⏱️ Examen 108 - Servicios Esenciales del Sistema

108.2 Logs del sistema

Teoría

Los logs del sistema son archivos que registran eventos importantes que ocurren en un sistema operativo y en las aplicaciones que se ejecutan en él. Son indispensables para:

- **Diagnóstico de Problemas:** Identificar la causa de errores, fallos o comportamiento inesperado.
- **Auditoría y Seguridad:** Rastrear actividad de usuarios, intentos de acceso, cambios de configuración y eventos de seguridad.
- **Monitorización:** Seguir el estado y el rendimiento del sistema y los servicios.

Conceptos Clave:

1. **Syslog Tradicional:** Un estándar para la generación y el registro de mensajes de log. Los programas envían mensajes a un demonio syslog local, que luego decide cómo manejarlos (guardarlos en un archivo, enviarlos a un servidor remoto, etc.).
    - **Facilidades (Facilities):** Indican el origen del mensaje (ej: `auth` para autenticación, `mail` para correo, `kern` para mensajes del kernel, `daemon` para servicios en segundo plano, `local0` - `local7` para uso personalizado).
    - **Prioridades o Severidades (Priorities/Severities):** Indican la importancia o gravedad del mensaje (ej: `emerg` emergencia, `alert` alerta, `crit` crítico, `err` error, `warning` advertencia, `notice` aviso, `info` informativo, `debug` depuración).
2. **Demonios Syslog (Syslog Daemons):** Software que implementa el protocolo syslog. Escuchan mensajes (a menudo a través de un socket de dominio Unix como `/dev/log` o `/run/systemd/journal/syslog`) y los procesan según las reglas de configuración.
    - **`rsyslogd`:** Un demonio syslog avanzado, común en la mayoría de las distribuciones modernas (tanto Debian como Red Hat) como reemplazo de la implementación original `syslogd`. Configuración principal en `/etc/rsyslog.conf` y archivos en `/etc/rsyslog.d/`.
    - **`syslog-ng`:** Otra alternativa popular a `rsyslogd`. Configuración principal en `/etc/syslog-ng/syslog-ng.conf`.
    - **Diferencias Debian vs. Red Hat (Implementación Syslog):** Ambas usan `rsyslogd` por defecto en las versiones recientes, aunque históricamente y en algunas variantes pueden haber usado otros. La forma de configurarlo es similar, pero la organización de los archivos de log de destino puede variar.
3. **`systemd-journald`:**

- El sistema de registro de logs nativo de `systemd`. Recopila logs de diversas fuentes (syslog tradicional, mensajes del kernel, salida estándar/error de servicios systemd, auditoría).
- Almacena los logs en un formato binario estructurado (el "journal"), no en archivos de texto plano por defecto.
- Ventajas: Búsqueda y filtrado potentes, datos estructurados (campos como unit, pid, uid, mensaje), logs de arranque a arranque persistentes (si está configurado).
- `journald` a menudo funciona en paralelo o integrando con un demonio syslog tradicional (`rsyslogd`). `journald` puede reenviar mensajes al socket syslog para que `rsyslogd` los escriba en archivos de texto plano como respaldo o por compatibilidad.

4. **Archivos de Log Tradicionales (`/var/log/`):**
    - Aunque `journald` es el sistema moderno, muchos sistemas aún escriben logs en archivos de texto plano bajo `/var/log/` para compatibilidad y facilidad de acceso.
    - **Ubicaciones Comunes (Pueden variar según la configuración de syslog y la distribución):**
        - `/var/log/messages`: Mensajes generales del sistema (más común en Red Hat).
        - `/var/log/syslog`: Mensajes generales del sistema (más común en Debian/Ubuntu).
        - `/var/log/auth.log`: Logs de autenticación y seguridad (Debian/Ubuntu).
        - `/var/log/secure`: Logs de autenticación y seguridad (Red Hat).
        - `/var/log/kern.log`: Mensajes del kernel.
        - `/var/log/boot.log`: Mensajes durante el arranque.
        - `/var/log/daemon.log`: Mensajes de demonios/servicios.
        - `/var/log/mail.log` / `/var/log/maillog`: Logs del sistema de correo.
        - `/var/log/cron.log` / `/var/log/cron`: Logs de la ejecución de trabajos cron.
        - `/var/log/dmesg`: Buffer de mensajes del kernel (también accesible con el comando `dmesg`).
    - **Diferencias Debian vs. Red Hat (Archivos de Log):** La principal diferencia está en el nombre de los archivos de logs generales (`syslog` vs `messages`) y de seguridad (`auth.log` vs `secure`).
5. **Visualización de Logs:**
    - **Archivos de Texto:** Puedes usar comandos de texto estándar: `cat`, `less`, `tail` (especialmente `tail -f` para ver nuevos mensajes en tiempo real), `grep` para filtrar.

- **Journald:** Usa el comando `journalctl`. Es la herramienta principal para interactuar con el journal binario.
  - `journalctl`: Muestra todos los logs desde el inicio más reciente.
  - `journalctl -f`: Muestra los logs en tiempo real (como `tail -f`).
  - `journalctl -u <nombre_servicio>`: Muestra logs de una unidad systemd específica (ej: `journalctl -u ssh.service`).
  - `journalctl -k`: Muestra solo mensajes del kernel (como `dmesg`).
  - `journalctl -p <prioridad>`: Muestra logs con una prioridad mínima (ej: `-p err`). Prioridades numéricas: 0 emerg, 1 alert, 2 crit, 3 err, 4 warning, 5 notice, 6 info, 7 debug.
  - `journalctl --since "YYYY-MM-DD HH:MM:SS"` / `--until ...`: Filtra por rango de tiempo.
  - `journalctl -b`: Muestra logs solo del arranque actual. `journalctl -b -1` para el arranque anterior, etc.
  - `journalctl _PID=<pid>`: Muestra logs de un PID específico.
  - `journalctl -o cat`: Muestra los mensajes sin metadatos adicionales (como un `cat`).

6. **Rotación de Logs (`logrotate`):**
   - Los archivos de log de texto plano pueden crecer indefinidamente y consumir todo el espacio en disco. `logrotate` es la utilidad estándar para gestionar esto.
   - Comprime, renombra y archiva los archivos de log periódicamente (ej: diariamente, semanalmente) y elimina las versiones antiguas.
   - Configuración principal en `/etc/logrotate.conf` y archivos específicos de aplicaciones en `/etc/logrotate.d/`.
   - **Diferencias Debian vs. Red Hat (Logrotate):** La configuración por defecto y la organización de los archivos en `/etc/logrotate.d/` pueden variar ligeramente, pero el comando y el formato general de configuración son los mismos.
7. **Envío de Logs Remotos:** Los demonios syslog (`rsyslogd`, `syslog-ng`) pueden configurarse para enviar logs a un servidor de log remoto centralizado, lo que es útil en entornos con múltiples servidores.