Configuración de alarma RMON y configuración de evento desde la interfaz de la línea de comandos (CLI)

Contenido

Introducción

En este documento se describe cómo configurar las alarmas y los eventos de Remote Monitoring (RMON) en un router desde la interfaz de línea de comandos (CLI).

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

Este documento no tiene restricciones específicas en cuanto a versiones de software y de hardware.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Antecedentes

RMON es un método similar al protocolo simple de administración de red (SNMP) para realizar un seguimiento de las estadísticas en las interfaces de los dispositivos de red o en los puertos.

La función RMON suele ser útil en un entorno de switch LAN, pero está disponible en los routers de acceso (por ejemplo, la serie 2x00) en la versión 11.1 o posterior del software del IOS® de Cisco. A veces, sólo necesita configurar RMON en routers remotos cuando no puede obtener acceso al equipo LAN (como concentradores) para ver el tráfico. RMON no requiere que sondee activamente las variables SNMP de manera regular. Los dispositivos almacenan la información necesaria y luego se envía periódicamente a una estación de administración de red RMON.

Nota: De forma predeterminada, todos los switches admiten mini-rmon, de modo que las alarmas, los eventos, las estadísticas y el historial se reciban directamente de los switches. Para recibir toda la información detallada de los switches, necesita Network Analysis Module (NAM).

Sintaxis Para Configurar Un Evento

El software Cisco IOS le permite configurar alarmas y eventos RMON desde la CLI. Esta sección y la siguiente proporcionan la sintaxis de los comandos requeridos, con los mismos nombres que se utilizan para la **tabla** de **eventos** y la **tabla de alarmas**.

```
1.3.6.1.2.1.16.9.1
eventTable OBJECT-TYPE

SYNTAX SEQUENCE OF EventEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
           "A list of events to be generated."
::= { event 1 }

.1.3.6.1.2.1.16.3.1
alarmTable OBJECT-TYPE

SYNTAX SEQUENCE OF AlarmEntry
MAX-ACCESS not-accessible
STATUS current
DESCRIPTION
           "A list of alarm entries."
::= { alarm 1 }
```

Sintaxis

rmon event *eventIndex* [log] [trap *eventCommunity*] [description *eventDescription*] [owner *eventOwner*]

Descripción de la Sintaxis

1. **event**: configure un evento RMON.
2. *eventIndex*: número de evento (1-65535)
3. **log**:(Opcional) Generar un registro RMON cuando se activa el evento.
4. **trap *eventCommunity*: (Opcional) Genere una trampa SNMP cuando se activa el evento,**

para la cadena de comunidad SNMP especificada.

5. descripción ***evento Descripción: (opcional) Especifique una WORD o una descripción del evento.***
6. **owner *eventOwner*** : (Opcional) Especifique un propietario para el evento.

- Si no especifica la opción **log** o **trap**, el objeto **alarmTable eventType (1.3.6.1.2.1.16.9.1.1.3)** se establece en none.
- Si sólo especifica **log**, **eventType** se establece en log.
- Si sólo especifica **trap**, **eventType** se establece en snmp-trap.
- Si especifica tanto **log** como **trap**, **eventType** se establece en log-and-trap.

Sintaxis Para Configurar Una Alarma

alarma rmon *alarmIndex alarmVariable alarmInterval* {absoluto | delta} umbral ascendente *alarmaUmbral ascendente [alarmRisingEventIndex]* umbral descendente *alarmaUmbral descendente [alarmFallingEventIndex]* [propietario *alarmOwner]*

Descripción de la Sintaxis

1. **alarma**: configure una alarma RMON.
2. *alarmIndex*: número de alarma (1-65535)
3. *alarmVariable*: objeto MIB a monitorear (WORD)
4. *alarmInterval*: intervalo de muestra (1-4294967295)
5. **absoluto**: pruebe cada muestra directamente.
6. **delta**: prueba delta entre muestras.
7. **umbral ascendente**: configure el umbral ascendente.
8. *alarmRisingThreshold*: valor de umbral ascendente (-2147483648-2147483647)
9. *alarmRisingEventIndex* : (opcional) Evento que se activará cuando se cruce el umbral ascendente (1-65535)
10. **umbral descendente**: configure el umbral descendente.
11. *alarmFallingThreshold*: valor del umbral de caída (-2147483648-2147483647)
12. *alarmFallingEventIndex* : (Opcional) Evento que se activa cuando se cruza el umbral descendente (1-65535)
13. ***Propietario de la alarma del propietario***: (opcional) Especifique un propietario para la alarma (WORD).

La *variable de alarma* se especifica de una de estas maneras:

- Como identificador de objeto (OID) de la Notación de Sintaxis Abstracta Uno (ASN.1) decimal con puntos completos para el objeto (como **.1.3.6.1.2.1.2.2.1.10.1**)
- Con el nombre de entrada de tabla seguido del número de objeto de tabla y la instanciaPor ejemplo, para especificar ifInOctets para la primera instancia, utilice **ifEntry.10.1** para la *variable de alarma*.

Examples

En los ejemplos de esta sección, "public" es la cadena de comunidad SNMP de sólo lectura (RO) y 171.68.118.100 es el host que recibe la trampa.

Para configurar un evento para enviar una trampa cuando se activa, ejecute estos comandos:

```
!--- Enter these commands on one line each. rmon event 3 log trap public
     description "Event to create log entry and SNMP notification"
     owner "jdoe 171.68 118.100 2643"

rmon alarm 2 ifEntry.10.12 30 delta
     rising-threshold 2400000 3 falling-threshold 1800000 3
     owner "jdoe 71.68 118.100 2643"
```

En este ejemplo, se configura un Cisco 2500 para enviar una trampa y registrar un evento, cuando el umbral de alarma que supervisa su propio ifInOctets (ifEntry.10.1) excede un valor absoluto de 90000:

```
snmp-server host 171.68.118.100 public

SNMP-server community public RO

rmon event 1 log trap public description "High ifInOctets" owner jdoe

!--- Enter this command on one line: rmon alarm 10 ifEntry.10.1 60 absolute
     rising-threshold 90000 1 falling-threshold 85000 owner jdoe
```

La supervisión se realiza cada 60 segundos y el umbral descendente es 85000. En este caso, la estación de administración de NetView recibió esta trampa:

```
router.rtp.cisco.com:
A RMON Rising Alarm:
Bytes received exceeded
  threshold 90000;

  VALUE=483123 (sample TYPE=1; alarm index=10)
```

Ejecute estos comandos para ver las alarmas y los eventos registrados:

- **show rmon events**—Muestra el contenido de la tabla de eventos RMON del router. Este comando no tiene argumentos ni palabras clave.

  ```
  Router#show rmon events

  Event 12 is active, owned by manager 1
   Description is interface-errors
   Event firing causes log and trap to community public, last fired 00:00:00
  ```

  `El evento 12 está activo, propiedad de manager1`: índice único en la **tabla de eventos**, que muestra el estado del evento como activo y el propietario de esta fila, como se define en la **tabla de eventos** de RMON.`La descripción es interface-errors`—Tipo de evento; en este caso, un error de interfaz.`El desencadenamiento de eventos causa el registro y la trampa`: tipo de notificación que el router realizará sobre este evento. Equivalente a **eventType** en RMON.`comunidad pública`: si se va a enviar una trampa SNMP, se envía a la comunidad SNMP especificada por esta cadena de octetos. Equivalente a *EventCommunity* en RMON.`Last fire`: la última vez que se generó el evento.
- **show rmon alarms**—Muestra el contenido de la tabla de alarma RMON del router. Este comando no tiene argumentos ni palabras clave.

```
Router#show rmon alarms

Alarm 2 is active, owned by manager1
 Monitors ifEntry.1.1 every 30 seconds
 Taking delta samples, last value was 0
 Rising threshold is 15, assigned to event 12
 Falling threshold is 0, assigned to event 0
 On startup enable rising or falling alarm
```

`Alarm2 está activo, propiedad de manager1`: índice único en la **tabla de alarmas**, que muestra el estado de alarma como activo y muestra el propietario de esta fila, como se define en la **tabla de alarmas** de RMON.`Monitorea ifEntry.1.1`: OID de la variable particular que se va a muestrear. Equivalente a *alarmVariable* en RMON.`cada 30 segundos`: intervalo en segundos sobre el que se muestrean los datos y se comparan con los umbrales ascendente y descendente. Equivalente a *alarmInterval* en RMON.`Tomar muestras delta`: método para mostrar la variable seleccionada y calcular el valor que se comparará con los umbrales. Equivalente a alarmSampleType en RMON.`El último valor fue`: valor de la estadística durante el último período de muestreo. Equivalente a alarmValue en RMON.`Umbral ascendente es`: Umbral para las estadísticas muestreadas. Equivalente a *alarmRisingThreshold* en RMON.`asignado a event`: Índice de EventEntry que se utiliza cuando se cruza un umbral ascendente. Equivalente a *alarmRisingEventIndex* en RMON.`El umbral de caída es`—Umbral para la estadística de muestra. Equivalente a *alarmFallingThreshold* en RMON.`Asignado al evento`: Índice de EventEntry que se utiliza cuando se cruza un umbral descendente. Equivalente a *alarmFalllingEventIndex* en RMON.`Al iniciar, active la activación de la alarma al alzar o al caer`: alarma que se puede enviar cuando esta entrada se establece por primera vez en válida. Equivalente a alarmStartupAlarm en RMON.

Información Relacionada

- Traducir OID con SNMP Object Navigator
- Soporte Técnico y Documentación - Cisco Systems