Signaling Delivery Controller

Release Notes

5.1 CF 36

Catalog Number: RG-022-51-3 Ver. 1

Publication Date: October 2022

Legal Information

Copyright

F5, 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, OpenBloX, OpenBloX (design), Rosetta Diameter Gateway, Signaling Delivery Controller, SDC, Traffix, and Traffix [DESIGN] are trademarks or service marks of F5, 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. The information in this document may be changed at any time without notice.

About F5

F5 (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-022-51-3 Ver. 1

Publication Date: October 2022

Document Objectives

This document provides information about the features introduced, known issues, and limitations included in the F5 SDC 5.1 release.

Document History

Revision Number	Change Description	Change Location

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

Convention	Use
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: s alt-srv5.1_35-1.noarch.rpm
- SDC Software: sdc5.1_35_1-5.1_35-1.x86_64.rpm
- Tripo: Tripo-1.5.0-201.x86_64.rpm
- File Server: FileServer-1.0.0-41.x86_64.rpm

1.2 ISO Image Information (Bare Metal Installations)

The F5 SDC software for bare metal installations is packaged and supplied as an ISO image.

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

- Filename: iso-5.1_35-1.iso
- MD5: 0e1ce198b4cf1e34066bc76e4fd83624
- Date: Mar 22, 2022 11:54:34 AM
- Size: 2,032,666,624 bytes

1.3 QCOW2 Image Information (OpenStack Virtual Installations)

The F5 SDC software for virtual OpenStack installations is packaged and supplied as two QCOW images – master and minion.

The following information describes the two QCOW images provided to install this release:

- Filename: master-5.1_35-1.qcow2
  - MD5: b5386acefdc408031002494c8c5b6b66
  - Date: Mar 22, 2022 12:01:42 PM

- Size: 3,099,525,120 bytes

- Filename: minion-5.1_35-1.qcow2
  - MD5: f2b94e3df2a7883b3d1868a1ed105323
  - Date: Mar 22, 2022 12:00:22 PM
  - Size: 1,365,901,312 bytes

1.4 Upgrading to This Release

Virtual deployments of SDC 5.1 support upgrades from earlier release builds. Virtual deployments of SDC 5.1 cannot be upgraded from previous SDC releases.

Bare metal deployments of SDC 5.1 support the following upgrade paths:

- Upgrade from an earlier SDC 5.1 build

Note: When you are doing a rolling upgrade to CF-25, you need to follow the upgrade procedure to support openJDK in the *SDC 5.1 Upgrade Guide (see section 4.1.4)*.

1.5 Supported Browsers

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

- Internet Explorer: 1836.1316
- Edge version: Version 88.0.705.56 (Official build) (64-bit)
- Mozilla Firefox 85.0.
- Google Chrome 88.0.4324.104 (Official Build) (64-bit)

1.6 Supported Operating Systems

OpenStack Virtual deployments of SDC 5.1 are certified to run on the following operating system:

- Red Hat Enterprise Linux (RHEL) 8.2 64 bit over OpenStack Platform 16.1

Bare Metal deployments of SDC 5.1 are certified to run on the following operating system:

- Red Hat Enterprise Linux (RHEL) 6.10 64 bit

1.7 Java Version

SDC supports OpenJDK 64-Bit Server VM 1.8.0_265-b01. See the upgrade procedure to support openJDK in the *SDC 5.1 Upgrade Guide* (section 4.1.4).

1.8 Tomcat Version

The supported Tomcat version is 8.5.75.

1.9 ELK Component Versions

The current supported packages and versions are:

- Elastic search: elasticsearch.x86_64 7.8.0-1
- Kibana: kibana.x86_64 7.8.0-1
- Fluent: td-agent.x86_64 3.8.0

1.10 Supported Firmware Versions

The following firmware is certified to run with HP C7000:

Firmware Type	Version
OA - BladeSystem c7000 DDR2	4.95(6 Nov 2019)

The following firmware is certified to run with BL Gen8:

Firmware Type	Version
HP FlexFabric 10Gb 2-port 534M Adapter	7.15.97
HP Flex-10 10Gb 2-port 530FLB Adapter	7.15.37
iLO	iLO 2.78 Apr 28 2021
Server Platform Services (SPS) Firmware	2.1.5.2B.4
Smart Array P420i Controller	8.32 Embedded
System ROM	I31 05/24/2019

The following firmware is certified to run with BL Gen9:

Firmware Type	Version
HP FlexFabric 10Gb 2-port 536FLB Adapter	7.18.82
HP FlexFabric 20Gb 2-port 630M Adapter	7.14.79
iLO4	2.78 Apr 28 2021
Server Platform Services (SPS) Firmware	3.0.6.267.4
Smart Array P244br Controller	7.00
System ROM	2.80

The following firmware is certified to run with BL Gen10:

Firmware Type	Version
HP Ethernet 10Gb 2-port 560M Adapter	1.2121.0
HP FlexFabric 10Gb 2-port 536FLB adapter	7.15.97
iLO5	2.44 Apr 30 2021
Server Platform Services (SPS) Firmware	04.01.04.423
HPE Smart Array P204i-b SR Gen10	3.53
System ROM	141 v2.32 (03/09/2020)

The following firmware is certified to run with DL Gen8:

Firmware Type	Version
HP Ethernet 1 Gb 4- port 331FLR Adapter	20.16.31 Embedded
HP Ethernet 1 Gb 4- port 331T Adapter	20.16.31 Slot 1
iLO	iLO 2.78 Apr 28 2021
Server Platform Services (SPS) Firmware	2.1.7.E7.4
Smart Array P420i Controller	8.32 Embedded
System ROM	P70 05/24/2019

The following firmware is certified to run with DL Gen9:

Firmware Type	Version
HP Ethernet 1 Gb 4- port 331FLR Adapter	20.18.31 Embedded
HP Ethernet 1 Gb 4- port 331i Adapter-NIC	20.16.31 Embedded
iLO	iLO 2.78 Apr 28 2021
Server Platform Services (SPS) Firmware	3.0.6.267.1
Smart Array P440ar Controller	7.70 Embedded
System ROM	P89 v2.80(10/16/2020)

The following firmware is certified to run with DL Gen10:

Firmware Type	Version
HP Ethernet 1 Gb 4- port 331FLR Adapter	20.18.31
HP Ethernet 1 Gb 4- port 331T Adapter	20.18.31
HP Ethernet 1 Gb 4- port 331i Adapter-NIC	20.18.31
HPE Smart Array P408i-a SR Gen10	3.53
iLO 5	2.44 May 7 2021
Server Platform Services (SPS) Firmware	04.01.04.423
System ROM	U30 2.42 (01/23/2021)

2. What's New in This Release?

This section describes the changes implemented in the F5® Traffix® Signaling Delivery Controller™ (SDC) 5.1 release.

2.1 Installation and Deployment Options

2.1.1 VMWare Support

SDC 5.1 expands the SDC cloud capabilities to support VMWare-based customer clouds. The customer cloud support provided for VMWare is similar to the existing support for OpenStack, and does not support orchestration integration. In addition, the VMWare virtual platform, like OpenStack, only supports SDC sites. EMS sites are not currently supported on the virtual platforms.

2.1.2 Small Scale Bare Metal Deployment Support

SDC 5.1 bare metal deployments can be installed using a minimum of two servers, running all SDC components over the two servers in A/A mode.

As in previous releases, a Virtual IP (VIP) for the FEP components is provided using the keepaliveD daemon. This requires additional memory for existing deployments currently running with 32GB of memory.

2.2 New Functionality

2.2.1 Session Lookup

The Session Lookup functionality, introduced in SDC 5.1, provides the ability to process incoming messages based on attributes contained in previously processed sessions. This functionality does not bind the two sessions, rather allowing each session to have a separate lifecycle and be routed according to separate routing decisions.

2.3 Administration and Configuration Improvements

2.3.1 UI Accessibility

SDC 5.1 includes UI accessibility (according to WCAG 2.0 standard), covering keyboard navigation and color contrast, provided over the AngularJS framework (powered by Google, MIT license).

2.3.2 Topology Editor

The Topology Editor, included in the SDC 5.1 release, is a standalone utility that is used to create and modify the site topology .xml files.

2.3.3 Reporting Engine Replacement

The reporting engine used in previous SDC releases – Splunk – is largely replaced in SDC 5.1 by GUI based reporting engine running over Cassandra DB. All collected KPIs and state information are saved in Cassandra, and synchronized between SDC sites and the EMS site.

TDRs (Transaction Data Records) and Administrative Tracing information (collected by specific condition definition by the user per specific transaction(s)) remain in Splunk.

Current EMS capabilities and limitations remain the same as previous versions.

2.3.4 Overload Protection Improvements

SDC 5.1 improves the server overload protection provided by the SDC. The state of each server is constantly monitored by a series of KPIs. Once a server is detected as overloaded, traffic sent to the server is prioritized until the overloaded state is cleared.

2.3.5 SNMP Security Enhancements

From Release 5.1 CF 9, SNMPv3 is supported, in addition to SNMP V2c (and SNMP V1), for retrieving MIB file information. SNMPv3 provides enhanced user security protection for internal users (between the NMS Agent and SDC components) and for external users (between the NMS Agent and an external SNMP applications). In addition, an SNMP V2

Trap Forwarding profile, is supported for sending alarms to an external SNMP application, with a configurable community (security name).

The enhanced security protections are configured per the different internal and external profiles, as described in the *5.1 SDC User Guide* and video documentation.

2.3.6 Network License Mechanism

Release 5.1 CF 10 introduces a network license mechanism. Previously, the SDC supported having a separate license per each IP address for a configured FEP. Now, in addition, the SDC supports having a network of licenses for multiple IP addresses for a configured FEP, based on a defined NetMask. For more information, refer to the *5.1 SDC User Guide*.

2.3.7 Supported Protocols Improvements

2.3.8 SS7 and IWF stability

The SDC infrastructure for SS7 support is split in SDC 5.1 to two modules to support both the SS7 (LB and router) functionality and the IWF (Diameter – SS7 transformation) functionality.

2.3.9 Global Title Routing

Global Title routing support, added in SDC 5.1, enables making routing decisions based on internal characteristics of the SS7 message.

2.3.10 Wi-Fi Offloading

SDC 5.1 extends the existing WiFi offloading functionality, providing EAP-SIM authentication data caching. In SDC 5.1, the SDC caches the subscriber's authentication vectors that were received from the HLR and reuses them in case the same subscriber sends another authentication request. The extended support reduces traffic toward the HLR.

Wi-Fi Offloading functionality requires specific license.

2.4 Enhancements

2.4.1 Enhancements in CF 30

For EMS deployments, Splunk is now replaced with ELK. There are three ELK components on the EMS (Fluentd, Elasticsearch and Kibana) and one component on the SDC (Fluentd Forwarder). These components receive and forward information to create an overview of the deployment's performance and support shared configuration across multiple sites (SDC-44).

2.4.2 Enhancements in CF 28

SDC now supports a non-standard RADIUS dictionary message header format, allowing users to configure the format type. To configure format types, refer to the *F5 SDC 5.1 User Guide, section 4.1*. (SDC-40)

2.5 Security Updates

2.5.1 Security Updates in CF 36

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin June 1, 2022 – October 1, 2022* (SDC-2066).

- Apache Tomcat vulnerabilities (CVE-2022-25762; CVE-2022-34305) are fixed and the Tomcat version is updated to 8.5.82.
- Linux kernel vulnerabilities (CVE-2022-0492; CVE-2021-27364; CVE-2021-22543) are fixed and Kernel version is updated to 2.6.32-754.48.1.
- OpenSSL vulnerabilities (CVE-2022-0778) is fixed and OpenSSL is updated to 1.0.1e-60.

2.5.2 Security Updates in CF 35

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin November 1, 2021– Jan 31, 2022* (SDC-1739).

- Apache Tomcat vulnerabilities (CVE-2022-23181; CVE-2020-9484) are fixed and the Tomcat version is updated to 8.5.75 (SDC-1737).

2.5.3 Security Updates in CF 34

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin August 1, 2021– October 31, 2021* (SDC-1390).

2.5.4 Security Updates in CF 33

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin May 1, 2021 – Jul 31, 2021* (SDC-1203).

- Apache Tomcat vulnerabilities (CVE-2021-33037; CVE-2021-30639; CVE-2021-30640) are fixed and the Tomcat version is updated to 8.5.69 (SDC-1291).
- An Apache Cassandra vulnerability (CVE-2021-13946) is fixed and the Cassandra version is updated to 2.2.19 (SDC- 1201).
- An Eclipse Jetty Vulnerability (CVE-2021-28165) is fixed and the Jetty version is updated to 9.4.39.v20210325 (SDC-1306)

2.5.5 Security Updates in CF 32

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin Feb 1, 2021 – April 30 2021* (SDC-1072).

- An Apache Tomcat vulnerability (CVE-2021-25122) is fixed and the Tomcat version is updated to 8.5.65 (SDC-1029).
- An Apache Tomcat vulnerability (CVE-2021-25329) is fixed and the Tomcat version is updated to 8.5.65 (SDC-1030).

2.5.6 Security Updates in CF 31

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin Aug 1,2020 - Jan 31. 2021* (SDC-781).

- Eclipse Jetty Vulnerabilities (CVE-2019-10241, CVE-2019-10247, CVE-2017-7656, CVE-2017-7657, CVE-2017-7658, CVE-2018-12536 are fixed (CPF-25219).
- A jackson-databind vulnerability (CVE-2020-8840) is fixed (SDC-658).
- A sudo vulnerability (CVE-2021-3156) is fixed and the sudo version is updated to sudo-1.8.6p3-29.el6_10.4.src.rpm (SDC-742).
- An Apache Tomcat vulnerability (CVE-2020-17527) is fixed and the Tomcat version is updated to 8.5.60 (SDC-660).
- When querying the salt-api on port 8000, the cherryPy server version information np longer appears in the response thereby removing a potential security threat (SDC-722).

2.5.7 Security Updates in CF 30

This CF does not include any security bulletin updates.

2.5.8 Security Updates in CF 29

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin March 2020 – July 2020* (CPF-25217).

Due to security alert CVE-2020-13935, the Tomcat version is upgraded to version 8.5.58-33 (CPF-25207)

Due to security alerts, the Java version is upgraded to JDK 1.8.0_265-b01.

2.5.9 Security Updates in CF 28

This CF does not include any security bulletin updates.

2.5.10 Security Updates in CF 27

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin December 2019 – February 2020* (Installer-3099).

2.5.11 Security Updates in CF 26

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin July 2019 - November 2019* (Installer-3098).

2.5.12 Security Updates in CF 25

This CF does not include any security bulletin updates.

2.5.13 Security Updates in CF 24

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin January 2019 - June 2019* (Installer-3096).

2.5.14 Security Updates in CF 23

This CF does not include any security bulletin updates.

2.5.15 Security Updates in CF 22

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin August 2018 - December 2018* (Installer-3095).

Due to security alerts (CVE-2018-3136, CVE-2018-3139, CVE-2018-3149, CVE-2018-3169, CVE-2018-3180) the Java version is upgraded to JDK 1.8.0_202 (CPF-25011).

2.5.16 Security Updates in CF 21

This CF does not include any security bulletin updates.

2.5.17 Security Updates in CF 20

Due to security alert CVE- 2018-11784, the Tomcat version is upgraded to version 8.5.34-31 (CPF-25000)

2.5.18 Security Updates in CF 19

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin May 2018 - July 2018* (Installer-3091).

2.5.19 Security Updates in CF 18

This CF does not include any security bulletin updates.

2.5.20 Security Updates in CF 17

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin January 2018 -April 2018* (Installer-3087).

2.5.21 Security Updates in CF 16

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin October 2017-January 2018* (Installer-3066).

Due to an RPM update (CVE-2017-12542), the iLo4 Firmware version was updated to 2.55 (CPF-24796).

2.5.22 Security Updates in CF 15

This CF does not include any security bulletin updates.

2.5.23 Security Updates in CF 14

This CF does not include any security bulletin updates.

2.5.24 Security Updates in CF 13

This CF does not include any security bulletin updates.

2.5.25 Security Updates in CF 12

This CF does not include any security bulletin updates.

2.5.26 Security Updates in CF 11

The installed RPMs included in this release were updated, based on the RPM updates approved in the *F5 SDC Security and Update Bulletin May 2017-September 2017* (Installer-3031).

Due to security alert CVE- 2017-7674, the Tomcat version is upgraded to version 8.0.46 (CPF-24579)

2.5.27 Security Updates in CF 10

This CF does not include any security bulletin updates.

2.5.28 Security Updates in CF 9

This CF does not include any security bulletin updates.

2.5.29 Security Updates in CF 8

This CF does not include any security bulletin updates.

2.5.30 Security Updates in CF 7

Due to security alert CVE- 2017-5648, the Tomcat version is upgraded to version 8.0.44 (Installer-2948)

2.5.31 Security Updates in CF 6

This CF does not include any security bulletin updates.

2.5.32 Security Updates in CF 5

This CF does not include any security bulletin updates.

2.5.33 Security Updates in CF 4

The F5 SDC Security and Update Bulletin January 2016-February 2017 document is updated with an upgrade procedure (Installer-2949).

2.5.34 Security Updates in CF 3

The installed RPMs included in this release were updated, based on the RPM updates approved in the F5 SDC Security and Update Bulletin January 2016-February 2017 document (CPF-23092).

2.5.35 Security Updates in CF 2

Due to security alert CVE-2016-8735, the Tomcat version is upgraded to version 8.0.39 (Installer-2832).

2.5.36 Security Updates in CF 1

This CF does not include any security bulletin updates.

3. Fixed Bugs

This section describes the bug fixes that are included in Release 5.1.

3.1 Fixed Bugs in CF 36

ID	Description	Related ID
SDC-1975	Config Manager certificate is updated and new expiration is November 13th 2030.	
SDC-1987	Previously, cassandraRepairKeySpaces.py may skip repair due to the below warning: WARNING - Cassandra nodes already runs Compactation on keyspace Now, issue is solved.	
SDC-1905 (SDC-1900)	Previously, multiconnect client peers may appear on WebUI with wrong IP after reconnecting the peers in a different order. Now, IP in WebUI is updated correctly.	
SDC-1950 (SDC-1900)	Previously, client peers may appear on WebUI with source port after reconnecting (using different source port) with wrong source port. Now, source port in WebUI is updated correctly.	
SDC-2000	Previously, Rolling Upgrade may fail on upgradeOamDB stage due to disconnection between Salt master and Salt minion. Now, if fails on 3 attempts the installation will stop.	
SDC-2080	Previously, catalina.out and localhost_access_log.log were enabled but were not managed by Logrotate. This can lead to a high disk space usage. Now, catalina.out and localhost_access_log.log to Logrotate.	

3.2 Fixed Bugs in CF 35

ID	Description	Related ID
SDC-1633	During rolling upgrade, tomcat upgrade was failing. Code was fixed and the issue no longer occurs.	
CPF-25175	Previously, message buffers with null values caused an OutOfDirectMemoryError exception. Now, the code was modified so that message buffers with null values will be ignored and no longer cause OutOfDirectMemoryError exceptions.	
SDC-2003	Previously, when CM was running Jetty version 9.4.39, The EMS <> SDC sync may fail with the below Jetty exception: "[SslConnection$DecryptedEndPoint.handleException()] javax.net.ssl.SSLHandshakeException: Encrypted buffer max length exceeded" * Jetty DEBUG level must be set in order to see the above Now, CM is running Jetty version 9.4.41 and EMS <> SDC sync is working as expected.	

3.3 Fixed Bugs in CF 34

ID	Description	Related ID
SDC-1391	Previously, in a multi-site setting, a session may have expired prematurely when the Tripo reset the session timeout timer using a wrong value, leading to CCR-U requests failures. Now, the timer mechanism is improved so that the original session timeout timer resets correctly upon each GET for session updates, such as CCR-U/RAR requests.	
SDC-1400	Previously, when setting the peer profile for an existing peer, the new peer profile configuration from the parent	

ID	Description	Related ID
	- peer profile was not inherited. Now, the default creation of "DualStackEnabled=false" from DiameterConfigurationHandler.java has been removed and the inherited peer profile configuration is enabled.	

3.4 Fixed Bugs in CF 33

ID	Description	Related ID
SDC-1311	From CF 30, EMS deployments, may have experienced root partition filling up due to heavy disk usage for elastic search (ELK) data. To move the existing ELK Data location so there is no issue of heavy disk usage, run the following: mkdir /data/elk mv /opt/elk/* /data/elk and in all the ***elasticsearch.yml*** files, change the path.data from /opt/elk/* to /data/elk/* Note: This should be done while ELK is down. For more information, refer to the *F5 SDC Bare Metal Upgrade Guide*.	
SDC-1272	Following an upgrade, the **Reports >Transaction Successful Answers vs Failures** graph now shows the failure statistics as expected.	

3.5 Fixed Bugs in CF 32

ID	Description	Related ID
SDC-755	Previously, during a FEP failover, the FEP may fail to find the remote client peer IP. This may happen when the peer disconnected just before the FEP tried to get its IP. As a result, a null pointer exception will be	

ID	Description	Related ID
	generated. Because of this exception, the FEP will not proceed to change the CPFs pool state to open, and, consequently, without CPFs being available, the FEP virtual server cannot bind. The fix is to reject the client handshake when the FEP cannot bind to the remote peer IPs. Now, when there is a FEP failover, the status of the CPFs are not impacted.	

3.6 Fixed Bugs in CF 31

3.6.1 Web UI

ID	Description	Related ID
SDC-523	A version validation was added to the peerProfile WebUI, and as a result when peer Association Rules are duplicated, an exception error is generated.	
SDC-615	The **Reports** > **Transaction Summary**> **Transaction Successful Answers vs Failures** graph now displays **SDC Errors and Discards** as expected.	

3.6.2 Monitoring

ID	Description	Related ID in Previous Releases
SDC-591	Garbage Collector logs for the Tomcat process are now generated as expected to make for easier debugging of a HeapDumpOnOutOfMemoryError.	
SDC-651	Previously, when selecting (**Administration** > **Tracing**), REPORT AND LOG or REPORT AND LOG WITH HEX-DUMP logging options, the logs were not generated as expected. Now, the UDP 514 port is open (in addition to TCP 514 port) for rsyslog, and the logs are generated as expected.	

3.6.3 Flow Management

ID	Description	Related ID
SDC-374	Connecting to port 555 no longer crashes the WebStatMgr, causing Tripo to shut down.	
SDC-571	The Configuration Manager memory leak error caused by the NMS sending the CM multiple sync messages is corrected. Listeners are only created now once per-node configuration, thus allowing the maximum number of messages per second when the license key value is changed.	
SDC-578	Previously, when a server was down and a request with a 'P" flag was configured with a pre-routing transformation script (**Flows > Flows > <Flow Name> > Transformation>Pre-Routing)**, then the returned answer was without the P flag. This is now corrected, and the P flag is copied into the answer.	

3.7 Fixed Bugs in CF 30

3.7.1 Flow Management

ID	Description	Related ID
SDC-267	Previously, when sending or receiving SSL messages, there was no handling of SCTP related information and as a result, the FEP failed to send the expected message. Now, the code was modified to include SCTP related information (such as the protocol ID) for Pre Capabilities Exchange TLS, and messages are processed by the FEP as expected.	CPF- 25221

3.8 Fixed Bugs in CF 29

3.8.1 Flow Management

ID	Description	Related ID in Previous Releases
CPF-25214	A memory leak bug was detected with the third-party library (Groovy script) that the CPF uses, causing traffic outages when making changes to the attribute lists (**Administration** > **Attribute Lists**). Now, the Groovy script version has been updated to 2.4.9, and the memory leak bug is resolved.	
SDC-240	A slow HTTP header vulnerability was found in SDC 5.1 CF26. Now, as SDC using only HTTPS, HTTP security vulnerabilities are no longer an issue.	

3.8.2 Monitoring

ID	Description	Related ID in Previous Releases
SDC-117	Previously, following an upgrade from 4.4 to 5.1, the Machine Summary and Network Usage reports (**Reports** > **Resources** > **Machine Summary/Network Usage**) did not show the relevant EMS data. Now, these reports display as expected.	INSTALLER-3097; CPF-25188 (duplicate)
SDC-171	Previously, during a rolling upgrade of more than one SDC site, TTA logs displayed all site logs, which slowed down the logging performance. Now, you can configure the TTA script, with a flag (-x, -<exclude-old logs>) to ignore the logs of older SDC versions, so only logs from the most recent versions are retrieved. For more information, see the *F5 SDC Troubleshooting Guide*.	
SDC-233	Previously, a Spring Security response exception exposed all message information, including the stack trace information. Now, the exception generated returns an	

ID	Description	Related ID in Previous Releases
	HTTP 401 error, thereby eliminating possible security vulnerabilities.	
CPF-25197	Previously, when running the ./tta-ng.sh script (in CF 26) for SDC and EMS sites, an error was generated that jps files were not found. Now, the path that references the jps and jstack files has been updated, TTA collects the relevant details, and the error is no longer generated.	

3.9 Fixed Bugs in CF 28

3.9.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-25185	The firmware that is certified to run with HP C7000 Gen8 was updated, see *Supported Firmware Versions*.	

3.9.2 Performance

ID	Description	Related ID in Previous Releases
CPF-25194	Previously in release 5.1, the CPF was configured to use the G1 Collector for efficient GC and improved SDC performance. N**ow,** this has been extended to the FEP.	

3.10 Fixed Bugs in CF 27

3.10.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-25171	Previously, after performing an upgrade, some FEPs were not upgraded as expected, due to a missing keytool symlink. Now, the keytool symlink code has been fixed and FEPs are upgraded as expected.	

3.10.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-25179	Previously, when the last routing row in a decision table was queried and no site ID was available, an exception error was generated. Now, in the unlikely chance that there is no site available for the last routing row, the current site ID is applied to the last decision table row number and no exception error is generated.	

3.10.3 Administration

ID	Description	Related ID in Previous Releases
CPF-25168	When there are audit logs from different years, the Audit page (**Administration** > **Audit**) sorting on a month/day/time basis did not work as expected. Now, the timestamp code has been modified and the sorting works as expected.	

3.11 Fixed Bugs in CF 26

3.11.1 Administration

ID	Description	Related ID in Previous Releases
CPF-25121	Users can now change their password on one SDC site and it is updated on other SDC sites, as the EMS is now automatically updated with the new password and then can update all the other SDC sites, accordingly.	

3.11.2 Topology

ID	Description	Related ID in Previous Releases
CPF-25152	Previously, when configuring a pool (**Topology > Pools > Add**), the **Ramp Up Split By** field size was set to 8 characters, limiting the message property text that you could enter. Now, the field size has been increased to 64 characters.	

3.11.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-25141	Previously (since CF 16), once a message's isTracing flag was set to false, all messages sent within the current second, regardless if their isTracing flag was set to true, were not traced until the end of the current second. Now, the isTracing flag conditions are corrected so that each message's isTracing flag is individually evaluated within the current second.	CPF-24845 in CF 16
CPF-25160	Previously, the peer Round Trip Time Thresholds statistic (**Topology > Specific Site Settings > <Site Name>> Peers**) did not consistently recognize the maximum threshold for dynamic peers, causing alarms to be erroneously generated. Now, the Round Trip Time Thresholds statistic accurately recognizes maximum thresholds.	

3.12 Fixed Bugs in CF 25

There were no fixed bugs in Release 5.1, CF 25.

3.13 Fixed Bugs in CF 24

This section describes the bugs fixed in Release 5.1, CF 24.

3.13.1 Topology

ID	Description	Related ID in Previous Releases
CPF-25113	Previously, the SDC accepted a client peer with the same name as an existing server peer, causing inconsistencies between the CPF peer table and what was displayed in the Web UI (**Topology > Specific Site Settings > <Site Name>> Peers**). Now, if a user assigns a new client peer with the same name as an existing server peer, the SDC will reject the client and generate a Warning log.	

3.13.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-25122	Previously, a memory leak error was generated when client peers connected without a handshake (not with a CER message). Now, the memory leak is fixed and such memory leak errors no longer occur when client peers connect using non-CER messages.	
CPF-25116	Previously, when re-establishing a multi-channel peer connection, the SDC peer counter was mistakenly configured to count the number of peers per each re-connection and this caused the handshake to be rejected when the number of peers exceeded the maximum allowable number of 5000. The multi-connection peer count is now configured not to count the peers for each re-connection.	

3.13.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-25099	Previously, a peer's health may show as "Poor" in the Web UI (**Topology > Specific Site Settings > <Site**	

ID	Description	Related ID in Previous Releases
	Name>> Peers) even though none of the relevant health parameter/statistics reached their thresholds. Now, the healthStats calculator was reconfigured to correctly asses the health parameter/statistics so that the peer's health is accurately displayed in the Web UI.	
Installer-3097	Previously, following an upgrade from 4.4 to 5.1, the Machine Summary and Network Usage reports (**Reports > Resources > Machine Summary/Network Usage**) did not show the relevant site data. Now, the NMS Collector code was corrected to point to the network role to retrieve the data, and the reports now display as expected.	

3.14 Fixed Bugs in CF 23

This section describes the bugs fixed in Release 5.1, CF 23.

3.14.1 Flow Management

ID	Description	Related ID in Previous Releases
CPF-25066	Previously, when submitting routing action scripts (for example, post-transformation scripts **(Flows > Flows <Flows Name> > Transformation)**) to a flow management decision table with multiple flows, the script would apply the routing action to only the first, default flow. Now, the Routing Handler was fixed to recognize the correct flow in a multiple flow decision table as long as a script includes the following argument: sendAsync() with TransactionEvent.	

3.14.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-25066	As a result of a related bug fix in CF-22, the Web UI did not refresh automatically after submitting changes to the **Flows** page. The impact was that if another user opened another Web UI, recent changes could not be seen, until the original user manually refreshed the Web UI. Now, upon submitting changes the Web UI is automatically refreshed and updated, as expected.	

3.14.3 Administration

ID	Description	Related ID in Previous Releases
CPF-25059	The **Administration > Audit > Time > Filter** (select a date) now works as expected.	CPF-24975

3.14.4 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24884	Previously, when configuring the splunk application, in the site topology XML file, the splunk indexer log rotation mechanism did not work as expected. Now, the logrotate configuration was changed and the hardcoded file name "splunk" was removed so that the splunk indexer log rotation mechanism works as expected. *Note: This was detected as a known issue in CF-17.*	
CPF-25063	Previously, when using a health monitoring script with the peer.getTps() function, the returned value was always mistakenly zero, even when there was traffic. Note, for the peer.getTps() function to accurately calculate the TPS, a rate limit must be configured for the peer (**Topology>Peer Profiles>Add/Edit>Rate Limit**). In	

ID	Description	Related ID in Previous Releases
	addition, the calculation mechanism was corrected to return the correct TPS value.	

3.15 Fixed Bugs in CF 22

This section describes the bugs fixed in Release 5.1, CF 22.

3.15.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-25007	A validation mechanism was added to the Site Topology file to verify the length of the hostname parameter (maximum length of 64 characters).	

3.15.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-25056	Previously, when making changes to both **Pre-Routing** or **Post-Routing** transformation scripts (**Flows > Flows <Flows Name> > Transformation**), and upon switching back and forth between the tabs, the changes no longer appeared when returning to the previous tab. Now, you can switch back and forth between the tabs and the configuration changes will appear in the relevant screen. *Note: Once you select **Submit**, only the configuration changes that appear under the specific open tab (**Pre-Routing**/ **Post-Routing**) are saved (and viewable) and any previously configured changes made in the other tab are not viewable nor saved.*	

3.15.3 Administration

ID	Description	Related ID in Previous Releases
CPF-24975	Selecting the **Administration > Audit > Time > Filter** (select a date) no longer causes the Web UI to freeze.	

3.16 Fixed Bugs in CF 21

This section describes the bugs fixed in Release 5.1, CF 21.

3.16.1 Topology

ID	Description	Related ID in Previous Releases
CPF-25002	Previously, when configuring an SS7 peer profile (**Topology > Peer Profiles**), the option to disable support for IPv6 - IPv4 enablement did not work as expected. Now, when you deselect the **Enable Manipulation Ext-PDP-Type for Roaming-Gr (outbound)** checkbox, this feature is disabled as expected.	

3.16.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-24988	Previously, when making changes to a flow's transformation decision tables (**Flows > Flows <Flows Name> > Transformation**), you were not able to submit additional changes to a pre/post transformation script, and an error message was generated. Now, you can successfully submit multiple changes to pre/post-transformation scripts.	

3.16.3 Administration

ID	Description	Related ID in Previous Releases
CPF- 24992	Previously, when adding a new Attribute List (**Administration** > **Attribute Lists** > **Add**), the new list was a duplicated list which included List Names/Descriptions from an existing list. Now, when selecting **Add**, you can successfully create a new Attribute List.	

3.16.4 Maintenance

ID	Description	Related ID in Previous Releases
CPF-25015	The Add FEP procedure now adds a FEP as expected. For more information, refer to the *F5 SDC 5.1 Bare Metal System Maintenance Guide*.	
CPF-25031	As a result of changes to a validation mechanism, you could not configure a route from a public VIP address to an external public network, either by changing the topology.xml or by applying the route-api.py script. Now, the validation mechanism has been corrected to recognize public VIP addresses, and a route can be successfully added.	

3.17 Fixed Bugs in CF 20

This section describes the bugs fixed in Release 5.1, CF 20.

3.17.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2911	The validation mechanism for the Site Topology file now checks that the applicationInstance and the interface network IP versions (v6/v4) are synced. If found to be invalid,	

ID	Description	Related ID in Previous Releases
	installation will fail and an error message will be generated in the/var/log/salt/master logs.	
CPF-24898	A validation mechanism was added to the Site Topology file to check if route gateway is valid. If found to be invalid, installation will fail and an error message will be generated in the/var/log/salt/master logs.	
CPF-24899	The topology validation mechanism for Tripo now checks as expected the max_host_name size (which is set to 64 characters minus one NULL character, meaning supports strings of 63 characters.)	

3.17.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-24983	The getSessionFromExternalStorage script is now supported with the API as expected.	
CPF-24990	Previously, after a master session was removed from the Tripo record (after a CCR-t or upon expiration), the CPF failed to route its slave session messages (CCR-u/t/RAR). Now, slave session data records are saved to Tripo so that even when a master session is terminated or expired, the CPF continues to route the slave session messages until the slave session is terminated or expired.	
CPF-24989	In a geo-redundant deployment, you can now configure a slave session (**Flows > Flows > <Flow Name> > Session Management > Session Persistence Policy > Persist and Replicate**) to be routed to the mated site, even if the master session is terminated, to see if the mated site's routing rules apply. This configuration is done by changing the	

ID	Description	Related ID in Previous Releases
	isLocalRoute, in the traffix_cpf_init script, to false. A default value of true means that the slave session will only be routed according to the local site's routing rules.	
CPF-24997	Previously, when configuring a persistent geo-redundant deployment (**Topology > Peers > Add/Edit > General >Use for Geo Redundant Sites Connection**) and (**Flows > Session Management > Session Persistence Policy > Persist and Replicate**), the SDC was mistakenly configured to send requests to both the Tripo and the FEP of the geo-redundant site, and this generated an exception in the CPF logs, as release 5.1, unlike release 4.4, does not support sending requests to the Tripo on the geo-redundant site. Now, the code has been fixed so that requests are not forwarded to the Tripo on the geo-redundant site.	

3.17.3 Web UI

ID	Description	Related ID in Previous Releases
CPF-24993	A previous bug fix (CPF-24610) in CF 11 did not fully correct the Date and Time sorting problem for displayed alarms. Now, this problem is corrected and displayed alarms (**Alarms > Active Alarms**) can now be sorted and displayed as expected in the **Date and Time** column.	CPF-24610

3.17.4 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24970	Previously, when the sdcCmEmsConnection alarm was generated, the eventID variable was incorrect as there was	

ID	Description	Related ID in Previous Releases
	a mismatch between the eventID variable in the SDC-MIB.mib file and the JAVA enum. Now, the eventID variable is generated as expected as shown in the EMS site nmsagent.log.	

3.18 Fixed Bugs in CF 19

This section describes the bugs fixed in Release 5.1, CF 19.

3.18.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-24914	Previously, when the firewall iptables were started (automatically by the Salt master) and the SDC was up and running, sessions were blocked to/from Cassandra. This was due to two Cassandra ports (7000 and 9042) only being defined as destination ports and not source ports. Now, these ports are defined, by default, also as source ports, and sessions are no longer dropped when the firewall iptables are started and the SDC is up and running.	
CPF-24915	The validation mechanism that was added in CF-17 to stop the upgrade process when the copyFromIso upgrade step failed did not include generating logs. Now, in the case of a failed mount, and the copyFromIso upgrade step fails, WARNING logs are generated in the upgrade log for improved troubleshooting.	
CPF-24958	Previously, in CF-17, there were two defective Red Hat rpms (dhclient-4.1.1-53.P1.el6_9.3.x86_64.rpm, libstdc++-4.4.7-18.el6_9.2.x86_64.rpm) that were included in the ISO build. These are now replaced with	

ID	Description	Related ID in Previous Releases
	new rpms and a verification mechanism has been added.	
CPF- 24959	A verification script was added to check that Red Hat rpm packages comply with size and other standard requirements prior to building an ISO.	

3.18.2 Topology

ID	Description	Related ID in Previous Releases
CPF-24916	Previously, the filters for Configuration Sync Status and Last Sync Status Change fields in the SDC Components table (**Topology > Specific Site Settings > Site > SDC Components> SDC Components**) did not work as expected. Now, the filters for these fields work as expected.	
CPF-24932	Previously, when configuring EU Local Breakout (LBO) for SS7 peer profiles (**Topology > Peer Profiles > SS7 > MAP Manipulations > Enable EUInternet LBO**), messages with InsertSubscriberData (ISD) requests were handled by multiple CPF threads and this caused incorrect ordering of outgoing ISD requests. Now, all ISD requests are processed on the same thread and there is no reordering of ISD requests.	

3.18.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24946	Previously, traps that were forwarded to an external listener system did not accurately show the trap date and time. Now, the eventDateAndTime parameter was reconfigured and the traps' date and time show as expected.	

3.19 Fixed Bugs in CF 18

This section describes the bugs fixed in Release 5.1, CF 18.

3.19.1 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24931	Logout events are now recorded in the webuiLogFile.log. After a user logs out, the following log entry is generated: User <user name> has logged out.	

3.20 Fixed Bugs in CF 17

This section describes the bugs fixed in Release 5.1, CF 17.

3.20.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-24637	Previously, during a rolling upgrade, the upgrade process continued when an ISO failed to mount. Now, a validation mechanism has been added to the copyFromIso upgrade step so that in the case of a failed mount, the upgrade process stops.	
CPF-24892	Previously, an SDC upgrade caused a reset to the default LDAP login. Now, following an SDC upgrade, a configured LDAP login is saved.j**ava**	
CPF-24893	Previously, configured Tripo host name and IP addresses over 43 bytes caused the Tripo to fail. Now, the Tripo host name and IP address size support a max_host_name size (of 64 bytes).	

3.20.2 Maintenance

ID	Description	Related ID in Previous Releases
CPF-24714	The changeNameserver API is now supported to add/delete a DNS to a site. For more information, see the *SDC Bare Metal Maintenance Guide*.	
CPF-24819	Previously, when running the addRoute API script, invalid IP address were mistakenly added to the site topology and Cassandra database. Now, the validation mechanism has been improved to check that only valid IP addresses are added. *Note: This was detected as a known issue in CF-15.*	
CPF-24844	The addNetwork and deleteNetwork APIs are now supported to add/delete a network to or from a site. For more information, see the *SDC Bare Metal Maintenance Guide.*	

3.20.3 Web UI

ID	Description	Related ID in Previous Releases
CPF-24212	After applying the Filter option in various Web UI tables, the filter icon now displays as expected, showing users that there is an applied filter.	

3.21 Fixed Bugs in CF 16

This section describes the bugs fixed in Release 5.1, CF 16.

3.21.1 Topology

ID	Description	Related ID in Previous Releases
CPF-24806	Previously, a server 's pool health (and its related peers) may have mistakenly displayed (Topology > Specific Site Settings > <Site Name>> Peers > Health) as red (poor) or orange (fair) even when the returned error rate was lower than the configured Error Thresholds (Topology>Peer Profiles>General), and a peerHealthTimeouts alarm was generated. Now, the code for the Error Answers Threshold was fixed so that pool and peer health are calculated and displayed as expected and no unexpected alarms are generated.	

3.21.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-24810	As a result of a problem with the peer.send script, NullPointerExceptions were generated when creating TDRs. Now, a validation mechanism was added for the sendingRequest object and TDR generation does not result in NullPointerExceptions.	
CPF-24824	Previously, when applying the peer.sendAsync script (**Flows > Transformation**) to fork a message to a second server peer for monitoring (SOR) the pending request queue filled up, affecting traffic. Now, the script points to the right parameter ID and messages can be forked as expected, without filling up the pending request queue.	
CPF-24828	Previously, after setting a display filter for the Routing Rules Web UI (**Flows > Routing Rules > Type Filter Text > Submit**), and then navigating to another Flows Web UI tab (such as **Flows > Routing Rules > Session**	

ID	Description	Related ID in Previous Releases
	Management), and then back to the Routing Rules table, resulted in the table rows jumping. Now, using the filter option, does not affect the Routing Rules table display.	

3.21.3 Administration

ID	Description	Related ID in Previous Releases
CPF-24812	Previously, when the system is overloaded, and you performed an audit restore (**Administration > Audit > Restore**), some of the configurations may not have been restored as expected. Now, the audit functionality works as expected.	
CPF-24840	Previously, when editing an Attribute List description (**Administration > Attribute Lists > Edit)**, the list data values were deleted. Now, you can edit an Attribute List description and the related data values are saved as expected.	

3.21.4 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24811	The geoSdcProxyConnection alarm is now cleared, as expected, after a fail-over when the SDC site is reconnected to its geo-redundant SDC site. When this alarm is generated following an initial fail-over, see the workaround provided for CPF-24683.	
CPF-24845	Previously, when setting Tracing to false (**Administration > Tracing > Disabled**), tracing reports/logs were generated. Now, the true/false setting	

ID	Description	Related ID in Previous Releases
	works as expected, so tracing reports/logs are only generated when **Enabled** is set to true. **Note**: If a user wants to stop tracing requests of a persisted session, the tracing decision rule must be disabled (deleting an enabled tracing decision row will not stop the tracing).	

3.21.5 Performance

ID	Description	Related ID in Previous Releases
CPF-24826	The repair script (cassandraRepairKeySpaces.py) now runs as expected and does not kill previous runs.	

3.22 Fixed Bugs in CF 15

This section describes the bugs fixed in Release 5.1, CF 15.

3.22.1 Topology

ID	Description	Related ID in Previous Releases
CPF-24694	Previously, when a dynamic peer profile was removed from a pool, all the related dynamic peers were removed, as expected, from the pool in the CPF configuration code, but this was not reflected in the Web UI (**Topology > Pools > Edit > Edit Peers**). Now, this action is reflected in the Web UI as expected.	
CPF-24735	In the **Topology > Specific Site Settings > <Site Name>> Peers** table, the **Status** parameter is now updated to Limited, as expected, even when one of the CPF processes is partially out of service.	

ID	Description	Related ID in Previous Releases
CPF-24773	Previously, when selecting and deleting multiple peer profiles (**Topology > Peer Profiles > Remove**), the system separately considered each selected peer profile, causing some selected peer profiles to not be restored as expected (**Administration > Audit > Restore**). Now, all peer profiles that are selected for the same **Remove** action are restored as expected.	

3.22.2 Administration

ID	Description	Related ID in Previous Releases
CPF-24797	When configuring the user password and selecting the **Warning expiration (days)** option in **Administration > User Management > Preferences**, the **Remind me Later** option now works as expected. In addition, a **Password Expiration Date Column** was added to the **Administration > User Management** table.	

3.22.3 Maintenance

ID	Description	Related ID in Previous Releases
CPF-24799	Previously, the add/delete route script (route-api.py), did not point to the correct interface (eth parameter) and this caused errors in the Cassandra database. Now, the add/delete route script (route-api.py) was corrected to point to the correct interface (eth parameter).	

3.23 Fixed Bugs in CF 14

This section describes the bugs fixed in Release 5.1, CF 14.

3.23.1 Topology

ID	Description	Related ID in Previous Releases
CPF-24597	Previously in OpenStack environments a virtual server mistakenly showed (**Topology > Specific Site Settings > Virtual Servers > Status**) as Limited if one of the FEPs was down, even though unlike other components, it is not expected behavior that both FEPs will be up. Now, the **Virtual Servers > Status** correctly shows as Open (green), when only one FEP is up.	

3.23.2 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24692	As a result of recent Google Chrome changes, a previous fix that enabled Splunk reports visibility from a Chrome browser is roll-backed, to ensure HTTPS connectivity in Google Chrome. Splunk reports for TDRs, Traced Messages and Splunk License Usage (in the **Reports** screen) now display as expected.	
CPF-24696	Previously, changes made to health monitoring scripts from the EMS Web UI (**Topology > Specific Site Settings > Health Monitoring > First Type**), were only updated for the site and not, as expected, for the EMS deployment. Now, the Health Monitoring tab is displayed for the EMS deployment (**Topology > Health Monitoring > First Type**) and not per site and upon submitting any health monitoring script configuration changes, they are made throughout the EMS deployment.	

3.23.3 Web UI

ID	Description	Related ID in Previous Releases
CPF-24706	Previously, when leaving the **Flows > Routing Rules** page, without submitting configuration changes made to a routing rule, there was no Leave Page prompt. Now, when leaving the **Flows > Routing Rules** page, without submitting routing rule configuration changes, the Leave Page prompt displays asking "Do you want to leave this page? Changes you made may not be saved."	
CPF-24720	A warning message is now displayed when a user submits changes to one browser which would overwrite configurations to the same Web UI page (Routing Rules, Transformation, Session Management, Tracing and Message Prioritization) that is concurrently opened in another browser. *Note: This issue was detected in CF -13.*	

3.24 Fixed Bugs in CF 13

This section describes the bugs fixed in Release 5.1, CF 13.

3.24.1 Administration

ID	Description	Related ID in Previous Releases
CPF-24676	Previously, upon an LDAP user logging in with an expired password, the SDC Change Password window mistakenly displayed. Now, for LDAP users, the SDC Change Password window is not displayed as the SDC does not manage LDAP user authentication.	

3.24.2 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24587	Previously, following a rolling upgrade, some **Dashboard** statistics (Success Rates/Failure Rates) did not display values as expected when the Web UI was opened from Internet Explorer. Now, following a rolling upgrade, when opening the Web UI with Internet Explorer 11, the **Dashboard** statistics display as expected.	
CPF-24683	Previously, the sdcUserAuthenticationFailure alarm (**Alarms> Alarm History Log**) incorrectly showed the hostname value as the Site ID value. Now, the generated trap shows, as expected, the hostName field as the server hostname.	

3.24.3 Web UI

ID	Description	Related ID in Previous Releases
CPF 24530 CPF-24523	The following accessibility/keyboard navigation issues are fixed: A selected main tab is now visible and readable as expected. In the Edit Peer window (**Topology**), the Type (Server/Client) field is now visible and readable as expected.	
CPF-24538	Previously, the wrong menu tab was highlighted after selecting **Stay** to the Leave Page prompt question. Now, when selecting **Stay** to the Leave Page prompt question, the highlighted menu tab remains the same as the displayed Web UI page, and only changes, as expected, when selecting **Leave**.	
CPF-24649	A **Move To** button was added to decision tables in the Web UI (such as **Flows > Routing Rules**) allowing users to easily move a routing rule to the bottom or top of a page.	

3.25 Fixed Bugs in CF 12

This section describes the bugs fixed in Release 5.1, CF 12.

3.25.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-3013	Previously, an incorrect status reading of a site peer being down triggered a busy process ID and an endless looping of an automatic run of a Cassandra repair script which, subsequently, caused a Bare Metal rolling upgrade to fail. Now, all site peers' status are recognized as expected and incorrect process IDs are not generated causing repair runs that could stop a rolling upgrade. *Note: This was detected as a known issue in CF 8.*	
CPF-24617	When performing an installation, the salt-install.sh script now has a built-in subnet validation process to check that the ip6sub and ip4sub subnet mask parameters are defined and if not a log file error: "Error - Metadata for netmask$i is empty" is generated and the installation run generates exit code 1.	

3.25.2 Topology

ID	Description	Related ID in Previous Releases
CPF-24605	The keepalived mechanism is now fully supported when using IPv6 protocol.	
CPF-24652	In addition to supported Application IDs, from your current build, you can now add additional Diameter Application IDs to SDC components (CPF /FEP), from the standard_dynamic.txt file (located in the	

ID	Description	Related ID in Previous Releases
	/opt/traffix/sdc/config folder). The added Application IDs appear in the SDC Web UI (**Topology > Specific Site Settings > Site > SDC Components > Diameter**). For more information, see the F5 SDC 5.1 Troubleshooting Guide.	

3.25.3 Flow Management

ID	Description	Related ID in Previous Releases
CPF-24615	Previously, Sy messages were defined as stateless and, consequently, were not saved in the SDC Session Repository (Tripo). Now, the Sy interface has been defined as stateful, and assuming the FEP and CPF components are configured for an Sy interface, Sy messages are now saved to the SDC Session Repository (Tripo).	
CPF-24631	Previously, when applying the validation mechanism to Flow action scripts (for example, **Flows > Routing > <routing row> Handle Errors > Static Compilation**), an invalid script could be submitted (with a second **Submit** attempt) even when an error warning was generated indicating that there was an invalid parameter or syntax. Now, invalid scripts cannot be submitted.	
CPF-24639	Previously, the Handle Client Error scripts (**Flows > Routing > <routing row>>Handle Errors**) mistakenly pointed source peer values to the destination peer instead of the source peer. Now, in Handle Client Error scripts, the source peer values correctly relate to the source peer.	
CPF-24648	Previously, Redirect groovy scripts (**Routing > Routing Check Error In Answer**) did not point to the right peer/pool and this meant that when a client peer (acting as	

ID	Description	Related ID in Previous Releases
	a server peer) returned a CLA error (3006) the CLR was not redirected as expected and this created a continuous loop, pressure on the log file and timeouts. Now, the code was modified and Redirect groovy scripts are recognized so that following a CLA error (3006), CLRs are redirected as expected to another peer.	

3.25.4 Monitoring

ID	Description	Related ID in Previous Releases
CPF-22623	When there are multiple SDC sites managed by an EMS site, changes to the log definitions for a single SDC site (in either a local Web UI or in the EMS Web UI: **Administration** > **<SDC Site>** > **Logging**) no longer impact the log definitions in the other SDC sites.	
CPF-24296	The active alarm (sdcComponentStatus) is no longer falsely generated (**Alarms** > **Active Alarms**) for a CPF component that has been removed with a scale-in API request. *Note: This issue was detected in CF 9.*	
CPF-24463	Previously, in the Transactions Data Records table (**Reports** > **TDRs** > **Transaction Data Records**), peer names may have displayed with quotation marks. Now, the peer names in the Transactions Data Records table appear as expected.	
CPF-24635	Previously, with the Splunk version upgrade, the Traced Messages table in the Web UI (**Reports** > **TDRs** > **Traced Messages**) did not display the full Traced Message entry as was recorded in the Splunk database due to a parsing issue. Now, the parsing issue was fixed, and the full Traced Message is displayed in the Web UI.	

ID	Description	Related ID in Previous Releases
CPF-24640	After restarting the CPF and FEP, the communicationOfFepCpf alarm is now cleared as expected indicating that the message channel between the FEP and CPF components is open again.	
CPF-24651	Previously, multiple failed log in attempts to the EMS Web UI caused a java.net.SocketException, as each time a new socket connection was opened to send the alarm (sdcComponentStatus). Now, the system does not become overburdened as it is now configured to use the same SNMP socket to send the alarm when there are multiple failed log in attempts.	
CPF-24663	Previously, sdcComponentStatus alarms were not cleared as expected (**Alarms > Active Alarms**) for SDC components (other than CPF and FEP) following a graceful shutdown (monit stop all) during a maintenance or rolling upgrade. Now, upon restarting the system, the NMS Agent is configured to check components' status with sdcComponentStatus alarms, and upon recognizing that the component is UP, it will clear the sdcComponentStatus alarm.	
CPF-24690	As a result of recent Google Chrome changes, a previous fix that enabled Splunk reports visibility from a Chrome browser is roll-backed, to ensure HTTPS connectivity in Google Chrome. Splunk reports for TDRs, Traced Messages and Splunk License Usage (in the **Reports** screen) display as expected.	5.1 CF 10: CPF-24272

3.25.5 Web UI

ID	Description	Related ID in Previous Releases
CPF-24047	When using keyboard navigation, the focus (highlight) is now maintained on a selected peer (**Topology**) after auto-refresh.	
CPF-24537	There is now a stronger color contrast between editable and non-editable fields in the Edit Virtual Server window (**Topology** > **Virtual Servers**).	

3.26 Fixed Bugs in CF 11

This section describes the bugs fixed in Release 5.1, CF 11.

3.26.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-24623	The following error notification is now generated if the copyFromIso procedure is not successfully carried out when performing a Bare Metal rolling upgrade: "Could not copy repo to second master", thereby notifying the user that the relevant RPMs were not copied to the second Master Installer.	

3.26.2 Topology

ID	Description	Related ID in Previous Releases
CPF-24531	SDC routed SCTP messages now include a specified Payload Protocol Identifier parameter (46 (Diameter) or 47 (Encrypted Diameter)).	
CPF-24608	The pool health calculation is fixed to correctly reflect any relevant generated or cleared alarm and, as a result, a pool's health now displays (red, yellow. green) as expected in **Topology > Pools >Health**.	

3.26.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24555	Previously, the Sent to SNMP targets setting (**Administration > SNMP > SNMP Settings**) did not work as expected (from an EMS or SDC site Web UI) and you could not select a specific alarm and set it to false so that it would not be sent to a defined SNMP target. Now, the true/false setting works as expected and alarms can be configured to be sent or not.	
CPF-24554	The sdcLicenseMpsViolation alarm is now cleared as expected after MPS drops below the set volume level.	

3.26.4 Web UI

ID	Description	Related ID in Previous Releases
CPF-24258	The "Does not contain" filter option (in **Flows >Flows > Filter** from the Flows table) now works as expected.	
CPF-24520	There is now a stronger color contrast between editable and non-editable fields to support accessibility in read-only fields.	
CPF-24526	The Web UI now switches, as expected, to a new menu tab after selecting Leave to the Leave Page prompt when changing a configuration without submitting the change. Note: This was detected as a known issue in CF 10.	
CPF-24610	Displayed alarms (**Alarms > Active Alarms**) can now be sorted as expected in the Date and Time column.	

3.26.5 Performance

ID	Description	Related ID in Previous Releases
CPF-24561	The cassandraRepairKeySpaces.py script now runs once a day, instead of once an hour, and, consequently uses much less CPU and IO resources.	

3.27 Fixed Bugs in CF 10

This section describes the bugs fixed in Release 5.1, CF 10.

3.27.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2991	Bond Eth parameters configured in the Site Topology file are now validated as expected *Note: This was detected as a known issue in CF 6.*	
CPF-24120	Previously, as the Linux pre-defined ephemeral port range was set to 50000-64000, when an SDC component used an external port within this range that was already being used by another component, such as an NMS Agent (port 61617), configuration manager (61616) or Web UI (61657), the component (with the set port) connection failed. Now the external port range for SDC components has been redefined to 50000-59999, so that when binding to another server, an SDC component cannot use one of the set ports reserved for the NMS Agent, configuration manager or the Web UI. *Note: When performing a rolling upgrade, you need to manually define the new port range. Refer to the 5.1 Bare Metal Upgrade Guide for more information.*	

ID	Description	Related ID in Previous Releases
CPF-24488	Previously, a bare metal installation or upgrade may have failed when a server hosts many components and there is a port collision as some ports (for NMS Agent) are already assigned to another component (FEP). Now, the method of assigning ports has been changed so that the ports assigned to an NMS Agent are fixed and the ports assigned to the FEP are calculated using the FEP index, and the same port cannot be used by multiple components.	

3.27.2 Topology

ID	Description	Related ID in Previous Releases
CPF-24254	Previously, after disabling and then re-enabling a Virtual Server (**Topology > Specific Site Settings > Virtual Servers > Enable/Disable**) its Transport Configuration parameters (such as **Send/Receive Buffer Size**) were not saved. Now, these parameters are saved after disabling and then re-enabling a Virtual Server.	
CPF-24313	The option to have multiple connections between one dynamic client peer and a FEP now works as expected, so that when evoking the Capabilities Exchange Answer script (**Topology > Peer Profiles > <the relevant Dynamic Peer Profile > Edit > Handshake Scripts>Capabilities Exchange Answer**), each new connection of the same peer is considered as a new peer with the same Origin Host name followed by a suffix (SN_<index #>).	
CPF-24527	Previously, loading a peer table list (**Topology > Peer Profiles**) containing peer profiles with many supported PLMNs may have taken a few minutes. Now, loading a peer table list takes less than half a minute as the retrieval process is done by peer profile and no longer by each peer.	

3.27.3 Web UI

ID	Description	Related ID in Previous Releases
CPF-24322	Previously, when reloading a page in the Web UI (CTRL-F5), after adding an SNMPv3 Profile (**Administration > SNMP > Add**), the Web UI may have shown the following error " Failed to retrieve SNMP dilution values" in some screens. Now, this error message no longer appears after adding an SNMPv3 Profile and reloading a page in the Web UI. *Note: This was detected as a known issue in CF 9.*	
	The following accessibility/keyboard navigation issues are fixed:	
CPF-24028	▪ The **Reports >Traced Messages and Reports > Splunk License Usage** screens now clearly display with color contrast.	
CPF-24455	▪ There is now a stronger color contrast between editable and non-editable fields in the Edit Virtual Server window (**Topology > Virtual Servers**).	
CPF-24456	▪ Upon saving changes in the **Administration > User Management >Add User** window, the cursor now returns to the relevant field when any invalid values are entered to show the user where the correction is needed.	
CPF-24457	▪ When selecting a **Cancel** or **Save** button, each is now clearly highlighted.	
CPF-24458	▪ The focused tab now displays clearly highlighted as expected.	

3.27.4 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24255	The "Splunk License Volume Used during last 30 Days" graph (**Reports > Splunk License Usage**) now displays as expected.	
CPF-24272	Splunk reports for TDRs, Traced Messages and Splunk License Usage (in the **Reports** screen) now display as expected when opening Splunk from Chrome, Firefox, or Internet Explorer. *Note: This was detected as a known issue in CF 9.*	
CPF-24291	Previously, in the **Reports > TDRs** Screen, there was no option to show the filter after selecting Hide Filter. Now, this option is available. *Note: This was detected as a known issue in CF 9.*	
CPF-24462	The multi-select option in the **Administration > Specific Site Settings > SNMP** now works as expected so you can now select multiple SNMP profiles and then select **Enable/Disable** to enable/disable multiple SNMP profiles with one action.	
CPF-24534	The Splunk License Usage page (**Reports**) now consistently shows the correct usage and the page has been updated for easier viewing and monitoring of daily and monthly Splunk license usage.	

3.27.5 Maintenance

ID	Description	Related ID in Previous Releases
	The following issues were fixed when applying the addRoute/delete Route script and addRoute API:	

ID	Description	Related ID in Previous Releases
CPF-23819	For improved troubleshooting, an error log "Failed to add routes" is now generated in the route logs when an addRoute script or AddRoute API fails at the end of the Linux platform process. *Note: This was detected as a known issue in CF 6.*	
CPF-23833	For improved troubleshooting, generated error codes now include an explanation of the error.	
CPF-23837	Added parameters are now validated to check that they have the correct syntax.	

3.28 Fixed Bugs in CF 9

This section describes the bugs fixed in Release 5.1, CF 9.

3.28.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-3008	Previously, when upgrading the Master Installers and running the saltupgrade command twice, the salt pillar data configuration failed. Now, when running the saltupgrade command, the second time, the system knows to point to the original salt pillar and the upgrade is continued as expected.	
CPF-24118	Previously, after performing a rolling upgrade, following a monit restart procedure, some minion environments (SDC components) may not have been upgraded as expected. Now, all minion environments are upgraded as expected. *Note: This issue was detected in CF 8.*	

ID	Description	Related ID in Previous Releases
CPF-24265	During an installation, the Splunk function file (/opt/traffix/components/Splunk) now points to the correct folder based on what is defined as the Splunk name in the topology file.	

3.28.2 Topology

ID	Description	Related ID in Previous Releases
CPF-22905	Configuring an empty pool with overload control, by setting the isActivatePrioritization parameter to false with the modifyPool Web Services API command no longer results in an NullPointerException in the CPF log.	
CPF-24362	In addition to supported Application IDs, you can now add additional Diameter Application IDs to SDC components (CPF /FEP), using the Web Service API Method: SetDiameterPropertiesforNode, in the supportedApplicationIds parameter and the added Application ID will appear in the SDC Web UI (**Topology > Specific Site Settings > Site > SDC Components** > **Diameter**).	

3.28.3 Flow Management

ID	Description	Related ID in Previous Releases
CPF-24116	A validation mechanism was added to a Forward routing rule to a pool, in that the **Exact Destination From** field (**Flows > Routing Rules > <RT-x>>Forward>Forward To Pool**) is now required to be filled in.	
CPF-24144	Previously, users could delete the Default flow (**Flows > Routing Rules > Default**). Now, the defaults cannot be deleted.	

3.28.4 Web UI

ID	Description	Related ID in Previous Releases
CPF-23987 CPF-24027	The following accessibility (keyboard navigation) issues are fixed: Drop-down menus (**traffix** and **Help**) now close as expected when using tab button. In the Add User window (**Administration > User Management**) the focus sequence of the tab key is now consistently from left to right.	
CPF-24052	After making Web UI changes, the message "Changes were saved successfully" now appears centrally located on the relevant screen before disappearing after a few seconds.	
CPF-24125	Previously, when removing an item based on an applied column filter (**Topology > Peer Profiles > Association Rules** or **Message Prioritization**), all items (including the unfiltered ones) were mistakenly removed. Now, the filter validation mechanism has been improved so that a **Remove** action on a filtered column only removes those matching the applied filter.	

3.28.5 Administration

ID	Description	Related ID in Previous Releases
CPF-24149	Previously, when applying a rollback (**Administration > Audit > Rollback**) after removing duplicated peer profiles (**Topology > Peer Profiles ><selected peer profile>>Duplicate >Remove <selected peer profile>**), not all the peer profiles were displayed as expected in the EMS Web UI. Now, all the relevant peer profiles are displayed after applying a rollback on duplicated peer profiles.	5.0: CPF-24147

3.28.6 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24293	The **Reports** > **Splunk License Usage** graph now displays the data as expected.	
CPF-23395	During a rolling upgrade, TTA logs that contain the status information of the SDC components, including those from the previous version that have not yet been upgraded, are now generated as expected after a failed rolling upgrade, for improved troubleshooting.	

3.28.7 Maintenance

ID	Description	Related ID in Previous Releases
CPF-23839	When applying the addRoute/delete Route script and addRoute API, manually added/deleted routes are now applied, as expected, to any machines that are added (with scaling out) after the initial installation. *Note: This issue was detected in CF 6.*	

3.29 Fixed Bugs in CF 8

This section describes the bugs fixed in Release 5.1, CF 8.

3.29.1 Topology

ID	Description	Related ID in Previous Releases
CPF-24035	The SDC now supports multiple connections between one dynamic client peer and the FEP (**Topology > Peer Profiles**). Refer to the *SDC 5.1 User Guide* for configuration details.	

3.30 Fixed Bugs in CF 7

This section describes the bugs fixed in Release 5.1, CF 7.

3.30.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2916	In a site topology file, different default gateways can now be defined and are supported for route and source networks.	
Installer-2992	When performing a rolling upgrade, the recently added validation mechanism of the upgradeOamDB process (in CF 6) did not include a timeout, and this may have caused long waiting times for unresolved upgradeOamDB processes. Now a timeout, was added so that after 500 seconds, the upgrade is stopped and the following message is displayed "Could not stop oamDB on server."	

3.30.2 Topology

ID	Description	Related ID in Previous Releases
CPF-23860	When applying an engineering script to an SDC site component (FEP, CPF, Configuration Manager) the **Name** field (**Administration > <SDC site>> Engineering Scripts >Cluster Nodes Engineering**), which must match the defined name of the relevant component, now points to the selected component.	

3.30.3 Flow Management

ID	Description	Related ID in Previous Releases
CPF-23868	Previously, running 20K TPS on many clients (1200) with a 150-millisecond delay may have resulted in an out of memory error, causing traffic to stop without recovery capabilities, even when the delay was removed. Now, the Netty version was upgraded to 4.1.10 to support traffic recovery, once the delay is removed.	

3.30.4 Monitoring

ID	Description	Related ID in Previous Releases
Installer-2816	TTA scripts now include upgrade log files to improve troubleshooting capabilities.	
CPF-22651	Previously, the **Reports > Network Usage> Sent/Received Bytes** graphs showed the accumulated value instead of the value per monitored period. Now, the value per monitored period is shown in the graphs as expected.	
CPF-23910	When performing a rolling upgrade, the following TDR error message no longer appears in the NMS, Configuration Manger and Tomcat logs: "ERROR [] GET/SET_CREATE_TDR doesn't have a value in logDescriptions.txt [http-nio-8080-exec-14_74248] [LoggingEnum.load()]," *Note: This issue was detected in CF6.*	
CPF-23965	The SDC supported Splunk version is upgraded to version 6.5.3 and the **Reports > TDR Dashboard/Transaction Data Records/Traced Messages** screens now support keyboard navigation.	

3.30.5 Maintenance

ID	Description	Related ID in Previous Releases
CPF-23959	The addroute functionality now supports using a FEP-VIP address as the source address as well as for the loopback VIP address.	

3.30.6 Web UI

ID	Description	Related ID in Previous Releases
CPF-23929	Previously, filtering for a value in a Comment field (**Administration** > **Tracing/Message Prioritization** > **More Details**) caused the Web UI to stop working. Now, the filtering functionality works as expected for values saved in the Comment field.	

3.31 Fixed Bugs in CF 6

This section describes the bugs fixed in Release 5.1, CF 6.

3.31.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2926	Now, during an installation, by selecting the Support checkbox in the Topology Editor (**Applications** > **Tripo** > **Add Properties** > **Support**), you can enable Tripo replication between sites. When checkbox not selected, Tripo replication between sites is disabled, and the secondSiteIP1 and IP2 addresses are defined as 1.1.1.1 and are not editable.	
Installer-2965	Previously, during the upgrade OAMDB process, the system did not validate if other processes had stopped prior to running this upgrade command, and this caused the upgradeOamDB process to fail. Now, a validation mechanism has been added to make sure that the upgradeOamDB process is not initiated while other processes are still running.	
CPF-23696	While performing an upgrade from Release 4.4 to 5.1, and the system is in mix-mode, the following exception is no longer generated:	

ID	Description	Related ID in Previous Releases
	UnrecognizedPropertyException: Unrecognized field" "Comment." Note: This issue was detected in CF 6.	

3.31.2 Topology

ID	Description	Related ID in Previous Releases
CPF-23073	Previously, virtual servers with the same port number could be added (**Topology > Virtual Servers > Add**). Now, a warning message displays when adding a virtual server with the same port number of an already existing virtual server and it is not saved.	
CPF-23720	Previously, the Received Buffer Size for dynamic client peer profiles was not configurable as expected for SCTP channels, and this resulted in the INIT_ACK > a_rwnd value being limited to the default value. Now, this value is configurable as expected (**Topology > Peer Profiles > Dynamic Peer Profiles > Transport Layer Options > Receive Buffer Size (Server & Client)**).	
CPF-23765	Previously, when configuring EU Local Breakout or IPV6 protocol for roaming (**Topology > Peer Profiles > Diameter/SS7 > Diameter Configuration/MAP Manipulation > Import**), imported .csv files did not upload as expected. Now, imported .csv files are uploaded as expected (without spaces). In addition, the system no longer allows users to upload files other than .csv files	
CPF-23770	Previously, traffic sent to a FEP on a geo-redundant site was not processed as expected because the GEO client peer did not successfully connect to a virtual server (FEP) peer profile. Now, GEO client peers are configured to accept a virtual server peer profile and traffic is processed as expected.	

ID	Description	Related ID in Previous Releases
CPF-23783	When configuring EU Local Breakout (**Topology > Peer Profile > Diameter Configuration/MAP Manipulations**), the following warning message is displayed "The imported data will delete all existing data."	

3.31.3 Flow Management

ID	Description	Related ID in Previous Releases
CPF-21880	Previously, changes to DNS Resolving values were not saved as expected (**Flows > Routing Rules > Resolve & Route >DNS Resolving > Add**). Now, added DNS Resolving values are added and deleted as expected.	
CPF-23182	RADIUS messages with a request.NAS-IP-Address AVP with an IP ADDRESS RANGE are now processed as expected.	
CPF-23731	Previously, a rule attribute with empty spaces was not validated and, as a result, an XML with invalid values (empty spaces) caused the SDC to not work as expected. Now, rule attributes with empty spaces are accepted and validated.	

3.31.4 Administration

ID	Description	Related ID in Previous Releases
CPF-23294	Read-only users are now blocked, as expected, from adding and removing **Flows**.	

3.31.5 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23623	Previously, the NMS log rotation mechanism did not work as expected. Now, the log rotation mechanism works as expected so that when the nmsagent-stdout file is full. logs are written to a new nmsagent1-stdout.log file under /var/log.	
CPF-23706	Previously, changes made to log levels (**Administration > Logging > Log Levels**) for one site were mistakenly applied to all the other environment sites. Now, any log configuration changes are only applied to the selected site. *Note: This issue was detected in CF 5.*	
CPF-23707	Previously, changes made to the Syslog address (**Administration > Logging > Syslog Addresses**) for one site were applied to all the other environment sites. Now, when making changes to a site' Syslog address, only the relevant site is updated. *Note: This issue was detected in CF 5.*	
CPF-23724	New Web Service API methods, setCreateTDR and getCreateTDR were added to the WSDL. These methods allow you to enable collecting and displaying Transaction Data Records for a selected routing row with a Web Service command. For more information, see the F5 SDC 5.1 Web Services API Guide.	
CPF-23852	Previously, the /var/log/rsyslog/cassandra-repair.log file was not saved as expected and this caused errors in the logrotate script. Now, the log rotation mechanism saves the file name with the correct date and time format to the log file.	
CPF-23870	Previously, the **Remove** option for **Health Monitoring** (**Topology**) did not work as expected. Now, you can remove health monitors.	

3.31.6 Maintenance

ID	Description	Related ID in Previous Releases
	The following changes were made to the addRoutes/deleteRoutes script (route-api.py) and the add/delete Route API so that routes are now added/deleted as expected:	
Installer-2962	▪ Validates that traffic is no longer rerouted to the other network when both the management and signaling networks are defined as IPV4 and one of the network fails. Note: This issue was detected in CF 5.	
Installer-2963	▪ For improved troubleshooting of the addRoutes/deleteRoutes script (route-api.py), the input parameters and content of the xml file were added to the logs.	
Installer-2964	▪ Validates for duplicated routes so that when trying to add/delete the same route twice, an error log message is generated that the route already exists/does not exist.	
Installer-2993	▪ The log rotation mechanism now saves the route-api. file name with the correct date and time format to the route-api logs.	
CPF-23730	▪ Validates the IP address netmask prior to adding or deleting the route.	
CPF-23733	▪ Accepts a FEP IP source.	
CPF-23734	▪ When applying the addRoutes/deleteRoutes script, the metaData attribute was removed from the routes xml file.	
CPF-23755	▪ When applying the addRoutes/deleteRoutes script, route names are now validated by checking the newly added parameter: -N {Name}.	
CPF-23763	▪ Validates that a route with the same name for the same interface cannot be added.	

ID	Description	Related ID in Previous Releases
CPF-23784	▪ Accepts non-FEP interfaces.	

3.31.7 Web UI

ID	Description	Related ID in Previous Releases
CPF-23068	Now, after removing a dynamic peer from a pool (**Topology > Pools > Edit > Dynamically add Peers matching Peer Profile(s) > Select peer profile…> Remove**), the peers associated with the removed peer profile are not listed under the Peers column for the pool (**Topology > Pools**). *Note: This issue was detected in CF 1.*	
CPF-23713	Online Help images now display as expected. *Note: This issue was detected in CF 5.*	5.1 CF 4: CPF-23666
	The following Web UI issues were fixed in this release:	
CPF-21583	▪ Leave Page pop-up messages no longer display after saving (**Submit**) Web UI changes and navigating to a different screen.	
CPF-21680	▪ The Transport Layer (**Administration**) fields are fully editable, so that after entering a numerical value, you can change back to the OS default option	
CPF-23102	▪ Statistic percentiles in the **Dashboard** no longer show as over 100%.	
CPF-23740	▪ The Add Route Record checkbox (**Flows > Routing Rules > Topology Hiding and Diameter Identity**) can now be cleared as expected for a routing rule.	
CPF-23762	▪ The Dashboard Site table details (to view the connectivity status between the EMS configuration manager and the SDC site configuration manager) are now easily readable.	

ID	Description	Related ID in Previous Releases
CPF-23764	▪ **Dashboard** percentage statistics for values of "100" and "0" are now displayed without any decimal points.	
CPF-23775	▪ The refresh button is now enabled on SDC site Web UIs.	
CPF-23785	▪ The **Reports > Network Usage**: Output Errors drop-down list now includes eth interface options.	
CPF-23786	▪ Required SS7 peer fields (**Topology > Peers > Add > Name > Protocol > SS7**) are now marked with a"*" and are saved as expected.	
CPF-23795	▪ The Alarms screen (Active Alarms and Alarm History) functionalities (**Clear Filter, Export, Refresh, More/Less Details**) are now enabled for SDC site Web UIs.	
CPF-23809	▪ When viewing the connectivity status between EMS and SDC site configuration managers (Dashboard) cleared column check boxes no longer show as checked.	
CPF-23810	▪ The **Dashboard** and **Topology > SDC Components** sorting functionality now works as expected.	
CPF-23811	▪ An error message is generated if a non-CSV data dictionary file is selected to be uploaded (**Administration >Data Dictionary > Add**).	
CPF-23812	▪ The Syslog Addresses IP column name (**Administration > Logging**) was updated to **IP Address:port**.	
CPF-23827	▪ The **Administration >Tracing** page **Enable** column no longer has an empty drop-down option and the rule attributes are now applied as expected.	
CPF-23859	▪ The **More Details** button in the **Flows > Session Management** Web UI now displays the **Comment** column as expected.	

ID	Description	Related ID in Previous Releases
CPF-23869	▪ When adding a **Health Monitor** (**Topology**), all fields are now validated and an "Error in fields validation" message displays when one of the fields is not filled in correctly.	

3.32 Fixed Bugs in CF 5

This section describes the bugs fixed in Release 5.1, CF 5.

3.32.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2913	The clearSdcSiteFromEms.py script that is used in the SDC site rollback procedure is no longer case sensitive and no longer generates Warning errors for case sensitive differences.	
Installer-2918	Previously, when configuring data volumes in the Site Topology file, the mounting order (mountPoint parameter) affected which folder the data was saved to. Now, the order does not matter, as part of the mounting process, the system checks the partition data type (such as cassandra, log/rsyslog) when saving it to the new data folder.	
CPF-23469	Previously, when an upgrade to release 5.1 failed on one SDC site, the rollback to release 4.4 needed to be performed on all SDC and EMS sites. Now, a rollback can be performed on an individual SDC site. For more information, see the *F5 SDC Bare Metal System Upgrade Guide*. *Note: This as a known issue in CF 3*.	
CPF-23550	Previously, after performing an upgrade from release 4.4 to release 5.1, the EMS and SDC site configuration managers were not always synchronized and this resulted in errors (unexpected error during ping from node) being generated in the EMS configuration manager logs. Now, following an	

ID	Description	Related ID in Previous Releases
	upgrade, the EMS and SDC site configuration managers are fully synchronized and such errors are no longer generated.	

3.32.2 Topology

ID	Description	Related ID in Previous Releases
CPF-20639	The Add Peers window (**Topology > Pools >Add/Edit**) was modified to make it easier for users to view and select a peer for a pool from the list of available peers.	
CPF-23370	Previously, as a result of a third-party, Netty release bug, the **So Linger (Server & Client)** parameter option did not work as expected for SCTP channels (**Administration > Specific Site Settings > Default Transport Configuration**). Now, the Netty code was overrode and the **So Linger (Server & Client)** parameter is fully supported.	
CPF-23420	When configuring a peer (**Topology > Peers > Add**), you can now define Local IP Addresses for a FEP as the way to set the primary and secondary IP addresses for SCTP channels.	
CPF-23473	The E2 Diameter interface is now supported as a Diameter Application ID (**Topology > SDC Components > FEP > SDC Components Properties > Diameter > Supported Application IDs**).	5.0: CPF-23373
CPF-23523	The Hd Diameter interface is now supported as a Diameter Application ID (**Topology > SDC Components > FEP > SDC Components Properties > Diameter > Supported Application IDs**).	5.0: CPF-23522
CPF-23614	Previously, you could only edit the peer list in a pool from an EMS Web UI. Now, the list of peers is also editable from an SDC Web UI (**Topology > Pools > Add > Add Peers > Select peers…/Dynamically add Peers matching Peer Profiles > Up/Down/Remove**).	

3.32.3 Administration

ID	Description	Related ID in Previous Releases
CPF-23413	The User Management mechanism was improved as follows: Web UI users defined as a User can now change their own password (**Traffix user icon> Change Password**). Only Web UI users defined as an Admin/Engineer can set and change the password policy (**Administration > User Management >Preferences**).	
CPF-23508	Previously, the password history (**Administration > User Management > Preferences > Enforce History**) was not enforced if you changed your password more than once per day. Now, even when changing the password more than once per day, the password history is enforced, meaning that the system will allow you to use a previous password after using the defined number (**Administration > User Management > Preferences > Enforce History**) of unique new passwords.	5.0: CPF-22852

3.32.4 Session Repository

ID	Description	Related ID in Previous Releases
CPF-23349	Previously, the time stamp of a message was set by the FEP-In (for the request) and by the FEP-out (for the answer), and when these times were not synchronized (in milliseconds), a message's time stamp was invalid and thereby the message could not be saved as expected in the session repository. Now, a message's time stamp is set only by the CPF, before it is sent to the session repository and there is no longer the possibility of an invalid time stamp	

3.32.5 Monitoring

ID	Description	Related ID in Previous Releases
CPf-23576	NMS Agent log message log levels (such as Warn, Notice , Info) can now be configured, as CPF and FEP logs are, from the Web UI (**Administration > Specific Site Settings > Logging**).	
CPF-23580	Previously, the sdcLicenseMpsViolation alarm was not calculated correctly, Now, it is calculated correctly per second and per each FEP and IP address.	

3.32.6 Web UI

ID	Description	Related ID in Previous Releases
CPF-23657	Previously, when resizing columns in decision tables (such as **Flows > Routing Rules**), and then navigating to another page, upon returning to the page with the resized columns, the decision table rows were no longer displayed, until refreshing the page. Now, resizing decision table columns no longer affects the display of the decision table and the content is displayed as expected.	

3.32.7 Maintenance

ID	Description	Related ID in Previous Releases
Installer-2885	The following fixes for better troubleshooting and easier use were made to the addRoute/delete Route script: ▪ Script logs are now generated on the rsyslog server and are rotated when reaching 10 Mb ▪ An error message is displayed in response to any invalid command syntax ▪ Can use a rounded netmask number instead of the full netmask number	

ID	Description	Related ID in Previous Releases
	▪ Only need to define the IPv6 or IPv4 parameter, depending on which is being used	

3.32.8 Performance

ID	Description	Related ID in Previous Releases
CPF-23436	The Garbage Collector mechanism for the NMS Agent has been upgraded to G1 to improve memory capabilities and performance.	5.0: CPF-23435

3.32.9 Web Services API

ID	Description	Related ID in Previous Releases
CPF-19572	The addOrEditExternalLookup Web Service API command now enables you to add or edit External Lookup items, that was previously only enabled from the Web UI (**Administration > External Lookup Management**).	

3.33 Fixed Bugs in CF 4

This section describes the bugs fixed in Release 5.1, CF 4.

3.33.1 Topology

ID	Description	Related ID in Previous Releases
CPF-23426	The **Broadcast Pool** policy drop-down list is now grayed out, showing Don't Wait, as it is the only supported behavior when a pool is configured as both a Notification and Broadcast Pool (**Topology > Pools > Add**).	
CPF-23557	Previously, after duplicating a selected peer profile in the Peer Profiles table (**Topology > Peer Profiles > Duplicate**), you	

ID	Description	Related ID in Previous Releases
	could not change its name. Now, the peer profile is duplicated with the "peer profile name _copy," which is then editable.	
CPF-23558	Previously, a user with a "User" role was not able to view the contents of rule attribute windows or of the SDC Components, Peers, Pools, Virtual Servers tables, when clicking on **Edit** (**Topology**). Now, for a user with a "User" role, these screens are enabled for viewing, but not editing.	
CPF-23567	Previously, when opening a peer profile script (**Topology > Peer Profiles > Edit > Handshake Scripts**), it was not displayed as expected. Now, peer profile scrips are displayed and editable.	
CPF-23615	The peerSelector.select function (**Topology > Pools > Add/Edit > General > Load Balancing Pool > External**) now works as expected and the message is routed to the destination peer that is defined in the script.	
CPF-23433	Previously, messages routed to a pool configured with an **External** load balancing policy (**Topology > Pools > Add/Edit > General > Load Balancing Pool > External**) mistakenly considered the FEP, and not the remote source peer, as the Origin Host. Now, the remote source peer, is recognized as the Origin Host, and messages are then routed as expected to the destination peer, according to the pool **External** policy script.	
CPF-23434	The Peer Selection script is now editable for pools configured with an External Policy (**Topology > Pools > Edit > Load Balancing Pool > External**).	
CPF-23637	Previously, the Internal Peer Selector Policy drop-down list (**Topology > Pools > Add/Edit > General > Load Balancing Pool > External**) mistakenly showed **External** as one of its options. Now, the drop-down list shows all the other load balancing policies, without **External**.	
CPF-23621	Previously, when configuring Local Breakout for Diameter or SS7 peer profiles (**Topology > Peer Profiles > New/ Edit >**	

ID	Description	Related ID in Previous Releases
	Diameter Configuration/MAP Manipulations > Enable Manipulation Ext-PDP-Type for Roaming-Gr (outbound)), the **IPv6 PLMN List** was limited to entries of more than six characters. Now, the **IPv6 PLMN List** supports entries as long as they have a minimum of three characters.	

3.33.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-23419	The Cluster Nodes Engineering Script tab is now removed from the EMS Web UI (**Administration>Engineering Scripts**) as it is not supported in EMS deployments.	
CPF-23610	Previously, when duplicating a decision table row, the row was added at the bottom of the table. Now, the duplicated row is added below the row that was selected to be duplicated.	

3.33.3 Performance

ID	Description	Related ID in Previous Releases
CPF-23568	Previously, rule attributes defined with the PREFIX Type (**Rule Attributes > Add > Type**), caused the CPF not to start. Now, rule attributes defined with a PREFIX Type work as expected.	

3.34 Fixed Bugs in CF 3

This section describes the bugs fixed in Release 5.1, CF 3.

3.34.1 Topology

ID	Description	Related ID in Previous Releases
CPF-22572	When setting custom values for the Default Transport Configuration (**Administration > Specific Site Settings > Transport Layer->Default Transport Configuration**), the SCTP_MAXSEG (Server & Client) parameter's valid range is now set to 0-65536.	
CPF-23283	Previously, the peer profile name (**Topology > Peer Profiles**) was editable, but not updated in the Peer Profiles Association Rules table. Now, the peer profile name is not editable to ensure a unique system-wide name. *Note: This was a known issue in CF 2.*	

3.34.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-23069	Previously, after deleting a pool from a routing rule pool list (**Flows > Routing Rules > Rule Configuration > Select pool...> Remove**), it continued to be listed in the routing rule Select pool... list. Now, after deleting a pool from a routing rule pool list, the pool no longer is listed in the routing rule **Select pool...** list. *Note: This was a known issue in CF 1.*	
CPF-23184	Routing rule attributes (for example, request.Host-IP-Address) with an OCTET STRING type, no longer adds a "0" to inputted IP addresses under the Attribute column (**Flows > Routing Rules > Rule Attributes**) and routing is now processed as expected. *Note: This was a known issue in CF 2.*	4.4: CPF-23185

3.34.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23044	Previously, Warning log level error messages included the stack trace of the error and line number of the script (in addition to the type of script and the error message) and this impacted the speed of the log generation. Now, for Warning log levels, the generation method has been changed so that only the type of script and the error message are included, and the speed of the log generation is not slowed down.	
CPF-23275	Previously, following an EMS installation, the sdcComponentStatus alarm may have been generated (**Alarms > Active Alarms**) indicating that an NMS Agent is down, even though the NMS Agent was up. Now, the sdcComponentStatus alarm will not be generated when the NMS Agent is up.	

3.34.4 Web UI

ID	Description	Related ID in Previous Releases
CPF-23366	The correct pop-up message now appears, ("There is no selected component, please select one and try again") when selecting Edit in SDC Components, without first selecting a specific component (**Topology > SDC Components > Edit**).	
CPF-23873	In the **Reports** screen, the filter functionality now works as expected, even when entering a number or part of a component name.	

3.34.5 Performance

ID	Description	Related ID in Previous Releases
CPF-23207	Previously, even when the cpfUseSS7 parameter was not selected (false) in the Site Topology file, IWF was enabled,	

ID	Description	Related ID in Previous Releases
	taking up resources. Now, when the cpfUseSS7 is not selected, IWF is not enabled.	
CPF-23369	By improving the validation mechanism of routing rules scripts, there is no longer a system delay after submitting new rows to decision tables and Peer Profile tables. *Note: This was a known issue in CF 2.*	

3.35 Fixed Bugs in CF 2

This section describes the bugs fixed in Release 5.1, CF 2.

3.35.1 Topology

ID	Description	Related ID in Previous Releases
CPF-22955	Previously, an exception was thrown when a non-geo-defined peer tried to connect to a geo--defined virtual server (FEP) (**Topology > Specific Site Settings > Site > Virtual Servers >Add/Edit >Use for Geo Redundant Sites Connection**) and the non-geo-defined peer was unable to connect to the FEP. Now, instead of the exception, the following error log is generated: Peer {0} is rejected. Reason: Regular peer is not allowed to connect to GEO virtual server.	
CPF-22973	As a result of using a different parser for the raw-XML response, the running time for the F5 CLI application is significantly reduced and responses to commands, such as show peers (for 900 peers), is less than ten seconds.	
CPF-23250	Previously, when editing an association rule with a different Dynamic Peer Profile (**Topology > Peer Profiles > Association Rules**), after clicking **Submit**, the association rule was not updated with the newly selected peer profile. Now, edited association rules are updated as expected.	

ID	Description	Related ID in Previous Releases
CPF-23292	The addPeerProfileAssociationColumn Web Services API command now adds a dynamic peer association rules condition, as expected.	

3.35.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-22975	Previously, when Topology Hiding was enabled (**Flows > Flows > <Flow Name> > Routing Rule > Topology Hiding/Diameter Identity**), the Route-Record AVP was not set to the dummy host name, and the actual host name was exposed. Now, the Route-Record AVP is set as expected to the dummy host name when Topology Hiding is enabled.	

3.35.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-22961	Peer related KPI Traffic by bytes' reports are now shown in a separate report screen **Reports > Peers > Traffic by Bytes**.	
CPF-22948	Previously, severity levels for active alarms were incorrectly based on the worse severity level (such as, Critical) per the defined time interval. Now, the severity level is based on the most recently changed severity level, assuming it is not a Cleared state.	
CPF-23040	Previously, in the FEP logs, the SIG_EXECUTION_EXCEPTION ERROR and the LOGGER_MONITOR_RESETTING_LEVEL ERROR logs were not generated with the correct content. Now, these logs are generated as expected.	
CPF-23103	Previously, an audit on an action (**Administration > Audit**) that was performed while one of the server's that hosts one of the	

ID	Description	Related ID in Previous Releases
	configuration managers was down, but after the downed configuration manager was back up and synchronized with the other configuration manager, failed. Now, the audit is performed as expected.	

3.35.4 Web UI

ID	Description	Related ID in Previous Releases
CPF-23173	An SDC user defined as a "user" (and not as an Engineer, Admin, or Expert) can now only view configurations without making any changes, as expected.	
CPF-23177	Previously, SDC users defined as a User (**Administration** > **User Management** > **Roles**), could not view the list of pools (**Topology** > **Specific Site Settings** > <**Site Name**> > **Pools**). Now, such users, with read-only status, can view the list of pools.	
CPF-23204	As a result of a Kendo (third party) limitation, decision table **Label** cell entries (**Rule Attributes** > **Add** > **Label**) cannot start with a number, there is now a validation process that checks if the value starts with a number and if so, an error message (invalid value field) is displayed and the value is not accepted.	

3.35.5 Maintenance

ID	Description	Related ID in Previous Releases
Installer-2534	Previously, the AddRoute API did not succeed if a value was defined for the "ip6" attribute for the interface the route would use. Now, the AddRoute API works as expected when the "ip6" attribute is populated.	

ID	Description	Related ID in Previous Releases
Installer - 2852	Previously, the showRoutes API request did not return the expected information (such as, name, interface, network) for the relevant server. Now, this API request generates the answer with the expected information.	

3.35.6 Performance

ID	Description	Related ID in Previous Releases
CPF-22723	Previously, when changing a row in a decision table containing more than a few hundred routing rows, the system experienced high latency and timeouts. Now, changes to decision tables with up to 1000 routing rules are processed without causing timeouts and high latency. *Note: This was a known issue in CF 0.*	

3.36 Fixed Bugs in CF 1

This section describes the bugs fixed in Release 5.1, CF 1.

3.36.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2753	The Splunk License Usage page (Monitoring) is now enabled and Splunk related daily alarms are now generated as expected.	5.0: Installer-2810
Installer-2819	Previously, when performing a CLI upgrade, the upgrade process was completed, even when required upgrade information was missing. Now, the CLI upgrade will present an error message and stop the upgrade process when upgrade information is missing.	5.0: Installer-2818

3.36.2 Topology

ID	Description	Related ID in Previous Releases
CPF-19304	Previously, HTTP peers remained as Open (**Topology > Peers >Status**), even when they could not handle traffic. Now, the HTTP peers state is reflected correctly as Open or Closed, according to their traffic processing capabilities.	4.4: CPF-17447 5.0: CPF-18595
CPF-22197	When a site's EMS configuration managers are shut down, they now show as Disconnected, as expected, in the local Web UI (**Topology > SDC Components > Site External Connections**).	
CPF-22594	Previously, the RADIUS peer Status may have shown as Closed (**Topology > Peers > Status**) even when traffic was running. Now, the RADIUS peer status is displayed as expected.	
CPF-22773	Previously, retrieval time of a pool list, using the getListFromPools Web Service API command from the CLI Application, was sometimes longer than expected. Now, using the getListFromPools Web Service API command from the CLI Application, retrieves a pool list in a timely manner.	5.0: CPF-22659
CPF-22791	Previously, when a client peer was assigned to a peer profile with Set as Server Peer (**Topology > Peer Profile > Dynamic Peer Profiles > General > Set a Server Peer**), the client peer would not re-connect as expected to the SDC. Now, a client peer assigned to a peer profile with Set as Server Peer will re-connect as expected.	5.0: CPF-22744
CPF-22831	Previously, an SDC component that was hosted on a downed server continued to display as Up (**Topology>SDC Components>Status**) for a few minutes. Now, the component shows as Closed, as expected, when its host server is down.	
CPF-22881	Previously, when configuring a pool, the Web UI mistakenly allowed users to define the pool with Message Prioritization enabled (**Topology > Pools > Add > Activate message prioritization upon approaching overload control criteria**) and as a Notification Pool (**Topology > Pools > Add >**	

ID	Description	Related ID in Previous Releases
	Notification Pools). Now, when adding or editing a pool and you select the **Activate message prioritization upon approaching overload control criteria** checkbox, the **Notification Pools** checkbox is grayed out. *Note: This was a known issue in CF 0.*	
CPF-22883	Previously, a pool's status may have shown as Limited (**Topology > Pools > Status**) even though its connection status to all CPFs was Out of Service. Now, the status of such a pool shows, as expected, as Closed. *Note: This was a known issue in CF 0.*	
CPF-22908	Previously, when dynamic peers were assigned to a pool according to their peer profile (**Topology > Pools> <Pool Name> > Edit > Dynamically add Peers matching the following Peer Profile(s)**), the peer was not always assigned to the correct pool. Now a monitoring thread has been added to ensure that dynamic peers are assigned to the correct pool based on their peer profile.	5.0: CPF--22907
CPF-23054	Previously, when adding to or removing peers from a pool with the addPeerToPool or removePeerFromPool Web Service API commands, all peers that were associated with the added or removed peer's dynamic peer profiles were mistakenly deleted from the pool. Now, the addPeerToPool or removePeerFromPool Web Service API commands only affect the selected peer.	
CPF-23058	Previously, upon saving a peer profile with a Name (**Topology > Peer Profiles > Add**) that included special characters that are not XML compliant, an error message was displayed. The peer profile was created and listed in the peer profiles table. Now, if the name of the peer profile is not validated it will not be added.	
CPF-23082	Previously, when removing a peer profile column rule value from a peer profile rule (**Topology > Peer Profiles > Association Rules**), the SDC was not configured to recognize an empty	

ID	Description	Related ID in Previous Releases
	value and attempted to parse the value, causing errors in the FEP and CPF. Now, the SDC is configured to check the field for empty, as well as, null values, and when found, no longer continues to parse the value, and the errors are no longer generated.	

3.36.3 Web UI

ID	Description	Related ID in Previous Releases
CPF-22654	Now, when selecting the general checkbox in the Peers or Virtual Servers table (**Topology**), all table rows are also selected, as expected. *Note: This was a known issue in CF 0.*	
CPF-22743	Previously,the Keep Alive mechanism to maintain a persistent HTTP connection could not be enabled in the Web UI even though the Keep Alive checkbox (**Topology > Specific Site Settings > <Site Name>> Peers>Add>Protocol>HTTP>General**) can be selected. Now, the Keep Alive mechanism can be enabled and disabled by selecting and unselecting the checkbox.	
CPF-22934	Previously, after executing the monit stop command for all components all connected SDC components showed, as expected, as Down, except the Web UI which showed, incorrectly, as Up (**Topology > SDC Components > Site Components**). Now, the status update mechanism in Cassandra and the OAM is corrected so that the status of all SDC Components, including the Web UI, are correctly displayed.	5.0: CPF-22239

3.36.4 Flow Management

ID	Description	Related ID in Previous Releases
CPF-22664	When adding a rule attribute, a Framed-IP-Address attribute now supports LIST **Filter Type**s.	5.0: CPF-22681
CPF-22886	Previously, pools configured as notification pools were mistakenly listed as an option under **(Flows > Flows > <Flow Name> > Routing Rules > Routing Rule Configuration** > **Select pool**). Now, pools configured as notification pools are no longer listed as an option for routing. *Note: This was a known issue in CF 0.*	
CPf-22889	Previously, notification pools assigned to a routing row **(Flows > Flows > <Flow Name> > Routing Rules > Routing Rule Configuration**), could be removed (**Topology >Pools >Remove**) without any error or warning message. Now, when trying to remove a notification pool that has been assigned to a routing row, a warning message about dependencies is displayed and the selected pools are not removed. *Note: This was a known issue in CF 0.*	
CPF-22906	Due to a change in the code, the SDC failed to reroute messages to a second peer in another pool when their routing rules were configured with a reroute rule attribute. Now, the code was modified so that the SDC recognizes a true flag that is sent from the Handle Server Error Script (**Flows > Flows > <Flow Name> > Routing Rules > Handle Errors**) so that messages are successfully rerouted in the event that they are returned with an error or timeout from their initial routing flow.	5.0: CPF-22928

3.36.5 Administration

ID	Description	Related ID in Previous Releases
CPF-22869	Previously, when importing an Attribute List (**Administration> Attribute List>Add>Import Items From File**), list items written with commas in the CSV import file were separated and displayed in different rows in the Attribute List Item table. Now, imported CSV files display as expected in the Attribute List Item table. *Note: This was a known issue in CF 0.*	5.0:22852

3.36.6 Monitoring

ID	Description	Related ID in Previous Releases
CPF-21155	Previously, the Routing ID that the message matched was not included in the information displayed for traced messages in the **Reports > TDRs > Traced Messages** screen. Now, the Routing ID is included, as expected.	5.0: CPF-21122
CPF-22541	The splunkLicenseViolation is now generated, as expected, on a daily basis and not more often.	
CPF-22833	Previously after applying a script with the userTraceLogger parameter, the CPF log was not correctly diluted by class level. Now, the CPF log is diluted as executed by class level after applying a script with the userTraceLogger parameter.	4.0: CPF-22830
CPF-22946	As a result of an earlier related bug fix, that changed the way statistics were collected for TTA reports, the TTA occasionally stopped generating reports when there were many (over 20,000 per night run) collected statistics. Now, the bash interpreter has been amended to be able to process a large number of collected statistics and TTA reports are generated as expected.	5.0: CPF- 22943

3.36.7 Performance

ID	Description	Related ID in Previous Releases
CPF-22962	Previously, the CPF used a CMS Collector for garbage collection (GC), which was less efficient and may have impacted performance. Now, the CPF has been configured to use the G1 Collector for efficient GC and improved SDC performance. *Note: Any server hosting a CPF requires an additional 1GB to support the G1 Collector.*	5.0: CPF-22958

4. Known Issues

This section describes the known issues that are included in Release 5.1.

4.1 Known Issues in CF 22-35

There were no new known issues detected in Release 5.1, CF 22-CF35.

4.2 Known Issues in CF 21

This section describes the known issues that are included in Release 5.1, CF 21.

4.2.1 Topology

ID	Description	Related ID in Previous Releases
CPF-25044	When applying the addRoute/deleteRoute script with the CLI, both IPv4 and IPv6 are supported. When applying the addRoute/deleteRoute script with the /*tmp/input file*, IPv4 is supported.	

4.3 Known Issues in CF 20

There were no new known issues detected in Release 5.1, CF 20.

4.4 Known Issues in CF 19

There were no new known issues detected in Release 5.1, CF 19.

4.5 Known Issues in CF 18

There were no new known issues detected in Release 5.1, CF 18.

4.6 Known Issues in CF 17

This section describes the known issues that are included in Release 5.1, CF 17.

4.6.1 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24884	When configuring the splunk application, in the site topology XML file, with an uppercase "S", the splunk indexer log rotation mechanism does not work as it is configured to recognize lowercase letters. Workaround: To avoid case sensitivity for a defined splunk application, replace the following in /srv/salt/<version>/system/logrotate/logrotate-traffix.conf: /var/log/rsyslog/*.splunk*.log to /var/log/rsyslog/*.*plunk*.log *Note: This issue was fixed in CF-23.*	

4.7 Known Issues in CF 16

There were no new known issues detected in Release 5.1, CF 16.

4.8 Known Issues in CF 15

This section describes the known issues that are included in Release 5.1, CF 15.

4.8.1 Maintenance

ID	Description	Related ID in Previous Releases
CPF-24819	When running the addRoute API script, an incorrect IP address in the site topology file interface parameter is not fully validated, yet the IP address is mistakenly added to the topology and Cassandra database. *Note: This issue is fixed in CF-17.*	

4.9 Issues in CF 14

There were no new known issues detected in Release 5.1, CF 14.

4.10 Known Issues in CF 13

This section describes the known issues that are included in Release 5.1, CF 13.

4.10.1 Web UI

ID	Description	Related ID in Previous Releases
CPF-24720	When multiple browsers are opened to access the SDC Web UI, submitted changes made on one browser can be overwritten if the same Web UI page is concurrently opened in another browser, as only the changes made in the second browser are saved, without any alert message. *Note: This issue is fixed in CF -14.*	

4.11 Known Issues in CF 12

There were no new known issues detected in Release 5.1, CF 12.

4.12 Known Issues in CF 11

This section describes the known issues that are included in Release 5.1, CF 11.

4.12.1 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24659	In **Reports** >**Transaction Data Records**, some of a message's AVP values might not be displayed as expected even though they are reflected in the Splunk database.	

4.13 Known Issues in CF 10

This section describes the known issues that are included in Release 5.1, CF 10.

4.13.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-3037	The split mirror process, a system validation prerequisite done prior to performing an upgrade for a Bare Metal site, yields the following error "Minions returned with non-zero exit code" even when there are no minion servers in the site and the split mirror process is successfully completed.	

4.13.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-24526	When selecting **Leave** to the Leave Page prompt after changing a configuration without submitting the change, the Web UI does not always change to a new menu tab page. Workaround: To switch to a different menu tab page, refresh the Web UI and log in. *Note: This issue is fixed in CF 11.*	
CPF-24538	When selecting **Stay** to the Leave Page prompt after changing a configuration without submitting the change, a different menu tab is highlighted than the displayed Web UI page. Workaround: To switch to a different tab menu page, refresh the Web UI.	

4.13.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23989	Following a new installation or rolling upgrade, the sdcComponentStatus alarm for the NMS Agent may be generated with the message that the component is down, even though the NMS Agent component is up and running.	

ID	Description	Related ID in Previous Releases
	Note: In CF- 12, this issue is fixed and documented in CPF-24663.	

4.14 Known Issues in CF 9

This section describes the known issues that are included in Release 5.1, CF 9.

4.14.1 Topology

ID	Description	Related ID in Previous Releases
Installer-3027	When adding CPF components (with scaling out API command) to a virtual deployment, they may appear with the wrong names in the Web UI (**Alarms** > **Active Alarms** >**Affected Object Name**) and CPF logs.	

4.14.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-24307	The Event Type filter option in the **Alarms** >**Active Alarm**s table does not display any expected filter options.	
CPF-24322	When reloading a page in the Web UI (CTRL-F5), after adding an SNMPv3 Profile (**Administration** > **SNMP** > **Add**), the Web UI may show the following error " Failed to retrieve SNMP dilution values" in some screens. *Note: This issue is fixed in CF 10.*	

4.14.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24291	In the **Reports** > **TDRs** Screen, there is no option to show the filter after selecting **Hide Filter**.	

ID	Description	Related ID in Previous Releases
	Note: This issue is fixed in CF 10.	
CPF-24296	Active alarms (sdcComponentStatus) continue to be generated (in **Alarms** > **Active Alarms**) for a CPF component even once it has been removed with a scale-in API request. *Note: This issue is fixed in CF 12.*	
CPF-24272	When opening Splunk from a Chrome browser, you may not be able to initially view the Splunk reports for TDRs, Traced Messages and Splunk License Usage (in the **Reports** screen). To view these reports, open the second EMS Web UI (**Reports** screen). *Note: This issue is fixed in CF 10.*	
CPF-24418	After performing an EMS rolling upgrade, the sdcComponentStatus alarm for the configuration manager may not be cleared (**Alarms** > **Active Alarms**), even though the configuration manager is up and running. *Note: In 5.1 CF- 12, this issue is fixed and documented in CPF-24663.*	
CPF-24428	During a rolling upgrade, TTA config and bin logs for SDC components from the previous version that have not yet been upgraded, are not generated as expected after a failed rolling upgrade	

4.15 Known Issues in CF 8

This section describes the known issues that are included in Release 5.1, CF 8.

4.15.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-3013	While performing a rolling upgrade, an automatic run of Cassandra repair causes the upgrade to fail. Workaround: Restart the upgrade process, with running the **resume** command. *Note: This issue is fixed in CF 12.*	
CPF-24118	After performing a rolling upgrade, following the monit restart procedure, some minion environments (SDC components) may not be upgraded as expected. *Note: This issue is fixed in CF 9.*	

4.16 Known Issues in CF 7

This section describes the known issues that are included in Release 5.1, CF 7.

4.16.1 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23918	The sdcComponentStatus alarm may not always be cleared when the configuration manager is back up. Workaround: Restart the configuration manager. *Note: In 5.1 CF-12, this issue is fixed and documented in CPF-24663.*	

4.17 Known Issues in CF 6

This section describes the known issues that are included in Release 5.1, CF 6.

4.17.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2801	Previously, the applicationInstance name in the site topology file was limited to 32 characters to avoid problems in the rsyslog system. Now, the related syslog tag is no longer limited to 32 characters, allowing for longer applicationInstance names in the site topology file. *Note: This was detected as a known issue in CF 0.*	
Installer-2991	Bond Eth parameters configured in the site topology file are not validated as expected. *Note: This issue is fixed in CF 10.*	
CPF-23914	Following a new installation or after restarting Tomcat services, not all the **Dashboard** screen data is immediately uploaded and displayed. Workaround: Refresh the Web UI or select a different screen tab and then return to the **Dashboard** screen.	

4.17.2 Maintenance

ID	Description	Related ID in Previous Releases
CPF-23814	The following issues were found when applying the addRoute/delete Route script and addRoute API: ▪ When deleting a route, the same subnet mask IP value must be used as was included in the addRoute script or addRoute API.	
CPF-23819	▪ In the case that the addRoute script or AddRoute API fails at the end of the Linux platform process after adding a route with the same interface, but a different name, no error logs are generated in the route logs as there is no Linux validation mechanism to check the added route names.	

ID	Description	Related ID in Previous Releases
	Note: This issue is fixed in CF 10.	
CPF-23838	▪ When running the addroute script or the addRoute API, the pillar (the dynamic component managed by Salt) may be missing vipInterfaces, causing the action to fail. Workaround: Refer to the F5 SDC 5.1 Troubleshooting Guide.	
CPF-23839	▪ Manually added/deleted routes are not applied to any machines that are added after the initial installation. *Note: This issue is fixed in CF 9.*	

4.17.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23910	When performing a rolling upgrade, the following TDR error message may appear in the NMS, Configuration Manger and Tomcat logs: "ERROR [] GET/SET_CREATE_TDR doesn't have a value in logDescriptions.txt [http-nio-8080-exec-14_74248] [LoggingEnum.load()]," without any impact on TDR generation. *Note: This issue is fixed in CF 7.*	

4.17.4 Web UI

ID	Description	Related ID in Previous Releases
	The following Web UI issues were found in this release:	
CPF-23813	▪ The SDC Success and Error pie charts (**Reports**) percentages are not displayed clearly.	
CPF-23817	▪ The true/false option in **Administration > SNMP > SNMP Settings > Sent to SNMP Targets** is not user-friendly.	

ID	Description	Related ID in Previous Releases
CPF-23831	▪ Invalid values are saved in the **Administration >Transport Layer** fields even though a message is displayed regarding the acceptable range of values. Workaround: Click **Refresh** for the OS, default value, to repopulate the field.	
CPF-23834	▪ After selecting a FEP component from the **Reports > Summary > All** drop-down list, the full FEP name will not display when it is long (more than 18 characters).	
CPF-23841	▪ Log Level changes made in an EMS Web UI (**Administration > Logging > Log Levels**) are not saved, after clicking **Refresh**.	
CPF-23888	▪ When using Firefox or Internet Explorer, you can only manually edit the user expiration date (**Administration > User Management > Edit User > Set user expiration date**), without selecting from the drop-down calendar.	

4.18 Known Issues in CF 5

This section describes the known issues that are included in Release 5.1, CF 5.

4.18.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-23708	While performing an upgrade from Release 4.4 to 5.1, and the system is in mix-mode, log level and syslog configuration changes (**Administration > Logging >Log Levels/Syslog Addresses**) made to an EMS site (upgraded to 5.1) are not applied to the relevant 4.4 sites. Once the upgrade is completed, configuration changes are applied as expected.	
CPF-23712	While performing an upgrade from Release 4.4 to 5.1, and the system is in mix-mode, logs are not generated	

ID	Description	Related ID in Previous Releases
	as expected for the 4.4 sites. Once the upgrade is completed, logs are generated as expected.	

4.18.2 Topology

ID	Description	Related ID in Previous Releases
Installer-2962	When adding a route (by API or by script), and both the management and signaling networks are defined as IPV4 and one of the network fails, instead of failing over to a secondary channel on the failed network, traffic is rerouted to the other network. *Note: This issue is fixed in CF 6.*	
CPF-23703	When configuring, from an EMS Web UI, the transport layer globally (**Administration><site>>Transport Layer**) for a site, the SDC Component drop-down lists all FEP components for all the sites, instead of those only relevant for the selected site. Workaround: Refresh the browser and then the relevant site FEP components are displayed.	

4.18.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23706	Changes made to log levels (**Administration > Logging > Log Levels**) for one site are applied to all the other environment sites. *Note: This issue is fixed in CF 6.*	
CPF-23707	Changes made to the Syslog address (**Administration > Logging > Syslog Addresses**) for one site are applied to all the other environment sites.	

ID	Description	Related ID in Previous Releases
	Note: This issue is fixed in CF 6.	

4.18.4 Web UI

ID	Description	Related ID in Previous Releases
CPF-23713	Some screenshot images in the Online Help do not display as expected. *Note: This issue is fixed in CF 6.*	5.1 CF 4: CPF-23666

4.19 Known Issues in CF 4

This section describes the known issues that are included in Release 5.1, CF 4.

4.19.1 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23605	While a peer will show as reconnected in the NMS logs after being reconnected and after the Cassandra (oamDB) is restarted, the PeerStateChanged cleared alarm is not sent (Alarms > Active Alarms) and the peer continues to show as having a Closed status (**Topology > Specific Site Settings > <Site Name>> Peers > Status**).	

4.20 Known Issues in CF 3

This section describes the known issues that are included in Release 5.1, CF 3.

4.20.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-23415	After an EMS installation the nmsagent1-stdout.log may show a NullPointer Exception, even though the installation was completed successfully.	

ID	Description	Related ID in Previous Releases
CPF-23469	In the event that an upgrade (to release 5.1) fails on one SDC site, the rollback to release 4.4 must be performed on all SDC and EMS sites. *Note: This issue is fixed in CF5.*	

4.20.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-23421	When removing pools from the Rule Configuration Select pool... table (**Flows > Routing Rules**) and moving to another screen, without clicking **Submit**, no warning pop-up message, asking if you want to leave the page and that changes will not be saved, appears.	5.0: CPF-19732

4.20.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23406	The description of the ratio between the Operating System's load average counter and the number of CPU cores for the machineLoadAverage alarm (**Alarms >Alarm History Log > Event**) is not clear.	

4.21 Known Issues in CF 2

This section describes the known issues that are included in Release 5.1, CF 2.

4.21.1 Topology

ID	Description	Related ID in Previous Releases
CPF-23283	When editing the name of a peer profile (**Topology > Peer Profiles > Edit**) that was previously assigned to a Peer	

ID	Description	Related ID in Previous Releases
	Profiles Association Rules, the new peer profile name is not updated in the Peer Profiles Association Rules table. *Note: This issue is fixed in CF 3.*	

4.21.2 Flow Management

ID	Description	Related ID in Previous Releases
CPF-23184	Routing rule attributes (for example, request.Host-IP-Address) with an OCTET STRING type, mistakenly adds a "0" to inputted IP addresses under the Attribute column (**Flows > Routing Rules > Rule Attributes**) and routing is not processed as expected. *Note: This issue is fixed in CF 3.*	4.4: CPF-23185

4.21.3 Monitoring

ID	Description	Related ID in Previous Releases
CPF-23275	Following an EMS installation, the sdcComponentStatus alarm may be generated (**Alarms > Active Alarms**) indicating that an NMS Agent is down, even though the NMS Agent is up. *Note: This issue is fixed in CF 3.*	

4.21.4 Performance

ID	Description	Related ID in Previous Releases
CPF-23369	The system may take time (up to a few minutes), depending on the amount of table rows, to update after submitting new rows to decision tables and Peer Profile tables. The SDC Web UI will display a spinning wait cursor while the system is being updated. *Note: This issue is fixed in CF 3.*	

4.22 Known Issues in CF 1

This section describes the known issues that are included in Release 5.1, CF 1.

4.22.1 Web UI

ID	Description	Related ID in Previous Releases
CPF-23068	After removing a dynamic peer from a pool (**Topology > Pools > Edit > Dynamically add Peers matching Peer Profile(s) > Select peer profile…> Remove**), the peers associated with the removed peer profile are still listed under the Peers column for the pool (**Topology > Pools**). *Note: This issue is fixed in CF 6.*	
CPF-23080	After submitting a Session Life-Cycle Script (**Flows> Session Management > Session Life-Cycle Scripts > Submit**), a Leave Page pop-up message is displayed stating that "Changes you made may not be saved" even though the changes were successfully submitted.	

4.22.2 Topology

ID	Description	Related ID in Previous Releases
CPF-23083	When an HTTP peer is closed from the server side, the status of the peer shows as Open, instead of Closed, (**Topology > Peers > Status**) as expected when there is no current connection to the SDC.	
CPF-23090; CPF-19541	After performing an upgrade from release 4.4 to 5.1, the EMS Web UI shows SDC site components Status as Down, even though they are connected (**Topology > SDC Components > Status**). Also, when SDC site components are down, they mistakenly show as Up in the EMS Web UI. Workaround: Restart the EMS NMS server.	

4.22.3 Flow Management

ID	Description	Related ID in Previous Releases
CPF-23069	After deleting a pool from a routing rule pool list (**Flows > Routing Rules > Rule Configuration > Select pool...> Remove**), it continues to be listed in the routing rule **Select pool...** list. *Note: This issue is fixed in CF 3.*	

4.22.4 Administration

ID	Description	Related ID in Previous Releases
CPF-23077	Items in an imported attribute lists from a CSV file (**Administration > Attribute Lists > Add > Import Items from File**) may be displayed in a different order (Date and Time) than were in the original CSV file.	

4.22.5 Performance

ID	Description	Related ID in Previous Releases
CPF-22723	When changing a row in a decision table containing more than a few hundred routing rows, the system experiences high latency since the CPF is busy committing the change and not implementing the routing rules. *Note: This issue is fixed in CF 2.*	

4.23 Known Issues in CF 0

This section describes the known issues that are included in Release 5.1, CF 0.

4.23.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2801	The applicationInstance name in the site topology file should not exceed 32 characters to avoid problems in the rsyslog system. *Note: This issue is fixed in CF 6.*	

4.23.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-19541	In an EMS deployment, when all applications are down on a local SDC site components in the EMS Web UI is erroneously displayed as up (**Topology>SDC site>SDC Components**).	5.0: CPF-19732
CPF-22654	The general check box used to select all items in the Peers table will remain selected following a **Submit** action. All table rows will be unchecked following the action. *Note: This issue is fixed in CF 1.*	

4.23.3 Topology

ID	Description	Related ID in Previous Releases
CPF-21659	When two Access Control List Rules (Topology>Access Control List) are configured with the same IP address and the first one is configured to Reject the client peer and the second rule is configured to Accept the client peer, the SDC continues to check for matching IP addresses with an Accept Action even after matching a Reject Action.	
CPF-22101	As a Virtual Server (FEP) tries to connect to a peer, its Status perpetually changes back and forth from Connecting to Closed, invoking a refresh of the screen information. Workaround: Disable the auto-refresh.	

ID	Description	Related ID in Previous Releases
CPF-22881	When configuring a pool, the Web UI mistakenly allows users to define the pool with Message Prioritization enabled (**Topology > Pools > Add > Activate message prioritization upon approaching overload control criteria**) and then to define the pool as a Notification Pool (**Topology > Pools > Add > Notification Pools**). *Note: This issue is fixed in CF 1.*	
CPF-22883	A pool's status may show as Limited (Topology > Pools > Status) even though its connection status to all CPFs is Out of Service. *Note: This issue is fixed in CF 1.*	

4.23.4 Flow Management

ID	Description	Related ID in Previous Releases
CPF-22319	On Session Update Scripts, in addition to On Session Create scripts, are mistakenly invoked for new sessions.	
CPF-22886	Pools configured as notification pools are mistakenly listed as an option under **Flows > Flows > <Flow Name>>Routing Rules > Rule Configuration > Select pool.** *Note: This issue is fixed in CF 1.*	
CPF-22889	Notification pools assigned to a routing row, can be removed without any error or warning message. *Note: This issue is fixed in CF 1.*	

4.23.5 Monitoring

ID	Description	Related ID in Previous Releases
CPF-18588	Wifi Offload statistics, with answers types (rad_peer) that are returned to a RADIUS client peer are generated in the statistics log, but are not displayed in the Web UI.	
CPF-19540	When the sdcComponentStatus alarm is raised for a Splunk component, the affectedObjectType is sent as "machine" instead of "Splunk".	5.0: CPF-19427
CPF-22885	A pool 's health continues to show as Poor (Topology > Pools > Health) even after the sdcPoolRateChanged alarm has been cleared.	

4.23.6 Administration

ID	Description	Related ID in Previous Releases
CPF-22739	Currently, there is no authentication mechanism for accessing the OAMDB.	5.0: CPF-18198
CPF-22869	When importing an Attribute List (**Administration> Attribute List>Add>Import Items From File**), list items written with commas in the CSV import file are separated and displayed in different rows in the Attribute List Item table. *Note: This issue is fixed in CF 1.*	

5. Limitations

This section describes the limitations that are included in Release 5.1.

5.1 Limitations in CF 31- CF 35

No new limitations were detected in Release 5.1, CF 31- CF 35.

5.2 Limitations in CF 30

ID	Description	Related ID
CPF- 25221	The TLS configuration code was only modified for Pre Capabilities to include SCTP related information (such as the protocol ID), so that SSL messages are processed by the FEP as expected. Post Capabilities Exchange TLS for SCTP related information is not supported.	SDC-267

5.3 Limitations in CF 25 - CF 29

No new limitations were detected in Release 5.1, CF 25 – CF 30

5.4 Limitations in CF 24

ID	Description	Related ID in Previous Releases
CPF- 25124	When creating a client peer (**Topology > Specific Site Settings > <Site Name>> Peers**), the peer name must be unique, even to any previously deleted server peers. If a client peer is accidentally created with the same name that was used previously for a deleted server peer, there will be synchronization problems upon restarting the SDC components. To solve this issue, see the Signaling Delivery Controller Troubleshooting Guide, Configuring Peers.	

5.5 Limitations in CF 23

No new limitations were detected in Release 5.1, CF 23.

5.6 Limitations in CF 22

This section describes the limitations that were detected in Release 5.1, CF 22.

5.6.1 Flow Management

ID	Description	Related ID in Previous Releases
CPF- 25056	*Note: This issue is fixed in CF- 22, but with the following limitation:* When making changes to both **Pre-Routing** or **Post-Routing** transformation scripts (**Flows** > **Flows <Flows Name>** > **Transformation**, once you select **Submit**, only the configuration changes that appear under the specific open tab (**Pre-Routing**/ **Post-Routing**) are saved (and viewable) and any previously configured changes made in the other tab are not viewable nor saved.	

5.7 Limitations in CF 21

No new limitations were detected in Release 5.1, CF 21.

5.8 Limitations in CF 20

No new limitations were detected in Release 5.1, CF 20.

5.9 Limitations in CF 19

No new limitations were detected in Release 5.1, CF 19.

5.10 Limitations in CF 18

No new limitations were detected in Release 5.1, CF 18.

5.11 Limitations in CF 17

No new limitations were detected in Release 5.1, CF 17.

5.12 Limitations in CF 16

This section describes the limitations that were detected in Release 5.1, CF 16.

5.12.1 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24863	After a new installation, a geoSdcProxyConnection alarm is not cleared, after an initial fail-over when the SDC site is connected again to its geo-redundant SDC site. After an initial fail-over and alarm generation, the alarm is cleared as expected (CPF-24811). Workaround: Go to **Alarms >Alarm History Log** and select **More** for the relevant alarm. Based on the source peer that is shown under **More**, go to **Topology > Specific Site Settings > <Site Name>> Peers** table and select the source peer and then **Disable** and then **Enable**.	

5.13 Limitations in CF 15

No new limitations were detected in Release 5.1, CF 15.

5.14 Limitations in CF 14

No new limitations were detected in Release 5.1, CF 14.

5.15 Limitations in CF 13

No new limitations were detected in Release 5.1, CF 13.

5.16 Limitations in CF 12

This section describes the limitations that were detected in Release 5.1, CF 12.

5.16.1 Web UI

ID	Description	Related ID in Previous Releases
CPF-24688	When using keyboard navigation, after entering a page number and the Web UI displays the selected page, the focus remains on the selected page (the first highlighted row) and not on the Page number field.	

5.17 Limitations in CF 11

No new limitations were detected in Release 5.1, CF 11.

5.18 Limitations in CF 10

This section describes the limitations that were detected in Release 5.1, CF 10.

5.18.1 Monitoring

ID	Description	Related ID in Previous Releases
CPF-24292	In the **Reports >TDRs** screen, there is no option to scroll left to right per table.	

5.19 Limitations in CF 9

No new limitations were detected in Release 5.1, CF 9.

5.20 Limitations in CF 8

No new limitations were detected in Release 5.1, CF 8.

5.21 Limitations in CF 7

This section describes the limitations that were detected in Release 5.1, CF 7.

5.21.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-23696	While performing an upgrade from Release 4.4 to 5.1, and the system is in mix-mode, the following log exception may be generated: "UnrecognizedPropertyException: Unrecognized field "Comment,"" with no impact on the upgrade process.	

5.22 Limitations in CF 6

No new limitations were detected in Release 5.1, CF 6.

5.23 Limitations in CF 5

No new limitations were detected in Release 5.1, CF 5.

5.24 Limitations in CF 4

No new limitations were detected in Release 5.1, CF 4.

5.25 Limitations in CF 3

No new limitations were detected in Release 5.1, CF 3.

5.26 Limitations in CF 2

This section describes the limitations that were detected in Release 5.1, CF 2.

5.26.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
CPF-23372	When upgrading from Release 4.4 to Release 5.1, the **TC Timer** parameter (**Topology > Specific Site Settings > Site> SDC Components or Topology >Remote Peers**) cannot be defined as more than 30,000 milliseconds. If it is, then the **Reestablish Connection Time** parameter in 5.1 (Topology >SDC	

ID	Description	Related ID in Previous Releases
	Components/Peers) cannot be validated and any other edits to the SDC Component Properties cannot be saved. Workaround: After the upgrade, manually edit the Reestablish Connection Time parameter to a value between 1-30,000 milliseconds.	

5.27 Limitations in CF 1

No new limitations were detected in Release 5.1, CF 1.

5.28 Limitations in CF 0

This section describes the limitations that were detected in Release 5.1, CF 0.

5.28.1 Installation and Upgrade

ID	Description	Related ID in Previous Releases
Installer-2769	The user cannot change the installation directory.	5.0: Installer-1999
CPF-21746	Splunk data (TDR and Traced Messages) that is collected during a site upgrade from SDC 4.4 to SDC 5.1 is not perpetuated.	
CPF-22690	As part of an upgrade from release 4.4 to release 5.1, after manually copying Splunk TDRs and Traced Messages data, site data that was stored locally cannot be retrieved.	5.0: CPF-21748
CPF-22695	The semicolon (";") syntax is not supported in XML Topology files or API requests. As a result, when multiple values for parameters are included, they are not validated and the installation process cannot be completed.This limitation also affects the siteProperties' parameters attribute for defined log servers, which sets which events are sent to the syslog server, according to source facility	5.0: CPF-20105

ID	Description	Related ID in Previous Releases
	and event security. The default value for this attribute ("*.*") is used and all events are sent to the syslog server.	
CPF-22712	The NMS Agent SNMP listen port is now 1161 instead of 161.	5.0: CPF-19550
CPF-22713	An upgraded EMS Web UI displays a value of "unknown" for the affectedObject and affectObjectType fields in traps sent from a SDC site that has not yet been upgraded to 5.1.	5.0: CPF-19632

5.28.2 Web UI

ID	Description	Related ID in Previous Releases
CPF-19759	After installing an SDC site to an existing EMS deployment, there is a 5 minute delay in the EMS Web UI, during which the decision table rules are not displayed and cannot be edited.	5.0: CPF-19690
CPF-21882	When using Keyboard Navigation to navigate through the Web UI, the focus on a selected tab or Web UI object may not be clearly marked on the Menu Bar.	
CPF-22714	To achieve EMS high availability for TDR and Traced Messages, the EMS site must contain at least three machines, where each machine contains the following (running) software modules: ▪ Splunk Indexer ▪ Splunk Master ▪ Splunk Search Head	
CPF-22715	The EMS Web UI displays TDR and Tracing data as expected when up to four concurrent sessions are open.	

5.28.3 Topology

ID	Description	Related ID in Previous Releases
CPF-20191	The File Server protocol is not supported on virtual and bare metal deployments.	
CPF-21430	When Peer Ramp Up is not configured, the simultaneous connection of 1200 peers may take up to one minute.	
CPF-22698	The pool rate limit is not dynamically updated between active CPFs once initially configured. Therefore, if one of the CPFs connected to the pool is stopped, the pool capacity will decrease according to the rate limit defined for the CPF.	5.0: CPF-18008
CPF-22699	When upgrading an EMS site and you have not yet upgraded all the local SDC sites, when deleting a Peer Profile from the EMS, a WARN message is generated in the FEP and CPF logs. There is no user impact.	5.0: CPF-18569
CPF-22718	Peer name length is limited to 255 characters.	5.0: CPF-17422; 4.4: CPF-15706
CPF-22717	The SDC only supports up to ten FEP applications.	5.0: CPF-11108
CPF-22719	When there is no connection to the EMS, you cannot add or remove a FEP or CPF component to one of the managed SDC sites.	5.0: CPF-19551
CPF-22720	Running the “monit stop all” command to stop all processes causes errors and is not supported. Workaround: To start or stop SDC applications, run the following script: /opt/traffix/scripts/trafficApps.sh start/stop	5.0: CPF-18408
CPF-22725	Disabled dynamic client peers may reconnect to the SDC. 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	5.0: CPF-19901; 4.4: CPF-10383

ID	Description	Related ID in Previous Releases
	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.	

5.28.4 Flow Management

ID	Description	Related ID in Previous Releases
CPF-6072	The CPF may fail if an invalid script is used in External Lookup Management.	5.0: CPF-19906
CPF-21857	The "Name" of a rule attribute with a SCRIPT type cannot be any of the pre-defined property names for decision tables. For a detailed list, see the Decision Table Rule Attributes section in the SDC User Guide.	
CPF-22412	Messages with long sesssionIDs (longer than 1024 bytes) are not processed and use up a lot of memory resources while waiting for a timeout until they are discarded.	
CPF-22726	When configuring session management (**Flow Management>Flows Table>Default>Session Management**), selecting the Delete Session upon Termination Event checkbox is not relevant for a REJECT Routing Action or when a Handle Locally script is configured (FORWARD, ROUTE, SITE PROXY Routing Actions).	5.0: CPF-16369; 4.4: 16319
CPF-22702	When adding a new rule attribute and selecting one filter type, there is no option to edit the **Filter Type**.	5.0: CPF-17793
CPF-23890	Messages with the Experimental-Result-Code AVP are now processed as expected.	

5.28.5 Session Repository

ID	Description	Related ID in Previous Releases
CPF-20992	Once the session repository reaches 95% of its capacity, some entries may not be replicated as expected between mated Session repositories.	5.0: CPF-20991; 4.4: CPF-13063
CPF-22704	Each session-ID can only contain up to 511 characters.	5.0: CPF-19869
CPF-22708	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.	5.0: CPF-19908; 4.0 and later: CPF-5757
CPF-22727, CPF-22703	It takes two mated Session Repositories, 15 seconds to recognize when one is down. As a result, you need to wait 15 seconds between two Session Repository graceful shutdowns to make sure the mated Session Repository is not down. When the connection is temporarily down, not all of the session data may be replicated on the mated Session Repository.	5.0: CPF-17246, CPF-17598
CPF-22729	Session data size is limited to 1k bytes. The user cannot save larger amounts of data over the session cookie.	5.0: CPF-19909; 4.0.5 and later: CPF-6879
CPF-22731	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.	5.0: CPF-19911; 4.4: 13089
CPF-22732	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.	5.0: CPF-19912; 4.4: 8676

5.28.6 Performance

ID	Description	Related ID in Previous Releases
CPF-22737	The addRoutingRow Web Service API command response time depends on the number of rows in the Routing Table.	5.0: CPF-15990
CPF-22738	When a FEP is restarted, pending requests sent by the CPF to the FEP will not be resent by the SDC. However, pending requests sent by the FEP to the server peer will be resent.	5.0: CPF-16708

5.28.7 Monitoring

ID	Description	Related ID in Previous Releases
CPF-22675	For Diameter peers, the PeerNetworkQueueSizeBytes statistic, is calculated based on the peernetwrokqueuesizebytes column, and as a result, in the Web UI, the statistic "Network Write Queue Usage (per sec)," in Reports> Peers>Peer Health, shows as 0 for Diameter protocol traffic. For Radius/HTTP peers, the statistic is based on the peernetwrokqueuesize. This difference is because the Diameter and Radius/HTTP peers reference different columns in the prod_view_agg_statistics_peer_<time unit> tables.	
CPF-22249	Configuration changes performed on a SDC site when the EMS site that manages it is disconnected are not displayed in the audit screen (**Administration> Audit**) in the EMS Web UI (even once the connection is reestablished).	5.0: CPF-18942; 4.0.2: CPF-7180
CPF-22410	The Reports> SDC Components table only shows values for CPU Usage and Used Memory KPIs for CPF and FEP components.	

ID	Description	Related ID in Previous Releases
CPF-22602	Due to an inherent synchronization problem between clocks on the different machines used to calculate the Answer Latency Diameter statistic, the related values and graph may appear with some deviations.	5.0: CPF-19672
CPF-22705	The sdcPoolRateChanged alarm is raised after a few minutes as it is based on collected threshold statistics that are only measured once per minute.	5.0: CPF-18965
CPF-22707	Once an EMS site is upgraded to 5.1, the EMS Web UI representing data collected prior to the upgrade (**Reports > Previous Release Reports > System View**) automatically presents the managed SDC sites as "Down". The current collected data for the managed SDC sites can be viewed in the 5.1 **Reports** screens.	5.0: CPF-19591
CPF-22706	In multi-site deployments, the sdcCommunicationOfNmsTripo alarm, which is raised and cleared when the connection between the NMS Agent and the Session Repository (Tripo) is down/up, can be sent by either one or both of the NMS agents depending on which NMS agent executed the Tripo collection task. The NMS Agent logs reflect from which NMS Agent the alarm was sent.	5.0: CPF-19166
CPF-22733	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.	5.0: CPF-19913
CPF-22734	Configuration changes performed on a SDC site when the EMS site that manages it is disconnected are not	5.0: CPF-18942

ID	Description	Related ID in Previous Releases
	displayed in the audit screen (**Administration> Audit**) in the EMS Web UI (even once the connection is reestablished).	
CPF-22735	When there is no traffic in an SDC site, the Dashboard Licensed MPS graph is not displayed, when it should be displayed with a value of zero.	5.0: CPF-19167
CPF-22736	The following scenarios do not calculate all discarded transactions as part of the Transactions KPI (**Reports>Peers Summary/Pools Summary**). These scenarios are only reported for the FEP/CPF. 1. When one of the SDC queues is overloaded, and a transaction is rejected because it cannot be handled. 2. When the SDC is configured wrong, and a transaction cannot be handled. 3. When two SDC components are disconnected (e.g FEP and CPF), and a transaction cannot be handled. 4. When there is an error in a script, and a transaction cannot be handled. 5. When the SDC component capacity is exceeded, and a transaction cannot be handled.	5.0: CPF-19211

5.28.8 Administration

ID	Description	Related ID in Previous Releases
CPF-22181	Removing a dictionary or deleting an added dictionary by performing a rollback (**Administration> Audit>Rollback**) is not supported.	

ID	Description	Related ID in Previous Releases
CPF-22711	After restarting a network or one of the interfaces that the Keepalived mechanism is running on, the mechanism is not automatically recovered and must be manually reloaded using the kill -HUP command.	5.0: CPF-19783

Glossary

The following tables list the common terms and abbreviations used in this document.

Table 2: Common Terms

Term	Definition
Answer	A message sent from one Client/Server Peer to the other following a request message
Client Peer	A physical or virtual addressable entity which consumes AAA services
Data Dictionary	Defines the format of a protocol's message and its validation parameters: structure, number of fields, data format, etc.
Destination Peer	The Client/Server peer to which the message is sent
Geo Redundancy	A mode of operation in which more than one geographical location is used in case one site fails
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)
Orchestrator	A workflow management solution to automate the creation, monitoring, and deployment of resources in your environment
Origin Peer	The peer from which the message is received
Pool	A group of Server Peers
QCOW2	A file format for disk image files
RADIUS	Remote Authentication Dial In User Service
REST	Representation of a resource between a client and server **(Re**presentational **S**tate **T**ransfer)
Request	A message sent from one Client/Server peer to the other, followed by an answer message
RPM	RPM Package Manager

Term	Definition
Salt-API	Manages and communicates between an Orchestrator and network master and minion servers
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
Transaction	A request message followed by an answer message
Tripo	Session data repository
Virtual Server	A binding point used by SDC to communicate with the Remote Peers (Clients and Servers)

Table 3: Abbreviations

Term	Definition
AAA	Authentication, Authorization and Accounting
ACL	Access Control List
AF	Application Function
API	Application Programming Interface
AVP	Attribute Value Pair
CLI	Command Line Interface
CPF	Control Plane Function
DEA	Diameter Edge Agent
DRA	Diameter Routing Agent
EMS Site	Element Management System Site

Term	Definition
FEP-In	In-Front End Proxy
FEP-Out	Out-Front End Proxy
HA	High Availability
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IaaS	Infrastructure as a Service
IMS	IP Multimedia Subsystem
JMS	Java Message Service
KPI	Key Performance Indicator
LDAP	Lightweight Directory Access Protocol
LTE	Long Term Evolution
MME	Mobility Management Entity
NGN	Next Generation Networking
Node	Physical or virtual addressable entity
OAM	Operation, Administration and Maintenance
OCS	Online Charging System
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function
PLMN	Public Land Mobile Network
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
SNMP	Simple Network Management Protocol

Term	Definition
SS7	Signaling System No. 7
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
UE	User Equipment
URI	Universal Resource Identification.
VIP	Virtual IP
VNFC	Virtualized Network Function Component
VPLMN	Visited Public Land Mobile Network
Web UI	Web User Interface
WS	Web Service