Release Notes for Cisco Videoscape Distribution Suite, Internet Streamer 3.3

This Release note covers Cisco Videoscape Distribution Suite, Internet Streamer Release 3.3.

First Published: December 13, 2013

OL-29883-02

Contents

The following information is included in these release notes:

Cisco Systems, Inc.
www.cisco.com

New Features in Release 3.3

Release 3.3 of Cisco Internet Streamer VDS introduces the following features:

- **Virtualization Support**

  The Cisco VDS-IS 3.3 Release introduces virtualization for SE, SR and CDSM modes of VDS-IS. This enables the SE, SR and CDSM to boot as a Virtual Machine in the UCS platform and in other server platforms.

- **Support for Content Deletion per Delivery Service per SE**

  The Cisco VDS-IS 3.3 Release enhances the content deletion feature present in the earlier releases. To simplify the earlier process of deletion new GUI and APIs are created for the following content deletion enhancements:

  - Per delivery service content deletion
  - Per delivery service per streamer content deletion
  - Synchronous deletion and Asynchronous deletion
  - Glob expression support in content URL
  - Feature compatibility
  - Security and Wholesale consideration
  - Version Inter operability

- **MPEG Dash (Live/VOD) Support**

  The Cisco VDS-IS 3.3 Release provides support for both VOD and Live profile of MPEG Dash.

  - VDS-IS is transparent to MPEG Dash contents for both MPD files and content fragments.
  - Support preposition of MPEG Dash contents for both MPD files and content fragments.
  - Support for generic transaction log for MPEG Dash.
  - Support for two segment formats for MPEG Dash, MPEG-2 TS and ISO base medial file format.

- **Delivery Services Monitoring Active TCP Sessions**

  A new type of snapshot transaction log is generated by WebEngine with following counters per DS per URL regex periodically:

  - Number of active TCP sessions.
  - Number of bytes sent since the previous snapshot.
  - Snapshot of the allocated bandwidth (in bits per second from the SE to the End User).
  - Number of HTTP requests received since the previous snapshot.

  The generation interval is configurable between the range of 1 minute to 10 minutes with a granularity of minutes per URL regex.

- **Support to Enable Session Logging on Root Location**

  VDS-IS 3.3 enables Session Tracking in all SEs attached to a delivery service. Upon receiving requests from Client the HTTP/HTTPS transactions will be tracked in Session by WebEngine.

- **Generic Session Tracking with Content Access Protection**

  In earlier Releases for Generic Session Tracking none of the requests were rejected. In VDS-IS 3.3 Generic Session Tracking is enhanced to reject request with 403 when the request can not be tracked and the requested content is protected.

- **Generic Session Tracking with HTTPS**

  In VDS-IS 3.3, Generic Session Tracking and Logging feature is verified to be working fine with HTTPS. No behavior change is made for Generic Session Tracking and Logging feature.

- **Geo Location Server Support**

  In VDS-IS 3.3, it provides support for latest release of Quova (Nestar). Another geo location service, Maxmind GeoIP web service will also be supported. New failover mechanism will be added to the Quova latest release and Maxmind. Other changes include, more geo location information fields are checked for geo protection, IPv6 IP address support for both Quova and Maxmind servers.

  Geo location information of an IP address is obtained from an external server. RESTful API is used to communicate with Quova (Nestar) latest release server and Maxmind server.

- **Support for IPv6**

  In Earlier Releases, IPv6 was supported for client facing interfaces by SEs and SRs. The IPv6 is supported by dual stack approach, so both IPv4 and IPv6 communication with clients are supported.

  In VDS-IS 3.3, IPv6 support is extended to enable IPv6 communication with the following VDS-IS's external servers:

  - Origin Server
  - FTP
  - NTP
  - Geo Location server (except Legacy Quova server)

- **Support of Open SSL Version 1.0.1c**

  In VDS-IS 3.3, the OpenSSL library is upgraded to 1.0.1c. Crypto hardware acceleration capability and improvement in the HTTPS performance are a result of the 1.0.1c upgrade.

- **HTTPS Mutual Authentication (Inc CRL)**

  In Mutual Authentication (two-way authentication), the SSL client verifies the identity of the SSL server, and then the SSL server verifies the identity of the SSL-client. With this verification of client, SSL server can make sure that the client is authorized.

  One-way HTTPS authentication only enables the SSL client verify the identity of the SSL server. This authentication for SSL server is currently supported.

  Certificate Revocation List (CRL) is also supported. CRL is a list of certificates that have been revoked before their scheduled expiration date. It is maintained by a CA which also provides information about revoked certificates that were issued by that CA.

- **Configurable HTTPS Cypher List**

  VDS-IS supports HTTPS streaming to client, VDS-IS 3.3 Release requires that the CDSM presents the list of all Cyphers supported by SE and the operator chooses to disable some of the Cyphers from the list.

  For HTTPS streaming between OS and Content Acquirer, Content Acquirer can also provide a supported Cypher list to OS.

  The Cypher list can be configured for individual Delivery Service or in system level. By default, all supported Cyphers are enabled. The configured Cypher list will be sent to SEs which is used by each SE to select Cypher during the SSL/TLS handshake with client/OS.

- **Secondary IP Address (Different Subnet) on Port Channel/Interface**

  In Earlier Releases, a network interface can be assigned more than one IP address. But for portchannel interface it is limited, multiple IP address can only be assigned in the same subnet.

  This feature enables access to a CDN from different subnet, more than one IP address is defined in different subnet on a portchannel.

- **Transaction Log Exporting Control**

  In Earlier Releases, transaction log exporting was controlled at the global level. Enhancements have been made to control the exporting of transaction logs individually by GUI and CLI. All transaction logs are still dumped to the disk as before.

  The FTP destination configuration and the achieving frequency are still controlled at the global level. The device group support and Splunk support follow the existing behavior.

- **DNS Redirection Based On WE Status**

  In VDS-IS 3.3 Release, a new option is added for SR to provide a configurable option to use Web Engine's status as the whole streamer's status for redirection. That is, if web engine reaches it's threshold, SR will not direct the traffic to the same streamer.

- **Option to Schedule Slowscan**

  In Earlier Releases, the Slowscan (which synchronizes the files from disks to ContentMgr) runs every 12 hours, this behavior is not configurable. It was found that the Slowscan was running unexpectedly at peak time. In VDS-IS 3.3 Release, an option is provided to schedule the Slowscan. The option is only available on SE.

- **VDS-IS Identification Feature**

  In Earlier Releases, when logging into VDS-IS devices through SSH/telnet device mode is displayed as "Cisco Service Engine", "Cisco Service Router" or "Cisco Content Delivery System Manager". In VDS-IS 3.3 Release, it is changed to “Service Engine”, “Service Router” and “Content Delivery System Manager” respectively.

  According to different use cases, the "Server" Header of SE/SR response is either "Cisco-CDS" or from Origin Server, like "Apache/2.2.22 (Debian)" for example. In VDS-IS 3.3 Release, this is configurable, operators could choose to keep the same behavior as before or operators could configure an arbitrary string.

  Server Header of SE/SR response is a per-delivery-service configuration.

- **Per Session DSCP Marking for FMS**

  VDS-IS 3.3 Release provides DSCP Marking for Flash Media Streaming use cases including VOD and Live. This is done through service rule file configuration. It allows for per session DSCP marking as well as some other flexible rules based on configurations.

Open Caveats in Release 3.3

Table 1 lists the issues open in the Cisco Internet Streamer CDS 3.3 Release.

Click on the bug ID to view the bug details. This information is displayed in the Bug Search.

Table 1 Open Caveats in Cisco Internet Streamer CDS 3.3 Release

Bug ID	Description
CSCuj16086	Fmsedge core dump with fms dscp configuration in performance testing
CSCul43691	VM: wrong value of BW shown form show service-router service-monitor
CSCuj41201	Fmscore core dump in std::_Rb_tree_rebalance_for_erase ()
CSCuj41288	Fmscore core dump in TCIOHandle::setDiffserv ()
CSCuh49257	M3u8 does not refresh when hls session tracking enabled
CSCul01278	Delete and re-add default gateway will cause network down with ova image
CSCul71323	Web Engine: datasource hangs after stress test of max-age=5
CSCuf24463	Edge SE sends revalidation requests to offloaded CA
CSCtk18297	Adobe2763034 fmsedge reaches4GB coredumpswhen SR burstctrlnotconf(RTMPT)
CSCtq45558	Adobe 2883922 Content Cached twice if query string has " : " character
CSCtr93692	Adobe 2763034 fmsedge core-dump with different BT found on 2.6.0 B420
CSCtt97134	Adobe:3016409 fmsedge coredumped during cache-hit longevity
CSCtq46851	Adobe2880638 CDS ISFMS logs notparsed by 3rdparty LogAnalysis products
CSCul93497	RFC: fails to handle chunked response to an HTTP/1.1 client
CSCul96548	HTTP 504 caused by stale entries in perdsvclocation.xml after downgrade
CSCty06704	Core.MetaDataReceive.3.0.0.b15 found in IPV6 enabled device
CSCul93537	SE page allocation failure issue
CSCul76853	Auths geo protection fails when the response data missed code info
CSCum11947	GUI responses slow when deleting content on 100+ SEs

Resolved Caveats in Release 3.3

Table 2 lists the issues resolved in the Cisco Internet Streamer CDS 3.3 Release.

Click on the bug ID to view the bug details. This information is displayed in the Bug Search.

Table 2 Resolved Caveats in Cisco Internet Streamer CDS 3.3 Release

Bug ID	Description
CSCuj81516	Delay In PSU Alarm Generation/Clearance
CSCuf75303	Very old contents is evicted regardless of its population
CSCui75160	Method to evict HLS/HSS Live content after an hour

Table 2 Resolved Caveats in Cisco Internet Streamer CDS 3.3 Release (continued)

Bug ID	Description
CSCui05393	UCS install fails
CSCul06122	Web Engine core dump when issue cache-miss request for hss vod assets
CSCul39975	WMT ingest logging does not work

Enhancement Features Added in Release 3.3

Table 3 lists the enhancements in the Cisco Internet Streamer CDS 3.3 Release.

Click on the bug ID to view the bug details. This information is displayed in the Bug Search.

Table 3 Enhancements in Cisco Internet Streamer CDS 3.3 Release

Bug ID	Description
CSCtl85479	CLI to know the rule hit by a URL
CSCtr03207	Word count option for CLI "show statistics netstat"
CSCue88914	Enhancement to add CLI "ps -aelf | wc -l"
CSCuj43468	SlowScan:default slow scan rate may cause whole SE unwork on high loads
CSCul39767	SE cannot take more than 6000 https sessions

Accessing Bug Search

This section explains how to use the Bug Toolkit to search for a specific bug or to search for all bugs in a release.

Step 1 Go to https://tools.cisco.com/bugsearch/.

Step 2 At the Log In screen, enter your registered Cisco.com username and password; then, click **Log In**. The Bug Toolkit page opens.

Note If you do not have a Cisco.com username and password, you can register for them at http://tools.cisco.com/RPF/register/register.do.

Step 3 To search for a specific bug, click the **Search Bugs** tab, enter the bug ID in the Search for Bug ID field, and click **Go**.

Step 4 To search for bugs in the current release, click the **Search Bugs** tab and specify the following criteria:

- Select Product Category—**Video**.
- Select Products—**Videoscape Distribution Suite for Internet Streaming**.
- Software Version—**[3.3].**
- Search for Keyword(s)—Separate search phrases with boolean expressions (AND, NOT, OR) to search within the bug title and details.

- Advanced Options—You can either perform a search using the default search criteria or define custom criteria for an advanced search. To customize the advanced search, click **Use custom settings for severity, status, and others** and specify the following information:
  - Severity—Choose the severity level.
  - Status—Choose **Terminated**, **Open**, or **Fixed**.

    Choose **Terminated** to view terminated bugs. To filter terminated bugs, uncheck the Terminated check box and select the appropriate suboption (Closed, Junked, or Unreproducible) that appears below the Terminated check box. Select multiple options as required.

    Choose **Open** to view all open bugs. To filter the open bugs, uncheck the Open check box and select the appropriate suboptions that appear below the Open check box. For example, if you want to view only new bugs in Prime Optical 9.5, choose only **New**.

    Choose **Fixed** to view fixed bugs. To filter fixed bugs, uncheck the Fixed check box and select the appropriate suboption (Resolved or Verified) that appears below the Fixed check box.
  - Advanced—Check the **Show only bugs containing bug details** check box to view only those bugs that contain detailed information, such as symptoms and workarounds.
  - Modified Date—Choose this option to filter bugs based on the date when the bugs were last modified.
  - Results Displayed Per Page—Specify the number of bugs to display per page.

Step 5 Click **Search**. The Bug Toolkit displays the list of bugs based on the specified search criteria.

Step 6 To export the results to a spreadsheet:

a. In the Search Bugs tab, click **Export All to Spreadsheet**.

b. Specify the filename and location at which to save the spreadsheet.

c. Click **Save**. All bugs retrieved by the search are exported.

If you cannot export the spreadsheet, log into the Technical Support website at http://www.cisco.com/cisco/web/support/index.html or contact the Cisco Technical Assistance Center (TAC).

Downgrading from Release 3.3

For software downgrades from Release 3.3 on systems with primary and standby CDSMs, you need to do the following:

Step 1 If you are using the CDSM GUI, downgrade the standby CDSM first, followed by the primary CDSM.

If you are using the CLI, downgrade the primary CDSM first, followed by the standby CDSM.

Step 2 After downgrading the primary and standby CDSMs, using the CLI, log in to each CDSM and run the following commands:

- To downgrade from 3.3 to 2.5.9 or 2.5.11

```
cms database downgrade script downgrade/Downgrade3_3_to3_2
cms database downgrade script downgrade/Downgrade3_1_2_b20_to_3_1_2_b19
cms database downgrade script downgrade/Downgrade3_1_1_to_3_1
cms database downgrade script downgrade/Downgrade3_1_to_3_0
cms database downgrade script downgrade/Downgrade3_0_to_2_6
cms database downgrade
cms enable
```

Then, consult the "Downgrading the Internet Streamer CDS Software" chapter in the Cisco Internet Streamer CDS 2.6 Software Upgrade Guide for downgrading from Release 2.6.x to Release 2.5.9 or 2.5.11.

- To downgrade from 3.3 to 2.6.x

```
cms database downgrade script downgrade/Downgrade3_3_to3_2
cms database downgrade script downgrade/Downgrade3_1_2_b20_to_3_1_2_b19
cms database downgrade script downgrade/Downgrade3_1_1_to_3_1
cms database downgrade script downgrade/Downgrade3_1_to_3_0
cms database downgrade script downgrade/Downgrade3_0_to_2_6
cms database downgrade
cms enable
```

After downgrade from 3.2.1 to 2.6.1, If SE does not come up in operational status in SR, restart the Service router and the operational state will be updated.

- To downgrade from 3.3 to 3.1.0

```
cms database downgrade script downgrade/Downgrade3_3_to3_2
cms database downgrade script downgrade/Downgrade3_1_2_b20_to_3_1_2_b19
cms database downgrade script downgrade/Downgrade3_1_1_to_3_1
cms database downgrade
cms enable
```

- To downgrade from 3.3 to 3.1.1 or 3.1.2.bN(N<20)

```
cms database downgrade script downgrade/Downgrade3_3_to3_2
cms database downgrade script downgrade/Downgrade3_1_2_b20_to_3_1_2_b19
cms database downgrade
cms enable
```

- To downgrade from 3.3 to 3.1.2.bN(N>=20) or 3.2

```
cms database downgrade script downgrade/Downgrade3_3_to3_2
cms database downgrade
cms enable
```

Step 3 Downgrade the software on the Service Routers, followed by the Service Engines.

Related Documentation

Refer to the following documents for additional information about Cisco Internet Streamer CDS 3.3:

- *Cisco Internet Streamer CDS 3.3 Software Configuration Guide*
- *Cisco Internet Streamer CDS 3.0–3.3 Quick Start Guide*
- *Cisco Internet Streamer CDS 3.3 API Guide*
- *Cisco Internet Streamer CDS 3.3 Command Reference Guide*
- *Cisco Internet Streamer CDS 3.3 Alarms and Error Messages Guide*
- *Cisco Internet Streamer CDS 3.3 Software Installation Guide for non-CDEs*
- *Cisco Content Delivery System 3.x Documentation Roadmap*
- *Open Source Used in Cisco Internet Streamer CDS 3.3*
- *Cisco Content Delivery Engine 205/220/250/420 Hardware Installation Guide*

  http://www.cisco.com/en/US/docs/video/cds/cde/cde205_220_420/installation/guide/cde205_220_420_hig.html
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engines*

  http://www.cisco.com/en/US/docs/video/cds/cde/regulatory/compliance/CDE_RCSI.html

- *Cisco UCS C200 Installation and Service Guide*
  http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C200M1/install/c200M1.html
- *Cisco UCS C210 Installation and Service Guide*
  http://www.cisco.com/en/US/docs/unified_computing/ucs/c/hw/C210M1/install/C210M1.html

The entire CDS software documentation suite is available on Cisco.com at:
http://www.cisco.com/en/US/products/ps7127/tsd_products_support_series_home.html
The entire CDS hardware documentation suite is available on Cisco.com at:
http://www.cisco.com/en/US/products/ps7126/tsd_products_support_series_home.html
The Cisco UCS C-Series Rack Servers documentation is available on Cisco.com at:
http://www.cisco.com/en/US/products/ps10493/prod_installation_guides_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.

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.