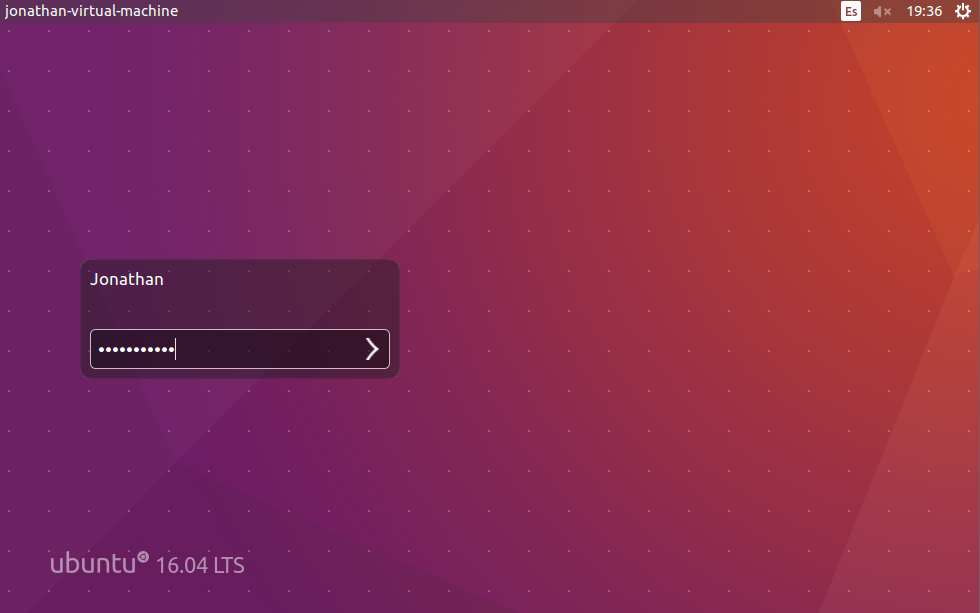
**Pruebas de aceptación - Sprint 2**

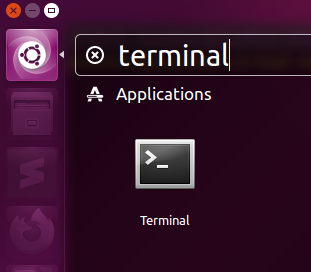
1. En primer lugar debemos descargar los archivos alojados en el siguiente Drive (demora bastante la descarga, considerar que son app 14 gb en total):

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

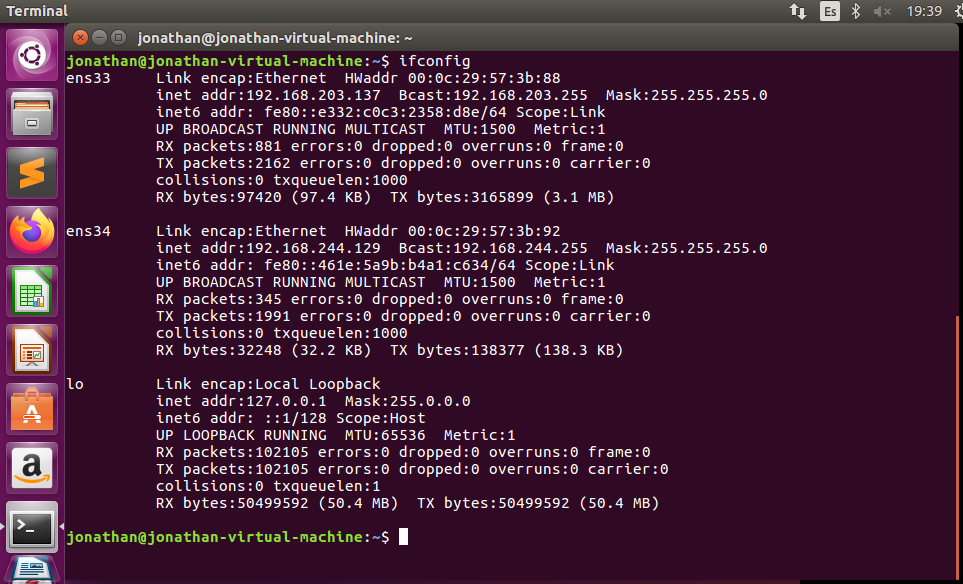
1. Posterior a esto o en paralelo debemos realizar es tener dentro de donde se administraran las maquinas virtuales el “Vmware Work Station”.
2. Luego hacemos doble click y cargamos la maquina virtual de “Graylog\_Unab” y la maquina virtual de “Mail\_Server\_Unab”. Dejamos de que ambos procesos de instalacion y asociación terminen en su totalidad.
3. 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.
4. Posterior a esto, encendemos las 2 maquinas virtuales “Graylog\_Unab” y “Mail\_Server\_Unab”, dejamos de que ambas maquinas finalicen su proceso de encendido.
5. Luego ingresamos a “Graylog\_Unab” a traves del usuario “jonathan”, en donde la password es “Temerac2018”.



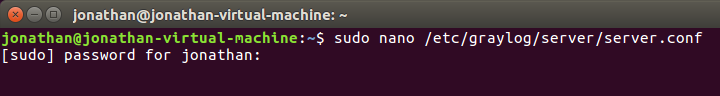
1. Estando dentro de esta abriremos una ventana terminal.



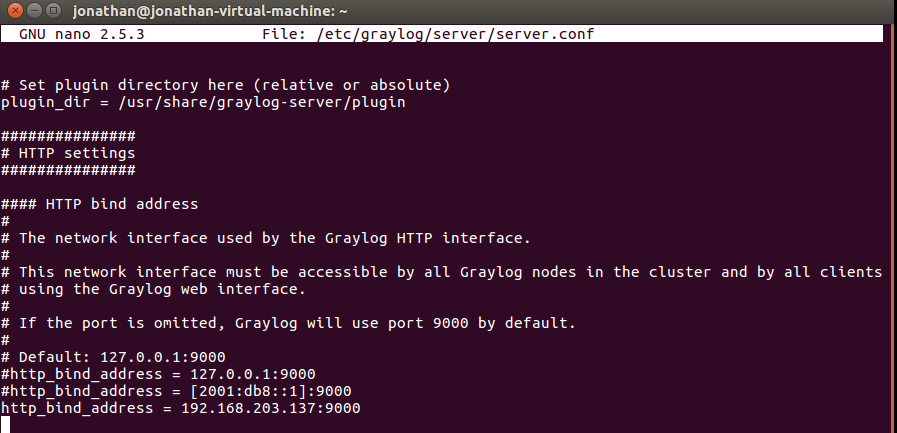
1. A traves del comando “ifconfig” consultamos direccionamiento de red.



1. 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.
2. Postrior a esto nos dirijimos al archivo de configuracion de Graylog, con el siguiente comando # **sudo nano /etc/graylog/server/server.conf.** Ingresaremos nuevamente la pass “Temerac2018”



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

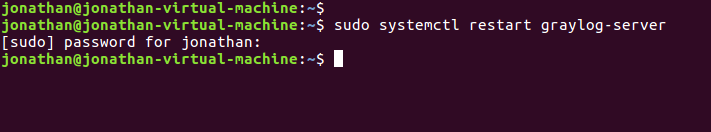


1. Dentro del mismo archivo y con las teclas “ctrl + w” tipeamos “email transport” y enter, llegando a esta seccion del archivo, debemos configurar la misma ip anterior, tal como se ve en la siguiente figura.

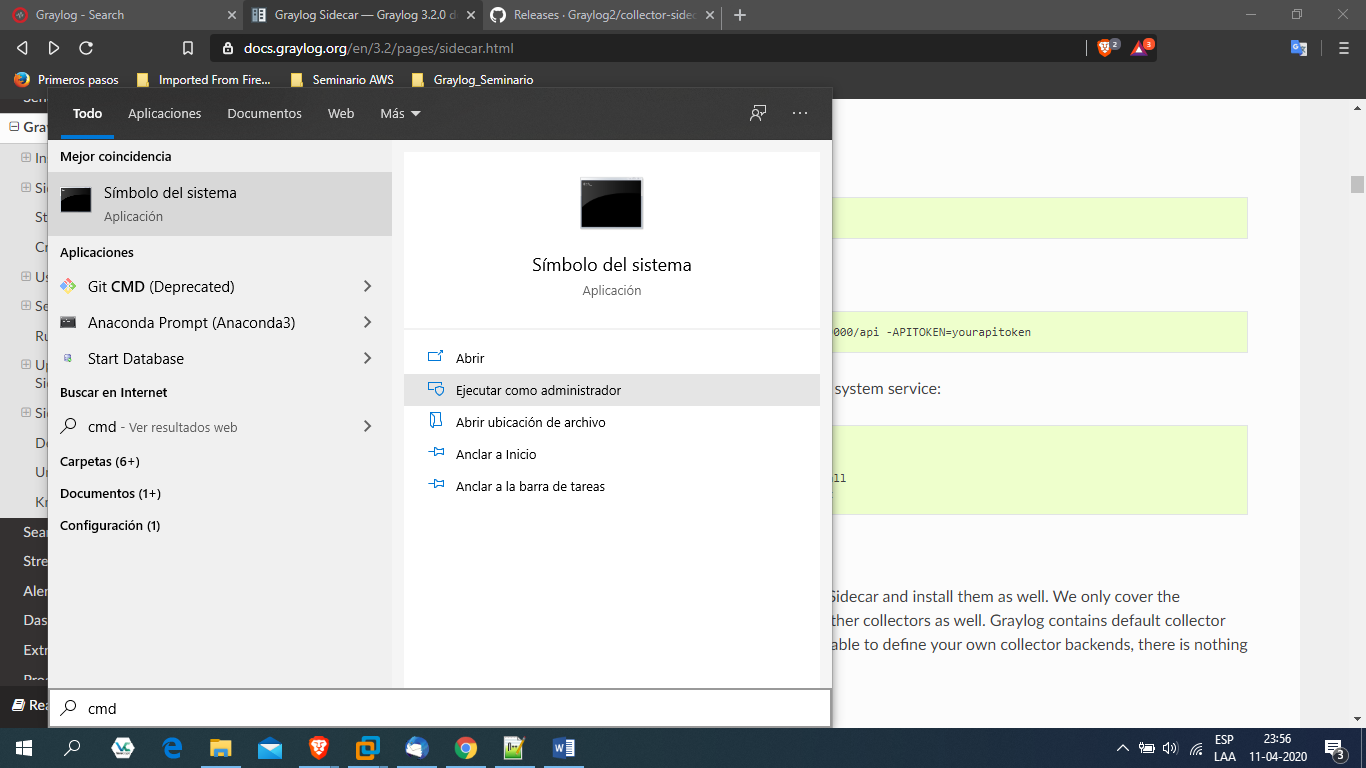


1. En la seccion recien vista del archivo (#Email transport), tambien se efectua la configuracion del servidor de correo (dominio @lab.cl), con el cual se establecera la comunicación, en este caso la configuracion ya esta realizada y solo se debe cambiar la ip de la Uri, de acuerdo a lo solicitado en el pto. 11. Posterior a esto presionamos “ctrl + o” y enter para guardar, luego “ctrl + x” para salir.
2. Posterior a esto reiniciamos el correlacionador, con el comando

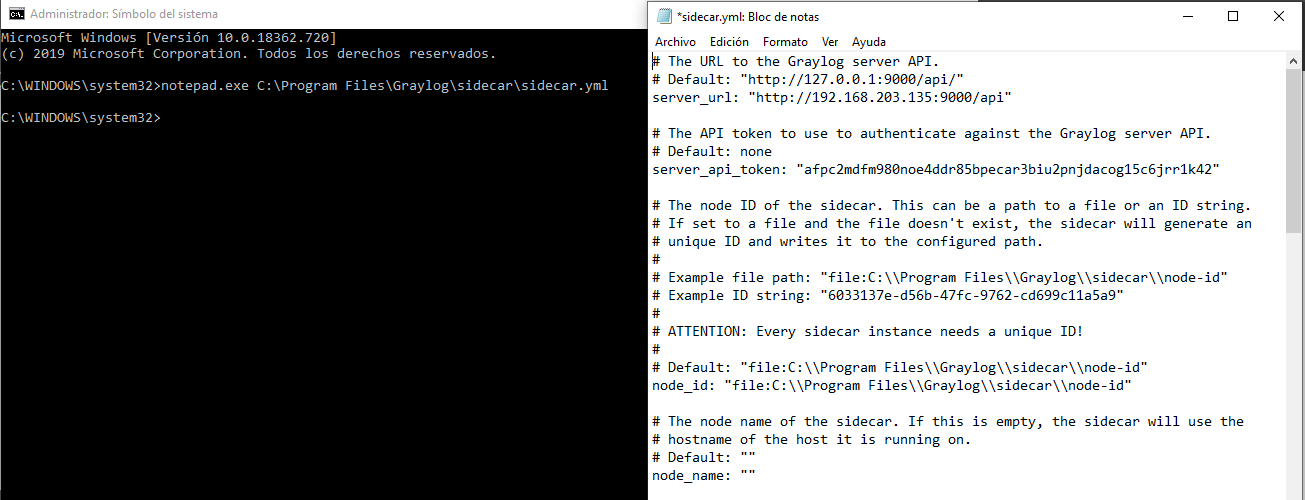
#sudo systemctl restart graylog-server



1. Ahora instalaremos y configuraremos Graylog-Sidecar (agente) en un equipo(s) windows, lo primero que haremos en equipo windows sera ejecutar el archivo **graylog\_sidecar\_installer\_1.0.2-1**, el cual estara junto a las maquinas virtuales, dejamos que el proceso de instalacion termine.
2. Posterior a esto buscamos CMD y lo ejecutamos como “administrador”



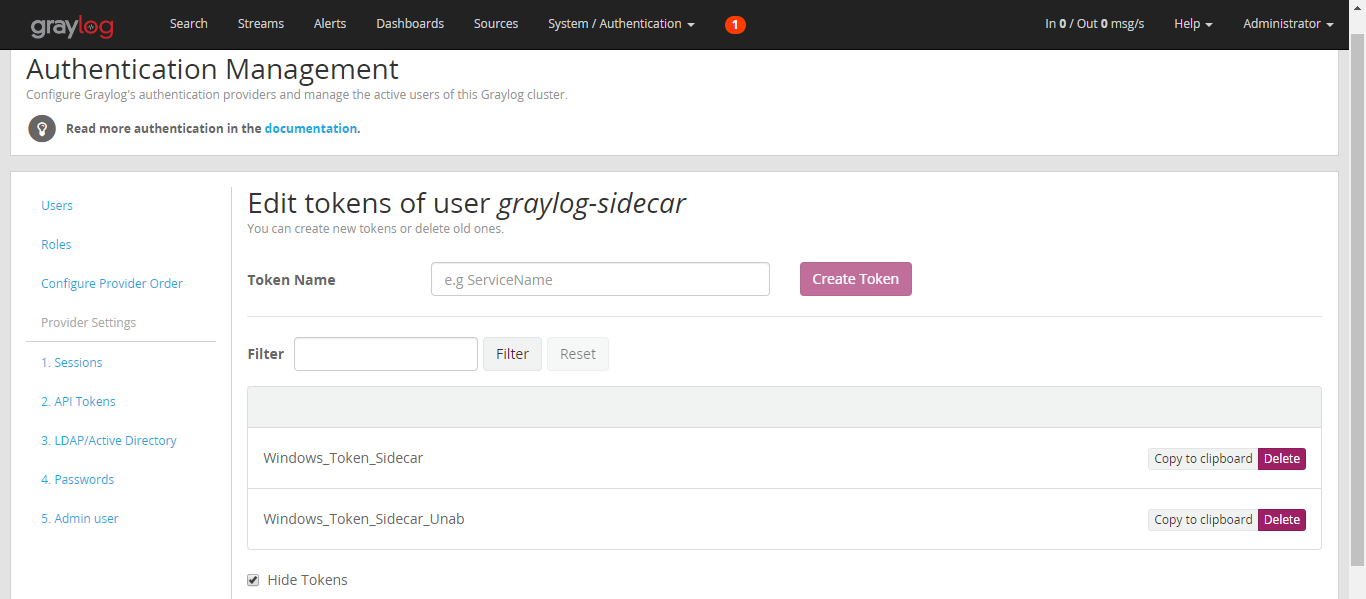
1. Estando dentro de CMD vamos al archivo de configuracion de Graylog-Sidecar, con el siguiente comando **notepad.exe C:\Program Files\Graylog\sidecar\sidecar.yml.** Aquí seteamos la direccion ip de Graylog\_Unab en la linea server\_url: <http://xxx.xxx.xxx.xxx:9000/api>, como aprece en la figura de abajo. Luego “ctrl + g” para guardar y cerramos el archivo.



1. 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 configuracion de Graylog\_Sidecar.

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

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



1. Luego dentro de CMD ejecutamos siguientes comandos:

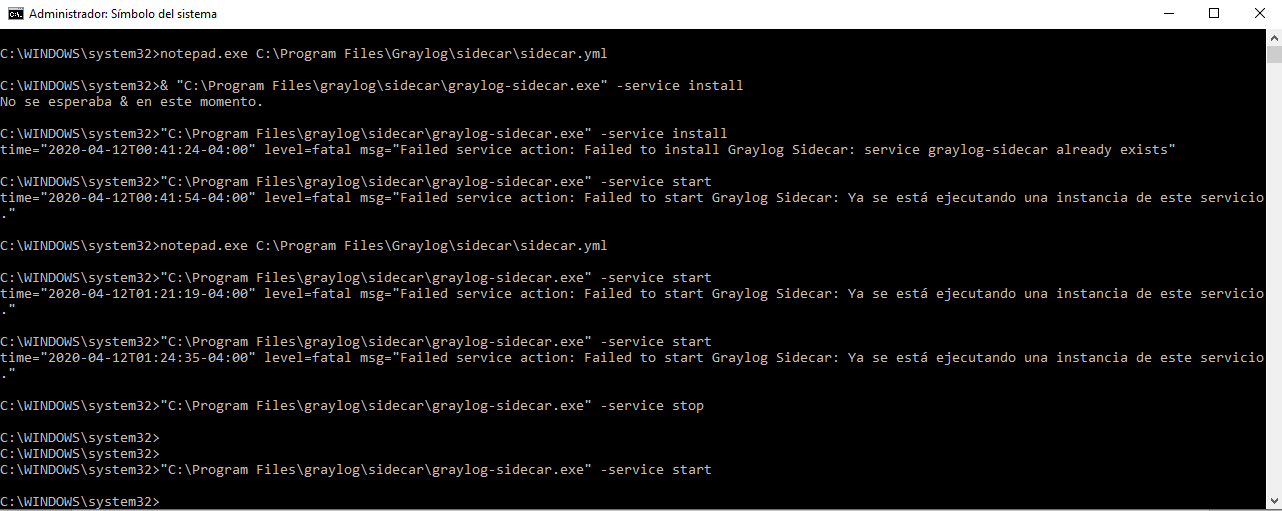
"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service install

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

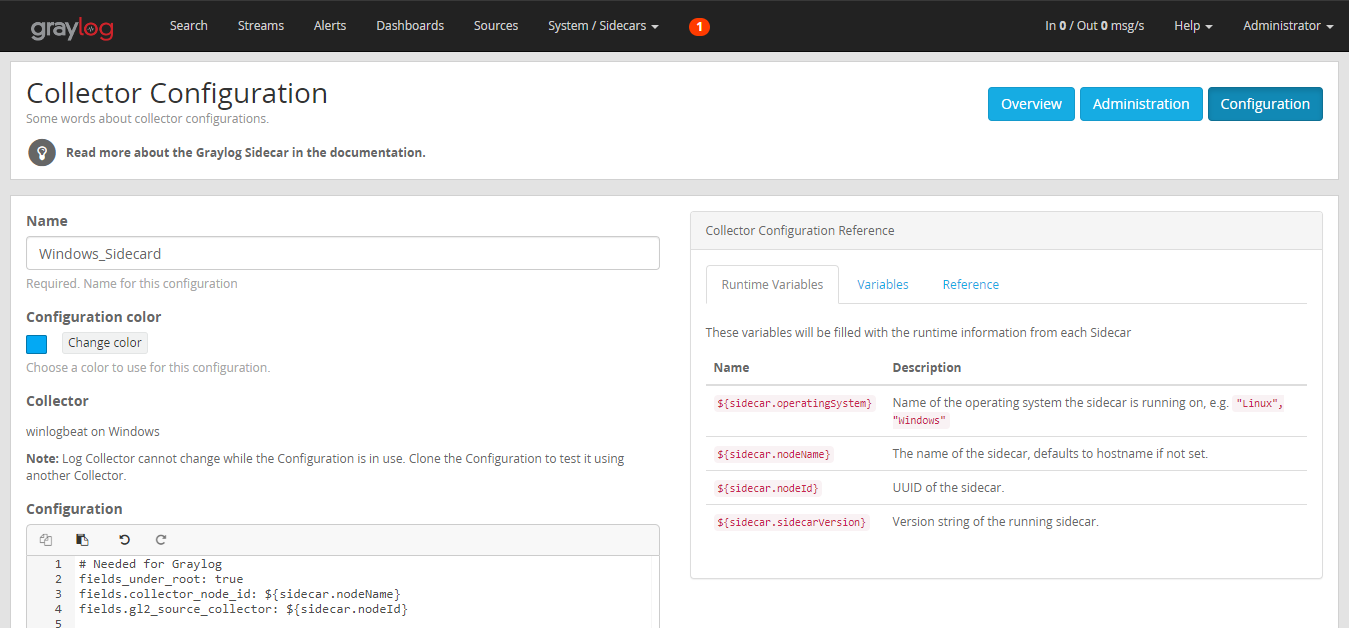
En el caso de que el proceso estuviera corriendo, ejecutamos:

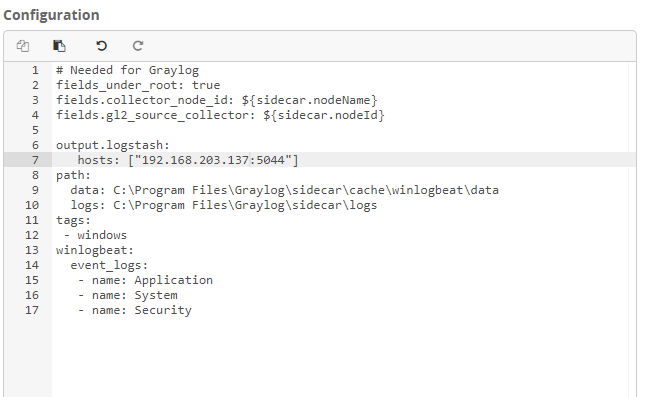
"C:\Program Files\graylog\sidecar\graylog-sidecar.exe" -service stop y luego:

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

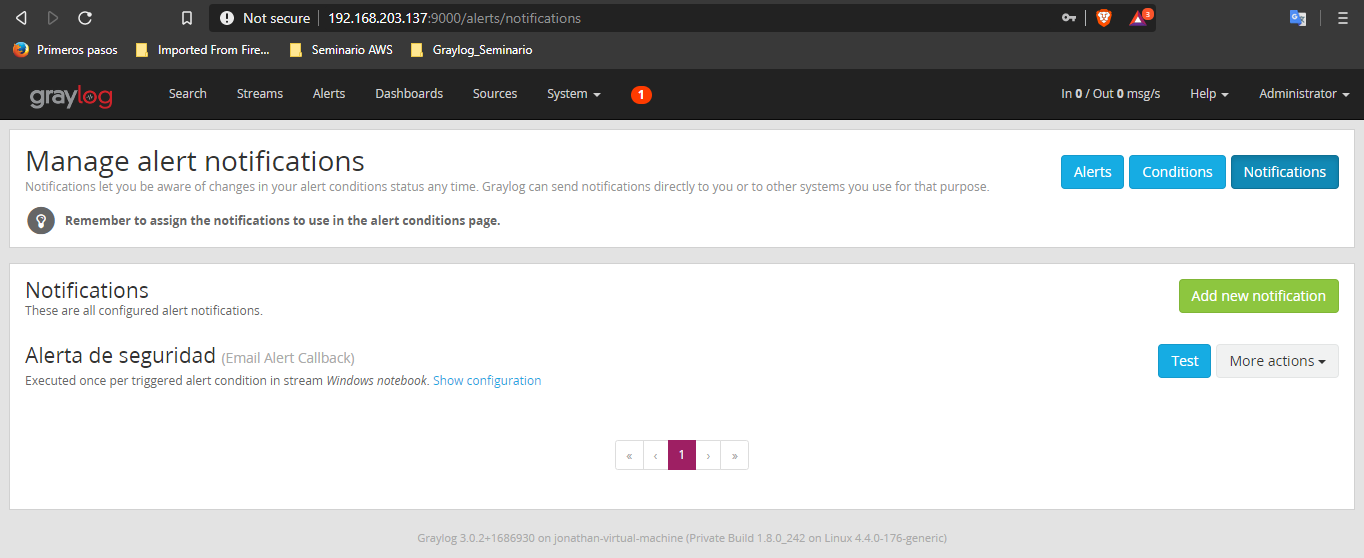


1. Luego ingresamos a Graylog <http://192.168.203.137:9000/> y nos dirimos a System/Sidecard/Configuration y en el archivo de configuracion en host seteamos la ip de Graylog\_Unab, como muestra la figura de abajo (hosts: ["192.168.203.137:5044"]) (en este caso es esa ip).

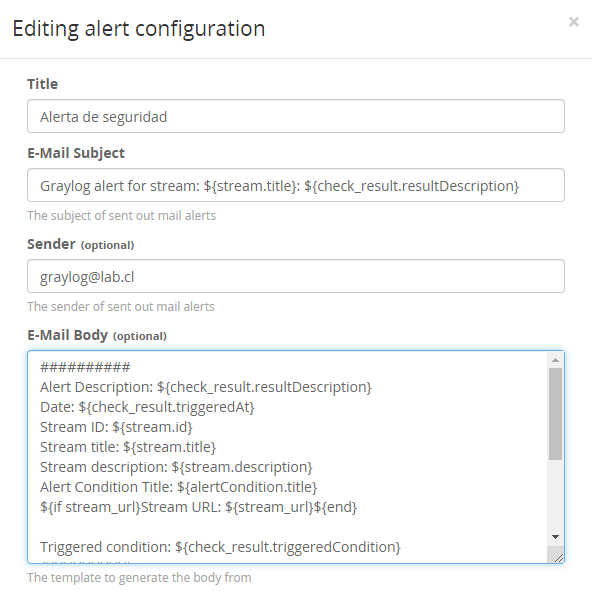


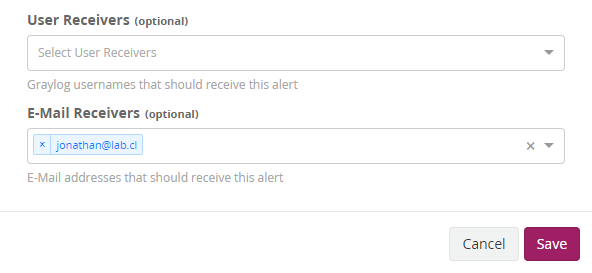


1. Luego abajo le damos “Update”
2. Posterior a estos nos dirigimos a “Alerts”, menu que se encuentra en el panel superior y vamos a “Notifications”, luego en “Alerta de seguridad” le damos click a “More actions” y le damos a “edit”.

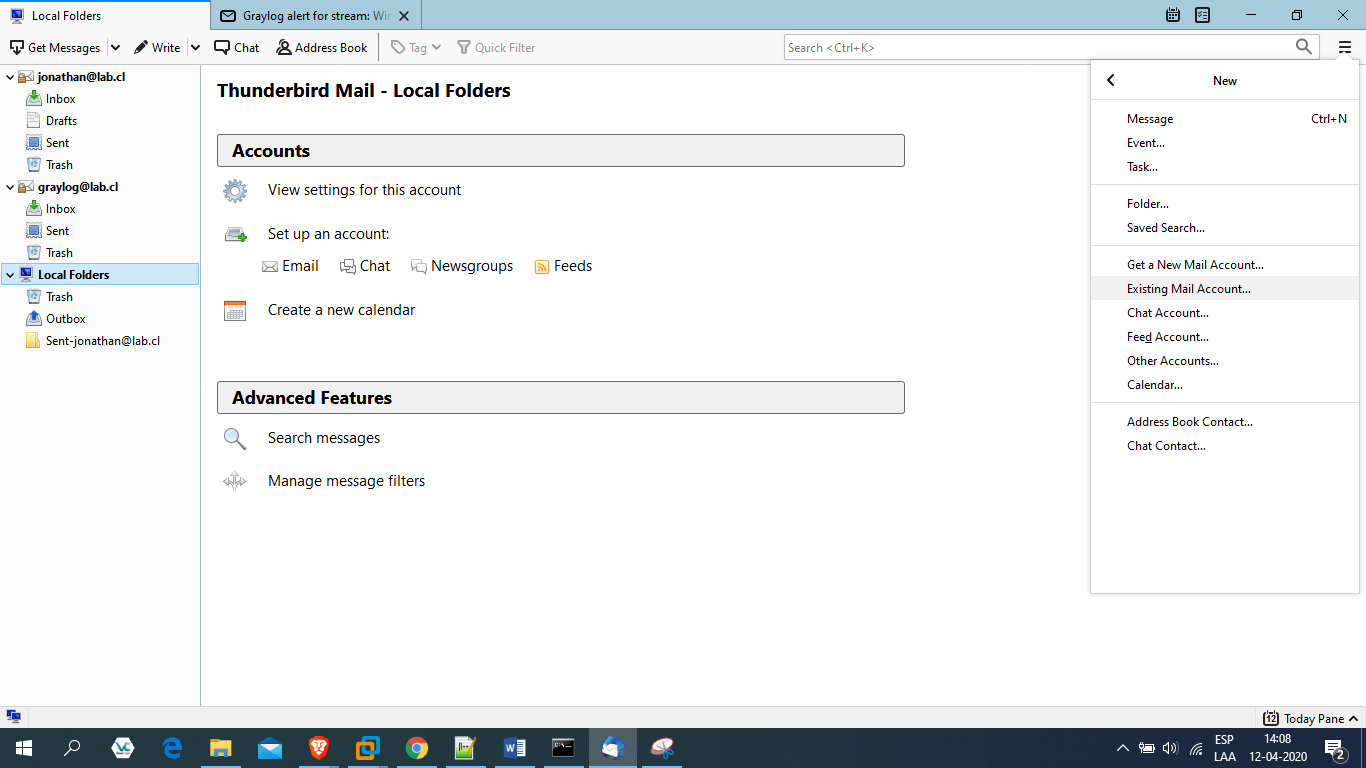


1. Debemos dejar siguiente configuracion, en E-mails receivers dejaremos la cuenta [jonathan@lab.cl](mailto:jonathan@lab.cl) que es el receptor y una de las cuentas configuradas en el servidor de correo “Mail\_Server\_Unab”, le damos “Save” con la cual guardaremos dicha configuracion:





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



Cuenta 1.

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

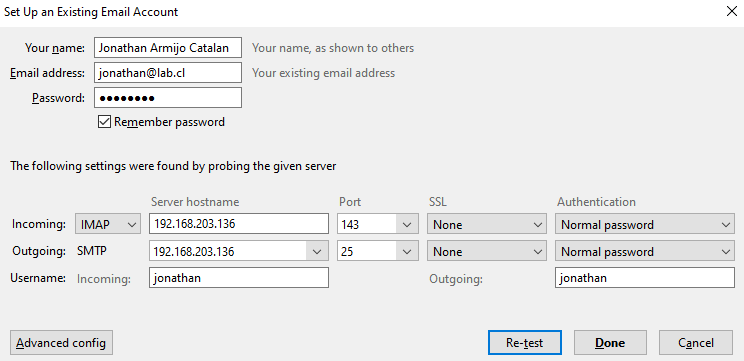
Cuenta 2.

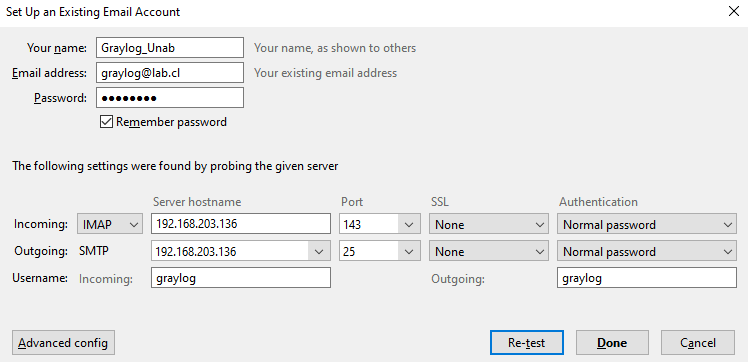
Nombre: [graylog@lab.cl](mailto:graylog@lab.cl)

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

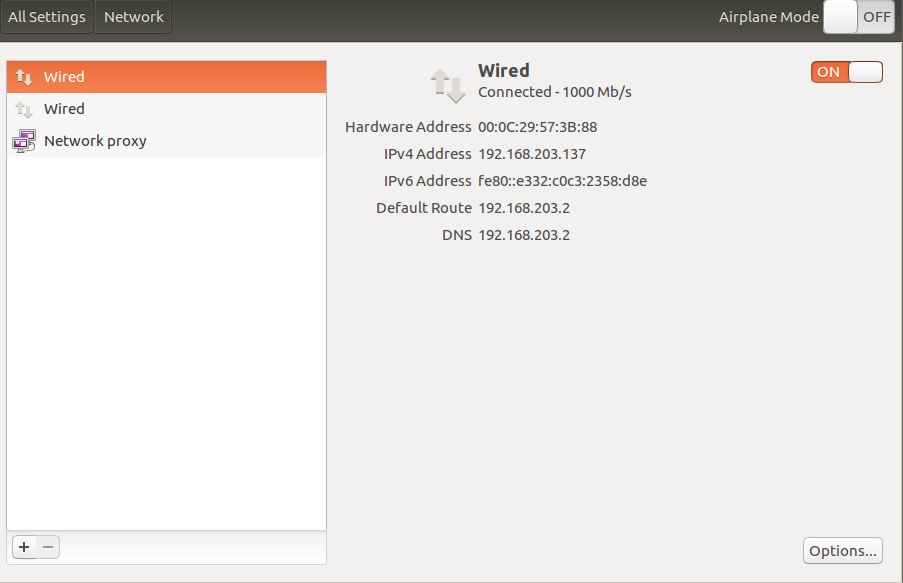
Se debe tener presente para ambas cuentas:

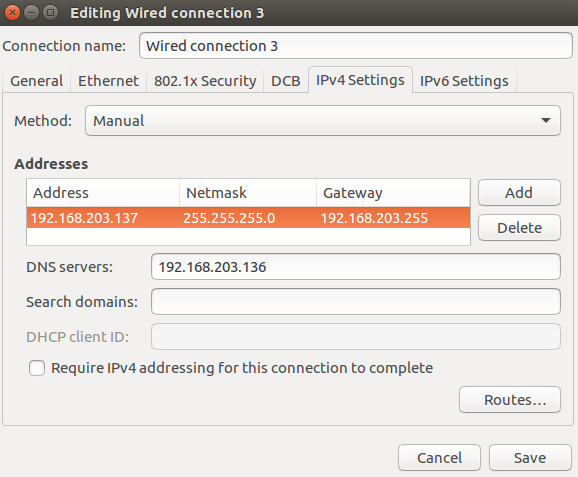
1. Your name: El que desee.
2. Email address: [jonathan@lab.cl](mailto:jonathan@lab.cl) (cuenta 1) y [graylog@lab.cl](mailto:graylog@lab.cl) (cuenta 2).
3. Password: **test2020**
4. Server hostname: Es la direccion ip del servidor de correo “Mail\_Server\_Unab”.
5. Puerto IMAP: 143
6. Puerto SMTP: 25



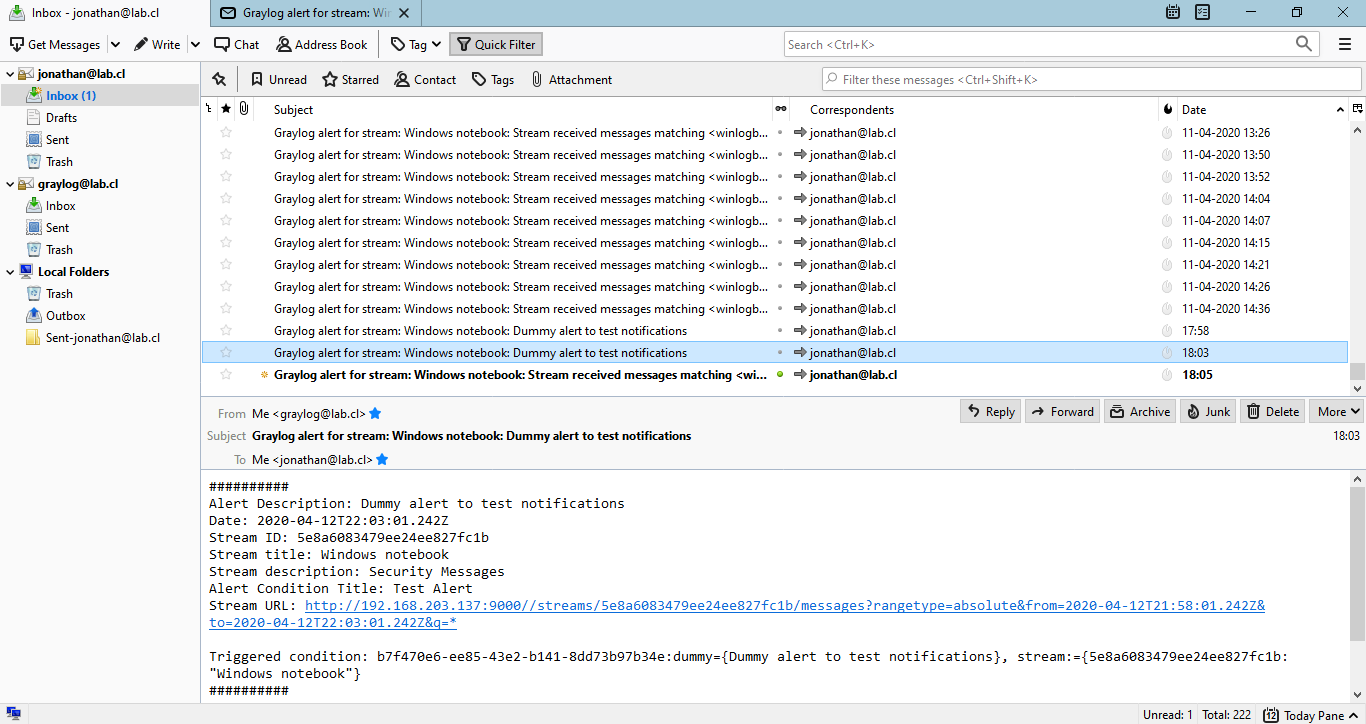


1. Posterior a esto nos vamos a la maquina “Graylog\_Unab” y seteamos como DNS de esta la direccion ip del servidor de correo “Mail\_Server\_Unab”, tambien como se muestar en las figuras siguientes se recomienda dejar direccionamiento IP en “Manual” y setear mismmos datos ya asignados (#ifconfig).

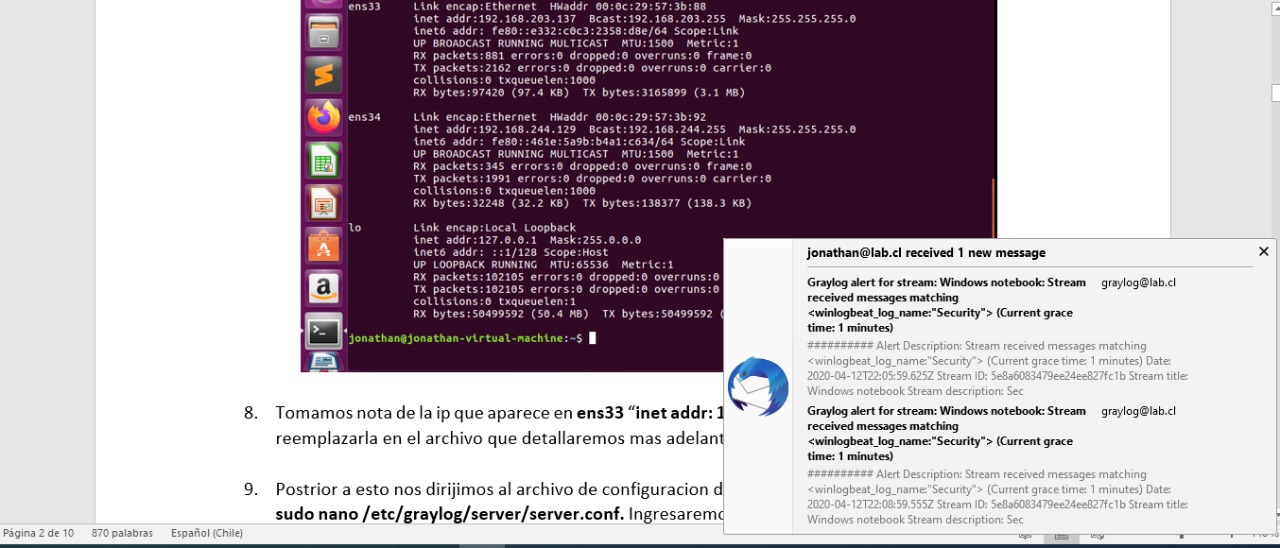




1. Objeto ver si configuracion esta correcta y las alertas (correos) quedaron bien seteados, nos dirigimos a “Alert”, dentro de este nos vamos a “Notifications” y buscamoos la alerta configurada que lleva por nombre “Alerta de Seguridad”, aquí hacemos click en el boton “Test”, si esta todo bien nos debiera 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. Respecto al servidor de correo “Mail\_Server\_Unab”, las credenciales para ingresar son las siguientes:

User: root

Pass: test

User:test

Pass:test

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

