Signaling Delivery Controller

Release Notes

4.4 CF 4

Catalog Number: RG-015-44-61 Ver.2

Publication Date: June 2015

Legal Information

Copyright

F5 Networks, Inc. (F5) believes the information it furnishes to be accurate and reliable. However, F5 assumes no responsibility for the use of this information, nor any infringement of patents or other rights of third parties which may result from its use. No license is granted by implication or otherwise under any patent, copyright, or other intellectual property right of F5 except as specifically described by applicable user licenses. F5 reserves the right to change specifications at any time without notice.

Trademarks

AskF5, F5, F5 [DESIGN], F5 Networks, OpenBloX, OpenBloX (design), Rosetta Diameter Gateway, Signaling Delivery Controller, SDC, Traffix, and Traffix [DESIGN] are trademarks or service marks of F5 Networks, Inc., in the U.S. and other countries, and may not be used without F5's express written consent.

All other product and company names herein may be trademarks of their respective owners.

Patents

This product may be protected by one or more patents indicated at: *http://www.f5.com/about/guidelines-policies/patents*

Confidential and Proprietary

The information contained in this document is confidential and proprietary to F5 Networks. The information in this document may be changed at any time without notice.

About F5 Networks

F5 Networks (NASDAQ: FFIV) makes the connected world run better. F5 helps organizations meet the demands and embrace the opportunities that come with the relentless growth of voice, data, and video traffic, mobile workers, and applications—in the data center, the network, and the cloud. The world's largest businesses, service providers, government entities, and consumer brands rely on F5's intelligent services framework to deliver and protect their applications and services while ensuring people stay connected. For more information, visit *www.F5.com* or contact us at *Tfx_info@f5.com*.

About this Document

Document Name: F5 Signaling Delivery Controller Release Notes

Catalog Number: RG-015-44-61 Ver.2

Publication Date: June 2015

Document Objectives

This document provides information about the features introduced, known issues, bug fixes, and limitations included in the F5 SDC release 4.4, CF 3.

Document History

Revision Number	Change Description	Change Location
June 2015 – Ver. 2	Added bug fix description.	*See Monitoring*

Conventions

The style conventions used in this document are detailed in Table 1.

Table 1: Conventions

Convention	Use
Normal Text Bold	Names of menus, commands, buttons, user-initiated CLI commands and other elements of the user interface
Normal Text Italic	Links to figures, tables, and sections in the document, as well as references to other documents
`Script`	Language scripts
`Courier`	File names
Note:	Notes which offer an additional explanation or a hint on how to overcome a common problem
Warning:	Warnings which indicate potentially damaging user operations and explain how to avoid them

Table of Contents

List of Tables

1. Release Information

1.1 Product Software Versions

This build consists of the following F5 SDC product software packages:

- Installer: Installer-4.4-121
- F5 Traffix Menu: 4.4-89
- SDC Software: Sdc-4.4.4-1
- Tripo: Tripo-1.2.5-27
- File Server: Fileserver-1.0.0-39

1.2 ISO Image Information

The F5 SDC software for installation is packaged and supplied as an ISO image.

The following information describes the ISO image provided to install this release:

- Filename: ctu.4.4.4-73.iso
- MD5: 50e8f3b8d921c85125c91259466e1503
- Date: Jun 14, 2015 1:24:58 PM
- Size: 1,544,415,232 bytes

1.3 Upgrading to This Release

This release can be upgraded to from SDC releases 4.0.2 and 4.0.5.

When upgrading to this release, take the following memory allocations into account:

- Each FEP resource requires 2GB of memory.
- Each CPF resource requires 3GB of memory.

1.3.1 Upgrade File Information

The F5 SDC software for upgrade is packaged and supplied as a tar.gz file.

The following information describes the tar.gz file for this release:

- Filename: sdc_media_pack-f5cli-1.0-14-FileServer-1.0.0-39-menu-4.4-91-sdc-4.4.4-1-Tripo-1.2.5-27-103.tgz
- MD5: 6100f6fdf44f07710fefaaa85d6965ed
- Date: Jun 14, 2015 1:19:35 PM
- Size: 979,112,651 bytes

1.4 Supported Browsers

The F5 SDC Web UI is supported by the following browsers:

- Internet Explorer 9 and higher
- Mozilla Firefox 14.0.1 and higher (excluding Firefox 36).

1.5 Supported Operating Systems

SDC is certified to run on the following operating systems:

- Red Hat Enterprise Linux (RHEL) 6.6 64 bit

2. What's New in This Release?

This section describes the following changes implemented in F5® Traffix® Signaling Delivery Controller™ (SDC) release 4.4:

- FEP – CPF Communication Improvements
    - Peer State Distribution
    - FEP – CPF Connectivity
- Overload Control Capability Improvements
    - SDC Overload Control
        - Incoming Rate Limit
        - Incoming Traffic
    - Remote Peers Overload Control
        - Outgoing Rate Limit for Requests
        - Outgoing TPS Threshold
- Session Logging Enhancements
    - Session Management Logging Parameters
    - Session Replication Troubleshooting Logs
- REST Based Configuration Distribution Mechanism
- ISSU Enhancement
- SDC OS Upgrade
- CLI Tool for Peer and Pool Management
- Accessibility
- Wi-Fi Offload
- Security Updates

2.1 FEP – CPF Communication Improvements

2.1.1 Peer State Distribution

In previous releases, the peer state distribution was based on JMX. Due to inherent limitations in JMX, sometimes these states were inconsistently distributed between SDC components. In release 4.4, the state of the peers is distributed between the FEP and the CPF using JSON over UDP.

2.1.2 FEP – CPF Connectivity

The connectivity mechanism between the FEP and the CPF was stabilized in release 4.4, alleviating disconnects between CPF and FEP experienced in previous releases.

2.2 Overload Control Capability Improvements

Increasing traffic volume required several improvements to the rate limit mechanism and to SDC behavior in overload scenarios:

2.2.1 SDC Overload Control

2.2.1.1 Incoming Rate Limit

In previous releases, the rate limit was measured in one second time frames. In release 4.4, the rate limit mechanism uses a sliding window mechanism.

2.2.1.2 Incoming Traffic Congestion

Increasing the SDC ability to react efficiently to sudden occurrences of high traffic, the overload control in release 4.4 was improved by adding a high watermark threshold for the incoming traffic. Once it is exceeded, the SDC limits the allowed volume of incoming traffic by modifying the transport layer behavior (for example, changing the TCP window size).

2.2.2 Remote Peers Overload Control

2.2.2.1 Outgoing Rate Limit for Requests

The previous overload control for remote peers provided by the SDC, which controlled the rate of outgoing traffic towards each server peer, was extended to client peers in release 4.4. This overload control protection is applied on requests only.

2.2.2.2 Outgoing TPS Threshold

Release 4.0.2 introduced configurable thresholds for outgoing traffic monitoring. These thresholds, merged into release 4.4, reflect the rate of the outgoing requests sent by SDC. These thresholds are defined per peer and per pool, and allow early detection of potential peer and pool overloads.

Upon reaching the defined thresholds, per pool and/or peer, the system sends an SNMP trap (Pool Rate Limit State Change and/or Peer Rate Limit State Change) indicating that the measured TPS has exceeded one of the configured peer and/or pool thresholds (Minor, Major, Critical).

2.3 Session Logging Enhancements

2.3.1 Session Management Logging Parameters

In release 4.4, custom parameters can be added by the user to the session life-cycle log messages that are generated upon session initialization. The additional parameters are added using the Web UI.

2.3.2 Session Replication Troubleshooting Logs

New log messages are generated upon:

- CPF initialization, to indicate if session replication is enabled, and if it is CPF or Tripo based.
- CPF replication failure (when enabled).

2.4 REST Based Configuration Distribution Mechanism

In previous releases, an ActiveMQ based mechanism was responsible for configuration distribution and synchronization between the SDC components. In release 4.4, the configuration distribution mechanism is based on the REST Web Service API, which ensures successful configuration distribution between the SDC components by invoking synchronization and re-synchronization operations. Following the change of the mechanism, the amount of configuration distributions is reduced and instead of broadcasting each configuration change, the configuration is distributed only to the relevant SDC components.

To secure the configuration channel between the EMS and SDC sites, the user can decide whether the EMS-SDC connection uses an HTTP or HTTPS transport layer.

2.5 ISSU Enhancement

From release 4.4 onwards, the EMS supports both ActiveMQ and REST API and can successfully maintain normal activity in a deployment where one managed SDC site works with ActiveMQ and another works with REST API. As a result of this dual support, it is possible to upgrade a deployment with multiple SDC sites managed by EMS in different maintenance windows.

For example:

Maintenance window 1:

Upgrade EMS from 4.0.2/4.0.5 to v4.4, upgrade SDC1 from 4.0.2/4.0.5 to v4.4

Maintenance window 2:

Upgrade SDC2 from 4.0.2/4.0.5 to v4.4

2.6 SDC OS Upgrade

SDC release 4.4 runs on RH-6.6.

2.7 CLI Tool for Peer and Pool Management

A CLI tool, introduced in release 4.0.5, is included in release 4.4. Access to this tool is available from each SDC site, as well as from the EMS sites. This tool allows monitoring of all peers and pools in the deployment. Adding a peer to a pool, as well as enabling and disabling peers, is possible using the CLI tool.

2.8 Accessibility

In release 4.4 the product Web UI's color palette was aligned with the accessibility standard. In addition, an option to navigate through the Web UI using the keyboard was added. This feature is disabled by default.

2.9 Wi-Fi Offload

Release 4.4 includes the Wi-Fi offload functionality – where the SDC is able to authenticate subscribers connecting to Wi-Fi networks using the EAP mechanism. By enabling the Wi-Fi offload functionality, the SDC authenticates subscribers based on their SIM. This feature implements the authentication flow from the Wi-Fi network (RADIUS) to HLR (SS7-MAP). Currently, the following authentication methods are supported:

1. EAP – SIM – Authentication of 2G subscribers
2. EAP – AKA – Authentication of 3G subscribers.

2.10 Security Updates

2.10.1 Security Updates in CF 3

This CF of release 4.4 does not include any security update fixes.

2.10.2 Security Updates in CF 2

Due to the Apache Tomcat CVE-2014-0227 alert, users should upgrade Apache Tomcat version 6.0.37 to any version later than 6.0.43 (including). (CPF-12794)

2.10.3 Security Updates in CF 1

This CF of release 4.4 does not include any security update fixes.

2.10.4 Security Updates in CF 0

This CF of release 4.4 does not include any security update fixes.

3. Fixed Bugs

This section describes the bugs fixed in Release 4.4.

3.1 Fixed Bugs in CF 4

This section describes the bugs fixed in Release 4.4, CF 4.

3.1.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1473	Previously after completing an ISSU, the Tomcat component running on the backup Installer server was not accessible. Now, the Tomcat component is accessible and starts up on the backup Installer as expected.	

3.1.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-14487	Previously, some requests could not be answered by the BEP as the BEP did not recognize the Hop-by-Hop AVP and CPF InstanceUid values that were generated by the CPF. Now, the CPF "mask" process is fixed so that generated Hop-by-Hop AVPs and CPF InstanceUid values are recognized by the BEP and requests are answered as expected.	

3.1.3 Session Repository

ID	Description	Related ID in Previous Releases
CPF-13774	Previously, Tripo entries were not deleted from the database if the replicated Tripo site just started up and was empty. Now, the system is configured to acknowledge a Delete request even if the entry is not found in the empty mated site.	4.0.5: CPF-13773

ID	Description	Related ID in Previous Releases
CPF-13960	Previously, when replicating sessions between Tripo instances, if the UI_viewStorage tool was connected, some SRR (Delete) requests were not replicated between Tripo instances. Now, the UI_viewStorage tool was reconfigured not to reset the state of the mated Tripo site to disconnect, thereby preventing SRR (Delete) requests from not being replicated between Tripo instances.	
CPF-14371	Previously, when performing and ISSU, and starting the upgraded Tripo in maintenance mode, the Tripo logs showed a fatal (ALERT) error message. Now, following changing the related log message to an INFO level, the Tripo instance starts in maintenance mode after an upgrade without any fatal error log messages.	4.0.5: CPF-13985

3.1.4 Monitoring

ID	Description	Related ID in Previous Releases
CPF-12149	Previously, the MPS statistic was not calculated correctly and did not appear in the SDC **Dashboard**. Now, the MPS statistic correctly counts all the incoming messages (requests and answers) received from the remote peers and not SRRs, Proxy Messages, and Watchdog messages. This statistic is now displayed in the SDC **Dashboard** per CPF and in the license.log file. In addition, an improved log rotation mechanism was added to the license.log file, so that this file no longer fills up, as it is configured to maintain a four month history.	
CPF-14076	Previously, when adding an AVP to a diameter message, during post-transformation, the TDR Sending_ Request_Length and Answer_	

ID	Description	Related ID in Previous Releases
	To_Client_Length values were not correctly calculated (**Reports**>**Transaction Data Records**). Now, the code was modified to correctly calculate and display these values.	
CPF-14404	Previously, FATAL "secondary key appears as primary in the received request" error messages were generated in the Tripo log files. The log level was changed from FATAL to WARN, and is now only displayed if the Storage.log is configured to a WARN level or higher.	4.0.5: CPF-13778

3.2 Fixed Bugs in CF 3

This section describes the bugs fixed in Release 4.4, CF 3.

3.2.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1329	Site configuration files that are created and/or edited with IPv6 addresses are now validated by the Installation Utility.	
Installer-1394	The `wget` RPM file is now automatically installed on all site servers.	
Installer-1419	The installer now saves the SNMP community string setting throughout the ISSU.	

3.2.2 Monitoring

ID	Description	Related ID in Previous Releases
CPF-13825	The cpfSiteReplicationTargetDown and	

ID	Description	Related ID in Previous Releases
	cpfSiteReplicationTargetUp alarms are now generated as expected.	
CPF-13808	The cpfNodeClientsQueueHighWatermarkAlarm alarm is now generated as expected.	

3.2.3 Session Repository

ID	Description	Related ID in Previous Releases
CPF-13822	The replication peer health status now accurately reflects the peer health as it fluctuates between red and green in the Web UI. (**Topology>Specific Site Settings>Remote Peers>Health**)	4.0.5: CPF-13729

3.3 Fixed Bugs in CF 2

This section describes the bugs fixed in Release 4.4, CF 2.

3.3.1 1Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1370	Previously, when the default gateway was not defined in the site configuration file, a null pointer exception was generated. Now, the correctly defined error log is printed in the installer log file.	
Installer-1358	Previously, errors were erroneously generated in the installer log files when the ISSU completed successfully. Now, successful ISSU processes do not generate errors.	
Installer-1409	Previously, after performing an ISSU rollback the site servers could not boot successfully, resulting in a red screen. The rollback procedure was updated, and the	

ID	Description	Related ID in Previous Releases
	site servers can now boot successfully. For more information, see the *F5 SDC Upgrade Guide*.	

3.3.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-13747	The **Administration > Specific Site Settings > SNMP > SNMP Dilution Manager** screen was updated and now includes the following traps: interCommunicationRetransmitTimeout and InterCommunicationNoMoreRoomForPendingMessagesAlarm.	
CPF-13534	Previously, refreshing the **Topology** > **Specific Site Settings** > **Remote Peers** and **Topology** > **Specific Site Settings** > **Pool** screens reopened the screen at the beginning of the table, regardless of the row the user was viewing in the table. Now, by disabling the default auto-refresh, the user is able to stay at a specific row of the table. Note: By default, auto-refresh is enabled for these screens. Auto-refresh must be disabled every time the screen is accessed.	
CPF-13450	Previously, the **ACL Accepted/Rejected** statistics do not appear correctly in the SDC Web UI (**Dashboard**). These statistics now appear correctly.	

3.3.3 Topology

ID	Description	Related ID in Previous Releases
CPF-13598	Previously, SCTP peers were perpetually in an “Out Of Service” state. Now, the channel state can reach low watermark and the peer state can be cleared.	4.0.5:CPF-13597

3.3.4 Flow Management

ID	Description	Related ID in Previous Releases
CPF-13115	Upon removing the last row in one of the tables (**Routing**, **Transformation**, **Session Management**, **Dynamic Peer Profiles**, **Pools**, **Tracing**), a timeout and exception warning were thrown. In addition, when creating/removing a row from the middle of a table, the system was not updated to refer to the correct row. RCA: The code was mistakenly designed to refer to a table's row ID as it appeared in the Web UI and not the unique row ID of the policy rule. Consequently, the system would try to access a non-existing row or a row with a different ID, and this caused an exception and timeout error. Fix Details: The code was modified that the matching process now references the unique ID of the routing policy rule instead of the Web UI row number.	4.0.5: CPF-12802
CPF-13888	Previously, the default timeout for transaction events (after sending requests to a server) was set for ten seconds. Fix Details: The default timeout for transaction events was reconfigured to three seconds.	

3.3.5 Session Repository

There are no bugs fixed in this category.

3.3.6 Performance

There are no bugs fixed in in this category.

3.3.7 Monitoring

ID	Description	Related ID in Previous Releases
CPF-13542	Previously, sending an SRR request to a disabled SDC server generated a Null Pointer Exception error in the SDC log files. This Null Pointer Exception is no longer generated.	
CPF-13543	Previously, configuring custom parameters to be added to the session life-cycle log messages (**Administration** > **Logging** > **Enable Session Logging**) failed if the attribute names contain a "." character. The "." Character is now a valid character.	
CPF-13061	The customStatistics files that were generated in the EMS file system were deprecated.	

3.3.8 Administration

There are no bugs fixed in this category.

3.3.9 Accessibility

ID	Description	Related ID in Previous Releases
CPF-13711	A hotkey was added to focus on the keyboard button and open the accessibility menu. To focus on the keyboard button, press **Alt+Ctrl+x**. When focused on the keyboard button, to open the accessibility menu, press **Enter**.	

3.3.10 HTTP

ID	Description	Related ID in Previous Releases
CPF-13473	Previously, when HTTP server peers configured with host IP addresses taken from DNS connected with the SDC,	4.0.5: CPF-13467

ID	Description	Related ID in Previous Releases
	the host IP address was resolved at the time of the first connection and then cached for all subsequent connections between the HTTP server peer and the SDC. Now, the resolving result is done each time without caching, thereby ensuring that the HTTP server peer is always configured with the updated IP address from the DNS server.	

3.4 Fixed Bugs in CF 1

This section describes the bugs fixed in Release 4.4, CF 1.

3.4.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1189	Previously, after upgrading the Operating System as part of the ISSU, some RPMs on the upgraded site stopped behaving as expected. RCA: The ISSU only upgrades a defined list of RPMs. If there are additional RPMs on the site that are not part of the defined list, or if there are RPMs with a different version, they are not upgraded. Fix Details: Before beginning the upgrade and after completing the upgrade, a file is generated for each site server with a list of RPMs that should be deleted. For more information, see the F5 SDC Upgrade Guide.	
Installer-1334	After an upgrade, the SS7 driver is not able to establish an SCTP connection with the SS7 peer.	

ID	Description	Related ID in Previous Releases
	RCA: The IP tables were not configured to allow the heartbeat and heartbeat_ack requests and responses. Fix Details: The IP tables were configured to allow the heartbeat and heartbeat_ack requests and responses.	

3.4.2 Web UI

There are no bugs fixed in this category.

3.4.3 Topology

There are no bugs fixed in this category.

3.4.4 Flow Management

There are no bugs fixed in this category.

3.4.5 Session Repository

There are no bugs fixed in this category.

3.4.6 Performance

There are no bugs fixed in in this category.

3.4.7 Monitoring

ID	Description	Related ID in Previous Releases
CPF-13306	Previously, pool rate limit thresholds could only be defined on the site level. Now, pool rate limit thresholds can be defined on the pool level as well as on the site level.	

ID	Description	Related ID in Previous Releases
CPF-13037	The cpfNMSCollectingStatisticsClear trap was added to the MIB file. This trap is the clear trap for the cpfNMSCollectingStatisticsFailure alarm.	

3.4.8 Administration

There are no bugs fixed in this category.

3.5 Fixed Bugs in CF 0

This section describes the bugs fixed in Release 4.4, CF 0.

3.5.1 Installation and Upgrade

There are no bugs fixed in this category.

3.5.2 Web UI

There are no bugs fixed in this category.

3.5.3 Topology

ID	Description	Related ID in Previous Releases
CPF-11076	The origin realm value configured per FEP-SCTP-Out was ignored and not sent in a CER. RCA: The inputted value for the Origin Realm is not updated. Fix Details: The code was modified so that before sending a CER, all values for Origin Realm are updated. Verification Steps: 1. Go to **Topology>Specific Site Settings>Remote Peers** and configure a SCTP remote peer, for example with the Address:10.3.124.195;10.3.124.227:4000	4.0.5: CPF-9176

ID	Description	Related ID in Previous Releases
	2. Go to **Topology>Specific Site Settings>Pools** and add the configured peer to a pool and then in **Routing**, assign the pool a **Route** action 3. Go to **Topology>Specific Site Settings>SDC Components** and edit the fep-sctp out-properties as follows: • In the **General tab**, set **Product Name** to "F5 fepsctpout-179 Traffix Systems Control Plane Function" • In the **Diameter** tab, set **Realm** to "traffixsystems_fepsctpout-179.comStart 4. Start Jmeter server to listen at port 4000 and verify that **Origin-Realm** now has the value "traffixsystems_fepsctpout-179.com"	

3.5.4 Flow Management

ID	Description	Related ID in Previous Releases
CPF-10714	In some cases, dynamically added peers received unexpected timeouts. RCA: This issue was caused by the fact that there were peers that did not successfully connect to all CPFs. As a result, many timeouts were generated. Fix details: The FEP-CPF communication improvements (see section 2.1) stabilized the connectivity between the CPFs and the peers.	

3.5.5 Session Repository

ID	Description	Related ID in Previous Releases
CPF-11855	Some proxied request messages failed to reach their mated SDC site, resulting in an internal warning (NullPointerException). RCA: The system was configured to check each routing row for each message, to determine the message's destination. However, proxied messages (i.e. SRRs), that were not associated with a specific routing row and had a pre-defined destination, had conflicting routing configurations to the system's standard routing configuration, and caused such messages to not be routed correctly and generated NullPointerExceptions. Fix Details: The code is modified to check if proxied messages are associated with a specific routing row and a pre-defined destination. Verification Steps: 1. Set environment with two SDC remote sites, Jmeter client, Jmeter server and Tripo Site Replication enabled. 2. Configure Routing (RESOLVE) and Session Management (Persist and Replicate) 3. Start sending CCRi requests from Jmeter client to one of the SDC sites 4. Observe traffic that all requests proxied to mated site. 5. Verify the logs that there are only WARN messages about failed to bind	4.0.5: CPF-11825

ID	Description	Related ID in Previous Releases
	the session and no NullPointerExceptions	

3.5.6 Performance

There are no bugs fixed in in this category.

3.5.7 Monitoring

ID	Description	Related ID in Previous Releases
CPF-11102	The **CpfPoolHealthStateChangedRedAlarm** was not generated when all the peers of a specific pool are down. When the peers were then re-enabled, then the **CpfPoolHealthStateChangedRedAlarm** was mistakenly generated. RCA: The health calculation formula of the pool did not accurately reflect the states (red, yellow, green) of the peers in a pool and did not correctly associate the relevant traps with each of these states. Fix Details: The code was modified to recognize the correct pool state and then to associate the correct SNMP trap with a specific state. Verification Steps: 1. Create a pool and associate to the pool, two server peers (Jmeter server). 2. Stop one server peer causing the pool's state to change to yellow. 3. Verify that a **CpfPoolHealthStateChangedYellowAlarm** trap was generated.	4.0.2: CPF-11100; 4.0.5: CPF-10911

ID	Description	Related ID in Previous Releases
	4. Stop the second peer, causing the pool state to change to red. 5. Verify that a **CpfPoolHealthStateChangedRedAlarm** trap was generated. 6. Restart one peer, causing the pool health state to change back to yellow and verify that a C**pfPoolHealthStateChangedYellowAlarm** trap is generated. 7. Restart the second peer, a causing the pool health state to change to green and verify that a **CpfPoolHealthStateChangedGreenAlarm** trap is generated.	
CPF-12429	Previously, the external peer selector did not successfully resume activity after the CPF is restarted. Now activity is resumed successfully.	4.0.2: CPF-7676

3.5.8 Administration

There are no bugs fixed in this category.

4. Known Issues

This section describes the known issues that are included in Release 4.4.

4.1 Known Issues in CF 4

This section describes the known issues that are included in Release 4.4, CF 4.

4.1.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1440	When performing a rolling upgrade (from 4.0.5 to 4.4) on IBM servers, and the OS upgrade process takes more than ten minutes, the upgrade may fail in phase 1 (OS goal) due to a timeout.	

4.1.2 Monitoring

ID	Description	Related ID in Previous Releases
CPF-14649	When log level is set to INFO, Timeout Worker license performance messages are frequently (every minute) generated in the CPF logs.	

4.2 Known Issues in CF 3

This section describes the known issues that are included in Release 4.4, CF 3.

4.2.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1467	Running the OS upgrade validation option from the F5 Traffix Menu generates an error message about the wrong menu version. This does not impact system performance.	

ID	Description	Related ID in Previous Releases
Installer-1473	After completing an ISSU, the Tomcat component running on the backup Installer server is not accessible. This does not impact system performance or the Web UI. *This issue was fixed in CF 4.*	
Installer-1206	After completing the second phase of the ISSU and switching the upgraded servers to online mode, there may be a delay before the “ClusterMon” and “Tripo” resources appear on the server.	
Installer-1511	When performing an upgrade (from 4.0.5 to 4.4), some resources may be marked as "failed actions" (as they are temporarily down) after Phase 2 of the upgrade. This has no impact on the overall upgrade process. Workaround: Run crm cleanup command for all failed resources.	
Installer-1512	Occasionally, after performing an ISSU, the Installer version is not upgraded as expected. Workaround: Repeat the Installer upgrade process.	

4.2.2 Topology

ID	Description	Related ID in Previous Releases
CPF-13884	Peers added locally to an SDC site that is managed by EMS disappear from the Web UI after one second, but appear in the configuration manager log files as successfully added. Workaround: 1. Add the peer a second time.	

4.2.3 Session Repository

ID	Description	Related ID in Previous Releases
CPF-13922	The SRR queue monitoring is initiated by default, even when site replication is not enabled. This does not impact system performance.	

4.2.4 Monitoring

ID	Description	Related ID in Previous Releases
CPF-13063	The alarm notifying users that the Tripo database has reached 95% of its defined capacity is not generated. This does not impact system performance.	

4.3 Known Issues in CF 2

This section describes the known issues that are included in Release 4.4, CF 2.

4.3.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1394	The `wget` RPM file may not be found on all site servers, stalling the repository upgrade goal. Workaround: 1. Verify that the `wget` RPM file is installed on all site servers by performing the following steps: a. Run the following command on each server: **rpm –qa|grep wget** b. If the `wget` RPM file is not installed, install it by running	

ID	Description	Related ID in Previous Releases
	the following command on each server: **yum install wget** *This issue was fixed in CF 3.*	
Installer-1424	Configuring Splunk in an SDC configuration file does not generate a validation error.	
Installer-1427	The ISSU does not successfully complete all the upgrade goals on the installer server. RCA: During the ISSU, the pacemaker process on the installer server is not successfully upgraded.	
CPF-13837	After upgrading an EMS site, the **Topology** > **Specific Site Settings** > **<Site Name>** > **SDC Components** > **Internal Connections** screen may display the wrong port number in some of the site CPF IP addresses.	

4.3.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-13822	Once a replication peer status is displayed as red because of timeouts, the peer status will not change until the peer is reconnected. *This issue was fixed in CF 3.*	
CPF-13880	The cpfNmsResourcesAlarm trap only appears in the SDC Web UI, and not in the Web UI of the EMS that manages the SDC site.	
CPF-13720	The collectingStatisticsClear trap does not appear in the SDC or EMS Web UI.	

4.3.3 Topology

There are no detected known issues in this category.

4.3.4 Flow Management

There are no detected known issues in this category.

4.3.5 Session Repository

ID	Description	Related ID in Previous Releases
CPF-13774	Tripo entries are not deleted from the database if the replicated Tripo site just started up and is empty. RCA: The SRR (Delete) request that is sent to the empty site does not find the key of the Tripo entry that should be deleted and therefore does not send a response. The SRR (Delete) request is then perpetuated in the request queue and the entry is not deleted from the original Tripo site. *This issue was fixed in CF 4.*	4.0.5: CPF-13773
CPF-13960	When replicating sessions between Tripo instances, if the UI_viewStorage tool is connected, some SRR (Delete) requests are not replicated between Tripo instances. *This issue was fixed in CF 4.*	4.0.5: CPF-13751

4.3.6 Performance

There are no detected known issues in this category.

4.3.7 Monitoring

ID	Description	Related ID in Previous Releases
CPF-13825	The cpfSiteReplicationTargetDown and cpfSiteReplicationTargetUp alarms are not generated.	

ID	Description	Related ID in Previous Releases
	This issue was fixed in CF 3.	
CPF-13808	The cpfNodeClientsQueueHighWatermarkAlarm is not generated. *This issue was fixed in CF 3.*	
CPF-14404	Fatal "secondary key appears as primary in the received request" error messages are generated in the Tripo log files. This does not impact system behavior. *This issue was fixed in CF 4*	4.0.5: CPF-13778

4.3.8 Maintenance

There are no detected known issues in this category.

4.3.9 Accessibility

There are no detected known issues in this category.

4.3.10 HTTP

There are no detected known issues in this category.

4.4 Known Issues in CF 1

This section describes the known issues that are included in Release 4.4, CF 1.

4.4.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1337	The snapshot created during the ISSU has limited capacity, according to the current available disk space.	
Installer-1370	When the default gateway is not defined in the site configuration file, a null pointer exception is generated.	

ID	Description	Related ID in Previous Releases
	This issue was fixed in CF 2.	
CPF-13591	During an ISSU of multiple SDC sites managed by an EMS site, when the EMS site is upgraded but the SDC sites are still running the previous SDC version, removing SDC site peers via the EMS Web UI may cause client peers to disconnect and reconnect. Workaround: When the EMS site is upgraded but the SDC sites are still running the previous SDC version, remove SDC site peers via the relevant SDC Web UI.	

4.4.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-13450	The **ACL Accepted/Rejected** statistics do not appear correctly in the SDC Web UI (**Dashboard**). RCA: The system is not configured correctly to draw the correct values for these statistics from the FEP log. *This issue was fixed in CF 2.*	

4.4.3 Topology

ID	Description	Related ID in Previous Releases
CPF-13598	SCTP channels are constantly in a high watermark state. RCA: The processWriteTaskQueue() method constantly invokes the selector.wakeup() method, erroneously resetting the list of available SCTP channels as empty and effectively blocking messages from being forwarded to one of those	

ID	Description	Related ID in Previous Releases
	channels. As a result, no messages are processed and the SCTP channels remain in a high watermark state. *This issue was fixed in CF 2.*	

4.4.4 Flow Management

There are no detected known issues in this category.

4.4.5 Session Repository

ID	Description	Related ID in Previous Releases
CPF-13542	Sending an SRR request to a disabled SDC server produces a Null Pointer Exception error in the SDC log files. *This issue was fixed in CF 2.*	

4.4.6 Performance

There are no detected known issues in this category.

4.4.7 Monitoring

ID	Description	Related ID in Previous Releases
CPF-13543	Configuring custom parameters to be added to the session life-cycle log messages (**Administration** > **Logging** > **Enable Session Logging**) fails if the attribute names contain a "." character. *This issue was fixed in CF 2.*	

4.4.8 Maintenance

ID	Description	Related ID in Previous Releases
Installer-1367	A server added to a site that has been upgraded using the ISSU, is configured with a different set of ports than the set of ports used by the existing site servers. RCA: During the ISSU, the site servers start using a secondary set of ports, while the added server is configured with the default set of ports.	
Installer-1371	When adding a new server defined only with a "FEP" role, the configuration manager also creates a folder for CPF configuration.	
Installer-1372	After adding a new server to an SDC site managed by an EMS site, information for the new server is not displayed in the **EMS** > **Monitoring** tab.	
Installer-1374	When adding a new FEP to an existing SDC site, all FEP UIDs in the sysconfig file are recalculated.	

4.4.9 Accessibility

There are no detected known issues in this category.

4.4.10 HTTP

ID	Description	Related ID in Previous Releases
CPF-13473	When HTTP server peers configured with host IP addresses taken from DNS connect with the SDC, the host IP address is resolved at the time of the first connection and then cached for all subsequent connections between the HTTP server peer and the SDC. *This issue was fixed in CF 2.*	

4.5 Known Issues in CF 0

This section describes the known issues that are included in Release 4.4, CF 0.

4.5.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-1189	During the ISSU, not all RPMs are upgraded. RPMs that are not upgraded may not behave as expected. RCA: The ISSU only upgrades a defined list of RPMs. If there are additional RPMs on the site that are not part of the defined list, or if there are RPMs with a different version, they are not upgraded. *This issue was fixed in CF 1.*	
Installer-1329	Site configuration files that are created and/or edited with IPv6 addresses are not validated by the Installation Utility. *This issue was fixed in CF 3.*	
Installer-1334	After an upgrade, the SS7 driver is not able to establish an SCTP connection with the SS7 peer. Workaround: During each phase of the ISSU, before switching the servers on, run the following commands on the servers affected in that phase: 1. #modprobe ip_conntrack_proto_sctp #echo 'modprobe ip_conntrack_proto_sctp >/dev/null 2>&1' >> /etc/sysconfig/modules/sctp.modules *This issue was fixed in CF 1.*	

4.5.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-13008	The configurable SNMP target IP address and port (**Administration** > **Specific Site Settings** > **<Site Name>** > **SNMP** > **SNMP Targets**) field does not generate a validation error when populated with an invalid value.	
CPF-13261	When configuring the Binding Key Selection parameters for a Session Binding "RESOLVE" rule, (**Routing** > **Session Management**) the Defined Keys field is only saved when it is submitted. Moving to another rule within the decision table, or to another screen, will cause the configured value to be lost.	

4.5.3 Topology

ID	Description	Related ID in Previous Releases
CPF-12625	The SDC sites do not reject Global property changes performed using the setEntityProperties WS method from an SDC site. This action should be performed on EMS sites only and avoided on SDC sites.	
CPF-12960	The values displayed for "Node Startup Time" and "Node Last Connection Time" (**Topology > Specific Site Settings > <Site Name> > SDC Components > Properties)** differ between the EMS and SDC Web UI. In addition, the value for "Node Startup Time" erroneously reflects the "Node Last Connection Time". RCA: The EMS Web UI displays the time of the last configuration synchronization between the EMS and the SDC, while the SDC Web UI displays the last time that the configuration was updated on the specific SDC component.	

4.5.4 Flow Management

There are no detected known issues in this category.

4.5.5 Session Repository

There are no detected known issues in this category.

4.5.6 Performance

There are no detected known issues in this category.

4.5.7 Monitoring

ID	Description	Related ID in Previous Releases
CPF-13058	"Vector clock conflict" error messages are generated in the EMS and SDC Configuration Manager log files after each global configuration change performed by the EMS. RCA: Both configuration managers on the site distribute configuration at the same time, resulting in this error message. This behavior does not impact system performance. *This issue was fixed in CF 3.*	
CPF-13061	customStatistics files are generated in the EMS file system, at a rate of once every minute. This file is deprecated and will be removed in future releases. This behavior does not impact system performance. *This issue was fixed in CF 2.*	
CPF-13306	Pool rate limit thresholds can only be defined on the site level. Rate limit thresholds cannot be defined per pool. *This issue was fixed in CF 1.*	
CPF-13023	The session_output.log log file rotation implementation results in log file numbering that does not reflect the timestamp. RCA:	

ID	Description	Related ID in Previous Releases
	Tripo session logging rotation works in reverse order - the log with the highest number is the most recent, except for the most current, which is session_output.log without any suffix. For example: session_output.log.0 - Time-5 ("time minus 5") session_output.log.1 - Time-4 session_output.log.2 - Time-3 session_output.log.3 - Time-2 session_output.log.4 - Time-1 session_output.log - current When Tripo reaches the maximum number of rotation files to keep, it continues the rotation from the oldest file (session_output.log.0). This can result in old log files with a high number that are not deleted, while more recent log files, with a lower number, are deleted.	

4.5.8 Administration

There are no detected known issues in this category.

4.5.9 Accessibility

The accessibility feature has the following known issues:

- When the accessibility feature is enabled, the mouse cannot always be used to navigate between screens and tabs within the Web UI.
- When editing a specific grid in a table (i.e. **Topology** > **Remote Peers**), the focus (blue box showing accessibility) sometimes moves from the selected grid, and several TAB entries are required to return the focus back to the selected grid.

- Following auto-refresh, the focus (blue box showing accessibility) on a specific table row disappears intermittently and several TAB entries are required to return the focus back to the specific row.
- When navigating within a window (i.e. Add Server Peer), the focus (blue box showing accessibility) sometime moves out of the window, and several Tab entries are required to return the focus back to the opened window.
- The EMS **Dashboard** is not accessible when the accessibility feature is enabled.
- In the **Reports** tab, several reports cannot be selected.
- In the **Reports** tab, the filters and **Time Resolution** options can only be selected using the arrow keys and not the TAB key as is done in the other Web UI screens.
- In the **Reports** tab, the **Chart type** option cannot be changed.
- Prior to disabling the accessibility feature, the user must first refresh (F5) the Web UI.

5. Limitations

This section describes the limitations that are included in Release 4.4.

5.1 Installation and Upgrade

ID	Description
CPF-12752	During an ISSU upgrade of an EMS site, after phase 2, when the upgraded servers are started, the “traffix_splunk-app-app-prim:0” resource on the upgraded servers may not start. RCA: Splunk may need to generate SSL keys. The SSL key generation takes time, and during this time the Splunk resource is down. Workaround: Clean the Splunk resource, or wait approximately ten minutes and the cluster will clean it automatically and it will start. To clean the resource, run the following command: 1. crm resource cleanup traffix_splunk-app-app-prim:0
CPF-13324	After an EMS site is upgraded, the client peers connected to the SDC site(s) it manages may not appear in the EMS Web UI (**Topology** > **Specific Site Settings** > **Site Name** > **Remote Peers** > **Client Peers**). Workaround: 1. On the local SDC site, submit a minor configuration change.
CPF-13803	The FEP component fails to switch over to the second server group during phase1 of the ISSU. The Active / Standby resources must be manually migrated (if needed) from the servers in the first server group (the servers that are upgraded are part of phase 1) to the servers in the second server group (the server that are upgraded are part of phase 3). For more information, see the F5 SDC Upgrade Guide.

5.2 Web UI

ID	Description
CPF-8118	To achieve EMS high availability, the EMS site must contain at least three machines, where each machine contains the following software modules: ▪ Splunk Indexer ▪ Splunk Master ▪ Splunk Search Head RCA: When the Splunk Master is initialized, it searches the EMS site machines for active Splunk Indexer instances. Once an active Splunk Indexer instance is identified, the Splunk Master registers its information. The Splunk Master then updates the Splunk Search Head with this information. The Splunk Search Head only enables data querying once the Splunk Master has information about at least two active Splunk Indexer instances.
CPF-6161	The EMS Web UI displays data as expected when up to four concurrent sessions are open.
CPF-12680	When accessing the SDC and EMS Web UI using the Firefox version 36 Web Browser, the Web UI screens do not correctly refresh and display their screen data.
CPF-7607	The severity icon is not displayed for the “pacemakerNotification” SNMP trap in the **Monitoring** > **Trap Viewer** screen.
CPF-13210	The Local Breakout APN/PLMN lists that are configured for Diameter and SS7 peers are not imported and exported as expected if the lists contain the ‘+’ symbol. If the lists contain this symbol, it is replaced during the import and export with a space.

5.3 Topology

ID	Description
CPF-9044	SDC enforces by default rate limit towards each remote server peer of 30,000 TPS, even if the rate limit is marked as not to be enforced. The user should define a higher limit when needed.
CPF-10383	Disabled dynamic client peers may reconnect to the SDC. RCA:

ID	Description
	Disconnecting a remote peer from the SDC (**Topology > Specific Site Settings > Site Name > Remote Peers > Client Peers** >**Administrative State>Disabled**) is not a permanent change. Whenever the FEP is restarted on a different site server (for example, after a failover), the **Administrative State** is reset as **Enabled**, and the remote peer remains connected to the SDC. Workaround: To permanently disconnect a remote peer from the SDC, configure the **Access Control List** to reject the remote peer.
CPF-11341	The Traffic Class parameter definition does not have any effect on the system.
CPF-11477	HTTP client peers always appear in the Web UI (**Topology** > **Specific Site Settings** > **<Site Name>** > **Remote Peers** > **Client Peers)** with an "Open" status Workaround: To close an HTTP client peer: 1. Go to **Topology** > **Specific Site Settings** > **<Site Name>** > **Remote Peers** > **Client Peers**. 1. Locate the HTTP peer and click **Disable**. 2. Click **Submit**.
CPF-11543	Once a remote peer is connected to the SDC and defined as a client peer, its definition cannot be modified to be identified a server peer. To change how the SDC views a remote peer, delete the peer from the SDC, adjust the association rules, and reconnect the peer as a server peer.
CPF-12518	A CPF instance must handle traffic client-initiated requests from a dynamic client peer before it can forward server-initiated requests to that same dynamic client peer. RCA: When Dynamic client peers connect to an SDC site, they connect to the site FEPs, and not to the CPF instances on the site. A CPF instance only recognizes a dynamic client peer after the client peer initiates requests that the FEP forwards to the CPF. Only at this stage does the CPF receive the dynamic client peer information from the FEP and connect to it. As a result, if a server-initiated request is processed by a CPF instance before this stage, the CPF instance will not yet have received the dynamic

ID	Description
	client peer information from the FEP, will not recognize it, and will not be able to route traffic towards it.
CPF-12857	When an EMS site manages a local SDC site, and the SDC site is restarted, the dynamic client peer tables in the EMS and SDC Web UI (**Topology** > **Specific Site Settings** > **<Site Name>** > **Remote Peers > Client Peers**) will not display the same list of client peers. RCA: Once a client peer is dynamically added to an SDC site, its information is sent to the EMS site, and both the SDC and EMS Web UI (**Topology** > **Specific Site Settings** > **<Site Name>** > **Remote Peers > Client Peers**) display the same list of client peers. When the SDC site is restarted, it does not save the dynamic client peer, and therefore does not display it in the list of client peers. The EMS site, however, retains the dynamic client peer information, and continues to display its information in the list of client peers.
CPF-6482	The web browser gets stuck upon login to the Web UI of the SDC when trying to display a large number of Routing Table statistics graphs. Workaround: Filter the graphs displayed in the SDC Dashboard to not display Decision Table statistics: 1. Go to **SDC Dashboard** > **Settings** > **Statistics Groups**. 1. Clear the **Decision Tables** checkbox. 2. Click **OK**.
CPF-7160	After clearing any Boolean TCP parameter, resetting the value does not reload the parameter's default value.
CPF-12626	The timeout value configured for an SS7 peer, configured in milliseconds, is not enforced as the configured value. Instead, it is enforced in seconds. RCA: The SS7 driver timeout is defined in seconds, and not milliseconds, like the SDC timeout. The SS7 driver timeout is calculated by taking the defined timeout for the SS7 peer, dividing it by 1000, and using the integer value of the result.

5.4 Flow Management

ID	Description
CPF-11678, 9021	If the dictionary contains multiple messages with the same Command_Code, but different Application_IDs, the SDC will use the last appearance of the command in the Groovy scripts. As a result, when using the following function in the Groovy script: def outgoingRequest = session.createRequest(Message msg) the Application_ID in the created request will be the last one defined in the dictionary with same Command_Code, and not necessarily the same as the application ID which is in the msg the user clones. Workaround: When using "super dictionary" in the SDC, add the following method in the groovy script after creating the outgoingRequest with the desired application id value : outgoingRequest.setProperty("APPLICATION_ID", xxx)
CPF-12721	When a Diameter request does not match any rule in the Routing decision table (Routing > Routing), the request does not return a “cannot route” answer and timeouts occur. RCA: In the Routing decision table (**Routing** > **Routing**), requests that do not match any rule cannot invoke one of the rule-related scripts. Therefore, the SDC cannot locally create the expected “cannot route” answer, and the request times out.
CPF-6072	The CPF may fail if an invalid script is used in External Lookup Management.
CPF-12271	In the flowManager API, the “addcolumn” method cannot define a column named “Enabled”. RCA: By default, each Decision Table contains a rule attribute column named “Enabled”, with a Boolean value reflecting the desired value for each rule.

5.5 Session Repository

ID	Description
CPF-5757	After an instance has recovered from a failover, the session entries are retained in the instance database longer than the configured session timeout, decreasing the system’s capacity to maintain new sessions.

ID	Description
CPF-6008,5972	When the connection between the Tripo instances is down, the Tripo instance will try backing up data to the other Tripo instance before checking and working with the defined session timeout. Session release will therefore be delayed 21 seconds longer than the defined session timeout.
CPF-6879	Session data size is limited to 1k bytes. The user cannot save larger amounts of data over the session cookie.
CPF-13012	When sessions are replicated between SDC sites and one of the Tripo instances is restarted before it replicates the sessions to its mated site, those sessions will not be replicated to the mated site.
CPF-13089	When sessions are replicated between SDC sites, if one of the Tripo instances running on the mated site is restarted before the Tripo instances on the mated sites are synchronized, some sessions may be lost and not stored on either Tripo instance in the mated site.
CPF-8676	By default, the onSessionRelease script can only refer to the Session ID for released sessions. Once the onSessionRelease script is modified, additional session data may be referred to. This additional session data can only be accessed for sessions that are added to the Tripo after the script was modified.

5.6 Performance

ID	Description
CPF-7871	The configuration files are not deleted, causing an excessive number of configuration files in the data folder.

5.7 Monitoring

ID	Description
CPF-7180	The health visual indication can be displayed wrongly when the peer is defined in more than one pool. The “Load based policy” Load balancing policy should not be selected for pools with a peer that is defined in multiple pools.

ID	Description
CPF-12002	Once a CPF instance on an SDC site shuts down or restarts, all site components displayed in the **Topology** screens are displayed as "disconnected" for approximately a minute and a half. The site components then return to being displayed correctly. RCA: The **Topology** screen polling timers are affected by the CPF shutdown, causing the site components to be displayed as disconnected.
CPF-12592	When a FEP is shutting down, any attempts that it makes to connect to one of its configured CPFs results in an "org.jboss.netty.channel.ChannelException: java.net.SocketException: Bad file descriptor" in the FEP logs.
CPF-12738	The "cpfLicenseAboutToExpire" SNMP alarm does not generate an alarm if the license is installed with an expiration date of the day it is installed.
CPF-12959	The EMS Monitoring screens do not display information for hosts and servers in SDC sites that are offline. RCA: The monitoring page evaluates every site/host/services dynamically, based on events generated from each site (each site's nmsagent is responsible for sending the relevant site/host/services events). When a site is down, no events related to its host/services are available in the EMS. The EMS therefore marks the site as down, and does not show any information related to the site hosts or services.
CPF-13093	The SDC Dashboard includes certain irrelevant graphs. The "Request Flow Overall Handle Time" is reported by the FEP-O (the last SDC component that processes the request before it is sent to the peer), and therefore this graph is irrelevant in the FEP-I screen. The "Answer Flow Overall Handle Time" is reported by the FEP-I (the last SDC component that processes the answer before it is sent to the peer), and therefore this graph is irrelevant in the FEP-O screen.
CPF-5793	Errors may appear in the CPF log file after a CPF shutdown.
CPF-7532	The Corosync on EMS sites attempts to activate the CPF upon startup, even though it is not configured to run on the EMS site.

ID	Description
CPF-7698	The CPF host name is displayed instead of CPF host IP when the traced message is initiated or targeted by the CPF.
CPF-13051	Sending a WS API request with an invalid site ID does not generate the expected error and error code. Instead of a specific error, stating that the site doesn't exist, a general error code is generated.
CPF-13106	After the Tripo is restarted, the session_output file contains broken entries (for example, entries that are missing their timestamp).
CPF-13269	The timestamp format that appears in the "All AVP-Level Messages of Selected Message Session report in the Reports > Traced Messages is different than the timestamp format of the other reports in the screen. While the other reports appear with a timestamp in the 24-hour clock format, this report appears with a timestamp in the 12-hour clock format.

5.8 Administration

ID	Description
CPF-12838	When enabling/disabling a peer using the modifyPeer WS method, two audit actions appear in the Web UI (**Administration** > **Audit**) for each performed action. One audit line states that the remote peer was edited, and the other audit line states that the remote peer was enabled/disabled.

5.9 RADIUS

ID	Description
CPF-12991	EMS sites that manage SDC sites that process RADIUS traffic cannot be upgraded. RCA: After upgrading the EMS site, and loading the RADIUS dictionary using the EMS Web UI (Routing > Data Dictionary), the dictionary is not distributed to the connected SDC sites and error messages describing the distribution failure appear in the SDC site configuration managers.
CPF-12577	When the CoA (Disconnect request) port is not configured in RADIUS peer profiles, the default port used by the RADIUS peer is 1812, and not 3799 as expected.

ID	Description
	RCA: The default value is not the expected value. Workaround: When configuring RADIUS peers, verify that the CoA port is configured in the RADIUS peer profile.
CPF-12607	Even when the FEP IP that a RADIUS virtual server communicates with is not licensed, the virtual server appears in the Web UI (**Topology** > **Specific Site Settings** > **<Site Name>** > **Virtual Servers**) with an "Open" status, until traffic is attempted to be passed and fails. RCA: FEP licensing is enforced only when attempts to pass traffic start and the connection establishment attempt fails. Before attempting to pass traffic, the FEP IP successfully binds itself to the virtual server. The FEP does not need a license for the bind to be successful, and therefore results in the "Open" status.
CPF-12608	When a RADIUS virtual server is created before the FEP IP it communicates with is licensed, the RADIUS virtual server will not listen on the port once the license is installed. Workaround: After the FEP IP is successfully licensed: 1. Go to **Topology** > **Specific Site Settings** > **<Site Name>** > **Virtual Servers**. 2. Select the row in the table with the desired RADIUS virtual server. 3. Click Disable. 4. Click Enable.
CPF-12609	A RADIUS virtual server that is successfully processing traffic will continue to process traffic even after the license installed on the FEP IP that it communicates with is removed.

Glossary

The following table lists the terms and abbreviations used in this document.

Table 2: Terms and Abbreviations

Term	Definition
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Application Function
Answer	A message sent from one Client/Server Peer to the other following a request message
API	Application Programming Interface
AVP	Attribute Value Pair
CLI	Command Line Interface
Client Peer	A physical or virtual addressable entity which consumes AAA services
CPF	Control Plane Function
Data Dictionary	Defines the format of a protocol's message and its validation parameters: structure, number of fields, data format, etc.
DEA	Diameter Edge Agent
Destination Peer	The Client/Server peer to which the message is sent
DRA	Diameter Routing Agent
EMS Site	Element Management System Site
FEP-In	In-Front End Proxy
FEP-Out	Out-Front End Proxy

Term	Definition
Geo Redundancy	A mode of operation in which more than one geographical location is used in case one site fails
HA	High Availability
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IMS	IP Multimedia Subsystem
JMS	Java Message Service
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
Master Session	The session for which the routing selection is performed based on the routing rules (Slave Sessions are applied with routing rules inherited from the Master Session)
MME	Mobility Management Entity
NGN	Next Generation Networking
Node	Physical or virtual addressable entity
OAM	Operation, Administration and Maintenance
OCS	Online Charging System
Origin Peer	The peer from which the message is received
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PLMN	Public Land Mobile Network
Pool	A group of Server Peers
RADIUS	Remote Authentication Dial In User Service

Term	Definition
Request	A message sent from one Client/Server peer to the other, followed by an answer message
SCCP	Signaling Connection Control Part
SCTP	Stream Control Transmission Protocol
SDC	Signaling Delivery Controller
SDC Site	The entire list of entities working in a single site
Server Peer	A physical or virtual addressable entity which provides AAA services
Session	An interactive information interchange between entities
Slave (Bound) Session	A session which inherits properties from a master session
SNMP	Simple Network Management Protocol
SS7	Signaling System No. 7
TCP	Transmission Control Protocol
TLS	Transport Layer Security
Transaction	A request message followed by an answer message
Tripo	Session data repository
UDP	User Datagram Protocol
UE	User Equipment
URI	Universal Resource Identification.
Virtual Server	A binding point used by SDC to communicate with the Remote Peers (Clients and Servers)
VPLMN	Visited Public Land Mobile Network
Web UI	Web User Interface
WS	Web Service

