Release Notes for Cisco LocalDirector Version 4.2.4

August 20, 2002

Note The most current Cisco documentation for released products is available on Cisco.com at http://www.cisco.com. The online documents may contain updates and modifications made after the hardcopy documents were printed.

Contents

These release notes describe the following topics:

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

Introduction

Use these release notes with the *Cisco LocalDirector Configuration and Command Reference Guide, Version 4.2.*

Caveats

Caveats describe unexpected behavior in Cisco LocalDirector (LD) software releases. This section lists the open and resolved caveats for LD software, Version 4.2.4.

Open Caveats - LocalDirector Software Version 4.2.4

This section describes open caveats in LD software version 4.2.4.

- CSCdx07160

  With two LDs configured for stateful failover and sticky and with spanning tree enabled on the LD ports, a system reload causes the primary active LD to fail over. The new active LD sends HTTP requests to a different server for about 30 seconds after booting up the primary LD. Workaround: Disable spanning tree completely.

- CSCdy08259

  With **reassign** set to a value of 2, the LD does not reassign a new server until the fourth SYN packet fails to get a response for the same connection. The LD should reassign a server on receipt of the third SYN packet.

- CSCin08842

  If you configure a non-port-bound real server on an LD, but then use it as a port-bound real server with the **probe real** command, the LD reboots.

- CSCdx13773

  With generic sticky configured (but not SSL sticky), occasionally an SSL session hangs. When an SSL session is about to end, the LD sends a reset (RST) to the client, but not to the real server. The next time the same client (source address) establishes a new connection (with a new source port) to the same VIP on the Local Director, the LD sends the request to the same server, which considers the new connection the same as the old connection. After a number of unsuccessful attempts, the LD tries another server, without marking the first server as Failed. As a result, the client application terminates.

- CSCdy16810

  When you are using the LD in cookie-insert mode, the day of the week is not RFC-compliant in the cookie expiration time.

- CSCdy16926

  LD generates traps with conflicting information for version and protocol data unit (PDU) type. This may cause problems for network management applications because the trap may not get processed or may get processed improperly, depending on the application behavior. There is no workaround.

- CSCdv21441

  The LD snmpwalk operation with the MIB variable cldexVirtualTotalBytes does not show all the virtual servers.

- CSCdx28331

  Sticky SSL does not work correctly when each real server IP address is the same, but the ports are different. The LD sends SSL packets originating from the same client with the same session ID to different real servers.

- CSCdy37648

  For defined UDP static translations, the LD does not translate fragmented packets.

- CSCdy37674

  For UDP static translations, the UDP real server must be defined for packets to flow.

- CSCdx47615

  The LD running software 4.2.3.106 stops operation and reboots unexpectedly.

- CSCdm62909

  The LD **snmpwalk** operation fails to fully traverse nodes in lexicographical order when starting at some nonleaf nodes. However, you can use **snmpwalk** to traverse the entire tree.

- CSCdx71253

  SSL sticky works only when the browser is Internet Explorer 5.5.

- CSCdx85558

  The LD does not respond to UDP traceroute queries.

Resolved Caveats - LocalDirector Software Version 4.2.4

All caveats listed in this section are resolved in LD software version 4.2.4.

- CSCdw64918

  The Local Director contains vulnerabilities in the processing of Simple Network Management Protocol (SNMP) messages. The vulnerabilities can be repeatedly exploited to produce a denial of service. In most cases, workarounds are available that may mitigate the impact.

  This advisory is available at http://www.cisco.com/warp/public/707/cisco-malformed-snmp-msgs-non-ios-pub.shtml, and it describes this vulnerability as it applies to Cisco products that do not run Cisco IOS software.

- CSCdx00651

  The LD does not properly send the maximum segment size (MSS) to the server for proxy code.

- CSCdx01304

  LocalDirector does not pass UDP fragmented packets when an interface has been secured using the **secure** command and the real servers the fragmented packets are arriving for have a bindid of 666.

- CSCin01718

  Configuring **cookie-insert sticky** causes the LD to load balance a client to an incorrect real server within the sticky time.

- CSCdx07813

  If you enter the **show tech** command, even from user mode, password information is visible. Password information should not be displayed.

- CSCdy09651

  The LD reboots unexpectedly when you enter a **backup config** command to back up an HTTPS VIP. Do not back up a VIP that has a redirect URL similar to 192.168.12.7:443:0:tcp.

- CSCin12776

  The **probe real** and the **probe virt** commands do not allow the default values of *real_id* and *virtual_id*, respectively. You must also provide the values for port, bind_id, and protocol field for *real_id* and *virtual_id*.

- CSCdt14979

  The **configuration net** command causes the LD to reboot if the configuration file on the TFTP server lists both virtual and real servers.

- CSCdw19342

  When you configure **sticky ssl** on the LD, entering **oos real** *real-id* **sticky** causes the subsequent client connections to be reset. Also, when HTTP to HTTPS redirection is configured, entering **oos real/dip** causes the subsequent client connections to be reset. The LD is denying the connections. When the real server or the dip are placed back in-service (IS), the LD operates properly.

- CSCdx22427

  When running HTTP to HTTPS redirection and with the **backup** command set to backup DIP1 with DIP2 and DIP2 with DIP1, the LD reboots without a stack trace if the real servers are out of service. Workaround: If you use the real IP address as the backup, the LD does not reboot.

- CSCdx24026

  If you configure **leastconns** with the default slowstart method of **roundrobin**, use the **predictor** command to configure **slowstart** to **none**, then use the **predictor** command again to reset **slowstart** to **roundrobin**, the LD generates the CLI error `Too many arguments`.

- CSCdu24361

  Both the DFP agent and the DFP manager are not functional.

- CSCdv29680

  In SSL sticky mode, the LD may drop the first data packet following the packet that contains the SSL session ID. This is because the unit is transitioning the connection from a proxied connection to an unproxied connection. During this transition phase, the LD drops packets from the server. The server resends the packet based on the behavior of TCP, but this causes a noticeable delay to the client.

- CSCdx30008

  If you add a port-bound real server to a probe when the LD configuration does not contain port-bound real servers, the LD reboots with a stack trace.

- CSCdu36452

  Documentation: A domain name for the DNS **boomerang client** command can have a maximum of 212 characters.

- CSCdw37702

  If you configure **cookie-insert** on the LD and the LD receives HTTP packets that contain cookie information that spans more than two packets, the LD does not transmit the HTTP sequence in the correct order.

- CSCdw39088

  Under certain circumstances (for example, if a PIX is involved), port/passive FTP fails with FTP proxy. The reason is that the LD does not add a CR+LF to the 227 answer sent back to the client.

- CSCdw39115

  The LD fails to accept a telnet session behind a SYN-defender feature available from a third-party firewall solution. The LD tries to move a TCP connection from SYN-RCVD to ESTABLISHED by sending an acknowledgement on behalf of the client with TCP Window=0. A real client packet is expected to continue the connection, but the LD does not send the password prompt.

- CSCdt39374

  If you issue the **out-of-service** command for a URL, then reload the LD, the update to the URL using the **out-of-service** command is lost. When rebooting the LD, the status of a URL depends on the status of the DIP that it is linked to, and not on, the last status given by the **out-of-service** command.

- CSCdu41822

  A failed standby LD reboots while it is trying to access configurations from the active LD.

- CSCdw44399

  The LD verifies all SNTP broadcast messages from specified servers. If the LD is configured to accept messages only from specified servers, it will update its clock only from those servers. However, if there is an error in messages from an unconfigured server, the LD sends an error message to syslog.

  For example, if there is an SNTP host that is broadcasting messages that are not of the version supported by the LD, it will verify the message as a first step. Then, the LD sends an error message to syslog stating that it received an unsupported version message.

- CSCds45864

  Documentation: The **no channel** command restores only the primary interface. The other interfaces are shut down to prevent a bridge loop. For example:

  channel 0 four - Channels four interfaces to one at interface 0.

  no channel 0 four - Undoes the previous command, but restores only interface 0. Interfaces 1, 2, and 3 are shut down to prevent a bridge loop. You must use the **no shutdown** command to restore interfaces 1, 2, and 3.

- CSCds47214

  Documentation: The **sticky** command is allowed on DIP virtual servers for completeness and to reduce the CLI complexity. However, it is not practical to have a sticky association on a virtual machine that can be bound to only one real server. To reduce unnecessary processing overhead in the LD, Cisco recommends that you do not specify a sticky association on a DIP.

- CSCdv49047

  The cookie passive hash table entries are not being replicated to the standby LD after it completes a reboot. This behavior occurs only with the LD-420 platform.

- CSCds51092

  Documentation: The **bind** command Usage Guidelines section of the Release Notes for Cisco LocalDirector 4.1 has incorrect examples of the **url** command usage. The URL specification requires the http:// prefix for a URL string.

- CSCdw61150

  If you configure virt:443 and virt:0 on the LD, when the LD reboots and comes into operation, it sends TCP RSTs to connections to virt:0. If you configure a **cookie-[insert|passive] sticky** association on the virt:0 and then remove the sticky association immediately, all subsequent connections to virt:0 work properly.

- CSCdv61279

  If you perform an snmpwalk of any column of the table enterprises.cisco.ciscoMgmt.ciscoLocalDirectorMIB.ciscoLocalDirectorMIBObjects.cldRealMachine.cldeRealTable (.1.3.6.1.4.1.9.9.99.1.2.2), the walk starts looping as soon as the LD returns an entry with a non-zero bindid value.

- CSCdv63786

  The LD does not fail the real server even when the data threshold is exceeded.

- CSCdu66091

  Documentation: The description of the **name** command in the Command Reference section of the *LocalDirector Configuration Guide* does not state the limit of the name length allowed. Currently the Name description is: Name assigned to the IP address. It should state that all names must be less than 32 characters in length.

- CSCdw72992

  If you configure the LD with an IP address and TFTP server, the LD will reboot if you enter the **conf net** command and the network config file being loaded contains the following two lines:

  ```
  failover
  failover ip address 0.0.0.0
  ```

- CSCdw79604

  If you configure **cookie-passive** on the LD, enable debug level syslog messages, and are running Microsoft® Internet Explorer version 5.5 on Windows® 2000, the LD delays the second continuation marking, which causes IE to pause for several seconds before answering the next request.

- CSCdw85676

  For outbound traffic, the LD changes the source IP address for all real servers when using the **static** command, regardless of the port that has been defined. For L4 flows, only the defined port should be NATed with the VIP for outbound traffic.

- CSCdw87752

  When you configure the LD in front of a multicast firewall cluster, the LD duplicates the responses from the server.

- CSCdv90797

  If CLB is enabled while the LD is under heavy load, the LD may reboot.

- CSCdt93431

  If you enter an invalid interface number when using the **shutdown ethernet** or **no shutdown ethernet** command, the LD interprets it as interface 0.

Related Documentation

The following documents provide additional information and should be used in conjunction with these release notes:

- *Cisco LocalDirector Configuration and Command Reference Guide, Version 4.2*
- *Cisco LocalDirector Hardware Installation Guide*
- *Cisco LocalDirector 417 Hardware Installation Guide*
- *Release Notes for Cisco LocalDirector 417G*
- *Regulatory Compliance and Safety Information for Cisco LocalDirector*
- *Cisco Content Router 4400 User Guide*

Obtaining Documentation

These sections explain how to obtain documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at this URL:

http://www.cisco.com

Translated documentation is available at this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription.

Ordering Documentation

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

  http://www.cisco.com/go/subscription

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. In the Cisco Documentation home page, click the **Fax** or **Email** option in the "Leave Feedback" section at the bottom of the page.

You can e-mail your comments to bug-doc@cisco.com.

You can submit your comments by mail by using the response card behind the front cover of your document or by writing to the following address:

Cisco Systems
Attn: Document Resource Connection
170 West Tasman Drive
San Jose, CA 95134-9883

We appreciate your comments.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain online documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you with these tasks:

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

If you want to obtain customized information and service, you can self-register on Cisco.com. To access Cisco.com, go to this URL:

http://www.cisco.com

Technical Assistance Center

The Cisco Technical Assistance Center (TAC) is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two levels of support are available: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Cisco TAC inquiries are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

The Cisco TAC resource that you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

You can use the Cisco TAC Web Site to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to this URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco service contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to this URL to register:

http://www.cisco.com/register/

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC Web Site, you can open a case online by using the TAC Case Open tool at this URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, we recommend that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses priority level 1 or priority level 2 issues. These classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer automatically opens a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to this URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled: for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). When you call the center, please have available your service agreement number and your product serial number.

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