Arquitectura

Moisés Gautier Gómez

31 de mayo de 2015

Vamos a analizar la posible estructura funcional del sistema para desgranar cada uno de los componentes el mismo en profundidad.

1. Monitor

Habrá una capa de monitorización por cada asset que reciba del sistema.

- Este monitor podría ser un demonio que se ejecutara en background y que pudiera levantarse cuando se quisiera hacer uso real del mismo.
- También podría ser un sistema sincrono restfull/nodejs o servicio web que solicitase información al dispositivo de red.
- Sistema de multiprocesamiento en el que cada hilo del proceso principal fuera para un asset de información distinta que manipula y obtiene los resultados deseados para que el padre sea capaz de compactarlos y enviarlos a su capa superior de monitorización.
- ¿Recibirá la información comprimida por tiempo, momento del día o constantemente? La idea más simple podría ser un socket de comunicación con el monitor en tiempo real que vaya haciendo minería sobre los datos extraídos.
- Data Warehouse, ¿se podría aplicar esto cómo metaconcepto? (Extraído de la wikipedia)
    - Bill Inmon1 fue uno de los primeros autores en escribir sobre el tema de los almacenes de datos, define un data warehouse (almacén de datos) en términos de las características del repositorio de datos:

- Orientado a temas.- Los datos en la base de datos están organizados de manera que todos los elementos de datos relativos al mismo evento u objeto del mundo real queden unidos entre sí.
- Variante en el tiempo.- Los cambios producidos en los datos a lo largo del tiempo quedan registrados para que los informes que se puedan generar reflejen esas variaciones.
- No volátil.- La información no se modifica ni se elimina, una vez almacenado un dato, éste se convierte en información de sólo lectura, y se mantiene para futuras consultas.
- Integrado.- La base de datos contiene los datos de todos los sistemas operacionales de la organización, y dichos datos deben ser consistentes.

Inmon defiende una metodología descendente (top-down) a la hora de diseñar un almacén de datos, ya que de esta forma se considerarán mejor todos los datos corporativos. En esta metodología los Data marts se crearán después de haber terminado el data warehouse completo de la organización.

- Simplemente puede ser algo que analice algo y nada más. Extraer información de unos ficheros con unos determinados formatos y extraer rasgos característicos.

2. Assets

Las distintas formas que tienen los assets de generar logs o información.

2.1. Firewall logs

- Iptables: `https://www.frozentux.net/iptables-tutorial/spanish/iptables-tutorial.html#LOGTARGET` Coge la información de sus logs mediante el registo del núcleo syslog que puede ser leía mediante dmesg. (Mirar también syslog.conf)

- Ipcop: `http://www.ipcop.org/` Ofrece monitorización de elementos de la red así cómo del pc en el que se encuentra instalado `http://www.ipcop.org/2.0.0/es/admin/html/status.html`. La forma en cómo obtiene registros del sistema viene descrita aquí: `http://www.ipcop.org/2.0.0/es/admin/html/logs.html` y es usando una vez más el demonio syslogd.

- Más firewalls: http://www.tecmint.com/open-source-security-firewalls-for-linux

2.2. IDS logs

https://www.alienvault.com/blogs/security-essentials/open-source-intrusion-de

- Suricata: http://suricata-ids.org/ Guía de usuario: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_User_Guide Tipo de logs que nos ofrece suricata:
  - syslog alerting:https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Syslog_Alerting_Compatibility
  - json.log output: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/What_to_do_with_files-jsonlog_output
  - Suricata with OOSIM: https://redmine.openinfosecfoundation.org/projects/suricata/wiki/Suricata_with_OSSIM
- Snort: https://www.snort.org/ - RSyslog rate limiting configuration: https://s3.amazonaws.com/snort-org-site/production/document_files/files/000/000/025/original/snort-rate-limiting-rev1.pdf?AWSAccessKeyId=AKIAIXACIED2SPMSC7GA&Expires=1433101726&Signature=wnGRl%2FEmKc%2BftdA6um3VT2O99R4%3D
- Para hosts: OSSEC - http://www.ossec.net/
- Otros:
  - Snorby: https://snorby.org/
  - Sguil: http://bammv.github.io/sguil/index.html