Mecanismo de rotación y archivado automático de alertas JSON generadas por Snort 3

Deian Orlando Petrovics

Abril de 2025

1. Introducción

El objetivo de este proceso es habilitar un mecanismo robusto y automatizado que permita la rotación, compresión y archivado de logs en formato JSON generados por Snort 3 en una Raspberry Pi 5. Esta funcionalidad busca mantener el sistema limpio, optimizar el espacio en disco y facilitar la gestión de logs históricos.

2. Creación de carpetas necesarias

Se han creado las siguientes carpetas con sus respectivos permisos para albergar los archivos de alertas, los logs rotados y los archivos comprimidos:

```
sudo mkdir -p /opt/snort/logs/live
sudo mkdir -p /var/log/snort/rotated
sudo mkdir -p /var/log/snort/archived
sudo chown -R snort:snort /opt/snort /var/log/snort
sudo chmod -R 750 /opt/snort /var/log/snort
```

3. Configuración de salida JSON en snort.lua

En el archivo de configuración `snort.lua`, se activa la salida de logs JSON mediante la siguiente sección:

```
alert_json = {
    file = true,
    limit = 50,
    fields = 'timestamp proto dir src_addr src_port dst_addr dst_port
       msg sid gid priority'
}
```

4. Configuración del servicio Snort

El archivo del servicio `/etc/systemd/system/snort.service` se modificó para que Snort escriba sus alertas en formato JSON:

```
[Unit]
Description=Snort NIDS Daemon
After=network.target

[Service]
```

```
ExecStart=/usr/local/snort/bin/snort -q -c /usr/local/snort/etc/snort/
    snort.lua \
  -i enxc8a362b4a702 -A alert_json -l /opt/snort/logs/live
ExecReload=/bin/kill -HUP ${MAINPID}
Restart=always
User=snort
Group=snort
LimitCORE=infinity
LimitNOFILE=65536
LimitNPROC=65536

[Install]
WantedBy=multi-user.target
```

5. Configuración de logrotate

Se creó el archivo `/etc/logrotate.d/snort` con la siguiente configuración para rotar, comprimir y mover los logs a la carpeta correspondiente:

```
/opt/snort/logs/live/alert_json.txt {
    daily
    rotate 30
    compress
    delaycompress
    missingok
    notifempty
    create 640 snort snort
    copytruncate
    postrotate
        [ -d /var/log/snort/rotated ] || mkdir -p /var/log/snort/rotated
        chown snort:snort /var/log/snort/rotated
        mv /opt/snort/logs/live/alert_json.txt.*.gz /var/log/snort/
           rotated/ 2>/dev/null || true
    endscript
}
```

6. Script de archivado automático

Se implementó el script `/usr/local/bin/archive_snort_logs.sh` para empaquetar los archivos rotados en un archivo `.tar.gz` por día:

```
#!/bin/bash
set -e

DATE=$(date +%Y-%m-%d)
ARCHIVE_DIR="/var/log/snort/archived"
mkdir -p "$ARCHIVE_DIR"
ARCHIVE_PATH="$ARCHIVE_DIR/snort_logs_$DATE.tar.gz"
SOURCE="/var/log/snort/rotated/*.gz"

if ls $SOURCE 1> /dev/null 2>&1; then
    tar -czf "$ARCHIVE_PATH" $SOURCE
    rm -f $SOURCE
fi
```

7. Programación del archivado con crontab

Se registró la tarea en `sudo crontab -e` para ejecutarse diariamente a las 1:21 AM:

```
21 1 * * * /usr/local/bin/archive_snort_logs.sh
```

8. Comprobación del funcionamiento

Mediante los siguientes comandos se puede verificar que el sistema está funcionando correctamente:

- Verificar los archivos actuales:

```
sudo ls -lh /opt/snort/logs/live/
sudo ls -lh /var/log/snort/rotated/
sudo ls -lh /var/log/snort/archived/
```

- Forzar la rotación y ejecución del script:

```
sudo logrotate -f /etc/logrotate.d/snort
sudo /usr/local/bin/archive_snort_logs.sh
```

9. Supervisión automática del archivo de alertas

Para evitar que el archivo `alert_json.txt` deje de existir (por ejemplo, tras una eliminación accidental), se ha creado un sistema de vigilancia automática usando `inotifywait`.

9.1 Instalación de inotify-tools

```
sudo apt install inotify-tools
```

9.2 Creación del script de supervisión

Archivo: `/usr/local/bin/watch_snort_log.sh`

```
#!/bin/bash

WATCH_FILE="/opt/snort/logs/live/alert_json.txt"

# Bucle infinito que supervisa el archivo
while true; do
    if ! inotifywait -e delete_self "$WATCH_FILE"; then
        echo "$(date): $WATCH_FILE ha sido eliminado, reiniciando Snort
            ..." >> /var/log/snort/log_monitor.log
        systemctl restart snort
        sleep 5
    fi
done
```

9.3 Permisos de ejecución

```
sudo chmod +x /usr/local/bin/watch_snort_log.sh
```

9.4 Creación del servicio de supervisión

Archivo: `/etc/systemd/system/snort-log-watch.service`

```
[Unit]
Description=Snort Log File Watcher
After=snort.service
Requires=snort.service

[Service]
ExecStart=/usr/local/bin/watch_snort_log.sh
Restart=always
RestartSec=10
User=root

[Install]
WantedBy=multi-user.target
```

9.5 Habilitar y arrancar el servicio

```
sudo systemctl daemon-reload
sudo systemctl enable snort-log-watch.service
sudo systemctl start snort-log-watch.service
```

Conclusión

El sistema está ahora preparado no solo para rotar y archivar alertas de Snort de forma automatizada, sino también para reaccionar en tiempo real ante eventos críticos como la eliminación del archivo principal de alertas. Este mecanismo mejora notablemente la resiliencia y disponibilidad del sistema de detección de intrusos.