Introdução

Muitos administradores de redes ignoram a importancia de logs no roteadores. Registro de logs pode ser usados para notificação de falhas, rede forense, e auditoria de segurança.

As mensagens de logs dos roteadores Cisco podem ser tratados em 5 maneiras diferentes:

- **Registro de log de console**: Por padrão, o roteador envia todas as mensagens de log para sua porta console. Portanto somente os usuarios que estão fisicamente conectados à porta console pode ver essas mensagens.
- **Registro de log do terminal**: É similar ao do console, mas mostra mensagens de log nas linhas VTY. Não é habilitado por padrão.
- **Registro de log de buffer**: Esse tipo de log usa a memoria RAM do roteador para o armazenamento das mensagens de log. O buffer tem um limite fixo para garantir que o log não irá esgotar memória valiosa do sistema. O roteador realiza isso deletando mensagens antigas do buffer assim como novas mensagens vão entrando.
- **Registro de log do servidor Syslog:** O roteador pode usar o syslog para encaminhar mensagens de log para servidores de syslog externo para o armazenamento.
- **Registro de log de trap SNMP**: O roteador é capaz de usar as traps de SNMP para enviar mensagens de log para servidores SNMP externos.

Exemplos de mensagens de log:

Level	Nome do Level	Mensagens do Roteador
0	Emergencias	Sistema desligando devido à falta de FAN
1	Alertas	Temperatura excedeu o limite
2	Critico	Falhas de alocação de memória
3	Erros	Interface Up/Down
4	Avisos	Configuração arquivo escrito no servidor via requisição SNMP
5	Notificações	Line protocol Up/Down
6	Informação	Log de violação de Access-list
7	Depuração	Mensagens de depuração

Configuração – Visão geral

Registro de Log de console:

O roteador não checa se o usuario esta logado na porta console ou um equipamento está conectado à ela; se o registro de log de console está habilitado, mensanges são sempre enviadas para a porta console que pode causar sobrecarga de CPU.

Para parar o log de console, use o " no logging console" no modo de configuração global. Voce pode querer limitar a quantidade de mensagens enviadas à console com o comando " logging console level" (por exemplo, "logging console informational"

Registro de log de buffer:

Voce gostaria do seu roteador registrar mensagens de log, ao invés de somente mostra-las no console. Use o comando de configuração de log de buffer para habilitar o armazenamento local das mensagens de log do roteador:

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging buffered informational
Router(config)#end
```

Voce também pode configurar o tamanho do log no roteador.

```
Router#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#logging buffered 64000
Router(config)#end
```

Registro de log de terminal:

Voce deseja que o roteador mostrasse mensagens de log na sua sessão VTY em tempo real. Use o comando "terminal monitor" para habilitar esse recurso.

```
Router#terminal monitor
Router#
```

Para desabilitar o log em sua sessão VTY, use o comando:

```
Router#terminal no monitor
Router#
```

Registro de log do servidor Syslog:

Voce deseja enviar mensagens de log para um servidor syslog remoto. Usando esse recurso podemos enviar mensagens para um dispositvo externo para armazenar os logs e o tamanho do armazenamento não depende do espaço disponivel no servidor syslog. Essa opção não é habilitada por padrão.

Se voce tiver algum servidor syslog, por favor a configuração está abaixo:

router#conf t

Router(config#logging host x.x.x.x

Router(config)#logging traps (i.e 0 1 2 3 4 5 .. de acordo com os seus requisitos)

Antes de habilitar o registro de log, tenha certeza que o roteador está configurado adequadamente para sincronizar com a hora certa de um servidor NTP ou manualmente configurado faze-lo.

O comando para configurar a hora manualmente no roteador é “set clock”, ou use um ntp server “ntp server x.x.x.x” para sincronizar a hora no roteador.

Use o comando “logging source-interface” para especificar um endereço IP particular para mensagens syslog.

Router(config)#logging source-interface Loopback0

Limpando o log do roteador:

Use o comando “clear logging” para limpar o buffer de log interno do roteador:

Para mostrar o estado do syslog e o conteúdo do buffer de mensagens de log do sistema, use o comando “show logging” no modo previlegiado.

Router# show logging

Syslog logging: enabled

Console logging: disabled

Monitor logging: level debugging, 266 messages logged.

Trap logging: level informational, 266 messages logged.

Logging to 10.1.1.1

SNMP logging: disabled, retransmission after 30 seconds

0 messages logged

Router#.