

Pasos de instalación y evidencias

Sergio Roselló Morell

Durante la practica, se han realizado una serie de procesos, desde la configuración del entorno awseducate de AWS a la configuración de la normas de firewall de las máquinas dentro de la VPC de AWS. En este documento, se redactan los pasos clave para una correcta **instalación del SOC SecurityOnion de forma distribuida en una VPC de AWS**.

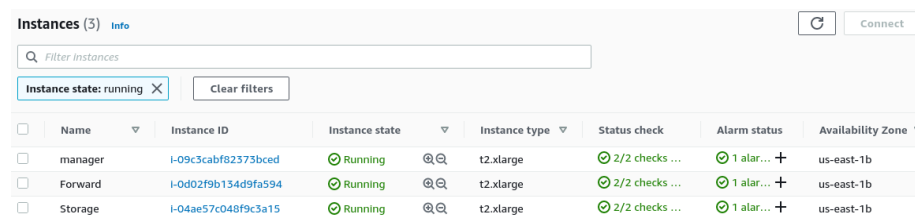
Configuración de la cuenta awseducate de AWS.

Este paso ha consistido en acceder al enlace ofrecido por el equipo docente y aceptar los contratos presentados. Una vez hecho esto, se nos proporcionaba acceso al entorno AWS en el que podíamos crear máquinas EC2 para realizar la práctica.

Creación de las imágenes

Se han elegido las imágenes Ubuntu 18.04 server para realizar la práctica.

Se han creado las tres instancias necesarias para una configuración distribuida de SecurityOnion. Esto implica que todas se han creado en la misma VPC, cumpliendo el primero de los requisitos, que puedan comunicarse entre ellas.



Instances (3) Info								Refresh	Connect
Filter instances									
Instance state: running X Clear filters									
<input type="checkbox"/>	Name ▾	Instance ID	Instance state ▾	Instance type ▾	Status check	Alarm status	Availability Zone ▾		
<input type="checkbox"/>	manager	i-09c3cabf82373bcd	Running	t2.xlarge	2/2 checks ...	1 alarm... +	us-east-1b		
<input type="checkbox"/>	Forward	i-0d02f9b134d9fa594	Running	t2.xlarge	2/2 checks ...	1 alarm... +	us-east-1b		
<input type="checkbox"/>	Storage	i-04ae57c048f9c3a15	Running	t2.xlarge	2/2 checks ...	1 alarm... +	us-east-1b		

Figure 1: Instancias

Puesta a punto de todas las maquinas

El primer paso es asegurar que todo el equipo esté al día, por tanto se ha actualizado el equipo.

```
sudo apt update
sudo apt upgrade
sudo apt autoremove
```

Una vez hecho esto, se procede a cambiar el **hostname** del equipo, simplemente para que sea mas sencillo trabajar durante el proceso de configuración de los nodos. Al nodo **manager**, se le asigna el **hostname manager**. Se añade además,

la línea `127.0.0.1 manager` al archivo `/etc/hosts`. Se hace este proceso por cada máquina, cambiando el `hostname`.

Se cambia la configuración del demonio `ssh` para que permita a las instancias conectarse mediante contraseña entre ellas. Esto es esencial para la configuración de los nodos.

El último paso para tener las máquinas configuradas es descargar el repositorio `git securityonion` en cada nodo.

```
git clone https://github.com/Security-Onion-Solutions/securityoniongit
```

Procedemos a ejecutar el script que nos ofrece el equipo de SecurityOnion llamado `so-setup-network`. Este script nos pregunta una serie de cosas importantes para la configuración, como el tipo de instalación que queremos configurar.

Configuración de los nodos `storage/search` y `forward`

Para estos dos nodos, es necesario añadir una nueva interfaz de red para cada uno de ellos. Esta servirá como interfaz de captura de paquetes y servicios.

Para hacer esto, debemos ir a la sección `network interfaces` dentro del portal AWS y configurar dos nuevas, con direcciones IP dentro de nuestra máscara de red, dentro de nuestra VPC.

Configuración del nodo `manager`

Según las recomendaciones del equipo de SecurityOnion, el primer nodo que se debe crear es el `manager`, para que el resto de nodos (`storage/search` y `forward`) se puedan configurar correctamente. Este paso es necesario porque ambos tipos de nodos deben conectarse al nodo `manager` para descargar la clave secreta que va a permitir que se comuniquen a través de la red por SSH.

Una de las primeras preguntas que se nos hace, es: que tipo de instalación se va a realizar. Para esta, seleccionamos `distributed`.

Más adelante, nos pregunta que servicios pretendemos correr en la máquina, seleccionamos todos los que ofrece (`graphana`, `osquery`, `wazhu`, `thehyve`, `playbook`, `strelka`).

Configuramos el correo y la contraseña del administrador de la red, para iniciar sesión en los portales y le indicamos que queremos que los equipos accedan a la IP del nodo `manager` con su `hostname`. De esta forma, el acceso es mucho más sencillo de recordar, en vez de tener que recordar una dirección IP, ahora podemos acceder al portal SOC mediante la siguiente dirección: `https://manager`.

Una vez acabada la configuración del nodo `manager`, comprobamos que todos los servicios están corriendo bien con `sudo so-status`. El resultado es favorable.

Configuración del nodo storage/search

Una vez configurado el primer nodo (**manager**), procedemos a configurar el siguiente. En nuestro caso, es el nodo **storage**.

Como en el caso anterior, la configuración este nodo es sencilla una vez te has hecho a la idea de la arquitectura de red distribuida y quedan claros los conceptos.

El paso mas importante, es seleccionar la opción que configura la maquina como nodo **search**. Cuando nos pregunte por la interfaz de red para **management**, seleccionamos **eth0** y dejamos **eth1** para **monitor**.

Además, se nos pregunta por la dirección IP del nodo `manager` para poder conectarse a él. Se la proporcionamos, conjuntamente con el `hostname`.

Durante la configuración, nos dice que necesita conectarse al nodo **nanager**, en este momento, se abre una consola y se debe introducir la contraseña añadida en la configuración del nodo **nanager**. Así, queda establecida la comunicación SSH. Esta es la razón por la que se ha tenido que habilitar el inicio de sesión por contraseña en las conexiones SSH.

Al acabar la configuración, nos aseguramos de que todos los servicios están corriendo correctamente:

```
root@kali:~# docker ps --status
Checking Docker status
Docker ..... ( ok )
Checking container statuses
so-curator ..... [ ok ]
so-elasticsearch ..... [ ok ]
so-filesystem ..... [ ok ]
so-ldapauth ..... [ ok ]
so-linea ..... [ ok ]
so-memorial ..... [ ok ]
so-telegraf ..... [ ok ]
so-zeus ..... [ ok ]
```

Figure 4: Storage status

Configuración del nodo forward

La configuración de este nodo y la configuración anterior no difieren en prácticamente nada, excepto el tipo de nodo que se quiere configurar. Para esta opción, seleccionamos **forward**.

Una vez acaba la instalación, revisamos que todos los servicios están corriendo adecuadamente:

```

root@server1:~# sudo ss -tstatus
Checking Docker status
Docker ----- [ OK ]
Checking container statuses
ss -tstatus ----- [ OK ]
ss -engine ----- [ OK ]
ss -engine2 ----- [ OK ]
ss -step ----- [ OK ]
ss -strata-backend ----- [ OK ]
ss -strata-coordinator ----- [ OK ]
ss -strata-filesystem ----- [ OK ]
ss -strata-front ----- [ OK ]
ss -strata-gatekeeper ----- [ OK ]
ss -strata-manager ----- [ OK ]
ss -suprieth ----- [ OK ]
ss -telnet ----- [ OK ]
ss -wazuh ----- [ OK ]
ss -zabbix ----- [ OK ]

```

Figure 5: Forward status

Acceso al portal de configuración del nodo manager

En la configuración del nodo **manager** hemos seleccionado que queríamos acceder al portal web mediante el **hostname** de la máquina.

Ahora que ya está todo configurado y corriendo, debemos acceder al SOC.

El primer paso es permitir el acceso al **VPC AWS** únicamente a la dirección IP de la máquina desde donde queremos acceder. Para hacer esto, debemos ir a las normas del **VPC** y añadir esa política de acceso a las normas de seguridad.

Una vez hecho esto, debemos añadir a nuestro **/etc/hosts** la dirección IP de la máquina y su **hostname**. De esta forma, accediendo a **https://manager** desde nuestra máquina, podemos acceder directamente al SOC de la **VPC** que hemos configurado.

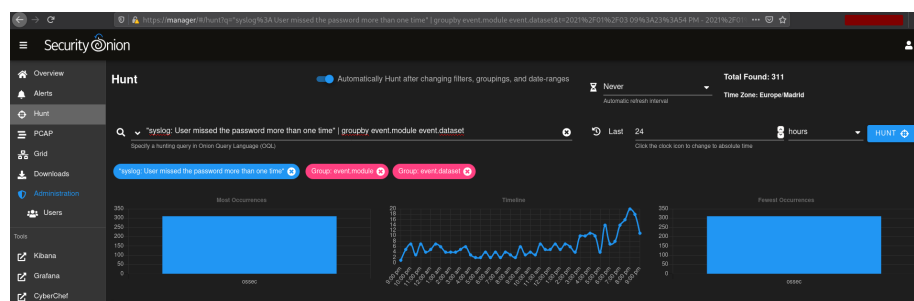


Figure 6: SOC

Desde aquí, ahora tenemos acceso a todos los servicios configurados previamente.

Podemos ver desde fleet nuestras máquinas conectadas y su descripción.

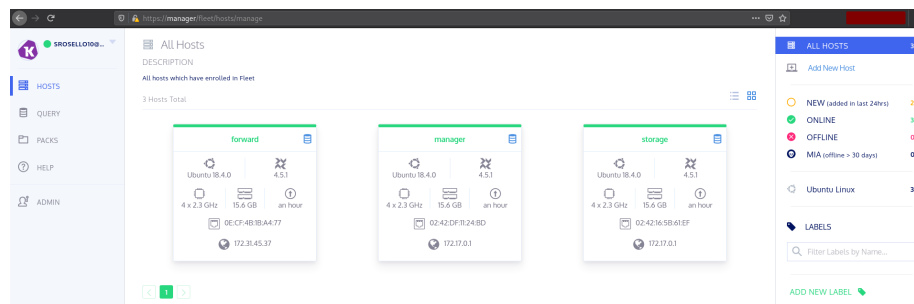


Figure 7: Fleet

Desde aquí, además, podemos ejecutar consultas **osquery** desde el apartado query en el menú lateral izquierdo.

Accediendo desde SecurityOnion, podemos ir directamente a grafana, una plataforma que te da acceso a los recursos del sistema, como se están usando.

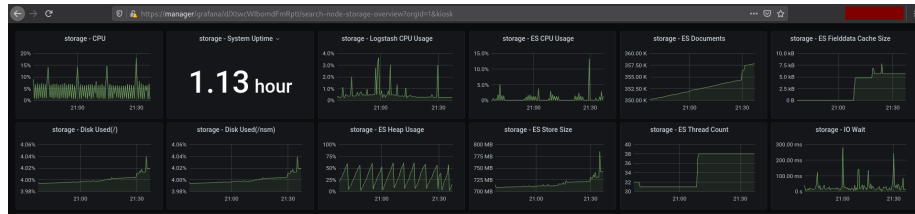


Figure 8: Grafana

Análisis de pcap con so-import-pcap

Una vez montado el SOC, se ha procedido a revisar que todo funcionase correctamente. Una forma de hacer esto, es importar unos pcap. Usando la herramienta proporcionada por SecurityOnion, **so-import-pcap** se han importado y usando Kibana, se ha procedido a revisarlos.



Figure 9: Kibana

Conclusión

Durante la instalación de este SOC distribuido preparado para un entorno de producción, se han aprendido varias técnicas bastante importantes.

Se ha aprendido, sobre todo a revisar los SOC existentes en el mercado, las ventajas que tienen y los posibles inconvenientes.

Una vez decidió el SOC que se quiere usar, su configuración es sencilla, si se siguen los pasos correctamente. Al fin y al cabo, son herramientas bastante comunes y la documentación existente es extensa.

La guía que mas me ha servido, sin duda ha sido la página web oficial de SecurityOnion.

Quedo bastante contento con todo el proceso de aprendizaje. Desde la investigación inicial, pasando por la lectura de la documentación, implementación y posterior revisión de que todo este bien configurado.