Como apoiar e configurar o SNMP traps do OS do Cisco catalyst

Índice

Introdução

Este documento descreve as interceptações (traps) compatíveis com o Catalyst OS (CatOS) e como configurá-las no switch.

As operações da armadilha permitem que os agentes do Simple Network Management Protocol (SNMP) enviem notificações assíncronas da ocorrência de um evento. As armadilhas são enviadas em uma base do melhor esforço e sem nenhum método para verificar seu recibo.

Pré-requisitos

Requisitos

Cisco recomenda que antes que você tente esta configuração, se assegure de que você configure corretamente as séries de comunidade snmp no interruptor.

> **Note**: Refira como configurar séries de comunidade snmp para mais informação.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- Catalizador 4500/4000, 5500/5000 de, e Switches do 6500/6000 Series
- Versão cactos 7.3

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando.

Como eu encontro que armadilhas são permitidas em meu interruptor?

Emita o **comando show snmp no** modo enable. Está aqui um exemplo de saída:

```
6509 (enable) show snmp

RMON:                          Enabled
Extended RMON Netflow Enabled : None.
Traps Enabled:
Port,Module,Chassis,Bridge,Repeater,Vtp,Auth,ippermit,Vmps,config,entity,stpx,syslog
Port Traps Enabled: 2/1-2,3/1-48,4/1-8

Community-Access     Community-String
....
....
!--- Output suppressed.
```

Como eu configuro o receptor de armadilha de SNMP no interruptor?

Emita o comando set snmp trap host string.

> **Note**: A sintaxe de comando inclui:
> - host **-** Endereço IP de Um ou Mais Servidores Cisco ICM NT ou pseudônimo IP do sistema para receber o SNMP traps.
> - corda - String de comunidade a usar-se a fim enviar armadilhas da autenticação.

Aqui está um exemplo:

```
6509 (enable) set snmp trap 1.1.1.1 public
SNMP trap receiver added.
```

Emita o **comando show snmp** a fim verificar a adição desta indicação da **armadilha SNMP do grupo**. Está aqui um exemplo de saída:

```
6509 (enable)  show snmp
6509 (enable)  show snmp
RMON:                          Enabled
Extended RMON Netflow Enabled : None.
!--- Output suppressed. .... .... !--- Output suppressed. Trap-Rec-Address  Trap-Rec-Community
--------------       -----------------
```

`1.1.1.1 public`

Como eu permito armadilhas no interruptor, e que cada armadilha significa?

Emita o **comando set snmp trap** a fim permitir ou desabilitar o SNMP traps diferente no sistema. O comando igualmente adiciona uma entrada na tabela do receptor de armadilha da autenticação SNMP.

Sintaxe

ajuste a armadilha SNMP {permita | desabilitação} [tudo | auth | bridge | chassi | config | entidade | entityfru | envfan | envpower | envshutdown | ippermit | módulo | repetidor | stpx | syslog | sistema | vmps | vtp]

> **Note**: Este comando deve estar em *uma* linha.

Descrição da sintaxe

Palavra-chave	Descrição	Armadilha	M
enable	Palavra-chave para permitir o SNMP traps.		
disable	Palavra-chave para desabilitar o SNMP traps.		
tudo	Palavra-chave (opcional) para especificar todos os tipos de armadilha. Refira a documentação do switch antes que você use esta opção.		
auth	Palavra-chave (opcional) para especificar a `armadilha de falha de autenticação do` RFC 1157 .	`authenticationFailure (.1.3.6.1.2.1.11.0.4)`	SN
bridge	Palavra-chave (opcional) para especificar as armadilhas do `newRoot` e do `topologyChange do` RFC 1493 . Refira o BRIDGE-MIB.	`newRoot (.1.3.6.1.2.1.17.0.1)` `topologyChange (.1.3.6.1.2.1.17.0.2)`	BR
chassi	Palavra-chave (opcional) para especificar o `chassisAlarmOn` (`.1.3.6.1.4.1.9.5.0.5`) e armadilha do `chassisAlarmOff` (`.1.3.6.1.4.1.9.5.0.6`) do CISCO-STACK-MIB.	`chassisAlarmOn (.1.3.6.1.4.1.9.5.0.5)` `chassisAlarmOff (.1.3.6.1.4.1.9.5.0.6)`	CI
config	Palavra-chave (opcional) para especificar a armadilha do `sysConfigChange do` CISCO-STACK-MIB.	`sysConfigChangeTrap (.1.3.6.1.4.1.9.5.0.9)`	CI
entidade	Palavra-chave (opcional) para especificar a armadilha do `entityMIB do` ENTITY-MIB.	`entConfigChange (.1.3.6.1.2.1.47.2.0.1)`	EN

entityfru	Palavra-chave (opcional) para especificar a entidade FRU[1].	cefcModuleStatusChange (.1.3.6.1.4.1.9.9.117.2.0.1) cefcPowerStatusChange (.1.3.6.1.4.1.9.9.117.2.0.2) cefcFRUInserted (.1.3.6.1.4.1.9.9.117.2.0.3) cefcFRURemoved (.1.3.6.1.4.1.9.9.117.2.0.4)	Cl
envfan	Palavra-chave (opcional) para especificar o fã ambiental.	ciscoEnvMonFanNotification (.1.3.6.1.4.1.9.9.13.3.0.4)	Cl
envpower	Palavra-chave (opcional) para especificar a potência ambiental.	ciscoEnvMonRedundantSupplyNotification (.1.3.6.1.4.1.9.9.13.3.0.5)	Cl
envshutdown	Palavra-chave (opcional) para especificar o fechamento ambiental.	ciscoEnvMonShutdownNotification (.1.3.6.1.4.1.9.9.13.3.0.1)	Cl
envtemp	Palavra-chave (opcional) para especificar a notificação de temperatura ambiental.	ciscoEnvMonTemperatureNotification (.1.3.6.1.4.1.9.9.13.3.0.3)	Cl
ippermit	A palavra-chave (opcional) para especificar a licença IP negou o acesso do CISCO-STACK-MIB.	ipPermitDeniedTrap (.1.3.6.1.4.1.9.5.0.7)	Cl
macnotification	Palavra-chave (opcional) que especifica a notificação do MAC address.	cmnMacChangedNotification (.1.3.6.1.4.1.9.9.215.2.0.1)	Cl
módulo	Palavra-chave (opcional) para especificar o `moduleUp` e as `armadilhas moduledown do` CISCO-STACK-MIB.	moduleUp (.1.3.6.1.4.1.9.5.0.3) moduleDown (.1.3.6.1.4.1.9.5.0.4)	Cl
repetidor	Palavra-chave (opcional) para especificar o `rptrHealth`, o `rptrGroupChange`, e as armadilhas `rptrResetEvent do` RFC 1516 . Refira o SNMP-REPEATER-MIB.	rptrHealth (.1.3.6.1.2.1.22.0.1) rptrGroupChange (.1.3.6.1.2.1.22.0.2) rptrResetEvent (.1.3.6.1.2.1.22.0.3)	SN
stpx	Palavra-chave (opcional) para especificar a armadilha STPX[2].	stpxInconsistencyUpdate (.1.3.6.1.4.1.9.9.82.2.0.1) stpxLoopInconsistencyUpdate (.1.3.6.1.4.1.9.9.82.2.0.3) stpxRootInconsistencyUpdate (.1.3.6.1.4.1.9.9.82.2.0.2)	Cl
syslog	Palavra-chave (opcional) para especificar as armadilhas da notificação de SYSLOG.	clogMessageGenerated (.1.3.6.1.4.1.9.9.41.2.0.1)	Cl
sistema	Palavra-chave (opcional) para especificar o sistema.	ciscoSystemClockChanged (1.3.6.1.4.1.9.9.131.2.0.1)	Cl
vmps	Palavra-chave (opcional) para especificar a armadilha do `vmVmpsChange do` CISCO-VLAN-MEMBERSHIP-MIB.	vmVmpsChange (.1.3.6.1.4.1.9.9.68.2.0.1)	Cl
vtp	Palavra-chave (opcional) para especificar o VTP[3] do CISCO-VTP-MIB.	vtpConfigDigestError (.1.3.6.1.4.1.9.9.46.2.0.2) vtpConfigRevNumberError (.1.3.6.1.4.1.9.9.46.2.0.1) vlanTrunkPortDynamicStatusChange	Cl

(.1.3.6.1.4.1.9.9.46.2.0.7)
vtpVersionOneDeviceDetected
(.1.3.6.1.4.1.9.9.46.2.0.6)

[1] FRU = unidade substituível de campo

[2] STPX = Ramais do Spanning Tree Protocol

[3] VTP = protocolo VLAN Trunk

Como eu permito armadilhas em portas individuais, tais como a associação/desativo o link?

Emita o **comando set port trap** a fim permitir ou desabilitar a operação da armadilha do link do padrão SNMP para uma porta ou uma faixa de porta. À revelia, todas as armadilhas de porta são desabilitadas.

> **Note**: O módulo Network Analysis Modules (NAM) não apoia este comando.

Sintaxe

*/porta modificação da **armadilha do set port {permita | desabilitação}***

Descrição da sintaxe

- ***modificação/número de porta do*** módulo e a porta no módulo.
- **permita -** Palavra-chave para ativar a armadilha do link SNMP.
- **desabilitação -** Palavra-chave para desativar a armadilha do link SNMP.

Se você permite as armadilhas, as armadilhas correspondentes que gerenciem são a `associação` (`.1.3.6.1.2.1.11.0.3`) e `desativam o link` (`.1.3.6.1.2.1.11.0.2`). Estas armadilhas são do IF-MIB.

Exemplo

Este exemplo mostra como permitir a armadilha de link SNMP para o módulo 1, a porta 2:

```
Console> (enable) set port trap 1/2 enable
Port 1/2 up/down trap enabled.
Console> (enable)
```

Que outras armadilhas podem o Catalyst Switch enviar?

Veja esta tabela:

Nome do objeto MIB	OID	MIB
ciscoFlashCopyCompletionTrap	.1.3.6.1.4.1.9.9.10.1.3.0.1	CISCO-FLASH-MIB
ciscoFlashDeviceChangeTrap	.1.3.6.1.4.1.9.9.10.1.3.0.4	CISCO-FLASH-MIB
ciscoFlashMiscOpCompletionTrap	.1.3.6.1.4.1.9.9.10.1.3.0.3	CISCO-FLASH-MIB
coldstart	.1.3.6.1.6.3.1.1.5.1	RFC1157-SNMP (SNMPv2-MIB)

warmStart	.1.3.6.1.6.3.1.1.5.2	RFC1157-SNMP (SNMPv2-MIB)
tokenRingSoftErrExceededTrap	.1.3.6.1.4.1.9.5.0.10	CISCO-STACK-MIB
lerAlarmOn	.1.3.6.1.4.1.9.5.0.1	CISCO-STACK-MIB
lerAlarmOff	.1.3.6.1.4.1.9.5.0.2	CISCO-STACK-MIB
entSensorThresholdNotification	.1.3.6.1.4.1.9.9.91.2.0.1	CISCO-ENTITY-SENSOR-MIB
fallingAlarm	.1.3.6.1.2.1.16.0.2	RMON-MIB
risingAlarm	.1.3.6.1.2.1.16.0.1	RMON-MIB

Verificar

No momento, não há procedimento de verificação disponível para esta configuração.

Troubleshooting

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Informações Relacionadas

- Produtos da Cisco & serviços - Switches
- Armadilhas de SNMP do Cisco IOS suportadas e como configurá-las
- Exemplos de configuração e TechNotes dos Serviços de aplicação IP
- Transferências do Network Management Software - MIBs (clientes registrados somente)
- Página de suporte da switching de LAN
- Suporte Técnico e Documentação - Cisco Systems