DROUET Eloi
GUELLE Mathieu
MARCOULY Hugo

TP : Supervision d’un Switch avec Nagios

Sommaire

Mise en place et paramétrage d'un serveur Nagios

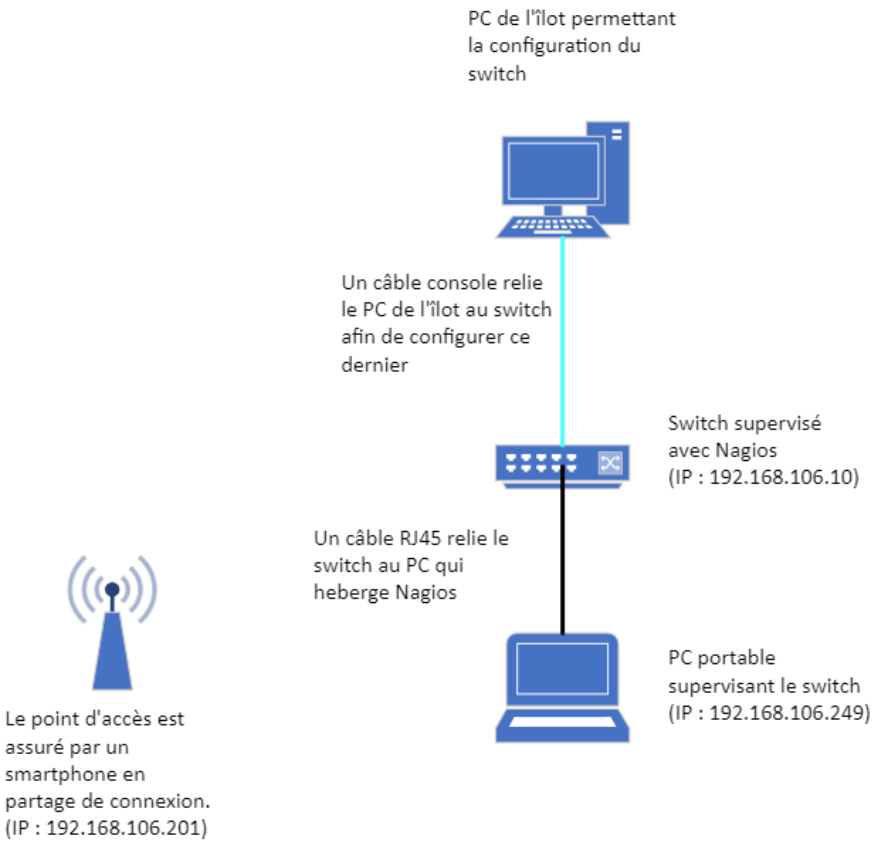
Matériels utilisés :

Pour ce TP nous utiliserons un serveur Linux pour la mise d'un outil de supervision. Notre choix se porte sur **Nagios** comme outil de supervision. Nous avons donc opté pour **Debian 11** comme distribution. Ce TP est réalisé depuis l'un de nos ordinateurs personnels qui sont sous Windows 10/11, nous devons donc utiliser un outil de virtualisation pour utiliser Debian 11. Pour ce faire, nous avons choisi **Oracle VM VirtualBox**. Concernant le matériel physique, nous utilisons un **switch CISCO Catalyst 2950 series**. Pour la configuration du switch nous utilisons le logiciel **MobaXterm.**

Disposition du poste de travail :

L'accès à internet se fait via une connexion sans fil (ici, un partage de connexion). Le switch est relié à notre ordinateur par un câble RJ45.

Pour configurer le switch, nous utiliserons un des PC de notre îlot et un câble console.



Attributions des adresses IP :

L’accès à internet est assuré tout le long du TP par un smartphone en partage de connexion. La PC portable ainsi que la machine virtuelle se voient donc attribuer des adresses IP.

Détenteur de l’adresse	Adresse IP
Smartphone	192.168.106.201
PC portable	192.168.106.249
Machine Virtuelle	192.168.106.85
Switch supervisé	192.168.106.10

(Tableau récapitulatif des adresses IP)

Tous nos appareils se trouvent sur le réseau 192.168.106.xxx c’est pourquoi nous donnons une adresse de ce réseau au switch que nous allons superviser. C’est pourquoi nous donnons l’adresse **192.168.106.10** au switch cisco.

Téléchargement des plugins :

Dans Nagios les plugins sont des programmes externes qui effectuent des vérifications spécifiques sur des hôtes et/ou des services et retournent le résultat à Nagios. Ces plugins jouent un rôle crucial dans le processus de surveillance, permettant à Nagios de recueillir des informations sur la disponibilité, les performances et l'état des services et des hôtes surveillés. Pour la supervision de notre switch nous allons installer les plugins SNMP (Simple Network Management Protocol). Ce protocole est utilisé pour gérer et superviser les équipements réseau comme les switchs et les routeurs ainsi que les machines connectées à un réseau comme les serveurs, les applications et les bases de données.

Pour cela, on va télécharger le fichier du paquet (`snmp-mibs-downloader_1.5_all.deb`)

```
wget http://ftp.de.debian.org/debian/pool/non-free/s/snmp-mibs-downloader/snmp-mibs-downloader_1.5_all.deb
```

On va installer notre notre paquet en .deb :

```
dpkg -i snmp-mibs-downloader_1.5_all.deb
```

On installe à nouveau le paquet grâce à cette commande :

```
apt-get install snmp-mibs-downloader
```

On va ensuite installer les plugins nagios pour avoir le fichier check_snmp :

```
apt-get install nagios-plugins
```

On copie le fichier `check_snmp` dans `/usr/lib/nagios/plugins`

On déplace le fichier `check_snmp` dans `usr/local/nagios/libexec`

Enfin, on redémarre le service :

```
nagios service nagios restart
```

Nagios est donc opérationnel pour superviser notre switch. Nous allons donc le paramétrer.

Paramétrage du switch

Attribution d'une adresse :

Pour attribuer une adresse IP au switch Cisco de notre îlot, nous relions le PC fixe au switch par un câble console (câble bleu), puis nous utilisons MobaXterm.

Une fois MobaXterm ouvert, nous allons rentrer les commandes suivantes pour donner l'adresse IP voulu à notre switch.

```
Switch>enable
Switch#conf t
Switch(config)#int vlan 1
Switch(config-if)#ip address 192.168.106.10 255.255.255.0
Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#write memory
```

Notre switch à donc maintenant une adresse du réseau de notre partage de connexion.

Activation des traps :

Les traps SNMP (Simple Network Management Protocol) sont des informations envoyées en utilisant le protocole SNMP depuis un équipement supervisé vers un serveur de supervision. Elles permettent aux switchs de signaler en temps réel des événements significatifs tels que les pannes ou les surcharges de CPU à l'outil de supervision. Il faut donc les activer afin de pouvoir superviser le switch.

```
Switch>enable
Switch#conf t
Switch(config)#snmp-server enable traps
Switch(config)#exit
Switch#write memory
```

Activation des communautés du switch :

```
Switch#conf t
Switch(config)#snmp-server community public RO
Switch(config)#snmp-server community private RW
Switch#write memory
```

La configuration de la communauté RO (Read Only) permet aux dispositifs de gestion d'interroger le switch pour obtenir des informations de supervision. Cela inclut la détection proactive des problèmes, la surveillance des performances en temps réel, et la récupération d'informations sur l'état global du switch.

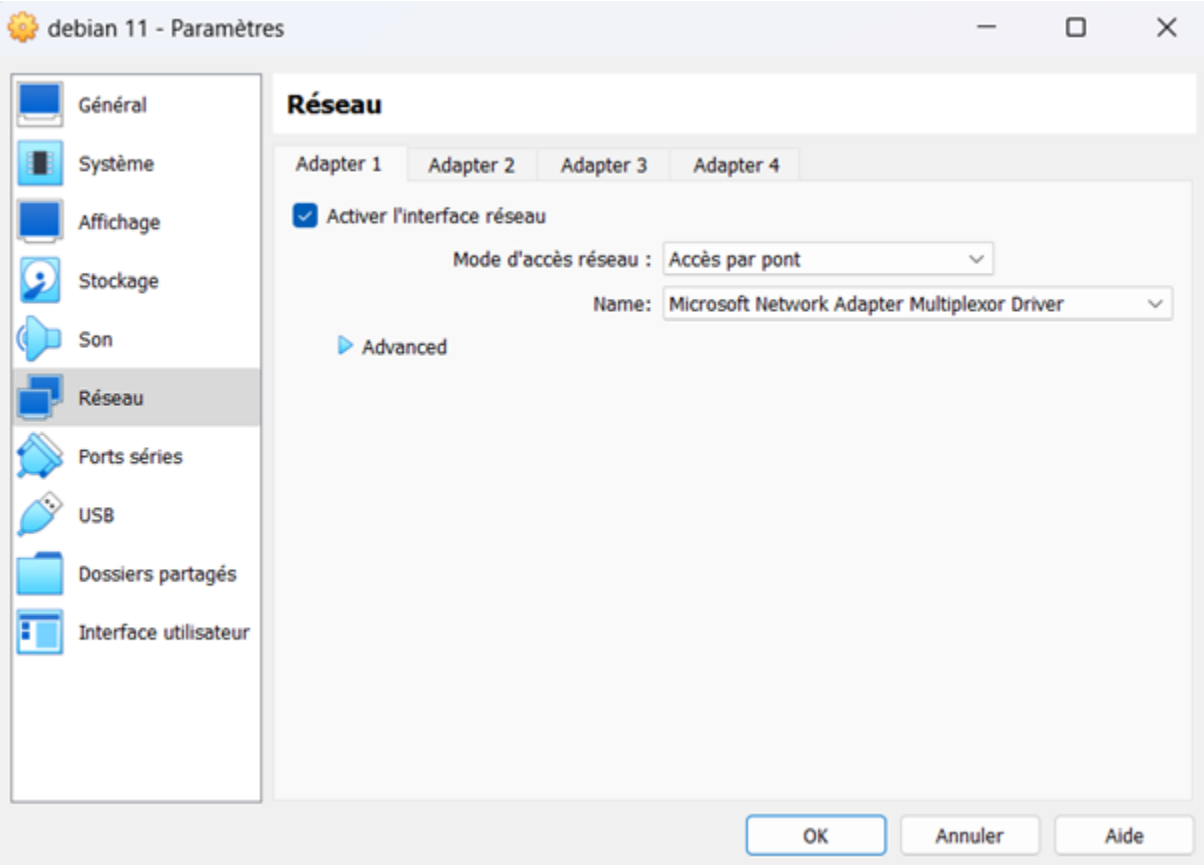
Configurer la communauté RW (Read & Write) autorise la modification de la configuration du switch à distance. Cela permet d' apporter des changements de configuration sans avoir à accéder physiquement au switch.

Supervision du switch

Création d'un pont :

Nagios étant bien configuré tout comme notre switch, nous faisons un test de ping pour savoir s' ils arrivent à communiquer ensemble. Nous remarquons que notre VM Debian n'arrive pas à ping avec le switch. Pour contourner cette difficulté, nous allons contourner le problème en créant un pont entre les cartes réseau wifi et Ethernet.

Dans VirtualBox il ne faut pas oublier de changer l'interface réseau et de sélectionner le pont.



Le pont est donc opérationnel, notre VM arrive donc à ping notre switch. La supervision pourra se faire sans problème.

Saisi des données :

Pour superviser des machines, Nagios utilise des fichiers cfg pour la configuration. On définit le nom d'hôte, l'adresse ip, le groupe dans lequel on veut classer et les différents plug-ins à utiliser.

```
##############################################################################
# SWITCH.CFG - SAMPLE CONFIG FILE FOR MONITORING A SWITCH
#
#
# NOTES: This config file assumes that you are using the sample configuration
#    files that get installed with the Nagios quickstart guide.
#
##############################################################################



##############################################################################
#
# HOST DEFINITIONS
#
##############################################################################

# Define the switch that we'll be monitoring

define host {

    use                     generic-switch                  ; Inherit default values from a template
    host_name               Switch                  ; The name we're giving to this switch
    alias                   Switch Cisco Catalyst 2950              ; A longer name associated with the switch
    address                 192.168.106.10                  ; IP address of the switch
    hostgroups              switches                        ; Host groups this switch is associated with
}



##############################################################################
#
# HOST GROUP DEFINITIONS
#
##############################################################################

# Create a new hostgroup for switches

define hostgroup {

    hostgroup_name          switches                        ; The name of the hostgroup
    alias                   Network Switches                ; Long name of the group
}
```

Pour ce TP, nous allons superviser le port 2 de notre switch.

```
# Monitor Port 2 status via SNMP

define service {

    use                     generic-service
    host_name               Switch
    service_description     Statut du port 2
    check_command           check_snmp!-C public -o ifOperStatus.2 -r 1 -m RFC1213-MIB
}
```

Voici, un exemple de configuration d'utilisation de plugin pour superviser l'état du port 2 de notre switch.

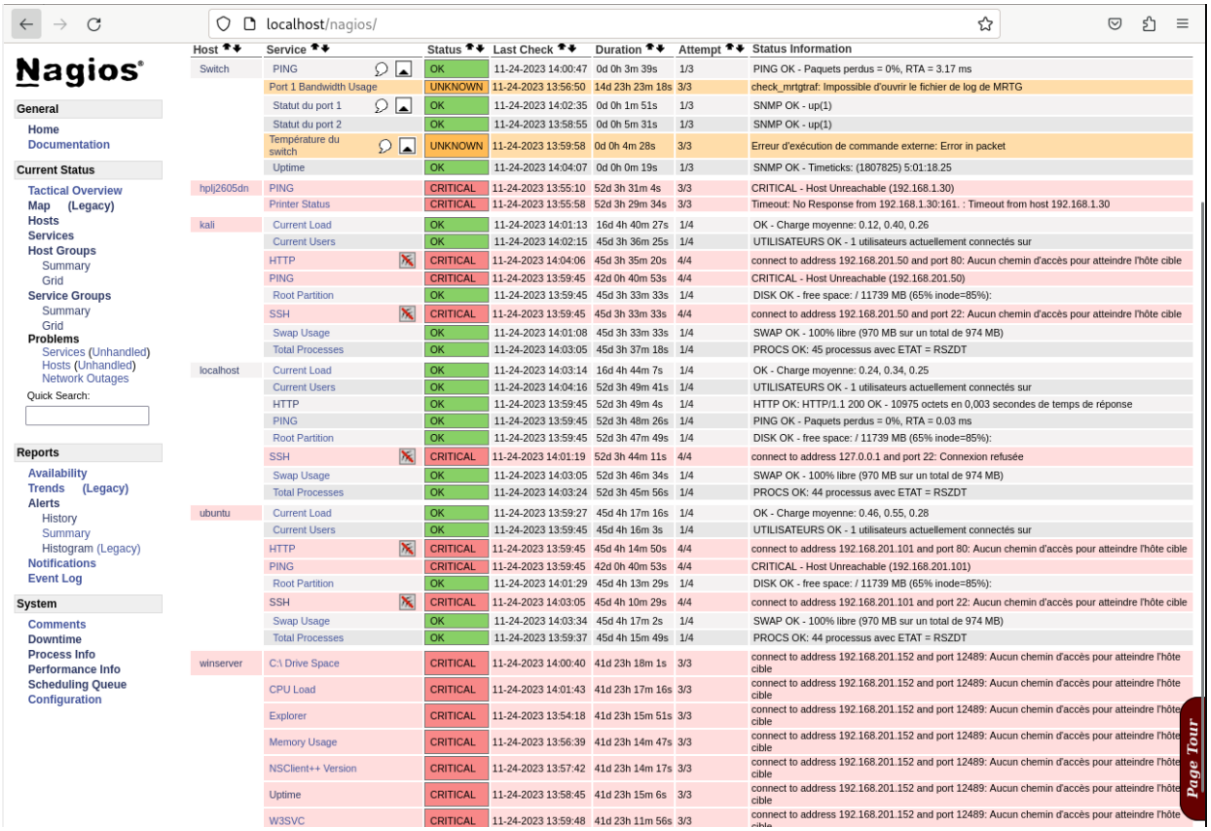
Une fois, les modifications effectuées, nous redémarrons Nagios afin qu'elles soient prisent en compte :

```
service nagios restart
```

Vérification de la supervision :

Pour vérifier les machines supervisées par Nagios, on utilise un navigateur dans lequel on saisit dans la barre d'adresse http://localhost/nagios ou http://192.168.106.85/nagios. Une fenêtre Nagios s'ouvre, pour avoir accès à notre écran de supervision nous allons dans l'onglet "Services".

Un tableau s'ouvre avec tout ce que nous supervisons grâce à Nagios.



Host	Service	Status	Last Check	Duration	Attempt	Status Information
Switch	PING	OK	11-24-2023 14:00:47	0d 0h 3m 39s	1/3	PING OK - Paquets perdus = 0%, RTA = 3.17 ms
	Port 1 Bandwidth Usage	UNKNOWN	11-24-2023 13:56:50	14d 23h 23m 18s	3/3	check_mrtgtraf: Impossible d'ouvrir le fichier de log de MRTG
	Statut du port 1	OK	11-24-2023 14:02:35	0d 0h 1m 51s	1/3	SNMP OK - up(1)
	Statut du port 2	OK	11-24-2023 13:58:55	0d 0h 5m 31s	1/3	SNMP OK - up(1)
	Température du switch	UNKNOWN	11-24-2023 13:59:58	0d 0h 4m 28s	3/3	Erreur d'exécution de commande externe: Error in packet
	Uptime	OK	11-24-2023 14:04:07	0d 0h 0m 19s	1/3	SNMP OK - Timeticks: (1807825) 5:01:18.25
hplj2605dn	PING	CRITICAL	11-24-2023 13:55:10	52d 3h 31m 4s	3/3	CRITICAL - Host Unreachable (192.168.1.30)
	Printer Status	CRITICAL	11-24-2023 13:55:58	52d 3h 29m 34s	3/3	Timeout: No Response from 192.168.1.30:161. : Timeout from host 192.168.1.30
kali	Current Load	OK	11-24-2023 14:01:13	16d 4h 40m 27s	1/4	OK - Charge moyenne: 0.12, 0.40, 0.26
	Current Users	OK	11-24-2023 14:02:15	45d 3h 36m 25s	1/4	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
	HTTP	CRITICAL	11-24-2023 14:04:06	45d 3h 35m 20s	4/4	connect to address 192.168.201.50 and port 80: Aucun chemin d'accès pour atteindre l'hôte cible
	PING	CRITICAL	11-24-2023 13:59:45	42d 0h 40m 53s	4/4	CRITICAL - Host Unreachable (192.168.201.50)
	Root Partition	OK	11-24-2023 13:59:45	45d 3h 33m 33s	1/4	DISK OK - free space: / 11739 MB (65% inode=85%):
	SSH	CRITICAL	11-24-2023 13:59:45	45d 3h 33m 33s	4/4	connect to address 192.168.201.50 and port 22: Aucun chemin d'accès pour atteindre l'hôte cible
	Swap Usage	OK	11-24-2023 14:01:08	45d 3h 33m 33s	1/4	SWAP OK - 100% libre (970 MB sur un total de 974 MB)
	Total Processes	OK	11-24-2023 14:03:05	45d 3h 37m 18s	1/4	PROCS OK: 45 processus avec ETAT = RSZDT
localhost	Current Load	OK	11-24-2023 14:03:14	16d 4h 44m 7s	1/4	OK - Charge moyenne: 0.24, 0.34, 0.25
	Current Users	OK	11-24-2023 14:04:16	52d 3h 49m 41s	1/4	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
	HTTP	OK	11-24-2023 13:59:45	52d 3h 49m 4s	1/4	HTTP OK: HTTP/1.1 200 OK - 10975 octets en 0,003 secondes de temps de réponse
	PING	OK	11-24-2023 13:59:45	52d 3h 48m 26s	1/4	PING OK - Paquets perdus = 0%, RTA = 0.03 ms
	Root Partition	OK	11-24-2023 13:59:45	52d 3h 47m 49s	1/4	DISK OK - free space: / 11739 MB (65% inode=85%):
	SSH	CRITICAL	11-24-2023 14:01:19	52d 3h 44m 11s	4/4	connect to address 127.0.0.1 and port 22: Connexion refusée
	Swap Usage	OK	11-24-2023 14:03:05	52d 3h 46m 34s	1/4	SWAP OK - 100% libre (970 MB sur un total de 974 MB)
	Total Processes	OK	11-24-2023 14:03:24	52d 3h 45m 56s	1/4	PROCS OK: 44 processus avec ETAT = RSZDT
ubuntu	Current Load	OK	11-24-2023 13:59:27	45d 4h 17m 16s	1/4	OK - Charge moyenne: 0.46, 0.55, 0.28
	Current Users	OK	11-24-2023 13:59:45	45d 4h 16m 3s	1/4	UTILISATEURS OK - 1 utilisateurs actuellement connectés sur
	HTTP	CRITICAL	11-24-2023 13:59:45	45d 4h 14m 50s	4/4	connect to address 192.168.201.101 and port 80: Aucun chemin d'accès pour atteindre l'hôte cible
	PING	CRITICAL	11-24-2023 13:59:45	42d 0h 40m 53s	4/4	CRITICAL - Host Unreachable (192.168.201.101)
	Root Partition	OK	11-24-2023 14:01:29	45d 4h 13m 29s	1/4	DISK OK - free space: / 11739 MB (65% inode=85%):
	SSH	CRITICAL	11-24-2023 14:03:05	45d 4h 10m 29s	4/4	connect to address 192.168.201.101 and port 22: Aucun chemin d'accès pour atteindre l'hôte cible
	Swap Usage	OK	11-24-2023 14:03:34	45d 4h 17m 2s	1/4	SWAP OK - 100% libre (970 MB sur un total de 974 MB)
	Total Processes	OK	11-24-2023 13:59:37	45d 4h 15m 49s	1/4	PROCS OK: 44 processus avec ETAT = RSZDT
winserver	C:\ Drive Space	CRITICAL	11-24-2023 14:00:40	41d 23h 18m 1s	3/3	connect to address 192.168.201.152 and port 12489: Aucun chemin d'accès pour atteindre l'hôte cible
	CPU Load	CRITICAL	11-24-2023 14:01:43	41d 23h 17m 16s	3/3	connect to address 192.168.201.152 and port 12489: Aucun chemin d'accès pour atteindre l'hôte cible
	Explorer	CRITICAL	11-24-2023 13:54:18	41d 23h 15m 51s	3/3	connect to address 192.168.201.152 and port 12489: Aucun chemin d'accès pour atteindre l'hôte cible
	Memory Usage	CRITICAL	11-24-2023 13:56:39	41d 23h 14m 47s	3/3	connect to address 192.168.201.152 and port 12489: Aucun chemin d'accès pour atteindre l'hôte cible
	NSClient++ Version	CRITICAL	11-24-2023 13:57:42	41d 23h 14m 17s	3/3	connect to address 192.168.201.152 and port 12489: Aucun chemin d'accès pour atteindre l'hôte cible
	Uptime	CRITICAL	11-24-2023 13:58:45	41d 23h 15m 6s	3/3	connect to address 192.168.201.152 and port 12489: Aucun chemin d'accès pour atteindre l'hôte cible
	W3SVC	CRITICAL	11-24-2023 13:59:48	41d 23h 11m 56s	3/3	connect to address 192.168.201.152 and port 12489: Aucun chemin d'accès pour atteindre l'hôte cible

Pour ce TP, on se concentre sur la supervision de notre switch.

Host	Service	Status	Last Check	Duration	Attempt	Status Information
Switch	PING	OK	11-24-2023 14:00:47	0d 0h 3m 39s	1/3	PING OK - Paquets perdus = 0%, RTA = 3.17 ms
	Port 1 Bandwidth Usage	UNKNOWN	11-24-2023 13:56:50	14d 23h 23m 18s	3/3	check_mrtgtraf: Impossible d'ouvrir le fichier de log de MRTG
	Statut du port 1	OK	11-24-2023 14:02:35	0d 0h 1m 51s	1/3	SNMP OK - up(1)
	Statut du port 2	OK	11-24-2023 13:58:55	0d 0h 5m 31s	1/3	SNMP OK - up(1)

Nous pouvons voir que le ping, est "OK" donc opérationnel. Tout comme le port 1 et le port 2.

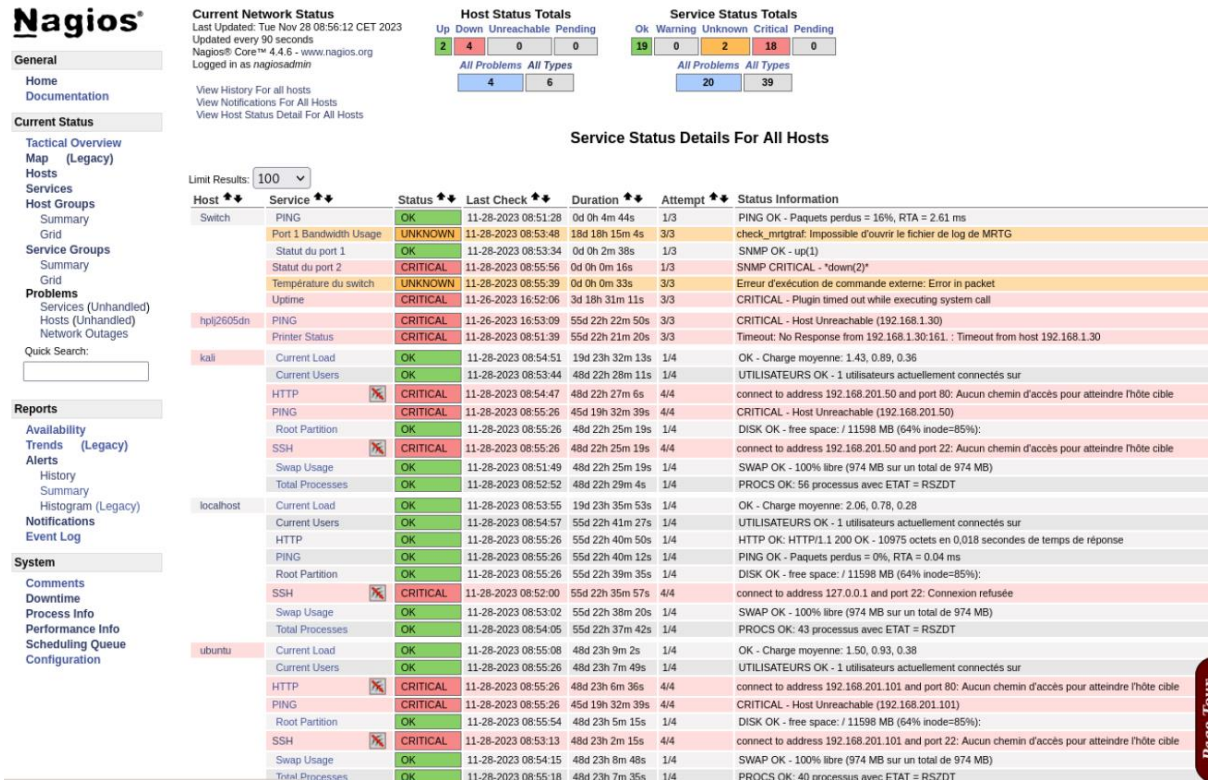
Tout est donc fonctionnel sur notre switch.

Simulation de panne :

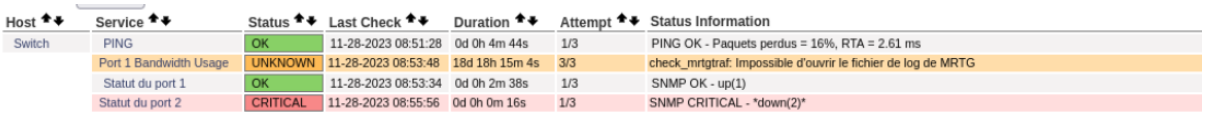
Pour vérifier que la supervision fonctionne correctement, nous allons simuler une panne sur le port 2 de notre switch. Pour cela, nous allons tout simplement débrancher le câble qui est branché à notre port 2. Nous gardons le port 1 branché pour qu'il servent de "port témoin".

Nous débranchons donc le câble relié au port 2 de notre switch.

Notre tableau s'actualise.



On se concentre sur notre switch.



Nous remarquons que le ping et le port 1 restent opérationnels mais le port 2 lui est passé en "CRITICAL". Dans "Status Information", on remarque que le port est "down" ce qui signifie que le port 2 n'est plus fonctionnel.

Notre a détecté que le port 2 n'était plus branché mais nous montre bien que le reste fonctionne toujours. Cette simulation de panne nous confirme donc que notre supervision fonctionne correctement.