monitorización, linux, logwatch, logcheck, snoopy, logs

Programas Monitorización

Existen varias alternativas para el monitoreo de servidores, pero si sólo queremos una simple monitorización del equipo podemos usar logwatch, logcheck y snoopy.

logcheck

es una utilidad que revisa los logs del sistema y genera un reporte, eliminando las entradas que son normales en un sistema (ejecuciones de cron, por ejemplo) para mostrar únicamente aquellas sospechosas.

snoopy

es una librería que funciona como wrapper del execve() de libc, para guardar un registro de todos los comandos ejecutados en el sistema, un .bash_history que no puede ser modificado o borrado por el usuario.

Un problema de tener estas dos utilidades corriendo es que snoopy va a guardar el registro de los comandos ejecutados por logcheck cuando parsea los logs, formando un circulo vicioso que terminara generando un reporte con las acciones de logcheck, ¡marcadas como alertas!. En palabras cristianas, un email de 500k con información repetida.

La solución es crear los archivos /etc/logcheck/ignore.d.server/snoopy y /etc/logcheck/violations.ignore.d/snoopy con esta línea (probado y usado en Debian GNU/Linux):

```
^\w{3} [ :0-9]{11} [._[:alnum:]-]+ snoopy.*uid\:109.*
```

El mismo esquema se puede usar para pasar por alto diferentes comandos del sistema, como sendmail y procmail, que generalmente son bastante comunes. Para validar que las expresiones regulares nos funcionen, se puede usar el útil grep o la página Rex V

LogWatch

es una utilidad que nos permite analizar los logs de un sistema Linux. En centos viene instalado por defecto, en caso contrario.

Para instalarlo

```
yum install logwatch
```



requiere usar el repositorio de rpmforge

configuración en /usr/share/logwatch/default.conf/logwatch.conf.

Por ejemplo podemos cambiar el nivel de detalle y el correo

```
Detail = High
MailFrom = micorreo@midominio.com
MailTo = root  updates to MailTo = administrador@midominio.com
```

Para verificar que todo funciona correctamente

```
    # logwatch --logfile secure --detail high --mailto
micorreo@midominio.com --range yesterday
```

Para que logwatch envíe correos con los resúmenes podemos utilizar por ejemplo nail o ssmtp

con nail

```
yum install nail
```

Editar /etc/nail.rc y colocar

```
set smtp=smtp://miservidorsmtp.com
```

Editar /etc/logwatch/conf/logwatch.conf y poner

```
mailer = /usr/bin/nail -t
MailTo = monitorcn en xxxxx.com.co
MailFrom = template_vm
MailSubject= "Logwatch for serverxxxx"
Range = yesterday
Detail = med
```

Con ssmtp

```
yum install ssmtp
```

```
vim /etc/ssmtp/ssmtp.conf
```

Y configurar la siguiente información:

```
  root=micorreo@midominio.com
```

```
  mailhub=miservidor.pop3.com
  rewriteDomain=midominio.com
  hostname=midominio.com
  FromLineOverride=YES // Necesario para re-escribir la cabecera From: de
nuestro correo
  AuthUser=MiUsuarioDeCorreo
  AuthPass=MiPassword
```

Para enviar un correo de prueba usando ssmtp

```
  cat - | /usr/sbin/ssmtp -v micorreo@midominio.com
```

Referencias

- http://lists.centos.org/pipermail/centos-es/2010-January/006852.html
- http://www.sisfo.com/blog/2009/08/usando-logwatch-para-recibir-informacion-de-nuestros-servidores/
- http://www.sisfo.com/blog/tag/sysadmin/

From:
https://wiki.intrusos.info/ - **LCWIKI**

Permanent link:
https://wiki.intrusos.info/doku.php?id=seguridad:monitorizacion

Last update: **182023/01/ 13:11**