



# Formation OpenClassrooms Administrateur Systèmes, Réseaux Et Sécurité

## Soutenance Projet-08

Stéphane Perfetti

04/11/2024



MEDIA SANTÉ

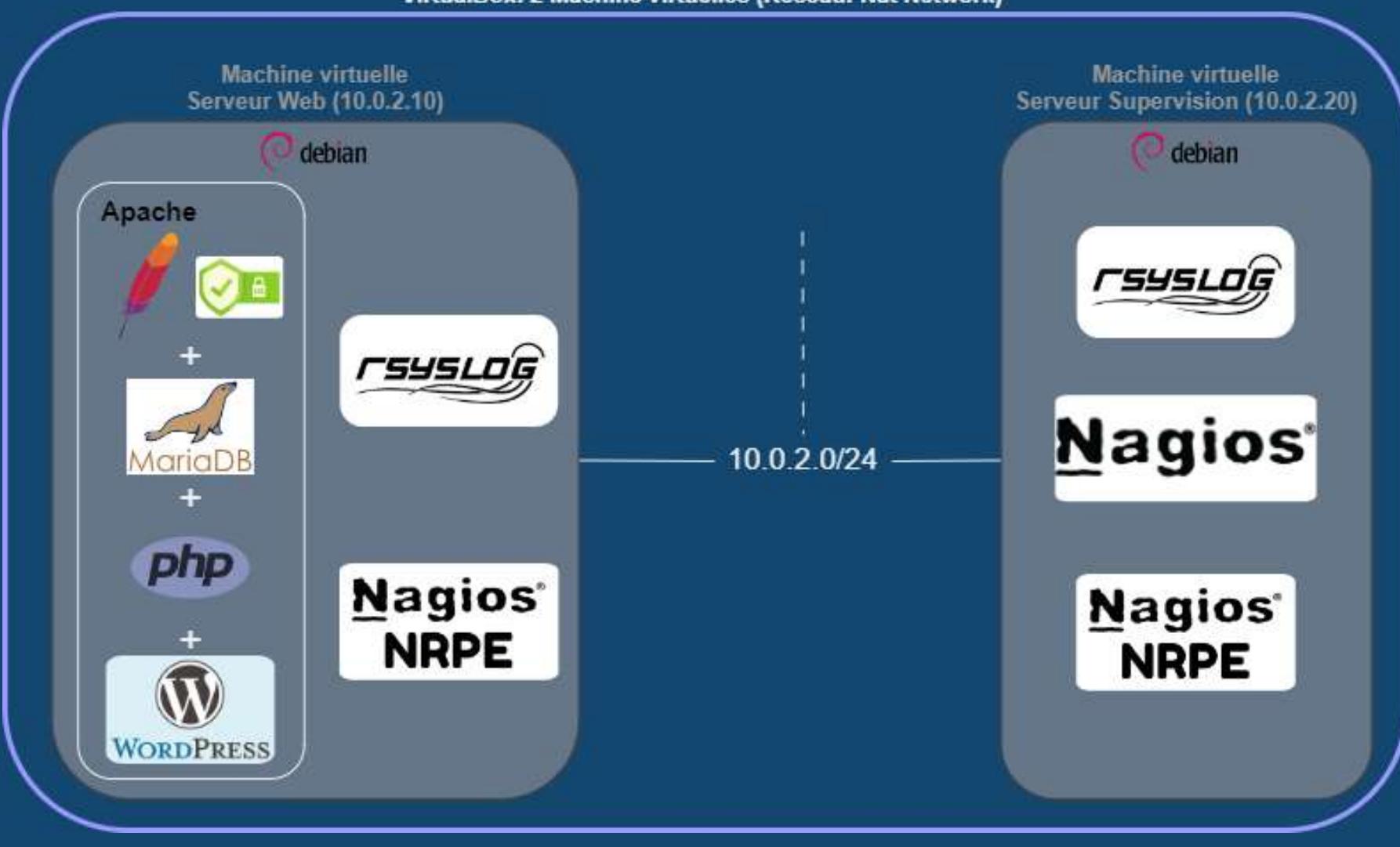
## Projet 08

-  
Supervisez le SI  
d'une entreprise

- Scénario :
  - L'entreprise MesiaSanté reçoit des plaintes quand à la vitesse de chargement de son site web.
  - L'objectif est de mettre en place un système de supervision et d'installer des sondes permettent de surveiller le site web
- Plan d'action :
  - Schéma de la maquette de simulation
  - Centralisation des logs
  - Système de supervision et détails des sondes

# Maquette sous VirtualBox:

VirtualBox: 2 Machine virtuelles (Réseau: Nat Network)



# Centralisation des logs: Rsyslog configuration

```
# /etc/rsyslog.conf configuration file for rsyslog

##### MODULES #####
module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
module(load="imudp")

```

## Serveur de Supervision (Serveur Rsyslog)

Activation du module de réception UDP (port 514)

```
# /etc/rsyslog.conf configuration file for rsyslog

##### MODULES #####
module(load="imuxsock") # provides support for local system logging
module(load="imklog") # provides kernel logging support
#module(load="immark") # provides --MARK-- message capability

# provides UDP syslog reception
#module(load="imudp")
#input(type="imudp" port="514"

# provides TCP syslog reception
#module(load="imtcp")
#input(type="imtcp" port="514")

##### GLOBAL DIRECTIVES #####
# Set the default permissions for all log files.
$FileOwner root
$FileGroup adm
$FileCreateMode 0640
$DirCreateMode 0755
$Umask 0022

# Where to place spool and state files
$WorkDirectory /var/spool/rsyslog

# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

##### RULES #####
# Log anything besides private authentication messages to a single log
#
*.auth,authpriv.none -/var/log/syslog
*.auth,authpriv.none @10.0.2.20:514

# Log commonly used facilities to their own log file
auth,authpriv.* /var/log/auth.log
cron.* -/var/log/cron.log
kern.* -/var/log/kern.log
mail.* -/var/log/mail.log
user.* -/var/log/user.log

#
# Emergencies are sent to everybody logged in.
#
*.emerg :omusrmsg:*
```

## Serveur Web (Client Rsyslog)

Règle d'émission de tous les log vers le serveur de supervision

# Supervision: Nagios Configuration

Current Network Status  
Last Updated: Thu Oct 31 16:19:15 CET 2024  
Updated every 90 seconds  
Nagios® Core™ 4.5.6 - www.nagios.org  
Logged in as *nagiosadmin*

View History For all hosts  
View Notifications For All Hosts  
View Host Status Detail For All Hosts

Host Status Totals				Service Status Totals				
Up	Down	Unreachable	Pending	Ok	Warning	Unknown	Critical	Pending
2	0	0	0	10	0	0	0	0
All Problems	All Types			All Problems	All Types			
0	2			0	10			

### Service Status Details For All Hosts

Limit Results: 100

Host	Service	Status	Last Check	Duration	Attempt	Status Information
MediaSante_NagiosServer	User Session Nagios	OK	10-31-2024 16:19:07	0d 21h 22m 28s	1/4	USERS OK: nagios(1)
MediaSante_WebServer	CPU Usage Pct	OK	10-31-2024 16:19:10	0d 0h 10m 6s	1/4	[CPU_INFO: .90% ] User: 0.00% - System: 0.40% - Idle: 99.10% - IOwait: 0.40%
	Current Load	OK	10-31-2024 16:18:29	0d 6h 26m 45s	1/4	OK - load average per CPU: 0.00, 0.01, 0.00
	Database	OK	10-31-2024 16:18:42	0d 6h 26m 32s	1/4	Uptime: 8393 Threads: 1 Questions: 17199 Slow queries: 0 Opens: 41 Open tables: 34 Queries per second avg: 2.049
	Disk Usage	OK	10-31-2024 16:18:55	0d 6h 27m 21s	1/4	DISK OK - free space: / 5406 MB (63.32% inode=86%)
	HTTP	OK	10-31-2024 16:18:13	0d 5h 15m 18s	1/4	HTTP OK: HTTP/1.0 200 OK - 85483 bytes in 0.169 second response time
	HTTPS	OK	10-31-2024 16:18:24	0d 5h 15m 48s	1/4	SSL OK - Certificate 'mediasante.eu' will expire in 360 days on 2025-10-26 16:59 +0100/CET.
	RAM Usage	OK	10-31-2024 16:18:37	0d 6h 26m 38s	1/4	[MEMORY] Total: 1967 MB - Used: 435 MB - 22% [SWAP] Total: 974 MB - Used: 0 MB - 0%
	URL	OK	10-31-2024 16:18:48	0d 5h 16m 17s	1/4	OK: URL mediasante.eu is available and it should - 200
	Web Page Index	OK	10-31-2024 16:19:05	0d 4h 41m 10s	1/4	HTTP OK: HTTP/1.0 200 OK - 85483 bytes in 0.335 second response time

## Configuration Nagios des deux serveurs

Rq: La supervision de certaines informations du serveur web s'effectuent par l'intermédiaire de l'addon NRPE.

# Supervision: Sonde de contrôle session utilisateur "nagios" sur le serveur

MediaSante_NagiosServer	User Session Nagios	OK	10-31-2024 16:19:07	0d 21h 22m 28s	1/4	USERS OK: nagios(1)
-------------------------	---------------------	----	---------------------	----------------	-----	---------------------

## Documentation:

Nom de la sonde: User Session Nagios

Objectif de la sonde: Contrôler le nombre de sessions de l'utilisateur "Nagios", ouvertes sur le serveur en parallèle.

Paramétrage de la sonde:

- Warning: deux sessions utilisateur "nagios" ouverte en même temps.
- Critical: trois sessions utilisateur "nagios" ouverte en même temps.

Action en cas d'anomalie:

- Identifier les sessions utilisateur "nagios" connecté au serveur et leurs PID: `who -uH`
- Clôturer la session identifiée par son PID: `sudo kill -9 <PID>`

Indicateur:				
Noms	Utilisation NRPE	Commande finale	Fonction / Paramètres	Test
User Session Nagios	Non	<code>show_users.sh -a "nagios" -w 2 -c 3</code>	- a : Nom d'utilisateur - w : Nombre d'utilisateur connecté résultant en un statut WARNING, si ≥ - c : Nombre d'utilisateur connecté résultant en un statut CRITICAL, si ≥	Ouvrir plusieurs session nagios en parallèle: 2 sessions pour un statut WARNING 3 sessions pour un statut CRITICAL

# Supervision: Sonde de contrôle utilisation CPU

MediaSante_WebServer	CPU Usage Pct	OK	11-04-2024 09:06:10	0d 0h 7m 16s	1/4	[CPU_INFO: 2.70%] User: 0.90% - System: 1.30% - Idle: 97.30% - IOwait: 0.00%
----------------------	---------------	----	---------------------	--------------	-----	--

## Documentation:

Nom de la sonde: CPU Usage Pct

Objectif de la sonde: Contrôler le pourcentage d'utilisation processeur.

Paramétrage de la sonde:

- Warning: supérieur à 70%
- Critical: supérieur à 90%

Action en cas d'anomalie:

- Identifier les processus ou les applications les plus consommateurs de CPU: `top`
- Arrêter les processus ou redémarrer les applications identifiés: `kill -9 <PID processus>` ou `systemctl restart <application>`

Indicateur:					
Noms	Utilisation NRPE	Commande finale	Fonction / Paramètres	Test	
CPU Usage	Oui	<code>check_cpu_info.sh -w 70 -c 90</code>	- w : Pourcentage d'utilisation total CPU résultant en un statut WARNING, si $\geq$ - c : Pourcentage d'utilisation total CPU résultant en un statut CRITICAL, si $\geq$	Augmenter temporairement la charge CPU: <code>stress -cpu 2 -timeout 45s</code>	

# Supervision: Sonde de contrôle de la charge CPU

MediaSante_NagiosServer	Current Load	OK	11-04-2024 09:07:11	0d 0h 17m 44s	1/4	OK - load average per CPU: 0.01, 0.03, 0.04
-------------------------	--------------	----	---------------------	---------------	-----	---

## Documentation:

Nom de la sonde: Current Load

Objectif de la sonde: Contrôler la charge moyenne courante du système, normalisé pour un cœur.

Paramétrage de la sonde:

- Warning: supérieur à 0.7 pour la dernière minutes, ou 0.6 pour les 5 dernières minutes, ou 0.5 pour les 15 dernières minutes.
- Critical: supérieur à 0.9 pour la dernière minutes, ou 0.8 pour les 5 dernières minutes, ou 0.7 pour les 15 dernières minutes.

Action en cas d'anomalie: se référer aux actions de la sonde numéro 2

Indicateur:					
Noms	Utilisation NRPE		Commande finale	Fonction / Paramètres	Test
Current Load	Oui		check_load -r -w .7,.6,.5 -c .9,.8,.7	-r : Normalisé pour un cœur -w : Charge moyenne pour les périodes 1, 5, 15 min résultant en un statut WARNING, si ≥ -c : Charge moyenne pour les périodes 1, 5, 15 min résultant en un statut CRITICAL, si ≥	Augmenter temporairement la charge CPU: Stress -cpu 2 -timeout 45s

# Supervision: Sonde de contrôle de la base de données

MediaSante_NagiosServer	Database	OK	11-04-2024 09:15:23	0d 0h 25m 4s	1/4	Uptime: 1589 Threads: 1 Questions: 3206 Slow queries: 0 Opens: 41 Open tables: 34 Queries per second avg: 2.017
-------------------------	----------	----	---------------------	--------------	-----	---

## Documentation:

Nom de la sonde: Database

Objectif de la sonde: Contrôler la disponibilité en local de la base de donnée "MediaSante".

Rq: Le contrôle s'effectue avec un test de connexion à la base avec l'utilisateur "nagios".

Paramétrage de la sonde:

- Critical: Base donnée non disponible ou arrêtée.

Action en cas d'anomalie:

- Vérifier le statut du service MariaDB: `sudo systemctl status mariadb.service`
- Redémarrer le service MariaDB: `sudo systemctl restart mariadb.service`

Indicateur:					
Noms	Utilisation NRPE	Commande finale	Fonction / Paramètres	Test	
Database	Oui	<code>check_mysql -H localhost -d MediaSante -u nagios -p nagios</code>	<code>-H</code> : Adresse IP ou hostname <code>-d</code> : Nom de la base de donnée <code>-u</code> : Nom d'utilisateur pour la connexion <code>-p</code> : Mot de passe utilisateur pour la connexion	Stopper et redémarrer le service MariaDB: <code>Systemctl stop mariadb.service</code> <code>Systemctl start mariadb.service</code>	

# Supervision: Sonde de contrôle de l'espace disque

MediaSante_NagiosServer	Disk Usage	OK	11-04-2024 09:20:36	0d 0h 31m 1s	1/4	DISK OK - free space: / 5363 MB (62.82% inode=86%):
-------------------------	------------	----	---------------------	--------------	-----	---

## Documentation:

Nom de la sonde: Disk Usage

Objectif de la sonde: Contrôler le pourcentage d'espace disque utilisé.

Paramétrage de la sonde:

- Warning: supérieur à 70% d'utilisation.
- Critical: supérieur à 80% d'utilisation.

Action en cas d'anomalie:

- Vérifier l'espace disque: `df -h /`
- Optimiser l'espace disque utilisé par le gestionnaire de paquet: `apt autoremove && apt clean`
- Lister les 10 dossiers les plus volumineux pour analyse: `du -a | sort -nr | head -n 10`
- Supprimer les fichiers log si identifiés

Indicateur:						
Noms	Utilisation NRPE		Commande finale	Fonction / Paramètres	Test	
Disk Usage	Oui		<code>check_disk -w 30% -c 20% -p /</code>	<code>-w</code> : Pourcentage d'espace disque libre restant résultant en un statut WARNING, si ≤ <code>-c</code> : Pourcentage d'espace disque libre restant résultant en un statut CRITICAL, si ≤ <code>-p</code> : Point de montage contrôlé	Augmenter l'utilisation disque: <code>dd if=/dev/zero of=/tmp/FichierTestDisque.txt bs=1000M count=4</code>	

# Supervision: Sonde de contrôle de la mémoire RAM

MediaSante_NagiosServer	RAM Usage	OK	11-04-2024 09:54:18	0d 1h 4m 39s	1/4	[MEMORY] Total: 1967 MB - Used: 419 MB - 21% [SWAP] Total: 974 MB - Used: 0 MB - 0%
-------------------------	-----------	----	---------------------	--------------	-----	---

## Documentation:

Nom de la sonde: RAM Usage

Objectif de la sonde: Contrôler le pourcentage d'utilisation de la mémoire RAM.

Paramétrage de la sonde:

- Warning: pourcentage d'utilisation RAM comprise entre 70 et 85%.
- Critical: pourcentage d'utilisation RAM supérieure ou égale à 85%.

Action en cas d'anomalie:

- Identifier les processus ou les applications les plus consommateurs de RAM: `top`
- Arrêter les processus ou redémarrer les applications identifiés: `kill -9 <PID processus>` ou `sudo systemctl restart <application>`

Indicateur:					
Noms	Utilisation NRPE	Commande finale	Fonction / Paramètres	Test	
RAM Usage	Oui	check_mem.sh -w 70 -c 85	-w : Pourcentage de RAM utilisé résultant en un statut WARNING, ≥ -c : Pourcentage de RAM utilisé résultant en un statut CRITICAL, ≥	Augmenter temporairement l'utilisation RAM: <code>Stress-ng --vm 2 --vm-bytes 512MBytes --timeout 10s</code>	

# Supervision: Sonde de contrôle du serveur web HTTP

MediaSante_NagiosServer	HTTP	OK	11-04-2024 09:25:53	0d 0h 35m 14s	1/4	HTTP OK: HTTP/1.0 200 OK - 85483 bytes in 0,182 second response time
-------------------------	------	----	---------------------	---------------	-----	--

## Documentation:

Nom de la sonde: HTTP

Objectif de la sonde: Contrôler le temps de réponse et la disponibilité du serveur web en HTTP.

Paramétrage de la sonde:

- Warning: temps de réponse compris entre 1 et 2 secondes.
- Critical: temps de réponse supérieure ou égale à 2 secondes ou connexion refusée.

Action en cas d'anomalie:

- Vérifier le statut (Nbs de tâches, Memoire, CPU) du service Apache: `systemctl status apache2.service`
- Vérifier la configuration d'apache et des virtualhost: `apachectl -t`
- Recharger la configuration apache: `apachectl -k graceful`

Indicateur:					
Noms	Utilisation NRPE	Commande finale	Fonction / Paramètres	Test	
HTTP	Non	<code>check_http -I \$HOSTADDRESS\$ -w 1 -c 2</code>	<code>-I</code> : Adresse IP cible, <code>\$HOSTADDRESS\$</code> fait référence à l'adresse de l'hôte nagios <code>-w</code> : Temps de réponse (seconde) résultant en un statut ALERTE, ≥ <code>-c</code> : Temps de réponse (seconde) résultant en un statut WARNING, ≥	Augmenter temporairement la charge d'Apache: <code>Ab -c 50 -n 10000 http://mediasante.eu/</code>	

# Supervision: Sonde de contrôle du serveur web HTTPS

MediaSante_NagiosServer	HTTPS	OK	11-04-2024 09:45:05	0d 0h 55m 44s	1/4	SSL OK - Certificate 'mediasante.eu' will expire in 356 days on 2025-10-26 16:59 +0100/CET.
-------------------------	-------	----	---------------------	---------------	-----	---

## Documentation:

Nom de la sonde: HTTPS

Objectif de la sonde: Contrôler la période de validité restante du certificat SSL/TLS et la disponibilité du serveur web en HTTPS.

Paramétrage de la sonde:

- Warning: période de validité restante comprise entre 30 et 15 jours.
- Critical: période de validité restante inférieure ou égale à 15 jours ou connexion HTTPS refusée.

Action en cas d'anomalie:

- Vérifier le certificat SSL/TLS et le renouveler si nécessaire
- Se référer aux actions de la sonde numéro 5

Noms	Utilisation NRPE	Commande finale	Indicateur:	Test
			Fonction / Paramètres	
HTTPS	Non	check_http -I \$HOSTADDRESS\$ -S -C 30,15	-I : Adresse IP cible, \$HOSTADDRESS\$ fait référence à l'adresse de l'hôte nagios -S : Connexion via SSL/TLS -C : Nombre de jours minimum pour que le certificat soit valide résultant en un statut WARNING, résultant en un statut CRITICAL, si ≤	Désactiver et réactiver le virtualhost https: A2dissite mediasante.eu-https.conf Systemctl reload apache2.service A2ensite mediasante.eu-https.conf Systemctl reload apache2.service

# Supervision: Sonde de contrôle du serveur web URL

MediaSante_NagiosServer	URL	OK	11-04-2024 09:49:29	0d 0h 59m 56s	1/4	OK: URL mediasante.eu is available and it should - 200
-------------------------	-----	----	---------------------	---------------	-----	--

## Documentation:

Nom de la sonde: URL

Objectif de la sonde: Contrôler l'accessibilité de l'URL "http://mediasante.eu".

Paramétrage de la sonde:

- Unknown: L'URL n'est pas accessible

Action en cas d'anomalie:

- Vérifier et se référer aux actions de la sonde numéro 5
- Vérifier les configurations liées aux DNS : nslookup http://mediasante.eu

Indicateur:					
Noms	Utilisation NRPE	Commande finale	Fonction / Paramètres	Test	
URL	Non	check_proxy_http_url.sh -u mediasante.eu	-u: URL à tester	Stopper et redémarrer le serveur web: systemctl stop apache2.service systemctl start apache2.service	

# Supervision: Sonde de contrôle de la page d'index

MediaSante_NagiosServer	Web Page Index	OK	11-04-2024 09:59:09	0d 1h 9m 22s	1/4	HTTP OK: HTTP/1.0 200 OK - 85483 bytes in 0,314 second response time
-------------------------	----------------	----	---------------------	--------------	-----	--

## Documentation:

Nom de la sonde: Web Page Index

Objectif de la sonde: Contrôler l'accessibilité à la page index.php sur le site mediasante.eu.

Paramétrage de la sonde:

- Warning: La page n'a pas accessible.

Action en cas d'anomalie:

- Vérifier la configuration WordPress, l'existence d'une page index.php ou de redirection pour l'URL "http://mediasante.eu/index.php"

Indicateur:					
Noms	Utilisation NRPE	Commande finale	Fonction / Paramètres	Test	
URL	Non	check_proxy_http_url.sh -u mediasante.eu	-u: URL à tester	Stopper et redémarrer le serveur web: systemctl stop apache2.service systemctl start apache2.service	

# Indicateurs:

Indicateur:				
Noms	Utilisation NRPE	Commande finale	Fonction / Paramètres	Test
User Session Nagios	Non	show_users.sh -a "nagios" -w 2 -c 3	- a : Nom d'utilisateur - w : Nombre d'utilisateur connecté résultant en un statut WARNING, si ≥ - c : Nombre d'utilisateur connecté résultant en un statut CRITICAL, si ≥	Ouvrir plusieurs session nagios en parallèle: 2 sessions pour un statut WARNING 3 sessions pour un statut CRITICAL
CPU Usage	Oui	check_cpu_info.sh -w 70 -c 90	- w : Pourcentage d'utilisation total CPU résultant en un statut WARNING, si ≥ - c : Pourcentage d'utilisation total CPU résultant en un statut CRITICAL, si ≥	Augmenter temporairement la charge CPU: stress -cpu 2 -timeout 45s
Current Load	Oui	check_load -r -w .7,.6,.5 -c .9,.8,.7	- r : Normalisé pour un cœur - w : Charge moyenne pour les périodes 1, 5, 15 min résultant en un statut WARNING, si ≥ - c : Charge moyenne pour les périodes 1, 5, 15 min résultant en un statut CRITICAL, si ≥	Augmenter temporairement la charge CPU: stress -cpu 2 -timeout 45s
Database	Oui	check_mysql -H localhost -d MediaSante -u nagios -p nagios	-H : Adresse IP ou hostname -d : Nom de la base de données -u : Nom d'utilisateur pour la connexion -p : Mot de passe utilisateur pour la connexion	Stopper et redémarrer le service MariaDB: Systemctl stop mariadb.service Systemctl start mariadb.service
Disk Usage	Oui	check_disk -w 30% -c 20% -p /	- w : Pourcentage d'espace disque libre restant résultant en un statut WARNING, si ≤ - c : Pourcentage d'espace disque libre restant résultant en un statut CRITICAL, si ≤ - p : Point de montage contrôlé	Augmenter l'utilisation disque: dd if=/dev/zero of=/tmp/FichierTestDisque.txt bs=1000M count=4
HTTP	Non	check_http -I \$HOSTADDRESS\$ -w 1 -c 2	- I : Adresse IP cible, \$HOSTADDRESS\$ fait référence à l'adresse de l'hôte nagios - w : Temps de réponse (seconde) résultant en un statut ALERTE, ≥ - c : Temps de réponse (seconde) résultant en un statut WARNING, ≥	Augmenter temporairement la charge d'Apache: Ab -c 50 -n 10000 http://mediasante.eu/
HTTPS	Non	check_http -I \$HOSTADDRESS\$ -S -C 30,15	- I : Adresse IP cible, \$HOSTADDRESS\$ fait référence à l'adresse de l'hôte nagios - S : Connexion via SSL/TLS - C : Nombre de jours minimum pour que le certificat soit valide résultant en un statut WARNING, résultant en un statut CRITICAL, si ≤	Désactiver et réactiver le virtualhost https: A2dissite mediasant.eu-https.conf Systemctl reload apache2.service A2ensite mediasant.eu-https.conf Systemctl reload apache2.service
RAM Usage	Oui	check_mem.sh -w 70 -c 85	- w : Pourcentage de RAM utilisé résultant en un statut WARNING, ≥ - c : Pourcentage de RAM utilisé résultant en un statut CRITICAL, ≥	Augmenter temporairement l'utilisation RAM: stress-ng --vm 2 --vm-bytes 512MBytes --timeout 10s
URL	Non	check_proxy_http_url.sh -u mediasante.eu	- u : URL à tester	Stopper et redémarrer le serveur web: systemctl stop apache2.service systemctl start apache2.service
Web Page Index	Non	check_http -I \$HOSTADDRESS\$ -u /index.php	- I : Adresse IP cible, \$HOSTADDRESS\$ fait référence à l'adresse de l'hôte nagios - u : url cible (default: /)	Modifier la valeur -u avec une page non existante

# Questions / Réponses

# Voies d'améliorations :