



F5 Signaling Delivery Controller

Troubleshooting Guide

Document Information

Software Version: 4.0.5

Publication Date: February 2014

Catalog Number: RG-014-405-21 Ver. 1



1	ABOUT THIS DOCUMENT	1
1.1	ABOUT THIS DOCUMENT.....	1
1.2	CONVENTIONS	1
1.3	GLOSSARY OF TERMS AND ABBREVIATIONS	2
1.4	DOCUMENT VERSION HISTORY	3
2	TROUBLESHOOTING BASICS.....	4
2.1	REFERENCING THE SDC DOCUMENTATION.....	4
2.2	VERIFYING SYSTEM SETUP	4
2.3	GENERAL PREVENTION	4
2.4	COLLECTING SYSTEM DATA	4
2.5	F5 SUPPORT CONTACT INFORMATION.....	5
3	IP CONNECTIVITY	6
3.1	FAILED TO ACTIVATE SCTP ASSOCIATIONS.....	6
3.1.1	<i>Error Description</i>	<i>6</i>
3.1.2	<i>Causes.....</i>	<i>6</i>
3.1.3	<i>Symptoms</i>	<i>6</i>
3.1.4	<i>Resolution</i>	<i>6</i>
3.2	SCTP CLIENT SHOWS IN GUI TOO MANY ADDRESSES	7
3.2.1	<i>Error Description</i>	<i>7</i>
3.2.2	<i>Causes.....</i>	<i>7</i>
3.2.3	<i>Resolution</i>	<i>7</i>
4	SDC CLUSTER.....	8
4.1	PREREQUISITES.....	8
4.2	GENERAL CLUSTER COMMANDS FOR TROUBLESHOOTING.....	8
4.3	RECURRING RESOURCE FAILURES	9
4.3.1	<i>Symptom – Current Failure Counts</i>	<i>9</i>
4.3.2	<i>Resolution – Current Failure Count.....</i>	<i>10</i>
4.3.3	<i>Symptom - Resource Fails to Shutdown.....</i>	<i>10</i>
4.3.4	<i>Resolution – Resource Fails to Shutdown</i>	<i>10</i>
4.4	CPF CONNECTIVITY.....	10
4.4.1	<i>CPF Failure to Launch.....</i>	<i>10</i>



4.4.2	CPF Appears Offline	12
4.5	FEP CONNECTIVITY	12
4.5.1	FEP Failure to Launch.....	12
4.5.2	Virtual Server Unable to Bind Address	13
4.5.3	FEP Cannot Return Answer Back to Client	14
4.5.4	FEP Appears Offline	15
4.5.5	Unknown SCTP library.....	15
4.6	FEP-CPF COMMUNICATION.....	16
4.6.1	CPF Cannot Communicate with FEP.....	16
4.6.2	CPF Cannot Return Answer Back to FEP	17
4.6.3	FEP-O Cannot Return Answer Back to CPF.....	17
4.7	WEB UI CONNECTIVITY	17
5	SDC PIPELINE	19
5.1	LICENSING AND ACCESS CONTROL	19
5.2	CPF ROUTING.....	19
5.2.1	Request is Not Routed Using the Routing Rows as Expected.....	20
5.2.2	No Pools are Selected for Routing	20
5.2.3	Endless Pending Request Timeouts toward Client	21
5.2.4	Routing of Server Side Request (CLR) Fails.....	22
5.3	CPF TRANSFORMATION.....	23
5.3.1	CPF Dictionary.....	23
5.3.2	Message Parsing Failures	25
5.3.3	Configured Transformation Does Not Take Effect	29
5.3.4	3GPP Destination Realm Normalization Does Not Work.....	30
6	PERFORMANCE	31
6.1	HTTP PERFORMANCE IS DEGRADED	31
6.1.1	Error Description	31
6.1.2	Causes.....	31
6.1.3	Symptoms	31
6.1.4	Resolution	31
7	OVERLOAD CONTROL.....	33
7.1	RECEIVE/SEND RATE LIMIT IS HALF THAN EXPECTED	33



7.1.1	<i>Error Description</i>	33
7.1.2	<i>Causes</i>	33
7.1.3	<i>Resolution</i>	33
7.2	WEB UI STATISTICS MEMORY USAGE INCREASE	33
7.2.1	<i>Symptoms</i>	33
8	EMS	34
8.1	EMS CONFIG MANAGER FAILS TO START	34
8.1.1	<i>Symptoms</i>	34
8.1.2	<i>Resolution</i>	34
8.2	EMS CANNOT CONNECT TO REMOTE SITES	34
8.2.1	<i>Symptoms</i>	34
8.2.2	<i>Resolution</i>	34
9	REPORTING	36
9.1	SPLUNK DATA IS NOT SHOWN IN WEB UI	36
9.1.1	<i>Symptoms</i>	36
9.1.2	<i>Resolution</i>	37



Legal Notices

Document Name: F5 Signaling Delivery Controller 4.0.5 Troubleshooting Guide

Catalog Number: RD-014-405-21 Ver.1

Publication Date: February 2014

Copyright

© 2005-2014 F5 Networks, Inc. All rights reserved.

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

Trademarks

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

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

Confidential and Proprietary

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



1 About this Document



1.1 About this Document

This document provides troubleshooting guidelines for the following SDC components and their related operations in Release 4.0.5.

1.2 Conventions

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

Table 1: Conventions

Convention	Use
Times New Roman	Regular text
Times New Roman	Names of menus, commands, buttons, and other elements of the user interface
<i>Times New Roman</i>	Links to figures, tables, and sections in the document, as well as references to other documents
<CAPS>	Represents a variable
Courier New	Language scripts
Calibri	File names
<i>Note:</i>	Notes which offer an additional explanation or a hint on how to overcome a common problem
	Warnings which indicate potentially damaging user operations and explain how to avoid them
	An example



1.3 Glossary of Terms and Abbreviations

Table 2: Glossary of Terms and Abbreviations

Term	Definition
AAA	Authentication, Authorization and Accounting.
Cluster	SDC's group of nodes used to provide translation and connectivity services.
CPF	Control Plane Function
Data Dictionary	Defines the format of a protocol's message and its validation parameters: structure, number of fields, data format, etc.
DRT	Data Transfer Request (GTP concept)
EMS	Element Management System
FEP	Front End Proxy
Flow	Logical combination of user defined rules that define the transaction procedures' flow routine.
FQDN	Fully Qualified Domain Name.
GTP	GPRS Tunneling Protocol
HTTP	Hypertext Transfer Protocol
IMSI	International Mobile Subscriber Identity
ISD	International Standard Dialing
JMS	Java Message Service
JNDI	Java Naming and Directory Interface
LDAP	Lightweight Directory Access Protocol
MAP	Mobile Application Part. An SS7 protocol that provides an application layer for the various nodes in GSM and UMTS mobile core networks.
NGN	Next Generation Networking.
NMS	Network Management System



Term	Definition
Peer	Physical or virtual addressable entity. A Client or Server Peer in the NGN network that provides or consumes AAA services.
Pool	A group of Server Peers.
RADIUS	Remote Authentication Dial In User Service
SDC	Signaling Delivery Controller
SNMP	Simple Network Management Protocol
SS7	Signaling System No. 7
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Universal Resource Identification.

1.4 Document Version History

Date – Version	Change	Reference



2 Troubleshooting Basics

This section describes recommended best practices to avoid errors and to help with troubleshooting when they do occur. To resolve specific issues, refer to the relevant chapter in this guide.

2.1 Referencing the SDC Documentation

The SDC product documentation provides a comprehensive overview of system functionality. Some issues may be solved by consulting the relevant product documentation:

- *F5 SDC Installation and Upgrade Guide*
- *F5 SDC User Guide*
- *F5 SDC SNMP Guide*
- *F5 SDC Release Notes*

2.2 Verifying System Setup

Each SDC build supports specific SDC and third-party software (browsers, operating systems, etc.). Refer to the Release Notes to verify that your installation includes the recommended versions.

2.3 General Prevention

Make sure that all relevant machines are up and running, that all nodes are online and all relevant resources are started.

2.4 Collecting System Data

The SDC logs contain valuable data about your system activity. In order to collect all raw data, configuration, and logs, from the SDC, a specific TTA support script has been developed.

Note: The script is constantly updated, so when it is needed, contact F5 Technical Support to request the most updated script.



- After receiving the script, follow the below procedure to run it:
 1. Copy the script file to: */opt/traffic/sdc/bin*.
 2. Login to the first server and change directory to: */opt/traffic/sdc/bin*.
 3. Run the following commands:
 - `chmod +x tta_log_collector_v<version>.sh`
 - `./tta_log_collector_v<version>.sh snapshot`
 4. The script creates a *.tar.gz* archive that should be copied off the server from */opt/traffic/sdc/output*.
 5. Repeat steps 2-4 for each of the SDC servers.

2.5 F5 Support Contact Information

Contact technical support at: <http://www.f5.com/support/support-services/contact/>.



3 IP Connectivity

This section describes troubleshooting issues and solutions relating to IP connectivity.

3.1 Failed to Activate SCTP Associations

3.1.1 Error Description

Dialogic application (gctload) tries to activate a SCTP association and then a M3UA layer using system.txt and config.txt files. If these files were not configured correctly, the assertions of SCTP are left in a Not Active state and then the heart bit messages of M3UA are not sent.

3.1.2 Causes

The Installer creates and configures system.txt/and config.txt files. Any wrong configuration causes failure of SCTP/M3UA layer activation.

3.1.3 Symptoms

Dialogic SCTP stack cannot work together with Linux native SCTP stack. The regular diameter scenarios, such as CCR will not work.

- In system.txt file, SCTP is not configured to use native SCTP.
 - There is a collision between native SCTP used by CPF and dialogic version of SCTP used by Dialogic.
- License file of Dialogic is not installed according to requirements.
 - The gctload application cannot activate any SS7 layer implementation application (M3UA,SCCP,TCAP)
- The config.txt file is configured with wrong parameters:
 - OPC,DPC,SCTP PORTs and IPs (remote and local)
 - SIGTRAN Signaling Link Initiate command (SNSLI)

3.1.4 Resolution

The following are ways to resolve the issue:

Proprietary and Confidential Information of F5 Networks



- Configure system.txt using native SCTP (Refer to relevant documentation, for example: U10SSS-SwEnv-PM.pdf).
- Get license from dialogic per specific server and put it in the */opt/DSI* directory
- Verify that the right parameters (based on customer's configuration) are configured in the config.txt file according to the relevant documentation (U10SSS-SwEnv-PM.pdf).
- Test SNSLI command. It should be configured as a SCTP client.

3.2 SCTP Client Shows in GUI Too Many Addresses

3.2.1 Error Description

In general SCTP's multi-homing enables any number of IP connections in one SCTP channel. The F5 SDC can only support at most two IP addresses for one SCTP channel. Each virtual server and each static client/server peer needs to be configured with at most two IP addresses.

3.2.2 Causes

Client tried to connect to more than two addresses.

3.2.3 Resolution

System's IP tables need to be configured such that only two IP addresses are connected to each SCTP connection.



4 SDC Cluster

To achieve maximum availability for cluster resources by detecting and recovering from node and resource-level failures, SDC uses Pacemaker, as its cluster resource manager, and Corosync, as its group communication layer for Pacemaker. For more information about Pacemaker and Corosync, refer to the following link:

http://clusterlabs.org/doc/en-US/Pacemaker/1.1/html-single/Clusters_from_Scratch/

4.1 Prerequisites

For Cluster Resource Manager troubleshooting, verify that there are a minimum of two nodes (Pizza Boxes, Blades, VMs).

4.2 General Cluster Commands for Troubleshooting

The following table summarizes the most used cluster commands that you will use when troubleshooting:

Cluster Command –What is Does?	CRM Command Example
Show Status – top view	crm_mon
Show Status – One-shot display	crm_mon -l
Show Status – Per-node view	crm_mon -n
Show Last Failures	crm_mon -l nf
Show cluster operations history	crm_mon -l o
Show cluster operations history with timing details	crm_mon -l t
List top-level resources	crm_mon -l grep -P '^\\s+Resource Clone'
Take node offline (on standby)	crm node standby sdclab001-01
Take mode online	crm node online sdclab001-01
Stop single resource	crm resource stop traffic_webui-grp
Start single resource	crm resource start traffic_webui-grp



Restart single resource	crm resource restart traffic_webui-grp
Stop all cluster resource	crm configure property stop-all-resources=true
Un-stop all cluster resources	crm configure property stop-all-resources=false
Migrate Web UI to a node (and lock it to stay there)	crm resource migrate traffic_webui-grp sdclab001-02
Remove lock forcing Web UI to run on particular node	crm resource unmigrate traffic_webui-grp
Relay migration of CPF VIP and SCTP	crm resource migrate traffic_cpf-vip-grp sdclab001-01
Remove migration of CPF VIP and SCTP	crm resource unmigrate traffic_cpf-vip-grp

*Note: It is recommended in most cases to only perform start/stop operations on top-level Resource Groups and Clones. Remember to always "unmigrate" resources before and to "migrate" resources after performing start/stop operations as otherwise the resource will get stuck on a node. When migrating, use the **crm configure edit** command that can be applied from the Linux command line. This opens an editable file that can be modified as shown in the following example:*

```
location traffic_webui-loc traffic_webui-grp \
    rule $id="traffic_webui-loc-rule" -inf: #uname ne sdcvm108-01 and #uname ne
    sdcvm108-03
```



Removing either #uname ne sdcvm108-01 or #uname ne sdcvm108-03 will result in migrating the resource to the other node.

4.3 Recurring Resource Failures

4.3.1 Symptom – Current Failure Counts

In response to the crm command to count all the nodes in a SDC site, only some are “counted.” In the following example, only nodes Node sdclab002-01 and Node sdclab002-09 are counted and there is a failure to count the other nodes 02-08.



```
# crm_mon -nf1

<...skip...>

Migration summary:
* Node sdclab002-01:
  trafficx_cpf-app-prim:1: migration-threshold=3 fail-count=2 last-
failure='Sun Aug 14 11:12:11 2011'
* Node sdclab002-09
```

4.3.2 Resolution – Current Failure Count

You can manually clear the resource failure count with either of the following `crm` commands:

- `crm resource failcount trafficx_cpf-app-prim delete sdclab001-01`
- `crm resource cleanup trafficx_cpf-app-clone sdclab001-01`

4.3.3 Symptom - Resource Fails to Shutdown

If you send a `crm resource stop<RESOURCE_NAME> shutdown` command and the resource fails to completely shut down in the allowed time, it displays still as “Started”, and is not shutdown.

4.3.4 Resolution – Resource Fails to Shutdown

- To resolve this issue:
 1. End the underlying process, if it is still running.
 2. Verify that the resource has not been already re-started by the cluster.
 3. Issue a "cleanup" command for the resource and node (where the resource has faulted), as shown in the following example:
 - `crm resource cleanup trafficx_cpf-app-clone sdclab001-01`

4.4 CPF Connectivity

4.4.1 CPF Failure to Launch

If the CPF crashes upon initialization, check the following possible causes:



- scripting errors.
- configuration manager.

4.4.1.1 Cause – Scripting Errors

One of the initialization/engineering/health monitoring scripts has errors, causing the SPF to crash.

4.4.1.2 Resolution – Verifying Scripts

You need to correct the faulty script.

Note: Usually you can access the scripts (SDC Life Cycle; Health Monitoring, Engineering) from the Web UI. However, because FEP/CPF are not running, they cannot accept any configuration changes

- To correct the scripts:
 1. Shut down all SDC processes (including config manager).
 2. Locate and correct the script errors in the most recent flowManager.xml file (of each FEP/CPF).
 3. Check the scripts in the following XML hierarchy:
 - FlowManagerMgmt/Administration/PostSystemInit
 - FlowManagerMgmt/Administration/StatusCheck/Condition+CheckStatus

4.4.1.3 Cause – Configuration Manager

The SDC component (CPF) is unable to retrieve its configurations from the config manager. By default, the connection between each SDC component and the config manager is done using a multicast auto discovery mechanism.

When this occurs the following message is the last message in the log file after the component was started:

```
2013-12-15 09:19:17,123 INFO [] Starting beans in phase 2147483647 [main_1]
[DefaultLifecycleProcessor$LifecycleGroup.start()]
```

4.4.1.4 Resolution – Configuration Manager

- Check that the configuration files are configured to use multicast



- Check that the problem is related to the config manager

For more information, contact F5 Technical Support.

4.4.2 CPF Appears Offline

4.4.2.1 Symptom

SDC component appears offline or does not appear at all in the **Topology** section of the Web UI.

4.4.2.2 Resolution

Refer to Section 4.4.1.3 *Cause – Configuration Manager* or 8.1. *EMS Config Manager Fails to Start*.

4.5 FEP Connectivity

4.5.1 FEP Failure to Launch

If the FEP crashes upon initialization, check the possible causes:

4.5.1.1 Cause – Scripting Errors

One of the initialization/engineering/health monitoring scripts has errors, causing the FEP to crash.

4.5.1.2 Resolution – Verifying Scripts

Note: Usually you can access the scripts (SDC Life Cycle; Health Monitoring, Engineering) from the Web UI. However, because FEP/CPF are not running, they cannot accept any configuration changes

- To correct the scripts:
 1. Shut down all SDC processes (including config manager).
 2. Fix the problematic scripts in each latest copy of the flowManager.xml (latest flowManager.xml of each FEP/CPF).
 3. Check the scripts of the following XML hierarchy:



- FlowManagerMgmt/Administration/PostSystemInit
- FlowManagerMgmt/Administration/StatusCheck/Condition+CheckStatus

4.5.1.3 Cause – Configuration Manager

The SDC component (FEP) is unable to retrieve its configurations from the config manager. By default, the connection between each SDC component and the config manager is done using a multicast auto discovery mechanism.

The following message is the last message in the log file after the component was started:

```
2013-12-15 09:19:17,123 INFO [] Starting beans in phase 2147483647 [main_1]
[DefaultLifecycleProcessor$LifecycleGroup.start()]
```

4.5.1.4 Resolution – Configuration Manager

- Check that the configuration files are configured to use multicast
- Check that the problem is related to the config manager

For more information, contact F5 Technical Support.

4.5.2 Virtual Server Unable to Bind Address

Virtual server does not succeed to bind to address that it is configured to listen to. This is relevant to both TCP and SCTP.

Note: This problem was found in a SDC running on a Redhat 6.3 installation.

4.5.2.1 Causes

- The machine is not listening on the selected port. There is another process, possibly another SDC virtual server that already binds to the same IP and port.
- Failure happens when at least one TCP connection was in an Established or Time Wait state, suggesting an OS configuration issue.

4.5.2.2 Symptoms

The following error message appears in the FEP logs:

- “Virtual Server {0} bind attempt failed. Cause: {1}. Verify that the port is not used by any other Virtual Server”.



- The Linux command `netstat -anp | grep <PORT>`, does not return the LISTEN answer as it should and instead only the prompt line displays.

The following is an example of a return LISTEN answer:

```
tcp    0    0 :::8080          :::*              LISTEN    8091/java
tcp    0    0 ::ffff:10.2.108.3:18080 :::*              LISTEN    8430/java
```

The following is an example of when the LISTEN answer does not display:

```
[root@sdcvm108-01 /]#
```

4.5.2.3 Resolution

- Use the following Linux command to stop the LISTEN process to that IP and port: `kill -9 <PORT>`.
- Configure the Port to bind it to a different address.
- Remove the VS and configure new one that binds on different available IP and port.

4.5.3 FEP Cannot Return Answer Back to Client

4.5.3.1 Error Description

Request is routed correctly to server, and answer is returned from server to FEP-O, CPF and then to FEP, but it is not forwarded from FEP back to client.

4.5.3.2 Causes

- Client disconnects before it receives answer.
- Client sent a CER to FEP, but does not wait for CEA before it sends its requests. So the requests are routed to server, which returns answers, and the answers arrive to FEP before CER was processed inside the FEP. This results in the return answers being routed to a closed peer (client).

4.5.3.3 Symptoms

The following WARN message appears in the FEP log with the client peer as origin: “Cannot route the answer back, request's Origin Peer {0} was disconnected. Failed to send {1}”



4.5.3.4 Resolution

- Make sure that the client's message timeout is not too short. If using JMeter you can find it inside the element "Diameter Peer Configuration" in "Message Timeout (ms)".
- Make sure the client waits until it receives CEA before it sends its first request. If using JMeter, do the following steps:
 - a) Select **Thread Group** of the scenario.
 - b) Right-click and select: **Add**, and then **Sampler**, and then **Test Action**.
 - c) In **Test Action**, change its name to **Wait for CEA**, select **Pause** and a duration of **500 milliseconds**.
 - d) Drag the element **Wait for CEA** to be after **Diameter Sampler** that sends CER.

4.5.4 FEP Appears Offline

4.5.4.1 Symptom

SDC component appears offline or does not appear at all in the **Topology** section of the Web UI.

4.5.4.2 Resolution

Refer to Section 4.4.1.3 *Cause – Configuration Manager* or 8.1. *EMS Config Manager Fails to Start*.

4.5.5 Unknown SCTP library

4.5.5.1 Error Description

The following error, "unknown lib libsctp.so" appears in the FEP log.

4.5.5.2 Causes

Unsuccessful installation of the SCPT library. The version of the installed libsctp.so may not be what was expected from the installed SDC.



4.5.5.3 Resolution

Use the installer to properly install SDC.

4.6 FEP-CPF Communication

4.6.1 CPF Cannot Communicate with FEP

4.6.1.1 Error Description

Channels are constantly opened by FEP toward CPF, but CPF rejects them.

4.6.1.2 Causes

The FEP's configuration for minimum channels toward CPF is greater than the corresponding configuration of CPF for maximum channels. This causes the FEP to connect to CPF more channels than CPF allows, so CPF rejects them.

4.6.1.3 Symptoms

The following WARN message appears in the CPF log:

“Channel {0} was rejected (for peer {1}) because the maximum allowed number of channels ({2}) was reached”

Instead of the following message:

{1} you should see a Diameter peer with the FEP's name.

4.6.1.4 Resolution

Make sure that the following configuration parameters have the same values for all FEPs and CPFs in the same site (default is 6 for all):

- Inside entry “ClientConnectionMaxSizes”: the value for “ClientConnectionMaxSize” of protocol Diameter.
- Inside entry "ConnectionPoolSizeLowLimits": the value for "ConnectionPoolSizeLowLimit" of protocol Diameter.
- Inside entry "ConnectionPoolSizes": the value for "ConnectionPoolSize" of protocol Diameter.



4.6.2 CPF Cannot Return Answer Back to FEP

4.6.2.1 Error Description

Request is routed correctly to server and answer is returned from server to FEP-O and to CPF, but is not forwarded from CPF back to FEP.

4.6.2.2 Causes

The connection between CPF to FEP is disconnected, possibly because one of them did not answer watchdog requests. This might happen when the system is overloaded with too much traffic or too busy with processes running on the machine, or when using a VM.

4.6.2.3 Symptoms

The following WARN message appears in the FEP log with the client peer as origin:

- “Cannot route the answer back, request's Origin Peer {0} was disconnected. Failed to send {1}”

The following INFO message appears in the CPF log with the FEP as {0}, or appears in the FEP log with CPF as {0}:

- “Idle channel. Closing {0}. Channel is: {1}”

4.6.2.4 Resolution

Reduce the load on the machine that is hosting the process that disconnected the channel or migrate the process to a stronger machine.



Do not use a VM for load testing.

4.6.3 FEP-O Cannot Return Answer Back to CPF

Refer to **Error! Reference source not found.** (Section 4.6.1) for a similar troubleshooting scenario.

4.7 Web UI Connectivity

4.7.1 Symptoms



- The Web UI login page does not load
- The Web UI rejects the user credentials even when they are right

4.7.2 Causes

- The server is running out of memory
- You are trying to connect to the wrong port
- The Web UI is failing to communicate with the Configuration Manager
- The Configuration Manager is failing to communicate with the CPF

4.7.3 Resolutions

- Log into the host and check the memory status
- Make sure you are connecting to port 8080
- Make sure at least one instance of the Configuration Manager is running in the cluster
- Make sure at least one instance of the CPF is running in the cluster
- Verify in the sysconfig scripts that all the services are using the same multicast group name



5 SDC Pipeline

5.1 Licensing and Access Control

Remote client peer fails to open a link to the SDC.

4.4.1 Error Description

Client peer sends a proper CER to the SDC, but link is not established.

4.4.2 Causes

- The SDC is configured not to allow connection to unknown peers
- The remote peer is sending the CER messages to an IP address not licensed by F5
- No common application-IDs between client peer to SDC

4.4.3 Resolution

- Check the CPF log for error messages (verify in all CPF nodes), and the NMS platform for SNMP traps
- If “peer rejected” messages appear:
 - In the Web UI, select **Topology** and then in the **Access Control List** section, enable the **Accept Unknown Peers** checkbox.

Or

- Configure the remote peer manually and validate the remote peer connection to the destination IP as follows:

In the Web UI, select **Administration** tab and verify that a valid license exists for the relevant peer

5.2 CPF Routing

This section describes commonly found errors, their causes, symptoms, and resolutions related to CPF routing functionality.



5.2.1 Request is Not Routed Using the Routing Rows as Expected

5.2.1.1 Error Description

When traffic is sent to SDC, and then a change is made to the routing table (i.e. added new rows, or edited existing rows), and then another request is sent to one of the servers, without it being routed using one of the added routing rows.

5.2.1.2 Causes

This is due to session stickiness for pools. The already existing session is being reused for the incoming request, and the sessions bypasses the routing table.

5.2.1.3 Symptoms

- The pool that should be the destination for the traffic does not accept it (if it is a different pool than before the routing change).
- Routing scripts, (Check Error in Answer, Handle Server Error, etc.) that belong to the new routing row that should be selected, do not run.
- The logging is in TRACE mode for TransactionManagement, and a message of the format “Pool {0} was selected for {1}” did not appear in CPF logs since the routing change.

5.2.1.4 Resolution

Change the session ID for the next request or wait for session expiration (default is 30 seconds).

5.2.2 No Pools are Selected for Routing

5.2.2.1 Error Description

No messages are routed to the pools configured in the routing rule, even though the rule was correctly configured with the **ROUTE** action. Error messages display in the log as described in the Symptoms section below.



5.2.2.2 Causes

- All pools are in “Out of Service” state (since all peers of each of these pools are in a “Close” state (disabled or not yet connected) or “Out of Service”).
- At least one pool is in an “Open” state – but all of its peers are overloaded (reached maximum rate limit), and all other pools, if exist, are in “Out of Service” state.

Note: A pool will be in “Out of Service” state when at least its “Minimum Number of Peers” (configurable, default is 1) is reached. That means that there are no “Minimum Number of Peers” peers in this pool such that their state is “Open”.

5.2.2.3 Symptoms

The following INFO message may appear in the CPF logs:

- “Unable to choose pool: {0}, reason: {1}” for each of the pools that belong to the selected routing row.

The following WARN message may appear in the CPF logs:

- “Failed to select a Pool to handle a request received from {0}. The selected routing row index is {1} with policy {2}, the incoming message is {3}”.

5.2.2.4 Resolution

- Check the condition of the peers of each pool of the selected routing row to make sure they are not overloaded/closed/disabled, etc.
- Change the logging of TransactionManagement to DEBUG and follow the CPF logs to trace the pool selection.

5.2.3 Endless Pending Request Timeouts toward Client

5.2.3.1 Error Description

When CPF reaches a state where it cannot route a request to a server, it sends an error answer to the client. This error answer can be edited for each row of the routing table using the “Handle Server Error” scripts. Faulty scripts can cause SDC to behave very strangely. For example, if a script returns answerFromServer and the RemoteNodeEvent is CANNOT_ROUTE, then the message that is sent to client is the request that was sent by it. Since it is a request that goes downstream, now CPF will set it as a pending request with a



timeout, and since clients usually do not respond to requests, the pending timeout will be invoked and cause another endless cycle of requests that will be sent to the client.

5.2.3.2 Causes

A bad “Handle Server Error” script is configured for the routing row that was selected for the request.

5.2.3.3 Resolution

In the “Handle Server Error” script, reconfigure the “answerFromServer” parameter for any RemoteNodeEvent. For example, for CANNOT_ROUTE and TIMEOUT there are no answers from server, so answerFromServer cannot be returned.

5.2.4 Routing of Server Side Request (CLR) Fails

5.2.4.1 Error Description

A CLR request arrives and is then forwarded (based on a forward routing rule) to a client peer whose name appears as the Destination-Host AVP of the request. When this routing rule is configured as a Roaming Proxy, and then post transformation is done on the Destination-Host AVP before the request searches for the destination peer with this name. If after post transformation, the peer with this name is not found, then routing fails.

5.2.4.2 Causes

A server side request, such as CLR is generated in response to a client side request, such as ULR (when a CLR is sent by the server then the Destination-Host AVP is taken from the Origin-Host of the ULR). The routing rule of the client side requests must also be marked as roaming proxy otherwise the CLR routing will fail.

Each client peer at the SDC from where the ULR messages come from must have a peer profile (not default), because a peer profile name is used at translation of the destination peer.

5.2.4.3 Symptoms

The following section describes the error conditions and their relevant error messages.



- Client side request, like ULR, routed through SDC, with Roaming Proxy is enabled. The routing of ULR was successful, but peer profile at the client peer is not configured.
 - Error Message: “Diameter client peer {some peer name} must have a peer profile for Roaming Proxy full functionality. Routing of future requests from server will fail!”
- Routing of “Forwarded” message of server side request, such as CLR, when roaming is enabled is failed.
 - Error Message: “Routing of roaming request from server failed, no suitable client peer found, at event {some event description}”
 - Error Message: After the above message there will be a regular SDC routing failed message.

5.2.4.4 Resolution

The following are ways resolve the issue:

- Make sure that the client peer of the SDC through which the ULR messages have been sent has a non-default peer profile.
- Make sure that the “Forward” routing rule of server side request, such as CLR, is configured as a roaming proxy and that its related client side, such as ULR, is also configured with a roaming proxy.
- Make sure no changes were made to SDC configuration in the time gap between the ULR request and its matching CLR request routing. For example, that the peer profile name of a client peer was not changed.

5.3 CPF Transformation

5.3.1 CPF Dictionary

Each diameter network element holds its own dictionary. A successful diameter connection between two network elements requires compatible dictionaries that maintain the same AVP data message format. All AVPs included in a diameter dictionary must have a unique AVP name.

5.3.1.1 Mismatch between Multiple AVPs

5.3.1.1.1 Error Description

Proprietary and Confidential Information of F5 Networks



When CPF loads a diameter dictionary, that has two AVPs defined with the same name, but with different commands or vendor IDs, only the first AVP is saved in the application.

5.3.1.1.2 Causes

Using a diameter dictionary in which the AVP name is not unique.

5.3.1.1.3 Symptoms

The following section describes the error conditions and their relevant error messages.

The diameter dictionary used by CPF contains several AVPs that do not have a unique AVP name.

For example, the following two AVPs contain the same name and command, but different vendor IDs.

```
<avp name="Service-Selection" code="493" format="utf8String" mRule="must"
vendorId="10415"/>
<avp name="Service-Selection" code="493" format="utf8String" mRule="must"
vendorId="0"/>
```

This results in a mismatch between the two AVPS, as they are not unique, though they have the same name and the following message displays in the log file:

```
ERROR [10155] Diameter Dictionary (SDC dictionary v9): Mismatch between AVP
definition <Content Definition 3GPP-Charging-Characteristics 13 10415 UTF8String>
and <Content Definition 3GPP-Charging-Characteristics 13 UTF8String>: Trying to
load two AVPs with identical names and different codes. [jmsContainer-1_11]
[DiameterDictionary.mismatchDetected()]
2013-10-15 15:23:23,006 ERROR [10155] Diameter Dictionary (SDC dictionary v9):
Mismatch between AVP definition <Content Definition Service-Selection 493 10415
UTF8String> and <Content Definition Service-Selection 493 UTF8String>: Trying to
load two AVPs with identical names and different codes. [jmsContainer-1_11]
[DiameterDictionary.mismatchDetected()]
```

5.3.1.1.4 Resolution

For diameter application messages, use the super dictionary. The super dictionary contains only AVPs with unique names.

The base part of the super dictionary contains messages with application ID 0. These messages are used by more than one diameter Interface (application ID).

The following are options on how to resolve different AVP dictionary issues:



- To add a message with an application ID according to spec (not 0):
 - Create a message so that the name of this message will be built as concatenation of name and needed interface. For example, for a S6b application:

```
<! -- applicationId="16777272" -->
<message name="RAR-S6b" code="258" applicationId="16777272"
isProxiable="true" isRequest="true" sentByClient="false"/>
<message name="RAA-S6b" code="258" applicationId="16777272"
isProxiable="true" isRequest="false" sentByClient="true"/>
```

- To add AVPs for a specific vendor whose codes are used by other interfaces:
 - Add a prefix (vendor name) to the AVP name. For example:

```
<! -- vendorId="12645" -->
<avp name="Vodafone-Radio-Access-Technology" code="260" format="enumerated"
mRule="may" vendorId="12645"/>
```

- To distinguish between two AVPs that have the same name, but a different code in the interface:

- Add suffix that defines the data type of AVP. For example, in 3GPP Vendor-Id 10415 Service-Type AVP has three commands code, so can add its data type at the end:

```
<avp name="Service-Type-Grouped" code="1483" format="grouped" mRule="must"
vendorId="10415"/>
<avp name="Service-Type-Unsigned32" code="2031" format="unsigned32"
mRule="must" vendorId="10415"/>
<avp name="Service-Type-Enumerated" code="6" format="enumerated"
mRule="must" vendorId="10415"/>
```

- If there is more than one AVP whose name ends with the same address and their data type are addresses too, than the first character before the address should be changed. For example:

```
<avp name="Served-Party-IP-Address" code="848" format="address" mRule="must"
vendorId="10415"/>
<avp name="Served-Party-Ip-Address" code="248" format="address" mRule="must"
vendorId="10415"/>
```

5.3.2 Message Parsing Failures

Message parsing can fail due to multiple reasons. This section presents some parsing troubleshooting issues including providing instructions on how to investigate them in order to find out the root cause of the issue.



5.3.2.1 Error Description

CPF fails to parse some diameter AVPs with an internal error due to a thrown InvalidAvpLengthValidationException. The message handling continues but a Wireshark capture shows that the incoming message to SDC and outgoing message from SDC are different (no transformation has occurred). The outgoing message is marked as an “Unreassembled Packet” and Wireshark is not able to parse all the AVPs in the message, which were parsed successfully in the incoming message, (as shown in the screenshots below).

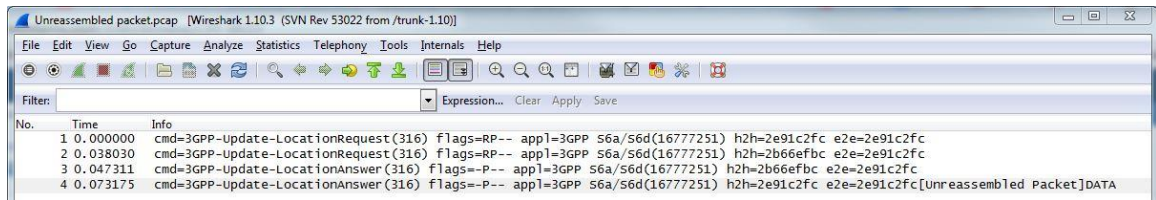


Figure 1: Unreassembled Packet

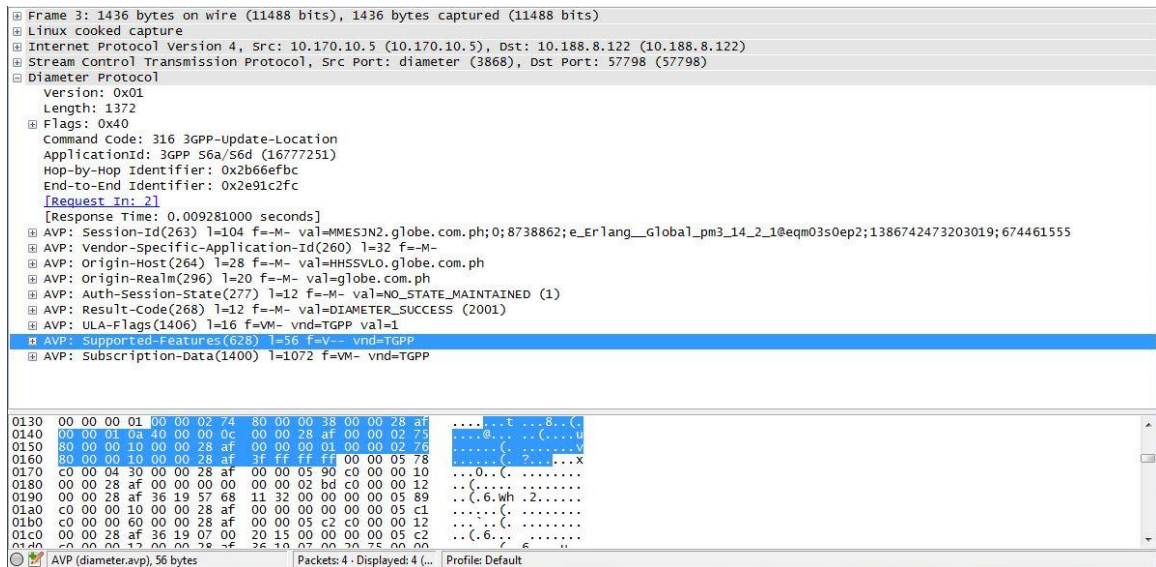


Figure 2: Incoming Message AVPs

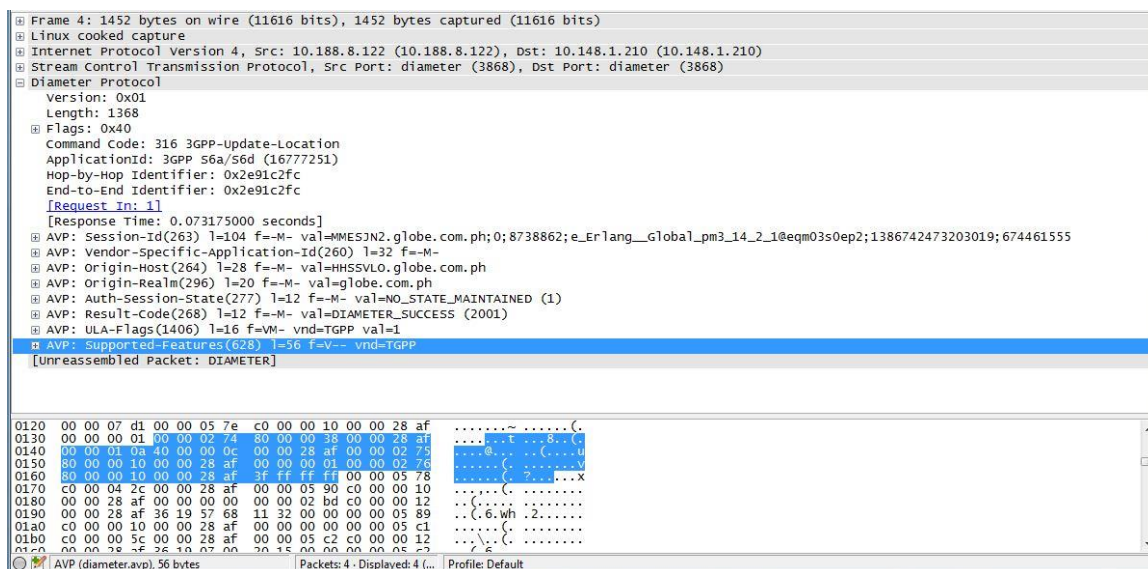


Figure 3: Outgoing Message AVPs

5.3.2.2 Causes

The cause for the illegal parsed value which then failed the parsing can be due to a buffer offset that was incorrectly incremented while parsing the message. A wrong buffer offset can cause AVPs to be parsed from the wrong index which can cause illegal values to be read. . Such errors in a buffer offset can be caused by a wrong AVP description in the used dictionary. Finding the location from which the buffer started incrementing incorrectly can lead to the root cause of the issue



Example:

The CPF Error message displays the failed AVP values. For example, the value in the error message in Section 5.3.2.3 is code=83886080 (0x5000000) and length=1435 (0x059b). Searching the incoming message for the length hex value found that the failed AVP length is an AVP code of “AMBR” AVP. The failed AVP code was found to be the data of the AVP which came before the “AMBR” AVP.



```

AVP: SS-Code(1476) l=13 f=VM- vnd=TGPP va1=c1
AVP: SS-Status(1477) l=13 f=VM- vnd=TGPP va1=05
  AVP Code: 1477 SS-Status
  AVP Flags: 0xc0
  AVP Length: 13
  AVP Vendor Id: 3GPP (10415)
  SS-Status: 05
  Padding: 000000
AVP: AMBR(1435) l=44 f=VM- vnd=TGPP
  AVP Code: 1435 AMBR
  AVP Flags: 0xc0
  AVP Length: 44
0200 c0 00 00 0d 00 00 28 af 05 00 00 00 00 00 05 9b .....(, ....
0210 c0 00 00 2c 00 00 28 af 00 00 02 04 c0 00 00 10 .....(, .....
0220 00 00 28 af 00 d5 9f 80 00 00 02 03 c0 00 00 10 ..(.....
0230 00 00 28 af 01 ab 3f 00 00 00 05 95 c0 00 03 54 ..(.....?.T
0240 00 00 28 af 00 00 05 8f c0 00 00 10 00 00 28 af ..(.....(
0250 00 00 00 01 00 00 05 94 c0 00 00 10 00 00 28 af .....(
0260 00 00 00 00 00 00 05 96 c0 00 01 90 00 00 28 af .....(
0270 00 00 05 8f c0 00 00 10 00 00 28 af 00 00 00 02 .....(
0280 00 00 05 b0 c0 00 00 10 00 00 28 af 00 00 00 02 .....(
0290 00 00 01 ed 40 00 00 18 4d 4d 53 2e 47 4c 4f 42 .....@...MMS:GLOB
02a0 45 2e 43 4f 4d 2e 50 48 00 00 05 97 c0 00 00 58 E.COM.PH .....X
02b0 00 00 28 af 00 00 04 04 c0 00 00 10 00 00 28 af .....(

```

Figure 4: Parsing Offset

This analysis shows that the error in the offset started when parsing the AVP which came before the “AMBR” AVP which is the “SS-Status” AVP.

After debugging the parsing of the “SS-Status” AVP, it was found that this AVP was parsed as a grouped AVP while it did not hold any grouped information. The reason for the parsing error was an error in the diameter dictionary in which the “SS-Status” AVP was marked as a grouped AVP instead of as an octet sting AVP. Changing the AVP type in the dictionary resolved the issue.

5.3.2.3 Symptoms

The following section describes the error condition and its relevant error message.

- The buffer offset is out of sync with the message AVPs during parsing. CPF starts parsing AVPs from the wrong buffer index causing illegal field values to be read.
- Error Message:

```

Internal warning: An attempt to create an AVP list from SlicedChannelBuffer(ridx=0,
widx=1328, cap=1328) had failed. [Client Worker_4_11]
[DiameterParsedGroupedAvp.getVendorSpecificAvpSet()]
com.traffic.openblox.diameter.exceptions.InvalidAvpLengthValidationException:
Invalid avp length 1435 to avp with code 83886080 and vendorId 0

```

5.3.2.4 Resolution

When encountering such parsing issues, you need to find the root cause (with Wireshark) to resolve the issue.

- To find the root cause of the AVP parsing error:

Proprietary and Confidential Information of F5 Networks



1. Take a Wireshark capture of the failed transaction.
2. Compare the message coming into the SDC to the message coming out of the SDC to see at what step Wireshark could not parse the AVPs.
3. Search for the failed AVP code and length value in the message coming into the SDC at the segments where Wireshark was not able to parse the message coming out of the SDC.
4. Identify the last AVP before the failed AVP from the error log.
5. Check the AVP definition in the used dictionary and compare it to the AVP which was sent to SDC.
6. Correct any dictionary mistake according to the actual sent data and the latest 3GPP Diameter application codes and identifiers specification document (for example, TS 29.230).
7. In case of conflict between the received data and the latest diameter application specification document, more detailed specification documents (such as TS 29.272 in the described example) should be referenced to verify that there are no mistakes in the diameter application specification document.

5.3.3 Configured Transformation Does Not Take Effect

5.3.3.1 Error Description

After configuring a Diameter Identity for some Routing Rules, the configured transformation does not take place. For example, the Destination Host/Realm of some request was not changed as was when the request was routed through SDC.

5.3.3.2 Causes

After the configuration, the request on which the transformation rule was configured was wrong, as it was a request from an existing session.

5.3.3.3 Symptoms

There are no special log errors/warnings for this problem.



5.3.3.4 Resolution

The transformation rule change is only visible once a new session is initiated and the request from the client is sent as only then the change takes place.

5.3.4 3GPP Destination Realm Normalization Does Not Work

5.3.4.1 Error Description

A routed request's destination realm is not normalized although it was configured.

5.3.4.2 Symptoms

The following section describes the error conditions and their relevant error messages.

- The AVP containing the IMSI from which MNC and MCC is calculated, but was not found at the request.
 - Error Message: "IMSI avp is not found, destination realm normalization will not work, at message {some request description}."
- The parsing of the IMSI number to MNC/MCC failed.
 - Error Message: "IMSI parsing failed, 3GPP realm normalization was canceled. Imsi: {the IMSI number}. Cause: {The cause for the fail}."

5.3.4.3 Resolution

The following are options on how to resolve the issue:

- The SDC takes the IMSI number from the following AVP's: For S6a or S6b application ID's the AVP is "User-Name". For Gx, Gy, Rx, Rf, Sy, S9 the AVP is inside the grouped AVP "Subscription-Id" and the one with AVP of "Subscription-Id-Type" equals to 1.

Note: Make sure that this AVP (User Name/Subscription-Id) is present at the request.

- Make sure the number is legal according to the RFC specification.
- When the "IMSI parsing failed..." error appears in the logDescription.txt file, look for the error, for example: `IllegalArgumentException ("IMSI length must be 14 or 15 digits")`, to correct the relevant input parameters.
- Make sure this error was not caused by a configured transformation error (as described in Section 5.3.3).



6 Performance

6.1 HTTP Performance is Degraded

6.1.1 Error Description

The TPS of the HTTP routing is much slower than expected.

6.1.2 Causes

- Keep-alive: server/client peers are not using keep-alive.
- Number of maximum connections (**Max Connections Count Limit (Per Server)**) configured when adding a Remote Peer) between the HTTP server peer and the server is too small to support the traffic load.
- Number of maximum connections between client peer to client is too small to support the traffic load.
- The HTTP virtual server disconnects after each response.
- Hosting machines are not strong enough. VM is being used.
- Size of messages is too big.

6.1.3 Symptoms

- Timeouts appear for the client or in the CPF. Timeouts by our side appear in the CPF log with the format “Peer Timeout event occurred for {0}, message {1}”.
- On the server side there are many TCP connections that are in a state: TIME_WAIT.

6.1.4 Resolution

- Check that the HTTP virtual server’s configuration for **Close Connection on Answer** is not enabled.
- Verify that **Keep Alive** is enabled when configuring an HTTP peer (server/client).
- Increase the **Max Connections Count Limit (Per Server)** configuration for the HTTP server peer.



Note: The default value is 10.

Generally there should be 20% more connections between the server peer and server than between the client peer.

- Verify that the **Max Connections Count Limit (Per Client)** configuration for the HTTP client peer value is configured to support expected traffic load.



The Default connection size is 1024.



7 Overload Control

7.1 Receive/Send Rate Limit is Half Than Expected

7.1.1 Error Description

Though you have configured a global message rate limit (Transaction receiving rate limit) or specific peer/profile message rate limits (Message sending rate limit), the TPS data graphs only show about half of the configured amount.

7.1.2 Causes

The discrepancy is because each counted message might be a request or a response, while each transaction of TPS is both a request and response.

7.1.3 Resolution

Refer to the Rate Limit table in the *F5SDC User Guide*.

7.2 Web UI Statistics Memory Usage Increase

7.2.1 Symptoms

The Web UI statistics show increased memory usage.

7.2.1.1 Cause

Sessions are accumulating in the CPF memory due to session timeout being too long.

7.2.1.2 Resolutions

- Set the session timeout parameter to a lower value.
- Update the transformation scripts to release the sessions after receiving the last message of a session.

Note: This may not be possible if SDC is unable to identify the last session message.



8 EMS

8.1 EMS Config Manager Fails to Start

8.1.1 Symptoms

The config manager shuts down upon initialization.

8.1.2 Resolution

The parameter that configures the TCP connections between the EMS and the remote sites is missing from the configuration.

➤ To add the missing parameter:

1. Add the following under `/opt/traffic/sdc/config/sysconfig/traffic_config_mgr:`

```
CONFIG_MGR_REMOTE_NETWORK_URI="static:(failover:(tcp://<CM_Site1_Node1
IP>:61617?wireFormat.maxInactivityDuration=0&keepAlive=true,tcp://<CM_Site1_Node2
IP>:61617?wireFormat.maxInactivityDuration=0&keepAlive=true)?randomize=false&
maxReconnectAttempts=0)"
```

8.2 EMS Cannot Connect to Remote Sites

EMS connects each remote site on the management network using destination port 61617. A possible problem is that the EMS cannot recognize any or some of the remote sites.

8.2.1 Symptoms

The following error message displays in the EMS config manager log:

```
2013-12-15 10:59:56,061 ERROR [] Failed to connect to
[tcp://172.29.49.43:61617?wireFormat.maxInactivityDuration=0&keepAlive=true]
after: 1 attempt(s) [ActiveMQ Task-1_1270] [FailoverTransport.doReconnect()]
```

8.2.2 Resolution

➤ To check the connection:



1. Use netstat to see which of the connections are in Established mode and which are missing.
2. Make sure the IP address that the EMS is trying to connect to is the correct remote site config manager management IP.

Note: All remote sites IP addresses are configured under /opt/traffic/sdc/config/sysconfig/traffic_config_mgr)

3. Check for network/firewall/IP table problems.



9 Reporting

Splunk is software that gathers, indexes, and arranges data from any application, server, or network device in your IT infrastructure. This data can then be generated into analytical reports with tables, charts, and graphs that are displayed in a Web UI.

This section describes commonly found errors with Splunk.

9.1 Splunk Data is Not Shown in Web UI

9.1.1 Symptoms

When browsing to one of Splunk's pages, the data is not displayed in the **Reports** tab as shown in the following screenshot:

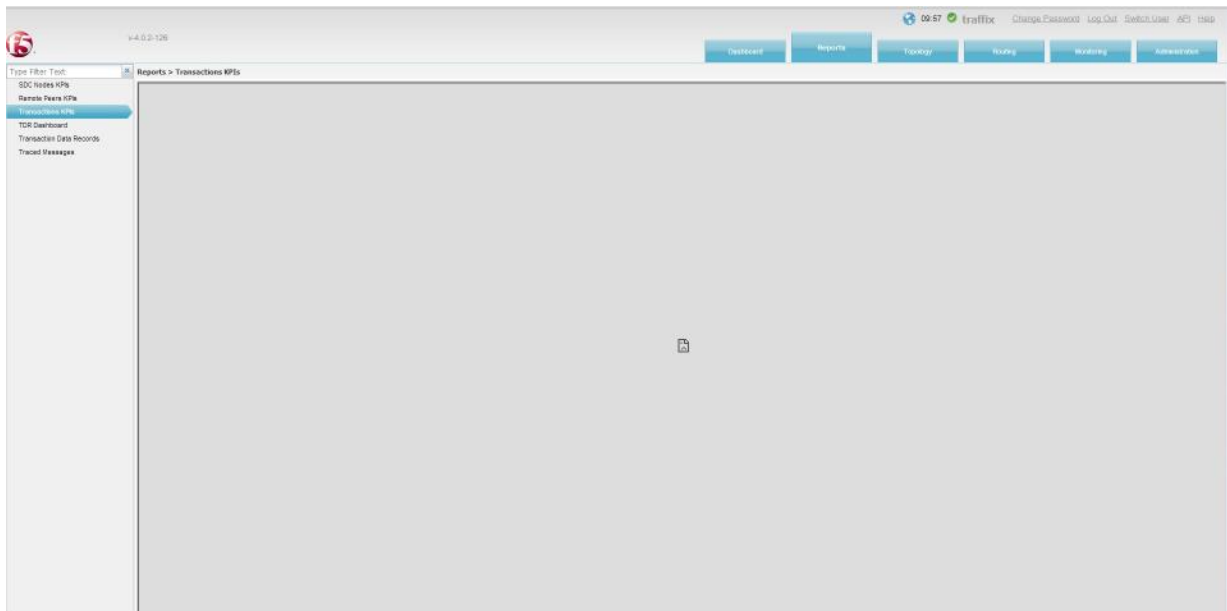


Figure 5: No Splunk Data Displayed

Another Splunk error can be that you get the following message as appears in the **Dashboard** tab: “Waiting for data” or “No selected job was found for saved search” as outlined in red in the screenshot below:

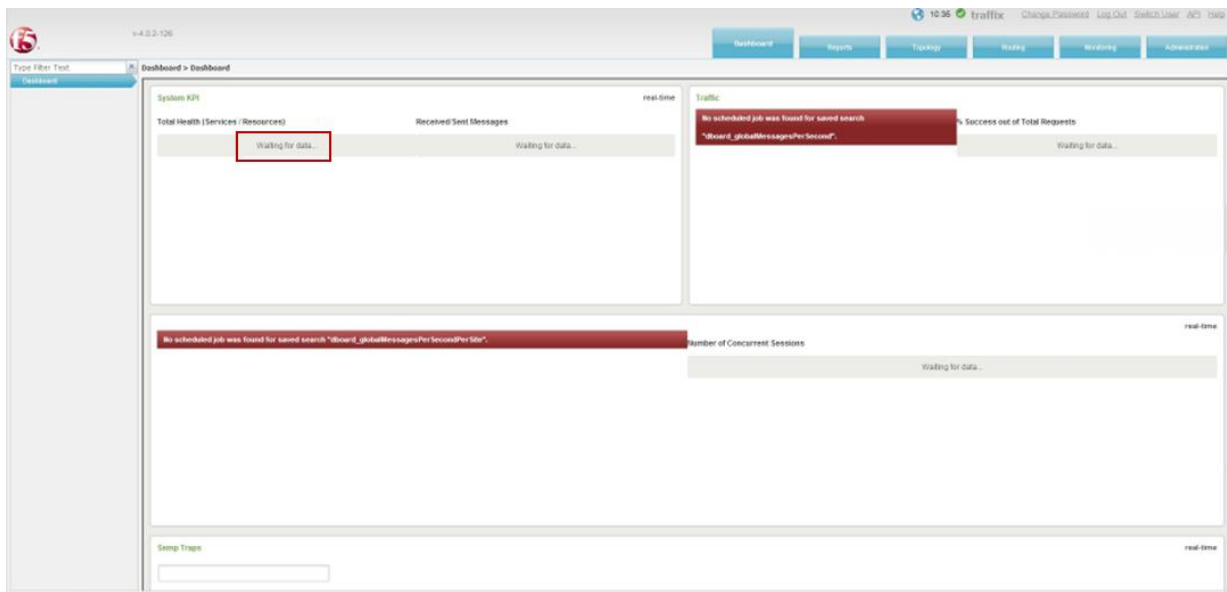


Figure 6: Waiting for Splunk Data

9.1.2 Resolution

You need to verify that the Splunk components are running correctly. The status of the different Splunk components can be checked by running CLI queries on the machine running the EMS.

To do this verification, contact F5 Technical Support.