

Konfigurieren von RMON-Alarm- und Ereigniseinstellungen über die Befehlszeilenschnittstelle (CLI)

Inhalt

[Einführung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Konventionen](#)

[Hintergrundinformationen](#)

[Syntax zum Einrichten eines Ereignisses](#)

[Syntax zum Einrichten eines Alarm](#)

[Beispiele](#)

[Zugehörige Informationen](#)

[Einführung](#)

In diesem Dokument wird beschrieben, wie Sie Remote Monitoring (RMON)-Alarmer und Ereignisse über die Befehlszeilenschnittstelle (CLI) auf einem Router einrichten.

[Voraussetzungen](#)

[Anforderungen](#)

Für dieses Dokument bestehen keine speziellen Anforderungen.

[Verwendete Komponenten](#)

Dieses Dokument ist nicht auf bestimmte Software- und Hardwareversionen beschränkt.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren (Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

[Konventionen](#)

Weitere Informationen zu Dokumentkonventionen finden Sie unter [Cisco Technical Tips Conventions](#) (Technische Tipps zu Konventionen von Cisco).

Hintergrundinformationen

[RMON](#) ist eine Methode, die dem Simple Network Management Protocol (SNMP) ähnelt, um Statistiken zu Netzwerkgeräteschnittstellen oder -ports zu verfolgen.

Die RMON-Funktion ist in der Regel in einer LAN-Switch-Umgebung nützlich, jedoch auf Access Routern (z. B. der Serie 2x00) in Cisco IOS® Software, Version 11.1 oder höher, verfügbar. Manchmal müssen Sie RMON nur auf Remote-Routern einrichten, wenn Sie keinen Zugriff auf die LAN-Geräte (z. B. Hubs) erhalten, um den Datenverkehr anzuzeigen. RMON erfordert keine regelmäßige aktive Abfrage von SNMP-Variablen. Die Geräte speichern die erforderlichen Informationen und werden dann regelmäßig an eine RMON-Netzwerkmanagementstation geleitet.

Hinweis: Standardmäßig unterstützen alle Switches Mini-Rmon, sodass Alarmer, Ereignisse, Statistiken und Verlaufsdaten direkt von den Switches empfangen werden. Um alle weiteren detaillierten Informationen von Switches zu erhalten, benötigen Sie das Network Analysis Module (NAM).

Syntax zum Einrichten eines Ereignisses

Mit der Cisco IOS-Software können Sie RMON-Alarmer und -Ereignisse über die CLI einrichten. Dieser und der nächste Abschnitt enthalten die Syntax der erforderlichen Befehle mit den gleichen Namen, die für die **eventTable** und die **alarmTable** verwendet werden.

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 }

Syntax

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

Syntaxbeschreibung

1. **event:** Konfigurieren Sie ein RMON-Ereignis.
2. **eventIndex** - Ereignisnummer (1-65535)
3. **log:** (Optional) Generieren Sie ein RMON-Protokoll, wenn das Ereignis ausgelöst wird.

4. **trap eventCommunity** - (Optional) Erstellen Sie für den angegebenen SNMP Community String ein SNMP-Trap, wenn das Ereignis ausgelöst wird.
 5. **description eventDescription**—(Optional) Geben Sie ein WORD oder eine Beschreibung des Ereignisses an.
 6. **owner eventOwner** (Optional) Geben Sie einen Besitzer für das Ereignis an.
- Wenn Sie weder das **log** noch die **trap**-Option angeben, ist der **alarmTable** object **eventType** (1.3.6.1.2.1.16.9.1.1.3) auf none festgelegt.
 - Wenn Sie nur **log** angeben, ist **eventType** auf log festgelegt.
 - Wenn Sie nur **Trap** angeben, wird **eventType** auf snmp-trap festgelegt.
 - Wenn Sie sowohl **log** als auch **trap** angeben, ist **eventType** auf log-and-trap festgelegt.

Syntax zum Einrichten eines Alarm

rmon alarm alarmIndex alarmVariable alarmInterval {absolut | delta} steigender Grenzwert alarmRisingThreshold [alarmRisingEventIndex] fallende Schwellenwertwarnung FallingThreshold [alarmFallingEventIndex] [Eigentümer alarmEigentümer]

Syntaxbeschreibung

1. **alarm** - Konfigurieren Sie einen RMON-Alarm.
2. *alarmIndex* - Alarmnummer (1-65535)
3. *alarmVariable* - zu überwachendes MIB-Objekt (WORD)
4. *alarmInterval* - Beispielintervall (1-4294967295)
5. **absolut** - Testen Sie jedes Beispiel direkt.
6. **delta**: Testdelta zwischen Stichproben.
7. **rising-threshold** - Konfigurieren Sie den steigenden Grenzwert.
8. *alarmRisingThreshold* - Steigender Grenzwert (-2147483648-2147483647)
9. *alarmRisingEventIndex*—(optional) Ereignis ausgelöst, wenn der steigende Grenzwert überschritten wird (1-65535)
10. **fall-threshold** - Konfigurieren Sie den fallenden Grenzwert.
11. *alarmFallingThreshold* - Fallender Schwellenwert (-2147483648-2147483647)
12. *alarmFallingEventIndex*—(Optional) Ereignis wird ausgelöst, wenn der fallende Grenzwert überschritten wird (1-65535)
13. **owner alarmOwner (Eigentümer)** - (Optional) Geben Sie einen Eigentümer für den Alarm (WORD) an.

Die *alarmVariable* wird folgendermaßen angegeben:

- Als die gesamte Punktzahl "Abstract Syntax Notation One" (ASN.1)-Objektkennung (OID) für das Objekt (z. B. .1.3.6.1.2.1.2.2.1.10.1)
- Mit dem Namen des Tabelleneintrags gefolgt von der Tabellenobjektnummer und der InstanzUm z. B. ifInOctets für die erste Instanz anzugeben, verwenden Sie **ifEntry.10.1** für die *alarmVariable*.

Beispiele

In den Beispielen in diesem Abschnitt ist "public" der Read-Only (RO) SNMP Community String

und 171.68.118.100 der Host, der das Trap empfängt.

Führen Sie folgende Befehle aus, um ein Ereignis einzurichten, das ein Trap sendet, wenn es ausgelöst wird:

```
!--- 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"
```

In diesem Beispiel wird ein Cisco 2500 so konfiguriert, dass ein Trap gesendet und ein Ereignis protokolliert wird, wenn der Alarmschwellenwert, der seinen eigenen ifInOctets überwacht (ifEntry.10.1), einen absoluten Wert von 90000 überschreitet:

```
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
```

Die Überwachung erfolgt alle 60 Sekunden, und der Schwellenwert für Downloads beträgt 85000. In diesem Fall erhielt die NetView-Managementstation dieses Trap:

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

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

Führen Sie folgende Befehle aus, um protokollierte Alarme und Ereignisse anzuzeigen:

- **show rmon events:** Zeigt den Inhalt der RMON-Ereignistabelle des Routers an. Dieser Befehl hat keine Argumente oder Schlüsselwörter.

```
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
```

Ereignis 12 ist aktiv, gehört manager1 - Eindeutiger Index in der **eventTable**, der den Ereignisstatus als aktiv anzeigt und den Besitzer dieser Zeile anzeigt, wie in der **eventTable** von RMON definiert. Beschreibung ist interface-errors - Art des Ereignisses; in diesem Fall ein Schnittstellenfehler. Ereignisauslösung verursacht Protokoll und Trap - Typ der Benachrichtigung, die der Router über dieses Ereignis ausführt. Entspricht **eventType** in RMON. community public - Wenn ein SNMP-Trap gesendet werden soll, wird es an die SNMP-Community gesendet, die durch diesen Oktett-String angegeben wird. Entspricht

eventCommunity in RMON.last burn (Letzter Auslöser) - Das letzte Mal, dass das Ereignis generiert wurde.

- **show rmon alarms** (RMON-Warnmeldungen anzeigen): Zeigt den Inhalt der RMON-Alarmtabelle des Routers an. Dieser Befehl hat keine Argumente oder Schlüsselwörter.

```
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 ist aktiv, gehört manager1 - Eindeutiger Index in der **alarmTable**, der den Alarmstatus als aktiv anzeigt und den Besitzer dieser Zeile anzeigt, wie in der **alarmTable** von RMON definiert. Überwacht ifEntry.1.1 - OID der zu beprobenden Variablen. Entspricht *alarmVariable* in RMON. alle 30 Sekunden - Intervall in Sekunden, über die die Daten abgetastet werden, verglichen mit den steigenden und fallenden Schwellenwerten. Entspricht *alarmInterval* in RMON. Entnahme von Deltaprobe - Methode zum Testen der ausgewählten Variable und zum Berechnen des mit den Schwellenwerten zu vergleichenden Werts. Äquivalent zu *alarmSampleType* in RMON. Letzter Wert war - Wert der Statistik während des letzten Samplingzeitraums. Äquivalent zu *alarmValue* in RMON. Rising threshold is - Threshold für die in die Stichprobe einbezogenen Statistiken. Entspricht *alarmRisingThreshold* in RMON. assigned to event - Index des EventEntry, der beim Überschreiten eines steigenden Schwellenwerts verwendet wird. Entspricht *alarmRisingEventIndex* in RMON. Falling threshold is - Threshold für die Sampling-Statistik. Entspricht *alarmFallingThreshold* in RMON. Assigned to event (Ereignis zugewiesen): Index des EventEntry, der beim Überschreiten eines fallenden Schwellenwerts verwendet wird. Entspricht *alarmFallingEventIndex* in RMON. Bei Systemstart Alarm - Alarm aktivieren, der bei der ersten gültigen Einstellung gesendet werden kann. Äquivalent zu *alarmStartupAlarm* in RMON.

[Zugehörige Informationen](#)

- [OID mit dem SNMP Object Navigator übersetzen](#)
- [Technischer Support und Dokumentation - Cisco Systems](#)