SYSLOG

German Hernandez P.
CCIE #24492

Que es Syslog?

Funcionalidad que permite a los equipos generar mensajes de auditoria y gestión que describen cuando ocurre un evento.

Estos mensajes se envían a la consola, a la memoria o bien a un servidor SYSLOG.

Los mensajes son enviados en tiempo real.

Que contiene el mensaje Syslog?

Timestamp: La fecha y hora en que ocurrió el evento.

Facility Code: Un identificador que categoriza cual funcionalidad o modulo del equipo genero el mensaje. Inicia con un símbolo de porcentaje %.

Severity: Un numero de 0 a 7 que indica la importancia o severidad del evento, entre mas bajo mas critico.

Mnemonic: Texto corto que categoriza el evento con un código.

Message Text: Un mensaje con una descripción del evento o la condición que disparo ese mensaje del Sistema.

Ejemplo de mensaje SYSLOG

```
*Dec 18 17:10:15.079: %LINEPROTO-5-UPDOWN: Line
protocol on Interface FastEthernet0/0, changed state
to down
```

Timestamp: *Dec 18 17:10:15.079

Facility code: %LINEPROTO

Severity level: 5

mnemonic : UPDOWN

Message Text: Line protocol on Interface FastEthernet0/0, changed state to down

Configuración de SYSLOG para enviar mensajes a Consola

Comando	Descripción
router(config)# logging console *severity*	Por defecto todos los mensajes de SYSLOG son enviados a la consola. Pero usted puede variar la severidad de los mensajes. Para ver estos mensajes DEBE estar conectado físicamente con el cable de consola.
router# terminal monitor	Cuando estas conectado por TELNET o por SSH, te permite ver los mensajes enviados a consola

German Hernandez P.
CCIE #24492

Configuración de SYSLOG para enviar mensajes a memoria buffer

Comando	Descripción
router(config)# logging buffered *severity*	Permite enviar los mensajes de SYSLOG a la memoria buffer del equipo. Por defecto viene deshabilitado. Los mensajes se borraran cuando se apague el equipo.
router# show logging	Despliega los mensajes almacenados en el buffer

Configuración de SYSLOG para enviar mensajes a servidor remoto

Comando	Descripción
router(config)# logging host *ip-address*	Permite enviar los mensajes de SYSLOG a un servidor que tenga el servicio de SYSLOG. Utiliza UDP puerto 514
router# show logging	Despliega los mensajes almacenados en el buffer

Adicionales

De forma predeterminada los equipos envían una mensaje bastante común que puede ayudar pero también puede ser molesto: cada vez que una interfaz se activa o se desactiva (UP/DOWN).

Puedes evitar esto con el siguiente comando:

router(config-if)# **no logging event link-status**

21w5d: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to down

23w2d: %SYS-5-CONFIG_I: Configured from console by vty0 (172.1.1.1)

German Hernandez P.
CCIE #24492

Adicionales

Adicionalmente y también de forma predeterminada los equipos solamente colocan el UPTIME en los mensajes. Así que se debe configurar el reloj del equipo o bien un servidor de NTP para ver la hora exacta del evento.

21w5d: %LINK-3-UPDOWN: Interface FastEthernet0/0, changed state to down
23w2d: %SYS-5-CONFIG_I: Configured from console by vty0 (172.1.1.1)

router#clock set 11:11:00 20 january 2016

Lab

German Hernandez P.
CCIE #24492