10.1 Arquitectura de registro del sistema

Objetivos

Tras finalizar esta sección, los estudiantes deberían poder describir la arquitectura básica de syslog en Red Hat Enterprise Linux 7.

Inicio de sesión del sistema

Los procesos y el núcleo del sistema operativo deben poder llevar un registro de los eventos que suceden. Estos registros pueden ser útiles para realizar una auditoría del sistema y solucionar problemas. Por convención, se almacenan de forma persistente en el directorio `/var/log`.

Red Hat Enterprise Linux incluye un sistema de registro estándar que se basa en el protocolo Syslog. Muchos programas utilizan este sistema para registrar eventos y organizarlos en archivos de registro. En Red Hat Enterprise Linux 7, hay dos servicios que se encargan de los mensajes de syslog: **systemd-journald** y **rsyslogd**.

El demonio **systemd-journald** proporciona un servicio de administración de registros mejorado que recopila mensajes del núcleo, las primeras etapas del proceso de arranque, la salida estándar y los errores de demonios a medida que se inician y ejecutan, y syslog. Escribe estos mensajes en un diario estructurado de eventos que, de manera predeterminada, no se conserva entre un reinicio y otro. Esto permite recopilar en una base de datos central los mensajes de syslog y los eventos que syslog omite. Los mensajes de syslog son reenviados de **systemd-journald** a **rsyslogd** para su posterior procesamiento.

El servicio **rsyslogd** luego ordena los mensajes de syslog por tipo (o utilidad) y prioridad, y los escribe en archivos persistentes en el directorio `/var/log`.

El directorio `/var/log` contiene diversos archivos específicos de sistemas y de servicios que mantiene **rsyslog**:

Generalidades de los archivos de registro del sistema

Archivo de registro	Propósito
`/var/log/messages`	La mayoría de los mensajes de syslog se registran aquí. Las excepciones son mensajes relacionados con tareas de autenticación y procesamiento de correos electrónicos, que realizan periódicamente trabajos, y aquellos relacionados exclusivamente con tareas de depuración.

Archivo de registro	Propósito
`/var/log/secure`	El archivo de registro para errores y mensajes relacionados con seguridad y autenticación.
`/var/log/maillog`	El archivo de registro con mensajes relacionados con el servidor de correo.
`/var/log/cron`	El archivo de registro relacionado con tareas ejecutadas en forma periódica.
`/var/log/boot.log`	Los mensajes relacionados con el arranque del sistema se registran aquí.

Referencias

páginas de manual **systemd-journald.service**(8), **rsyslogd**(8) y `rsyslog.conf`(5)

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/

Next