Ce cours

Commencé le	dimanche 19 mars 2023, 14:20
État	Terminé
Terminé le	jeudi 23 mars 2023, 21:59
Temps mis	4 jours 7 heures
Points	13,50/15,00
Note	**4,50** sur 5,00 (**90%**)

QUESTION 1

Terminé

Non noté

Prénom et nom des étudiants ayant contribué au labo :

Alexis Martins

QUESTION 2

Terminé

Note de 1,00 sur 1,00

Montrez, avec une copie d'écran, les événements reçus par votre serveur Syslog

Mar 03 22:14:15	127.0.0.1	mymachine	user	debug	TestMessage	Message pour Alexis Martins
Mar 03 22:14:15	127.0.0.1	mymachine	daemon	crit	TestMessage	Message pour Alexis Martins
Mar 03 22:14:15	127.0.0.1	mymachine	auth	notice	TestMessage	Message pour Alexis Martins

Commentaire :

QUESTION 3

Terminé

Note de 1,00 sur 1,00

Montrez votre fichier de configuration (les commandes importantes)

Il suffit d'ajouter la ligne ci-dessous dans le fichier de configuration (/etc/rsyslog.conf). Elle spécifie que tous les types de logs sont redirigés vers le serveur de logs.

. @192.168.81.10

Après cela, il en faut pas oublier de redémarrer le service :
systemctl restart rsyslog

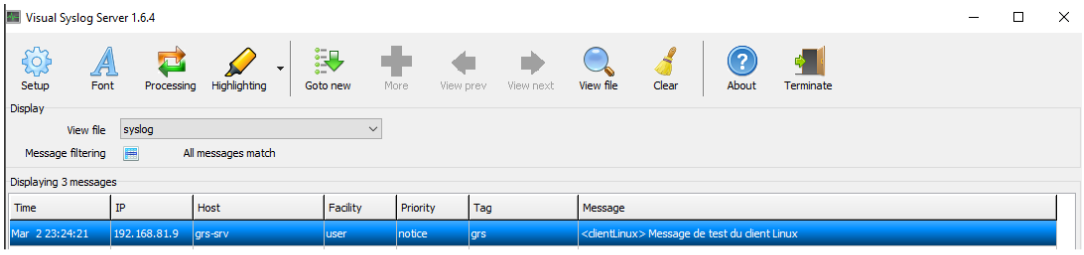
Commentaire :

QUESTION 4

Terminé

Note de 1,00 sur 1,00

Montrez les messages reçus sur la console du serveur syslog distant (Windows 10 B).



Logger

reboot

Mar 2 23:31:18	192.168.81.9	grs-srv	authpriv	notice	sudo	grs : TTY=tty1 ; PWD=/home/grs ; USER=root ; COMMAND=/usr/sbin/reboot now

sudo

Mar 2 23:31:18	192.168.81.9	grs-srv	authpriv	info	sudo	pam_unix(sudo:session): session opened for user root(uid=0) by grs(uid=1000)
Mar 2 23:31:18	192.168.81.9	grs-srv	authpriv	info	sudo	pam_unix(sudo:session): session closed for user root

Commentaire :

QUESTION 5

Terminé

Note de 0,50 sur 1,00

Donnez plusieurs exemples de messages qui vous semblent utiles dans la gestion des réseaux.

- Erreurs de connexion : Les messages de connexion échouée peuvent aider à identifier les problèmes de réseau ou de sécurité, en particulier lorsque ces erreurs se produisent fréquemment.

- Changements de configuration : Lorsqu'un changement est effectué sur un élément actif du réseau, un serveur ou autre, celui-ci est notifié sur le serveur syslog. Ainsi, en cas de disfonctionnement du réseau suite à la mise à jour d'un routeur par exemple, il est facile de retracer que le réseau à cesser de fonctionner à cause de cette mise à jour.

- Surveillance des ressources et performances : On peut imaginer cela par exemple dans le cas de serveurs de stockages sur lesquels on va s'attendre à recevoir des logs concernant le taux d'occupation des disques. On pourrait aussi imaginer appliquer cela à des serveurs pour vérifier en permanence que leur débit et temps de réponse soit acceptable.

Commentaire :
ok, mais quels messages réels générés par le système ?

QUESTION 6

Terminé

Note de 1,00 sur 1,00

Que pouvez-vous dire sur la sécurité des échanges de messages Syslog ?

Par défaut Syslog envoie ses informations sans aucun chiffrement, ni authentification.
Il est cependant possible d'activer Syslog avec SSL/TLS avec la RFC5424.

Cela peut permettre à des personnes malveillantes d'envoyer/changer des messages d'alerte faux.
Cela pourrait provoquer du stress et/ou des routines automatiques de traitement d'alertes.

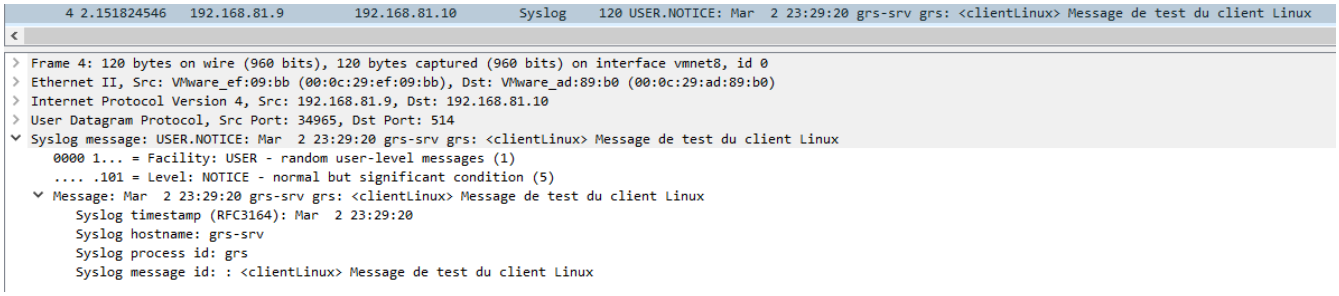
Commentaire :

QUESTION 7

Terminé

Note de 1,00 sur 1,00

Présentez et expliquer la captures wireshark d'un message Syslog.



Dans cette capture, on voit en effet que c'est le protocole Syslog qui est utilisé.

Toutes les informations du messages sont bien mises en claires comme annoncé dans la précédente question.

On y retrouve donc toute la structure que ça soit le Timestamp, la machine source du message, le level et la facility.

On remarque aussi la spécification de la RFC utilisée.

Commentaire :

QUESTION 8

Terminé

Note de 0,00 sur 1,00

Modifiez votre configuration afin que les messages Syslog générés par la commande sudo (et exclusivement ceux-ci) soient stockés dans le fichier local /var/log/sudos.log

Montrez le(s) directive(s) utilisée(s).

Dans un premier temps, on peut faire un alias sur le fichier log dans le fichier ʔetc/rsyslog.d/50-default.conf. Ainsi on pourra le réutilisé pour indiqué où stocké ces logs.

`
local1.* /var/log/sudos.log
`

Ensuite il faut modifier le fichier des sudoers en utilisant la commande ùsudo visudoèt uniquement celle-ci. On ajoute en fin de fichier la ligne suivante ci-dessous.

`
Defaults syslog:local1
`

Finalement, on peut redémarrer le service ʔsyslog,`

`
sudo systemctl restart rsyslo
`

On peut voir maintenant que suite à l'exécution de la commande ùsudo apt update ʔle message se trouve bien dans le fichier sudos.log.

```
grs@grs-srv:~$ cat /var/log/sudos.log
Mar  3 07:46:05 grs-srv sudo:      grs : TTY=tty1 ; PWD=/home/grs ; USER=root ; COMMAND=/usr/bin/apt
 update
```

Commentaire :
Qu'entendez-vous par "créer un alias dans le fichier" ?

Cela ne correspond pas à une redirection syslog, mais à la manière dont sudo génère des logs. En utilisant local1, vous recevrez potentiellement d'autres messages que ceux émis par sudo.

QUESTION 9

Terminé

Note de 1,00 sur 1,00

Montrer les commandes IOS que vous avez utilisé.

en

conf t

logging 192.168.81.10

logging on

logging facility local3

logging trap debugging

Commentaire :

QUESTION 10

Terminé

Note de 1,00 sur 1,00

Montrer les commandes IOS que vous avez utilisé.

Dans mon cas, mon serveur était déjà avec l'heure suisse.
J'ai lu dans la documentation Cisco que c'était normal, car le routeur utilise son propre serveur NTP par défaut.
Cela serait suffisant dans notre cas, parce qu'on possède qu'un seul routeur. Mais si on souhaitait en avoir plusieurs, on aurait meilleur temps d'utiliser un serveur NTP partagé.
Pour faire cela, on peut utiliser la commande ci-dessous.

```
ntp server ch.pool.ntp.org
```

Pour afficher les millisecondes, on peut utiliser cette commande.

```
service timestamps log datetime msec localtime
```

Commentaire :

QUESTION 11

Terminé

Note de 1,00 sur 1,00

Montrer les commandes IOS que vous avez utilisé.

en
conf t
archive
log config
logging enable
notify syslog
hidekeys

Commentaire :

QUESTION 12

Terminé

Note de 1,00 sur 1,00

Déposez une copie d'écran montrant lisiblement le message reçu par votre serveur Syslog

On peut voir que lorsque j'ai apporté des modifications sur l'une des interfaces du routeur, celui-ci nous a bien remonté la modification au serveur.

Mar 16 10:33:57	192.168.81.1		local3	notice	134	*Mar 16 10:33:55.546: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:interface GigabitEthernet2
Mar 16 10:34:02	192.168.81.1		local3	notice	135	*Mar 16 10:34:00.974: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:no ip address

Commentaire :

QUESTION 13

Terminé

Note de 1,00 sur 1,00

Copiez/collez la commande complète utilisée ainsi que le message reçu sur le serveur Syslog (copie d'écran)

logger.exe -p 3 "Message de test de logger.exe"

Mar 3 22:53:01	127.0.0.1	win10-GRS-A	user	err		Message de test de logger.exe

Commentaire :
ok, car utilise l'@loopback par défaut.

QUESTION 14

Terminé

Note de 1,00 sur 1,00

Montrez la commande complète utilisée et les messages reçus par le serveur Syslog (copie d'écran)

Send-SyslogMessage -Server 127.0.0.1 -Message "Message avec la RFC 5424" -Facility user -Severity Warning

Send-SyslogMessage -Server 127.0.0.1 -Message "Message avec la RFC 3164" -RFC3164 -Facility user -Severity Warning

Mar 03 11:10:10	127.0.0.1	1	user	warning		2023-03-03T11:10:08.896414+01:00 win10-GRS-A PowerShell 5684 - - Message avec la RFC 5424
Mar 03 11:11:10	127.0.0.1	Mars	user	warning		3 11:11:09 win10-GRS-A PowerShell Message avec la RFC 3164

Les différences que l'on peut remarquer sur les deux messages sont assez moindres :
- On remarque que le temps est donné plus précisément dans la RFC5424
- La RFC 5424 inclut aussi l'id du processus concerné par le log

Commentaire :

QUESTION 15

Terminé

Note de 1,00 sur 1,00

Créez un script PowerShell qui vérifie toutes les 2 minutes la présence d'un processus (par exemple cmd.exe) et qui génère un message Syslog en cas d'absence.

Copiez/collez le script ainsi que le message reçu sur le serveur Syslog (copie d'écran).

```
while ($true) {
   $process = Get-Process -Name "cmd" -ErrorAction SilentlyContinue
   if (!$process) {

      Send-SyslogMessage -Server 127.0.0.1 -Facility daemon -Severity warning -Message "Le processus cmd.exe est absent."
   }

   Start-Sleep -Seconds 120
}
```

Mar 03 11:29:12	127.0.0.1	1	daemon	warning		2023-03-03T11:29:11.761183+01:00 win10-GRS-A CheckCMD.ps1 8780 - - Le processus cmd.exe est absent.

Commentaire :

QUESTION 16

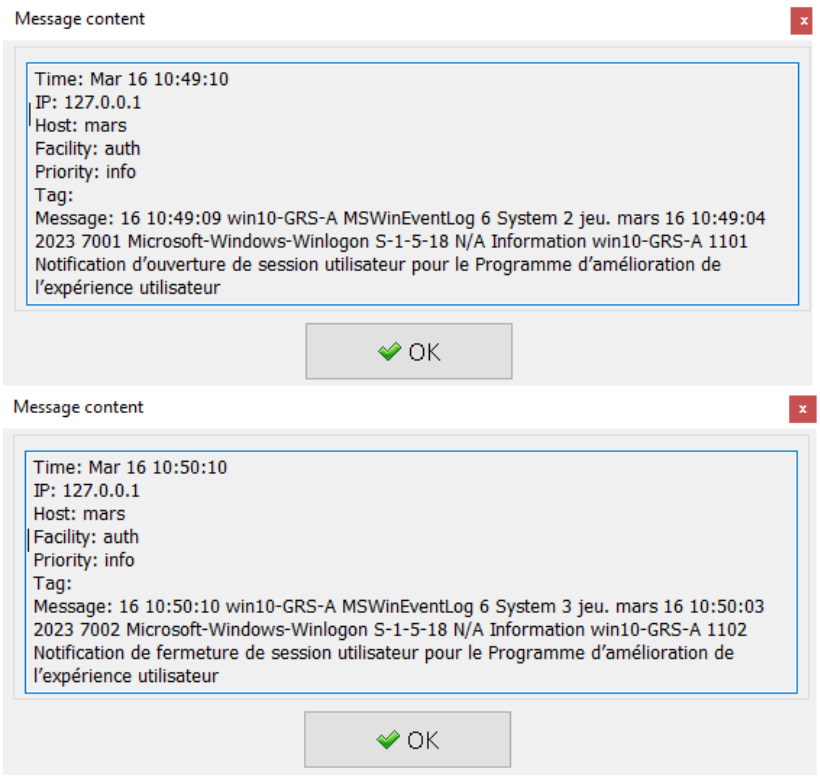
Terminé

Note de 1,00 sur 1,00

Montrez le bon fonctionnement de la redirection à l'aide d'une copie d'écran du serveur Syslog (copie d'écran)

Le programme "SolarWinds Log Forwarder" ne fonctionnait pas directement si on l'utilisait sur le compte GRS.
J'ai donc décidé de créer un second compte appelé "Forward". Le but étant de lancer le serveur Syslog et le Forwarder sur le compte GRS et d'utiliser l'autre compte pour tester.

Ci-dessous un exemple avec une connexion et une déconnexion.



Commentaire :
ok, contournement intéressant

◄ LABO 1 - SYSLOG

Aller à...

LABO 2 - SNMP-WMI ►