

Commencé le vendredi 10 mars 2023, 15:18**État** Terminé**Terminé le** mercredi 15 mars 2023, 16:55**Temps mis** 5 jours 1 heure**Points** 13,00/15,00**Note** 4,33 sur 5,00 (86,67%)**QUESTION 1**

Terminé

Non noté

Prénom et nom des étudiants ayant contribué au labo :

Timothée Van Hove

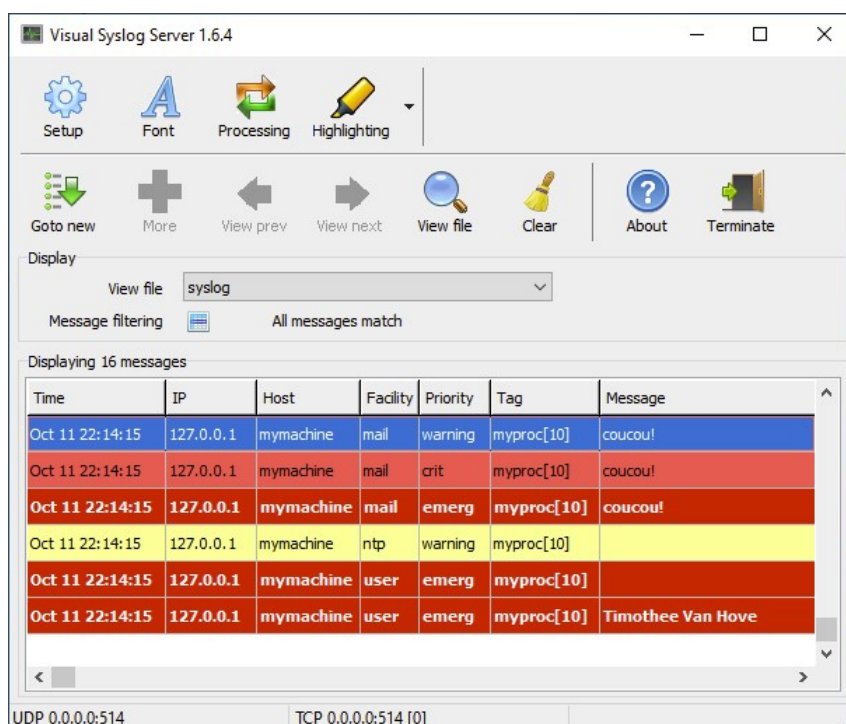
Anthony David (Certaines questions seulement)

QUESTION 2

Terminé

Note de 1,00 sur 1,00

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



Commentaire :



QUESTION 3

Terminé

Note de 1,00 sur 1,00

Montrez votre fichier de configuration (les commandes importantes)

Il suffit d'ajouter l'une des 2 lignes suivantes dans le fichier:

xxx.xxx.xxx.xxx represents your Syslog server ip address

#For sending syslog message to the server via UDP:

*. @xxx.xxx.xxx.xxx:514

#For sending syslog message to the server via TCP:

.* @@xxx.xxx.xxx.xxx:514

Commentaire :

Si pas de TLS/SSL, TCP inutile. Mettez votre adresse IP dans l'exemple (il s'agit d'un labo).



QUESTION 4

Terminé

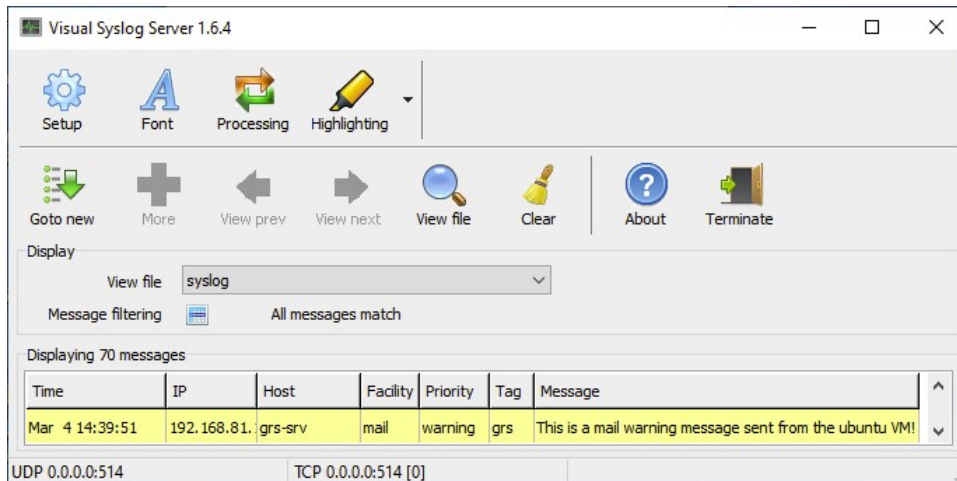
Note de 1,00 sur 1,00

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

Message envoyé depuis la machine ubuntu:

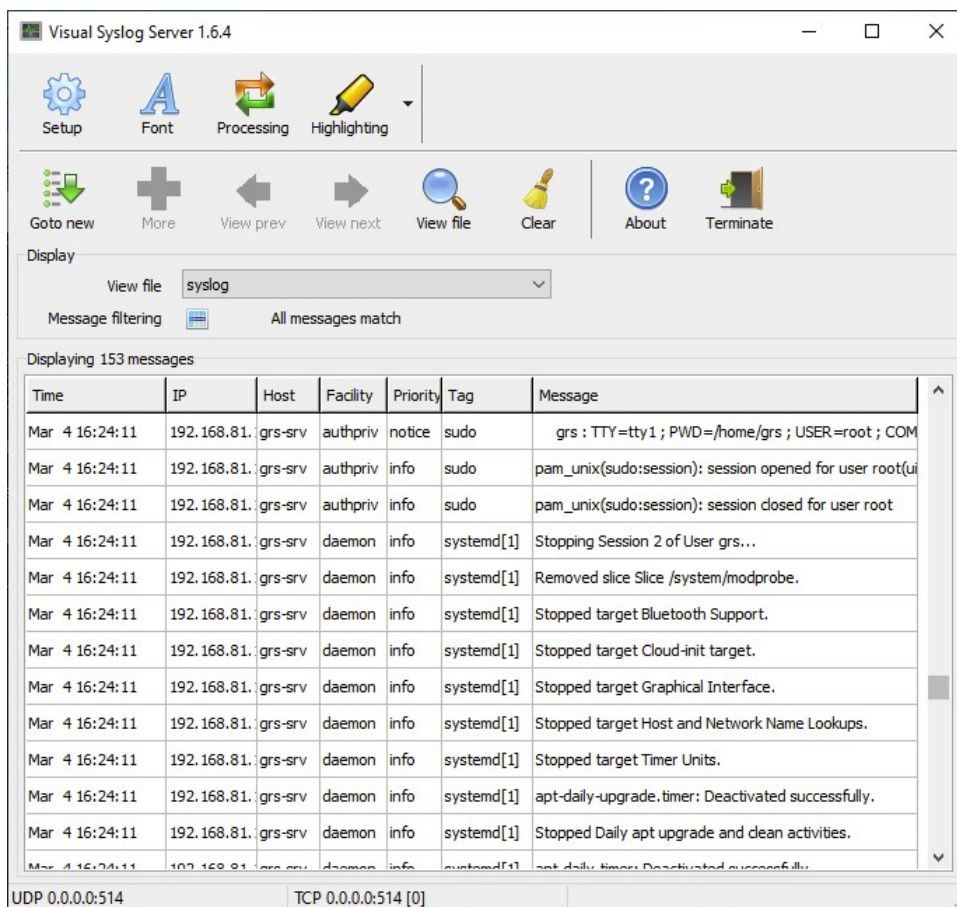
logger -p mail.warning This is a mail warning sent from the ubuntu VM!

Résultat dans le serveur syslog:



Depuis la machine ubuntu: sudo reboot now

Messages dans le serveur syslog:



Analyse wireshark après sudo reboot now:



QUESTION 5

Terminé

Note de 0,00 sur 1,00

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

- 1 . Notifier si une interface réseau tombe
- 2 . Notifier le changement de statut d'un protocole réseau (OSBF/BGP)
- 3 . Notifier les tentatives / échecs de logging SSH pour détecter des menaces
- 4 . Notifier les erreurs système (Software et hardware) pour détecter des instabilités des systèmes
- 5 . Notifier le dépassement d'un seuil de l'utilisation de la bande passante

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 ?

Les messages Syslog ne sont pas chiffrés et pas authentifiés. Le RFC 5224 permet l'utilisation de TCP + TLS/SSL. Un attaquant pourrait intercepter les messages pour se renseigner sur l'architecture réseau d'une entreprise. Il pourrait aussi envoyer de faux messages concernant des problèmes réseau.

Commentaire :



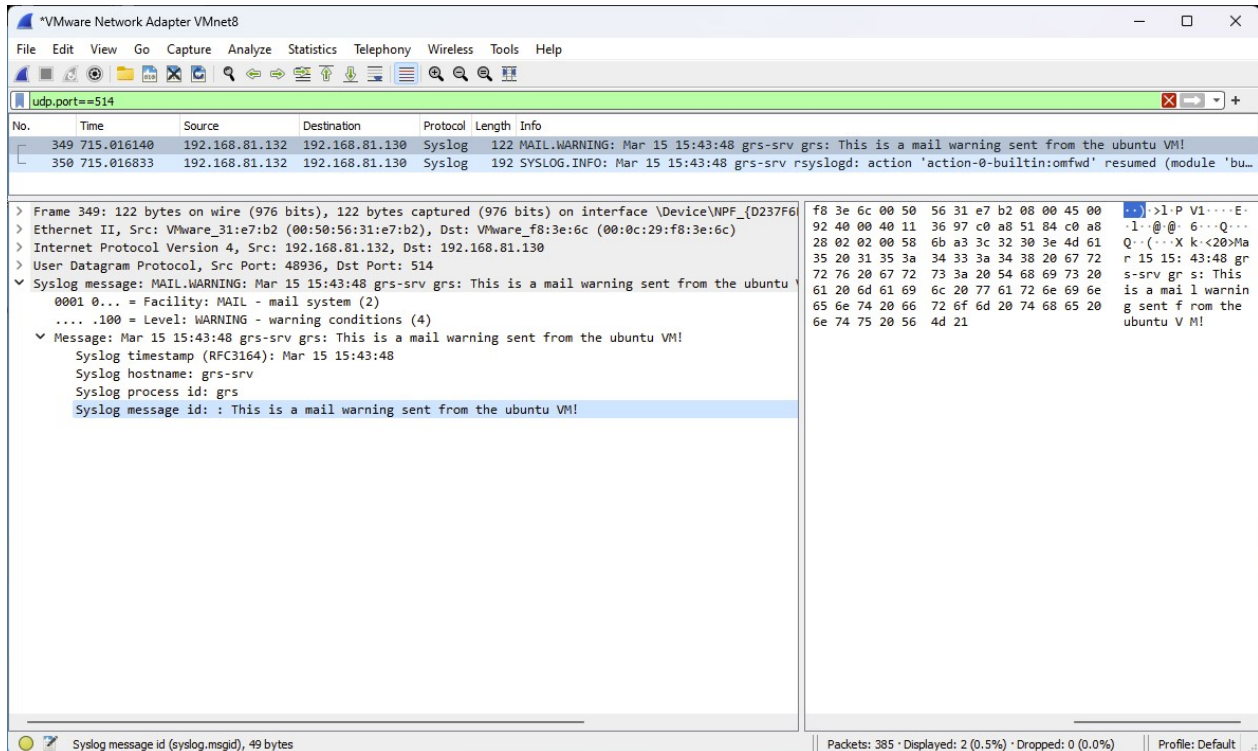
QUESTION 7

Terminé

Note de 0,00 sur 1,00

Présentez et expliquez la capture Wireshark d'un message Syslog.

On peut voir ci-dessous la capture d'un message syslog.



Voici la structure du message:

```

      VERSION                                PROCID
      PRI | TIMESTAMP                        HOSTNAME | APP-NAME | MSGID
<165>1 | 2003-10-11T22:14:15.003Z | mymachine.example.com | evntslog | - ID47
[exampleSDID@32473 iut="3" eventSource="Application" eventID="1011"] BOMan application event log entry...
| STRUCTURED-DATA | MSG
```

• HEADER

- **PRI** ou "priority", est un entier calculé à partir de la Facility et la Severity:

```
PRI = Facility * 8 + Severity
```

- **VERSION** la version est toujours "1" pour la RFC 5424
- **TIMESTAMP** exemples de timestamps (doit suivre le format ISO 8601):
 - 1985-04-12T23:20:50.52Z
 - 2003-08-24T05:14:15.000003-07:00
 - - (Valeur "nil") si la date n'est pas disponible
- **HOSTNAME** — L'utilisation d'un FQDN (fully qualified domain name) est recommandé, p.ex. mymachine.example.com
- **APP-NAME** — Normalement le nom de l'appareil ou de l'application qui a envoyé le message
- **PROCID** — Souvent utilisé pour identifier le PID (process id) de l'application
- **MSGID** — Identifie le message
- **STRUCTURED-DATA** — Listes sous forme clé-valeur pour faciliter la recherche et le parsing
- **MSG** Détails concernant l'évènement
 - Si le message est encodé en UTF-8, le string doit commencer avec le "Unicode byte order mask" (BOM)

Commentaire :



mais ceci correspond-il au format de votre message ?

QUESTION 8

Terminé

Note de 1,00 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).

1. Dans le fichier /etc/rsyslog.conf, il faut ajouter la ligne de code suivante :
if \$programname == 'sudo' then /var/log/sudos.log
2. Enregistrer le fichier /etc/rsyslog.conf et redémarrer le service rsyslog:
sudo systemctl restart rsyslog

Commentaire :



QUESTION 9

Terminé

Note de 1,00 sur 1,00

Montrer les commandes IOS que vous avez utilisé.

```
enable
conf t
logging on
logging 192.168.81.130
logging trap debugging
logging facility local3
```

Commentaire :



QUESTION 10

Terminé

Note de 1,00 sur 1,00

Montrer les commandes IOS que vous avez utilisé.

enable

conf t

service timestamps log datetime msec

ntp server 195.141.111.5

clock timezone CET 1

ntp source GigabitEthernet1

Commentaire :

ntp source pas nécessaire



QUESTION 11

Terminé

Note de 1,00 sur 1,00

Montrer les commandes IOS que vous avez utilisé.

```
enable
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

J'ai changé le niveau de logging de warning à debug dans le routeur cisco et le serveur syslog à reçu ce log:

Mar 15 15:29:14	192.168.81.131		local3	notice	20	%Mar 15 15:29:13.084: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:logging trap debugging
-----------------	----------------	--	--------	--------	----	--

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)

Commande utilisée : `logger.exe -p local3.info -l localhost test`

Log reçu:

Mar 15 15:06:43	127.0.0.1	win10-GRS-A	local3	info	test
-----------------	-----------	-------------	--------	------	------

Commentaire :



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)

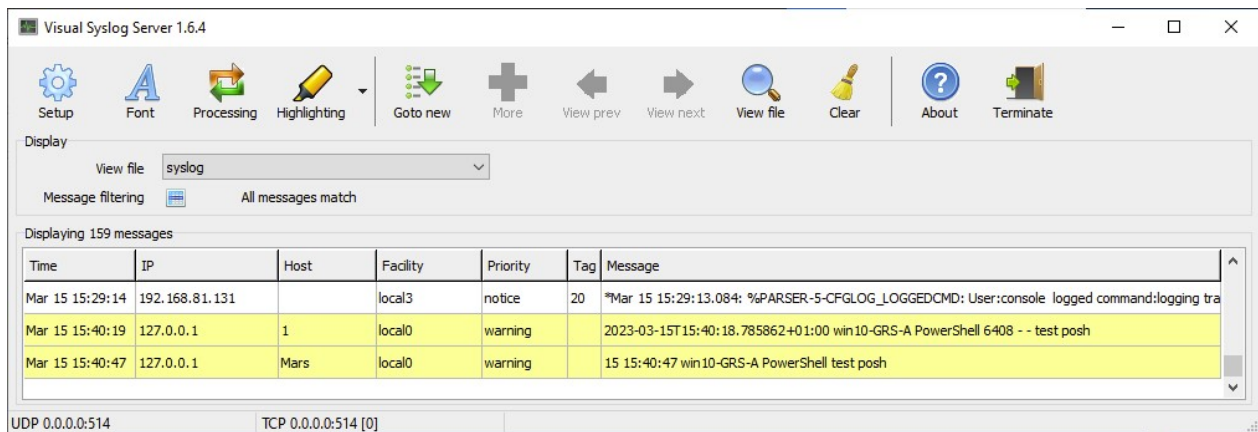
Commande avec RFC5424 (par défaut)

```
PS C:\WINDOWS\system32> Send-SyslogMessage -Server localhost -Severity 4 -Facility 16 -Message "test posh"
```

Commande avec RFC3164

```
PS C:\WINDOWS\system32> Send-SyslogMessage -Server localhost -Severity 4 -Facility 16 -Message "test posh" -RFC3164
```

Logs reçus:



The screenshot shows the Visual Syslog Server 1.6.4 application window. The interface includes a toolbar with icons for Setup, Font, Processing, Highlighting, Goto new, More, View prev, View next, View file, Clear, About, and Terminate. Below the toolbar, there is a 'Display' section with a 'View file' dropdown set to 'syslog' and a 'Message filtering' section with a button for 'All messages match'. The main area displays a table of 159 messages. The table has columns for Time, IP, Host, Facility, Priority, Tag, and Message. The following messages are visible:

Time	IP	Host	Facility	Priority	Tag	Message
Mar 15 15:29:14	192.168.81.131		local3	notice	20	*Mar 15 15:29:13.084: %PARSER-5-CFGLOG_LOGGEDCMD: User:console logged command:logging tra
Mar 15 15:40:19	127.0.0.1	1	local0	warning		2023-03-15T 15:40:18.785862+01:00 win10-GRS-A PowerShell 6408 - - test posh
Mar 15 15:40:47	127.0.0.1	Mars	local0	warning		15 15:40:47 win10-GRS-A PowerShell test posh

At the bottom of the window, there is a status bar showing 'UDP 0.0.0.0:514' and 'TCP 0.0.0.0:514 [0]'.

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).

PS Script:

```
# Import the Posh-SYSLOG module
Import-Module -Name Posh-SYSLOG

# Define the IP address of the syslog server
$syslogServer = "192.168.81.130"

# Define the message to be sent in the syslog message
$message = "cmd.exe is not running"

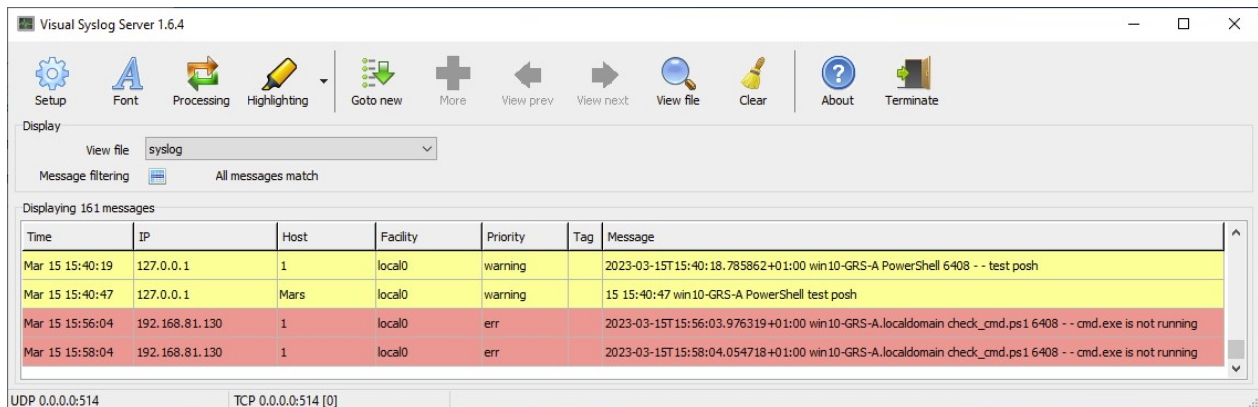
# Define the interval for checking if cmd.exe is running (in seconds)
$interval = 120

# Loop indefinitely
while ($true) {
    # Check if cmd.exe is running
    if (Get-Process -Name cmd -ErrorAction SilentlyContinue) {
        # If cmd.exe is running, sleep for the specified interval and continue the loop
        Start-Sleep -Seconds $interval
        continue
    }

    # If cmd.exe is not running, send a syslog message
    Send-SyslogMessage -Server $syslogServer -Severity Error -Facility Local0 -Message $message

    # Sleep for the specified interval before checking again
    Start-Sleep -Seconds $interval
}
```

Capture:



Time	IP	Host	Facility	Priority	Tag	Message
Mar 15 15:40:19	127.0.0.1	1	local0	warning		2023-03-15T15:40:18.785862+01:00 win10-GRS-A PowerShell 6408 - - test posh
Mar 15 15:40:47	127.0.0.1	Mars	local0	warning		15 15:40:47 win10-GRS-A PowerShell test posh
Mar 15 15:56:04	192.168.81.130	1	local0	err		2023-03-15T15:56:03.976319+01:00 win10-GRS-A.localdomain check_cmd.ps1 6408 - - cmd.exe is not running
Mar 15 15:58:04	192.168.81.130	1	local0	err		2023-03-15T15:58:04.054718+01:00 win10-GRS-A.localdomain check_cmd.ps1 6408 - - cmd.exe is not running

UDP 0.0.0.0:514 TCP 0.0.0.0:514 [0]

Commentaire :

A mon avis, votre script génère un message toutes les 2 minutes en sortant du if, même si cmd is running...

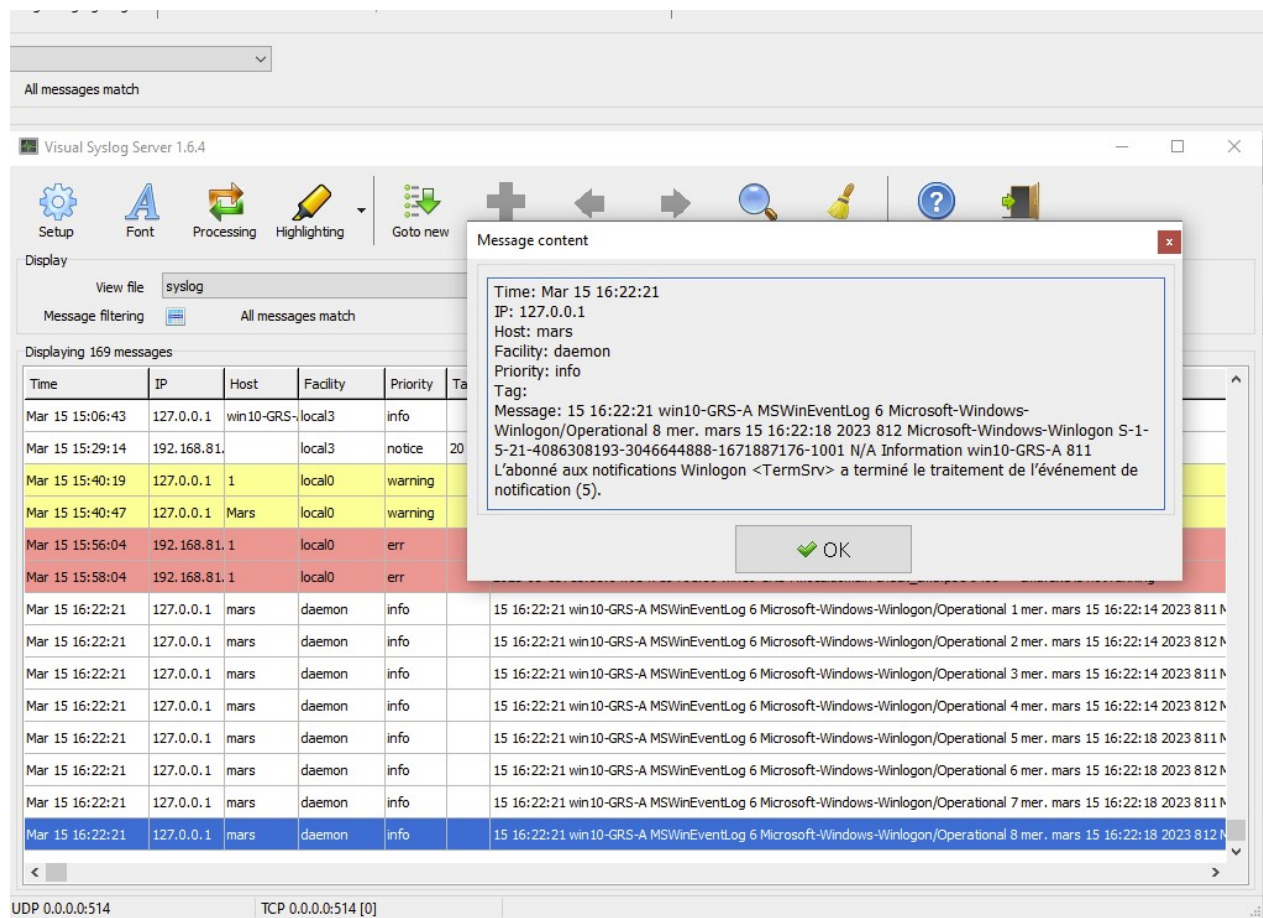


QUESTION 16

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)



Commentaire :

◀ LABO 1 - SYSLOG

Aller à...

LABO 2 - SNMP-WMI ▶

