Lesson 3 (of 11)

10.3 Revisión de archivos Syslog

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder interpretar las entradas en los archivos syslog correspondientes para solucionar problemas o revisar el estado del sistema.

Revisión de archivos Syslog

Muchos programas usan el protocolo *syslog* para registrar eventos en el sistema. Cada mensaje se clasifica por facility (tipo de mensaje) y prioridad (gravedad del mensaje). Los facilities que están disponibles se documentan en la página de manual `rsyslog.conf`(5).

Las ocho prioridades también se estandarizan y clasifican de la siguiente manera:

Descripción general de las prioridades de syslog

Código	Prioridad	Gravedad
0	emerg	El sistema no se puede usar.

Código	Prioridad	Gravedad
1	alert	Se debe implementar una acción de inmediato.
2	crit	Condiciones críticas.
3	err	Condición de error no crítica.
4	warning	Advertencia.
5	notice	Evento normal pero importante.
6	info	Evento informativo.
7	debug	Mensaje de nivel de depuración.

El servicio rsyslogd usa el facility y la priority de los mensajes de registro para determinar cómo resolverlos. Esto se configura mediante el archivo `/etc/rsyslog.conf` y los archivos `*.conf` de `/etc/rsyslog.d`. Los programas y los administradores pueden cambiar la configuración de **rsyslogd** de tal manera que no pueda sobrescribirse con las actualizaciones de **rsyslog** mediante la inclusión de archivos personalizados que tienen el sufijo .conf en el directorio `/etc/rsyslog.d`.

En la sección `#### RULES ####` de `/etc/rsyslog.conf`, se incluyen directivas que definen dónde se almacenan los mensajes de registro. En el lado izquierdo de cada línea, se indican el facility y la gravedad del mensaje de registro que se corresponde con la directiva. El archivo rsyslog.conf puede contener el carácter * como comodín en los campos de facility y gravedad, donde es válido para todos los facilities o todas las gravedades. En el lado derecho de cada línea, se indica en qué archivo se debe guardar el mensaje de registro. Generalmente, los mensajes de registro se guardan en archivos ubicados en el directorio `/var/log`.

nota

Los archivos de registro son conservados por el servicio **rsyslog** y el directorio `/var/log` contiene una variedad de archivos de registro específica para determinados servicios. Por ejemplo, el servidor web Apache o Samba generan sus propios archivos de registro en el subdirectorio correspondiente del directorio `/var/log`.

Un mensaje manejado por **rsyslog** puede aparecer en varios archivos de registro diferentes. Para evitar eso, el campo de gravedad puede configurarse como **none**, que significa que ninguno de los mensajes dirigidos hacia este facility se agregan al archivo de registro especificado.

En lugar de registrar mensajes de syslog en un archivo, pueden imprimirse en las terminales de todos los usuarios que hayan iniciado sesión. En el archivo `rsyslog.conf` predeterminado, esto se hace para todos los mensajes que tienen la prioridad "emerg".

Sección de reglas de muestra de `rsyslog.conf`

```
#### RULES ####
# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                 /dev/console
# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none        /var/log/messages
# The authpriv file has restricted access.
authpriv.*                              /var/log/secure
```

```
# Log all the mail messages in one place.
mail.*                                  -/var/log/maillog
# Log cron stuff
cron.*                                  /var/log/cron
# Everybody gets emergency messages
*.emerg                                 :omusrmsg:*
# Save news errors of level crit and higher in a special file.
uucp,news.crit                          /var/log/spooler
# Save boot messages also to boot.log
local7.*                                /var/log/boot.log
```

nota

El archivo `rsyslog.conf` está documentado en la página de manual **rsyslog.conf**(5) y en la amplia documentación HTML de `/usr/share/doc/rsyslog-*/manual.html` que está en el rsyslog-doc, y está disponible en el canal de software de Red Hat Enterprise Linux 7, pero no está incluida en el medio de instalación.

Rotación del archivo de registro

Los registros se "rotan" mediante la utilidad **logrotate** para evitar que llenen el sistema de archivos que contiene `/var/log/`. Cuando se rota un archivo de registro, se le cambia el nombre con una extensión que indica la fecha en que se rotó: el archivo `/var/log/messages` antiguo puede convertirse en `/var/log/messages-20141030` si se rota el 30 de octubre de 2014. Una vez que se rotó el archivo de registro anterior, se crea un nuevo archivo de registro y se notifica al servicio que escribe en este.

Después de una determinada cantidad de rotaciones, habitualmente después de cuatro semanas, el archivo de registro anterior se descarta para liberar espacio en disco. Una tarea de cron ejecuta el programa de rotación de archivos de registros a diario para verificar si es necesario rotar algún registro. La mayoría de los archivos de registro se rotan semanalmente, pero el programa de rotación de archivos de registros rota algunos más rápido o más lento, o cuando alcanzan un tamaño determinado.

La configuración de logrotate no está tratada en este curso. Para obtener más información, consulte la página de manual **logrotate**(8).

Análisis de una entrada de syslog

Los registros del sistema escritos por **rsyslog** comienzan con el mensaje más antiguo en la parte superior y el mensaje más nuevo al final del archivo de registro. Todas las entradas en los archivos de registro administrados por **rsyslog** se graban en formato estándar. El siguiente ejemplo explicará la anatomía de un mensaje de archivo de registro en el archivo de registro `/var/log/secure`:

Feb 11 20:11:48 localhost sshd[1433]: Failed password for student from 172.25.0.10 port 59344 ssh2

La marca de tiempo cuando se grabó la entrada de registro.

El host desde donde se envió el mensaje de registro.

El programa o el proceso que envió el mensaje de registro.

El mensaje real enviado.

Monitoreo de un archivo de registro con tail

Para reproducir problemas e inconvenientes, puede ser especialmente útil controlar uno o más archivos de registro para eventos. El comando **tail -f /path/to/file** proporciona las últimas 10 líneas del archivo especificado y continúa ofreciendo líneas nuevas a medida que se escriben en el archivo monitoreado.

Para monitorear los intentos de inicio de sesión fallidos en una terminal, ejecute **ssh** como usuario root mientras otro usuario intenta iniciar sesión en la máquina serverX:

```
[root@serverX ~]$ tail -f /var/log/secure
...
Feb 10 09:01:13 localhost sshd[2712]: Accepted password for root from 172.25.254.254 port 56801 ssh2
Feb 10 09:01:13 localhost sshd[2712]: pam_unix(sshd:session): session opened for user root by (uid=0)
```

Envío de un mensaje de syslog con logger

El comando **logger** puede enviar mensajes al servicio **rsyslog**. De manera predeterminada, envía el mensaje al facility usuario con el aviso de gravedad (**user.notice**), a menos que se especifique lo contrario con la opción **-p**. Es especialmente útil, probar los cambios en la configuración de `rsyslog`.

Para enviar un mensaje a **rsyslogd** que se graba en el archivo de registro `/var/log/boot.log`, ejecute:

```
[root;@serverX ~]$ logger -p local7.notice "Log entry created on serverX"
```

Referencias

Páginas de manual **logger**(1), **tail**(1), **rsyslog.conf**(5) y **logrotate**(8)

Manual de **rsyslog**

- `/usr/share/doc/rsyslog-*/manual.html` provisto por el paquete rsyslog-doc

Es posible encontrar información adicional en la *Guía del administrador del sistema Red Hat Enterprise Linux* para Red Hat Enterprise Linux 7, que se puede encontrar en https://access.redhat.com/documentation/

Back Next