**Despliegue de Infraestructura**

A continuación se indicara como desplegar la infraestructura.

1. En primer lugar debemos descargar los archivos alojados en el siguiente Drive (demora bastante la descarga, considerar que son app 14 Gb en total):

https://drive.google.com/open?id=1A38iMwh4PAiq0uZ25KOAOY5woKr-csHv

2. Posterior a esto o en paralelo debemos realizar es tener dentro de donde se administraran las maquinas virtuales el “Vmware Work Station”.

3. Luego hacemos doble click y cargamos la maquina virtual de “Graylog\_Unab” y la maquina virtual de “Mail\_Server\_Unab”. Dejamos de que ambos procesos de instalación y asociación terminen en su totalidad.

4. Debemos asignar IP´s del mismo segmento de red a ambas maquinas virtuales, esto con el objeto de que ambas se puedan visualizar e intercambiar datos.

5. Posterior a esto, encendemos las 2 maquinas virtuales “Graylog\_Unab” y “Mail\_Server\_Unab”, dejamos de que ambas maquinas finalicen su proceso de encendido.

6. Luego ingresamos a “Graylog\_Unab” a través del usuario “jonathan”, en donde la password es “Temerac2018”.

7. Estando dentro de esta abriremos una ventana terminal.

8. A través del comando “ifconfig” consultamos direccionamiento de red.

9. Tomamos nota de la ip que aparece en ens33 “inet addr: 192.168.203.137” (en este caso), ya que esta debemos reemplazarla en el archivo que detallaremos mas adelante.

10. Posterior a esto nos dirigimos al archivo de configuración de Graylog, con el siguiente comando # sudo nano /etc./Graylog/server/server.conf. Ingresaremos nuevamente la pass “Temerac2018”.

11. Visualizaremos siguiente archivo, en donde nos debemos dirigir a “http\_”, esto lo podemos hacer mas rápido a través de “ctrl + w” y tipeamos “http\_bind\_address”, aquí debemos reemplazar el valor con la ip que habíamos copiado anteriormente (xxx.xxx.xxx.xxx:9000). Posterior a este cambio “ctrl + o” y enter para guardar.

12. Dentro del mismo archivo y con las teclas “ctrl + w” tipeamos “email transport” y enter, llegando a esta sección del archivo, debemos configurar la misma ip anterior, tal como se ve en la siguiente figura.

13. En la sección recién vista del archivo (#Email transport), también se efectúa la configuración del servidor de correo (dominio @lab.cl), con el cual se establecerá la comunicación, en este caso la configuración ya esta realizada y solo se debe cambiar la ip de la Uri, de acuerdo a lo solicitado en el pto. 11. Posterior a esto presionamos “ctrl + o” y enter para guardar, luego “ctrl + x” para salir.

14. Posterior a esto reiniciamos el correlacionador, con el comando

#sudo systemctl restart graylog-server

15. Ahora instalaremos y configuraremos Graylog-Sidecar (agente) en un equipo(s) Windows, lo primero que haremos en equipo Windows será ejecutar el archivo graylog\_sidecar\_installer\_1.0.2-1, el cual estará junto a las maquinas virtuales, dejamos que el proceso de instalación termine.

16. Posterior a esto buscamos CMD y lo ejecutamos como “administrador”.

17. Estando dentro de CMD vamos al archivo de configuración de Graylog-Sidecar, con el siguiente comando notepad.exe C:\Program Files\Graylog\sidecar\sidecar.yml. Aquí seteamos la dirección ip de Graylog\_Unab en la línea server\_url: http://xxx.xxx.xxx.xxx:9000/api, como aparece en la figura de abajo. Luego “ctrl + g” para guardar y cerramos el archivo.

18. Creamos un API Token para este input desde System/Autenthication aquí seleccionamos provider setting del panel izquierdo y le damos un nombre al nuevo Token, posterior a esto lo copiamos y reemplazamos en este archivo ya editado de configuración de Graylog\_Sidecar.

Nota: Ya hay creado un Api Token “Windows\_Token\_Sidecar\_Unab”, también se puede copiar este y reemplazar en el archivo ya editado.

server\_api\_token: "d52sfsoiridmrk8ju25q2s1u2p93flm9qmv1okm2qt802nn1noj" (Token ejemplo).

19. Luego dentro de CMD ejecutamos siguientes comandos:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service install

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service start

En el caso de que el proceso estuviera corriendo, ejecutamos:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service stop y luego:

"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service start

20. Luego ingresamos a Graylog http://ipa.ddr.ess.ss:9000/ y nos dirigimos a System/Sidecard/Configuration y en el archivo de configuración en host seteamos la ip de Graylog\_Unab, como muestra la figura de abajo (hosts: ["ipa.ddr.ess.sss:5044"]) (en este caso es esa ip).

21. Luego abajo le damos “Update”.

22. Posterior a estos nos dirigimos a “Alertas”, menú que se encuentra en el panel superior y vamos a “Notifications”, luego en “Alerta de seguridad” le damos click a “More actions” y le damos a “edit”.

23. Debemos dejar siguiente configuración, en E-mails receivers dejaremos la cuenta jonathan@lab.cl que es el receptor y una de las cuentas configuradas en el servidor de correo “Mail\_Server\_Unab”, le damos “Save” con la cual guardaremos dicha configuración.

24. Ahora instalaremos en otros equipo (Que seria el equipo donde efectuare el monitoreo y donde recibiré los correos) un gestor de correo, las pruebas e implementación se realizaron con Thunderbird, posterior a la instalación configuraremos 2 cuentas de correos en este gestor, de acuerdo a siguiente detalle:

**Cuenta 1.**

Nombre: jonathan@lab.cl

**Cuenta 2.**

Nombre: graylog@lab.cl

Ambas cuentas deben que configuradas de acuerdo a las figuras (figura 1 – figura 2) de mas abajo.

Se debe tener presente para ambas cuentas:

a) Your name: El que desee.

b) Email address: jonathan@lab.cl (cuenta 1) y graylog@lab.cl (cuenta 2).

c) Password: test2020

d) Server hostname: Es la dirección ip del servidor de correo “Mail\_Server\_Unab”.

e) Puerto IMAP: 143

f) Puerto SMTP: 25

25. Posterior a esto nos vamos a la maquina “Graylog\_Unab” y seteamos como DNS de esta la direccion ip del servidor de correo “Mail\_Server\_Unab”, también como se muestra en las figuras siguientes se recomienda dejar direccionamiento IP en “Manual” y setera mismos datos ya asignados (#ifconfig).

26. Objeto ver si configuración esta correcta y las alertas (correos) quedaron bien seteados, nos dirigimos a “Alert”, dentro de este nos vamos a “Notifications” y buscamos la alerta configurada que lleva por nombre “Alerta de Seguridad”, aquí hacemos click en el boton “Test”, si esta todo bien nos debiera llegar un correo a la cuenta jonathan@lab.cl.

27. Mientras usted se encuentra trabajando en otras actividades frente al computador, las notificaciones deben aparecer como pop-up.

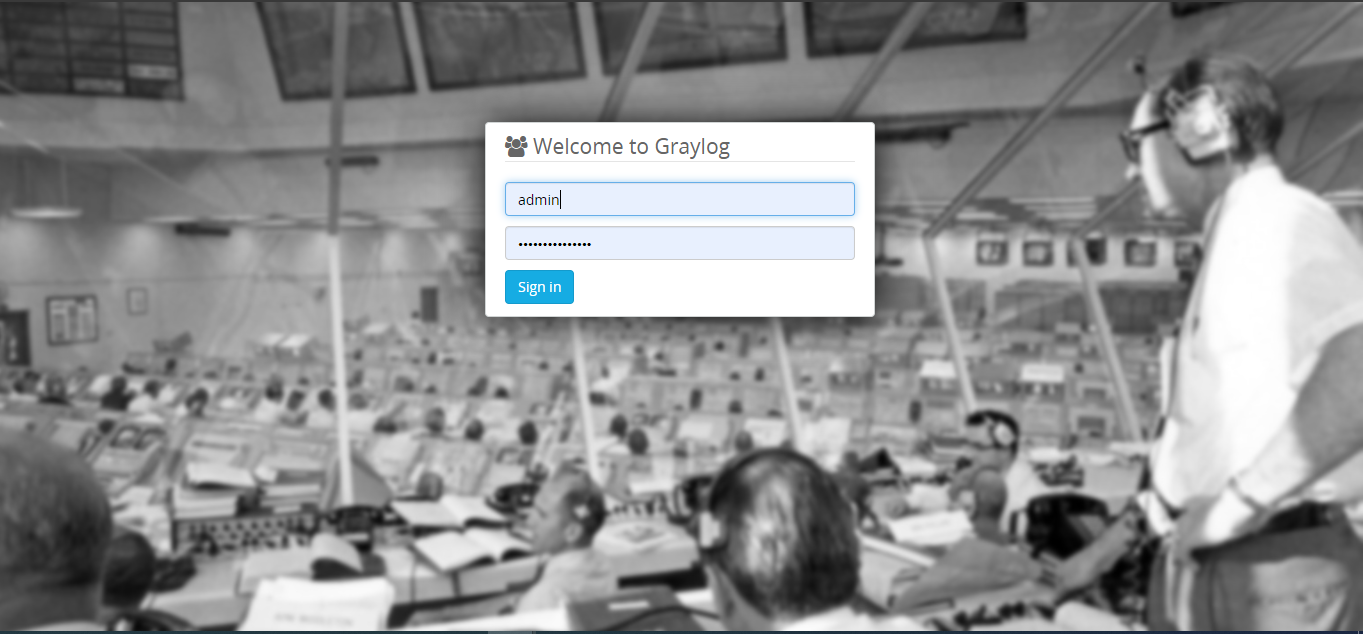
28. Respecto al servidor de correo “Mail\_Server\_Unab”, las credenciales para ingresar son las siguientes:

User: root / Pass: test

User: test / Pass: test

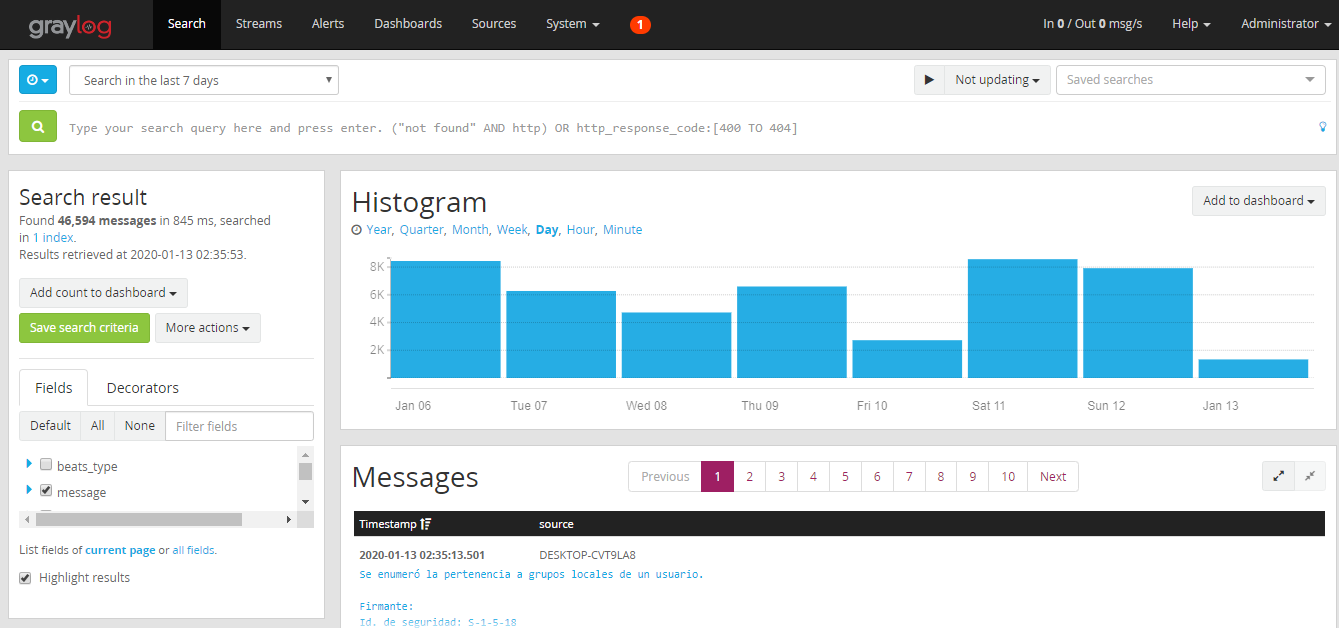
29. En el caso de que servidor de correo presente problemas, se debe verificar a través del comando #nano etc/bind/db.lab.cl que las ip´s que tiene configuradas son las asignadas (misma ip del servidor de correo).

A continuación se despliega la visualización del sistema de correlación.



**Ilustración 11: Ingreso a Graylog**

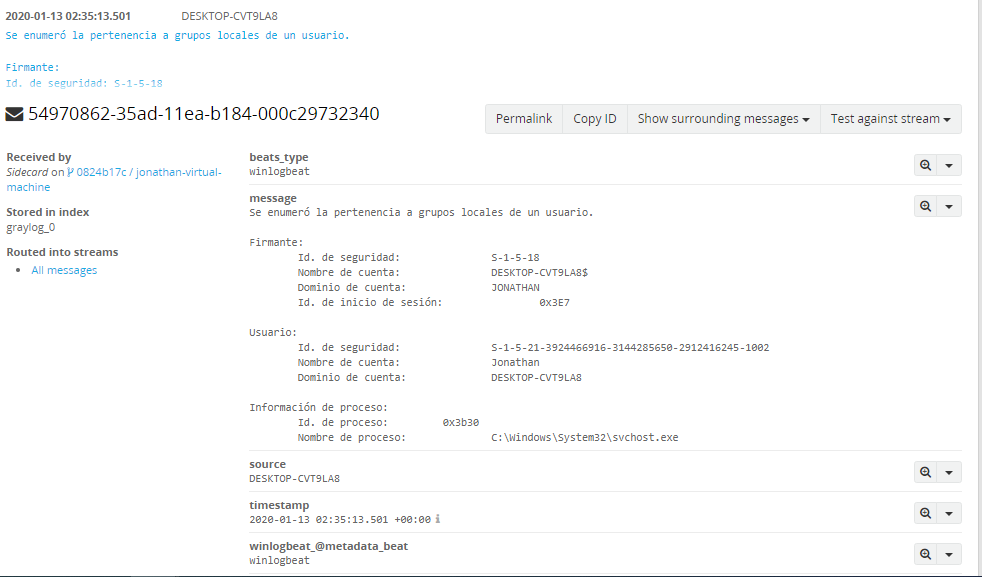
Esta es la visualización que debemos ver para hacer ingreso al correlacionador de eventos Graylog, con las credenciales entregadas.



**Ilustración 12: Histograma**

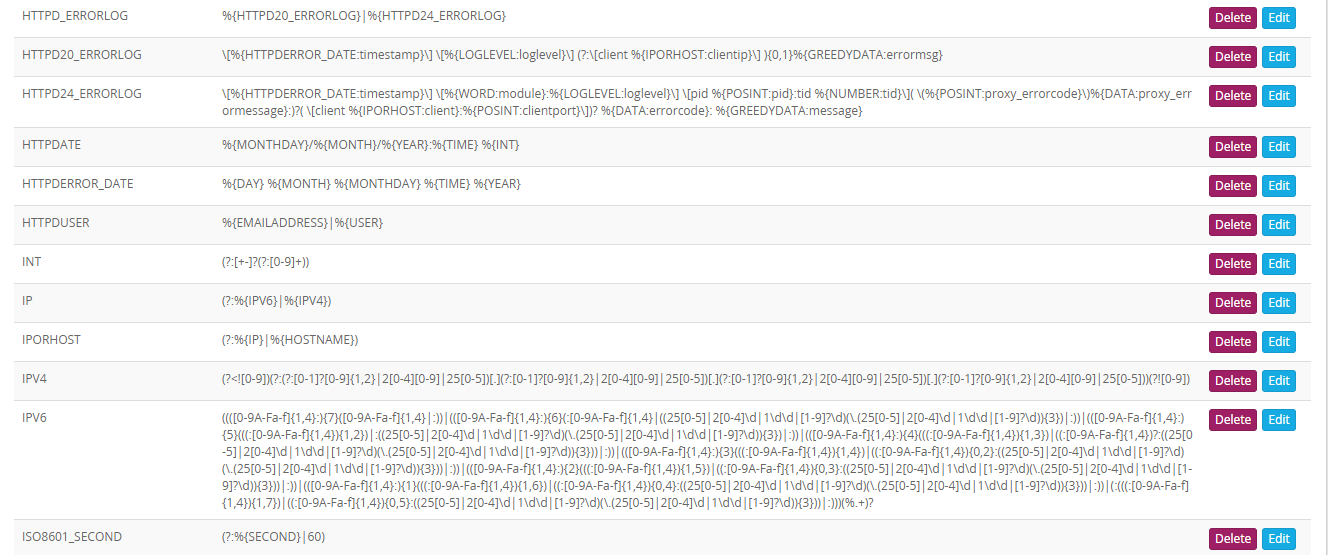
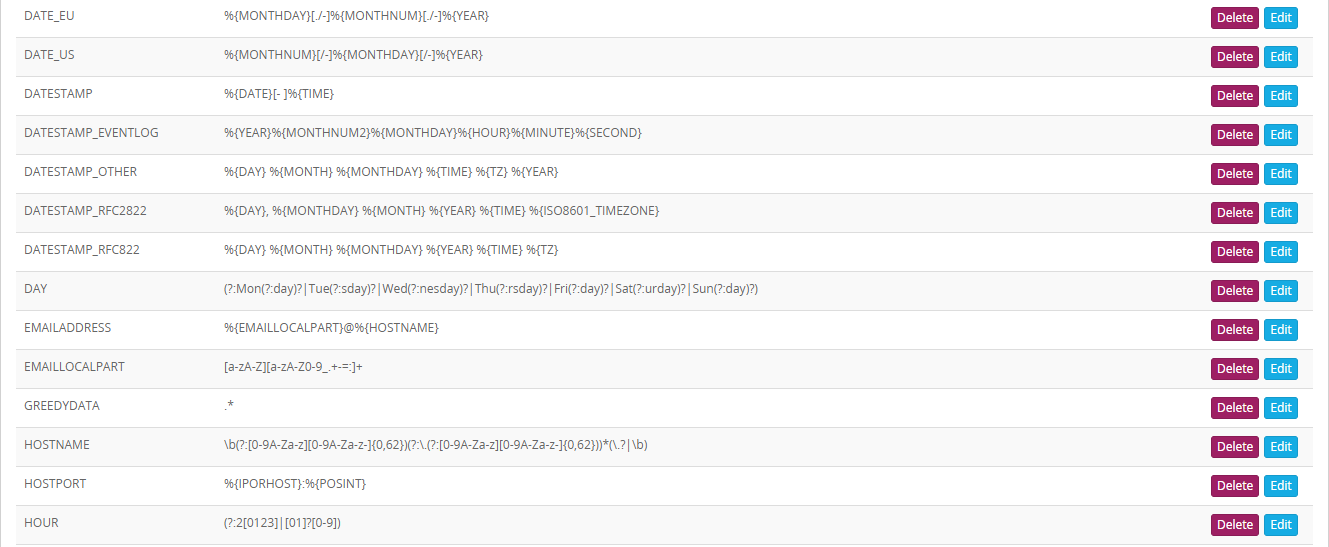
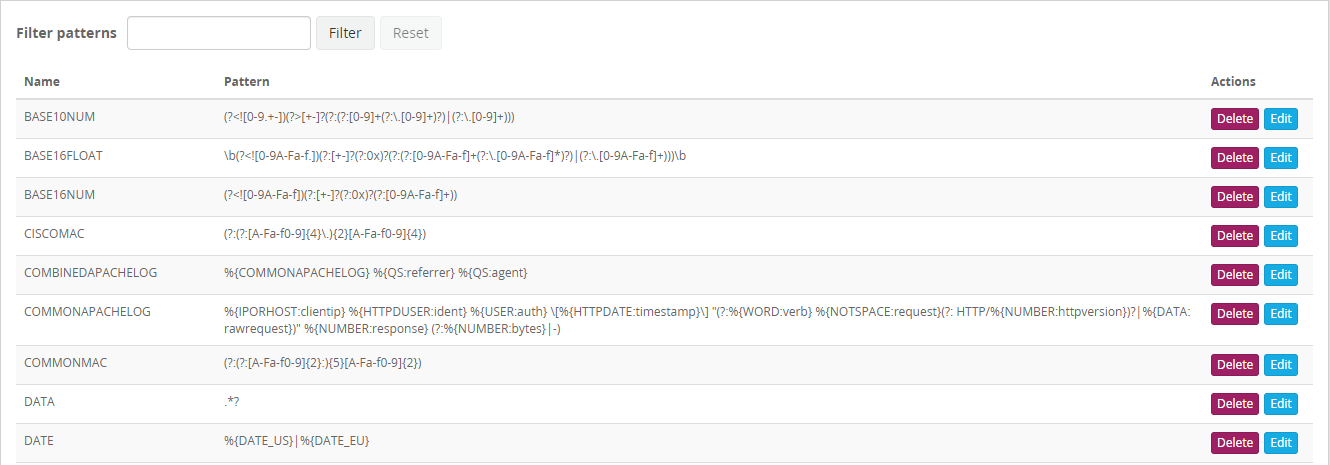
Una de las primeras visualizaciones que tendremos es esta en donde podemos ver el Histograma, en donde se pueden apreciar los eventos que están ingresando al sistema.

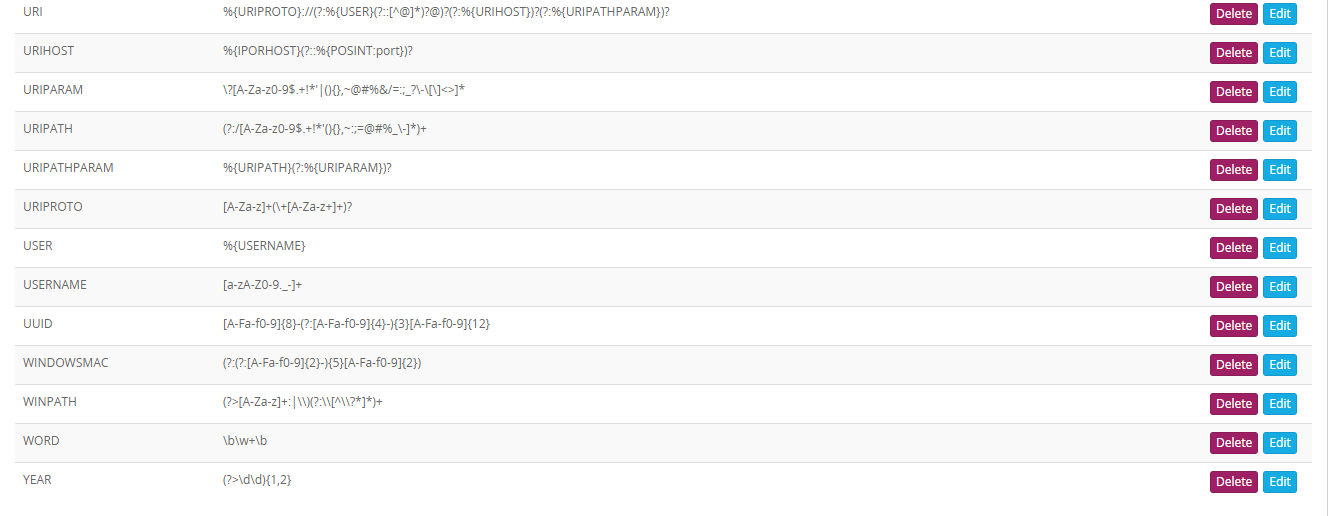
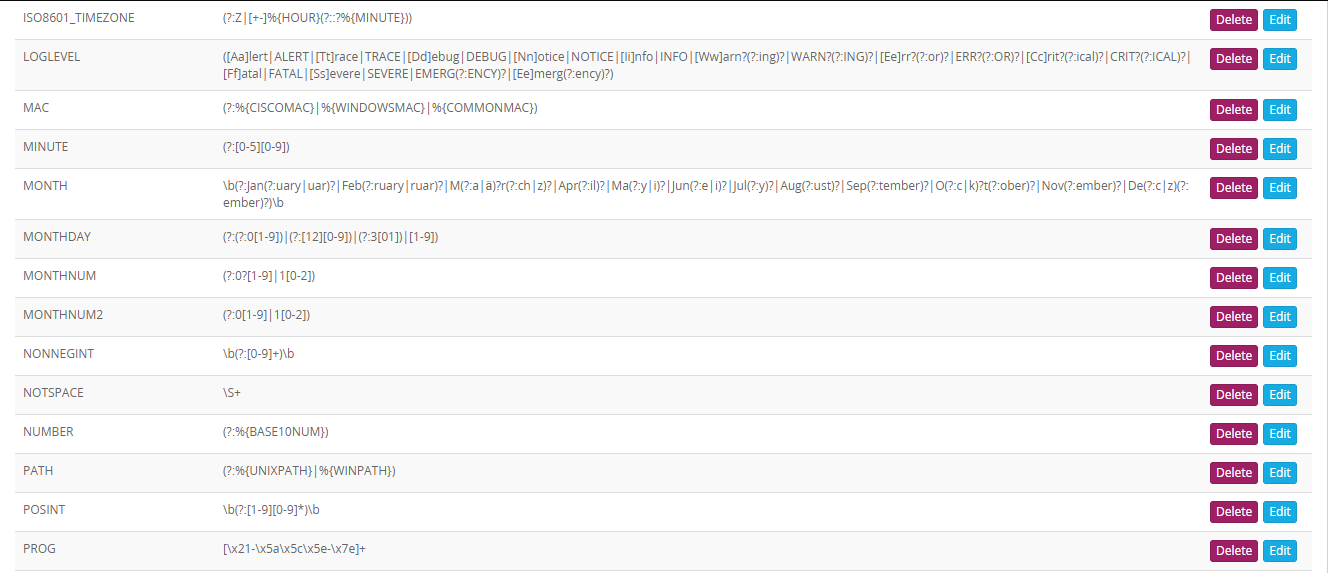
En el costado derecho podemos visualizar la cantidad de eventos recolectada y la cantidad de tiempo empleada en esta, lo cual nos hace ver que efectivamente el flujo de datos es considerable.



**Ilustración 12: Desglose del Log**

Si hacemos clic sobre uno de los eventos que se encuentran bajo el Histograma, notaremos que se despliega este evento y se pueden visualizar todos los componentes que forman parte de ese determinado log. Esto quita una gran carga de trabajo a los encargados de Seguridad TI, ya que podemos apreciar de forma rápida y certera quien es el origen del evento, su dominio, dependencia, hora de ocurrencia y otros datos que son de vital importancia para en caso lo requiera mitigar un incidente informático.





**Ilustraciones: Correspondientes a detalle de patrones Grok configurados**

En las imágenes anteriores podemos apreciar un listado de patrones Grok, los cuales nos ayudan a que los extractores de datos Graylog realicen su trabajo de mejor forma.

Graylog también admite la extracción de datos utilizando el popular lenguaje Grok para permitirle utilizar sus patrones existentes.

Grok es un conjunto de expresiones regulares que se pueden combinar con patrones más complejos, lo que permite nombrar diferentes partes de los grupos coincidentes.

Al usar patrones Grok, puede extraer múltiples campos de un campo de mensaje en un solo extractor, lo que a menudo simplifica la especificación de extractores.

Las expresiones regulares simples a menudo son suficientes para extraer una sola palabra o número de una línea de registro, pero si conoce de antemano la estructura completa de una línea, por ejemplo, para un registro de acceso o el formato de un registro de firewall, es ventajoso usar Grok.