Instalación y Configuración de Icinga

Alumnos:
Esteban Cicovich
Leonardo Di Carlo
Nicolas Falcón

Profesor:
Jose Luis Di Biase

Indice

¿Que es Icinga?

Instalación

Configuración

Problemas

¿Que es Icinga?

Una curiosidad de la aplicación es su nombre, “Icinga” proviene del Zulú y significar “el que busca” o “el que examina”.

Icinga es un sistema de monitoreo para redes, servidores y aplicaciones, de una forma segura y confiable. Lo que nos permite mantenernos al tanto de los problemas de nuestra estructura.

Es un sistema Open source,impulsado por la Fundación Icinga, derivado de Nagios (uno de los sistemas de monitoreo más usado) del cual utiliza el nagios remote plugin executor (nrpe).

Notifica al usuario los errores, las recuperaciones y genera el rendimiento de la información para la creación de los informes.
Escalable y extensible, Icinga puede monitorear grandes entornos complejos a través de su interfaz gráfica.

Permite tener un control detallado de la topología de red de nuestra empresa, provee muchos recursos que facilitan el mejor control de los host de una red, etc. Nos permite obtener información sobre los servicios que se estén ejecutando en un servidor específico, así también como el estado de las particiones de los mismos.

Uno de los fuertes de esta aplicación es su alto grado de configuración, tanto de las evaluaciones que efectúa sobre los equipos como las acciones consecuentes de la respuestas de los mismos. Icinga permite la interacción con aplicaciones instaladas en el equipo. Esto significa a nivel funcional que no se limita a las funcionalidades provistas por defecto ni la dependencia de actualizaciones o plugins para ampliarlas.

Características principales:

- Monitorización de servicios de red (Ej: SMTP, POP3, HTTP, NTP, ping, ...)
- Monitorización de componentes de red (hosts, servers, switches, routers, etcétera)
- Notificación visual del estado de los servicios.
- Alertas configurables (EMail, SMS, llamada telefónica, ...)
- Dos interfaces web opciones (Icinga Clasic UI e Icinga Web)

Instalación

Primero agregaremos el link del repositorio a nuestro listado de fuentes. Para esto abrimos el archivo en cuestión con algun editor de texto:

```
# nano /etc/apt/sources.list
```

o

```
# sudo gedit /etc/apt/sources.list
```

Y agregamos los enlaces:

```
deb http://ppa.launchpad.net/formorer/icinga/ubuntu xenial main
deb-src http://ppa.launchpad.net/formorer/icinga/ubuntu xenial
main
```

Luego desde el terminal agregamos la clave pública del repositorio:

```
# gpg --keyserver keyserver.ubuntu.com --recv-keys 36862847
# gpg --export --armor 36862847 | sudo apt-key add -
```

A continuación actualizaremos apt

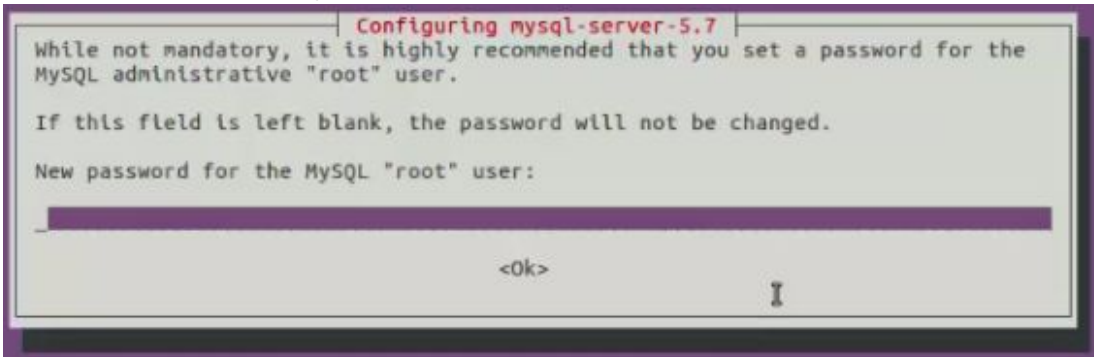
```
# sudo apt-get update
```

Ahora instalamos Icinga y sus dependencias

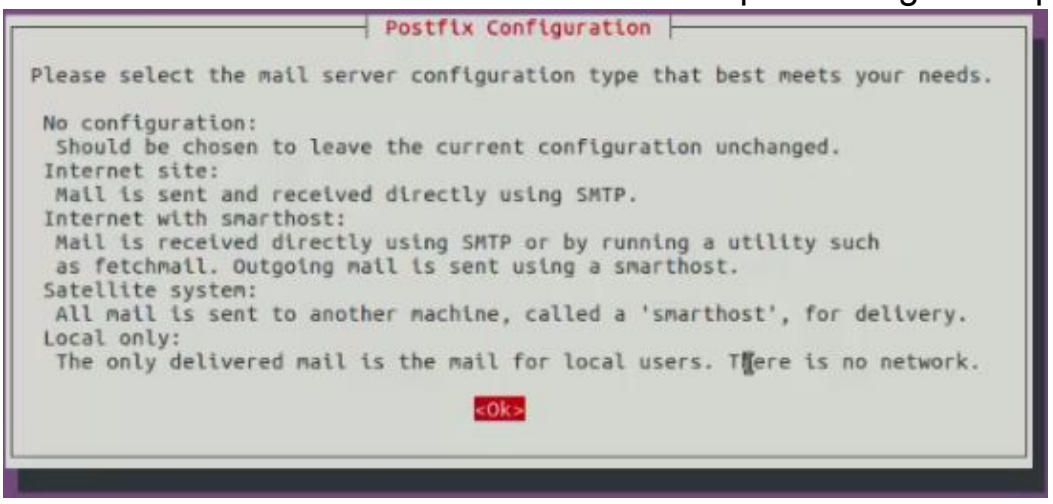
```
# sudo apt-get install icinga icinga-doc icinga-idoutils
mysql-server libdbd-mysql mysql-client
```

Durante la instalación se solicita la configuracion necesaria para poder dejar funcional la aplicacion una vez concluido el proceso.

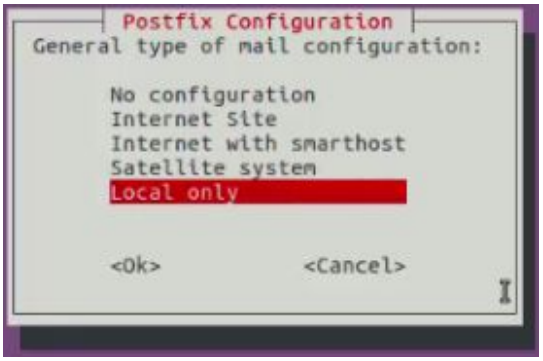
Lo primero que se nos pide es estableceremos la contraseña del usuario “root” de mysql:



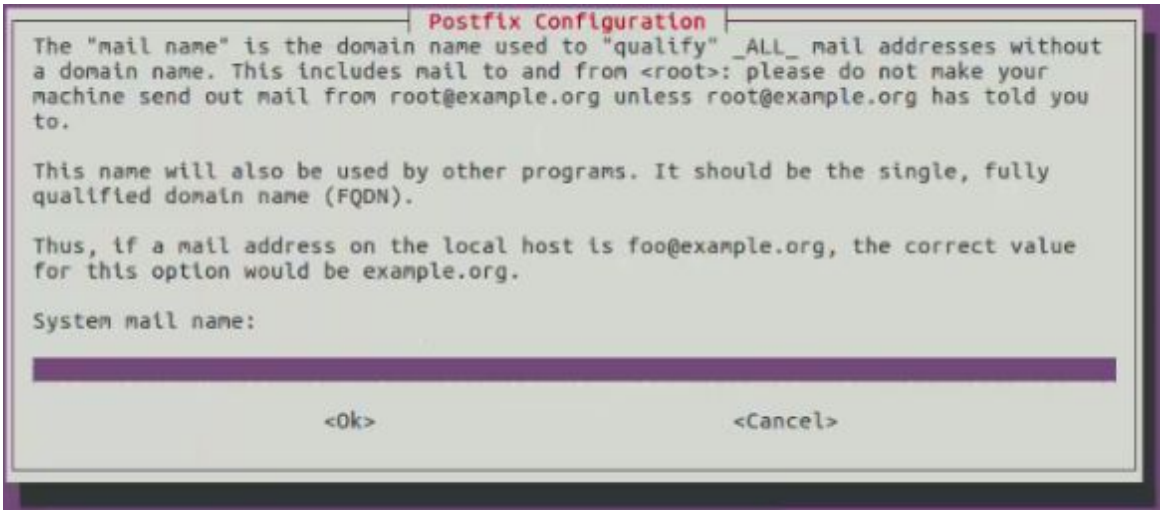
Una vez confirmada nuestra elección se nos pide configurar el postfix.



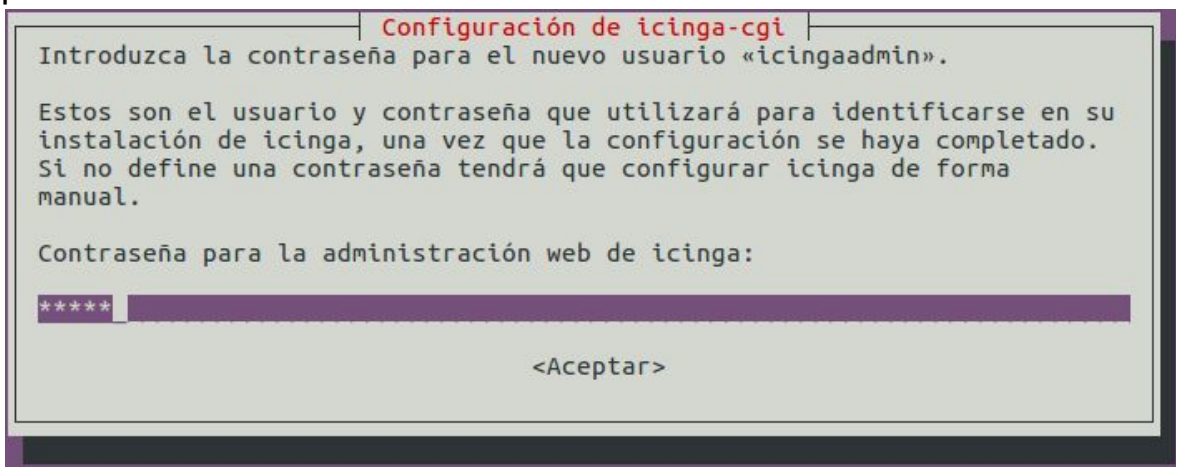
Inicialmente nuestra elección fue “Local only” para investigar un poco más esta opción una vez nos enfoquemos en las notificaciones por EMail.



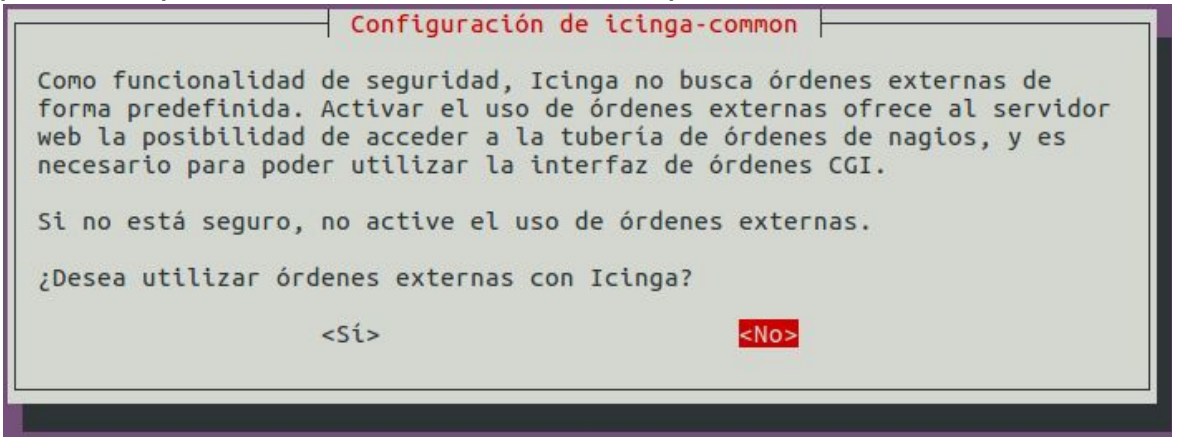
Ingresamos el dominio de mail que mas adelante configuraremos en el sistema.



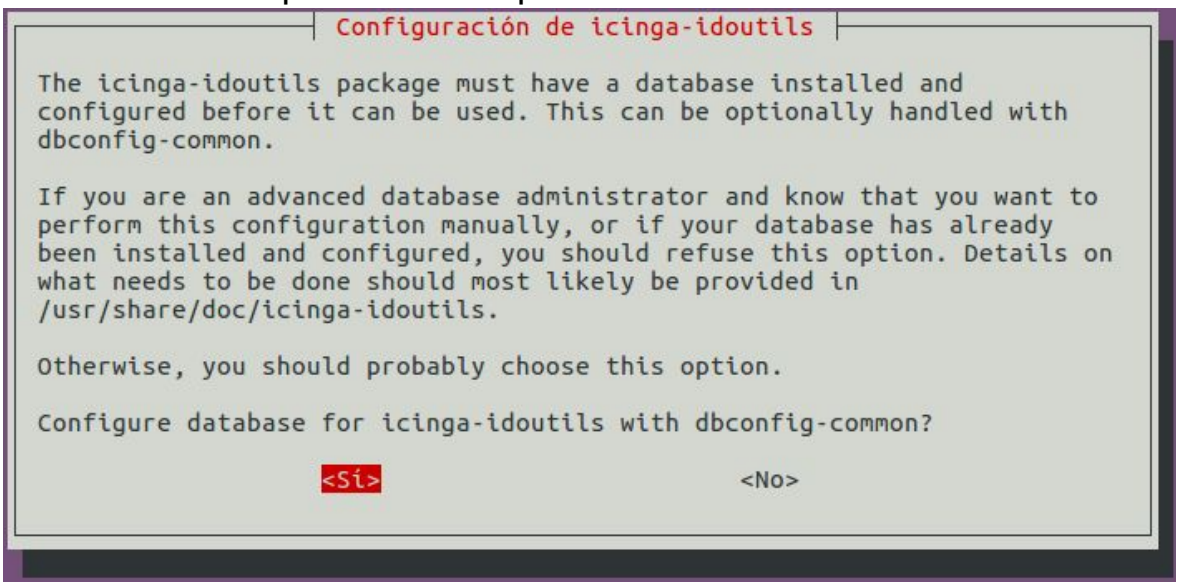
Para ingresar y configurar Icinga, agregamos una contraseña al usuario “icingaadmin” que es el usuario con permisos administrativos designado por defecto.



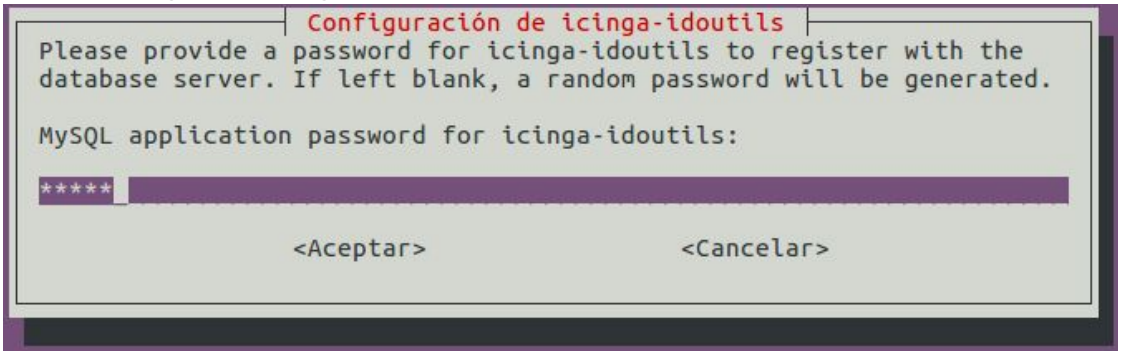
En este punto se nos pide decidir sobre la comunicación con comandos externos. Al igual que en la configuración del Postfix, no habilitamos los permisos para esta funcionalidad hasta que necesitaramos usarla.



La instalación ofrece una configuración automática de la conección con la base de datos para usuarios primerizos.



A continuación configuramos la contraseña de mysql que se utilizara para configurar icinga-idoutils en la base de datos.



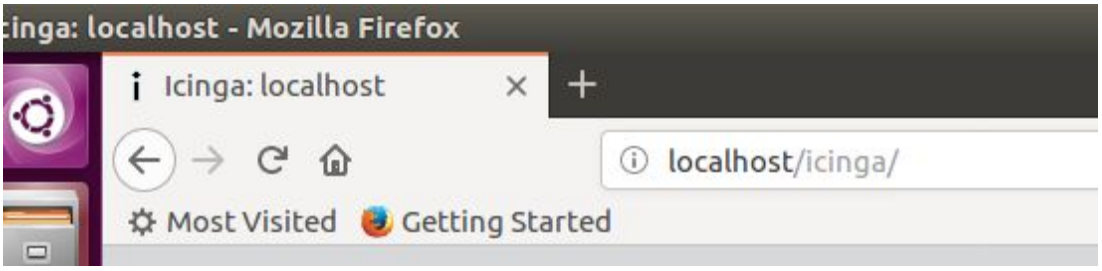
Reiniciamos el servicio de Icinga, Apache y Mysql

```
# sudo service icinga restart
# sudo service apache2 restart
# sudo service mysql restart
```

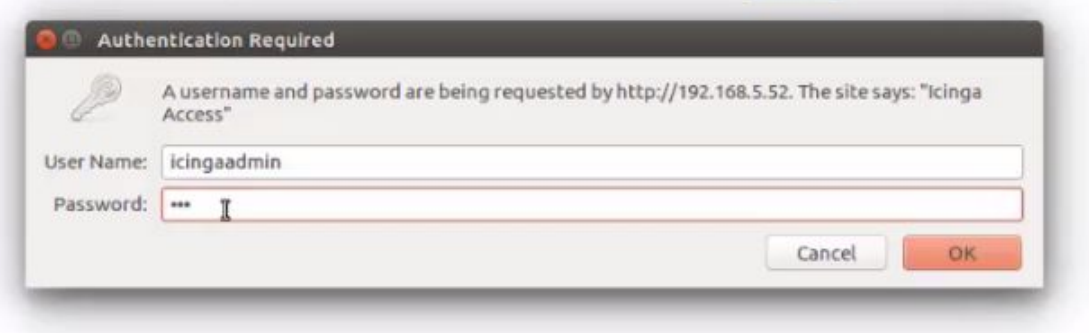
Revisamos que Icinga este en ejecucion y funcional con el siguiente comando:

```
# service icinga status
```

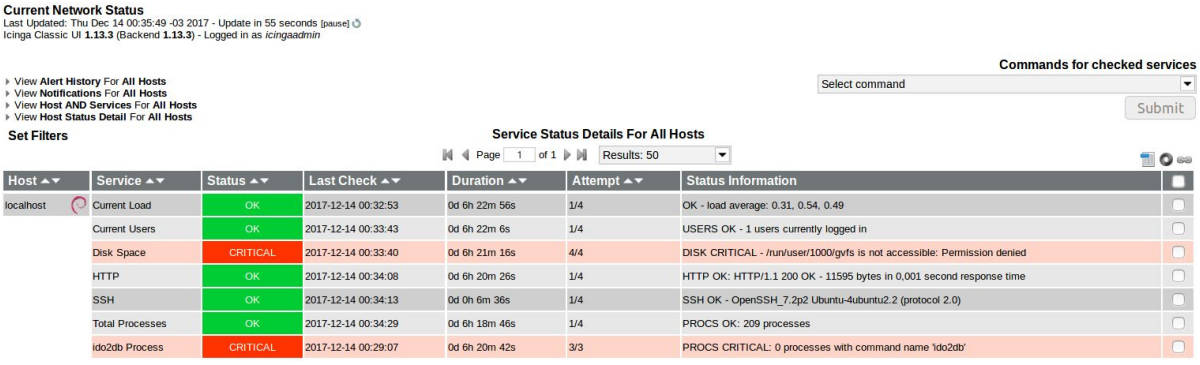
Abrimos nuestro navegador y tipeamos http://localhost/Icinga para visualizar la interfaz de usuario que instalamos.



Ingresamos el nombre de usuario y contraseña que configuramos durante la instalacion.



El asistente de Icinga nos aparece de la siguiente manera



Current Network Status
Last Updated: Thu Dec 14 00:35:49 -03 2017 - Update in 55 seconds [pause]
Icinga Classic UI **1.13.3** (Backend **1.13.3**) - Logged in as *icingaadmin*

- View **Alert History** For **All Hosts**
- View **Notifications** For **All Hosts**
- View **Host AND Services** For **All Hosts**
- View **Host Status Detail** For **All Hosts**

Commands for checked services
Select command
Submit

Set Filters

Service Status Details For All Hosts

Page 1 of 1 Results: 50

Host	Service	Status	Last Check	Duration	Attempt	Status Information
localhost	Current Load	OK	2017-12-14 00:32:53	0d 6h 22m 56s	1/4	OK - load average: 0.31, 0.54, 0.49
	Current Users	OK	2017-12-14 00:33:43	0d 6h 22m 6s	1/4	USERS OK - 1 users currently logged in
	Disk Space	CRITICAL	2017-12-14 00:33:40	0d 6h 21m 16s	4/4	DISK CRITICAL - /run/user/1000/gvfs is not accessible: Permission denied
	HTTP	OK	2017-12-14 00:34:08	0d 6h 20m 26s	1/4	HTTP OK: HTTP/1.1 200 OK - 11595 bytes in 0,001 second response time
	SSH	OK	2017-12-14 00:34:13	0d 0h 6m 36s	1/4	SSH OK - OpenSSH_7.2p2 Ubuntu-4ubuntu2.2 (protocol 2.0)
	Total Processes	OK	2017-12-14 00:34:29	0d 6h 18m 46s	1/4	PROCS OK: 209 processes
	ido2db Process	CRITICAL	2017-12-14 00:29:07	0d 6h 20m 42s	3/3	PROCS CRITICAL: 0 processes with command name 'ido2db'

Configuración

La configuración de los equipos definidos y las evaluaciones en cuestión se definieron en “/etc/icinga/objects/configuracion.cfg”. Las pruebas las realizamos definiendo un equipo en la red a la que nos encontrábamos conectados. Luego se definieron los tests de ciertos servicio que estábamos interesados en evaluar para dicho equipo. Para solucionar uno de los problemas presentados en la ejecución del test de espacio en disco tuvimos que redefinir el comando definido por defecto en la aplicación. Esto originalmente nos limitó en el avance de los otros objetivos pero nos permitió aclarar un poco más el comportamiento de la aplicación.

Una vez que estuvimos satisfechos con los tests iniciales nos conectamos en la configuración de las notificaciones vía EMail de las alertas. Para esto definimos un grupo de contactos al que se alertará en caso de que se dispare alguno de los eventos mencionados. En la configuracion del contacto se puede especificar que eventos se notificaran para cada servicio al que se lo asocie. Los eventos pueden ser la desconeccion del equipo, warning, critical, restablecimiento, entre otros. Además se define el comando que se ejecutara cuando se dispare alguno de estos eventos.

Para las notificaciones por EMail fue necesaria la definición de un nuevo comando que interactuara con el programa “mailx”. Este comando es el que se asociará al contacto para completar la notificación.

Se adjunta una copia del contenido del archivo definido por el grupo:

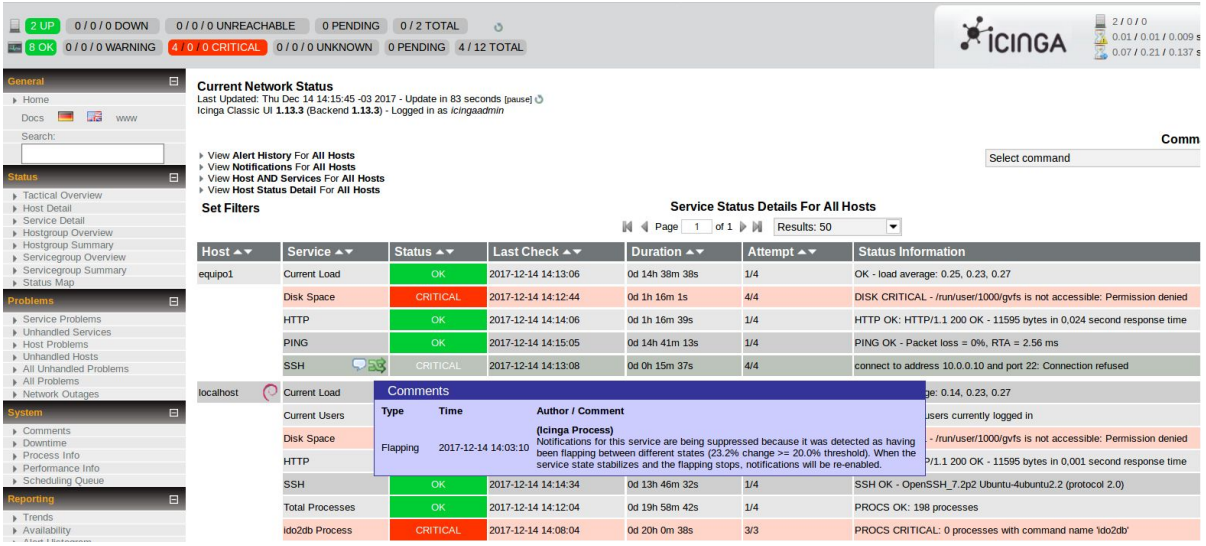
```
define host {
     use                     generic-host
     host_name               equipo1
     alias                   PC-Esteban
     address                 10.0.0.3
}
# PING
define service {
     use                     generic-service
     host_name               equipo1
     service_description     PING
     check_command           check_ping!100.0,20%!500.0,60%
     notifications_enabled   1
}
```

```
# HTTP
define service {
     use                        generic-service
     host_name                  equipo1
     service_description        HTTP
     check_command              check_http
     notifications_enabled   1
}
# SSH
define service {
     use                        generic-service
     host_name                  equipo1
     service_description        SSH
     check_command              check_ssh
     notifications_enabled   1
     contacts                   admins
}
# Espacio en Disco
define service {
     use                        generic-service
     host_name                  equipo1
     service_description        Disk Space
     check_command              check_all_disks_plus!20%!10%
}

define contact {
     contact_name                    admins
     host_notifications_enabled      1
     host_notification_period        24x7
     host_notification_options       d,u,r
     host_notification_commands      notificacion-email
     service_notifications_enabled     1
     service_notification_period     24x7
     service_notification_options    w,u,c,r
     service_notification_commands     notificacion-email
     email                           estebancicovich@gmail.com
}

# definicion del comando “notificacion-email”
define command {
     command_name   notificacion-email
     command_line   echo "***** Nagios Monitor XI Alert
*****\n\n \
           Notification Type: $NOTIFICATIONTYPE$\nHost:
$HOSTNAME$\n \
           State: $HOSTSTATE$\n \
           Address: $HOSTADDRESS$\n \
           Info: $HOSTOUTPUT$\n\n \
```

```
            Date/Time: $LONGDATETIME$\n" | /bin/mailx -v -s "**
$NOTIFICATIONTYPE$ Host Alert: $HOSTNAME$ is $HOSTSTATE$ **
(C)" -S smtp=[smtp.gmail.com]:587 -S
from=estebancicovich@gmail.com $CONTACTEMAIL$
}

define command {
    command_name    check_all_disks_plus
    command_line    /usr/lib/nagios/plugins/check_disk -w
$ARG1$ -c $ARG2$ -e -u GB -A -i .gvfs
}
```

Pudimos lograr que se disparara el comando de notificación pero por falta de configuracion de postfix no logramos recibir un correo para demostrarlo. Sin embargo en el log de eventos se evidenciaba la ejecución del comando.

Para hacer algunas pruebas sobre los tests definidos habilitamos y deshabilitamos servicios como ssh repetidamente, esto ocasionó que se marcara al mismo como “flapping”.



Problemas

- Nos encontramos con algunos inconvenientes como por ejemplo un bug que no permite la visualización correcta del espacio en disco, algo que resolvimos incorporando unas lineas de codigo que evitan el monitoreo gvfs sobre el servicio de discos.
- Al ser un branch de nagios, la mayoría de las ayudas y foros se expiden sobre este, por lo tanto hay menos información directa de icinga.
- La instalación del sistema en el equipo de uno de los compañeros resultó distinta a la de los otros 2. El problema se debió a la falta de inserción de las claves publicar para la validación de autenticidad del repositorio haciendo que algunos de los componentes no se instalara.
- El mayor problema encontrado fue la configuración de las notificaciones por correo. Si bien la documentación provee detalle de su configuración, esta depende de la instalación en el ordenador de un sistema de transferencia de correos. Para esto nos decidimos por instalar Postfix pero por inexperiencia y falta de tiempo no logramos configurarlo correctamente.