SNMP MIB and Trap Information

This appendix describes the Simple Network Management Protocol (SNMP) traps sent by the Cisco Videoscape Distribution Suite-TV (VDS-TV).

Overview

You can manage the servers by way of SNMP from a Network Management System (NMS). To implement SNMP management, the servers must be configured with a management IP address, SNMP community strings, and contact information.

For more information about configuring the server for SNMP communication, see the "Configuring the SNMP Agent" section on page 4-95.

Note We recommend configuring a VLAN for management traffic.

SNMP management features on the servers include:

- SNMPv1, SNMPv2c, and SNMPv3
- Standard MIBs

SNMP Agent

The SNMP agent of the server uses certain variables that are included in a Cisco Management Information Base (MIB) file.

The SNMP agent is controlled by the following commands:

```
# service snmpd start
# service snmpd stop
# service snmpd restart
```

The snmpd service **rc** script automatically configures the snmpd service to be started in Linux run-levels 5 and 6. To make any changes to this behavior, the **chkconfig** or **ntsysv** commands can be used. The following command configures snmpd to be managed by using the **chkconfig** command:

```
# chkconfig --add snmpd
```

The following command configures snmpd to be turned on in run levels 5 and 6:

```
# chkconfig --level 56 snmpd on
```

SNMP Log

The SNMP log file, snmpd.log, is located in the /arroyo/log directory. All log entries use UTC for the time stamp. All VDS-TV-specific SNMP traps are logged in the snmpd.log file.

SNMP Agent on a CDSM or VVIM

The SNMP agent on the CDSM must be manually configured, you cannot configure the SNMP settings on the CDSM by using the **Configure > Server Level > SNMP** page. Check that the snmpd.conf file on the CDSM is properly configured by logging in to the CDSM as user *root*, going to the /usr/local/share/snmp directory and viewing the snmpd.conf file. If the SNMP settings are not correct, manually configure them by editing the snmpd.conf file.

SNMP Management Objects and Traps

The VDS SNMP agent and Management Information Base (MIB) file are compliant with the Internet Engineering Task Force (IETF) standards for SNMP v1, SNMP v2c, and SNMPv3. For a list of SNMP-associated Request For Comment (RFC) specifications, see the "RFC Compliance" section on page D-6.

The Cisco CDS-TV MIBs consist of the following:

- CISCO-CDS-TV-MIB.my
- CISCO-CDSTV-SERVICES-MIB.my
- CISCO-CDSTV-FSI-MIB.my
- CISCO-CDSTV-INGESTMGR-MIB.my
- CISCO-CDSTV-BWMGR-MIB.my
- CISCO-CDSTV-INGEST-TUNING-MIB.my
- CISCO-CDSTV-CS-STATS-MIB.my
- CISCO-CDSTV-AUTHMGR-MIB.my
- CISCO-CDSTV-SERVER-MIB.my
- CISCO-CDSTV-ISA-MIB.my (Only applicable to ISA environments)

The Cisco CDS-TV MIBs are available through the CDSM, and are dependent on the following MIBs distributed on Cisco.com:

- ftp://ftp.cisco.com/pub/mibs/v2/CISCO-SMI.my
- ftp://ftp.cisco.com/pub/mibs/v2/CISCO-TC.my
- ftp://ftp.cisco.com/pub/mibs/v2/CISCO-PRODUCTS-MIB.my
- ftp://ftp.cisco.com/pub/mibs/v2/INET-ADDRESS-MIB.my
- ftp://ftp.cisco.com/pub/mibs/v2/DIFFSERV-DSCP-TC.my

You can download the MIBs by doing the following:

Step 1 Choose **Configure > Server Level > SNMP Agent**. The SNMP Agent page is displayed with a list of the MIB files at the bottom of the page.

Step 2 To save the file locally, right-click the MIB filename, and choose **Save As**, **Save Target As**, or a similar save command.

To view the file, click the MIB filename.

The CISCO-CDS-TV-MIB.txt file has the following MIB nodes:

- cdstvConfigObjects—Configuration of servers
- cdstvMonitorObjects—Monitoring of cache-fill, streaming, disk states, and services running
- cdstvNotifyObjects—Objects specific to traps (notifications), for example, Managed Services Architecture (MSA) event objects

Table D-1 describes the traps in the CISCO-CDS-TV-MIB.

Table D-1 Cisco VDS-TV Traps

Trap	Description
cdstvDiskHealthUp	Previously inactive disk is now active and ready, that is, the disk has returned to the OK (0) state.
cdstvDiskHealthDown	Active disk is now inactive, that is, it has left the OK (0) state.
cdstvMSAEvent	MSA event (error) has occurred.
cdstvServiceUp	Previously stopped service is now running, that is, it has left the not running state. The cdstvServiceName object, which contains the name of the service, is sent with the trap.
cdstvServiceDown	Previously running service is now stopped, that is, it has left the running state. The cdstvServiceName object, which contains the name of the service, is sent with the trap.
cdstvDiskUsageHigh	Disk usage on the system has crossed the maximum usage threshold. The cdstvDiskUsagePercent object, which contains the percentage of the disk that is used, is sent with the trap. This trap corresponds to the Disk Capacity Notify field on the System Threshold page. For more information, see the "Setting System Thresholds" section on page 7-15. When the disk usage exceeds the threshold set for the Disk Capacity Notify field, the cdstvDiskUsageHigh trap is sent.
cdstvDiskUsageNormal	Disk usage on the system has returned to a value within the usage threshold. The cdstvDiskUsagePercent object, which contains the percentage of the disk that is used, is sent with the trap.
cdstvLinuxFSUsageHigh	Linux file system (FS) usage on the server has crossed the maximum usage threshold. The cdstvLinuxFSMountPoint and cdstvLinuxFSUsagePercent objects, which contain the mount point and the percentage used, are sent with the trap.

Table D-1 Cisco VDS-TV Traps (continued)

Trap	Description
cdstvLinuxFSUsageNormal	Linux file system (FS) usage on the server has returned to a value within the usage threshold. The cdstvLinuxFSMountPoint and cdstvLinuxFSUsagePercent objects, which contain the mount point and the percentage used, are sent with the trap.
cdstvPortLossHigh	Port loss on the system has crossed the maximum threshold. The cdstvPortLossPercent object, which contains port loss percentage, is sent with the trap.
cdstvPortLossNormal	Port loss on the system has returned to a value within the threshold. The cdstvPortLossPercent object, which contains port loss percentage, is sent with the trap.
cdstvSysHealthUp	Previously abnormal system health parameter is now normal; that is, it has left the not OK state. See Table D-2 on page D-6 for the descriptions of the objects sent with this trap.
cdstvSysHealthDown	Previously normal system health parameter is now abnormal; that is, it has left the OK state. See Table D-2 on page D-6 for the descriptions of the objects sent with this trap.
cdstvBrokenAsset	Signifies that one or more assets on a Vault or ISV are broken. A trap is sent whenever the number of broken assets found changes, whether from 0 to *n*, *n* to *m*, or *m* to 0. The trap contains one object, cdstvBrokenAssets, which specifies the current number of broken assets. The broken asset information stays in memory and is not persisted in the database. **Note** The cdstvBrokenAssets value is only valid if the Vault is the master Vault, which can be verified by the cdstvVaultMasterSlaveStatus object.
cdstvServerStatusSlave	This server is now a slave. The cdstvServerMasterSlaveStatus object is set when the server status changes to master or slave; it has two possible values: master (1) and slave (2). A value of 0 means that the status is not yet available from statsd.
cdstvServerStatusMaster	This server is now a master. The cdstvServerMasterSlaveStatus object is set when the server status changes to master or slave; it has two possible values: master (1) and slave (2). A value of 0 means that the status is not yet available from statsd.
cdstvSetupIpChanged	Setup IP address has changed (Streamer and ISV only). If Setup IP and Control IP are the same (Setup/Control IP) and both change simultaneously, both cdstvSetupIpChanged and cdstvControlIpChanged traps are sent.
cdstvControlIpChanged	Control IP address has changed (Streamer and ISV only). If Setup IP and Control IP are the same (Setup/Control IP) and both change simultaneously, both cdstvSetupIpChanged and cdstvControlIpChanged traps are sent.

Table D-1 Cisco VDS-TV Traps (continued)

Trap	Description
cdstvDbConnectionFailed	Database synchronization connection from this VDS server to another VDS server has failed. The cdstvDbConnectionFailedIp OID contains the IP address of the server to which a database connection failed.
cdstvLinuxFSReadOnly	Signifies that the Linux partition indicated by cdstvLinuxFSMountPoint is read-only.
cdstvLinuxFSReadWrite	Signifies that the Linux partition indicated by cdstvLinuxFSMountPoint is now back to normal (read-write).
cdstvLinkUp	Signifies that the Ethernet interface and the Ethernet cable is up and/or connected
cdstvLinkDown	Signifies that the Ethernet interface and the Ethernet cable is down and/or not connected

Monitored Broken Assets SNMP Traps

After the statsd process is started, it waits 5 minutes (300 seconds) before collecting statistics. If a broken asset occurs within these 5 minutes, it is detected and the cdstvBrokenAsset trap is sent.

After the first cycle of collecting statistics is complete, statsd waits 60 minutes from the beginning of the previous cycle before collecting statistics again. This repeats every 60 minutes.

Note If at any point mirroring is active, the statistics collection is skipped.

The time delay in receiving the cdstvBrokenAsset trap after a broken asset occurs depends on how much time is left until the next time statsd collects content statistics.

Monitored Services SNMP Traps

The services reported as up or down in SNMP correspond to the services on the Service Monitor page. For more information on the monitored services, see the "Services Monitor" section on page 5-42.

For the cdstvServiceUp and cdstvServiceDown traps in the CISCO-CDSTV-SERVICES-MIB, if the database shuts down, a cdstvServiceDown trap is sent for the Cisco DB server, but no other services can be monitored without the database running. No SNMP traps are sent for services until the database is functional again.

If the SNMP agent itself is down, the CDSM shows the Cisco SNMP Server as "Not Running" but no SNMP trap can be sent for this service because the SNMP agent itself is down.

If the VDS server is shut down cleanly, there may be a cdstvServiceDown trap sent for the Cisco SNMP Server before the entire server shuts down. No traps can be sent until the SNMP agent is running.

System Health Threshold Crossing Alerts

The temperature, fans, and power are monitored on the VDS servers and the states and thresholds are displayed on the Server Vitals page. See the "Server Vitals" section on page 5-37. If a threshold is exceeded, an alarmed event is registered on the CDSM and the cdstvSysHealthDown trap is sent with information about the threshold crossing alert (TCA).

Note The Server Vitals page is displayed only if the CDSM Health Monitor feature is enabled. For more information, see the "CDSM or VVIM Health Monitoring" section on page F-19.

Table D-2 describes the objects that are sent with the cdstvSysHealthUp and cdstvSysHealthDown traps.

Table D-2 System Health SNMP Trap Objects

Descriptor	Possible values	Description
cdstvSysHealthName	String	Name of the system health monitoring parameter, for example, VBAT Voltage.
cdstvSysHealthType	1—Fan-speed 2—Voltage 3—Temperature 4—Chassis intrusion 5—Power supply failure	Type of the system health monitoring parameter.
cdstvSysHealthReading	Integer	Current reading (value) of the system health parameter; for example, fan speed, voltage, or temperature. Fan speed is expressed in rpm, voltage in mV and temperature in degree Celsius. For chassis intrusion and power-supply failure, 1 denotes an error condition, and 0 denotes normal condition.
cdstvSysHealthHighLimit	Integer	Higher limit (threshold) of the system health parameter. Voltage is expressed in mV and temperature in degree Celsius. Not applicable for other parameters such as fan speed.
cdstvSysHealthLowLimit	Integer	Lower limit (threshold) of the system health parameter. Fan speed is expressed in rpm and voltage in mV. Not applicable for other parameters such as temperature.
cdstvSysHealthStatus	1—Normal 2—Low 3—High 4—Not-OK	Current status of the system health parameter. The not-ok value applies to power supply failure and chassis intrusion, because high and low limits do not apply to these parameters.

RFC Compliance

Table D-3 is a list of SNMP RFC standards.

Table D-3 SNMP RFC Standards

RFC Standard	Title
RFC 1155 (STD0016)	Structure and Identification of Management Information for TCP/IP-based Internets
RFC 1157 (STD0015)	Simple Network Management Protocol (SNMP)
RFC 1212 (STD0016)	Concise MIB Definitions
RFC 1213 (STD0017)	Management Information Base for Network Management of TCP/IP-based internets:MIB-II

Table D-3 SNMP RFC Standards (continued)

RFC Standard	Title
RFC 2790 (Draft Standard)	Host Resources MIB
RFC 1901(Historic)	Introduction to Community-based SNMPv2
RFC 1902 (Draft Standard)	Structure of Management Information for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1903 (Draft Standard)	Textual Conventions for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1904 (Draft Standard)	Conformance Statements for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1905 (Draft Standard)	Protocol Operations for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1906 (Draft Standard)	Transport Mappings for Version 2 of the Simple Network Management Protocol (SNMPv2)
RFC 1910 (Historic)	User-based Security Model for SNMPv2
RFC 2011(Proposed Standard - Updates RFC 1213)	SNMPv2 Management Information Base for the Internet Protocol using SMIv2
RFC 2012 (Proposed Standard)	SNMPv2 Management Information Base for the Transmission Control Protocol using SMIv2
RFC 2013 (Proposed Standard)	SNMPv2 Management Information Base for the User Datagram Protocol using SMIv2
RFC 2096 (Proposed Standard)	IP Forwarding Table MIB
RFC 2863 (Draft Standard)	The Interfaces Group MIB
RFC 3410 (Informational)	Introduction and Applicability Statements for Internet-Standard Management Framework
RFC 3411 (STD0062)	An Architecture for Describing Simple Network Management Protocol (SNMP) Management Frameworks
RFC 3412 (STD0062)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 3413 (STD0062)	Simple Network Management Protocol (SNMP) Applications
RFC 3414 (STD0062)	User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 3415 (STD0062)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 3416 (STD0062)	Version 2 of the Protocol Operations for the Simple Network Management Protocol (SNMP)
RFC 3417 (STD0062)	Transport Mappings for the Simple Network Management Protocol (SNMP)
RFC 3418 (STD0062)	Management Information Base (MIB) for the Simple Network Management Protocol (SNMP)

Table D-3 SNMP RFC Standards (continued)

RFC Standard	Title
RFC 2570 (Informational)	Introduction to Version 3 of the Internet-standard Network Management Framework
RFC 2571 (Draft Standard)	An Architecture for Describing SNMP Management Frameworks
RFC 2572 (Draft Standard)	Message Processing and Dispatching for the Simple Network Management Protocol (SNMP)
RFC 2573 (Draft Standard)	SNMP Applications
RFC 2574 (Draft Standard)	User-based Security Model (USM) for Version 3 of the Simple Network Management Protocol (SNMPv3)
RFC 2575 (Draft Standard)	View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)
RFC 2576 (Proposed Standard)	Coexistence between Version 1, Version 2, and Version 3 of the Internet-standard Network Management Framework
RFC 2578 (STD0058)	Structure of Management Information Version 2 (SMIv2)
RFC 2579 (STD0058)	Textual Conventions for SMIv2
RFC 2580 (STD0058)	Conformance Statements for SMIv2