

Integración con antivirus

ClamAV

Wazuh detecta archivos maliciosos mediante la integración con ClamAV , el cual es un motor antimalware gratuito y de código abierto para detectar varios tipos de malware, incluidos virus y troyanos.

ClamAV es un conjunto de herramientas antimalware de código abierto diseñado para diversos casos de uso, como seguridad de terminales, escaneo web y tiene las siguientes características:

- Ofrece protección en tiempo real para puntos finales de Linux.
- Proporciona actualizaciones automáticas a la base de datos de malware.
- Admite todos los formatos de archivos de correo estándar de forma predeterminada.
- Admite varios formatos de archivo como ZIP y RAR.
- Admite archivos de documentos comunes, como archivos de MS Office y Mac Office, HTML, RTF y PDF.
- Está diseñado con un actualizador de bases de datos avanzado que puede aprovechar actualizaciones programadas o firmas digitales.
- Utiliza un escáner de línea de comandos.
- Tiene soporte integrado para ejecutables ELF y archivos ejecutables portátiles empaquetados con UPX, FSG, Petite, NsPack, wwpack32, MEW, Upack y ofuscados con SUE y otros.

Configuración.

Puede configurar ClamAV y recopilar sus registros desde puntos finales de Linux y Windows. Para recopilar registros de ClamAV de puntos finales de Linux, elimine la etiqueta de comentario `#` antes de la declaración `"LogSyslog true"` en el archivo de configuración. Quitar el comentario a esta declaración reenvía los registros de ClamAV al archivo Syslog `/var/log/syslog`.

Para instalar el entorno de prueba tendremos que ejecutar los siguientes comandos.

```
sudo apt-get update
sudo apt-get install clamav-daemon
sudo chmod 644 /etc/clamav/clamd.conf
sudo chmod 644 /etc/clamav/freshclam.conf
sudo chown clamav:adm /etc/clamav/clamd.conf
```

```
sudo chown clamav:adm /etc/clamav/freshclam.conf
```

```
root@debian12:/etc/clamav# ls -lh
total 20K
-rw-r--r-- 1 root clamav 2,0K abr  1 11:28 clamd.conf
-rw-r--r-- 1 root clamav 682 mar 28 17:08 freshclam.conf
drwxr-xr-x 2 root root  4,0K sep  9 2023 onerrorexecute.d
drwxr-xr-x 2 root root  4,0K sep  9 2023 onupdateexecute.d
drwxr-xr-x 2 root root  4,0K sep  9 2023 virusevent.d
```

Instalación de Rsyslog.

```
sudo apt-get install rsyslog -y
```

Configuración daemon de Clamav.

Modificar los datos en el archivo de configuración.

```
sudo nano /etc/clamav/clamd.conf
```

```
LogSyslog true
#LogFile /var/log/clamav/clamav.log
```

```
sudo nano /etc/clamav/freshclam.conf
```

```
LogVerbose true
LogSyslog true
```

Modificar los siguientes apartados en clamd.conf que es el scanner mediante linea de comandos.

```
sudo nano /usr/local/etc/clamd.conf
```

```
# Comment or remove the line below.
# Example
```

```
sudo nano /usr/local/etc/freshclam.conf
```

```
# Comment or remove the line below.
# Example
UpdateLogFile /var/log/clamav/freshclam.log
```

```
systemctl restart clamav-daemon
systemctl enable clamav-daemon
systemctl restart wazuh-agent
```

```
sudo usermod -aG clamav $USER
sudo usermod -aG adm $USER
sudo chmod 666 /var/run/clamav/clamdctl
```

Comando de prueba para análisis y almacenamiento en syslog:

```
clamscan --stdout --no-summary -i -r /directorio/de/escaneo | logger -t "clamd[5286]"
```

Comando de prueba para respuesta en consola de archivos infectados:

```
clamscan --stdout --no-summary -i -r /home/rchavez/Descargas/Malware
```

Agente de Wazuh.

Si no se lee por defecto se debe añadir el apartado **localfile** que obliga a realizar el registro del directorio **syslog** para que Wazuh agent lo analice cada vez que se realice un escaneo de cualquier directorio.

```
nano /var/ossec/etc/ossec.conf
```

```
<localfile>
  <log_format>syslog</log_format>
  <location>/var/log/syslog</location>
</localfile>
```

```
systemctl restart wazuh-agent
```

Una vez realizados los ajustes podemos observar diferentes tipos de alertas generadas.

Cuando se detiene el servicio de clamAV tenemos:

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 3, 2024 @ 12:16:52.985	017	cgil-rchavez	T1562.001	Defense Evasion	Clamd stopped	6	52510
<div>TableJSONRule</div>							
@timestamp		2024-04-03T16:16:52.985Z					
_id		rne_pl4BZbkDNsF913W-					
agent.id		017					
agent.ip		192.168.24.68					
agent.name		cgil-rchavez					
data.aws.accountid							
data.aws.region							
decoder.name		clamd					
full_log		2024-04-03T12:16:52.447861-04:00 rchavez clamd[861]: --- Stopped at Wed Apr 3 12:16:52 2024					
id		1712161012.41789352					
input.type		log					
location		/var/log/syslog					
manager.name		cgil-wazuh					
predecoder.program_name		clamd					
predecoder.timestamp		2024-04-03T12:16:52.447861-04:00					
rule.description		Clamd stopped					
rule.firedtimes		1					
rule.gpg13		4.14					

Quando se detecta un archivo infectado tenemos:

Time	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Apr 1, 2024 @ 11:27:39.084	017	cgil-rchavez			ClamAV: Virus detected	8	52502
<div>TableJSONRule</div>							
@timestamp		2024-04-01T15:27:39.084Z					
_id		r3VFmo4BZbkDNsF9-vVf					
agent.id		017					
agent.ip		192.168.24.68					
agent.name		cgil-rchavez					
data.aws.accountid							
data.aws.region							
decoder.name		clamd					
decoder.parent		clamd					
full_log		2024-04-01T11:27:37.530796-04:00 rchavez clamd[5286]: /home/rchavez/Descargas/pago.r09: Win.Packed.Msilheracies-10020638-0 FOUND					
id		1711985259.13726231					
input.type		log					
location		/var/log/syslog					
manager.name		cgil-wazuh					
predecoder.program_name		clamd					
predecoder.timestamp		2024-04-01T11:27:37.530796-04:00					
rule.description		ClamAV: Virus detected					
rule.firedtimes		8					

Quando se tiene un error inesperado o mala configuración tenemos:

Time ↓	Agent	Agent name	Technique(s)	Tactic(s)	Description	Level	Rule ID
Mar 27, 2024 @ 11:48:28.008	017	cgli-rchavez			Clamd error	10	52503
Table	JSON	Rule					
@timestamp		2024-03-27T11:48:28.008Z					
_id		3nS2gi4BZbkDNsF9PpIP					
agent.id		017					
agent.ip		192.168.24.68					
agent.name		cgli-rchavez					
data.aws.accountid							
data.aws.region							
decoder.name		clamd					
full_log		2024-03-27T11:48:27.673102-04:00 rchavez clamd[18730]: ERROR: Can't open/parse the config file /etc/clamav/clamd.conf					
id		1711554508.64071554					
input.type		log					
location		/var/log/syslog					
manager.name		cgli-wazuh					
predecoder.program_name		clamd					
predecoder.timestamp		2024-03-27T11:48:27.673102-04:00					
rule.description		Clamd error					
rule.firedtimes		2					

Actualización automática de freshclam.

Configuración de cantidad de veces al día que se actualiza clamav-freshclam de forma automática modificando el archivo de configuración. Por defecto se establece en 24 pero dependiendo de la cantidad de recursos del equipo esta puede modificarse.

```
sudo nano /etc/clamav/freshclam.conf
```

```
#Para una actualización de 6 veces al dia.  
Checks 6
```

```
sudo systemctl restart clamav-freshclam
```

Actualización manual de freshclam.

Configuración manual para actualizar clamav-freshclam realizando los siguientes comandos:

```
sudo systemctl stop clamav-freshclam.service  
sudo freshclam  
sudo systemctl restart clamav-freshclam.service
```

Programación regular análisis con clamscan.

Para realizar un análisis periódico y que los archivos analizados por clamscan y visualizados en wazuh se puede programar un crontab en terminales linux de la siguiente manera.

Accedemos como usuario con privilegios debido a que la detención de programas y posterior "*restart*" utilizan permisos root.

```
sudo su
crontab -e
```

Dentro de crontab utilizamos horarios en los que los equipos no tengan una utilización demandante.

```
10 12 * * * sudo systemctl stop clamav-freshclam.service
11 12 * * * sudo freshclam
15 12 * * * sudo systemctl restart clamav-freshclam.service
20 12 * * * /usr/local/bin/clamscan --stdout --no-summary -i -r /home/rchavez/Descargas/Malware
2>&1 | logger -t "clamd[ 5286]
```

Utilizamos la ruta completa de *clamscan* para que sea interpretado de manera correcta, obteniendo alerta de actualización con *freshclam* así como también de malware en caso de encontrarse una coincidencia positiva.

Revision #10

Created 9 abril 2024 17:33:27 by Ricardo Alberto

Updated 18 abril 2024 15:19:47 by Ricardo Alberto