

CURSOS
INTERSEMESTRALES



PROTECO

Introducción a Syslog

¿Qué es?

- Es un estándar.
- Captura y procesa mensajes de registro del sistema.
- Tiene la capacidad de recopilar información de registro para el control y la resolución de problemas.
- Capacidad de seleccionar el tipo de información de registro que se captura



Syslog

- Un mensaje de registro suele tener información sobre la seguridad del sistema
- Acceso.
- Anomalías.
- Errores.



syslog

La estructura del mensaje de registro:

- Prioridad
- Cabecera
- Texto



Prioridad.

0	Mensajes del kernel
1	Mensajes del nivel de usuario
2	Sistema de correo
3	Demonios de sistema
4	Seguridad/Autorización
5	Mensajes generados internamente por syslogd
6	Subsistema de impresión
7	Subsistema de noticias sobre la red
8	Subsistema UUCP
9	Demonio de reloj
10	Seguridad/Autorización
11	Demonio de FTP
12	Subsistema de NTP
13	Inspección del registro
14	Alerta sobre el registro
15	Demonio de reloj
16	Uso local 0
17	Uso local 1
18	Uso local 2
19	Uso local 3
20	Uso local 4
21	Uso local 5
22	Uso local 6
23	Uso local 7

$$\text{Prioridad} = \text{Recurso} * 8 + \text{Severidad}$$

0	<i>Emergencia:</i> el sistema está inutilizable
1	<i>Alerta:</i> se debe actuar inmediatamente
2	<i>Crítico:</i> condiciones críticas
3	<i>Error:</i> condiciones de error
4	<i>Peligro:</i> condiciones de peligro
5	<i>Aviso:</i> normal, pero condiciones notables
6	<i>Información:</i> mensajes informativos
7	<i>Depuración:</i> mensajes de bajo nivel

Rsyslog

- Es un eficiente y rápido sistema de procesamiento de registros de sistema.
- transporte de syslog a través de tcp.
- encargado de recolectar los mensajes de servicios que provienen de aplicaciones y el núcleo para luego distribuirlos en archivos de registros.

