Cisco Videoscape Control Suite 3.1 Release Note

Introduction

This release note provides information for Cisco Videoscape VCS 3.1.

Release Details

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

Release Type:	Official Release
Release Version:	VCS 3.1
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:	3.1
Management Console Version:	CMC 3.1
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)

Release Type:	Official Release 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 20

Hardware Requirements

VCS software version 3.1 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 3.1 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.

- It is no longer necessary to upgrade the operating system each time a new update is released. Pluggable COP files allow you to update only those files required for the new release. The following COP files need to be upgraded for this release:

  Conductor_3.1_ServicesBundle.zip

  - cisco.conductor-epmFiler-3.1-0-0.tmp.xml
  - cisco.conductor-upmcda-3.1-0-6125.cop.sgn
  - cisco.conductor-endpointManager-3.1-0-1.tmp.xml
  - cisco.conductor-lcs-data-3.1-0-2.cop.sgn
  - cisco.conductor-epmFiler-3.1-0-0.cop.sgn
  - cisco.conductor-oms-3.1-0-6128.tmp.xml
  - cisco.conductor-lcs-3.1-0-3.tmp.xml
  - cisco.conductor-nosqlcb-3.1-0-0.tmp.xml
  - cisco.conductor-upmcda-3.1-0-6125.tmp.xml
  - cisco.conductor-oms-3.1-0-6128.cop.sgn
  - cisco.conductor-alertManager-3.1-0-1.tmp.xml
  - cisco.conductor-billingAdaptor-3.1-0-2.cop.sgn
  - cisco.conductor-lcs-3.1-0-3.cop.sgn
  - cisco.conductor-billingAdaptor-3.1-0-2.tmp.xml

  - cisco.conductor-nosqlcb-3.1-0-0.cop.sgn
  - cisco.conductor-wfe-3.1-0-0.cop.sgn

  Conductor_3.1_CmcBundle.zip

  - cisco.conductor-cmc-3.1-0-1877.cop.sgn

- Enhancements for version 3.1 support newer browser versions (Internet Explorer 9 and Firefox 20).
- This version has more pluggable COPs for all ECS services and BOA.
- Location Service
  - Back-end support for Highly Available Location Service deployment (multiple Active nodes), using Couchbase-persisted configuration data.
  - Support for Canadian Standard Geographical Classification (SGC) encoding.
  - Updated location data files.
- OMS:
  - UPM and OMS properties synchronization: OMS and UPMCDA support multi-namespace for user and account metadata.
  - OMS can publish unexpired historical messages to new group subscribers.
  - FTP password enhancement request: OMS supports special characters for OMS server password except &<>,".
- BSS/OSS Adaptor (BOA). In this release, the BOA REST interface has been expanded to manage new household preferences (parental PIN, purchase PIN, max device count, and max credit limit), support household authorizations, and includes more granular household data retrievals. The BOA web service interface has also been expanded in this release with household-centric transactions to manage households, devices, users, services, and authorizations.

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
CSCuh07533	Capability to retain role privilege association for pluggable approach
CSCui17607	Videoscape control nodes do not fix to top and bottom correctly
CSCui29130	UPG:nosql installed UI have been lost after upgraded to 3.0
CSCuj46242	UPG: System Setting is missed after upgraded to Denali
CSCul09649	CMC: On WFE pages, some information can't displayed
CSCul28315	User group page doesn't load on first click Ttv6105376c
CSCul84692	EPM analytics purge script does not execute and throws an error
CSCul63191	Cannot change VCS cluster secret after Conductor ISO installation
CSCuj24642	UPMCDA: timeout when adding many users under one account
CSCuf56579	MHA:CMC may fail to start if active node crash during standby node start
CSCuh79961	CBD:oms not work if disconnect cb node network and failover/rebalance
CSCui76856	MHA: sometimes setup HA fail and login cmc fail on one testbed

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
CSCui71793	CSDL: WebCM responses 200ok when appscan access unavailable file(BOSH)

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 **3.1** 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.
3. 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

December 2013 Part Number OL-31117-01