

Configurando as definições de alarme e eventos RMON na interface de linha de comando (CLI)

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Conventions](#)

[Informações de Apoio](#)

[Sintaxe Para Configurar Um Evento](#)

[Sintaxe Para Configurar Um Alarme](#)

[Examples](#)

[Informações Relacionadas](#)

[Introduction](#)

Este documento descreve como configurar alarmes e eventos de Monitoração Remota (RMON) em um roteador com interface de linha de comando (CLI).

[Prerequisites](#)

[Requirements](#)

Não existem requisitos específicos para este documento.

[Componentes Utilizados](#)

Este documento não se restringe a versões de software e hardware específicas.

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.

[Conventions](#)

Consulte as [Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos](#).

[Informações de Apoio](#)

[RMON](#) é um método semelhante ao SNMP (Simple Network Management Protocol) para rastrear estatísticas em interfaces ou portas de dispositivos de rede.

O recurso RMON geralmente é útil em um ambiente de switch LAN, mas está disponível em roteadores de acesso (por exemplo, a série 2x00) no Cisco IOS® Software Release 11.1 ou posterior. Às vezes, você precisa configurar o RMON em roteadores remotos somente quando não pode obter acesso ao equipamento de LAN (como hubs) para visualizar o tráfego. O RMON não exige que você pesquise ativamente variáveis SNMP regularmente. Os dispositivos armazenam as informações necessárias e são enviados periodicamente para uma estação de gerenciamento de rede RMON.

Observação: por padrão, todos os switches suportam minirmon, de modo que alarmes, eventos, estatísticas e histórico sejam recebidos diretamente dos switches. Para receber todas as outras informações detalhadas dos switches, você precisa do Network Analysis Module (NAM).

Sintaxe Para Configurar Um Evento

O software Cisco IOS permite configurar alarmes e eventos RMON a partir da CLI. Esta seção e a próxima fornecem a sintaxe dos comandos necessários, com os mesmos nomes usados para a `eventTable` e a `alarmTable`.

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 }
```

Sintaxe

[rmon event eventIndex \[log\] \[trap eventCommunity\] \[description eventDescription\] \[owner eventOwner\]](#)

Descrição da sintaxe

1. **event** — Configure um evento RMON.
2. **eventIndex** — Event number (1-65535)
3. **log** —(Opcional) Gerar um log RMON quando o evento é acionado.
4. **trap eventCommunity** —(Opcional) Gere uma interceptação SNMP quando o evento é acionado, para a string de comunidade SNMP especificada.

5. **description** *eventDescription* —(Opcional) Especifique uma PALAVRA ou uma descrição do evento.
 6. proprietário *eventOwner* —(Opcional) Especifique um proprietário para o evento.
- Se você não especificar a opção **log** ou **trap**, **alarmTable** object **eventType** (1.3.6.1.2.1.16.9.1.1.3) está definido como none.
 - Se você especificar apenas **log**, **eventType** será definido como log.
 - Se você especificar apenas **trap**, o **eventType** será definido como snmp-trap.
 - Se você especificar **log** e **trap**, **eventType** será definido como log-and-trap.

Sintaxe Para Configurar Um Alarme

rmon alarm alarmIndex alarmVariable alarmInterval {absolute | delta} crescente alarmRisingThreshold [alarmRisingEventIndex] declinando alarmFallingThreshold [alarmFallingEventIndex] [owner alarmOwner]

Descrição da sintaxe

1. **alarm** — Configure um alarme RMON.
2. *alarmIndex* —Número do alarme (1-65535)
3. *alarmVariable* — objeto MIB a monitorar (WORD)
4. *alarmInterval* — Intervalo de amostra (1-4294967295)
5. **Absoluto** — Teste cada amostra diretamente.
6. **delta** — Testar delta entre amostras.
7. **rise-limite** — Configure o limite de elevação.
8. *alarmRisingThreshold* — Valor limite crescente (-2147483648-2147483647)
9. *alarmRisingEventIndex* —(opcional) Event to fire when the rise threshold is crossed (1-65535) (Evento para disparar quando o limite de elevação é ultrapassado)
10. **fall-threshold** — Configure o limite de queda.
11. *alarmFallingThreshold* — Valor limite de queda (-2147483648-2147483647)
12. *alarmFallingEventIndex* —(Opcional) Evento para disparar quando o limiar de queda é ultrapassado (1-65535)
13. **owner** *alarmOwner* —(Opcional) Especifique um proprietário para o alarme (WORD).

A *alarmVariable* é especificada de uma destas maneiras:

- Como o identificador de objeto (OID) da Notação de Sintaxe de Abstrato Um (ASN.1) decimal inteiro para o objeto (como .1.3.6.1.2.1.2.1.10.1)
- Com o nome da entrada da tabela seguido pelo número do objeto da tabela e pela instância Por exemplo, para especificar iflnOctets para a primeira instância, use **ifEntry.10.1** para a *alarmVariable*.

Examples

Nos exemplos desta seção, "public" é a string de comunidade SNMP somente leitura (RO) e 171.68.118.100 é o host que recebe a interceptação.

Para configurar um evento para enviar uma armadilha quando disparada, emita estes 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"
```

Neste exemplo, um Cisco 2500 é configurado para enviar uma interceptação e registrar um evento, quando o limite de alarme que monitora seu próprio ifInOctets (ifEntry.10.1) excede um 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
```

O monitoramento ocorre a cada 60 segundos e o limiar de queda é 85000. Nesse caso, a estação de gerenciamento NetView recebeu essa armadilha:

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

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

Emita estes comandos para exibir alarmes e eventos registrados:

- **show rmon events** —Exibe o conteúdo da tabela de eventos RMON do roteador. Este comando não tem argumentos ou palavras-chave.

```
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
```

O evento 12 está ativo, de propriedade do manager1 — Índice exclusivo na **eventTable**, que mostra o status do evento como ativo e mostra o proprietário desta linha, conforme definido na **eventTable** de RMON.A descrição é interface-errors — Tipo de evento; nesse caso, um erro de interface.O disparo de eventos causa o registro e a armadilha — Tipo de notificação que o roteador fará sobre esse evento. Equivalente a **eventType** em RMON.community public — Se uma interceptação SNMP for enviada, ela será enviada para a comunidade SNMP especificada por esta string de octeto. Equivalente a **eventCommunity** em RMON.último disparo — A última vez que o evento foi gerado.

- **show rmon alarms** —Exibe o conteúdo da tabela de alarme RMON do roteador. Este comando não tem argumentos ou palavras-chave.

```
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 ativo, de propriedade do gerente1 — índice exclusivo na **alarmTable**, que mostra o status do alarme como ativo e mostra o proprietário desta linha, conforme definido na **alarmTable** do RMON. Monitora ifEntry.1.1 — OID da variável específica a ser amostrada. Equivalente a *alarmVariable* em RMON. a cada 30 segundos — Intervalo em segundos sobre o qual os dados são amostrados e comparado com os limiares de elevação e queda. Equivalente a *alarmInterval* em RMON. Tomando amostras delta — Método para amostrar a variável selecionada e calcular o valor a ser comparado com os limiares. Equivalente a *alarmSampleType* em RMON. Último valor foi — Valor da estatística durante o último período de amostragem. Equivalente a *alarmValue* em RMON. Limite de elevação é — Limite para as estatísticas de amostra. Equivalente a *alarmRisingThreshold* no RMON. atribuído ao evento — Índice da EventEntry usado quando um limite de aumento é ultrapassado. Equivalente a *alarmRisingEventIndex* em RMON. o limiar de queda é — Limite para a estatística de amostra. Equivalente a *alarmFallingThreshold* no RMON. Atribuído ao evento — Índice da EventEntry usado quando um limite de queda é ultrapassado. Equivalente a *alarmFallingEventIndex* no RMON. Na inicialização, ative o alarme de elevação ou queda — Alarme que pode ser enviado quando esta entrada for definida pela primeira vez como válido. Equivalente a *alarmStartupAlarm* em RMON.

[Informações Relacionadas](#)

- [Traduzir OID com o SNMP Object Navigator](#)
- [Suporte Técnico e Documentação - Cisco Systems](#)