Release Notes for Cisco Internet Streamer CDS 2.0.3-b1

Revised: April 2, 2008, OL-13494-02

Contents

This information is in the release notes:

System Requirements

The CDS Internet Streaming 2.0 release runs on the CDE-100 and CDE-200 hardware models. The CDE-100 may run as the CDSM, while the CDE-200 may run as the Service Router or the Service Engine. See the *Cisco Content Delivery Engine Hardware Installation Guide* for set up and installation procedures.

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

Limitations and Restrictions

This release contains the following limitations and restrictions:

- The Movie Streamer functionality in release 2.0 is capable of MPEG1/2/4 and H.264 streaming over RTP/RTSP to a wide range of devices including PC, Mac, PDA, and cell phones, with 3GPP release 6 support for rate adaptation and capability exchange. However, this Movie Streamer functionality is available only on a demo and lab trial basis in release 2.0.3, and the software enforces a hard limit of 20 concurrent sessions. If you are interested in running the Movie Streamer in a field trial or production environment, please contact your Cisco account team.
- There is no NAT separating the CDEs from one another.
- Do not run the CDE with the cover off, this disrupts the fan air flow and causes overheating.

Important Notes

To maximize the content-delivery performance of a CDE-200, we recommend you do the following:

1. Use port channel for all client-facing traffic.

   Configure interfaces number 3, 4, 5, and 6 (those on the quad-port Gigabit Ethernet Card) into a single port-bonding interface. Use this bonding channel, which provides instantaneous failover between ports, for all client-facing traffic. Use interfaces number 1 and 2 (the two on-board Ethernet ports) for intra-CDS traffic such as the management traffic, and configure these two interfaces either as standby or port-channel mode. Refer to the *Cisco Internet Streamer CDS 2.0 Software Configuration Guide* for detailed instruction.

2. Use the client IP address as the load balancing algorithm.

   Assuming ether-channel (also known as port-channel) is used between the upstream router/switch and the SE for streaming real-time data, the ether-channel load balance algorithms on the upstream switch/router and the SE should be configured as "Src Only" and "Destination IP" respectively. Using this configuration ensures session stickiness and general balanced load distribution based on client's IP addresses. Also, distribute your client IP address space across multiple subnets so that the load balancing algorithm is effective in spreading the traffic among multiple ports.

3. Tune the TCP parameter.

   On the CDE-200, execute the following commands once (this tunes the internal TCP configuration for better content delivery performance over HTTP):

   ```
   Config#tcp server-satellite
   Config#tcp client-satellite
   Config#write memory
   ```

4. For high-volume traffic, separate HTTP and WMT.

   The CDE-200 performance has been optimized for HTTP and WMT bulk traffic, individually. While it is entirely workable to have mixed HTTP and WMT traffic flowing through a single CDE-200 simultaneously, the aggregate performance may not be as optimal as the case where the two traffic types are separate, especially when the traffic volume is high. So, if you have enough client WMT traffic to saturate a full CDE-200 capacity, you are recommended to provision a dedicated CDE-200 to handle WMT; and likewise for HTTP. In such cases, we do *not* recommended you mix the two traffic types on all CDE servers which could result in suboptimal aggregate performance and require more CDE-200 servers than usual.

5. For mixed traffic, turn on the HTTP bitrate pacing feature.

   If your deployment must have Streamers handle HTTP and WMT traffic simultaneously, it is best that you configure the Streamer to limit each of its HTTP sessions below a certain bitrate (for example, 1Mbps, 5Mbps, or the typical speed of your client population). This prevents HTTP sessions from running at higher throughput than necessary, and disrupting the concurrent WMT streaming sessions on that Streamer. To turn on this pacing feature, use the HTTP bitrate field in the CDSM Delivery Service GUI page.

Open Caveats

This release contains the following open caveats:

Web Engine

- CSCsi84922

  Symptom:

  For a cache miss scenario, the http bitrate configured for the delivery service does not take effect. The client is served at the rate origin at which the server sends the response.

  Workaround:

  Once the content is cached on the SE, for subsequent requests which are cache hit, the bitrate takes effect. However, you may choose not to configure any bitrate for the delivery service, and let TCP congestion control determine the optimal rate of each HTTP progressive download session.

Service Router

- CSCsi68373

  Symptom:

  When the Service Router is at peak load (approximately beyond 4000 to 8000 session set-ups a second), depending on the routing algorithms being used (consult the data sheet performance section), a few of the client requests may fail with 404 response. The maximum Service-Router performance as published in the data sheet is measured by ensuring that no more than 0.2% of the requests may result in 404 failure; and typically only 0.001% results in 404 failures.

  Workaround:

  If the client retries, it almost always gets successfully routed. The operator can further reduce the failure rate by adequately provisioning and deploying enough Service Router to absorb not only the average but also the peak workload. If the deployment is not provisioned properly, and the aggregate load on the Service Router goes beyond the published performance number (for example, 8000 HTTP or ASX redirections a second), then the number of 4xx failures may increase dramatically. However, if the load is at or below the published performance limit, then only a tiny faction fails.

CDSM

- CSCsj30486

  Symptom:

The CMS does not come up when the CDSM is reloaded and the CDSM GUI is not accessible (this happens extremely rarely). The following exception (or similar) is logged:

```
06/18/2007 06:19:25.189(Local) [W] cdm(Scheduler): java.sql.SQLException: ERROR: Index
sys_mess_time_idx is not a btree: java.sql.SQLException: ERROR: Index
sys_mess_time_idx is not a btree
```

Workaround:

Execute the following command to run database maintenance:

```
DT-612-10#cms database maintenance full ?
```

Platform

- CSCsj87235

  Symptom:

  In performance tests, when 1000 concurrent HTTP sessions are ungracefully shutdown without sending the SE the normal TCP teardown messages, the SE takes up to 40 minutes to clean up all the zombie TCP sessions from its memory. The impact is that the memory resource and connections are temporarily held up by the zombie sessions in the period. If another 1000 to 2000 sessions are immediately sent to the SE before the previous 1000 sessions are cleaned up, it is possible that some of the new sessions are denied due to the 2000 concurrent sessions limit of web-engine.

  Workaround:

  There is no workaround. This is not a real deployment scenario because typical clients always tear down the session before exiting and the only time a client does not is when it is abruptly power-cycled. Therefore, it is extremely hard to have such an ungraceful tear-down happen in a synchronized fashion across thousands of sessions going to the same CDE. Considering that each session had been properly authorized by the operator’s entitlement servers, it is also unlikely any malicious user can feasibly launch such an attack.

Storage

- CSCsi32228

  Symptom:

  After a reload, the CDNFS statistics are incorrect until the SE has synchronized all the content information in the system. The cached content database restoration can take a few hours if there are more than a million assets in the SE. During this time, content delivery, including cache hits, continues to work properly, buy the statistics are inaccurately displayed.

  Workaround:

  Allow the cache database to complete the restoration before checking the CDNFS statistics. Since database restoration can take even longer if there is constant and heavy traffic on the server, you are not recommended to direct too much traffic to a SE that has just reloaded.

- CSCsk82154

  Symptom:

  Under heavy stress, during mixed traffic of WMT and HTTP, the storage layer may report errors indicating corruption of storage metadata files. This is due to race conditions that occur when the content is being modified and looked atsimultaneously.

  Workaround:

These errors are transient and only result in a failure of a single request. New requests will not see this failure when the content is fully cached and the race condition does not exist.

Acquisition and Distribution

- CSCsi48105

  Symptom:

  The error reported for manifest file parsing may not provide the exact location of the parsing error. It is usually off by a few lines.

  Workaround:

  There is no workaround. This is an inherited problem from the open-source XML parser and is a known problem of the parser.

- CSCsj26190

  Symptom:

  If content deletion of preposition contents is occurring at the same time as newer contents are getting acquired, the content deletion may be very slow. This is noticeable when the number of assets >20 K.

  Workaround:

  There is no workaround.

SNMP

- CSCsk11560

  Symptom:

  SNMP Server authentication does not work if the privacy password is using SHA.

  Workaround:

  Use an MD5 based privacy password instead.

- CSCsk09674

  Symptom:

  When you execute the following config command in the SE to view the MIB, you receive an error.

  ```
  (config)#snmp-server view see ciscoServiceEngineMIB excluded
  ```

  Workaround:

  Use the object identifier (OID) instead of the symbolic name for the MIB subtree.

Caveats Not Caused by CDS Software

This release contains the following open caveats that are not caused by the CDS software:

Network Configuration

- CSCsi29008

  Symptom:

Traffic loss occurs for a few seconds when a failover from primary to standby is triggered. This is an intrinsic property of the standby network interface mode.

Workaround:

Configure the port channel on both CDE and the connected switch, instead of standby interface. Port channel can recover interface failures in sub-seconds.

Windows Media Streaming

- CSCsi57903

  Symptom:

  Client cannot use RTSPU when it is behind a NAT. This is an expected behavior as the client IP address is translated and not visible to server.

  Workaround:

  Configure the client to use RTSPT instead of RTSPU in its network configurations.

- CSCsh91171

  Symptom:

  The Windows Media Player controls are enabled for live sessions. This is a Windows Media Player issue.

  Workaround:

  There is no workaround. This problem exists with or without CDS.

- CSCsh90306

  Symptom:

  During playback of high bit-rate files, server streams the data at five times the rate of the bit-rate. This issue is seen even when the CDS is not used. It is Windows Media Player issue.

  Workaround:

  Turn off the fast cache feature on the server (Windows Media Server or CDS WMT), when serving high bitrate content (more than 780Kbps).

Web Engine

- CSCsi08778

  Symptom:

  Windows Media Player cannot play media files with a size greater than or equal to 4GBytes that are progressively downloaded. This is a Windows Media Player issue as it does not work whether the origin server is IIS or Apache and whether CDS is used.

  Workaround:

  There is no workaround.

- CSCsi50430

  Symptom:

  When the Origin Server is Windows Media Server, and the client request causes a progressive download to occur, content playback fails in a hierarchical setup.

Workaround:

Make sure the file is streamed through WMT streaming.

- CSCsh85626

  Symptom:

  For contents in the origin server which are authenticated using NTLM, the Web-Engine download fails for those contents. It is commonly believed in the Internet community that supporting this for a proxy is a security hole, because we have multiple clients sharing same back end connection to origin server, since NTLM is a connection-based authentication scheme. For this same reason web proxies like Squid and Apache proxy module do not support this nor does the CDS.

  Workaround:

  Do not use NTLM authentication on the origin server.

Resolved Caveats

Release 2.0.3-b1 consists of 37 bug fixes since 2.0.1-b5. Not all the fixes are mentioned here. The following list highlights the fixes associated with customer deployment scenarios.

CDSM

- CSCsk72356

  Sympton:

  When type=”cache” is used in the Manifest file for a delivery service, the CDSM reports the replication status incorrectly. The CDSM reports the replication status as “cannot scan content length.”

WMT

- CSCsk72328

  Symptom:

  In a broadcast playlist with multiple entries, when the file wraps around, live-splitting fails and multiple incoming streams are shown in the SE.

- CSCsk45181

  Symptom:

  If a multi-bit rate (MBR) file is used as the source for the broadcast playlist, once the files wraps around, any new requests takes up to seven seconds to start streaming.

- CSCsk84601

  Symptom:

  For RTSP requested URLs, even though the URL validation is enabled through PCMM configuration for the delivery service, URL validation does not take place. As a result, even if the URL is unsigned, it always passes validation.

- CSCsk76598

  Symptom:

For multicast programs, when the source is a publishing point that is created with SSPL, multiple incoming streams are shown in the CLI **show statistics wmt streamstat** command.

Service Router

- CSCsk11667

  Symptom:

  Quova is an external geo-location database that CDS uses to route off-net traffic. If the secondary Quova server is not configured, and for some reason the primary Quova server fails (for example, due to license expiry), then core files are generated by the Service Router back end binary.

Platform

- CSCsk81050

  Symptom:

  If the CLI **restore factory-default preserve basic-config** command is run when RAID is used, an error is generated and the CLI is aborted.
- CSCsk82571

  Symptom:

  When interfaces participating in a standby group are manually shutdown or started up by using the interface command's shutdown option, the standby priorities do not work as expected. Specifically, if a high priority interface is activated by using the **no shutdown** option, the interface does not become active as expected.
- CSCsk37714

  Symptom:

  Port 514 is left open on the SE. This is a management port and should be kept closed to outside traffic.
- CSCsk7975

  Symptom:

  Port 5279 is a management port and is left open on the SE. This port should be kept closed to outside traffic.

Storage

- CSCsl03560

  Symptom:

  Enhancements were made to the storage component, so that upon reboot the Internet Streamer is not preoccupied entirely by the storage scanning tasks.

Documentation Updates

There are no documentation updates for this release.

Notices

The following notices pertain to this software license.

OpenSSL/Open SSL Project

This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/).

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com).

This product includes software written by Tim Hudson (tjh@cryptsoft.com).

License Issues

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License:

Copyright © 1998-2007 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment:

   "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)".

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT "AS IS"' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN

NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License:

Copyright © 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

   "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)".

   The word 'cryptographic' can be left out if the routines from the library being used are not cryptography-related.
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)".

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License].

Related Documentation

Refer to the following documents for additional information about the Cisco Internet Streamer CDS 2.0:

- *Cisco Content Delivery Engine 100/200/300/400 Hardware Installation Guide* (OL-13478-03)

  http://www.cisco.com/en/US/docs/video/cds/cde/installation/guide/CDE_Install_Book.html
- *Cisco Internet Streamer CDS 2.0-2.1 Software Configuration Guide* (OL-13493-02)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/configuration/guide/is_cds20_22-cfguide.html
- Cisco Internet Streamer CDS 2.0-2.1 Quick Start Guide (OL-15479-01)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/quick/guide/ISCDSQuickStart.html
- *Cisco Internet Streamer CDS 2.0-2.1 API Guide* (OL-14319-02)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/developer/guide/cds20_21apiguide.html
- *Release Notes for Cisco Internet Streamer CDS 2.0* (OL-13494-02)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/release_notes/CDS_RelNotes2_0.html
- *Release Notes for the Cisco Internet Streamer CDS 2.1* (OL-15751-01)

  http://www.cisco.com/en/US/docs/video/cds/cda/is/2_0/release_notes/CDS_RelNotes2_1.html
- *Cisco Content Delivery System 2.x Documentation Roadmap* (OL-13495-03)

  http://www.cisco.com/en/US/products/ps7127/products_documentation_roadmaps_list.html
- *Regulatory Compliance and Safety Information for Cisco Content Delivery Engine 100/200/300/400* (78-18229-02)

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

Obtaining Documentation, Obtaining Support, and Security Guidelines

For information on obtaining documentation, obtaining support, providing documentation feedback, security guidelines, and also recommended aliases and general Cisco documents, 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

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