Eventos RMON em Switches Gerenciados 200/300 Series

Objetivo

O Monitoramento Remoto de Rede (RMON - Remote Networking Monitoring) permite que um switch monitore proativamente estatísticas de tráfego e envie um alarme se o tráfego exceder um limite predefinido. A vantagem do RMON é que o switch não precisa de uma solicitação do gerenciador SNMP para enviar informações, ele pode enviar informações quando necessário. Isso diminui o tráfego entre o gerenciador e o switch.

Nos Switches Gerenciados 200/300 Series, você pode determinar quais eventos disparam um alarme e que tipo de resposta ocorre quando um alarme é disparado. O registro de eventos registra os alarmes que foram desativados. Este artigo explica como criar um evento (ações que ocorrem quando um alarme é disparado), determinar os critérios que disparam um alarme e exibir o log de eventos.

Dispositivos aplicáveis

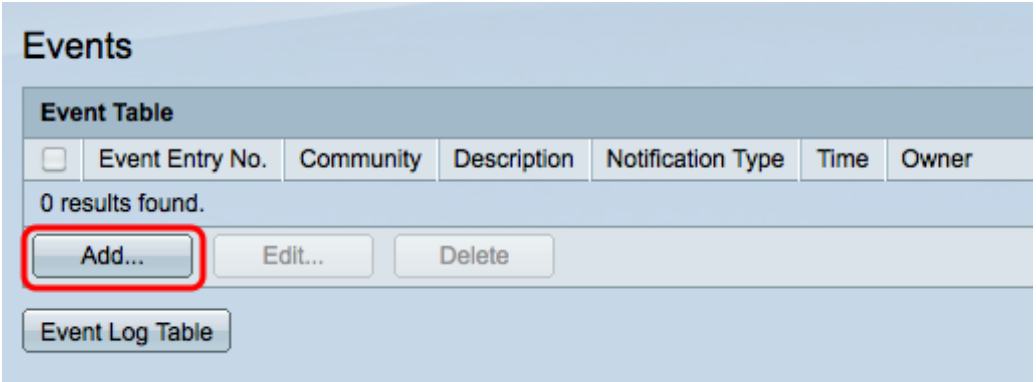
·Switches gerenciados SF/SG 200 e SF/SG 300 Series

Versão de software

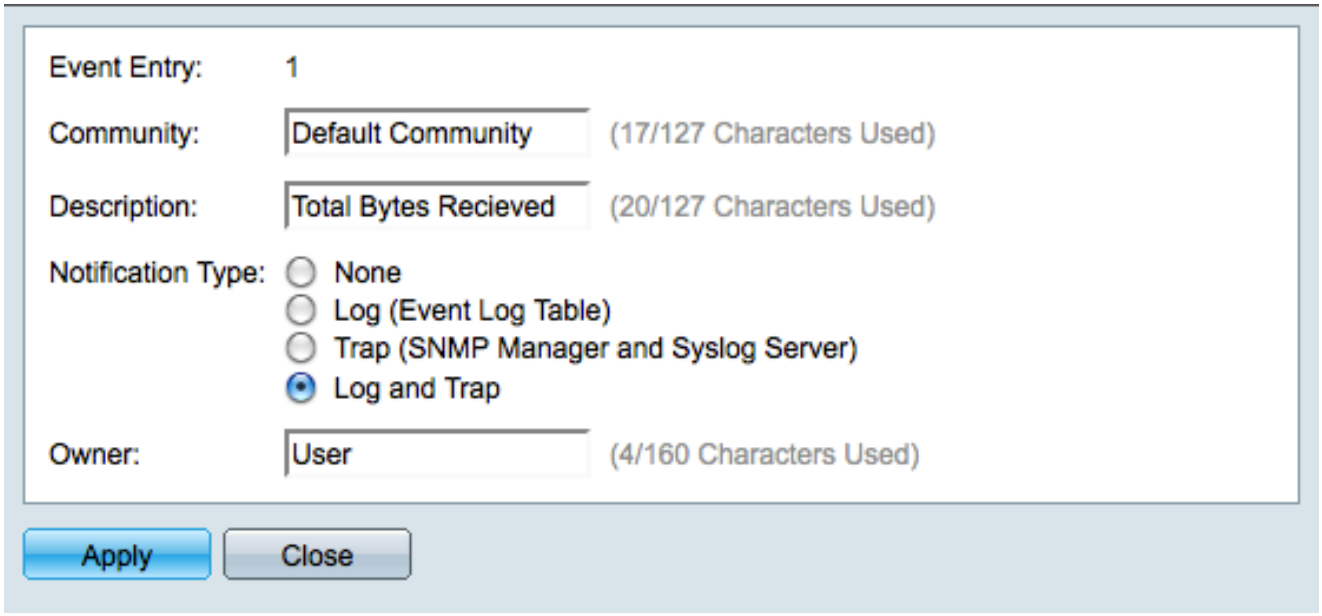
•1.3.0.62

Criar evento RMON

Etapa 1. Efetue login no utilitário de configuração da Web e escolha **Status and Statistics > RMON > Events**. A página *Eventos* será aberta:



Etapa 2. Clique em **Adicionar** para criar um novo evento na Tabela de Eventos. A janela *Add RMON Events* é exibida.



Etapa 3. (Opcional) Digite a string de comunidade SNMP a ser incluída quando mensagens de alarme forem enviadas no campo Comunidade.

Etapa 4. Digite uma descrição do evento que disparará o alarme no campo Descrição. Este é o nome usado para anexar um alarme ao evento.

Etapa 5. Clique no botão de opção que corresponde à ação resultante desse evento no campo Tipo de notificação. As opções disponíveis são:

·Nenhum — Nenhuma ação ocorre quando o alarme do evento é desligado.

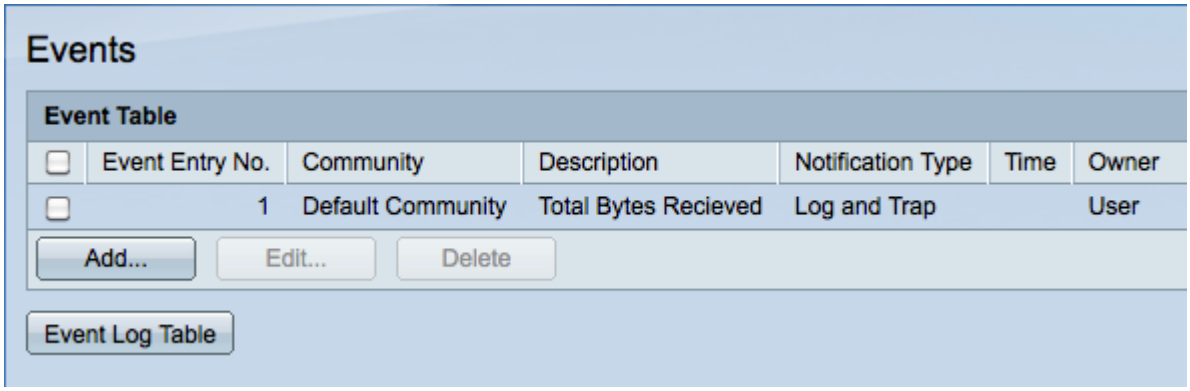
·Log (Event Log Table) — Adiciona uma entrada de log à tabela Event Log quando o alarme é desligado.

·Trap (SNMP Manager e Syslog Server) — Envia uma interceptação (mensagem de alarme) ao servidor de registro remoto quando o alarme é desligado.

·Log and Trap — Adiciona uma entrada de log à tabela Event Log e envia uma interceptação ao servidor de log remoto quando o alarme é desligado.

Etapa 6. Digite o nome do dispositivo ou do usuário que configurou o evento no campo Proprietário.

Passo 7. Clique em **Apply** para salvar as configurações e clique em **Close** para sair da janela *Add RMON Events*.



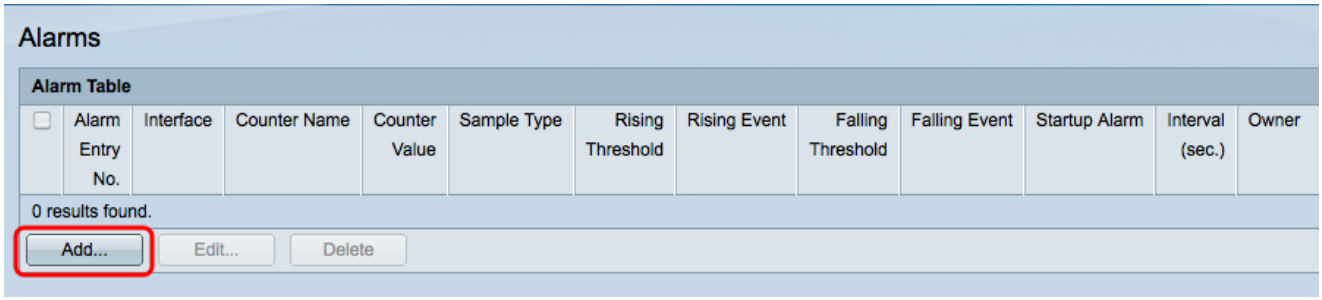
Etapa 8. (Opcional) Marque uma caixa de seleção de evento na Tabela de Eventos e clique

em **Editar** para editar o evento.

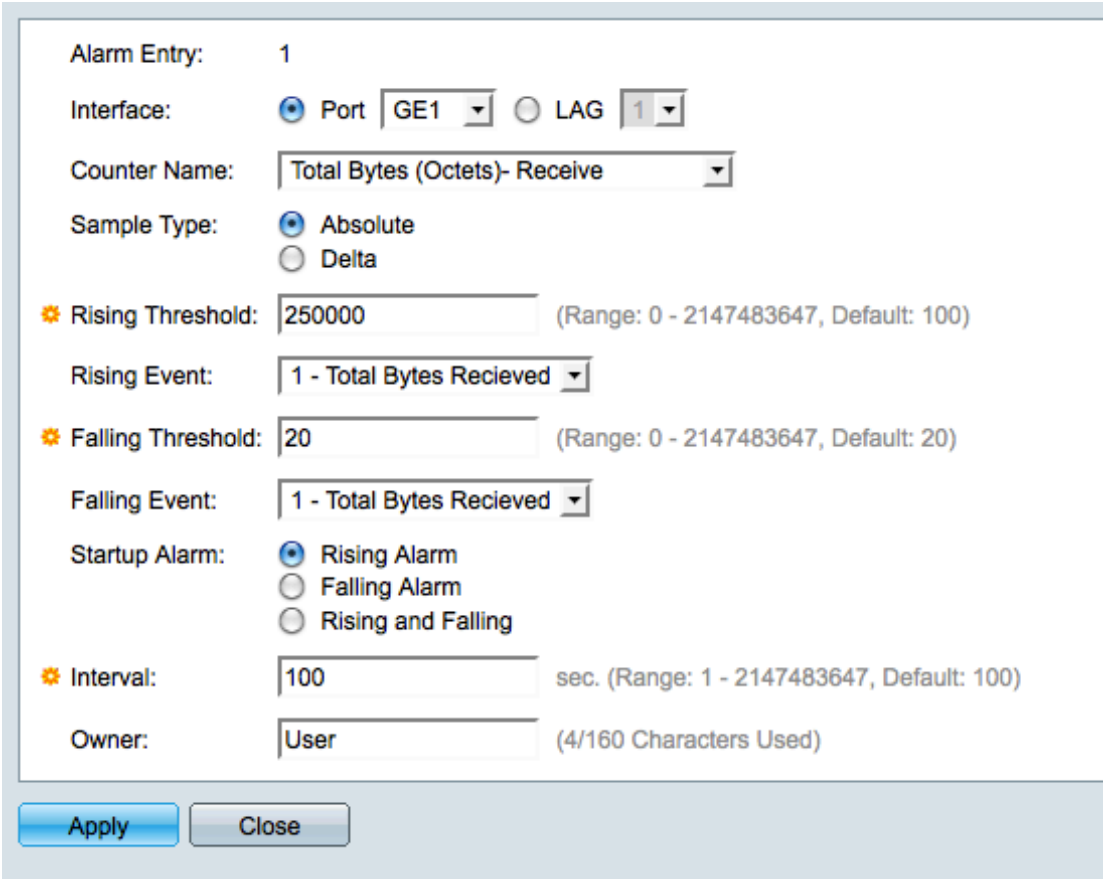
Etapa 9. (Opcional) Marque uma caixa de seleção de evento na Tabela de Eventos e clique em **Deletar** para deletar o evento.

Definir um alarme RMON

Etapa 1. Inicie a sessão no utilitário de configuração da Web e escolha **Status and Statistics > RMON > Alarms**. Será aberta a página *Alarmes*:



Etapa 2. Clique em **Adicionar** para criar um novo alarme. A janela *Add Alarm Entry* é exibida.



Etapa 3. No campo Interface, clique no botão de opção apropriado para definir a interface para a qual o alarme está definido e escolha a interface na lista suspensa apropriada.

·Porta — A porta física no switch.

·LAG — Um grupo de portas que atua como uma única porta.

Etapa 4. Na lista suspensa Nome do contador, escolha a variável a ser medida.

Etapa 5. No campo Tipo de amostra, clique no botão de opção que corresponde ao método de amostragem para gerar um alarme.

·Absoluto — O alarme é acionado quando o limite é ultrapassado.

·Delta — O último valor da amostra é subtraído do valor atual. O alarme será disparado se a diferença nos valores exceder o limite.

Etapa 6. No campo Limite de elevação, insira o valor que dispara o alarme de limite de elevação.

Passo 7. Na lista suspensa Evento crescente, escolha um evento a ser executado quando um evento crescente for disparado. Este evento foi criado na página *Eventos* e é explicado na seção acima.

Etapa 8. No campo Limite de queda, insira o valor que dispara o alarme de limite de queda.

Nota: Depois que um limiar ascendente é ultrapassado, nenhum alarme ascendente adicional ocorrerá até que o limiar descendente também seja ultrapassado. Quando o limiar de queda for ultrapassado, o alarme de limiar de elevação será ativado novamente.

Etapa 9. Na lista suspensa Evento de queda, escolha um evento a ser executado quando um evento de queda for disparado.

Etapa 10. No campo Alarme de inicialização, clique no botão de opção que corresponde ao método que dispara o evento.

·Alarme ascendente — Um valor ascendente aciona o alarme ascendente de limiar.

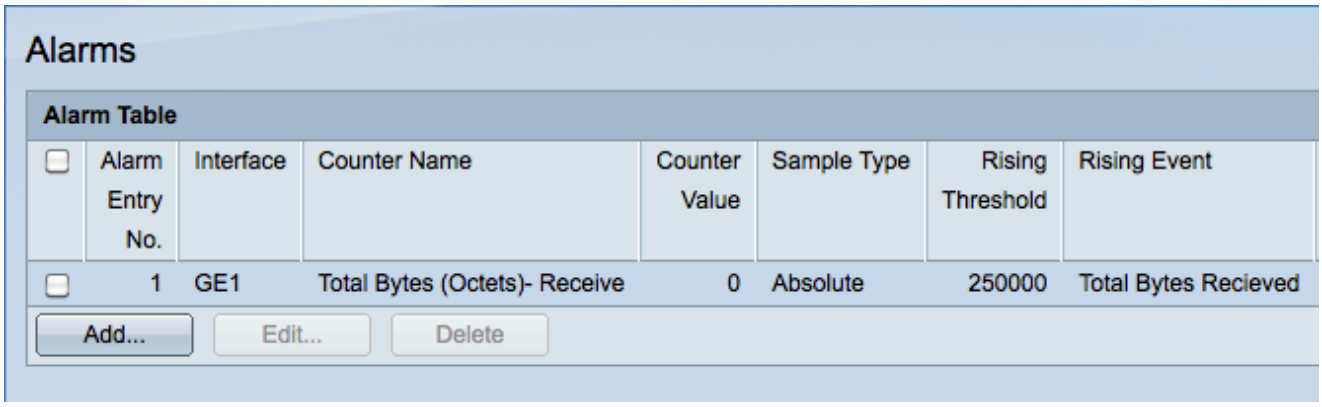
·Alarme de queda — Um valor de queda aciona o alarme de limiar de queda.

·Ascensão e Queda — Tanto os valores de subida como de descida acionam o alarme.

Etapa 11. No campo Intervalo, insira o tempo do intervalo de alarme (em segundos). Esta é a quantidade de tempo que o alarme aguarda antes de verificar se as condições foram atendidas para disparar o alarme.

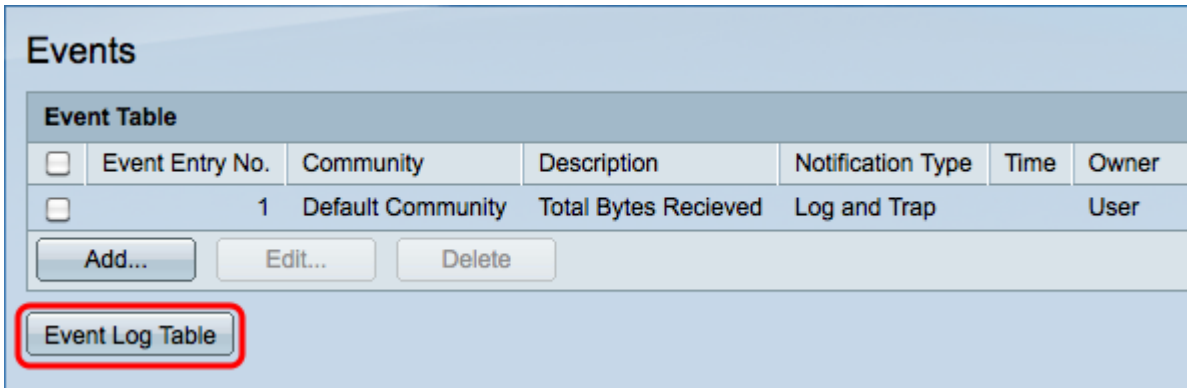
Etapa 12. No campo Proprietário, digite o nome do sistema de gerenciamento de rede que recebeu o alarme ou o nome do usuário que criou o alarme.

Etapa 13. Clique em **Apply** para salvar as alterações e clique em **Close** para sair da janela *Add Alarm Entry*.



Verificar Tabela de Log de Eventos RMON

Etapa 1. Efetue login no utilitário de configuração da Web e escolha **Status and Statistics > RMON > Events**. A página *Eventos* será aberta:



Etapa 2. Clique em **Event Log Table**. A página *Tabela de registro de eventos* é aberta e exibe as seguintes informações:

Observação: as entradas serão gravadas apenas na tabela de log de eventos se Log tiver sido escolhido na Etapa 5 da seção *Criar Evento RMON*.

·Nº de entrada do evento — O número de entrada de log do evento.

·Número de registro — Número de registro no evento.

·Tempo de log — O tempo da entrada do log.

·Descrição — Descrição do evento que disparou o alarme.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.