Release Notes for Cisco Video Assurance Management Solution 3.0

Revised: September 14, 2010, OL-16499-03

Contents

Note Visit http://www.cisco.com/en/US/products/ps9518/prod_release_notes_list.html to view the latest version of these release notes.

Introduction

Cisco VAMS 3.0 provides service providers with a modular, end-to-end video assurance management architecture, including real-time, centralized monitoring of headends, hubs, core, distribution, regional, and aggregation networks for broadcast video services.

Cisco VAMS includes a service-aware dashboard that pinpoints and correlates alarms related to video service availability and quality from the headend or the transport network. Using Cisco VAMS you can monitor and manage video services, such as linear broadcast and video on demand (VoD) based on MPEG-2 transmission streams (TS) and uncompressed flows.

See Solution Requirements, page 6 for descriptions of the solution components and required software versions.

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Cisco VAMS 3.0 uses Cisco Multicast Manager (CMM 3.1) with patch 3.1.1 for multicast monitoring and troubleshooting functions, such as monitoring of VidMon devices, and the Cisco ROSA Copernicus Network Management System (NMS) for monitoring of video headend events.

Additionally, the Cisco VAMS 3.0 system architecture includes an interface between Cisco Info Center and CMM. This interface is provided by:

- The Cisco Info Center Object Server (central DB)
- IBM Tivoli Business and Services Manager (TBSM), a service dashboard and visualization tool
- IBM Tivoli Impact, which supports the definition of service and network correlations

This accomplishes two key objectives for Cisco VAMS 3.0. It provides:

- Connectivity between Cisco ANA, CMM, the Cisco ROSA NMS, and Cisco Info Center.
- A "Single Pane of Glass" toolset[1] for Cisco VAMS 3.0.

Cisco Info Center contains rules files that specify the rules that define multicast alerts from various sources, such as probes, routers, Cisco 7600 series routers, Cisco ASR 9000 aggregation series routers, Digital Content Managers (DCMs), and other network management systems. The rules files contains code that extracts the multicast group and source information from these alerts and provides the operator with a Launch CMM Multicast Trace option and a Launch CMM Tree Change report option.

By integrating CMM and the Cisco ROSA NMS with Cisco Info Center you can view all the alarm conditions and data for service level correlation and analysis. Additionally, for CMM events, you can launch troubleshooting and diagnostic analysis directly from Cisco Info Center.

Cisco VAMS 3.0 supports several third-party video probes.CMM supports video probes in two ways:

- CMM can receive SNMP traps directly from the following video probes or element managers:
  - IneoQuest iVMS
  - BridgeTech probes
  - Mixed Signals probes

Note Although CMM does not generate events or status from iVMS traps, CMM displays the traps.

- In addition, CMM can display flow trace status for probes for which it can be configured to poll directly:
  - IneoQuest probes
  - BridgeTech probes

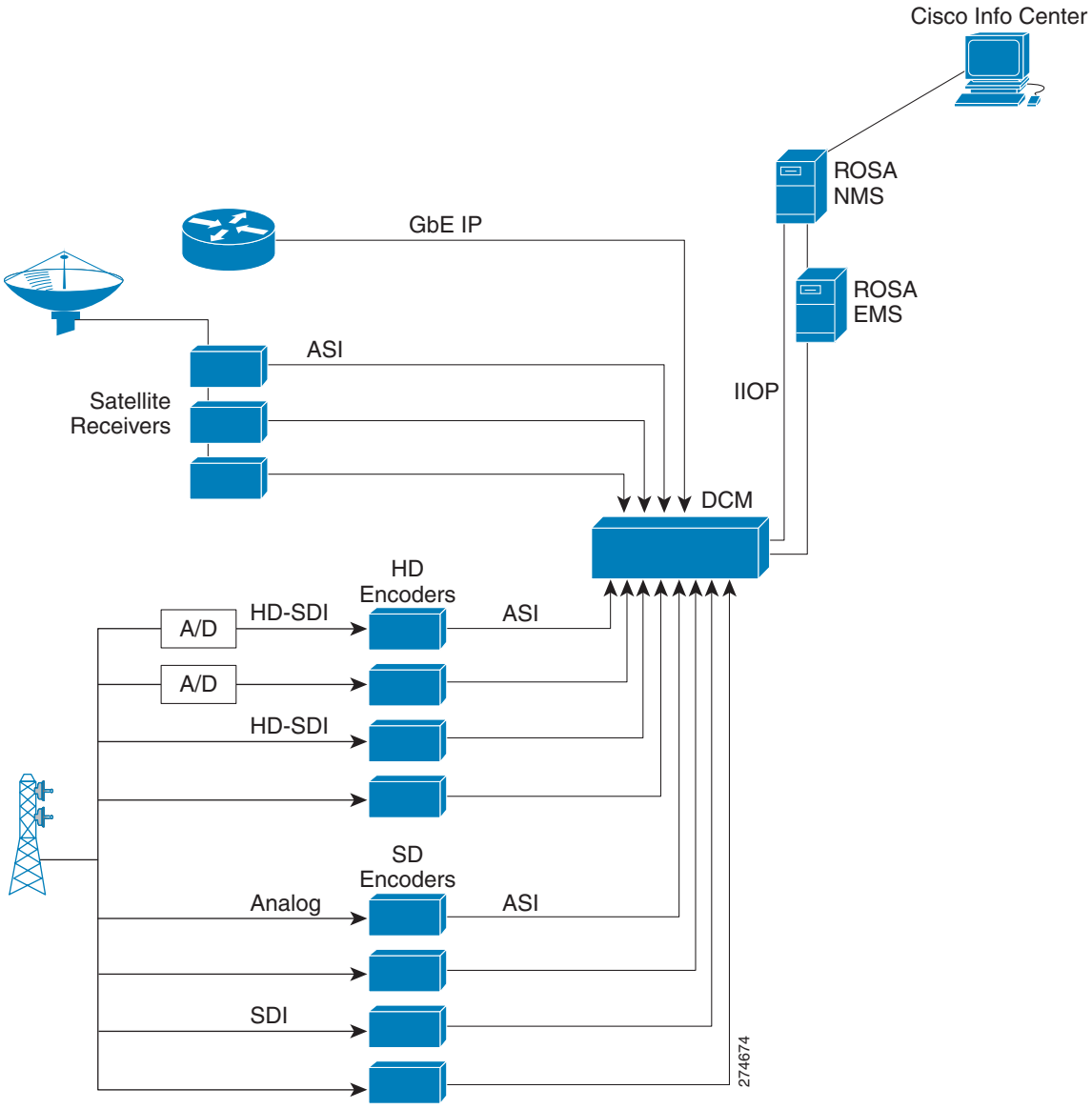
For a list of the video probes and element managers that you can use with CMM, and information on software and firmware versions, see Table 1 on page 6.

Cisco VAMS 3.0 can be used with Cisco ANA 3.7 to build an abstracted network model through a set of virtual network elements (VNEs). Each VNE represents an element in the managed network.

See Figure 1 and Figure 2 for an overview of the Cisco VAMS components (the topologies shown in the figures are examples). Figure 1 shows Cisco VAMS in the video headend network, and Figure 2 shows Cisco VAMS in a video transport network.

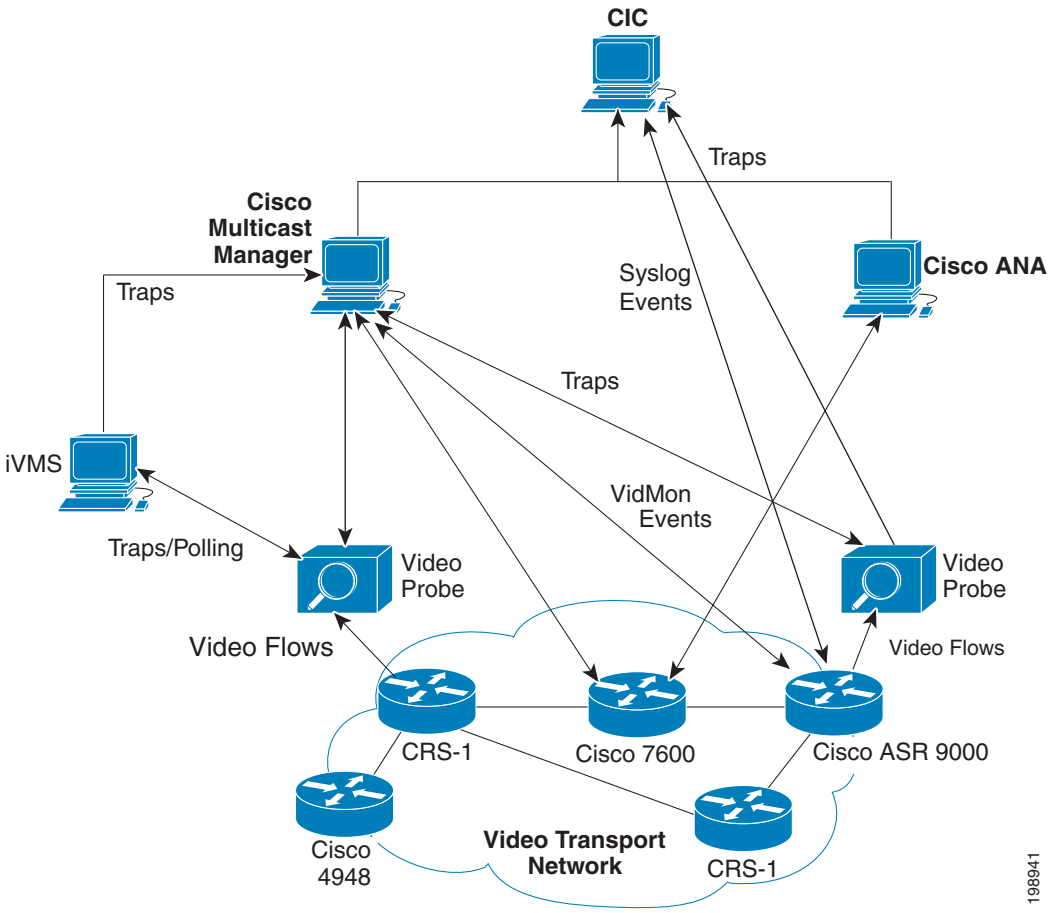
1. Single Pane of Glass—The ability to utilize multiple interconnected tools to monitor, diagnose, and troubleshoot network and video impairments from a single console.

Figure 1 ***Cisco Video Assurance Management Solution 3.0 Components for Video Headend Monitoring***



The ROSA Copernicus NMS receives events either directly from the DCM, or, if the ROSA EMS is deployed in the headend network, from the ROSA EMS.

Figure 2 Cisco Video Assurance Management Solution 3.0 Components



New Features with Release 3.0

Cisco VAMS 3.0 provides the following new features and functionality:

- **Support for IOS Video Monitoring (VidMon)**—VAMS 3.0 provides support for VidMon metrics on Cisco 7600 devices and on Cisco ASR 9000 Series Aggregation Series Routers. VAMS VidMon support includes:

  - Polling of VidMon metrics from routers, including:

    - **MRV—**Media Rate Variation: This metric allows the measurement of packets per second of an IP constant bit rate (CBR) flow against a user-configured nominal setting for that flow. MRV is most applicable for uncompressed flows such as serial digital interface (SDI) and high definition SDI (HD-SDI) where it is not possible to inspect the payload. MRV is supported on the Cisco 7600 Series Ethernet Services Plus (ES+) line card and Cisco ASR 9000 Series.

      MRV is also applicable to Real-Time Transport Protocol (RTP) encapsulated compressed video, as the current implementation of 7600 VidMon MDI does not support RTP encapsulation.

    - **MDI-MLR**—Media Delivery Index – Media Loss Rate: This metric is derived by summarizing the total missing MPEG frames for a given reporting period for a given PID (program). MDI-MLR is supported on the Cisco 7600 ES+ line card.

    - **DF**—Delay Factor: This metric is applicable to both MDI and MRV and measures the difference between the arrival and drain rates of a media stream.
      The DF over an interval period represents the buffering required to handle variations in transmission at a point in the transmission path.

      DF is supported on the Cisco 7600 ES+ line card as MDI:DF and MRV:DF; and on the Cisco ASR 9000 Series as MRV:DF.

    - **MDC**—Media Discontinuity Counter: This measures the number of MPEG discontinuities and provides the MDC, which gives the frequency of the discontinuities for a TS. MDC is supported on the Cisco 7600 ES+ line card.

    - **MSE—**Media Stop Event: As Cisco devices are control-plane aware, it is possible to isolate unexpected media loss at a point in the network from loss that occurs as a result of normal control-plane changes. This is reported as a Media Stop Event. MSE is supported on the Cisco 7600 ES+ line card and Cisco ASR 9000 Series.

  - Correlation of Syslog events to video services.

- **Syslog Event Support**—Support for Syslog events from Cisco 7600 devices and Cisco ASR 9000 devices.

- **Support for ASSR Alerts from the ROSA NMS**—Through the Cisco ROSA NMS, 4.1, VAMS 3.0 supports Aggregated Service Status Reflection (ASSR) alerts for probes using IneoQuest iVMS 4.1.2, Patch 5.

  ASSR alerts are traps that contains the service name and service location data. Cisco Info Center uses the information in ASSR alerts to identify the geographic location of devices used to transmit a video service that is monitored by VAMS.

- **CMM 3.1.1 Support**— Cisco VAMS 2.0 worked with Cisco Multicast Manager 2.5. Cisco VAMS 3.0 works with CMM Release 3.1.1.

  The major new CMM 3.1 features used by VAMS 3.0 include:

  - **CMM VidMon Metrics**—CMM 3.1 includes polling of VidMon metrics from routers, including MLR Reporting, DF reporting, and MRV reporting. When a specified MRV or MDI threshold is exceeded, CMM generates a HIGH or LOW alert corresponding the VidMon metric. For example, when a specified MRV Maximum threshold is exceeded, CMM generates a VIDMON MRV HIGH alert, and when a specified MRV Minimum threshold is reached, CMM generates a VIDMON MRV LOW alert.

  - **Dashboard Metrics Graphs**—The CMM 3.1 Dashboard provides a new dashboard metrics graph feature that allows users to monitor the traffic flow (metrics) for a selected set of configured polling entries. Three types of graphs can be displayed:
    - **SG**—Display a Source, Group statistics graph. For a configured router, BPS/PPS for specified device and S,G can be displayed.
    - **Video Probe**—Display statistics for a video probe. For a Video Probe graph, you can choose to display DF (Delay Factor) or MLR (Media Loss Rate) for a video probe on a specified device.
    - **Vidmon**—Display statistics for a Vidmon device. For specified Vidmon devices you can choose to display DF, MLR, or MRV (Media Rate Variation) for a specified device and S,G.
  - **Historical Graphs—**Historical graphs provide visual representation of trends and performance of multicast flows over time.
  - **Configurable SNMP Trap Descriptor—**CMM 3.1 provides support for user configuration of the descriptor for SNMP traps issued by CMM. This configuration is on a per domain-basis.
- **Enhanced Cisco Info Center Functionality**—Enhanced Cisco Info Center Functionality includes:
  - **Enhanced Cisco Info Center Dashboard**—The enhancements to the Cisco Info Center Dashboard include:
    - **Video Assurance Management Service Dashboard**—The Service Dashboard provides a Service Tree that lets you browse the video services in your network, service maps showing the devices in a selected service, and service event lists showing the events related to the video service.
    - **Customized Event Views for Video Events—** The Service Dashboard provides customized event views for ROSA events, CMM events, video events, VidMon events, ANA events, and all events.
    - **Rules for Syslog Events**—Additional rules to process Syslog messages from VidMon devices and correlate the Syslog messages, as well as SNMP traps with specific video services.

Solution Requirements

Table 1 lists the software and firmware requirements for the Cisco VAMS components.

Table 1 Requirements for VAMS Solution Components

Solution Component	Version Information	Notes
Cisco VAMS	3.0	Installation script
Active Network Abstraction (ANA)	3.7	ANA Gateway—Sun Fire V490, Solaris 10[1] ANA Unit—Sun Fire V480, Solaris 10[1] ANA Client—IBM or PC compatible work station, Windows 2000 or Windows XP[1]
Cisco Multicast Manager	3.1.1	Sun —Solaris 8, 9, or 10 Linux— Linux 4 or 5

Table 1 Requirements for VAMS Solution Components (continued)

Solution Component	Version Information	Notes
ROSA Copernicus Element Management System	4.0.4.8	The ROSA EMS is supported on the following operating systems: • Microsoft Windows 2000 • Microsoft Windows Server 2003 • Windows XP, Service Pack 2 • Microsoft Windows Vista
ROSA Copernicus NMS	4.0.4.8	—
Digital Content Manager	DCM software V8.01.86	Model D9900 and D9901 with GbE interface card
Cisco 7600 Series router	12.2(33)ZI or 15.0(1)S	Supervisor card: 7600-SUP720-3BXL with redundant SUP720-3BXL. Line cards include the following Ethernet Services Plus (ES+) line cards: 76-ES+T-4TG,76-ES+T-40G, 7600-ES+4TG3C, 7600-ES+20G3C, and several other versions. Cisco 7600 Series Route Switch Processors (RSPs) 720 with 10 Gigabit Ethernet uplinks include the RSP720-3C-GE and the RSP720-3CXL-10GE.
Cisco ASR9000 series routers	IOS XR 3.9.1	Apply IOS-XR Software Maintenance Upgrade (SMU) *asr9k-mcast-3.9.1.CSCtf69443-1.0.0* to all ASR 9000 routers.
Cisco uBR10K	12.2(33)SCB4	
Cisco Catalyst 6500 switch	12.2(33)SXI	—
Cisco Carrier Routing System-1 (CRS-1)	IOS-XR 3.9	Line cards include CRS-MSC, CRS1-SIP-800 (with SPA-8X1GE), 8-10GE
Cisco Catalyst 4948 switch (CAT 4948-10GE)	12.2(46)SG	—
Cisco Info Center	—	VAMS release 3.0 includes the following Cisco Info Center IBM Tivoli Netcool components: • ObjectServer - 7.3 • TBSM - 4.2.1 • Impact - 5.1
IneoQuest iVMS	Version 4.02.001.02.29	

Table 1 Requirements for VAMS Solution Components (continued)

Solution Component	Version Information	Notes
IneoQuest video probes	• Singulus G1-T Media Analyzer, Geminus G1-T	• Firmware Version: TB6x-3.10a-120109.iqz Software Version: 3.10a
	• Geminus G10 Geminus G2x	• Firmware Version: Denali-2.1-4a-120109.iqz Software Version 2.14a
	• IQ Media Monitor	• Firmware Version: MA6x-3.10a -120109.iqz Software Version: 3.10a
	• Cricket - ASI version	• Firmware version: Cricket-MS6x-2.11a-120109.iqz Software Version: 2.11aa
	• Cricket - MS version	• Firmware Version: Cricket-6x-2.10a-120109.iqz Software Version: 2.10a
	• Cricket - IP version	• Firmware version: Firmware Version: Cricket-6x-2.10a-120109.iqz Software Version: 2.10a
	• Cricket - QAM and 8VSB versions	• Firmware Version: Cricket-Q6x-2.10a-120109.iqz Software Version: 2.10a
	• Cricket - QAM Plus versions	• Cricket-DQ-1.4a-120109.iqz Software Version: 1.4a
Mixed Signals video probe	Sentry 136 Digital Content Monitor[2]	Sentry Engine Version: PDM (build 1460.84) Sentry Database Version: 3.0.31 Sentry Configuration: TRANSPORT
Bridge Technologies	VB Series	Version: 3.1.0-26, including the VB260 QAM probe. • VB220—Version 4.2.0-15 • VB250—Version 4.2.0-15 • VB260—Version 4.2.0-15 • VB270—Version 4.2.0-15 • VB280—Version 4.2.0-15

1. See the *User Guide for Cisco Video Assurance Management Solution 2.0* at http://www.cisco.com/en/US/docs/net_mgmt/cisco_video_assurance_mgt_solution/2.0/user/guide/vams_20_user.html for detailed specifications.
2. Cisco VAMS 3.0 does not support carousel-related traps for the Mixed Signals Sentry 136.

ROSA NMS Requirements

Table 2 indicates the requirements for the computer used to run the ROSA NMS client.

Table 2 ROSA NMS Client Requirements

Item	Minimum Requirements	Recommended
Processor	600 Mhz Pentium III compatible or higher	1 Ghz Pentium III compatible or higher
Memory	Minimum 192 MB	512 MB
Free disk space	1 GB	10 GB
Operating System	Windows 2000, Windows Server 2003, Windows XP, Windows Vista	
Web browser	Microsoft Internet Explorer v. 5 or higher	
Serial Ports	One or more serial ports (RS-232 and/or RS-285 if needed)	
Ethernet Adapter	Required	

TBSM Requirements

Hardware Requirements

TBSM requires:

- A 4-CPU system with 2.0 GhZ or greater CPUs
- 8 GB of RAM

Software Requirements

The IBM Tivoli Service Manager (TBSM) console supports the IBM 1.5 Java Runtime Environment (JRE). TBSM 4.2.1 also supports Sun Microsystems JRE version 1.6.

TBSM 4.2.1 requires one of the following browsers:

- Internet Explorer 6.0 or 7.0
- Mozilla Firefox 2.0

JRE level 1.6 or later is recommended.

Installation Notes

Installation of Cisco VAMS involves installation of its key components:

Hardware Installation

- The core network elements of the video transport network:
  - Cisco 7600 Series router
  - Cisco ASR 9000
  - Cisco Catalyst 6500 Series switch
  - Cisco uBR 10000
  - Cisco CRS-1
  - Cisco Catalyst 4948 Series switch
- Management servers for Cisco Multicast Manager (CMM) 3.1.1
- Management servers for Cisco Active Network Abstraction (ANA) 3.7 (includes gateway, unit, and client installation)
- ROSA Copernicus NMS 4.0.4.8
- Digital Content Manager and related video headend equipment
- Third-party video probes:
  - Bridge Technologies VB Series, including the VB260 QAM probe
  - IneoQuest probes
  - Mixed Signals Sentry Digital Content Monitor
- Management servers for Cisco Info Center Tivoli Integrated Portal (TIP) and TBSM

Software Installation

- The IPTV-enabled IOS software versions:
  - 12.2(33)ZI on the Cisco 7600 Series
  - 12.2(33)SCB4 on the uBR10K
  - IOS XR 3.9 on the Cisco ASR 9000 and Cisco CRS-1
  - 12.2(46)SG on the Cisco Catalyst 4948 Series switch
- Cisco ANA 3.7 (includes gateway, unit, and client installation)
- Cisco Multicast Manager (CMM) 3.1.1 software on dedicated server

- VAMS release 3.0 includes the following Cisco Info Center IBM Tivoli Netcool components:
  - Object Server 7.3
  - Impact 5.1
  - TBSM 4.2.1

Note Cisco Advanced Services will assist you in any modifications that might be required for the Impact component or other Cisco Info Center components.

For complete details of the VAMS 3.0 installation workflow, including procedures and references to installation documents, see the *User Guide for Cisco Video Assurance Management Solution, 3.0*, available online at:

http://www.cisco.com/en/US/products/ps9518/products_user_guide_list.html .

For details on the VAMS 3.0 installation workflow, consult with your Cisco Advanced Services representative.

Uninstall

You uninstall Cisco VAMS 3.0 by deleting the Cisco Info Center components The uninstallation procedure is described in the *User Guide for Cisco Video Assurance Management Solution 3.0*.

Important Notes

This section contains the following note:

- Increasing the Heap Size Used by Netcool Impact to Handle High Event Loads, page 11

Increasing the Heap Size Used by Netcool Impact to Handle High Event Loads

By default, the allocated heap size for IBM Tivoli Netcool Impact is 1204 MB. If your VAMS installation has high event loads, you might receive alerts regarding Impact's heap size. For example, the following alert might appear:

```
Alert: Impact's Heap size is very close to Max Heap Size! Impact's Heap using 1707M out of
1200M, Free System Memory Available: 5499M, Impact requires at least: 1350M of memory
```

To prevent this issue, we recommend that you increase Impact's maximum heap size to 3072 MB to handle the high event loads.

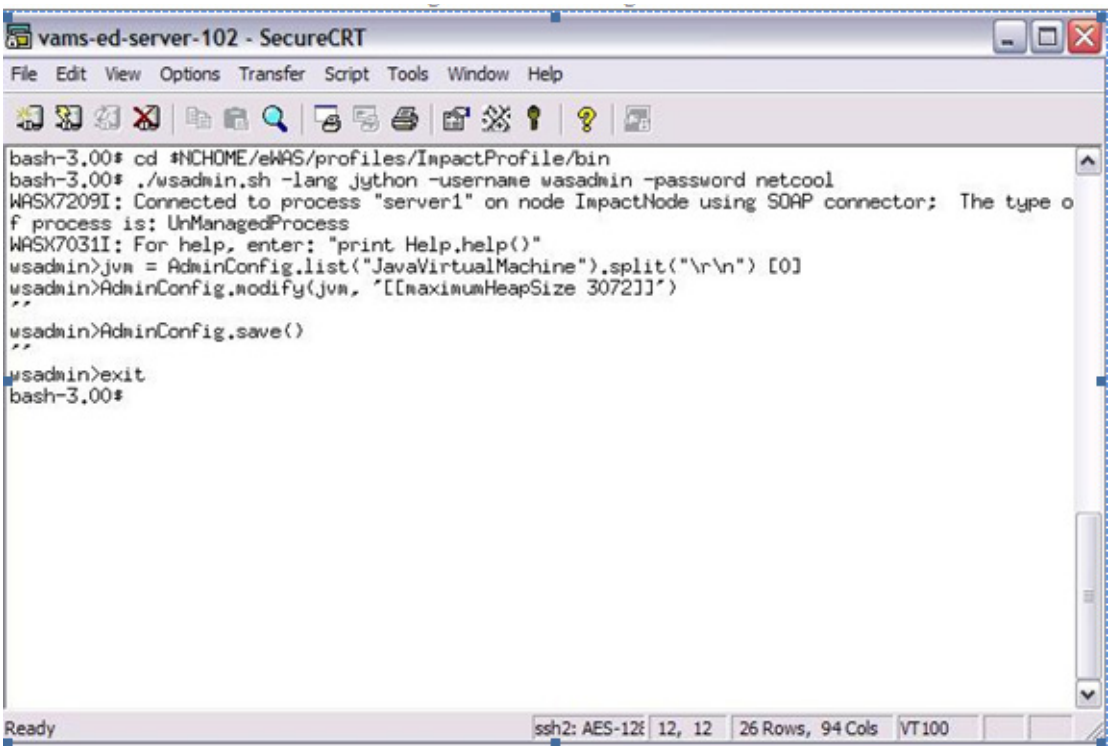
To increase the maximum heap size for Impact:

Step 1 On the VAMS host device, change directory to the */bin* directory for Impact:

```
bash-3.00# cd $NCHOME/eWAS/profiles/ImpactProfile/bin
```

Step 2 Enter the commands shown in Figure 3 to start the *wsadmin* utility and increase Impact's heap size.

Figure 3 Increasing Maximum Heap Size Used by Impact



Open Caveats

Table 3 indicates the open caveats for Cisco VAMS 3.0.

Table 3 Open Defects in Cisco VAMS 3.0

Defect ID	Description
CSCsx44279	IP Multicast Heartbeat trap source is 0.0.0.0 **Conditions** IP Multicast Heartbeat traps from a RSP720-3C-10GE running IOS version 12.2(33)SRD do not have the source address set. This was also observed when running IOS version 12.2(33)ZI and 15.0(1)S. The unset source address of 0.0.0.0 is breaking CMM and VAMS functionality. The Multicast Heartbeat traps show the following: `enterprises.9.10.2.1.1.4.1.2.239.1.1.77 value 0.0.0.0` The issue could not be reproduced when testing the same SRD image on a RSP720-3C-GE. **Workaround** Use CMM S, G polling to generate an alarm when a flow rate drops below a preset threshold. For example, setting the S,G polling minimum packets per second (PPS) threshold to 1 causes CMM to generate an alarm when the flow is lost.

CSCtf84258	ASR9000 did not generate PIM-MIB:Neighbor Loss trap
	
	Conditions When a PIM neighbor is lost, the AS 9000 does not generate a trap, which breaks CMM key functionality.
	SNMP is configured as follows:
	`snmp-server host 10.10.100.216 traps version 2c public`
	`snmp-server community public RO`
	`snmp-server community private RW`
	`snmp-server traps pim neighbor-change`
	`snmp-server traps pim interface-state-change`
	
	When the interface was shut down, I only received a `pim interface up/down trap` from ASR9K, no `pim neighbor loss trap`.
	
	In the ASR 9000 implementation, this trap is generated only if the ASR 9000 interface has a lower IP address than the connecting interface. In the Cisco 7600 platform implementation, this trap is generated all the time, regardless of the interface's IP address.
	
	Workaround None.

Table 3 Open Defects in Cisco VAMS 3.0 (continued)

Defect ID	Description
CSCti05747	VidMon CLI command in CMM UI cannot be run in IOS XR **Conditions** This occurs under the following conditions: 1. There is a VidMon ASR 9000 in the domain. 2. The user navigates to **Diagnostics > Video Diagnostics > Vidmon Flow Status**, and on the Vidmon Flow Status page, clicks **Vidmon Troubleshooting**. 3. The user selects a Cisco ASR 9000 device, and from the drop-down list in the Interface field, selects an interface that has a VidMon policy map defined, for example, gi0/0/0/3, and logs in to the device. 4. The user fills in the username and password 5. The user enters a CLI command in the CMM command window, for example, **show policy-map type performance-traffic interface gigabitEthernet 0/0/0/3**, and then clicks the **Run Command** button. IOS XR returns the following message: `Not able to find iosVersion` IOS XR should return VidMon flow data. **Workaround** None.
CSCtg90468	CIC Did not clear PIM neighbor loss event upon PIM neighbor recovery **Conditions** CIC Did not clear the PIM neighbor loss event after the PIM neighbor was recovered. CMM displayed both PIM neighbor loss and recovery traps; however, the CIC PIM Neighbor Loss event never cleared. **Workaround** None.
CSCti23864	VidMon device status is not shown when a VidMon policy has no active flows **Conditions** CMM 3.1.1 does not display the VidMon status of a VidMon router if any VidMon policy on the router has no active VidMon flows. **Workaround** None.

Table 3 Open Defects in Cisco VAMS 3.0 (continued)

Defect ID	Description

CSCth41158	CIC cannot process all TCA syslog messages from router.
	
	Conditions CIC cannot process syslog messages for all TCA severity alarms. Specifically, it can only process syslog messages with a "critical" severity.
	
	The following SYSLOG examples are for two severity levels: "critical," which worked in CIC, and "notification," which did not work.
	
	Example 1: "Critical" Severity syslog for MSE
	`Jun 18 15:19:32 [10.10.100.103.246.231] 593: Jun 18 15:19:31.309: %FLOWMON-1-ALERT_CRI_SET: [MSE]: SRC_IP:11.1.0.2, SRC_PORT:49152, DST_IP:232.1.1.11, DST_PORT:5001, Te4/1, Output`
	
	`Jun 18 15:19:38 [10.10.100.103.246.231] 594: Jun 18 15:19:37.453: %FLOWMON-1-ALERT_CRI_SET: [MSE]: SRC_IP:11.1.0.2, SRC_PORT:49152, DST_IP:232.1.1.11, DST_PORT:5001, Te4/3, Input`
	
	`Jun 18 15:20:28 [10.10.100.103.246.231] 596: Jun 18 15:20:27.877: %FLOWMON-1-ALERT_CRI_CLEAR: [MSE]: SRC_IP:11.1.0.2,SRC_PORT:49152, DST_IP:232.1.1.11, DST_PORT:5001, Te4/3, Input`
	
	`Jun 18 15:20:23 [10.10.100.103.246.231] 595: Jun 18 15:20:22.769: %FLOWMON-1-ALERT_CRI_CLEAR: [MSE]: SRC_IP:11.1.0.2,SRC_PORT:49152, DST_IP:232.1.1.11, DST_PORT:5001, Te4/1, Output`
	
	Example 2: "Notification" Severity syslog for MSE
	`Jun 18 15:52:36 [10.10.100.103.246.231] 607: Jun 18 15:52:35.984: %FLOWMON-3-ALERT_NOTIFY_SET: [MSE]: SRC_IP:11.1.0.2, SRC_PORT:49152, DST_IP:232.1.1.11, DST_PORT:5001, Te4/1, Output`
	
	`Jun 18 15:52:43 [10.10.100.103.246.231] 608: Jun 18 15:52:42.128: %FLOWMON-3-ALERT_NOTIFY_SET: [MSE]: SRC_IP:11.1.0.2, SRC_PORT:49152, DST_IP:232.1.1.11, DST_PORT:5001, Te4/3, Input`
	
	`Jun 18 15:54:04 [10.10.100.103.246.231] 609: Jun 18 15:54:03.029: %FLOWMON-3-ALERT_NOTIFY_CLEAR: [MSE]: SRC_IP:11.1.0.2, SRC_PORT:49152, DST_IP:232.1.1.11, DST_PORT:5001, Te4/1, Output`
	
	`Jun 18 15:54:04 [10.10.100.103.246.231] 610: Jun 18 15:54:03.029: %FLOWMON-3-ALERT_NOTIFY_CLEAR: [MSE]: SRC_IP:11.1.0.2, SRC_PORT:49152, DST_IP:232.1.1.11, DST_PORT:5001, Te4/3, Input`
	
	Workaround None.

Table 3 Open Defects in Cisco VAMS 3.0 (continued)

Defect ID	Description
CSCtg31358	Inconsistent alarm in CIC "Service Dashboard" and CIC "ROSA events" **Symptom** ETR-290 first priority alarms clear traps from the Bridge Networks probe show up in the ROSA Events by themselves without a description. The corresponding alarm raise trap is not displayed in the ROSA Events. The alarm clear trap should not be displayed in the ROSA Events if the alarm raise trap is not displayed there. **Conditions** This occurs because: 1. All BridgeTech traps forwarded from ROSA have "Bridge Networks" as the class value, because these traps have the *trpMsgInfoType* field set to 3 included in the trap. Therefore, these events are displayed in the Video Events, and not in the ROSA Events. However, the alarm clear traps for these alarms do not have the *trpMsgInfoType* varbind included in the trap. Therefore these traps will have the class field value as "ROSA NMS" and events are displayed in ROSA Events. 2. The alarm clear traps only have two fields in the trap: *trpMsgID* and *trpMsgSourceName*. As a result, the ROSA Events list does not display the meaning of the trap info in the summary; just the *trpMsgID,* for example, `Message ID 9191919 has cleared.` **Workaround** None at present. The proposed solution is: 1. These alarms should only show up in the Video Events and Service Dashboard. 2. CIC should include the *trpMsgInfoType* field include in the alarm clear traps so the class field can be changed from "ROSA NMS" to "Bridge Networks." 3. The following additional fields should be included in the alarm clear traps: *trpMsgID*, *trpMsgSourceName*, *trpMsgInfoType*, *trpMsgInfo*, *trpMsgText*, and *trpMsgObjectTypeID*.

CSCth14237	CMM trap 34 Video probe DF values not to scale
	
	Symptom In CMM, trap 34—*videoDfThresholdExceeded*, the values for the 'threshold' and 'value' are not in milliseconds as defined by the MIB. This is resulting in incorrect DF values reported.
	
	Conditions Trap 34 events from IneoQuest and BridgeTech probes.
	This is seen in a capture of a CMM trap for an BridgeTech probe DF event:
	`channelNames`
	`domainVAMS`
	`gaugeValue1000`
	`group239.0.1.51`
	`groupDesc`
	`probeRouter172.16.1.18`
	`routerID10.86.1.231`
	`routerNameVAMS-BT-220`
	`source172.16.1.250`
	`sourceDescIQ Stim 60`
	`threshold500`
	`transportDescVIDMON_51`
	
	The Event Summary says "Video Probe Delay Factor, 1000, Exceeds 500"
	
	Workaround None.

Table 3 Open Defects in Cisco VAMS 3.0 (continued)

Defect ID	Description

CSCth14227	CMM trap forwarding of BridgeTech traps does not send alarm text
	
	Symptom BridgeTech video probe traps forwarded by CMM do not have the *alarmtext* varbind set.
	
	Conditions Value sent by BridgeTech probe to CMM. For example:
	`BtechAlarm-MIB::alarmTextT.1 (1.3.6.1.4.1.24562.300.1.8.1): aty=ETH|stn=VIDMON_41|sta=239.0.1.41|stp=45001|ssm=172.16.1.250|CC skips:35 discontinuities:5 - counting`
	
	Value forwarded by CMM:
	`BtechAlarm-MIB::alarmTextT.1 (1.3.6.1.4.1.24562.300.1.8.1): aty`
	
	Workaround None.

CSCth03817	VAMS CIC dashboard VOD service scalability **Conditions** The VAMS 3.0 Service dashboard in CIC creates a child service per video on demand (VOD) flow under the source VOD server in the dashboard service tree. This might result in a performance issue when using the VAMS 3.0 dashboard in a large scale VOD environment. A rules change is required to not create the VOD flow child service in the service tree and to instead populate the VOD event under the corresponding VOD server that is the source of the VOD flow. **Workaround** None.
CSCtg85605	CMM displays the *ifindex* for VidMon int name after router software upgrade **Conditions** After upgrading the software on an ASR 9000 or Cisco 7600, CMM displays the *ifindex* in place of the interface name. Re-discovery of the router does not correct this. **Workaround** If the ASR 9000 or Cisco 7600 devices are already at the correct software revision when the CMM domain is initially discovered, this should not be an issue. If the ASR 9000 or Cisco 7600 devices are upgraded after CMM is running, you can resolve this issue by deleting the domain in CMM and re-discovering the network.

Table 3 Open Defects in Cisco VAMS 3.0 (continued)

Defect ID	Description
CSCti45608	Existence of a time zone will break the rules for MSE Syslog events **Conditions** For MSE syslog events sent to Cisco Info Center, the presence of a time zone setting causes rules processing to fail. Cisco Info Center has a distinct rule for handling syslog events for each VidMon metric (MDI, MRV, MSE, DF). For all metrics except for MSE, Cisco Info Center event parsing of the event does not process time zone information in syslog events, if it is present. However, for MSE events, syslog messages that include time zone information cause rule parsing to fail. **Workaround** Turn off time zone logging for syslog messages from the device by issuing the **service timestamps** command without the **show timezone** argument.
CSCti50129	Device trap received by CMM is not forwarded to CIC in Solaris installation **Conditions** CMM is not forwarding received “multicast heartbeat missing” traps from router to CIC. This occurs because the CMM 3.1.1 installation script does not updating the CMM root path in the trap.pl file. This only applies to Solaris installations (not Linux). **Workaround** None.

Related Documentation

See the following sections for information on related documentation:

- Cisco VAMS 3.0 Documentation, page 18
- Documentation for VAMS Components, page 19

Cisco VAMS 3.0 Documentation

In addition to the *User Guide for Cisco Video Management Solution, 3.0*, the Cisco VAMS documentation set comprises:

- *User Guide for Cisco Video Management Solution, 3.0*

  Provides an overview of the solution features and architecture, installation and configuration instructions, and information on using the TBSM and Webtop interfaces to view events and troubleshoot events in the video network. This document is viewable online at:

  http://www.cisco.com/en/US/products/ps9518/products_user_guide_list.html

- *Documentation Guide for Cisco Video Management Solution, 3.0*

  Provides links to the documentation for the Cisco VAMS 3.0 component products and for related products. This document is available online at:

  http://www.cisco.com/en/US/products/ps9518/products_documentation_roadmaps_list.html

Documentation for VAMS Components

For links to the documentation for the VAMS product components, see the *Documentation Guide for Cisco Video Management Solution, 3.0,* viewable online at:

http://www.cisco.com/en/US/products/ps9518/products_documentation_roadmaps_list.html

Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html

Subscribe to the *What's New in Cisco Product Documentation* as a Really Simple Syndication (RSS) feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service and Cisco currently supports RSS version 2.0.