Cisco Videoscape Control Suite 3.0 Release Note

Introduction

This release note provides information for Cisco® Videoscape™ VCS 3.0.

Release Details

This section lists component version numbers and other details verified for this release.

Release Type:	Official Release
Release Version:	VCS 3.0
Hardware Platform:	Minimum hardware configuration supported: ■ 96 GB RAM ■ 2 Processors (CPUs) (X5680 or faster) ■ 2 x 500 GB hard drives For more information, see Hardware Requirements.
Virtual Machine Platform:	VMWare ESXi5.0
OS Name:	Videoscape-OS (VS-OS)
OS Version:	3.0
Management Console Version:	CMC 3.0
High Availability (HA) Configuration:	1:1 Active/Standby
Data Storage:	SQL DB (External Oracle RAC) noSQL DB (Couchbase 3.0)
Message Infrastructure:	MsgInfra (XCP-XMPP) 2.5

Supported Services:	Alert Manager (AM) Applications Manager (AppsManager) BSS/OSS Adapter (BOA) CMC Device Profile Services (DPS) Endpoint Manager (EPM) Explorer Control Service (ECS) GeoFilter Service Headend Purchase (HEP) HornetQ Location Services (LCS) NOSQLCB Operator Messaging Service (OMS) PORTPROXY PPS Session Resource Manager (SRM) Target Messaging System (TMS) Unified Notification Gateway (UNG) User Profile Manager (UPM) User Profile Manager Adaptor (UPMCDA) Workflow Engine (WFE)
Deprecated Services:	Client Directory (CD) 2.1
Supported browsers:	■ Internet Explorer 9 (IE8 compatibility mode) ■ Mozilla FireFox 5

Hardware Requirements

VCS software version 3.0 has been tested on the following hardware platforms:

- UCS C-Series:
  - C200 (M2)
  - C210 (M2)
  - C220 (M3)
  - C240 (M3)
- UCS B-Series (preferred):
  - B200 (M2)
  - B200 (M3)

Installation

See the following publication for installation information for this release:

Videoscape Control Suite Installation and Upgrade Guide (part number OL-29939)

Document Version

This is the first formal release of this document.

Videoscape Control Suite Software

Cisco VCS software provides service providers with multi-platform device and service management capabilities. VCS is standards-based, extensible, and provides real-time, cross-platform capabilities previously unavailable in video environments. VCS provides asynchronous real-time messaging and presence awareness for clients, such as set-tops, Apple iOS devices, Android devices, and PCs, from the cloud.

VCS also provides a comprehensive set of tools and software development kits (SDKs) for service development and integration. In addition, VCS provides a comprehensive management console and supports running in a virtual machine (VM) on the Cisco Unified Computing System (UCS).

New Features and Benefits

VCS software version 3.0 provides the following new features and benefits.

For details on any of the features listed in this release note, visit www.cisco.com and search for "Videoscape Control Suite" to find white papers and data sheets, or, contact your account representative.

- DeviceProfileServices (DPS). DPS provides interface to different services that require the device profiles for their different functionalities. It provides the service level asset bundle definition which can be based on devices/players, asset quality, encryption, fallback policy and encoding details for those devices.
- Explorer Control Suite (ECS). ECS is a collection of Conductor XMPP-managed services that centrally manage broadband controllers.
- Location Services. The Location Service is a Cisco cloud resident, video control plane service that determines the location of a device, subscriber home, or server, based on the device's, subscriber's, or server's identifier.
- Target Messaging System (TMS). The Targeted Messaging System synchronizes the UPM configuration with the cache in the STB. This ensures that any change made to the headend user profile is immediately updated in the STB.
- User Profile Manager (UPM). UPM is a CA independent data storage system which allows high performance management of the users' personal information for TV systems.
- Message Infrastructure (MsgInfra). MsgInfra provides virtual connections and message routing functionality, which is key behavior required to support service and overall cloud scalability.
- Operator Messaging Service (OMS). OMS is a high-availability and scalable application in the VCS group of services that enables service providers to easily preview, publish, search, and manage messages to targeted client devices.

- Unified Notification Gateway (UNG). UNG provides a unified interface for applications to publish notifications to all kinds of devices without caring about the device types and online/offline status.
- Endpoint Manager (EPM). In this release, the EPM adds the ability to update the metadata received from the associated endpoint. In addition, the EPM has the capability to monitor the count of endpoints associated with each group. EPM has the capability to determine how many endpoints have received watches, log performances, or configurations. To support debug, the EPM Filer provides the ability to receive and display an extended Reboot Event file from an endpoint. Enhanced Configurations to include the ability to cancel configurations for an endpoint or group. Added support for Configuration Restore.
- Alert Manager (AM). AM interfaces with EAR/EAC to receive CAP1.2 and CAP-CP EAS messages, in addition to SCTE-18 and DVS-168. It uses HTTP to receive both CAP-CP trigger and its associated audio file, while using HTTP to receive CAP1.2 trigger and FTP for the associated audio file.
- BSS/OSS Adapter (BOA). In this release, the BOA adds the ability to access and store household, device, and user data in UPM using its REST interface. Further additions to the REST interface enable the BOA dashboard presented in the VCS console. The BOA web service interface has also been enhanced to store data in UPM.
- Virtual Session and Resource Management (VSRM). The VSRM is a VCS component that provides sessions and resources that enable clients to gain access to VCS services, such as video.
- Data Analytics. This release adds the ability to view MsgInfra analytics (real-time and historical) on a dashboard.

Known Issues

This section provides a list of open CDETS defect IDs that were identified during testing of VCS 2.5. Resolution of these defects is in progress.

This list is not intended to be comprehensive. If you have questions about a particular defect, contact your account representative.

Notes:

- Defects are identified by a case tracking number (Defect ID) and a headline that briefly identifies the case.
- The headlines in this section are presented exactly as they appear in the issue tracking system.

Defect ID	Headline
CSCuh79961	CBD:oms not work if disconnect cb node network and failover/rebalance
CSCuj46242	UPG: System Setting is missed after upgraded to Denali
CSCuf56579	MHA:CMC may fail to start if active node crash during standby node start
CSCui76856	MHA: sometimes setup HA fail and login cmc fail on one testbed
CSCuf87965	ALM: show all filter is not work in event GUI page
CSCuh07533	Capability to retain role privilege association for pluggable approach
CSCui26817	MHA: Sometimes standby node can't be active if cut network and recover.
CSCui72094	CPC:EPM cenAlarmType and cenAlarmCategoryDefinition is wrong

Remaining CSDL Bugs

In addition to the issues listed above, the following CSDL bugs also remain.

Notes:

- Defects are identified by a case tracking number (Defect ID) and a headline that briefly identifies the case.
- The headlines in this section are presented exactly as they appear in the issue tracking system.

Defect ID	Headline
CSCuj63613	CSDL: Redhat missing security updates - speex (31988)
CSCue96256	CSDL:Close unused CMC ports
CSCui71793	CSDL:WebCM response 200ok when appscan access unavailable file(BOSH)
CSCuj63597	CSDL: Redhat missing security updates - sos (69162)
CSCuj63601	CSDL: Redhat missing security updates - gdm (69795)
CSCuj63605	CSDL: Redhat missing security updates - kernel (70163)
CSCuj69055	CSDL: Cross-Site Request Forgery (CBUI)
CSCuh25356	CSDL: Remote Host supports the use of weak SSL ciphers
CSCuh25408	CSDL: Remote web server prone to cookie injection attack.
CSCuh25441	CSDL: remote web server is prone to a cross-site scripting attack
CSCuh25529	CSDL: Redhat missing security updates - vsftpd
CSCuh28111	CSDL: Redhat missing security updates - kexec-tools
CSCuh28209	CSDL: Redhat missing security updates - sudo
CSCuh28487	CSDL: Redhat missing security updates - openssl
CSCuh30320	CSDL: Redhat missing security updates - glibc
CSCuh37229	CSDL: JBOSS has Insecure HTTP Methods Enabled issue
CSCuh90791	CSDL:MAMA process got crashed during system security scan by Nessus
CSCuh92335	CSDL:Redhat missing security updates - net-snmp
CSCue74848	CSDL:Insecure HTTP Methods Enabled

Bug Search Tool

The Bug Search Tool is an online tool that allows registered users to search for bugs by release or by a bug number.

To log on to the Bug Search Tool, go to **https://tools.cisco.com/bugsearch,** and log on with your user name and password. The Bug Search Tool page opens.

Note: If you have not set up an account on www.cisco.com, click **Register Now** and follow the on-screen instructions to register.

Search for Bugs in This Release

1. In the product type-in field (to the right of the product drop-down box), type **Conductor**. Then select **Conductor** from the list that appears. (Do *not* press **Enter**.)
2. In the Releases field, type **3.0** and press **Enter**.

The Bug Search Tool displays the list of bugs for this release. You can use the filters to restrict the bugs that you want to view.

If you want to view a specific bug, enter the ID of the bug you want to view in the **Search For** field and press **Enter**.

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

http://www.cisco.com
Tel: 408 526-4000
800 553-6387
Fax: 408 527-0883

October 2013 Part Number OL-30244-01