

Gestion des réseaux et sécurité opérationnelle (GRS)

Syslog

Professeur : Alain Bron

Assistant :

Version : 2.1

Objectifs

1. Configurer un serveur et des clients Syslog
2. Configurer Syslog sur des composants du réseau
3. Rediriger les événements Windows sur un serveur Syslog

Délai

La date de remise (via le formulaire cyberlearn) sera définie en classe.

Introduction

Dans ce laboratoire, vous allez utiliser un premier protocole standard utilisé dans la gestion des réseaux, Syslog, supporté par la plupart des équipements (réseau, imprimantes, ordinateurs sous Windows ou Linux) et permettant à chaque client/agent d'envoyer ses logs sur un serveur central. Ce protocole est utilisé dans la gestion des systèmes informatiques, pour des audits de sécurité, ainsi que pour l'analyse et le dépannage dans un cadre plus général.

Notation

Notation sur 15 points (note finale = 1.0 + nb de point /3)

Infrastructure

L'infrastructure virtuelle utilisée est celle mise en place au labo 0.

Les programmes `SyslogGenerator.exe` et `visualsyslog_setup.exe` sont disponibles sur la VM Windows 10.

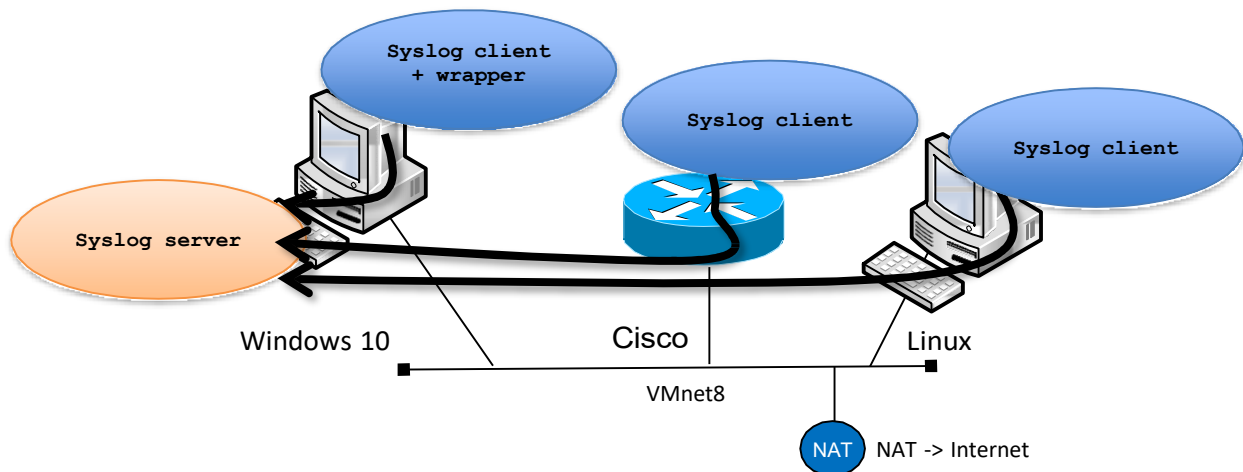
`rsyslog` est installé sur le noeud Linux.

Son fichier de configuration principal est `/etc/rsyslog.conf` et les fichiers liés se trouvent dans le répertoire `/etc/rsyslog.d/`

Gestion manuelle du daemon : `sudo systemctl start|stop|restart|status rsyslog`

La nœud Windows 10 opère en tant que serveur de collecte Syslog.

Les nœuds Windows 10, Linux et Cisco seront configurés pour transmettre des événements au serveur Syslog.

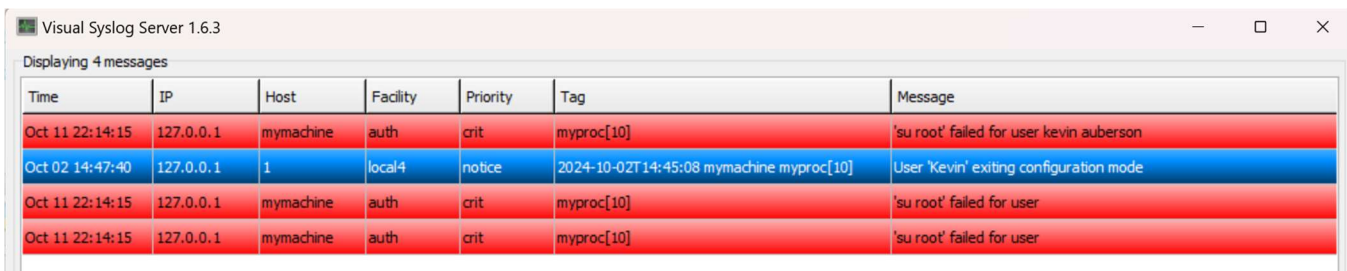


1 Configurer un serveur Syslog

Sur le nœud **PC Windows 10**.

- Démarrez le serveur `Visual Syslog Server`.
- Lancez `SyslogGenerator`. A l'aide de cet outil vous pouvez tester que votre serveur Syslog reçoit bien les messages générés localement. Faites quelques tests avec différents types de message et notamment un message contenant votre nom.

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



The screenshot shows the 'Visual Syslog Server 1.6.3' application window. It displays a table of received messages. The table has columns for Time, IP, Host, Facility, Priority, Tag, and Message. There are four messages listed, with three showing failed login attempts and one showing a configuration mode exit.

Time	IP	Host	Facility	Priority	Tag	Message
Oct 11 22:14:15	127.0.0.1	mymachine	auth	crit	myproc[10]	'su root' failed for user kevin auberson
Oct 02 14:47:40	127.0.0.1	1	local4	notice	2024-10-02T14:45:08 mymachine myproc[10]	User 'Kevin' exiting configuration mode
Oct 11 22:14:15	127.0.0.1	mymachine	auth	crit	myproc[10]	'su root' failed for user
Oct 11 22:14:15	127.0.0.1	mymachine	auth	crit	myproc[10]	'su root' failed for user

2 Configurer un client Linux

Sur le nœud **Linux**.

- Configurer Syslog (`rsyslog`), en modifiant le fichier de configuration qui se trouve dans le répertoire `/etc/rsyslog.conf/` pour qu'il redirige les logs sur le serveur situé sur le PC Windows 10 (Port UDP 514).

2. Montrez votre fichier de configuration (les commandes importantes)

```
#
# Redirect all log on windows syslog server
#
*. * @192.168.81.1
```

Une fois cette ligne ajoutée dans le fichier « `rsyslog.conf` ».
Il faut redémarrer le service avec la commande : « `sudo restart systemctl rsyslog` »

- Générez des messages depuis la VM Linux (`reboot`, `sudo` et en utilisant la commande `logger`) et capturez simultanément le trafic Syslog à l'aide de Wireshark.

3. Montrez les messages reçus sur la console du serveur Syslog distant (Windows 10).
4. Donnez plusieurs exemples de messages qui vous semblent utiles dans la gestion des réseaux.
5. Que pouvez-vous dire sur la sécurité des échanges de messages Syslog ?
6. Présentez et expliquez la capture Wireshark d'un message Syslog.
7. 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`

3. Logger

Oct 2 13:37:14	192.168.81.128	grs-srv	user	notice	grs	Message test VM LINUX
----------------	----------------	---------	------	--------	-----	-----------------------

Reboot

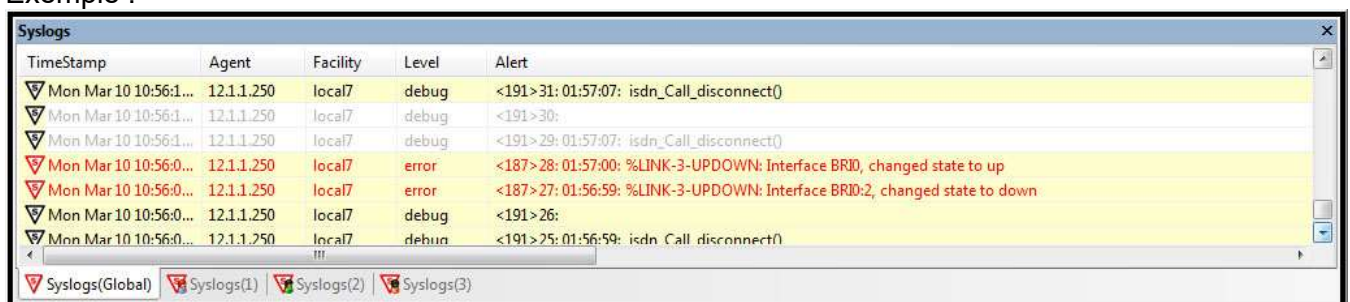
Oct 2 13:37:33	192.168.81.128	grs-srv	auth	notice	systemd-logind[886]	System is rebooting.
----------------	----------------	---------	------	--------	---------------------	----------------------

Sudo

Oct 2 13:43:41	192.168.81.128	grs-srv	authpriv	info	sudo	pam_unix(sudo:session): session opened for user root(uid=0) by grs(uid=1000)
----------------	----------------	---------	----------	------	------	--

4. Les messages relatifs à l'état des interfaces réseau qui permettent de surveiller les connexions, et les journaux de pare-feu, qui aident à identifier les tentatives de connexion et les attaques potentielles. Il y a aussi d'autres types de messages liés aux protocoles de routage, aux tentatives d'authentification, et aux alertes matérielles comme les surchauffes ou les défaillances.

Exemple :



TimeStamp	Agent	Facility	Level	Alert
Mon Mar 10 10:56:1...	12.1.1.250	local7	debug	<191>31:01:57:07: isdn_Call_disconnect()
Mon Mar 10 10:56:1...	12.1.1.250	local7	debug	<191>30:
Mon Mar 10 10:56:1...	12.1.1.250	local7	debug	<191>29:01:57:07: isdn_Call_disconnect()
Mon Mar 10 10:56:0...	12.1.1.250	local7	error	<187>28:01:57:00: %LINK-3-UPDOWN: Interface BR10, changed state to up
Mon Mar 10 10:56:0...	12.1.1.250	local7	error	<187>27:01:56:59: %LINK-3-UPDOWN: Interface BR10/2, changed state to down
Mon Mar 10 10:56:0...	12.1.1.250	local7	debug	<191>26:
Mon Mar 10 10:56:0...	12.1.1.250	local7	debug	<191>25:01:56:59: isdn_Call_disconnect()

https://www.loriotpro.com/Products/On-line_Documentation_V5/images/I9-D4_img/acksyslog.jpg

5. Les messages Syslog ne sont pas chiffrés et surtout pas authentifiés. Le RFC 5224 permet l'utilisation de TCP + TLS/SSL. Un attaquant pourrait envoyer de faux messages de pannes ou d'événements.

6.

51 419.308087	192.168.81.128	192.168.81.1	Syslog	142 DAEMON.INFO: Oct 2 14:08:41 grs-srv systemd[1]: Starting Ubuntu Adv...
<pre>> Frame 51: 142 bytes on wire (1136 bits), 142 bytes captured (1136 bits) on interface \Device\NPF_{6:0000 00 50 56 c0 00 08 00 0c 29 c8 68 65 08 00 45 00} > Ethernet II, Src: VMware_c8:68:65 (00:0c:29:c8:68:65), Dst: VMware_c0:00:08 (00:50:56:c0:00:08) > Internet Protocol Version 4, Src: 192.168.81.128, Dst: 192.168.81.1 > User Datagram Protocol, Src Port: 34404, Dst Port: 514 > Syslog message: DAEMON.INFO: Oct 2 14:08:41 grs-srv systemd[1]: Starting Ubuntu Advantage Timer for running repeated jobs... 0001 1... = Facility: DAEMON - system daemons (3) 110 = Level: INFO - informational (6) Message: Oct 2 14:08:41 grs-srv systemd[1]: Starting Ubuntu Advantage Timer for running repeated jobs... Syslog timestamp (RFC3164): Oct 2 14:08:41 Syslog hostname: grs-srv Syslog process id: systemd Syslog message id: [1]: Starting Ubuntu Advantage Timer for running repeated jobs...</pre>				

Toutes les informations du message sont en claires. On y retrouve toute la structure :Facility, Level, Timestamp, hostname, process id, message id.

7.

Dans le fichier `/etc/rsyslog.conf`, il faut ajouter cette ligne de code :

```
#
# Redirect log from sudo into /var/log/sudo.log
#
if $programname == 'sudo' then /var/log/sudo.log
```

Puis enregistrer le fichier et redémarrer le service rsyslog avec la commande « `sudo systemctl restart rsyslog` »

```
grs@grs-srv:~$ cat /var/log/sudo.log
Oct 2 14:22:32 grs-srv sudo: pam_unix(sudo:session): session closed for user root
Oct 2 14:24:49 grs-srv sudo: grs : TTY=tty1 ; PWD=/home/grs ; USER=root ; COMMAND=/usr/bin/systemctl restart rsyslog
Oct 2 14:24:49 grs-srv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by grs(uid=1000)
Oct 2 14:24:49 grs-srv sudo: pam_unix(sudo:session): session closed for user root
Oct 2 14:25:13 grs-srv sudo: grs : TTY=tty1 ; PWD=/home/grs ; USER=root ; COMMAND=/usr/bin/nano /var/log/sudo.log
Oct 2 14:25:13 grs-srv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by grs(uid=1000)
Oct 2 14:25:16 grs-srv sudo: pam_unix(sudo:session): session closed for user root
Oct 11 13:25:19 grs-srv sudo: grs : TTY=tty1 ; PWD=/home/grs ; USER=root ; COMMAND=/usr/bin/systemctl status rsyslog
Oct 11 13:25:19 grs-srv sudo: pam_unix(sudo:session): session opened for user root(uid=0) by grs(uid=1000)
Oct 11 13:25:24 grs-srv sudo: pam_unix(sudo:session): session closed for user root
```

3 Configurer Syslog sur un équipement réseau

Sur le nœud [Cisco](#).

- Configurez votre routeur de manière à récupérer les messages de niveau Debug, en tant que Local_3, sur votre serveur Syslog.

8. Montrer les commandes IOS que vous avez utilisé.

```
enable
conf t
logging on
logging 192.168.81.1
logging trap debugging
logging facility local3
```

- Configurer votre routeur afin qu'il soit possible d'assurer une corrélation précise (précision à la milliseconde) des événements reçus par le serveur Syslog, en utilisant le protocole NTP.

9. Montrer les commandes IOS que vous avez utilisé.

```
GRS_rtr#conf t
Enter configuration commands, one per line. End with CNTL/Z.
GRS_rtr(config)#ntp server ch.pool.ntp.org
GRS_rtr(config)#service timestamps log datetime msec localtime
GRS_rtr(config)#_
```

- Configurez votre routeur Cisco de manière à récupérer un message contenant la commande utilisée, lors d'une modification de la configuration. Par hypothèse, les logs sont maintenant fixés au niveau Warning et plus Debug.

10. Montrer les commandes IOS que vous avez utilisé.

11. Montrer les messages reçus.

10.

```
enable
conf t
archive
log config
logging enable
notify syslog
hidekeys
```

11.

Oct 11 15:52:53	192.168.81.10		local3	warning	92	*Oct 11 15:52:51.664: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tft
Oct 11 15:52:59	192.168.81.10		local3	notice	93	*Oct 11 15:52:57.261: %SYS-5-CONFIG_I: Configured from console by console
Oct 11 15:53:31	192.168.81.10		local3	warning	94	*Oct 11 15:53:29.667: %SYS-4-CONFIG_RESOLVE_FAILURE: System config parse from (tft

4 Rediriger les événements Windows sur un serveur Syslog

Sur le nœud Windows 10.

- A l'aide de la commande `logger.exe`, envoyez un message à votre serveur Syslog.

12. Montrez la commande et le message reçu sur le serveur Syslog

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

Log reçu :

Displaying 2 messages						
Time	IP	Host	Facility	Priority	Tag	Message
Oct 16 15:55:53	127.0.0.1	ACER-KEVIN	local3	info		test

- Générez un message Syslog à l'aide de la cmdlet `Send-SyslogMessage` (module `Posh-SYSLOG`) en mode RFC 3164 et 5424 et comparez les messages

13. Montrez la commande utilisée et les messages reçus par le serveur Syslog

Commande :

- `Send-SyslogMessage -Server localhost -Severity 4 -Facility 16 -Message "test message"`
- `Send-SyslogMessage -Server localhost -Severity 4 -Facility 16 -Message "test message" -RFC3164`

Log reçu:

Oct 16 16:17:05	127.0.0.1	1	local0	warning		2024-10-16T16:17:05.263651+02:00 ACER-KEVIN PowerShell 15252 - - test message
Oct 16 16:17:34	127.0.0.1	ACER-KEVIN	local0	warning		PowerShell test message

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

14. Montrez le contenu du script et le message reçu par le serveur Syslog

```
$processName = "cmd.exe" # Nom du processus à surveiller
$syslogServer = "192.168.81.1" # Adresse IP du serveur Syslog
$syslogPort = 514 # Port Syslog par défaut (UDP)
$syslogFacility = "local0" # Changez en fonction de vos besoins
$syslogSeverity = "Error" # Niveau de sévérité Syslog

# Boucle infinie pour surveiller le processus
while ($true) {
    # Vérifier si le processus est en cours d'exécution
    $process = Get-Process -Name $processName -ErrorAction SilentlyContinue

    if (-not $process) {
        # Si le processus n'est pas trouvé, envoyer un message Syslog
        $message = "Process $processName is not running on the system."

        Write-Host "[$(Get-Date)] $message" # Pour affichage local (facultatif)

        # Envoyer le message Syslog avec Send-SyslogMessage
        Send-SyslogMessage -Server $syslogServer -Port $syslogPort -Message $message -
        Facility $syslogFacility -Severity $syslogSeverity
    }

    # Attendre 2 minutes avant de revérifier
    Start-Sleep -Seconds 120
}
```

Displaying 2 messages

Time	IP	Host	Facility	Priority	Tag	Message
Oct 17 16:32:07	192.168.81.1	1	local0	err		2024-10-17T16:32:07.067636+02:00 192.168.81.1 MonitorProcess.ps1 9244 - - Process cmd.exe is not running on the system.
Oct 17 16:34:08	192.168.81.1	1	local0	err		2024-10-17T16:34:07.592604+02:00 192.168.81.1 MonitorProcess.ps1 9244 - - Process cmd.exe is not running on the system.

A l'aide de <https://www.solarwinds.com/free-tools/event-log-forwarder-for-windows> ou le cmdlet `Send_syslogMessage`:

- Redirigez, vers le serveur Syslog, l'événement Windows (Observateur d'événements) liés à un échec de login local.

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

J'ai créé ce script powershell, car Forwarder Log Event ne fonctionnait pas.

```
$syslogServer = "192.168.81.1" # Syslog server address
$syslogPort = 514 # Syslog port

# Define the event log query for failed login attempts (Event ID 4625)
$query = @"
<QueryList>
<Query Id="0" Path="Security">
<Select Path="Security">*[System[(EventID=4625)]]</Select>
</Query>
</QueryList>
"@

# Continuously check for new failed logon events
while ($true) {
    # Get the latest failed logon events
    $events = Get-WinEvent -FilterXml $query -MaxEvents 5

    foreach ($event in $events) {
        # Extract event details for the Syslog message
        $logTime = $event.TimeCreated
        $userName = $event.Properties[5].Value # User who failed to log in
        $sourceIp = $event.Properties[18].Value # Source IP address (if available)
        $logMessage = "Failed logon detected at $logTime User: $userName, Source IP: $sourceIp"

        # Send the failed logon event to the Syslog server
        Send-SyslogMessage -Message $logMessage -Server $syslogServer -Port $syslogPort -
        Facility "Local0" -Severity "Error"
    }

    # Wait for 2 minutes before checking again
    Start-Sleep -Seconds 120
}
```

Message filtering							All messages match	
Displaying 6116 messages								
Time	IP	Host	Facility	Priority	Tag	Message		
Oct 17 17:21:07	192.168.81.1	1	local0	err		2024-10-17		
Oct 17 17:21:07	192.168.81.1	1	local0	err		2024-10-17		
Oct 17 17:21:07	192.168.81.1	1	local0	err		2024-10-17		
Oct 17 17:21:07	192.168.81.1	1	local0	err		2024-10-17		
Oct 17 17:21:08	192.168.81.1	1	local0	err		2024-10-17		
Oct 17 17:23:08	192.168.81.1	1	local0	err		2024-10-17		
Oct 17 17:23:08	192.168.81.1	1	local0	err		2024-10-17		
Oct 17 17:23:09	192.168.81.1	1	local0	err		2024-10-17 17:23:09.202327+02:00 192.168.81.1 CheckLogin.ps1 12608 -- Failed logon detected at 10/17/2024 16:3		
Oct 17 17:23:09	192.168.81.1	1	local0	err		2024-10-17 17:23:08.941780+02:00 192.168.81.1 CheckLogin.ps1 12608 -- Failed logon detected at 10/17/2024 16:3		
Oct 17 17:23:09	192.168.81.1	1	local0	err		2024-10-17 17:23:09.202327+02:00 192.168.81.1 CheckLogin.ps1 12608 -- Failed logon detected at 10/14/2024 16:2		

Message content

Time: Oct 17 17:23:09
 IP: 192.168.81.1
 Host: 1
 Facility: local0
 Priority: err
 Tag:
 Message: 2024-10-17 17:23:09.202327+02:00 192.168.81.1 CheckLogin.ps1 12608 -- Failed logon detected at 10/17/2024 16:3
 Failed logon detected at 10/14/2024 16:23:18 User: -, Source IP: C:\Windows\System32\svchost.exe

OK

5 Utilisation de Sysmon

Sur le nœud **Windows 10**.

- Installez l'extension `sysmon` (*Microsoft Sysinternals*) et configurez-le, via un fichier XML, de manière que les connexions vers le port 80 et les requêtes DNS sur le site `lematin.ch` soient journalisée et visible dans l'Observateur d'événements.

16. Montrez le contenu de votre fichier XML.

17. Montrez le message reçu.

16.

```
<Sysmon schemaversion="4.50">
  <EventFiltering>
    <!-- Log process creation -->
    <ProcessCreate onmatch="include">
      <CommandLine condition="contains">lematin.ch</CommandLine>
    </ProcessCreate>

    <!-- Log TCP connections -->
    <NetworkConnect onmatch="include">
      <DestinationPort condition="is">80</DestinationPort>
    </NetworkConnect>

    <!-- Log DNS queries -->
    <DnsQuery onmatch="include">
      <QueryName condition="contains">lematin.ch</QueryName>
    </DnsQuery>
  </EventFiltering>
</Sysmon>
```

17.

Network connection detected:

```
RuleName: -
UtcTime: 2024-10-17 17:22:08.509
ProcessGuid: {e3e19251-1db8-6711-a30a-000000007a00}
ProcessId: 14380
Image: C:\Program Files (x86)\Microsoft\Edge\Application\msedge.exe
User: ACER-KEVIN\kevin
Protocol: tcp
Initiated: true
SourceIsIpv6: false
SourceIp: 192.168.1.9
SourceHostname: ACER-KEVIN
SourcePort: 38780
SourcePortName: -
DestinationIsIpv6: false
DestinationIp: 3.165.190.46
DestinationHostname: server-3-165-190-46.zrh55.r.cloudfront.net
DestinationPort: 80
DestinationPortName: http
```

Log Name:	Microsoft-Windows-Sysmon/Operational		
Source:	Sysmon	Logged:	17/10/2024 19:22:09
Event ID:	3	Task Category:	Network connection detected (rule
Level:	Information	Keywords:	
User:	Système	Computer:	ACER-KEVIN
OpCode:	Info		
More Information:	Event Log Online Help		