur.
Dans la partie **« Template »** nous sélectionnons **« Add a new entry »** :



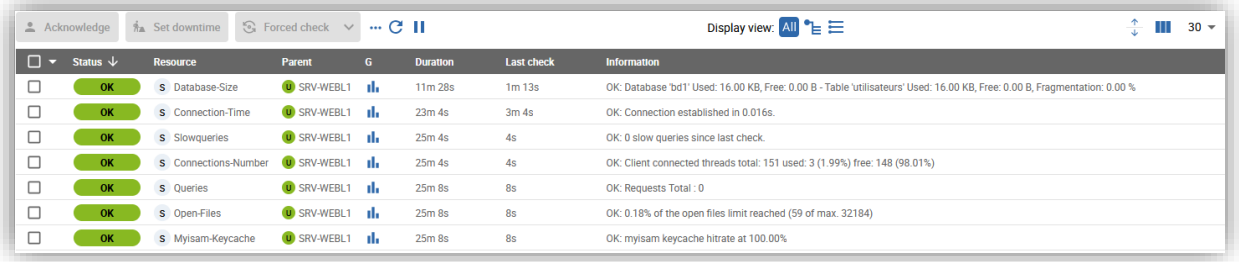
Nous choisissons donc le template associé à « **Mysql »** et créons les services associés :



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) :

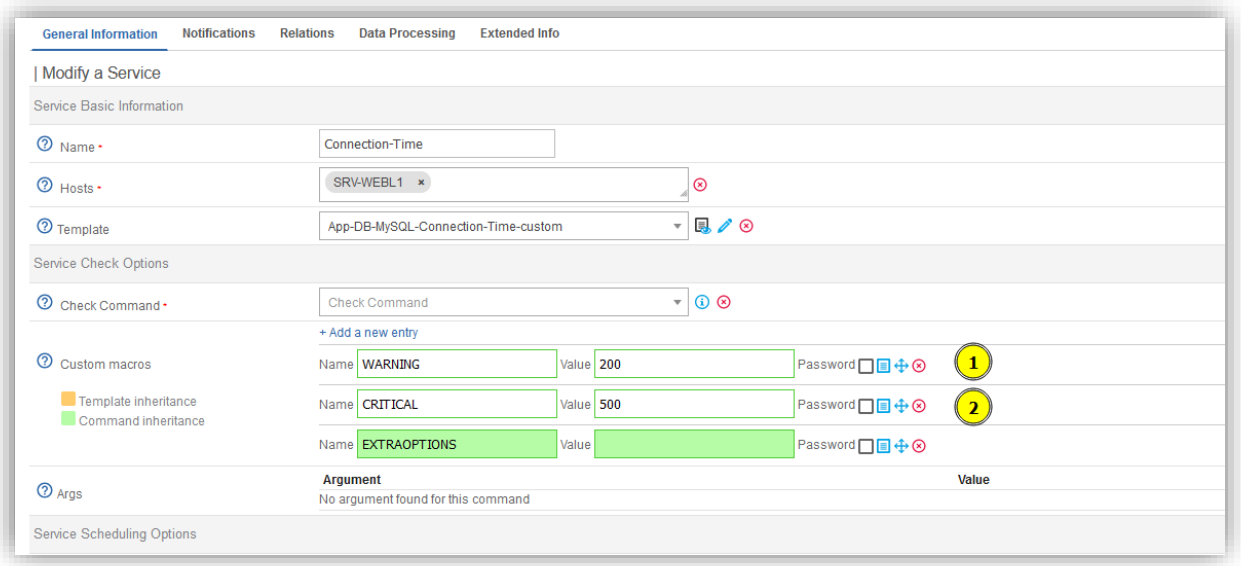


Nous sauvegardons la configuration et redémarrons le pooler.
Plusieurs nouveaux services sont maintenant rattachés à notre hôte :



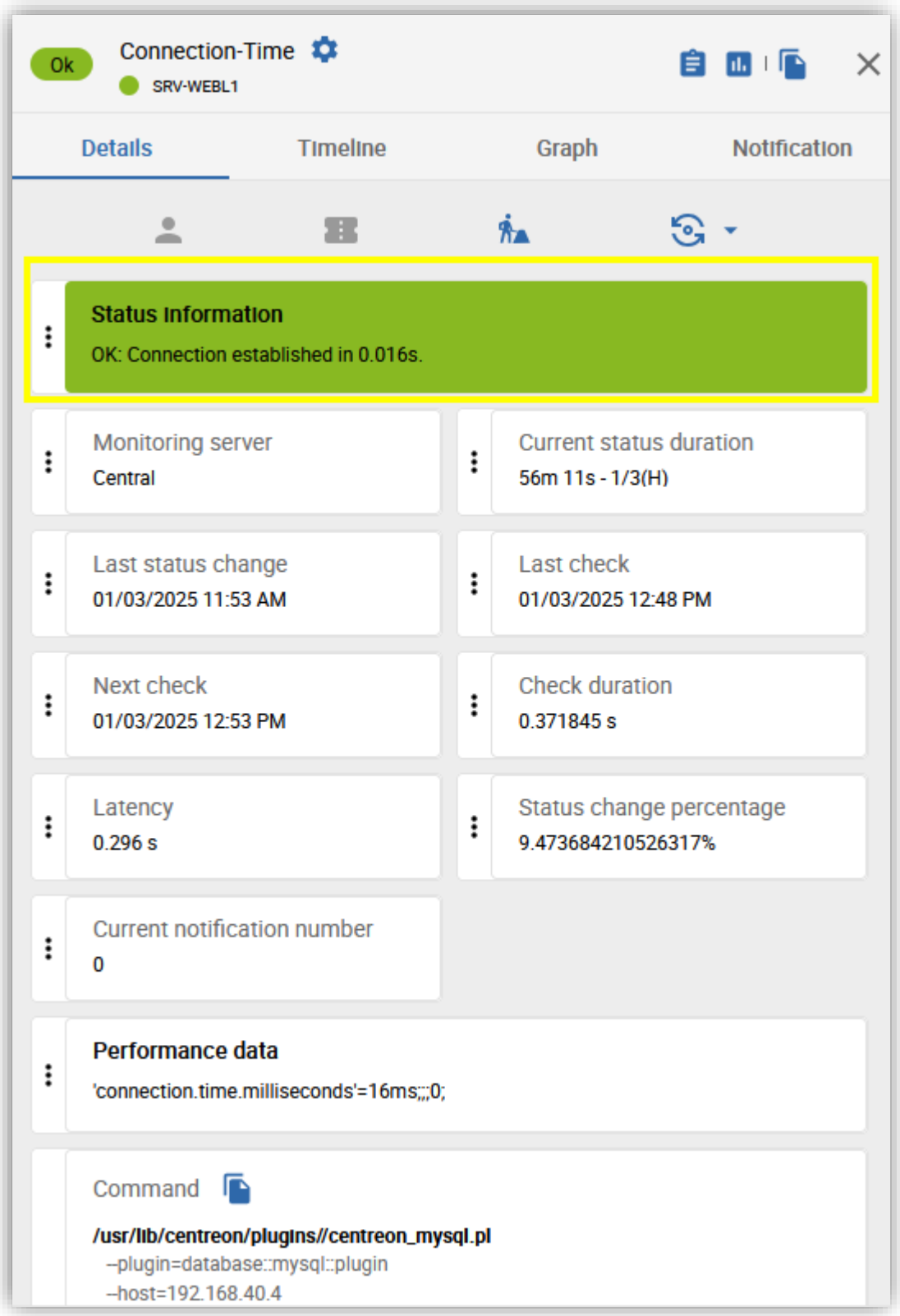
Beaucoup de paramétrages sont possibles pour affiner les données ressorties par le serveur Centreon, nous allons voir un exemple avec le check du temps de connexion au serveur.

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



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 :



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 :

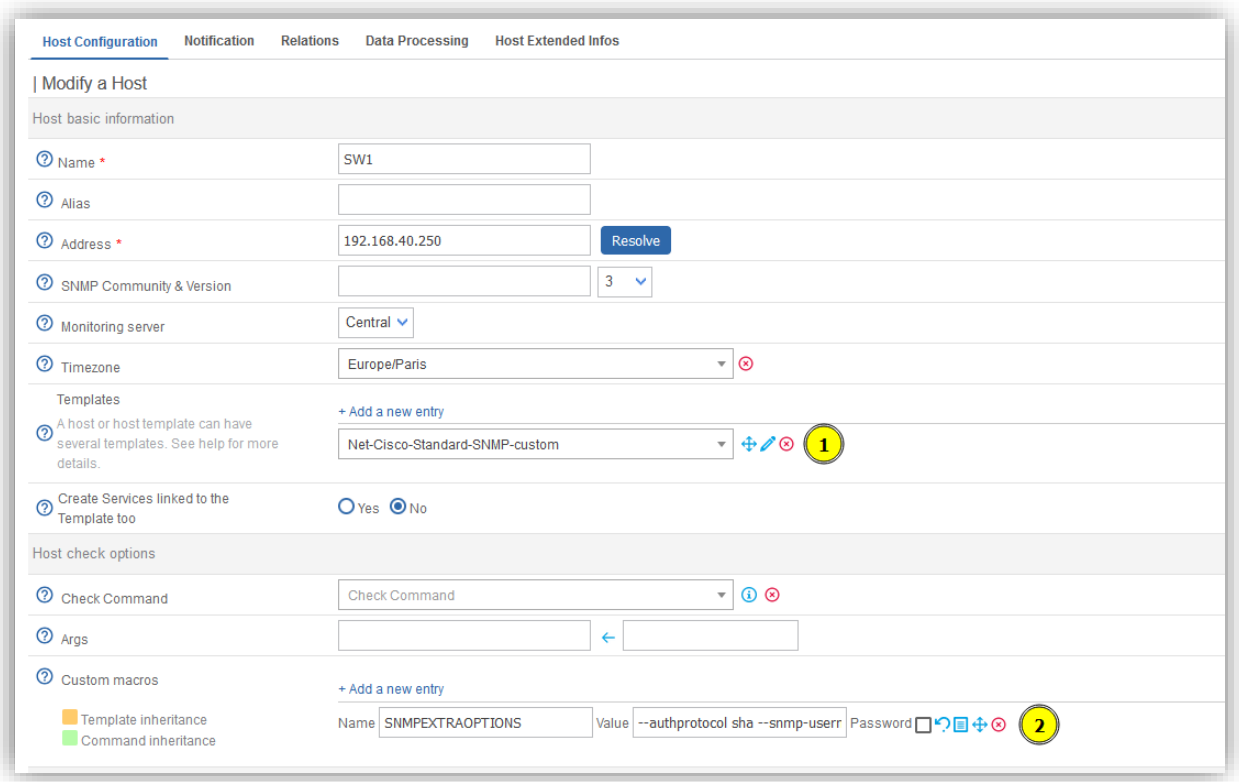
```
enable
conf t
snmp-server group ADMIN v3 priv
snmp-server user snmpuser groupe1 v3 auth sha ***** priv aes 256 ******
```

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
```

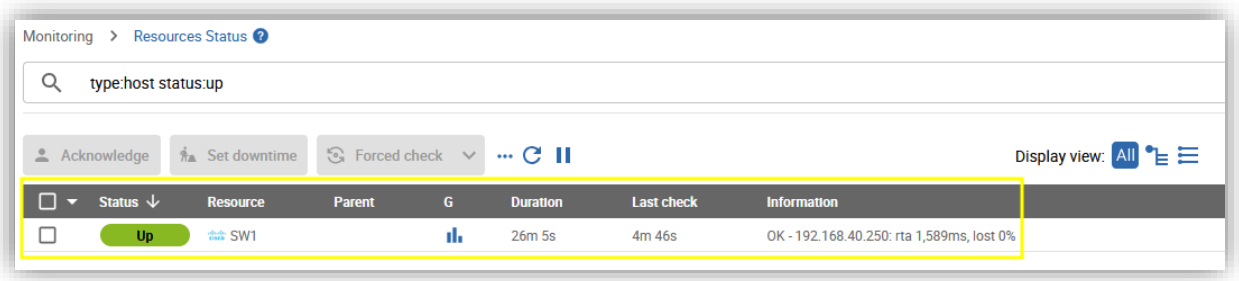
Une fois cela fait, nous allons pouvoir créer notre hôte sur le serveur Centreon de la même manière que dans les exemples précédents.
Nous allons modifier l'IP, le template et ajouter les options nécessaires pour le SNMPv3 :



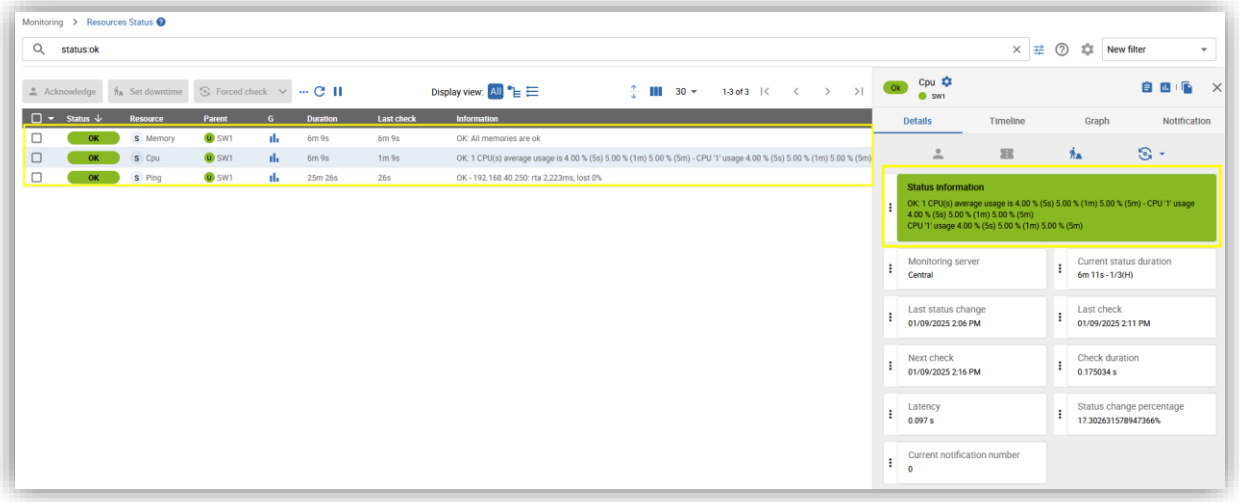
1. Nom du template pour les équipements Cisco

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.

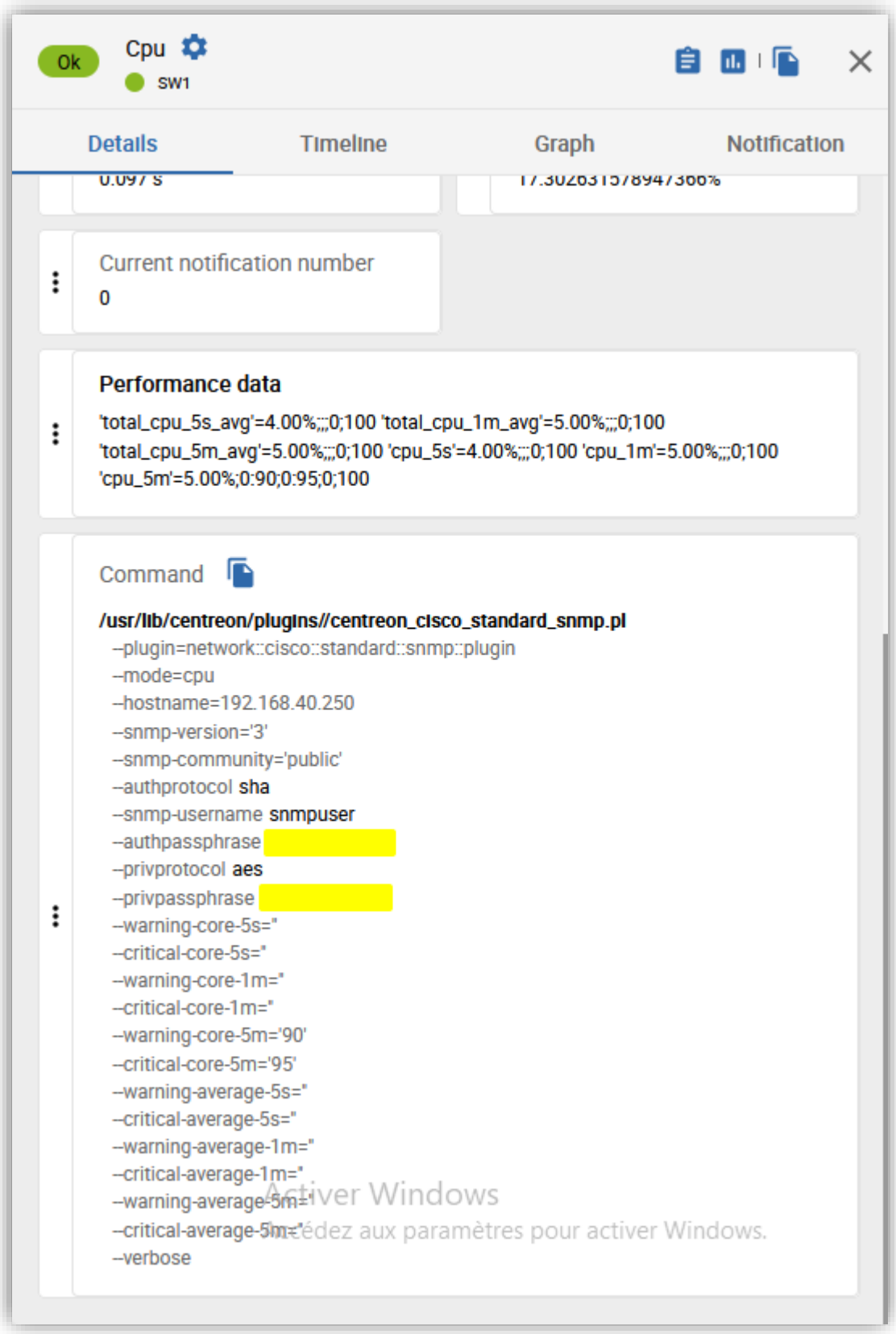
Dans notre menu **« host »** nous voyons désormais notre switch :



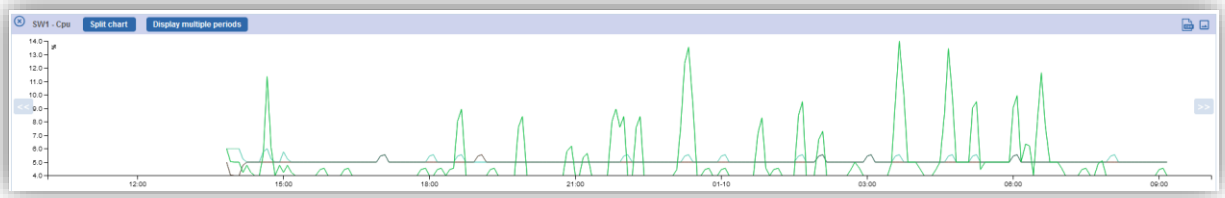
Puis nous allons vérifier les services associés à celui-ci :



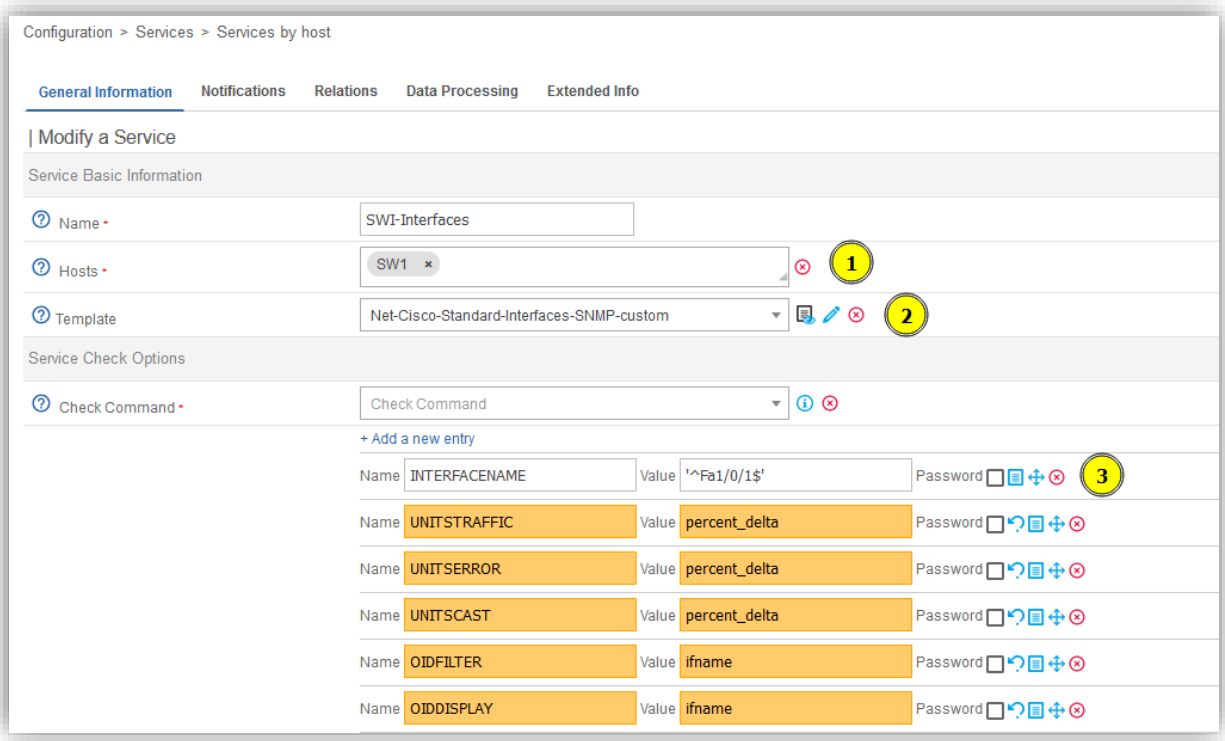
Nous constatons bien l'utilisation de SNMPv3 :



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

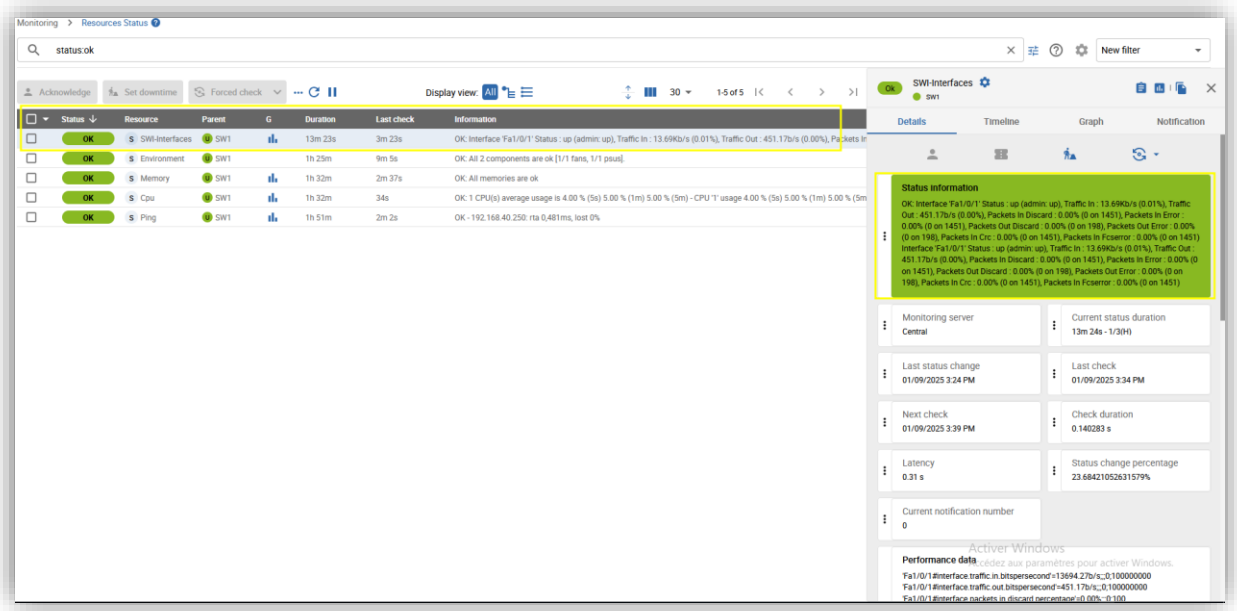


Nous allons maintenant pouvoir ajouter un nouveau service à notre hôte via le menu **« Services By Host** » comme vu précédemment.
Dans notre cas, nous allons superviser les interfaces de notre switch :



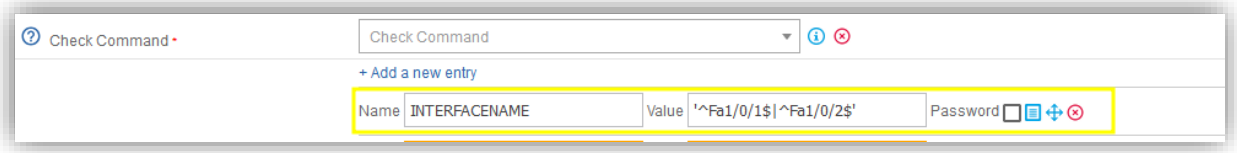
1. Service attaché à notre hôte SW1
2. Template de supervision des interfaces Cisco
3. Filtre sur l'interface Fa1/0/1. Attention à la syntaxe à respecter à l'identique pour le filtre sur une interface (si le paramètre est vide Centreon va checker toutes les interfaces par défaut)

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

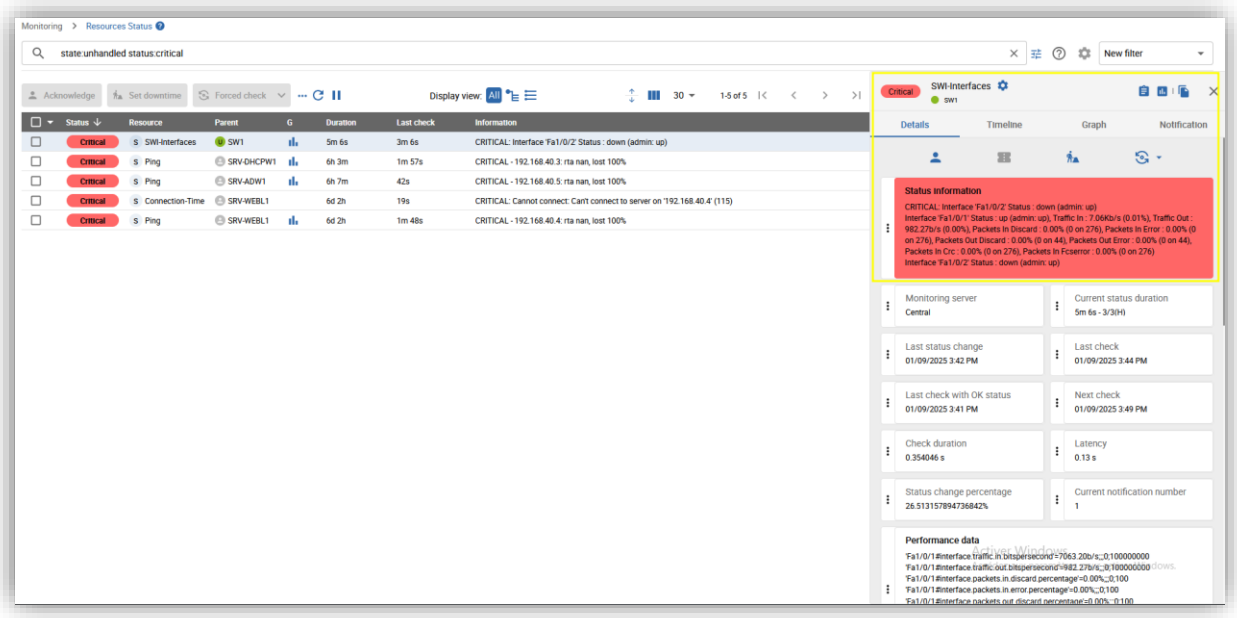


Dans la capture ci-dessus, nous voyons que l'interface est up ainsi que toutes les informations concernant le trafic, les paquets en erreurs ect…

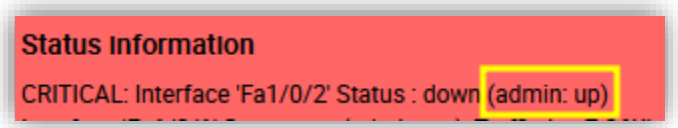
Nous allons maintenant superviser une interface supplémentaire la **« Fa1/0/2 »**.
Pour cela, nous allons dans la configuration du service et ajoutons notre interface dans l'option **« Interface Name »** en respectant la syntaxe suivante :



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 :



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 supervisons 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/anssi-guide-recommandations_configuration_commutateurs_pare-feux_hirschmann.pdf