如何支持和配置Cisco Catalyst OS SNMP陷阱

目录

简介

本文描述Catalyst OS的陷阱(CatOS)支持和如何配置他们在交换机。

陷阱操作允许简单网络管理协议(SNMP)代理程序发送事件的出现的异步通知。陷阱被发送在尽力而为基础和，不用任何方法验证他们的收据。

先决条件

要求

思科建议，在您尝试此配置前，请保证您适当地配置在交换机的SNMP团体字符串。

> **注意**：参考如何配置SNMP团体字符串欲知更多信息。

使用的组件

本文档中的信息基于以下软件和硬件版本：

- Catalyst 4500/4000， 5500/5000和6500/6000系列交换机
- CatOS版本7.3

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原

始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

如何发现什么陷阱在我的交换机启用？

发出**show snmp命令**在特权模式。以下为示例输出：

```
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.
```

如何配置在交换机的SNMP陷阱接收器？

发出set snmp trap host string命令。

> **注意**：命令语法包括：
> -主机-收到SNMP陷阱的系统的IP地址或IP别名。
> -字符串-使用的社区字符串为了发送验证陷阱。

示例如下：

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

发出**show snmp命令**为了验证此**集合SNMP陷阱**语句的新增内容。以下为示例输出：

```
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
```

如何启用在交换机的陷阱，并且每个陷阱是什么意思？

发出**set snmp trap命令**为了启用或禁用在系统的不同的SNMP陷阱。命令也添加一个条目到SNMP验证陷阱接收器表。

语法

设置SNMP陷阱{enable (event)|禁用} [全部|验证|网桥|机箱|设置|实体|entityfru|envfan|envpower|envshutdown|ippermit|模块|中继器|stpx|Syslog|系统|VMPS|VTP]

> **注意**：此命令应该在一行上。

语法说明

关键字	说明	陷阱
enable (event)	启用SNMP陷阱的关键字。	
禁用	禁用SNMP陷阱的关键字。	
所有	(指定所有陷阱类型的可选)关键字。在您使用此选项前，参考交换机文档。	
验证	(指定从RFC 1157的可选)关键字。	authenticat (.1.3.6.1.2
网桥	(指定newRoot和topologyChange陷阱的可选)关键字从RFC 1493。参考的BRIDGE-MIB。	newRoot (.1.3.6.1.2 topologyCha

机箱	(可选）规定来自CISCO-STACK-MIB 的chassisAlarmOn (1.3.6.1.4.1.9.5.0.5)和chassisAlarmOff (1.3.6.1.4.1.9.5.0.6)陷阱的关键字。	chassisAlar chassisAlar
设置	(指定从CISCO-STACK-MIB的sysConfigChange陷阱的可选)关键字。	sysConfigCh (.1.3.6.1.4
实体	(指定从ENTITY-MIB的entityMIB陷阱的可选)关键字。	entConfigCh (.1.3.6.1.2
entityfru	(指定实体FRU的可选)关键字[1]。	cefcModuleS (.1.3.6.1.4 cefcPowerSt (.1.3.6.1.4 cefcFRUInse (.1.3.6.1.4 cefcFRURemo (.1.3.6.1.4
envfan	(指定环境风扇的可选)关键字。	ciscoEnvMon (.1.3.6.1.4
envpower	(指定环境电源的可选)关键字。	ciscoEnvMon (.1.3.6.1.4
envshutdown	(指定环境关闭的可选)关键字。	ciscoEnvMon (.1.3.6.1.4
envtemp	(指定环境温度通知的可选)关键字。	ciscoEnvMon (.1.3.6.1.4
ippermit	(指定从CISCO-STACK-MIB的IP Permit拒绝访问的可选)关键字。	ipPermitDen (.1.3.6.1.4
macnotification	(指定MAC地址通知的可选)关键字。	cmnMacChang (.1.3.6.1.4
模块	(指定moduleUp和可选)关键字从CISCO-STACK-MIB。	moduleUp (.1.3.6.1. moduleDown (.1.3.6.1.
中继器	(指定rptrHealth、rptrGroupChange和rptrResetEvent陷阱的可选)关键字从RFC 1516 。参考的SNMP-REPEATER-MIB。	rptrHealth (.1.3.6.1.2 rptrGroupCh (.1.3.6.1.2 rptrResetEv (.1.3.6.1.2
stpx	(指定STPX2陷阱的可选)关键字。	stpxInconsi (.1.3.6.1.4 stpxLoopInc (.1.3.6.1.4 stpxRootInc (.1.3.6.1.4
Syslog	(指定系统日志通知陷阱的可选)关键字。	clogMessage (.1.3.6.1.4
系统	(指定系统的可选)关键字。	ciscoSystem (1.3.6.1.4.
VMPS	(指定从CISCO-VLAN-MEMBERSHIP-MIB的vmVmpsChange陷阱的可选)关键字。	vmVmpsChang (.1.3.6.1.4
VTP	(指定从CISCO-VTP-MIB的VTP的可选)关键字[3]。	vtpConfigDi (.1.3.6.1.4 vtpConfigRe (.1.3.6.1.4 vlanTrunkPo (.1.3.6.1.4

vtpVersionO
(.1.3.6.1.4

[1] FRU =现场可换部件

[2] STPX =生成树协议扩展

[3] VTP = VLAN中继协议

如何启用在单个端口的陷阱，例如联结/链路down ？

发出**set port trap命令**为了启用或禁用标准SNMP链路陷阱的操作端口或端口范围的。默认情况下，所有端口陷井禁用。

> **注意**：网络分析模块(NAM)不支持此命令。

语法

set port trap mod/port {enable (event)|禁用}

语法说明

- *mod/port-number*模块和端口模块的。
- **Enable关键字**激活SNMP链路陷阱。
- **禁用**-撤销SNMP链路陷阱的关键字。

如果启用陷阱，生成的对应的陷阱是(.1.3.6.1.2.1.11.0.3)和down (.1.3.6.1.2.1.11.0.2)。这些陷阱是从IF-MIB。

示例

此示例显示如何启用模块的1 SNMP链路陷阱，端口2 ：

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

其他陷阱能Catalyst交换机发送什么？

参见此表：

MIB对象对象名	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	RFC 1157 SNMP (SNMPv2-MIB)
热启动	.1.3.6.1.6.3.1.1.5.2	RFC 1157 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

验证

当前没有可用于此配置的验证过程。

故障排除

目前没有针对此配置的故障排除信息。

相关信息

- 思科产品&服务-交换机
- >支持Cisco IOS SNMP陷阱以及如何配置他们
- IP应用服务配置示例和TechNotes
- 网络管理软件下载- MIB (仅限注册用户)
- LAN 交换技术支持页
- 技术支持和文档 - Cisco Systems