**Guia Operador**

1. Ingresamos a la plataforma Graylog, de acuerdo a siguiente detalle:

URL : <http://192.168.25.129:9000/>

User : admin

Pass : Temeracbeta2020

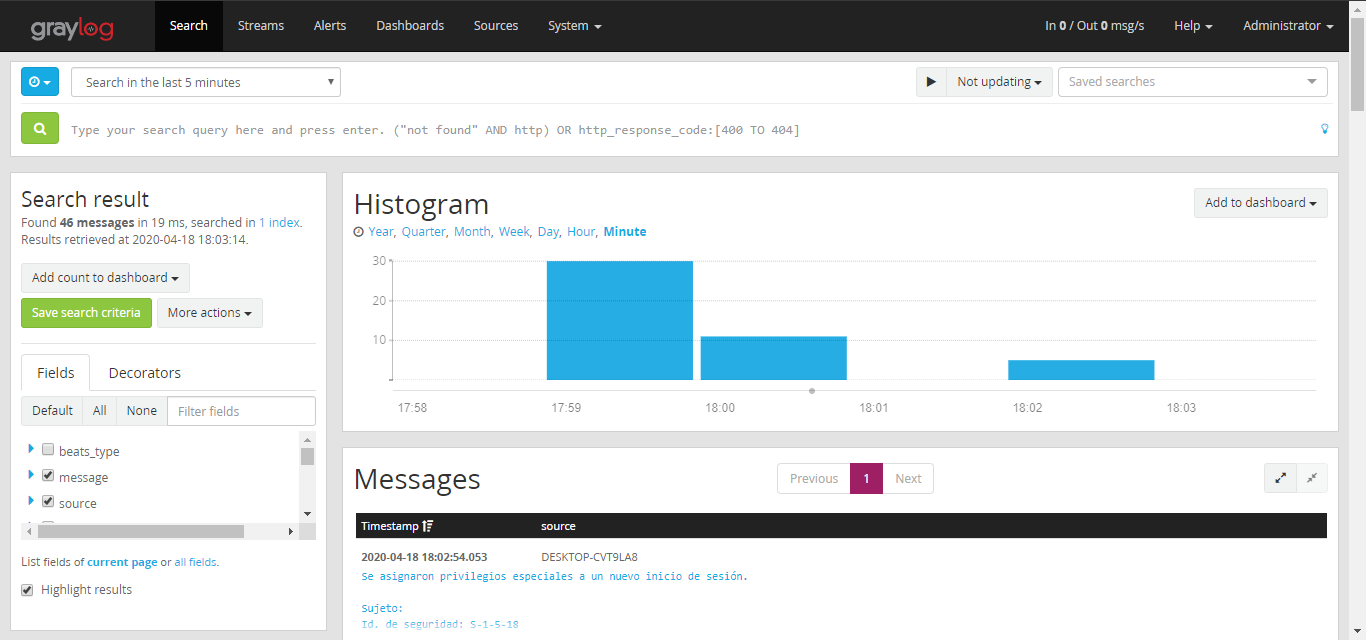
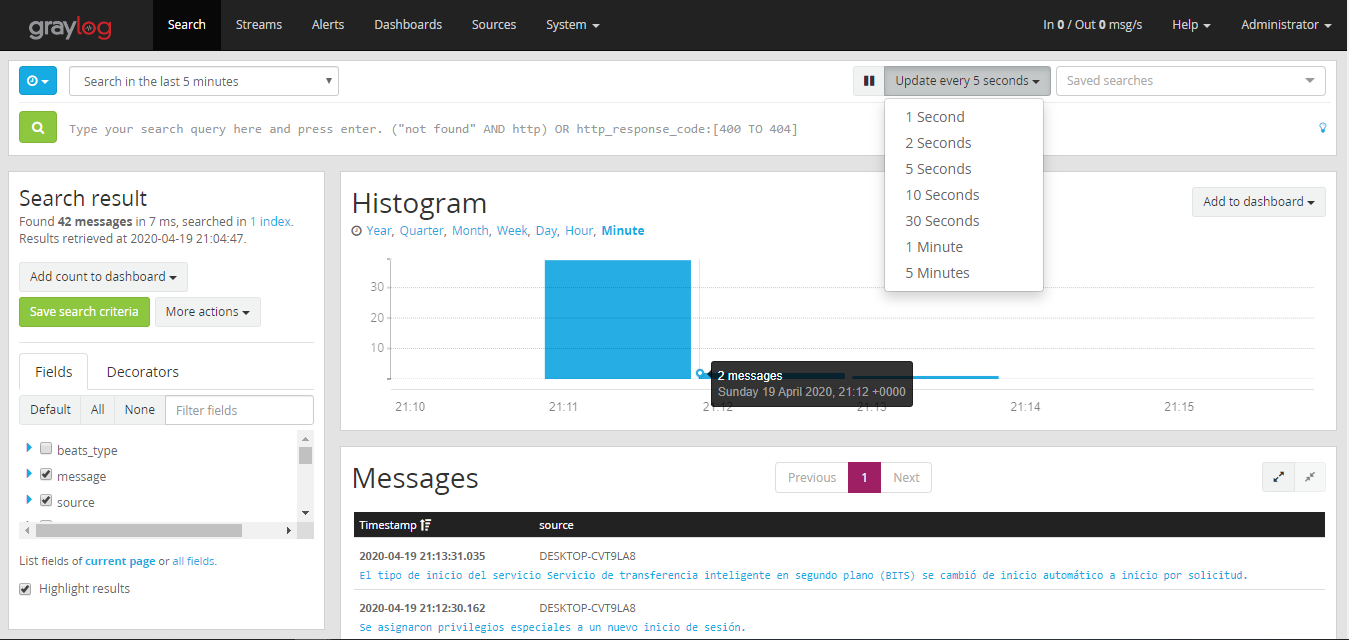


Figura N° 1 “Search”

Una visualizacion como la figura N° 1 se desplegara en su navegador.

1. A continuacion nos dirigimos al simbolo de “Play”, donde debe tener la opción “Not updating” y le damos click y seleccionamos la opcion que necesitemos, esto le da la intruccion al sistema de que actualice sus datos y log en el tiempo configurado.

Figura N° 2

1. A continuacion le damos click al boton “Show alerts”, aquí visualizaremos todas las alertas que se han gatillado.

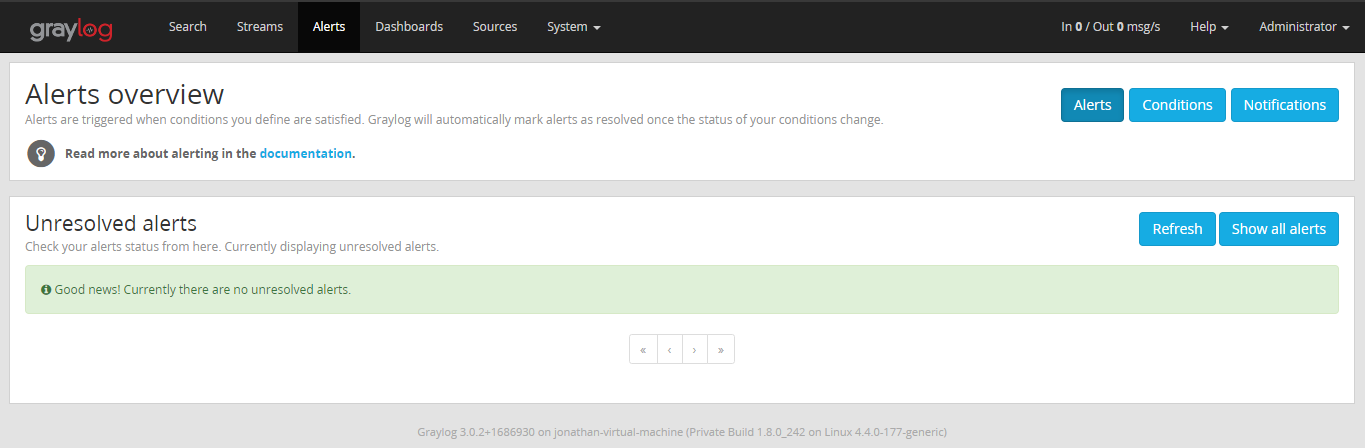


Figura N° 3

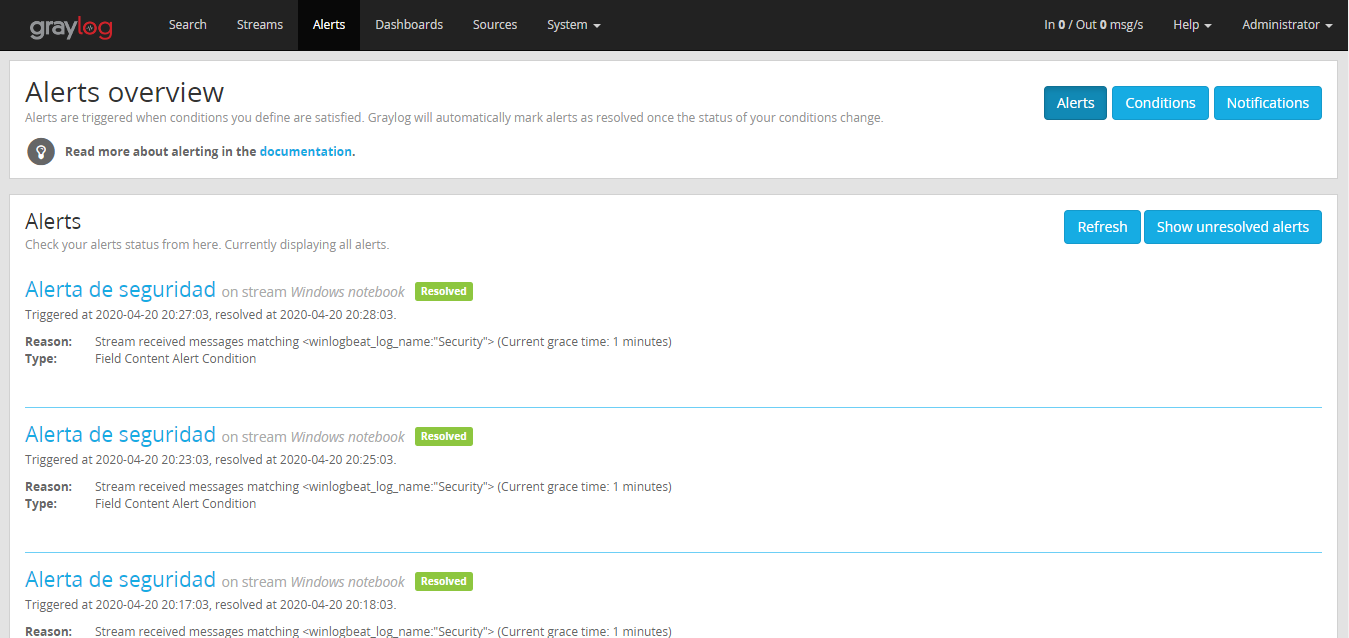


Figura N° 4

1. Posterior a estos nos dirigimos al menu “Alerts”, el cual se encuentra en el panel superior, vamos a “Notifications”, luego en “Alerta de seguridad” le damos click a “More actions” y le damos a “edit”.

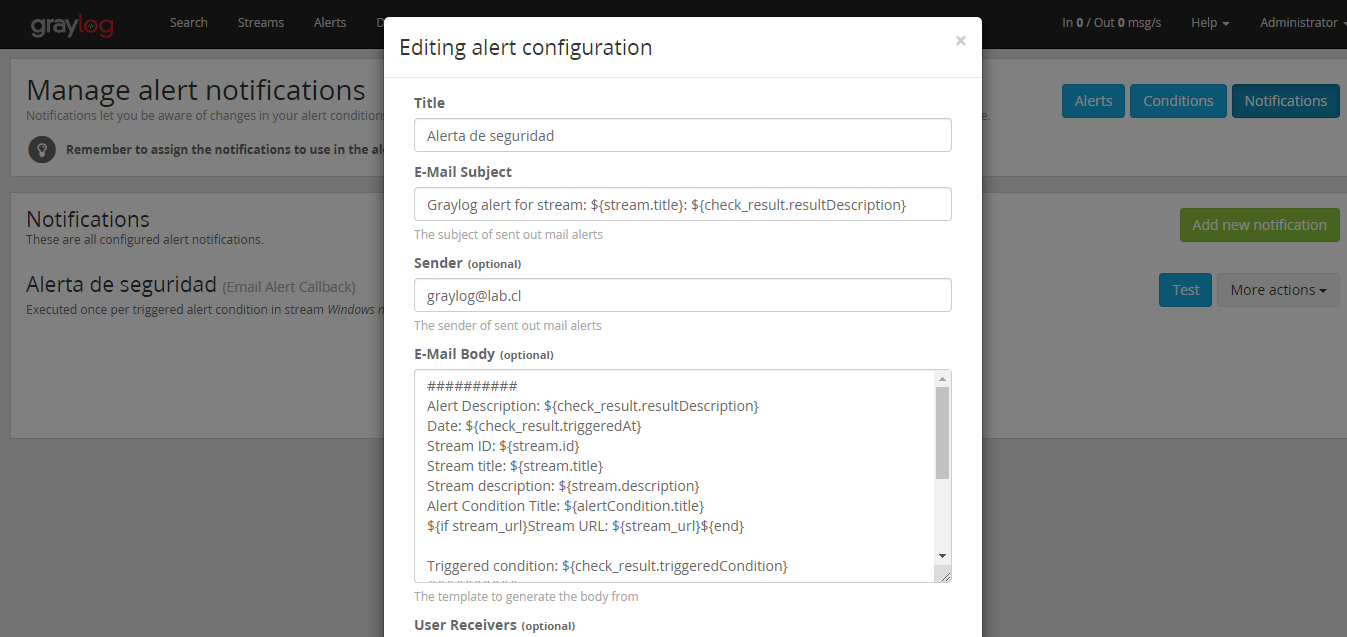


Figura N° 5

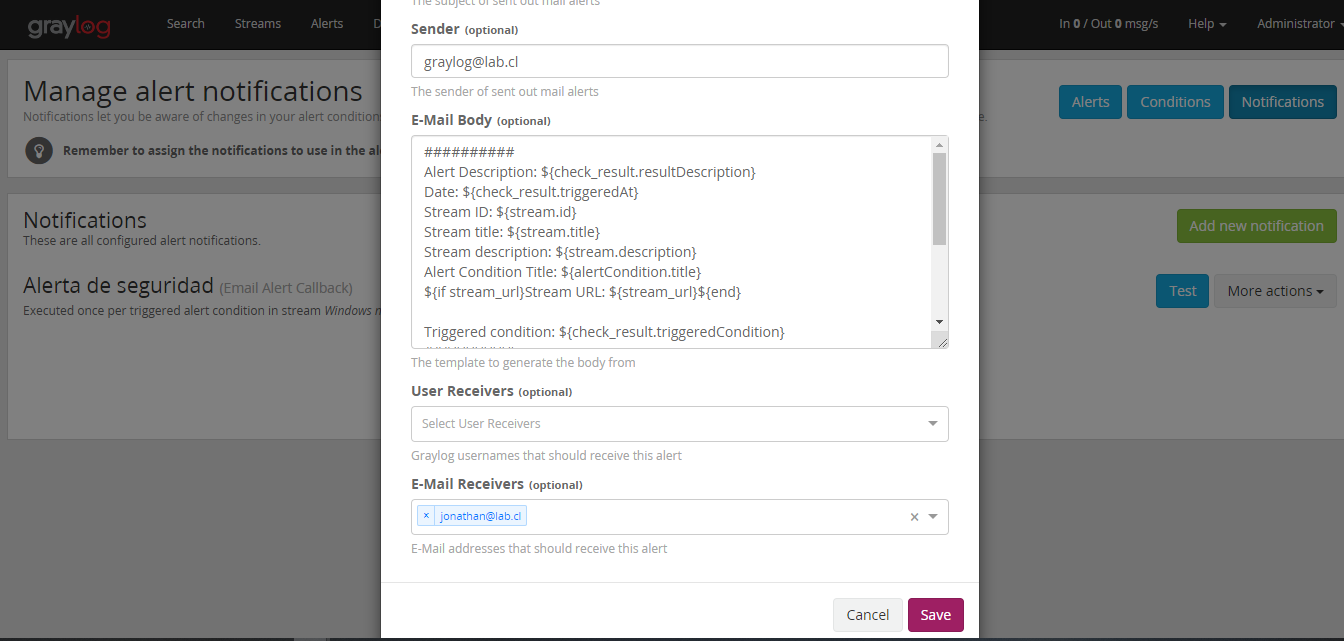


Figura N° 6

1. En las figura N° 5 y N° 6 podemos ver el originador y el destinatario de las cuentas de correo a la cual se enviara el correo con la notificacion de la alerta de seguridad. Esto con el objeto de que el personal de seguridad TI o el encargado tome las acciones de mitigación.
2. Si nuestra intencion es solo visualizar la configuración de la notificación y no efectuar cambios en esta dentro de la pestaña “Notifications”, hacemos click en “show configuration”, opcion que se encuentra en la parte inferior de Alerta de seguridad.

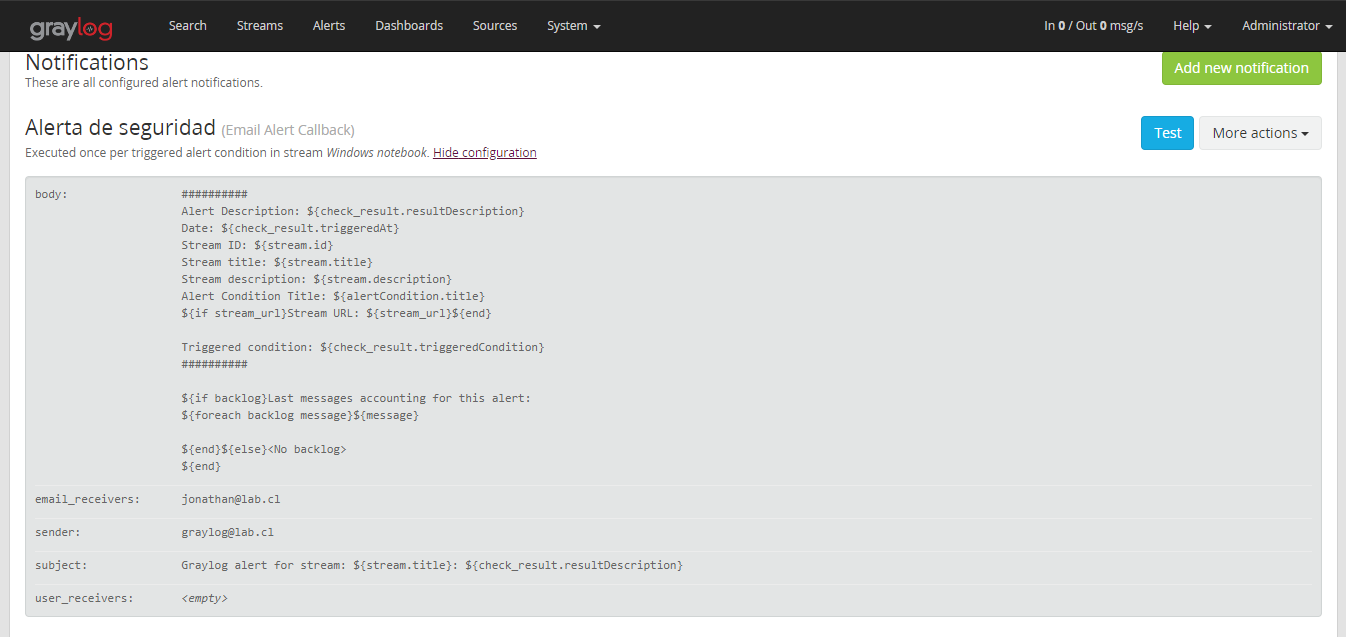


Figura N° 7

1. En el equipo destinado para monitoreo se configuro un gestor de correo (Thunderbird) la cuenta para la recepción de las notificaciones ([jonathan@lab.cl](mailto:jonathan@lab.cl), para pruebas), esta cuenta sera la encargada de recibir los distintos correos con notificaciones de Alertas de Seguridad.

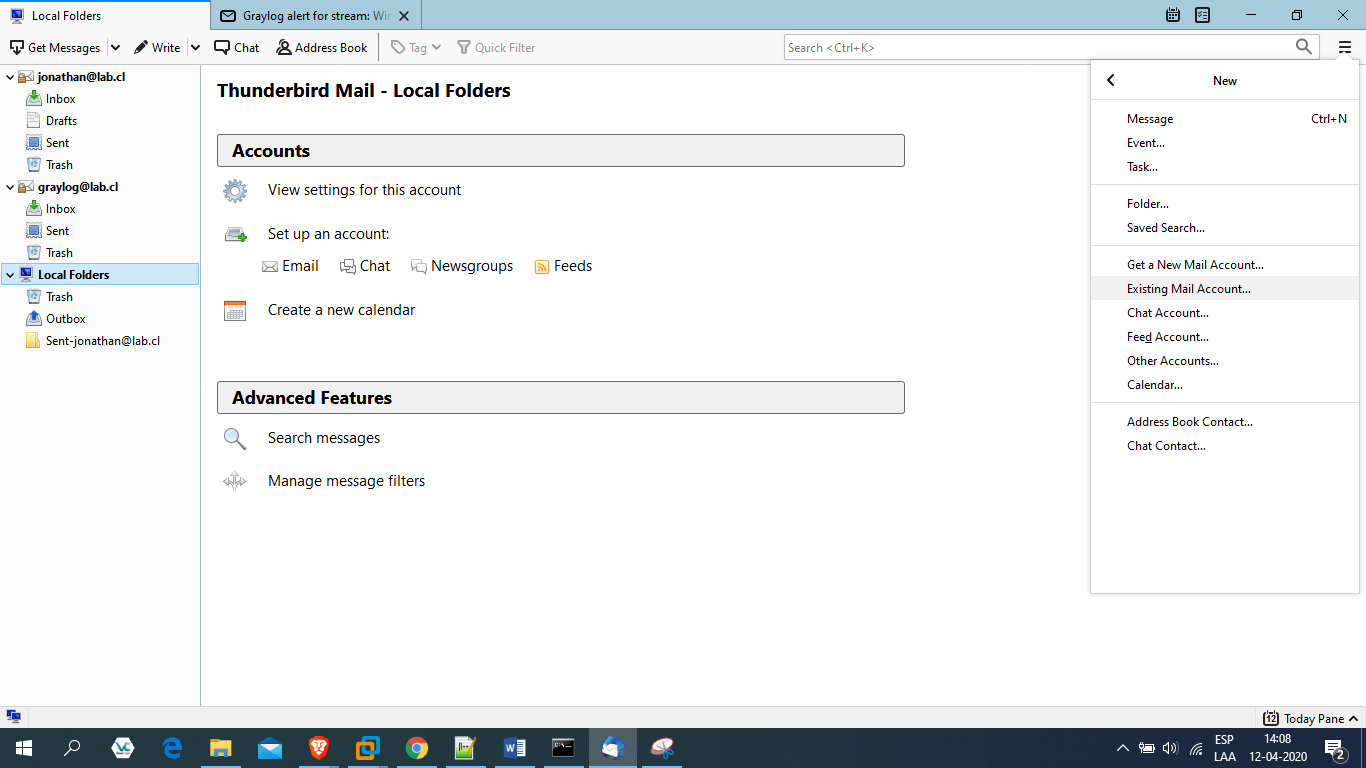


Figura N° 8

Cuenta 1.

Nombre: [jonathan@lab.cl](mailto:jonathan@lab.cl)

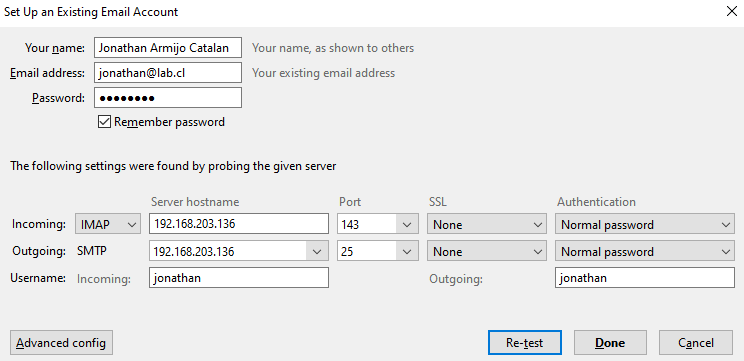
Cuenta 2.

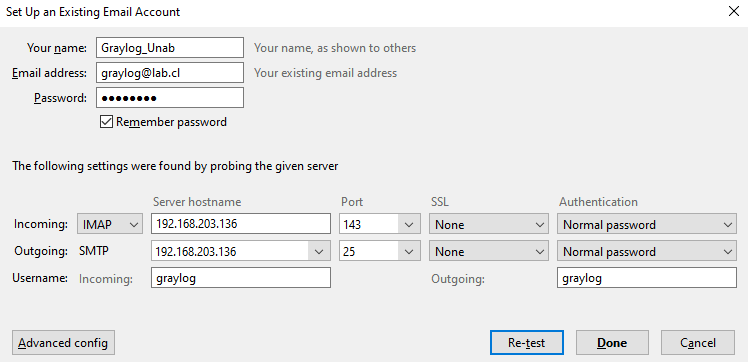
Nombre: [graylog@lab.cl](mailto:graylog@lab.cl)

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

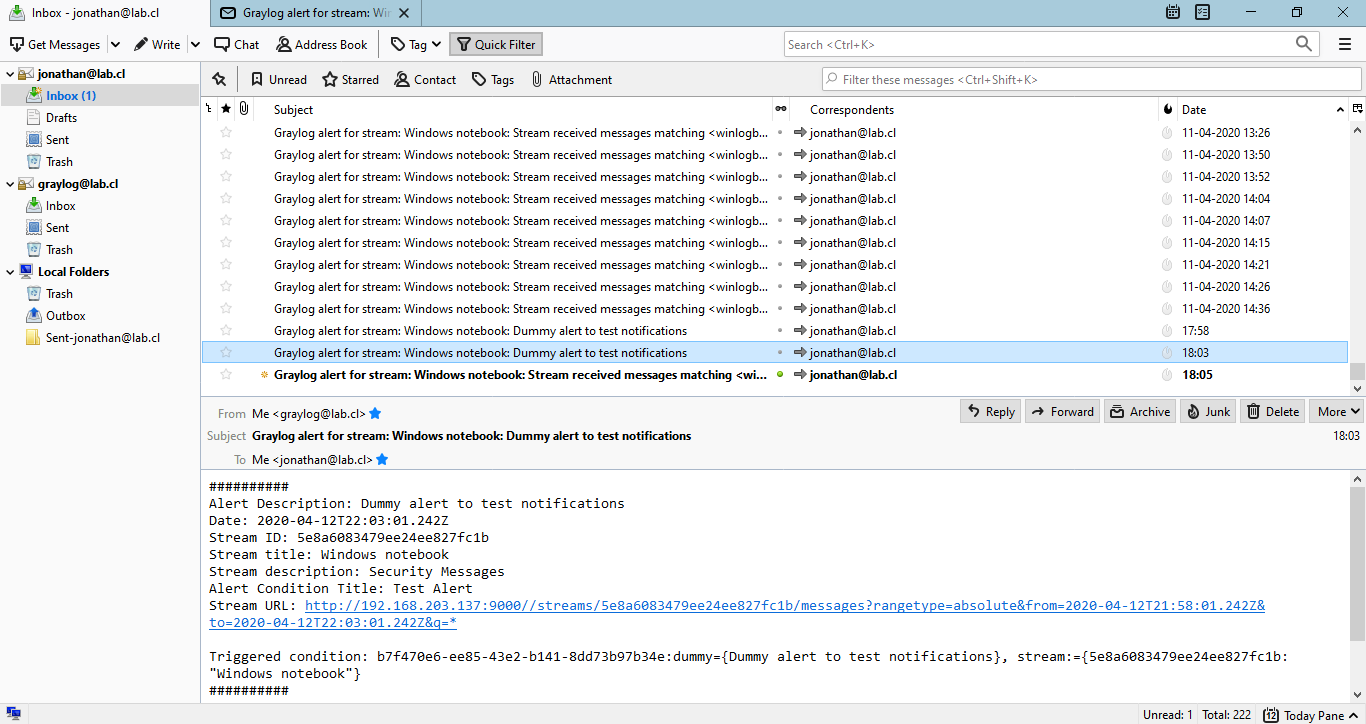
Se debe tener presente para ambas cuentas:

1. Your name: Jonathan Armijo (Ejemplo).
2. Email address: [jonathan@lab.cl](mailto:jonathan@lab.cl) (cuenta 1) y [graylog@lab.cl](mailto:graylog@lab.cl) (cuenta 2).
3. Password: **test2020**
4. Server hostname: Es la direccion ip del servidor de correo “Mail\_Server\_Unab”.
5. Puerto IMAP: 143
6. Puerto SMTP: 25

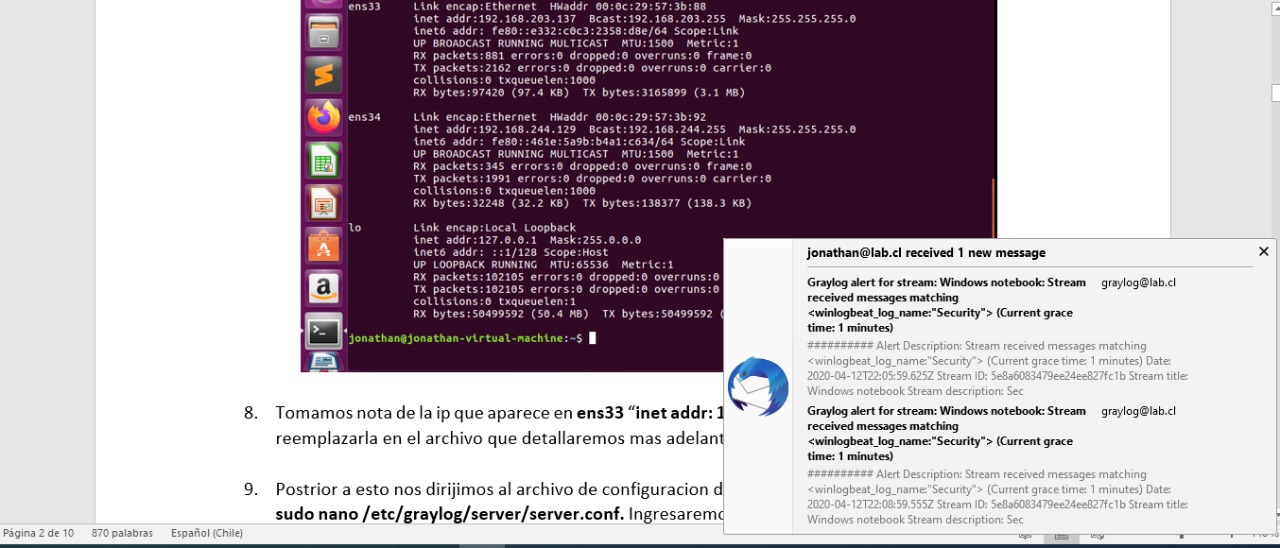




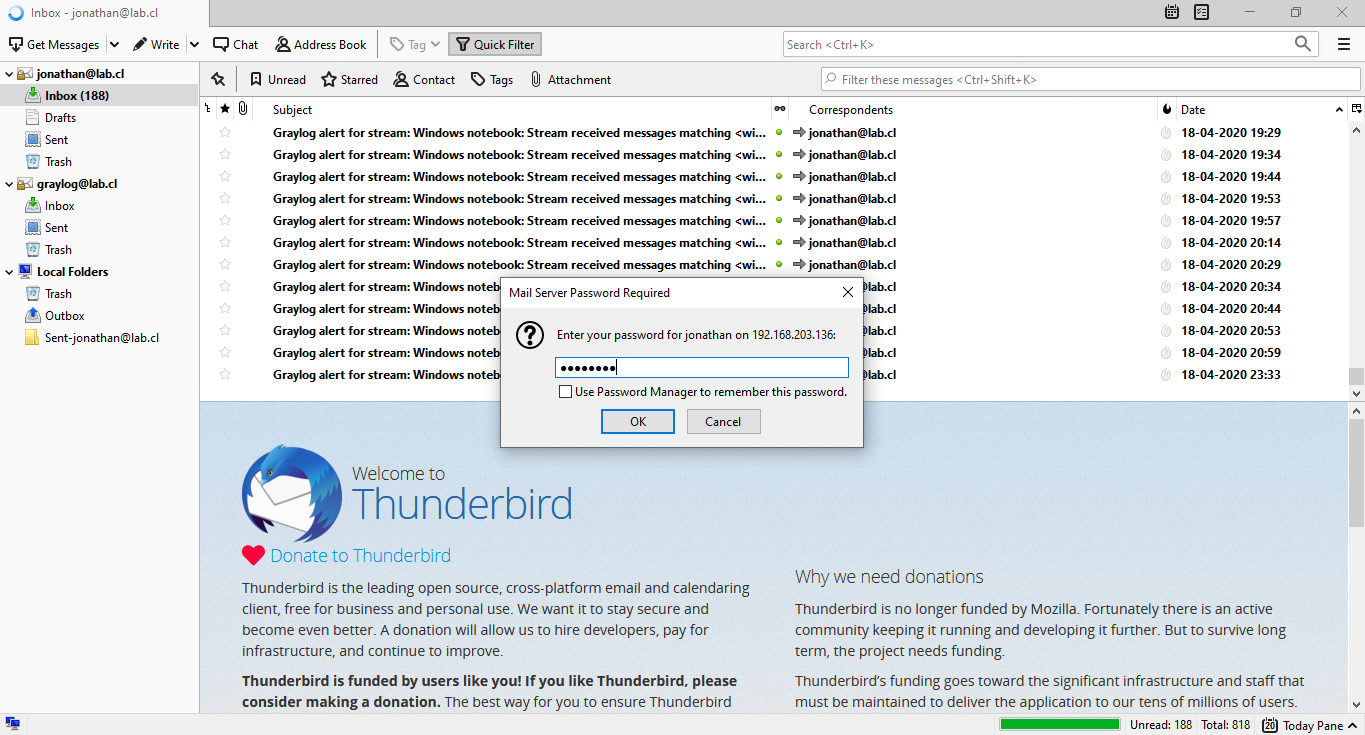
1. Objeto ver si configuracion esta correcta y las alertas (correos) quedaron bien seteados, nos dirigimos a “Alert”, dentro de este nos vamos a “Notifications” y buscamoos la alerta configurada que lleva por nombre “Alerta de Seguridad”, aquí hacemos click en el boton “Test”, si esta todo bien nos debiera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



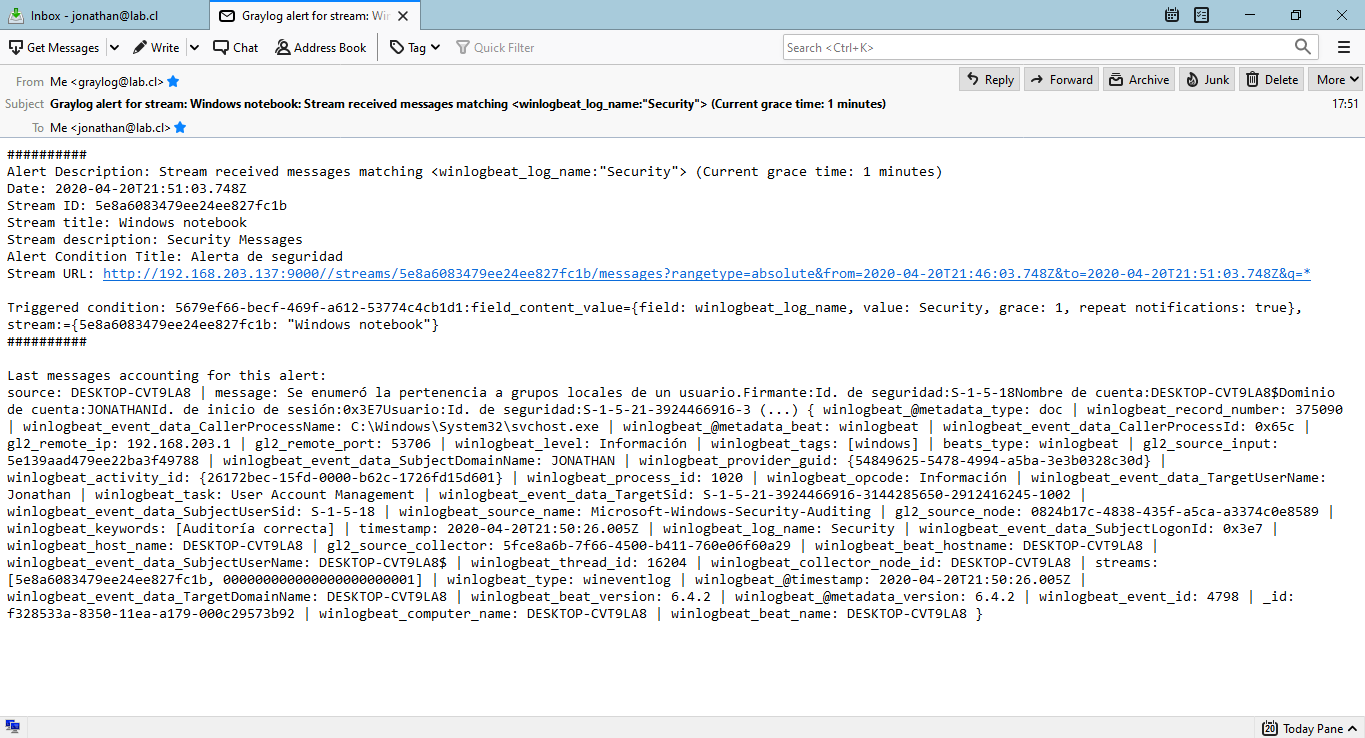
1. Mientras usted se encuentra trabajando en otras actividades frente al computador, las notificaciones deben aparecer como indica la siguiente figura:



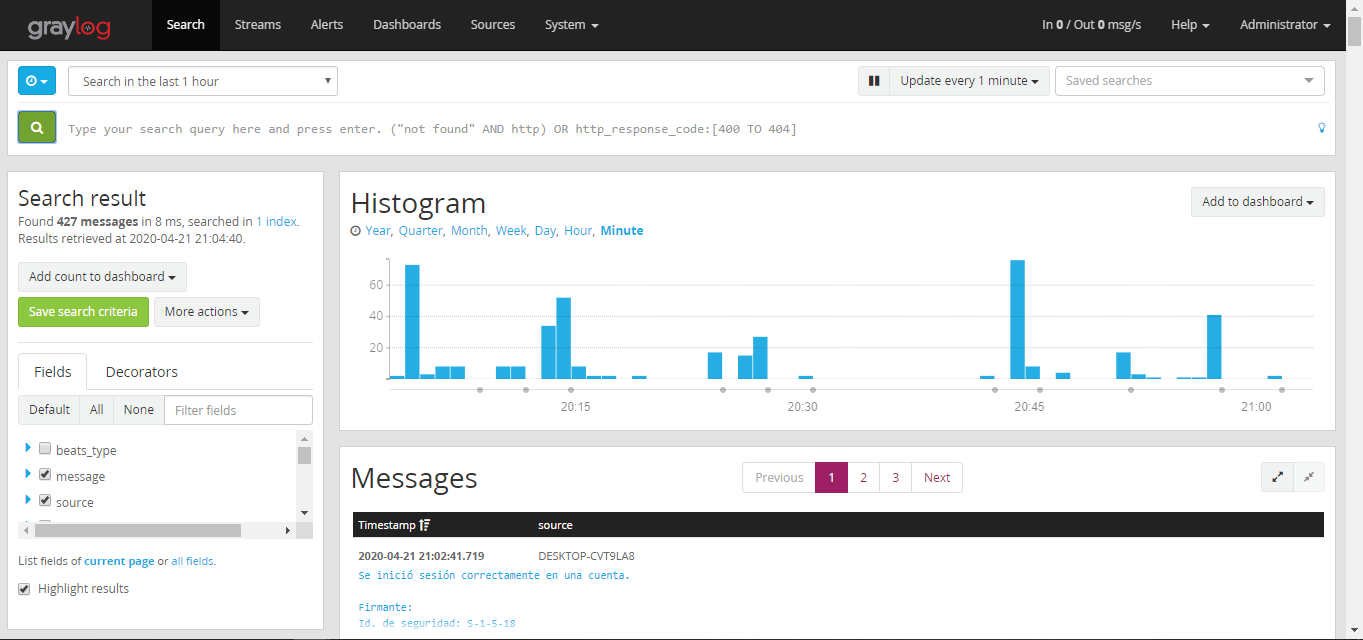
1. Al abrir el gestor de correo, este le solicitara la password del usuario, esta es **test2020**, ingresamos esta password y le damos ok.



1. Al recibir un correo electronico con el detalle de una alerta de seguridad, lo que procederemos a realizar es hacer click en esta alerta desplegando los detalles de esta, si los detalles que se aprecian en este no son convincentes de que efectivamente estamos frente a un incidente informatico, haremos click en el link “Stream URL” inserto en el mismo correo, este link nos redigira hacia el sistema de correlacion de eventos, desde donde fue gatillada y enviada la alerta. Aquí podremos revisar en detalle la alerta enviada por el sistema

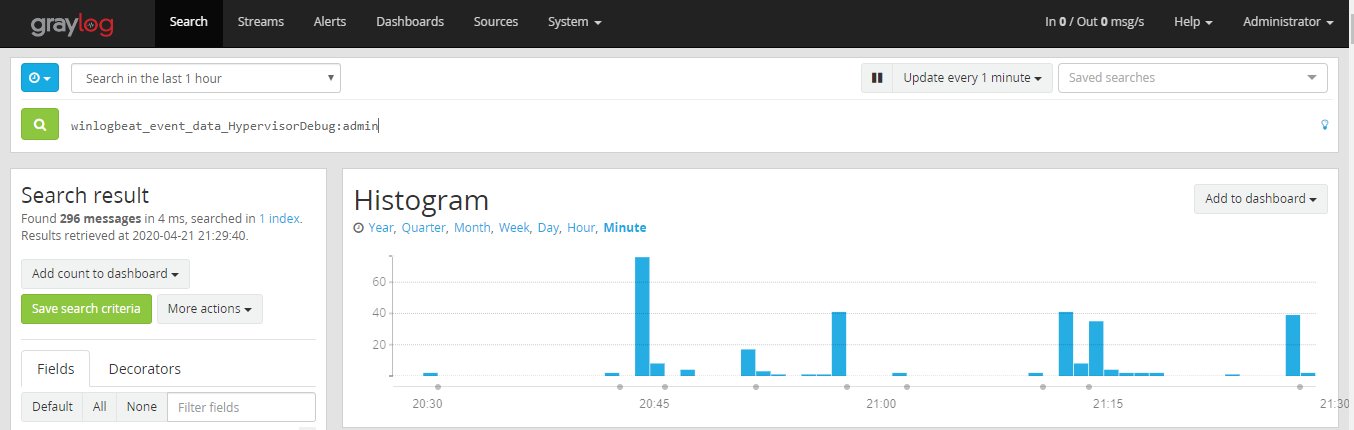


1. Normalmente el operador de seguridad o la persona encargada de informatica, en el caso que tenga la diponibilidad para monitorear la red debiera mantener en visual este dashboard, el cual muestra bastante detalles de lo que esta circulando por la red.

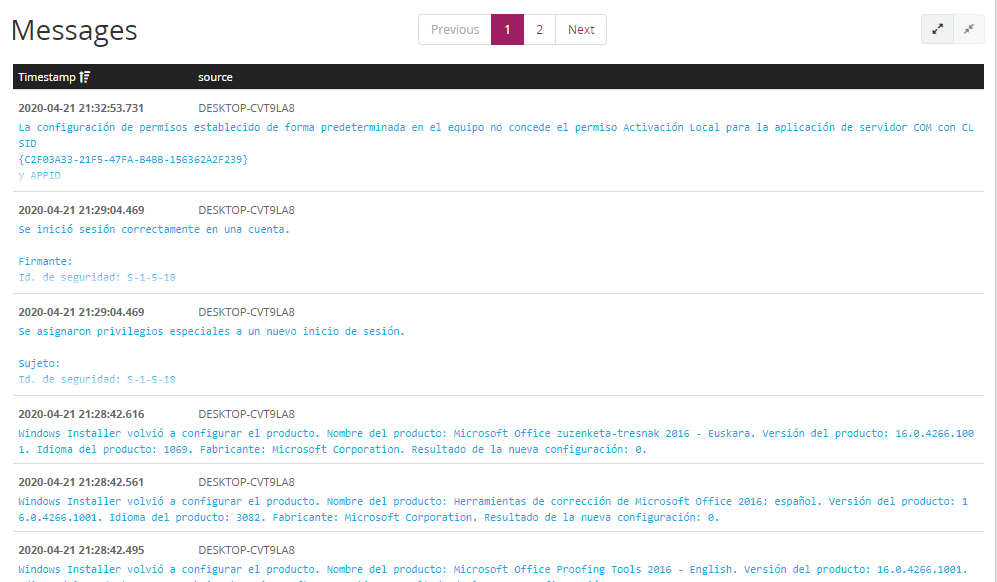


Desde este Dashboard podemos visualizar y realizar siguientes acciones:

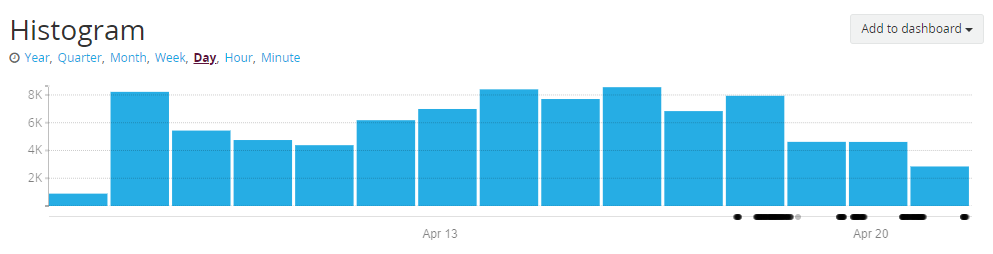
1. Busqueda de eventos o logs (Type your search…..)



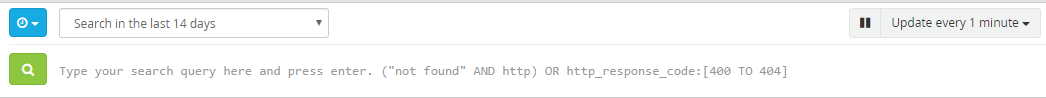
1. Visualizacion de los distintos mensajes (Messages)



1. Peak de eventos (Histogram)



1. Busqueda historica e en tiempo real (Search in the last….)



1. Despliegue en detalle de los distintos eventos (Click en messages)

