So unterstützen und konfigurieren Sie Cisco Catalyst OS SNMP-Traps

Inhalt

Einführung

Dieses Dokument beschreibt die Traps, die vom Catalyst OS (CatOS) unterstützt werden, und wie diese auf dem Switch konfiguriert werden.

Mithilfe von Trap-Vorgängen können SNMP-Agenten asynchrone Benachrichtigungen über das Auftreten eines Ereignisses senden. Traps werden nach bestem Bemühen und ohne jede Methode zur Verifizierung ihres Empfangs gesendet.

Voraussetzungen

Anforderungen

Cisco empfiehlt, vor dem Versuch dieser Konfiguration sicherzustellen, dass Sie die SNMP-Community-Strings auf dem Switch ordnungsgemäß konfiguriert haben.

> **Hinweis**: Weitere Informationen finden Sie unter Konfigurieren von SNMP-Community-Strings.

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf den folgenden Software- und Hardwareversionen:

- Catalyst Switches der Serien 4500/4000, 5500/5000 und 6500/6000
- CatOS Version 7.3

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.

Wie finde ich heraus, welche Traps auf meinem Switch aktiviert sind?

Geben Sie den Befehl **show snmp** im Aktivierungsmodus aus. Hier eine Beispielausgabe:

```
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.
```

Wie konfiguriere ich den SNMP-Trap-Empfänger auf dem Switch?

Geben Sie den Befehl **set snmp trap** *host string ein*.

> **Hinweis**: Die Befehlssyntax umfasst Folgendes:
> - host **-** IP-Adresse oder IP-Alias des Systems für den Empfang von SNMP-Traps.
> - String - Community String, der zum Senden von Authentifizierungsfallen verwendet wird.

Hier ein Beispiel:

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

Geben Sie den Befehl **show snmp** ein, um das Hinzufügen dieser **set snmp trap-**Anweisung zu überprüfen. Hier eine Beispielausgabe:

```
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
```

Wie aktiviere ich Traps auf dem Switch, und was bedeuten diese Traps?

Geben Sie den Befehl **set snmp trap** ein, um die verschiedenen SNMP-Traps im System zu aktivieren oder zu deaktivieren. Der Befehl fügt außerdem einen Eintrag in die Empfängertabelle für SNMP-Authentifizierungsprofile hinzu.

Syntax

set snmp trap {enable | disable} [Alle | auth | Brücke | Chassis | Konfiguration | Einheit | entityfru | umbenennen | Mittel | Umschalten | ippermit | Modul | Repeater | stpx | Syslog | System | vmps | vtp]

> **Hinweis**: Dieser Befehl sollte in *einer* Zeile stehen.

Syntaxbeschreibung

Schlüsselwort	Beschreibung	Trap
aktivieren	Schlüsselwort zum Aktivieren von SNMP-Traps.	
deaktivieren	Schlüsselwort zum Deaktivieren von SNMP-Traps.	
alle	(Optional) Schlüsselwort, um alle Trap-Typen anzugeben. Bevor Sie diese Option verwenden, lesen Sie die Switch-Dokumentation.	
Eier	(Optional) Schlüsselwort zur Angabe des `authenticationFailure`-Traps aus RFC 1157.	`AuthenticationFailure (.1.3.6.1.2.1.11.0.4)`
Brücke	(Optional) Schlüsselwort zur Angabe der `neuenRoot-` und `Topologieänderungen` Traps aus RFC 1493. Siehe BRIDGE-MIB.	`newRoot (.1.3.6.1.2.1.17.0.1)` `Topologieänderung (.1.3.6.1.2.1.17.0.2)`
Gehäuse	(Optional) Schlüsselwort zur Angabe der `ChassisAlarmOn` (`.1.3.6.1.4.1.9.5.0.5`)- und `ChassisAlarmOff` (`.1.3.6.1.4.1.9.5.0.6`)-Traps der CISCO-STACK-MIB.	`ChassisAlarmOn (.1.3.6.1.4.1.9.5.0` `ChassisAlarmOff (.1.3.6.1.4.1.9.5.`
Konfiguration	(Optional) Schlüsselwort zur Angabe des Traps `sysConfigChange` aus der CISCO-STACK-MIB.	`sysConfigChangeTrap (.1.3.6.1.4.1.9.5.0.9)`
Einheit	(Optional) Schlüsselwort zum Angeben des `entityMIB`-Traps aus der ENTITY-MIB.	`entConfigChange (.1.3.6.1.2.1.47.2.0.1)`
Tityfru	(Optional) Schlüsselwort, um die Einheit FRU[1] anzugeben.	`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)
beneiden	(Optional) Schlüsselwort zur Angabe des Umgebungslüfters.	ciscoEnvMonFanNotification (.1.3.6.1.4.1.9.9.13.3.0.4)
umsetzen	(Optional) Schlüsselwort zur Angabe der Umgebungsleistung.	ciscoEnvMonRedundantSupplyNotifica (.1.3.6.1.4.1.9.9.13.3.0.5)
Umschalten	(Optional) Das Schlüsselwort, um das Herunterfahren der Umgebung anzugeben.	ciscoEnvMonShutdownNotification (.1.3.6.1.4.1.9.9.13.3.0.1)
umplanen	(Optional) Schlüsselwort zur Angabe der Umgebungstemperatur-Benachrichtigung.	ciscoEnvMonTemperatureNotificatior (.1.3.6.1.4.1.9.9.13.3.0.3)
vertreiben	(Optional) Schlüsselwort zur Angabe des IP Permit Denied Access from the CISCO-STACK-MIB.	ipPermitDeniedTrap (.1.3.6.1.4.1.9.5.0.7)
Maknotifizierung	(Optional) Schlüsselwort, das die MAC-Adressenbenachrichtigung angibt.	cmnMacChangedNotification (.1.3.6.1.4.1.9.9.215.2.0.1)
Modul	(Optional) Schlüsselwort zur Angabe der `ModulUp-` und `ModulDown-`Traps aus der CISCO-STACK-MIB.	ModulUp (.1.3.6.1.4.1.9.5.0.3) ModulDown (.1.3.6.1.4.1.9.5.0.4)
Repeater	(Optional) Schlüsselwort zur Angabe der `rptrHealth-`, `rptrGroupChange`- und `rptrResetEvent-`Traps aus RFC 1516. Weitere Informationen finden Sie unter 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)
stpx	(Optional) Schlüsselwort zur Angabe des STPX[2]-Traps.	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)
Syslog	(Optional) Schlüsselwort zur Angabe der Syslog-Benachrichtigungsfallen.	clogMessageGenerated (.1.3.6.1.4.1.9.9.41.2.0.1)
System	(Optional) Schlüsselwort, um das System anzugeben.	ciscoSystemClockChanged (1.3.6.1.4.1.9.9.131.2.0.1)
VMPS	(Optional) Schlüsselwort zur Angabe des `vmVmpsChange-`Traps aus der CISCO-VLAN-MEMBERSHIP-MIB.	vmVMPSChange (.1.3.6.1.4.1.9.9.68.2.0.1)
VTP	(Optional) Schlüsselwort zur Angabe des VTP[3] aus der 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 (.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 = vor Ort austauschbare Einheit

[2] STPX = Spanning Tree Protocol Extensions

[3] VTP = VLAN-Trunk-Protokoll

Wie aktiviere ich Traps auf einzelnen Ports, z. B. linkUp/linkDown?

Geben Sie den Befehl **set port trap** ein, um den Betrieb des Standard-SNMP-Link-Traps für einen Port oder Port-Bereich zu aktivieren oder zu deaktivieren. Standardmäßig sind alle Port-Traps deaktiviert.

> **Hinweis**: Das Network Analysis Module (NAM) unterstützt diesen Befehl nicht.

Syntax

Port Trap *Mod/Port* {enable} einstellen | Deaktivieren}

Syntaxbeschreibung

- ***mod/port:*** Nummer des Moduls und des Ports des Moduls.
- **enable -** Schlüsselwort zum Aktivieren des SNMP-Verknüpfungsfadens.
- **disable -** Schlüsselwort zum Deaktivieren des SNMP-Link-Traps.

Wenn Sie die Traps aktivieren, sind die entsprechenden Traps, die generiert werden, `linkUp` (`.1.3.6.1.2.1.11.0.3`) und `linkDown` (`.1.3.6.1.2.1.11.0.2`). Diese Traps stammen von der IF-MIB.

Beispiel

Dieses Beispiel zeigt, wie das SNMP-Link-Trap für Modul 1, Port 2 aktiviert wird:

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

Welche weiteren Traps kann der Catalyst Switch senden?

Siehe folgende Tabelle:

MIB-Objektname	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
Kaltstart	.1.3.6.1.6.3.1.1.5.1	RFC 1157-SNMP (SNMPv2-MIB)
WarmStart	.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
fallenderAlarm	.1.3.6.1.2.1.16.0.2	RMON-MIB
steigendAlarm	.1.3.6.1.2.1.16.0.1	RMON-MIB

Überprüfen

Für diese Konfiguration ist derzeit kein Überprüfungsverfahren verfügbar.

Fehlerbehebung

Für diese Konfiguration sind derzeit keine spezifischen Informationen zur Fehlerbehebung verfügbar.

Zugehörige Informationen

- Cisco Produkte und Services - Switches
- Unterstützte Cisco IOS SNMP-Traps und Konfigurieren dieser Traps
- Konfigurationsbeispiele für IP-Anwendungsdienste und technische Hinweise
- Netzwerkmanagement-Software-Downloads - MIBs (nur registrierte Kunden)
- Support-Seite für LAN-Switching
- Technischer Support und Dokumentation - Cisco Systems