

Commencé le mercredi 12 avril 2023, 07:21

État Terminé

Terminé le lundi 17 avril 2023, 13:15

Temps mis 5 jours 5 heures

Note 22,00 sur 23,00 (95,65%)

QUESTION 1

Terminé

Non noté

Prénom et nom des étudiants ayant contribué au labo :

Timothée Van Hove

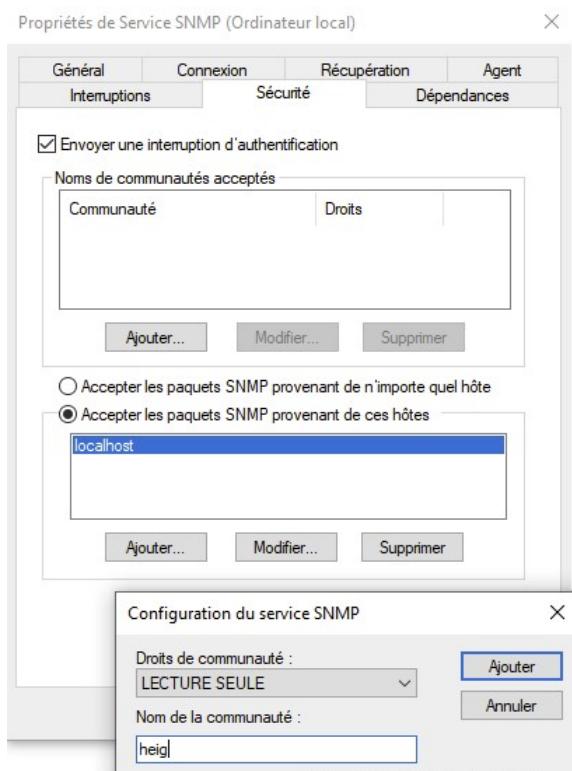
QUESTION 2

Terminé

Note de 1,00 sur 1,00

Montrez à l'aide de captures d'écran les changements de configuration que vous avez réalisés

Pour configurer l'agent SNMP, il suffit de modifier le service SNMP de windows, comme dans l'image qui suit:



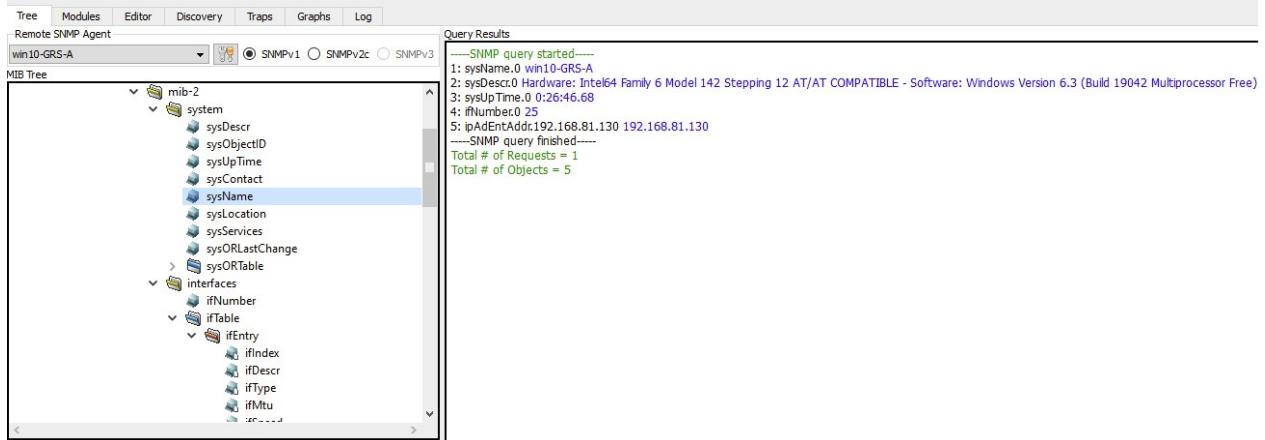
Commentaire :

QUESTION 3

Terminé

Note de 1,00 sur 1,00

Montrez les valeurs retournées par les 5 objets SysDescr, SysName, SysUpTime, ifNumber, et l'adresse IP de votre cible.



On peut voir que le MIB sysDescr.0 décrit notre hardware comme étant un Intel64 Family 6 Model 142, ce qui correspond à une architecture de processeur Kaby Lake (intel 7th gen), ce qui n'est pas le cas de ma machine, mais nous sommes dans une machine virtuelle, donc c'est probablement les informations de notre hyperviseur. En termes logiciel, le MIB indique Windows Version 6.3, (équivaut à Windows 8.1), et a un numéro de build de 19042. Ce numéro de build correspond à Windows 10 version 20H2, ce qui est la version notre OS.

Le MIB ifNumber me semble être faux, car notre machine ne possède pas 25 interfaces, mais bien 3:

C:\Users\labo>netsh interface ipv4 show interfaces				
Idx	Mét	MTU	État	Nom
1	75	4294967295	connected	Loopback Pseudo-Interface 1
10	25	1500	connected	Ethernet0 2
14	65	1500	disconnected	Connexion réseau Bluetooth

Commentaire :

de nombreuses interfaces "virtuelles" sont cachées par défaut. Visibles via netsh ou le gestionnaire de périphériques par exemple

QUESTION 4

Terminé

Note de 1,00 sur 1,00

Montrez la configuration du routeur cisco de manière à ce qu'il puisse être géré via SNMPv2 (choisissez cisco pour community string RO et ciscorw pour community string RW). Configurez également le routeur pour qu'il envoie ses traps snmp au manager SNMPb sur Windows A. Prévoyez la synchro temps et l'affichage des événements en ms.

Configuration pour le paramétrage de SNMPv2:

```
enable
conf t
snmp-server community ciscoRO ro
snmp-server community ciscorW rw
snmp-server enable traps
snmp-server host 192.168.81.130 version 2c ciscoRW
snmp-server host 192.168.81.130 traps ciscoRW
snmp-server view mib2 mib-2 included
```

Commentaire :

A quoi servent les string **ciscoRW** sur les avant-dernières commandes ?

A quoi sert la commande **snmp-server view mib2 mib-2 included** ?

QUESTION 5

Terminé

Note de 1,00 sur 1,00

Montrez les valeurs retournées par les 5 objets SysDescr, SysName, SysUpTime, sysObjectID, et l'adresse IP de votre cible.

The screenshot shows a software interface for managing network devices. At the top, there's a menu bar with tabs: Tree, Modules, Editor, Discovery, Traps, Graphs, and Log. Below the menu is a toolbar with icons for Remote SNMP Agent, GRP_tr, SNMPv1, SNMPv2c, and SNMPv3. A 'MIB Tree' section displays a tree structure with nodes like mgmt, mib-2, and system, with further sub-nodes under system such as sysDescr, sysObjectID, sysUpTime, sysContact, sysName, sysLocation, sysServices, and sysORLastCh... A 'Query Results' panel on the right contains the following text:

```
----SNMP query started----
1: sysDescr.0 Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.2, RELEASE SOFTWARE (fc3) Technical Support:
2: sysUpTime.0 3:05:47.33
3: sysName.0 GRS_tr
4: rNumber.0 5
5: ipAdEntAddr.192.168.81.131 192.168.81.131
----SNMP query finished----
Total # of Requests = 1
Total # of Objects = 5
```

Below the MIB Tree is a 'Node Info' panel containing detailed information about the selected object (sysDescr):

Name:	sysDescr
OID:	1.3.6.1.2.1.1.1
Composed Type:	DisplayString
Base Type:	OCTET STRING
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size:	0 .. 255
Module:	SNMPv2-MIB
Description:	A textual description of the entity. This value should include the full name and version identification of

Commentaire :

QUESTION 6

Terminé

Note de 1,00 sur 1,00

A quoi sert/correspond la valeur renvoyée par sysObjectID ? Que vous manque-t-il pour l'interpréter correctement ?

La valeur de sysObjectID est un OID qui identifie l'identificateur d'objet attribué par le fabricant du périphérique. Cet identificateur d'objet est généralement attribué par le fabricant pour identifier de manière unique ses dispositifs. Les gestionnaires SNMP peuvent utiliser sysObjectID pour déterminer le type de périphérique et ses fonctionnalités. La valeur de sysObjectID peut être croisée avec un module MIB pour déterminer les détails spécifiques du périphérique, tels que ses versions matérielles et logicielles. Par exemple, chez moi la valeur sysObjectID est **enterprises.9.1.1537**, cela indique que le périphérique est un routeur Cisco. Le préfixe **enterprises** indique que l'identifiant est attribué par une entreprise privée, et **9.1.1xxx** est l'identifiant attribué par Cisco pour leurs routeurs. Le code de node de notre cisco est 1537, ce qui correspond à un routeur ciscoCSR1000v

Avec quelques recherches sur le net j'ai donc pu interpréter correctement quel est ce matériel, maintenant, il faudrait intégrer le fichier MIB de description pour avoir les informations détaillées de l'appareil.

J'ai cherché ici, mais je n'ai pas trouvé de MIB pour le CSR1000v.

Commentaire :

MIB générique CISCO-PRODUCT-MIB pour commencer

QUESTION 7

Terminé

Note de 1,00 sur 1,00

A l'aide de Wireshark, capturez et présentez de manière lisible les trames lorsque la machine Windows 10 interroge le routeur Cisco pour obtenir le nom de l'équipement (les champs concernant SNMP doivent être visibles et commentés).

1. SNMP GET-REQUEST

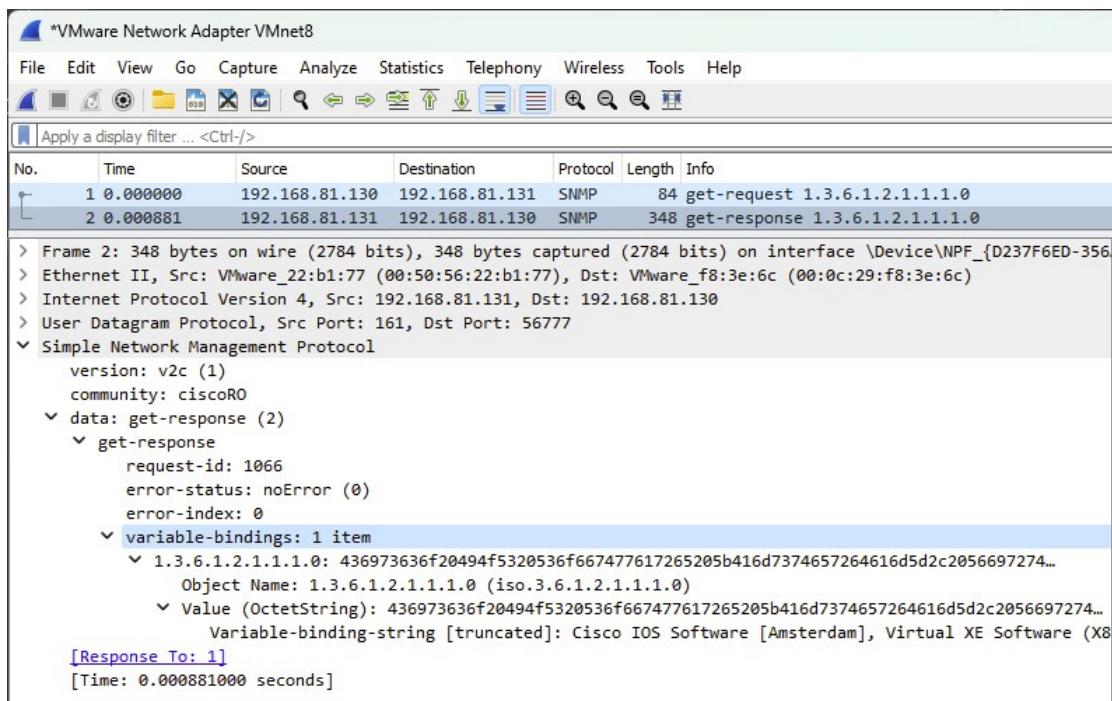
Nous allons d'abord analyser la requête SNMP (uniquement le protocole SNMP)

The screenshot shows a Wireshark capture window titled "VMware Network Adapter VMnet8". The packet list pane displays two frames: a GET-REQUEST from source 192.168.81.130 to destination 192.168.81.131, and a GET-RESPONSE from source 192.168.81.131 to destination 192.168.81.130. The details pane shows the SNMP protocol structure of the request, including version (v2c), community (ciscoRO), and a single variable-binding for OID 1.3.6.1.2.1.1.1.0 with a null value. The bytes pane shows the raw hex and ASCII data of the frame.

1. Version: Il s'agit de la version 2c du protocole SNMP
2. Community: Il s'agit du community string utilisé pour "l'authentification" pour accéder au device.
3. data: get-request: Message SNMP de type get-request utilisé pour avoir la valeur d'un OID.
 1. request-id: L'ID de demande est défini sur 1066, qui est un identificateur unique utilisé pour faire correspondre la demande avec la réponse correspondante.
 2. error-status: L'état de l'erreur est défini sur noError (0), ce qui indique qu'aucune erreur ne s'est produite lors du traitement de la demande SNMP.
 3. error-index: L'index d'erreur est défini sur 0, ce qui indique qu'aucune erreur n'a été commise avec l'OID spécifié dans la demande.
4. variable-bindings: Il s'agit d'une liste de paires OID-valeur qui spécifie les objets pour lesquels la demande est effectuée. Dans ce cas, il n'existe qu'une seule paire OID-valeur:
 1. OID: 1.3.6.1.2.1.1.1.0 (iso.3.6.1.2.1.1.1.0), qui correspond à l'objet de description du système.
 2. Value: Null. Cela signifie que la valeur de l'objet de description système est demandée mais n'est définie avec aucune valeur.

2. SNMP GET-RESPONSE

Maintenant analysons la réponse SNMP



1. version: v2c (1): Indique que cette trame SNMP utilise la version 2c du protocole SNMP.
2. community: ciscoRO: community string utilisée pour "l'authentification" entre le gestionnaire SNMP et l'agent SNMP.
3. data: get-response (2): Indique qu'il s'agit d'une réponse à une demande get-request SNMP. Le champ de données contient les informations demandées.
4. get-response:
 1. request-id: 1066 : ID de la demande SNMP d'origine à laquelle répondre.
 2. error-status : noError (0) : indique qu'aucune erreur ne s'est produite lors du traitement de la requête SNMP.
 3. error-index: 0 : indique qu'aucune erreur ne s'est produite lors du traitement de la requête SNMP.
 4. variables-bindings: 1 item : nombre de variables dans la réponse SNMP.
 1. 1.3.6.1.2.1.1.1.0: : Variable demandée dans la demande de réception SNMP d'origine, ainsi que sa valeur.
 2. Value (OctetString): Valeur de la variable demandée, représentée sous forme de chaîne d'octet. Cela correspond à la description système de l'agent SNMP. La variable-binding-string fournit la valeur de la chaîne de description du système : " Cisco IOS Software [Amsterdam], Virtual XE Software (X86_64_LINUX_IOSD-UNIVERSALK9-M), Version 17.3.2, RELEASE SOFTWARE (fc3)\r\nSupport technique : http://www.cisco.com/techsupport\r\nCopyright (c) 198 ".

Commentaire :

Pour la requête, les valeurs *error-status* et *error-index* n'ont pas de signification

QUESTION 8

Terminé

Note de 1,00 sur 1,00

Montrez et analysez l'échange de messages capturés par Wireshark lors du changement de nom (*hostname*) de votre routeur,

1. SNMP SET-REQUEST

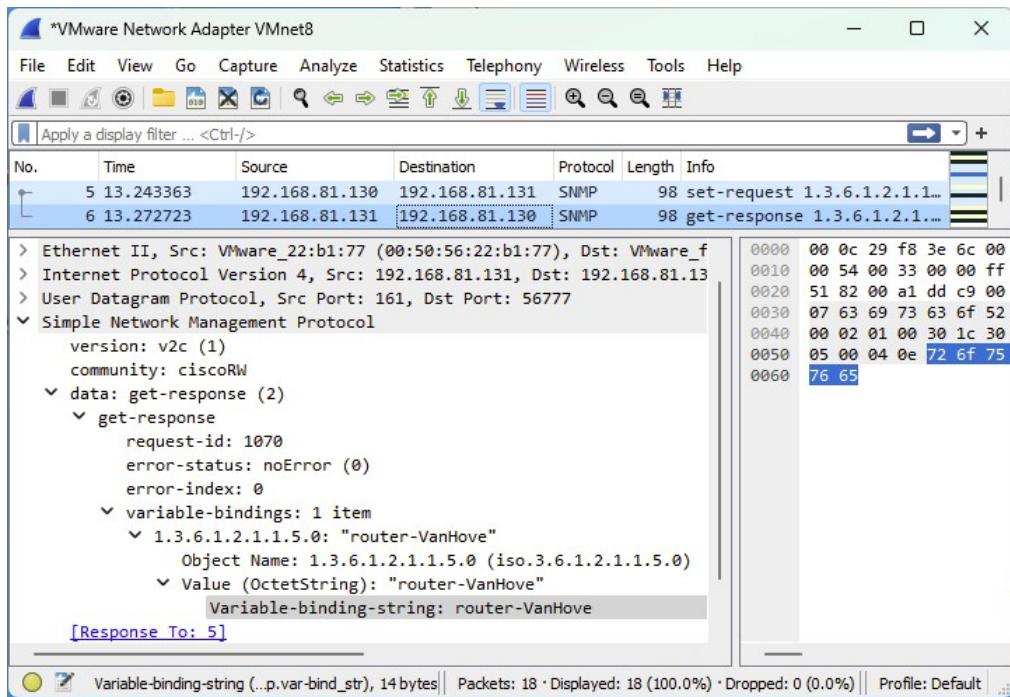
Analysons les trames d'une requête SNMP pour un changement de hostname:

The screenshot shows a Wireshark capture window titled "*VMware Network Adapter VMnet8". The packet list pane shows two SNMP messages: a set-request from 192.168.81.130 to 192.168.81.131 and a get-response from 192.168.81.131 back to 192.168.81.130. The details pane displays the SNMP protocol structure of the selected set-request message. The selected message is a "set-request" with request-id 1070, noError error-status, and index 0. It contains one variable-binding for the OID 1.3.6.1.2.1.1.5.0 with the value "router-VanHove". The bytes pane shows the raw hex and ASCII data of the captured frame.

1. Version: version du protocole SNMP utilisée dans le message. Dans ce cas, v2c (version 2c).
2. Community: Community string utilisé pour l'authentification. Dans ce cas, ciscoRW.
3. Data: payload du message SNMP. Dans ce cas, une set-request.
4. Set-request: type de message SNMP utilisé pour définir la valeur d'une variable sur le périphérique distant.
5. Request-id: identificateur unique de la requête SNMP. Dans ce cas, 1070.
6. Error-status: code d'état indiquant si une erreur s'est produite lors du traitement de la demande. Dans ce cas, noError (0) indique que la demande a réussi.
7. Error-index: index indiquant quelle liaison de variable a provoqué une erreur en cas d'échec de la demande. Dans ce cas, 0 n'indique aucune erreur.
8. Variable-bindings: liste de paires OID-valeur qui spécifie les objets pour lesquels la demande est effectuée. Dans ce cas, il n'existe qu'une seule paire OID-valeur:
 1. Object Name : identificateur d'objet (OID) en cours de modification. Dans ce cas, 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0) correspond hostname.
 2. Value(OctetString) : nouvelle valeur de l'objet en cours de modification. Dans ce cas, "router-VanHove" est le nouveau nom défini pour le système.

1. SNMP GET-RESPONSE

Étonnamment, dans Wireshark, la réponse à une set-request s'appelle une "get-response":



Cette capture est une réponse à une set-request SNMP. Il contient les informations suivantes :

1. Version SNMP : v2c
2. Community string : ciscoRW
3. data: get-response
4. Request ID: réponse à la requête 1070
5. Error status: noError
6. Error status: noError
7. Variable bindings: 1 item
 1. Object Identifier (OID): 1.3.6.1.2.1.1.5.0 (iso.3.6.1.2.1.1.5.0)
 2. Value (OctetString): "router-VanHove"

La demande Set concernait le changement du nom système (1.3.6.1.2.1.1.5.0) et la réponse contient la valeur "router-VanHove". Cela signifie que l'agent SNMP exécuté sur le périphérique a répondu avec le nom du système qui a été modifié.

Commentaire :

QUESTION 9

Terminé

Note de 1,00 sur 1,00

Montrez les messages (traps) reçus par l'application SNMPb.

Pour générer un trap cisco offre la possibilité de faire des tests:

```
router-VanHove#test snmp trap?  
trap  
  
router-VanHove#test snmp trap ?  
call-home      Test CISCO-CALLHOME-MIB trap  
config         Test CISCO-CONFIG-MAN-MIB Trap  
config-copy    Test CISCO-CONFIG-COPY-MIB trap  
entity         Test CISCO-ENTITY-MIB Traps  
entity-diag   Test CISCO-ENTITY-DIAG-MIB traps  
entity-qfpmib  Test CISCO-ENTITY-QFPMIB-MIB traps  
flash          Test CISCO-FLASH-MIB Trap  
snmp           Test SNMPv2-MIB and IF-MIB trap  
syslog         Test CISCO-SYSLOG-MIB trap  
trustsec-sxp   Test CISCO-TRUSTSEC-SXP-MIB traps  
  
router-VanHove#test snmp trap entity  
Generating entConfigChange Trap  
router-VanHove#_
```

J'ai donc utilisé la commande "**test snmp trap entity**".

Voici ce que SNMPb a relevé suite à la commande:

SnmpB

File Tools Options Help

Tree Modules Editor Discovery Traps Graphs Log

Trap log

No	Date	Time	Timestamp	Notification Type	Message Type	Version
0020	2023-04-12	20:41:53	0:00:55.38	mib-2.47.2.0.1	Trap(v2)	SNMPv2c
0021	2023-04-12	20:41:58	0:00:55.38	coldStart	Trap(v1)	SNMPv1
0022	2023-04-12	20:42:02	0:00:55.38	mib-2.47.2.0.1	Trap(v1)	SNMPv1
0023	2023-04-12	20:42:07	0:00:55.39	enterprises.9.9.658.0.4	Trap(v2)	SNMPv2c
0024	2023-04-12	20:42:11	0:00:55.39	enterprises.9.9.658.0.4	Trap(v1)	SNMPv1
0025	2023-04-12	20:42:16	0:00:55.39	enterprises.9.9.831.1.13	Trap(v2)	SNMPv2c
0026	2023-04-12	20:42:20	0:00:55.39	enterprises.9.9.831.1.0.13	Trap(v1)	SNMPv1
0027	2023-04-12	20:42:25	0:01:06.91	enterprises.9.9.221.0.1	Trap(v2)	SNMPv2c
0028	2023-04-12	20:42:29	0:01:06.91	enterprises.9.9.221.0.1	Trap(v1)	SNMPv1
0029	2023-04-12	20:42:34	0:01:48.31	mib-2.47.2.0.1	Trap(v2)	SNMPv2c
0030	2023-04-12	20:42:38	0:01:48.31	mib-2.47.2.0.1	Trap(v1)	SNMPv1

Trap content Trap info

- Bindings (1)
 - #0 mib-2.47.1.4.1.0: 0:00:15.27

Community: ciscoRW

Pour trouver l'OID dans la colonne "Notification Type", il faut remplacer le préfixe par son OID. Par exemple, le message de test que j'ai envoyé correspond à la notification **mib-2.2.47.2.0.1**. mib-2 a l'OID 1.3.6.1.2.1, donc l'OID complet du message est **1.3.6.1.2.1.47.1.4.1**. Il correspond à:

"Valeur de sysUpTime au moment où une ligne conceptuelle est créée, modifiée ou supprimé les tables : entPhysicalTable, entLogicalTable, entLPMappingTable, entAliasMappingTable ou entPhysicalContainsTable".

OID après un démarrage du routeur (cold start):

On peut aussi voir qu'après un cold start le routeur envoie plusieurs traps. J'en ai pris une au hasard:

enterprises.9.9.221.1.1.2.1.18.10.8 Qui correspond à **1.3.6.1.4.1.9.9.221.1.1.2.1.18**, ce qui correspond à l'objet **cempMemBufferPeakTime** : "Indique l'heure de la modification la plus récente du pic nombre de tampons (objet **cempMemBufferPeak**) dans le pool. "

Commentaire :

Bien

QUESTION 10

Terminé

Note de 0,50 sur 1,00

Analysez les trames de la capture précédente et décodez la signification des différents messages SNMP en recherchant la signification du « OID code » à l'aide du SNMP Object Navigator Cisc

J'ai répondu à cette question dans la question précédente =)

Commentaire :

Merci de répondre aux questions au bon endroit, sinon, ça rend la correction compliquée.

Maque la capture.

QUESTION 11

Terminé

Note de 1,00 sur 1,00

Montrez la configuration de votre routeur de manière à ce qu'il n'accepte des requêtes SNMP que de la part de votre machine Windows 10 uniquement.

Il faut configurer des access-lists:

```
# Création de l'ACL qui autorise uniquement la machine windows  
access-list 10 permit 192.168.81.130  
access-list 10 deny any
```

Application de l'access list:

```
snmp-server community ciscoRO RO 10
```

Vérification de la config

```
show snmp
```

Commentaire :

"access-list 10 deny any" implicite.

ACL à appliquer sur toutes les commandes "snmp-server community ..." "

QUESTION 12

Terminé

Note de 1,00 sur 1,00

Montrez le(s) fichier(s) de configuration nécessaires à la configuration de SNMP sur votre nœud Linux

Commandes :

```
# Installer snmpd  
sudo apt install snmp snmpd
```

```
# Accès au fichier de configuration
```

```
sudo nano /etc/snmp/snmpd.conf
```

Ajouter l'adresse ip de l'interface dans agentaddress et changer la ligne qui concerne le community
en spécifiant l'adresse IP du manager:

```
GNU nano 6.2                               /etc/snmp/snmpd.conf *
```

```
# are concatenated together (using ':'s).  
# arguments: [transport:]port[@interface/address],...  
agentaddress  udp:127.0.0.1:161,udp:192.168.81.128:161 ←  
  
#####  
# SECTION: Access Control Setup  
#  
# This section defines who is allowed to talk to your running  
# snmp agent.  
  
# Views  
#   arguments viewname included [oid]  
  
# system + hrSystem groups only  
view  systemonly included   .1.3.6.1.2.1.1  
view  systemonly included   .1.3.6.1.2.1.25.1  
  
# rocommunity: a SNMPv1/SNMPv2c read-only access community name  
#   arguments: community [default|hostname|network/bits] [oid | -V view]  
  
# Read-only access to everyone to the systemonly view  
rocommunity heig 192.168.81.130 ←  
  
# Redémarrer le service snmpd  
sudo systemctl restart snmpd  
  
# Ouvrir le port 161 dans le firewall  
sudo ufw allow snmp
```

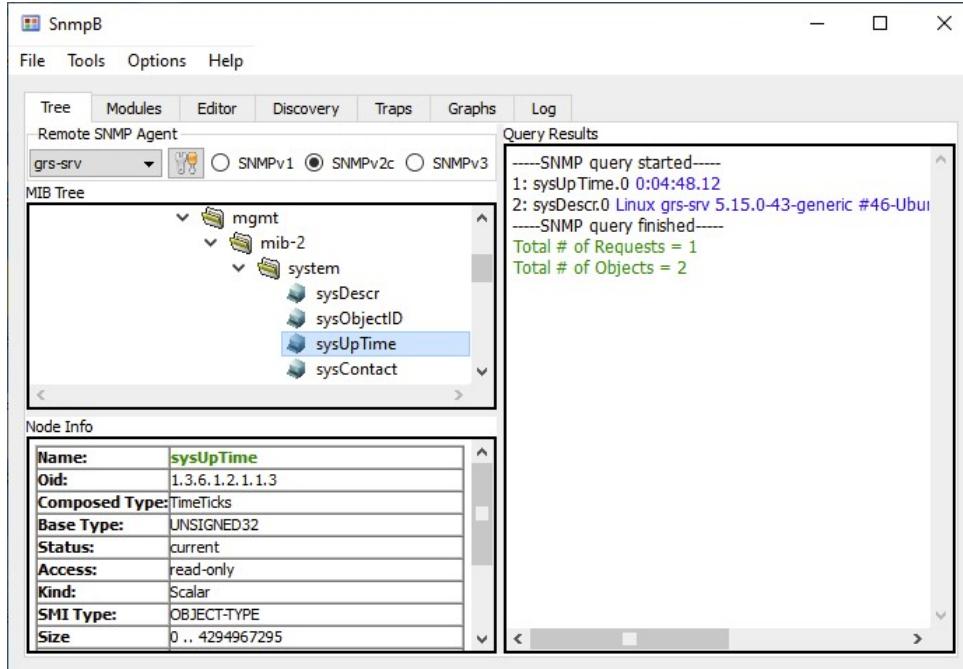
Commentaire :

QUESTION 13

Terminé

Note de 1,00 sur 1,00

Montrez le résultat dans SNMPB d'une requête permettant de connaître la durée de fonctionnement de votre nœud Linux.



Commentaire :

QUESTION 14

Terminé

Note de 1,00 sur 1,00

Montrez la commande (cmdlet) utilisée depuis Windows pour récupérer le nom de votre routeur.

```
# Crée l'object COM permettant de gérer les commandes SNMP
$SNMP = New-Object -ComObject olePrn.OleSNMP

# Etabli la connexion SNMP v2 avec le router.
$SNMP.open('192.168.81.131';'ciscoRO';2,1000)

#Effectue une requête GET avec l'OID sysName
$RESULT = $SNMP.get('1.3.6.1.2.1.1.5.0')

# Ferme la connexion
$SNMP.Close()

#Affiche ne nom du router
Write-Output "Device name: $RESULT"
```

Commentaire :

OK, mais plus simple avec une seule cmdlet...

QUESTION 15

Terminé

Note de 1,00 sur 1,00

Montrez la commande (*cmdlet*) ou le script utilisé pour récupérer toutes les minutes la liste des processus/programmes actifs sur votre machine Windows.

```
$SNMP = New-Object -ComObject olePrn.OleSNMP  
$SNMP.open('127.0.0.1';'heig';2,1000)
```

Le script qui suit va afficher dans une grid view tous les processus qui tournent sur la machine windows et leur memory usage:

```
while ($true) {  
  
    # Nom du process  
    $SNMPDATA = $SNMP.GetTree("1.3.6.1.2.1.25.4.2.1.2")  
  
    #Memory Usage  
    $SNMPMEM = $SNMP.GetTree("1.3.6.1.2.1.25.5.1.1.2")  
  
    $RESULT = for($i=0;$i-It $SNMPDATA.Length/2;$i++) {  
  
        # Création d'un objet pour enregistrer les 2 données  
        [PSCustomObject]@{  
            "Process Name" = $SNMPDATA[1,$i]  
            "Memory Usage (KB)" = $SNMPMEM[1,$i]  
        }  
    }  
  
    #Afficher le résultat trié par memory usage dans une GridView  
    $RESULT | Select-Object "Process Name", "Memory Usage (KB)" | Sort-Object -Descending "Memory Usage (KB)" | Out-  
    GridView -Title "SNMP Processes" -Wait  
  
    # Attendre 5 minutes avant de fetch à nouveau les OID  
    Start-Sleep -Seconds 300  
}  
  
$SNMP.Close()
```

Commentaire :

QUESTION 16

Terminé

Note de 1,00 sur 1,00

Donnez la liste des fichiers MIBs que vous avez chargé et expliquez comment vous avez déterminé ce choix.

- 1) D'abord j'ai essayé de trouver le modèle CSR1000v sur [ce repository](#), ce qui n'a rien donné.
- 2) Ensuite j'ai parcouru le forum de cisco pour tomber sur [celui-ci](#), qui fournit le lien vers [cette page](#).
- 3) Ensuite, j'ai téléchargé le contenu du MIB "CISCO-FLASH-MIB"
- 4) Dans SNMPb j'ai vérifié la syntaxe et me suis rendu compte que j'avais deux dépendance, donc besoin de 2 autres fichiers: CISCO-SMI et CISCO-QOS-PIB-MIB.

Commentaire :

CISCO-QOS-PIB-MIB: je ne suis pas certain

QUESTION 17

Terminé

Note de 1,00 sur 1,00

Montrez, via une requête SNMPb, le nom des 10 premiers fichiers stockés sur la mémoire flash de votre routeur Cisco.

J'ai modifié mon script powershell pour l'afficher de manière propre:

```
$SNMP = New-Object -ComObject olePrn.OleSNMP
$SNMP.open('192.168.81.131;ciscoRO;2,1000')

$SNMPDATA = $SNMP.GetTree("1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5")
$RESULT=@()
for($i=0;$i-lt 10;$i++){
    RESULT+=[pscustomobject]@{
        "SNMP ID"=$SNMPDATA[0,$i];
        "File name"=$SNMPDATA[1,$i];
        "OID"=($snmp_OIDFromString(($SNMPDATA[0,$i])) -join "") }
}
$RESULT | out-gridView
$SNMP.Close()
```

Et le résultat:

SNMP ID	File name	OID
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.2	/bootflash/	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.2
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.11	/bootflash/lost+found	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.11
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.12	/bootflash/csr1000v-mono-universalk9.17.03.02.SPA.pkg	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.12
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.13	/bootflash/csr1000v-rboot.17.03.02.SPA.pkg	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.13
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.14	/bootflash/packages.conf	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.14
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.15	/bootflash/mode_event_log	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.15
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.16	/bootflash/ios_core.p7b	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.16
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.17	/bootflash/trustidrootx3_ca.ca	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.17
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.18	/bootflash/throughput_monitor_params	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.18
.iso.org.dod.internet.private.enterprises.9.9.10.1.1.4.2.1.1.5.1.1.19	/bootflash/cvac.log	1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5.1.1.19

Ce qui correspond bien à ce que j'obtiens avec snmpb:

The screenshot shows the SnmpB application interface. On the left, the MIB Tree pane displays the structure of the CISCO-FLASH-MIB, specifically the ciscoFlashFiles table. The right pane, titled 'Query Results', shows the output of an SNMP query. The results list 10 file names from the bootflash partition, each associated with its corresponding OID. The 'Node Info' pane at the bottom provides detailed information about the OID selected in the tree.

OID	Description
1.3.6.1.4.1.9.9.10.1.1.4.2.1.1.5	Flash file name as specified by the user copying in the file. The name should not include the colon (:) character as it is a special separator character used to delineate the device name, partition name, and the file name.

Commentaire :

Bien, bonne démarche

QUESTION 18

Terminé

Note de 1,00 sur 1,00

Montrez la configuration de votre router afin qu'il n'accepte plus que des requêtes SNMPv3 en mode authentifié et chiffré.

D'abord, j'ai supprimé la configuration SNMP v2 faite précédemment.

```
no snmp-server community ciscoRO RO 10
no snmp-server community ciscoRW RW 10
no snmp-server host 192.168.81.130 version 2c ciscoRO
```

Ensuite, il faut configurer le SNMP v3:

```
snmp-server group group1 v3 priv
snmp-server user user1 group1 v3 auth sha password1 priv aes 128 password2
snmp-server host 192.168.81.130 version 3 priv user3
```

Commentaire :

Dernière commande pas nécessaire dans le cadre de cet exercice.

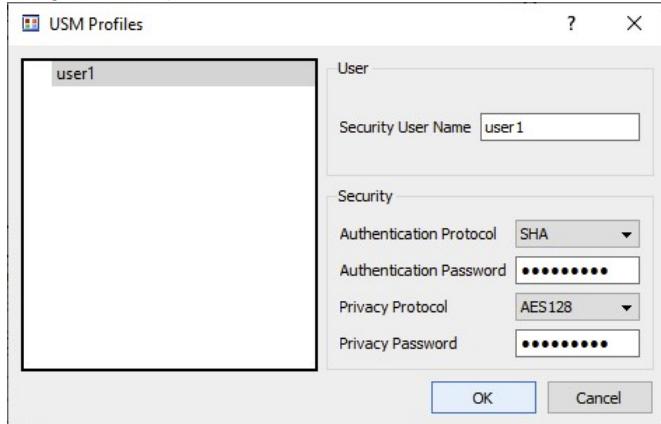
QUESTION 19

Terminé

Note de 0,50 sur 1,00

Montrez la configuration en mode SNMPv3 de votre application SNMPb et montrer le résultat d'une requête sur la valeur SysUpTime (MIB-2) en SNMPv3.

Configuration du profil user1:



Requête sysUpTime:

The application interface includes:

- MIB Tree:** Shows the hierarchy: dod > internet > directory > mgmt > mib-2 > system > sysUpTime (which is selected).
- Node Info:** Details for sysUpTime:

Name:	sysUpTime
Oid:	1.3.6.1.2.1.1.3
Composed Type:	TimeTicks
Base Type:	UNSIGNED32
Status:	current
Access:	read-only
Kind:	Scalar
SMI Type:	OBJECT-TYPE
Size:	0 .. 4294967295
Module:	SNMPv2-MIB
Description:	The time (in hundredths of a second) since the network management portion of the system was last re-initialized.
- Query Results:** Displays the output of the SNMP query:

```
----SNMP query started----  
1: sysUpTime.0 3:55:28.79  
----SNMP query finished----  
Total # of Requests = 1  
Total # of Objects = 1
```

Commentaire :

Avez-vous défini le mode **authPriv** ?

QUESTION 20

Terminé

Note de 1,00 sur 1,00

Capturez/analysez les messages lors d'une requête SNMP v3.

Capture d'une requête sur sysDescr:

The screenshot shows a Wireshark capture window titled "VMware Network Adapter VMnet8". It displays two SNMPv3 requests. The first request (packet 1) has a timestamp of 0.000000, source 192.168.81.130, destination 192.168.81.131, protocol SNMP, and length 168. The second request (packet 2) has a timestamp of 0.000947, source 192.168.81.131, destination 192.168.81.130, protocol SNMP, and length 436. Both requests are encrypted PDUs with private keys and unknown MAC addresses. The details pane shows the SNMPv3 message structure, including msgVersion (snmpv3), msgGlobalData (msgID: 1441820, msgMaxSize: 4096, msgFlags: 07), msgAuthoritativeEngineID (80000009030000505622b177), msgAuthParameters (9e2d75d1f0f338d925060696), and msgData (encryptedPDU). The bytes pane shows the raw hex and ASCII data of the messages.

Explications:

- msgVersion: snmpv3 (3) - indique SNMP version 3 utilisé
- msgGlobalData:
 - msgID: 1441820 - Spécifie l'identifiant du message, qui est unique pour chaque message envoyé par le gestionnaire SNMP.
 - msgMaxSize: 4096 - Spécifie la taille maximale des messages pouvant être envoyés par le gestionnaire SNMP.
 - msgFlags: 07 - Spécifie les flags de traitement des messages. Dans ce cas :
 - Reportable: Set - Indique que le gestionnaire SNMP s'attend à recevoir un PDU de rapport en réponse à ce message.
 - Encrypted: Set - Indique que le message est chiffré.
 - Authenticated: Set - Indique que le message est authentifié.
 - msgSecurityModel: USM (3) - Spécifie le modèle de sécurité utilisé, à savoir le modèle de sécurité basé sur l'utilisateur (USM).
- msgAuthoritativeEngineID: 80000009030000505622b177 - Spécifie l'ID du moteur SNMP qui fait autorité et qui identifie de manière unique l'entité SNMP qui a généré le message.
 - Engine ID Conformance: RFC3411 (SNMPv3) - Indique que l'identifiant du moteur est conforme à la norme RFC3411.
 - Engine Enterprise ID: ciscoSystems (9) - Spécifie l'identifiant d'entreprise de l'organisation qui a fabriqué l'entité SNMP.
 - Engine ID Format: MAC address (3) - Indique que le format de l'ID du moteur est une adresse MAC.
 - Engine ID Data: Cisco type: Agent (0x00) - Spécifie que l'entité SNMP est un agent.
 - Engine ID Data: MAC address: VMware_22:b1:77 (00:50:56:22:b1:77) - Spécifie l'adresse MAC de l'entité SNMP.
- msgAuthoritativeEngineBoots: 16 - Spécifie le nombre de fois où l'entité SNMP a redémarré.
- msgAuthoritativeEngineTime: 3140 - Spécifie le temps (en centièmes de seconde) écoulé depuis le dernier redémarrage de l'entité SNMP.
- msgUserName: user1 - Spécifie le nom de l'utilisateur qui a généré le message.
- msgAuthenticationParameters: 9e2d75d1f0f338d925060696 - Spécifie les paramètres d'authentification qui ont été utilisés pour authentifier le message.
- msgPrivacyParameters: 000090590000cf08 - Spécifie les paramètres utilisés pour chiffrer le message.
- msgData: encryptedPDU (1) - Spécifie le type de message envoyé, qui est un PDU chiffré.
 - encryptedPDU: a981044824417c0c6f560d74036132e801e296d24f2f011650039b726da9c3d3e69350dd... - Spécifie le PDU chiffré qui contient le message SNMP envoyé.

Commentaire :
Bien détaillé

QUESTION 21

Terminé

Note de 1,00 sur 1,00

Quelle(s) bonne(s) pratique(s) supplémentaires suggérez-vous pour sécuriser votre trafic SNMP v3 ?

- 1 . Utiliser un management out-of-band
- 2 . Utiliser des mots de passe forts pour les utilisateurs SNMP afin d'empêcher tout accès non autorisé aux appareils du réseau.
- 3 . Configurer le routeur pour n'autoriser l'accès SNMP qu'à partir d'adresses IP spécifiques.
- 4 . Utiliser les vues SNMPv3 pour restreindre l'accès aux seuls objets SNMP nécessaires.
- 5 . Désactiver SNMPv1 et SNMPv2c.
- 6 . Configurer les traps en SNMPv3
- 7 . Surveiller le trafic SNMP pour détecter toute activité inhabituelle ou suspecte (accès non autorisé ou dump de données)

Commentaire :

QUESTION 22

Terminé

Note de 1,00 sur 1,00

A l'aide de WMI explorer, retrouver les caractéristiques du processeur de votre VM Windows ainsi que le SID de l'utilisateur grs.

Montrez le résultat avec des captures d'écran.

Voici les captures d'écran:

CPU:

The screenshot shows the WMI Explorer interface with the 'CPU' class selected. The left pane displays a list of WMI classes, and the right pane shows the properties of a specific instance of the Win32_Processor class. The properties listed include DeviceID (CPU0), AddressWidth (64), Architecture (9), AssetTag, Availability (3), Caption (Intel® Core™ i7-10510U CPU @ 1.80GHz), Characteristics (44), CpuStatus (1), CreationClassName (Win32_Processor), CurrentClockSpeed (2304), CurrentVoltage (33), DataWidth (64), Description (Intel® Family 6 Model 142 Stepping 12), Family (2), L2CacheSize (256), L3CacheSize (8192), L3CacheSpeed (0), Level (6), LoadPercentage (2), Manufacturer (GenuineIntel), MaxClockSpeed (2304), Name (Intel® Core™ i7-10510U CPU @ 1.80GHz), NumberOfCores (4), NumberOfEnabledCore (4), NumberOfLogicalProcessors (4), PartNumber, PowerManagementSupported (False), and ProcessorId.

SID:

The screenshot shows the WMI Explorer interface with the 'UserAccount' class selected. The right pane displays the properties of a specific instance of the Win32_UserAccount class. The properties listed include Domain (WIN10-GRS-A), Name (GRS), AccountType (512), Caption (WIN10-GRS-A\GRS), Description, Disabled (False), FullName, LocalAccount (True), Lockout (False), PasswordChangeable (True), PasswordExpires (False), PasswordRequired (False), SID (S-1-5-21-4086308193-3046644888-1671887176-1001), SIDType (1), and Status (OK).

Commentaire :

QUESTION 23

Terminé

Note de 1,00 sur 1,00

Ecrivez un script PowerShell permettant de lister, à l'aide de WMI, les partitions de la VM Windows avec leur lettre de lecteur et de retourner le pourcentage d'espace vide.

En cas d'espace insuffisant, une alarme Syslog est générée et récupérée sur votre serveur Syslog

Montrez votre script

Voici le script:

```
Import-Module Posh-SYSLOG
$threshold = 20

# Get partitions with WMI. The filter is used to only get partitions with a DriveType of 3 (local disks)
$partitions = Get-WmiObject -Class Win32_LogicalDisk -Filter "DriveType=3" | Select-Object DeviceID, FreeSpace, Size

# Loop through partitions
foreach ($partition in $partitions) {
    $freeSpaceGB = [Math]::Round($partition.FreeSpace / 1GB, 2)
    $partitionSizeGB = [Math]::Round($partition.Size / 1GB, 2)

    # Free space percentage
    $freeSpacePercent = 0
    if ($partitionSizeGB -gt 0) {
        $freeSpacePercent = [Math]::Round(($freeSpaceGB / $partitionSizeGB) * 100, 2)
    }

    # Output partition details
    Write-Host "Drive $($partition.DeviceID) Free Space: $($freeSpaceGB) GB Size: $($partitionSizeGB) GB
    $($freeSpacePercent)% free space."

    # Generate Syslog alarm if free space % is < threshold
    if ($freeSpacePercent -lt $threshold) {
        $syslogMessage = "Partition $($partition.DeviceID) has less than $threshold% free space."
        Write-Host "Generating Syslog alarm: $syslogMessage"

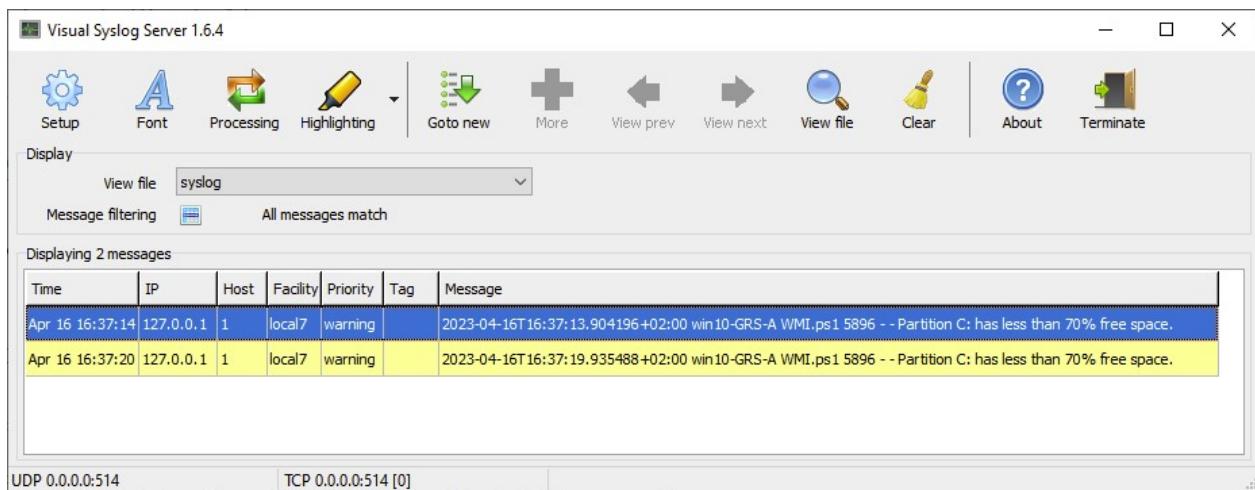
        # Send Syslog message to server
        $sysLogParams = @{
            Server = "127.0.0.1"
            Port = 514
            Facility = 23
            Severity = 4
            Message = $syslogMessage
        }
        Send-SyslogMessage @sysLogParams
    }
}
```

Comme j'ai plus de 20% d'espace libre, j'ai baissé la valeur du threshold pour tester l'envoi de l'alarme syslog:

Output powershell:

```
PS C:\Users\labo\Desktop> C:\Users\labo\Desktop\WMI.ps1
Drive C: Free Space: 33.64 GB Size: 49.4 GB 68.1% free space.
Generating Syslog alarm: Partition C: has less than 70% free space.
```

Syslog server:



Commentaire :

QUESTION 24

Terminé

Note de 1,00 sur 1,00

Ecrivez un script PowerShell permettant de lister, à l'aide de WMI, les partitions de la VM Windows avec leur lettre de lecteur et de retourner le pourcentage d'espace vide.

En cas d'espace insuffisant, une alarme Syslog est générée et récupérée sur votre serveur Syslog

Montrez le résultat (valeurs obtenues et message Syslog reçu)

J'ai tout mis dans la question précédente

Commentaire :

Merci de répondre dans les bonnes rubriques, sinon la correction devient compliquée.

◀ LABO 2 - SNMP-WMI

Aller à...

LABO 3 - YAML NETCONF/RESTCONF ►