



Signaling Delivery Controller

Bare Metal System Upgrade Guide 5.1

Catalog Number: RG-016-51-31 Ver. 25

Publication Date: January 2022



Legal Information

Copyright

© 2005-2022 F5 Inc. All rights reserved.

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 Bare Metal System Upgrade Guide

Catalog Number: RG-016-51-31 Ver. 25

Publication Date: January 2022

Document Objectives

This document provides describes the supported upgrades for the SDC 5.1 release installed on bare metal.



Note: In this document, “server” and “machine” are used interchangeably.

Document History

Revision Number	Change Description	Change Location
Ver. 2 – November 2016	Added description of ports used by the SDC	<i>Port Settings Used by the SDC</i>
Ver. 3 – January 2017	Added rollback procedure to a previous CF. Added procedure for manually configuring ports when in mix-mode. Added information about EMS Web UI screens during an upgrade. Added section to restart EMS NMS server	<i>Performing an Upgrade Rollback to a Previous CF, Performing an Upgrade Rollback to a Previous CF</i>
Ver. 4 – February 2017	Added ports used by the SDC. Added prerequisites for EMS Upgrade	<i>Port Settings Used by the SDC,</i>
Ver. 5 – March 2017	Updated SS7 pre-and post – procedure. Updated SDC site	



Revision Number	Change Description	Change Location
	rollback. Updated operating system upgrade procedure.	
Ver. 6 – April 2017	Updated SDC site rollback procedure.	<i>For release 4.4- no longer published in ver. 20 and higher</i>
Ver. 7 – May 2017	Updated the New ISO image procedure.	<i>New ISO Image</i>
Ver. 8 – June 2017	Updated the rolling upgrade process	<i>Rolling Upgrade to a New Release Version</i>
Ver. 9 – August 2017	Added a note about SNMPv3 functionality while in mix-mode. Updated the port descriptions	<i>Port Settings Used by the SDC</i>
Ver. 10 – September 2017	Updated the port descriptions. Added prerequisite (setting external port range) for rolling upgrade	<i>Port Settings Used by the SDC</i>
Ver. 11 – November 2017	Added note about copyFromIso procedure. Added prerequisite for rolling upgrade.	
Ver. 12 – December 2017	Edited saltupgrade procedure for rolling upgrade	<i>Upgrading the Master Installer</i>
Ver. 13 – September 2018	Edited different sections of rolling upgrade procedure	<i>Upgrading the Master Installer</i>
Ver. 14 – December 2018	Updated System Resources for Gen 10	
Ver. 15 – January 2019	Updated rollback procedure	<i>Rolling Back an EMS Site Upgrade to a Previous CF before Activating the Backup Array</i>



Revision Number	Change Description	Change Location
Ver. 16 – August 2019	Added prerequisite to update Splunk certificate in rolling upgrade	<i>From CF30, Splunk no longer supported, so removed from version 20 and higher of the guide</i>
Ver. 17 – September 2019	Added procedure for updating to OpenJDK	
Ver. 18 – January 2020	Updated Rolling Upgrade procedure	<i>Rolling Upgrade to a New Release Version</i>
Ver. 19 – May 2020	Added prerequisite to verify JAVA Heap memory allocation Corrected location of OpenJDK procedure	<i>Verifying the Java Heap memory allocation Supporting OpenJDK</i>
Ver. 20 – November 2020	Removed upgrade support from 4.4 Replace Splunk with ELK	<i>Throughout document</i>
Ver. 21 – December 2020	Updated Supporting OpenJDK and SALT files section. Removed Setting the External Port Changes	<i>Supporting OpenJDK</i>
Ver. 22- June 2021	Corrected command syntax Start all SDC component services	<i>Upgrading the Operating System</i>
Ver. 23- August 2021	Added note to prevent heavy disk usage for ELK when doing a rolling upgrade	<i>Updating from Splunk to ELK</i>
Ver. 24- December 2021	Add note to overcome Config Manager backward computability issue during Upgrade	<i>Upgrading the Master Installer</i>
Ver. 25 - January 2022	Modify “Upgrading from CF 29 or lower: file edits needed”: 1.Update HTTP to HTTPS step	<i>Upgrading from CF 29 or lower</i>



Revision Number	Change Description	Change Location
	2. Add create ELK table step	

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
<i>Normal Text Italic</i>	Links to figures, tables, and sections in the document, as well as references to other documents
Script	Language scripts
Courier	File names
 Note:	Notes which offer an additional explanation or a hint on how to overcome a common problem
 Warning:	Warnings which indicate potentially damaging user operations and explain how to avoid them



Table of Contents

1. Introduction	1
2. Rolling Upgrade to a New Release Version	2
2.1 Prerequisites	2
2.1.1 CLI Application	2
2.1.2 New ISO Image	3
2.1.3 Pre-Upgrade Health Check	3
2.1.4 Supporting OpenJDK	4
2.1.5 Extracting and Replacing the Salt Files	5
2.1.6 Verifying the Java Heap memory allocation	6
2.1.7 Upgrading from CF 29 or lower	7
2.2 Uploading the New ISO image for the Component Upgrade	8
2.3 Upgrading the Master Installer	9
2.4 Upgrading the OAM Database	11
2.5 Upgrading the Tomcat Version	11
2.6 Upgrading the SDC Components	11
2.7 Restarting the API Flows Post-Upgrade	12
2.8 Updating from Splunk to ELK	13
2.8.1 Adding the ELK Reports Configuration to an EMS site	14
2.8.2 Adding the ELK Components to an EMS site	17
2.8.3 Adding the ELK Components to an SDC site	18
2.9 Upgrading the Operating System	19
2.9.1 Prerequisites for Upgrading the Operating System	19
2.9.2 Uploading the New ISO Image	20
2.9.3 Upgrading the Operating System	21
2.10 Post-upgrade Procedures	22
2.10.1 Monitoring the Rolling Upgrade Process	22
2.10.2 Validating the SDC Processes	22
2.10.3 Monitoring the Status of SDC Components	23
2.10.4 Monitoring SDC Release Versions	23
2.10.5 Monitoring the Upgrade Logs	24
2.10.6 Monitoring Salt Packages	24
3. Performing an Upgrade Rollback to a Previous CF	25
3.1 Rolling Back an SDC Site Upgrade to a Previous CF	25
3.2 Rolling Back an EMS Site Upgrade to a Previous CF before Activating the Backup Array	29
3.3 Rolling Back an EMS Site Upgrade to a Previous CF after Activating the Backup Array	32
Appendix A: Port Settings Used by the SDC	34
A.1 EMS Site Internal Ports	34
A.2 EMS Site External Ports	35
A.3 SDC Site Internal Ports	37
A.4 SDC Site External Ports	39
A.5 HP Integrated Lights-Out (iLO) Port Settings	41
Glossary	43



List of Figures

Figure 1: Upgrade CLI Application Login	3
Figure 2: Example of Monitoring SDC Release Versions.....	23

List of Tables

Table 1: Conventions	V
Table 2: EMS Internal Ports	34
Table 3: EMS External Ports	35
Table 4: SDC Internal Ports	37
Table 5: SDC External Ports.....	39
Table 6: HP iLO Ports.....	41
Table 7: Common Terms	43
Table 8: Abbreviations	44



1. Introduction

The F5® Traffix® Signaling Delivery Controller™ (SDC) 5.1 release can be upgraded from any previous SDC 5.1 release.

The following procedures are described in this document:

- *Rolling Upgrade to a New Release Version*
- *Performing an Upgrade Rollback to a Previous CF*



Note: From 5.1 CF 30, EMS deployments will use ELK components, instead of Splunk components, to manage all SDC reporting functionalities. This change is reflected in version 20 and higher of the *Upgrade Guide*. This version of the guide assumes that you are upgrading from CF11 or higher.



2. Rolling Upgrade to a New Release Version

You can perform a rolling upgrade from a 5.1 release to a new 5.1 release version. The rolling upgrade is performed using Salt commands from the CLI application. It includes the following steps:

1. Uploading the new ISO image to a Master Installer (Component Upgrade)
2. Upgrading the Master Installer
3. Upgrading the OAM database
4. Upgrading the SDC components
5. Upgrading the operating system

Throughout the upgrade, you can monitor the process and check to see which SDC components are up and running. In the event that certain components are not successfully upgraded, you can choose to either resume the upgrade process or perform a rollback. While the length of an upgrade process varies with the size of the deployment, for a deployment with four servers (and ten SDC components), the upgrade process takes approximately 40 minutes, with minimal downtime. After completing the upgrade of all the components (applications), you need to upgrade the operating system.

2.1 Prerequisites

This section describes the prerequisites of a rolling upgrade.

2.1.1 CLI Application

This upgrade process uses the upgrade CLI Application. To proceed with the upgrade process, you must be logged in to the CLI Application.

To access the upgrade CLI Application:

1. Run the following commands:

```
/srv/traffic/upgrade/upgrade-cli
```



2. Log in with your SDC Web UI username and password.

Figure 1: Upgrade CLI Application Login

```
login as: root
root@10.240.12.141's password:
Last login: Mon Apr 11 08:44:21 2016 from 192.168.190.38
[root@sdclab006-09 ~]# cd /srv/traffix/upgrade/
[root@sdclab006-09 upgrade]# ./upgrade-cli
webui Username: traffix
webui Password:
```

2.1.2 New ISO Image

The ISO image contains the operating system and it is packaged and provided as bootable media by F5. Verify that you have saved the ISO image in a location that you can later point to to load it.

2.1.3 Pre-Upgrade Health Check

It is recommended that you check the status (disconnected/connected) of the SDC components prior to performing the upgrade. In this way, you will have a baseline to compare which SDC components are connected during and after the upgrade. The health check is performed with the CLI command: **healthcheck**.

The following is an example of a healthcheck



```
[upgrade-cli: 5.0-638]# healthcheck
sdclab006-14_vnf : SUCCESS
sdclab006-09_fep-out-tcp : SUCCESS
sdclab006-14_fep-out-tcp : SUCCESS
sdclab006-09_cpf1 : SUCCESS
sdclab006-14 : SUCCESS
sdclab006-14_webui-unique : SUCCESS
sdclab006-09_vnf : SUCCESS
sdclab006-09_cm-unique : SUCCESS
sdclab006-09_keepalived : SUCCESS
sdclab006-14_keepalived : SUCCESS
sdclab006-09_oamDB-unique : SUCCESS
sdclab006-09_webui-unique : SUCCESS
sdclab006-09_tripol : SUCCESS
sdclab006-14_cm-unique : SUCCESS
sdclab006-09_nmsagent-unique : SUCCESS
sdclab006-09_fep-Geo : SUCCESS
sdclab006-14_tripol : SUCCESS
sdclab006-09 : SUCCESS
sdclab006-14_cpf2 : SUCCESS
sdclab006-09_fep-in-A : SUCCESS
sdclab006-14_oamDB-unique : SUCCESS
sdclab006-14_nmsagent-unique : SUCCESS
sdclab006-14_fep-in-A : SUCCESS
sdclab006-14_fep-Geo : SUCCESS
```

2.1.4 Supporting OpenJDK

From CF 25 and higher, OpenJDK is built-in and you do not need to do this step. If you are upgrading from a 5.1 CF 24 or lower release to a 5.1 CF 25 or higher, you need to support OpenJDK. This is done by replacing the following current files with the newly extracted files.



Note: It is recommended to back up the current files before they are replaced.

Current File	New File
/opt/traffix/scripts/copyRpmFromIso.py	/<DIRECTORY_OF_EXTRACTED_TAR>/salt/system/scripts/copyRpmFromIso.py
/srv/traffix/upgrade/upgrade-cli	/<DIRECTORY_OF_EXTRACTED_TAR>/traffix/upgrade/upgrade-cli



2.1.5 Extracting and Replacing the Salt Files



Note: This procedure is required for both EMS and SDC site deployments. This procedure needs to be performed on both master Installer servers.

To extract the Salt files:

1. Backup the /srv folder on each of the master Installer servers.
2. Create a temporary folder:

```
mkdir /tmp/patch
```

3. Upload the salt-srv package from the ISO of the new CF to the /tmp/patch folder.

- a. Copy the new CF ISO to the server to the relevant <path>, for example: /root/
- b. Mount the new CF ISO:

```
mkdir -p /mnt/tmp_mount
```

```
mount -o loop /<path>/iso-<New CF ISO Version>.iso /mnt/tmp_mount/
```

- c. Copy the new Salt version from the mounted ISO:

```
cp /mnt/tmp_mount/traffic/repositories/traffic/salt-srv<version>.rpm  
/tmp/patch/
```

- d. Unmount the ISO:

```
umount /mnt/tmp_mount
```

4. Extract the rpm contents:

- a. Go to *cd /tmp/patch/*
- b. Run the following command:

```
rpm2cpio salt-srv< New CF ISO Version >.noarch.rpm | cpio -idmv
```



5. Go to the following folder and extract the file:

```
cd /tmp/patch/opt/traffix/salt-srv/<New CF ISO Version>/  
  
tar xvf archive.tar
```

6. To replace the files:

Run the following commands from the directory from which you extracted the tar file:

```
cp  
/<DIRECTORY_OF_EXTRACTED_TAR>/salt/system/scripts/copyRpmFromIso.py  
/srv/salt/<Old CF ISO Version>/system/scripts/copyRpmFromIso.py  
  
cp /<DIRECTORY_OF_EXTRACTED_TAR>/traffix/upgrade/upgrade-cli  
/srv/traffix/upgrade/upgrade-cli
```

7. Proceed with the override prompt question.

8. Copy the following file to both Master Installers:

```
cp  
/<DIRECTORY_OF_EXTRACTED_TAR>/salt/system/scripts/copyRpmFromIso.py /opt/traffix/scripts
```

2.1.6 Verifying the Java Heap memory allocation

In the case that the Java Heap Memory allocation has been modified, the allocation reverts to the default level, after the upgrade. You need to save the modified Salt files before performing the upgrade. Upon completing the upgrade, you need to contact F5 Support to have the previously customized allocation level implemented again.



2.1.7 Upgrading from CF 29 or lower

If you are upgrading from CF29 or lower, you need to perform the below steps.

2.1.7.1 Update healthCheck.py script to use HTTPS

1. Edit the `/srv/traffic/upgrade/healthCheck.py` file (lines 53, 54):
2. Change port 8080 to 8443
3. Change http to https.

```
def prepareClients(self):
    self.clients = []
    for webui in self.webUIHosts:
        auth_url = self.__get_auth_url('https', webui, 8443)
        wsd1_url = self.__get_wsd1_url('https', webui, 8443)
        client = self.__get_soap_client(wsd1_url, auth_url)
        if client != None:
            self.clients.append(client)
```

2.1.7.2 Create ELK table in Cassandra DB

1. Log in using ssh to one of the Cassandra machines (nodes)
2. Log in to the Cassandra DB
`# /opt/cassandra/bin/cqlsh <MGMT IP>`
3. Create ELK table by copy paste the below

```
CREATE TABLE topology.elk (
    "siteId" text,
    "vmName" text,
    name text,
    "IPv" text,
    "index" int,
    "listenInterfaceName" text,
    status text,
    PRIMARY KEY ("siteId", "vmName", name)
) WITH CLUSTERING ORDER BY ("vmName" ASC, name ASC)
    AND bloom_filter_fp_chance = 0.01
```



```
AND caching = '{"keys":"ALL", "rows_per_partition":"NONE"}'  
AND comment = ''  
AND compaction = {'class':  
'org.apache.cassandra.db.compaction.SizeTieredCompactionStrategy'}  
AND compression = {'sstable_compression':  
'org.apache.cassandra.io.compress.LZ4Compressor'}  
AND dclocal_read_repair_chance = 0.1  
AND default_time_to_live = 0  
AND gc_grace_seconds = 864000  
AND max_index_interval = 2048  
AND memtable_flush_period_in_ms = 0  
AND min_index_interval = 128  
AND read_repair_chance = 0.0  
AND speculative_retry = '99.0PERCENTILE';
```

4. Exit cqlsh mode

2.2 Uploading the New ISO image for the Component Upgrade

You first need to upload the new ISO image to one of the Master Installers. Once you do this, you then need to copy it to the `/opt/repo/traffix` folder.

To load the ISO image:

1. Perform the required pre-installation configurations needed for the console that is being used. The following steps assume that the ILO Integrated Remote Console is being used:
 - a. Configure the ILO IP address.
 - b. Connect to the ILO Integrated Remote Console and select Virtual Drives.
 - c. Select Image file CD -ROM/ DVD to set with ISO file.
 - i. Mount the ISO image from where it is saved on your computer.
 - ii. Open the upgrade-cli, with the following command:



`/srv/traffic/upgrade/upgrade-cli`

- iii. Log in with the Web UI username (traffic) and password.
- iv. Run the following command to copy the new ISO image to the `/opt/repo/traffic` folder:

copyFromIso



Note: If the `copyFromIso` procedure is not successfully carried out, the following message is displayed to notify the user that the relevant RPMs were not copied to the second Master Installer:

"Could not copy repo to second master"

2.3 Upgrading the Master Installer

During this phase, the Master Installers are upgraded with the operating system included in the new ISO image.

To upgrade both master installers:

1. Run the following command on one of the master Installers:

saltupgrade



Note: The `saltUpgrade` command checks for any manually applied changes in the salt state files. If there are any, the following message appears in the upgrade CLI interface and in the logs: "Salt state files have been manually modified." The `saltupgrade` automatically generates a patch file located in `/srv/salt/salt.patch` before exiting from the CLI Application. You need to copy any newly created set of state patch files to the new state files in `/srv/salt/<51.-new rpm salt srv version>`.

Once the files have been copied, and only in the case the `saltupgrade` was interrupted because of changes in the state files, continue with upgrading the Master Installers and then run the **saltEngineUpgrade** command.



2. After running the saltupgrade or the saltEngineUpgrade command, verify, by logging into Cassandra, that the Master Installer components upgrade status is “started” with the following command:

```
/opt/cassandra/bin/cqlsh
```

```
SELECT * FROM statusflow.appflow
```

After running this command, you will be logged out of the CLI Application.



Note: When upgrading from CF-30 or lower to CF-31 or higher, please follow the below steps:

Backup Rolling Upgrade script

```
# cp /srv/traffix/upgrade/rollingUpgrade.py /tmp
```

Edit origin Rolling Upgrade script

```
# vi /srv/traffix/upgrade/rollingUpgrade.py
```

Find "def nmsHealthCheck():" function, replace the "return -1" with "return 0"

Save and exit

```
def nmsHealthCheck():
    '''nmsHealthCheck: checking health of system'''
    log.info('nmsHealthCheck: waiting for the system to stabilize')
    for i in xrange(0, 18):
        time.sleep(10)
        ret = nmsHealthCheckClient.shallWeContinueStateless(ignoreList, failList)
        log.debug('healthCheck stateless ret=%s' % ret)
        if ret:
            time.sleep(10)
            ret = nmsHealthCheckClient.shallWeContinue(ignoreList, failList)
            if ret:
                log.info('nmsHealthCheck: Success')
                return 0
            log.info('nmsHealthCheck: transient effect, checking again')
        log.info('nmsHealthCheck: Not ok!')
    return 0
```

The above will disable the nmsHealthCheck during the "upgrade" stage.

After the stage is completed successfully, please run "healthcheck".



Note: When upgrading from CF-33 or lower, you need to unmonitor the WebUI process using the "monit unmonitor <NODENAME_WEBUI>"

2.4 Upgrading the OAM Database

During this phase, the OAM database is upgraded with the data included in the new release version.



Note: You must log in again (with the following command: `./upgrade-cli`) to the CLI Application before proceeding with this step.

To upgrade the OAM database:

1. Run the following command:

upgradeOamDB

2.5 Upgrading the Tomcat Version

During this phase, the Tomcat version is upgraded with the version included in the new release version.



Note: You must be logged in to the CLI Application before proceeding with this step

To upgrade the Tomcat version:

1. Run the following command:

tomcatUpgrade

2.6 Upgrading the SDC Components

During this phase, each SDC component is upgraded. The system knows inherently to upgrade each SDC component by component layer, starting with Tripo. Once the CLI command is executed, an internal process is carried out with the following phases:



preUpgrade, stop, install, update Links, postUpgrade (includes an nmsHealthCheck, to see if Upgrade was successful).

To upgrade the SDC components:

1. Run the following command:

upgrade



Note: Only components that are connected, can be upgraded.

2.6.1.1 Resuming the SDC Component Upgrade

If the SDC component upgrade stops in the middle of the process, you will see a prompt that the "Upgrade is not successful." You then have the option to continue the upgrade process.

To restart the SDC Upgrade process:

1. Run the following command:

Resume

2.7 Restarting the API Flows Post-Upgrade

Upon completing the upgrade and checking that all SDC components are up and running, you need to unlock the API flows that were stopped during the upgrade. This essentially resets the API request flows to an idle state so the system is fully ready to run all API requests.

To restart the API flows:

1. Run the following command:

finalizeUpgrade



Note: Initially, after running this command, you will get a response that the "lock is busy" and that the API request "flow lock not idle". Run the command again after thirty seconds, and the following response is displayed:

Unlocking flow

enabling highstate on all hosts

lock is idle

2.8 Updating from Splunk to ELK



Note: When updating from any previous CF 30 release to post CF30 or higher release, you need to configure both the upgraded EMS and SDC sites for ELK, in place of Splunk.

You can work in mix-mode with ELK and Splunk, until you are confident to update all sites to ELK. For example, you can have ELK and Splunk running on the EMS site, while can have Splunk running on the SDC site. For sites that are already updated with ELK, TDR reports are sent to the */opt/traffix/reports/elk* folder of the EMS site, and for those sites that have not yet been updated, TDR reports are sent to the */opt/traffix/reports/tdr* folder of the EMS site.

Removing Splunk components should only be done after you are sure that you want your sites to only work with ELK.

To prevent heavy disk usage for elastic search (ELK) data, move the existing ELK Data location. Run the following:

```
mkdir /data/elk
```

```
mv /opt/elk/* /data/elk
```

and in all *elasticsearch.yml* files change the *path.data* from */opt/elk/** to */data/elk/**:

For example in the following files:



```
vi /srv/salt/5.1-1941/elk/elasticsearch/elasticsearch_config_data
```

```
vi /srv/salt/5.1-1941/elk/elasticsearch/elasticsearch_config_master
```

```
vi /etc/elasticsearch/elasticsearch_master/elasticsearch.yml
```

```
vi /etc/elasticsearch/elasticsearch_data/elasticsearch.yml
```

Run Monit start on the ems site for _elasticsearch_data and elasticsearch_master

Note: This should be done while ELK is down.

The current supported versions for ELK packages 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

2.8.1 Adding the ELK Reports Configuration to an EMS site

To support ELK reporting, you need to add the ELK Dashboard reports configuration to the NMS.

To add the ELK Reports configuration:

1. On both Master Installer servers stop CM, NMS and tomcat process, with the following commands:

- **monit stop <ems master node>_traffix_config_mgr-config1**
- **monit stop <ems master node>__nmsagent1**
- **monit stop <ems master node>_tomcat**

2. On both Master Installer servers, go to the NMS configuration folder and add the following section to DEFAULT_LB_CONFIGURATION.xml file in the data/backup/<EMS_Site_Name>:



Note: Once the following script is added, the Elk Reports will be added to:



```
<properties>
<entry key="ResourceGroupName" value="SnmpSystemStates"/>
<entry key="ResourceList">
```

```
cd /data/backup/sdclab010-15-ems/sdclab010-15-ems-1_traffix_config_mgr-
config1/nmsConfigurations/DEFAULT_NMS_AGENT_CONFIGURATION
```

```
# cat latestVersion.xml
```

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE properties SYSTEM "http://java.sun.com/dtd/properties.dtd">
```

```
<properties>
```

```
<comment>latest version</comment>
```

```
<entry key="status">ACTIVE</entry>
```

```
<entry key="key">v1:ts=1</entry>
```

```
<entry key="fileName">1602662363444</entry>
```

```
</properties>
```

```
vim 1602662363444/DEFAULT_LB_CONFIGURATION.xml
```

```
<!-- Elk reports -->
```

```
<entry key="ElkReports">
```

```
<properties>
```

```
<entry key="ElkDashboardPanel">
```

```
<properties>
```



```
<entry key="ElkNodeParentName" value="TDRs"/>

<entry key="ElkNodeDisplayName" value="TDR
Dashboard"/>

<entry key="ElkNodePanelUrl"
value="/MgmtConsole/kibana/s/tdr/app/kibana#/dashboard/sdc-kibana-tdr-
dashboard"/>

</properties>

<properties>

<entry key="ElkNodeParentName" value="TDRs"/>

<entry key="ElkNodeDisplayName" value="Traced
Messages"/>

<entry key="ElkNodePanelUrl"
value="/MgmtConsole/kibana/s/traced-messages/app/kibana#/dashboard/sdc-
kibana-traced-messages"/>

</properties>

<properties>

<entry key="ElkNodeParentName" value="TDRs"/>

<entry key="ElkNodeDisplayName" value="Transactions
Data Records"/>

<entry key="ElkNodePanelUrl"
value="/MgmtConsole/kibana/s/transactions-data-
records/app/kibana#/dashboard/sdc-kibana-transactions-data-records"/>
```




```
        </properties>

    </entry>

</properties>

</entry>
```

3. On both Master Installer servers, stop CM, NMS and tomcat process, with the following commands:

- **monit start <ems master node>_traffix_config_mgr-config1**
- **monit start <ems master node>__nmsagent1**
- **monit start <ems master node>_tomcat**

2.8.2 Adding the ELK Components to an EMS site

To add the ELK components:

1. From the first Master Installer server, run the following command:

```
salt-run traffix.addApplication elk
```



Note: This can take a few minutes until the components are installed.

2. Run **monit summary** to verify that the components were installed and are running:



```
[root@sdclab010-06-ems-1 ~]# monit summary
The Monit daemon 5.14 uptime: 11d 4h 28m

System 'system-sdclab010-06-ems-1' Running
Program 'sdclab010-06-ems-1_webui1' Status ok
Process 'sdclab010-06-ems-1_tomcat' Running
Process 'salt-minion' Running
Process 'sdclab010-06-ems-1_installer' Running
Process 'salt-api' Running
Process 'ntpd' Running
Process 'sdclab010-06-ems-1_nmsagent1' Running
Process 'sdclab010-06-ems-1_kibana' Running
Process 'sdclab010-06-ems-1_fluent' Running
Process 'sdclab010-06-ems-1_elasticsearch_master' Running
Process 'sdclab010-06-ems-1_elasticsearch_data' Running
Process 'sdclab010-06-ems-1_traffix_config_mgr-config1' Running
Process 'sdclab010-06-ems-1_oamDB' Running
```

2.8.3 Adding the ELK Components to an SDC site

Once the upgrade procedure is completed (See 2.1-2.6) for each SDC site, and you are ready to add the ELK site component, (fluent) in place of the splunkforwarder, you need to do the following migration. To replace the Splunk component and add the ELK components:

1. Stop the splunkforwarder on each server where found, with the following command:

monit stop <SDC site node>_splunkforwarder

2. From the first Master Installer server, run the following command:

salt-run traffix.addApplication elk



Note: This can take a few minutes until the component is installed.

3. Remove the Splunk components from the SDC site and the EMS site with the following commands:

- a. from the SDC site first Master Installer server:

salt-run traffix.removeApplication splunk

- b. Wait a few minutes and then run **monit summary** to verify that the Splunk FWD was removed.

- c. from the EMS site first Master Installer:



salt-run traffix.removeApplication splunk

4. Run **monit summary** to verify that the Splunk components were removed and that the ELK components were installed and are running:

```
[root@sdclab010-06-site-1-1 ~]# monit summary
The Monit daemon 5.14 uptime: 11d 4h 17m

System 'system-sdclab010-06-site-1-1' Running
Program 'sdclab010-06-site-1-1_webui1' Status ok
Process 'sdclab010-06-site-1-1_tripol' Running
Process 'sdclab010-06-site-1-1_tomcat' Running
Process 'salt-minion' Running
Process 'sdclab010-06-site-1-1_vnf' Running
Process 'salt-api' Running
Process 'ntpd' Running
Process 'sdclab010-06-site-1-1_nmsagent1' Running
Process 'sdclab010-06-site-1-1_keepalived' Running
Process 'sdclab010-06-site-1-1_fluent' Running
Process 'sdclab010-06-site-1-1_fepTcpInOut' Running
Process 'sdclab010-06-site-1-1_fepRadius' Running
Process 'sdclab010-06-site-1-1_fepHttp' Running
Process 'sdclab010-06-site-1-1_fep-site-1-sctp-in' Running
Process 'sdclab010-06-site-1-1_cpfl' Running
Process 'sdclab010-06-site-1-1_traffix_config_mgr-config1' Running
Process 'sdclab010-06-site-1-1_oamDB' Running
```

2.9 Upgrading the Operating System

After the SDC components have been upgraded, you must upgrade the operating system.



Note: Always perform the OS upgrade first on the machines that have Tripo on them.

2.9.1 Prerequisites for Upgrading the Operating System

This section describes the prerequisites for upgrading the operating system. You might have already performed these prerequisites when upgrading the SDC components.

2.9.1.1 New ISO Image

The new ISO image with the new operating system should already be uploaded and accessible as part of the component upgrade.



2.9.1.2 Copy Data Center/ Customer Environment RPMs

The upgrade process includes an OS installation. This upgrade removes any installed Data Center/Customer environment specific RPMs. Copy the RPMs that you want to reinstall after the upgrade.

2.9.1.3 Split Mirror for Rollback

Perform HP Split Mirror with Salt (this might have been done as part of the APP upgrade)..

2.9.1.4 Pre-OS Upgrade Health Check

Prior to upgrading the operating system (OS) with the new RPMs, you should check the status of the SDC components. It is recommended that you save this healthcheck for comparison purposes post-upgrade to check if any components that were previously up are down post-upgrade.

To check the status of the components post-component upgrade:

1. If you are not logged in to the CLI Upgrade application, do so. For more information, refer to *CLI Application*.
1. Run the following command:

Healthcheck

2.9.2 Uploading the New ISO Image

In this step, you will load the ISO and save the RPM packages in repo folders.

To upload the ISO:

1. Run the following command:

/opt/traffix/scripts/osRollingUpgrade.sh -l



Note: Only the latest version of each loaded RPM package is saved in the repo folder. If you need to remove any packages that were uploaded by mistake, do the following:

Log in to each master Installer server.

Delete the relevant file from */opt/repo/updates*

Run the command: **createrepo /opt/repo/updates**

2.9.3 Upgrading the Operating System

The upgrade must be performed remotely for each server (hostname) in the site. Remote actions are done using the Salt cmd.run module. After upgrading the RPM package, you need to restart the SDC components on the server. Prior to restarting, it is recommended that you check which components are up and running on the server.

To upgrade the RPM package:

1. Run the following command:

```
salt 'hostname*' cmd.run "/opt/traffic/scripts/osRollingUpgrade.sh -u"
```

2. Run the following command for local servers:

```
/opt/traffic/scripts/osRollingUpgrade.sh -u
```



Note: If you need to see a list of the host names, run the following command:

```
grep "# host" /etc/hosts
```

To restart the server (host):

1. Check which SDC components are up and running on the server with the upgraded OS:

```
salt 'hostname*' monit.summary
```

2. Stop the SDC component services: CPF, FEP, Tripo, OAM (configuration manager, NMS Agent, Web UI) as well as Tomcat and all elk services:



```
salt '<hostname>*' monit.stop <SDC instance name>:
```



Note: The OAM database (cassandra) must be the last service to be stopped. Closing a wrong service, such as Salt-minion, will prevent the restart from working

3. Restart with the following command:

```
salt 'hostname*' "reboot"
```



Note: Wait for the server to finish rebooting.

4. Start all SDC component services:

```
salt 'hostname*' monit.start all
```

5. Repeat the above steps for all the site servers.

2.10 Post-upgrade Procedures

2.10.1 Monitoring the Rolling Upgrade Process

Throughout the rolling upgrade process, there are a few ways to monitor the process. If you want to roll back the upgrade process, you can do so. For more information, see *Performing an Upgrade Rollback to a Previous CF*.

2.10.2 Validating the SDC Processes

Post-OS upgrade, you should check to see that all the processes are up and running. For examples. You should see the following processes:

- vInstaller (master)
- cm (config manager)
- nms (nms agent)
- oamDB (cassandra)
- salt-api



- salt-minion
- cpf
- fep
- Tripo
- ELK

To check the processes:

1. Run the following command:

```
salt '*' monit.summary
```

2.10.3 Monitoring the Status of SDC Components

The CLI Upgrade application command healthcheck checks the connectivity status of each SDC component. This command can be executed throughout the upgrade process. See *Pre-Upgrade Health Check* for more information and an example.

2.10.4 Monitoring SDC Release Versions

You can check which SDC release versions are available to support your deployment. Upon completing the upgrade, the previous version and the new version should be displayed.

To view the SDC release versions:

1. Run the following command:

```
ls -l /opt/repo/traffix/
```

Figure 2: Example of Monitoring SDC Release Versions

```
[root@sdclab006-09 upgrade]# ls -l /opt/repo/traffix/
total 12
drwxr-xr-x. 2 root root 4096 Apr  3 16:45 5.0-613
drwxr-xr-x  2 root root 4096 Apr  6 15:13 5.0-638
drwxr-xr-x  2 root root 4096 Apr  6 15:13 repodata
```



2.10.5 Monitoring the Upgrade Logs

You can check the upgrade logs for general troubleshooting. The upgrade logs are located in the `/var/log/upgrade.log` folder.

2.10.6 Monitoring Salt Packages

You can check which salt-srv packages are being used.

To view which Salt packages are being used:

1. Run the following command:

```
- yum search salt-srv
```




3. Performing an Upgrade Rollback to a Previous CF

This upgrade process includes the option to roll back an upgrade that has encountered errors.

- To roll back an upgrade of an SDC site managed by an EMS site, follow the *Rolling Back an SDC Site Upgrade to a Previous CF* procedure.
- To roll back an upgrade of an EMS site before activating the backup array, follow the *Rolling Back an EMS Site Upgrade to a Previous CF before Activating the Backup Array* procedure.
- To roll back an upgrade of an EMS site after activating the backup array, follow the *Rolling Back an EMS Site Upgrade to a Previous CF after Activating the Backup Array* procedure.

3.1 Rolling Back an SDC Site Upgrade to a Previous CF

This procedure is used to roll back an upgrade of an SDC site that is managed by an EMS site. This procedure uses the backup array as the master copy.

To perform the upgrade rollback:

1. Stop all traffic on the SDC site.
2. From the first Master Installer server, remove the ELK component, with the following command:

```
salt-run trafix.removeApplication elk
```



Note: This step is **only** relevant if rolling back from CF 30 or higher to to a CF 29 release or earlier. This can take a few minutes until the components are installed.

3. Stop the applications running on the SDC site and the EMS site by running the following command on the relevant servers:



monit stop all

4. Run the following commands on each EMS site server to delete the SDC site data:

cd /data/backup

mv <SDC rolled back site name> /var/tmp/

5. Start the EMS site.

6. On the SDC site, re-mirror the two arrays using the backup array:

a. Access the HP Storage Controller Administrator BIOS Interface by performing the following steps:

i. Enter “HP SSA” in the remote console.

ii. Reboot the SDC site server.

iii. At the prompt, enter “HP Storage Controller Administrator”.

iv. Select **F5** (for Gen8) or **F10** (for Gen9) or **F11** (for Gen10) to start the **HP Storage Controller Administrator**.

b. Define and activate the active array as the master array by performing the following steps on the SDC site servers:

i. Under "Array Controller(s)" select the active array.

ii. From Actions list - Click "Configure"

iii. Under "Controller Devices", select "Arrays"

iv. Under "Arrays", select the active array.

v. Under "Actions" select "Manage Split Mirror Backup".

c. Define the rollback procedure:



- i. Select the following option: "Re-mirror the array and rollback the contents of the backup array. Discard existing data", to roll back to the previous OS image, make it the master and sync the upgraded drive to it.
- ii. Confirm the selection.
- d. Click "X" at the top right corner of the SSA Menu screen and confirm the exit.
- e. Click the Power Icon at the top right corner of the screen and confirm the reboot action.

7. Run the following scripts on the servers running Tripo:



Note: The Tripo environment must be active before applying these scripts. You can do so as follows:

```
su - traffic
```

```
cd /home/traffic/Tripo/env/linux-x86_64/
```

```
. DefEnv Tripo
```

stopsh

Cleansh

start.sh

8. Start the SDC site by running the following command on the relevant servers:

monit start all



Note: After rolling back an SDC site that is managed by an EMS site, the EMS global configuration parameters will be distributed to the local SDC site. Any local configuration changes made on the local SDC site after the upgrade and before the rollback will be deleted from both the local SDC site and from the EMS site that manages it.



9. When a local SDC site is managed by an EMS, you need to revert the SDC version saved in the EMS Cassandra to the original SDC version.

- a. After the rollback, log in to Cassandra and run the following commands on one of the Casandra hosted servers:

```
SELECT * FROM statusflow.appflow ;
```

```
SELECT * FROM statusflow.flow ;
```

- b. Run the following commands with the following relevant parameters on each database row in the app flow table and in the flow table, respectively:

- i. Update command for each database row (meaning for each SDC component/application) in the app flow table with the following parameters:



Note: You need to run this command for each SDC component/application per VM.

```
UPDATE statusflow.appflow SET "version" = '<previous SDC version>'  
WHERE "siteId"= '<SDC site name>' AND "vmName"= '<VM name>' AND  
"appType"= '<SDC component/application>' AND "appName"= '<SDC  
component/application name>' ;
```

- version = previous SDC version
- siteID = SDC site name
- vmName = VM that is associated with the appType
- appType = the SDC component/application type (such as Web UI, CPF)
- appName = name of a SDC component/application type

- ii. Update command for the flow table:

```
UPDATE statusflow.flow SET "current version" = '<current SDC version>'  
WHERE "siteId" = '<SDC site name>' AND "flowType" = 'statusApi';
```



- `currentVersion` = current SDC version
- `siteID` = SDC site name
- `flowType=status Api`

Upon completing this step, the SDC version saved in the EMS Cassandra is reverted back to the original SDC version.

3.2 Rolling Back an EMS Site Upgrade to a Previous CF before Activating the Backup Array

This procedure is used to roll back an EMS site upgrade, before the backup array was activated. This procedure uses the backup array as the master copy.

To perform the upgrade rollback:

1. From the first Master Installer server, remove the ELK components, with the following command:

```
salt-run trafix.removeApplication elk
```



Note: This step is **only** relevant if rolling back from CF 30 or higher to a CF 29 release or earlier. This can take a few minutes until the components are removed.

2. Stop the applications running on the EMS site by running the following command on the relevant servers:

```
monit stop all
```

3. Re-mirror the two arrays using the backup array:

- a. Access the HP Storage Controller Administrator BIOS Interface by performing the following steps:
 - i. Enter “HP SSA” in the remote console.
 - ii. Reboot the SDC site server.



- iii. At the prompt, enter “HP Storage Controller Administrator”.
- iv. Select **F5** (for Gen8) or **F10** (for Gen9) or **F11** (for Gen10) to start the **HP Storage Controller Administrator**.
 - b. Define and activate the active array as the master array by performing the following steps on the SDC site servers:
 - i. Under "Array Controller(s)" select the active array.
 - ii. From Actions list - Click "Configure"
 - iii. Under "Controller Devices", select "Arrays"
 - iv. Under "Arrays", select the active array.
 - v. Under "Actions" select "Manage Split Mirror Backup".
 - c. Define the rollback procedure:
 - i. Select the following option: "Re-mirror the array and rollback the contents of the backup array. Discard existing data", to roll back to the previous OS image, make it the master and sync the upgraded drive to it.
 - ii. Confirm the selection.
 - d. Click “X” at the top right corner of the SSA Menu screen and confirm the exit.
 - e. Click the Power Icon at the top right corner of the screen and confirm the reboot action.
- 4. Start the EMS site by running the following command on the relevant servers:
monit start all
- 5. After the rollback, log in to Cassandra and run the following commands on one of the Casandra hosted servers:

SELECT * FROM statusflow.appflow ;



```
SELECT * FROM statusflow.flow ;
```

- a. Run the following commands with the following relevant parameters on each database row in the app flow table and in the flow table, respectively:
 - i. Update command for each database row (meaning for each EMS component/application) in the app flow table with the following parameters:



Note: You need to run this command for each EMS component/application per VM.

```
UPDATE statusflow.appflow SET "version" = '<previous EMS version>'  
WHERE "siteId"= '<EMS site name>' AND "vmName"= '<VM name>' AND  
"appType"= '<EMS component/application>' AND "appName"= '<EMS  
component/application name>' ;
```

- version = previous EMS version
- siteID = EMS site name
- vmName = VM that is associated with the appType
- appType = the EMS component/application type (such as cm, nms, oamDB)
- appName = name of an EMS component/application type

- ii. Update command for the flow table:

```
UPDATE statusflow.flow SET "current version" = '<current EMS version>'  
WHERE "siteId" = '< EMS site name>' AND "flowType" = 'statusApi';
```

- currentVersion = current EMS version
- siteID = EMS site name
- flowType=status Api

Upon completing this step, the EMS version saved in the EMS Cassandra is reverted back to the original EMS version.



3.3 Rolling Back an EMS Site Upgrade to a Previous CF after Activating the Backup Array

This procedure is used to roll back an EMS site upgrade, after the backup array was activated. This procedure uses the backup array as the master copy.

To perform the upgrade rollback:

1. Access the HP Storage Controller Administrator BIOS Interface by performing the following steps:
 - a. Enter “HP SSA” in the remote console.
 - b. Reboot the server.
 - c. At the prompt, enter “HP Storage Controller Administrator”.
 - d. Select **F5** (for Gen8) or **F10** (for Gen9) or **F11** (for Gen10) to start the **HP Storage Controller Administrator**.
2. Define and activate the active array as the master array by performing the following steps:
 - i. Under "Array Controller(s)" select the active array.
 - ii. From Actions list - Click "Configure"
 - iii. Under "Controller Devices", select "Arrays"
 - iv. Under "Arrays", select the "Active Array".
 - v. Under "Actions" select "Re-Mirror Array" and select **Backup array as a source**.



Note: Use the following command to monitor the status of the re-mirroring: `hpssaccli ctrl all show config`



3. Restore the original VG name, that was modified during the upgrade, by performing the following steps:

- a. Reboot the server and direct it to a RH recovery media.
 - i. In the first Rescue dialogue, select Skip, so that filesystems will not be mounted.
 - ii. In the next dialog window, select Start Shell.
 - iii. At the shell prompt, running the following command to rename the VG:

```
vgrename vg1_clone vg1
```

The volume group “vg1_clone” is successfully renamed to “vg1”.

4. Unmount the ISO and reboot the server.

Appendix A: Port Settings Used by the SDC

During an upgrade, a set of ports was enabled to ensure communication both between the different SDC components within the deployment, and between the SDC components and the necessary network elements.

This section describes the ports that have been validated for use by the SDC.

A.1 EMS Site Internal Ports

Table 2: EMS Internal Ports

Transport Protocol	Port	Network	Description
TCP	2812	IC	Monit
TCP	9200/9201 9300/9301	IC	ElasticSearch Discovery
TCP	5601	MGMT	Kibana Web Access
TCP	13868	IC	Traffic load balancing between the FEP and CPF instances
TCP	61616	IC	Communication between the configuration manager and the SDC components
TCP	61657	IC	Web UI Communication on cluster
UDP	161	IC	SNMP GET functions provided by OS snmpd service
UDP	162	IC	SNMP traps listener
UDP	1162		OS trap daemon listener

Transport Protocol	Port	Network	Description
TCP	7000	MGMT	Cassandra Database inter-site communication
TCP	7001	MGMT	Cassandra Database inter-site communication
TCP	7199	MGMT	Cassandra JMX monitoring inter-site communication
TCP	9042	MGMT	Cassandra client

A.2 EMS Site External Ports

Table 3: EMS External Ports

Transport Protocol	Port	In/Out	Network	Description
TCP	22/443	In	MGMT	SSH remote consoles
TCP	80	In	MGMT	HP Blade System web consoles
UDP	123	Out	OAM	NTP Process
UDP	514	Out	OAM	Syslog Process
UDP	1161	Out	MGMT	For External EMS Statistics Analysis
UDP	User-defined Ports (and IPs)	Out	MGMT	Trap Forwarding: For External EMS Trap listeners

Transport Protocol	Port	In/Out	Network	Description
TCP	9300 & 9320	In/Out	MGMT	Elastic search sync between two EMS nodes
TCP	5601	In/Out	MGMT	Kibana Web Access
TCP & UDP	10046	In	MGMT	Fluentd Fwd EMS (Receive TDR & Traces from site to EMS; UDP for Hearbeats)
TCP	3868	In/Out	H-TCP	Inter-site communication link for geo-redundancy
SCTP	3868	In/Out	H-SCTP-A	Primary SCTP path for domestic traffic
SCTP	3868	In/Out	H-SCTP-B	Secondary SCTP path for domestic traffic
TCP	4505/6	In/Out	MGMT	Salt Master
TCP	8000	In/Out	MGMT	Salt API
TCP	8080/8443	In	MGMT	SDC web console (Web UI)
TCP	10040	Out	MGMT	NMS Agent to NMS Manager

Transport Protocol	Port	In/Out	Network	Description
				for system status synchronization
TCP	61617	In	MGMT	Communication between the EMS and the SDC servers for new configuration propagation
TCP	7000	In/Out	MGMT	Cassandra Database inter-site communication
TCP	7001	In/Out	MGMT	Cassandra Database inter-site communication
TCP	7199	In/Out	MGMT	Cassandra JMX monitoring inter-site communication
TCP	9042	In/Out	MGMT	Cassandra client

A.3 SDC Site Internal Ports

Table 4: SDC Internal Ports

Transport Protocol	Port	Network	Description
TCP	2812	IC	Monit

Transport Protocol	Port	Network	Description
TCP	61616	IC	Communication between the configuration manager and the SDC components
TCP	13868	IC	Traffic load balancing between the FEP and the CPF instances
TCP	11812	IC	RADIUS listening port between the FEP and the CPF
TCP	18080	IC	HTTP listening port between the FEP and the CPF
TCP	13386	IC	GTP listening port between the FEP and the CPF
TCP	1389	IC	LDAP listening port between the FEP and the CPF
TCP	4444	IC	NMS to CPF communication port
TCP	23210	IC	Tripo - CPF connection to Tripo
TCP	43211	IC	Tripo – inter-site connection
TCP	23212	IC	Tripo - connection between Tripo mates within the same site
TCP	61627	IC	Default configuration REST communication
TCP	61637	IC	Default configuration REST communication
TCP	61647	IC	Default configuration REST communication NMS Agent

Transport Protocol	Port	Network	Description
TCP	61657	IC	Default configuration REST communication - UI
TCP & UDP	10046	MGMT	Fluentd Fwd Site (FWD TDR & Traces from site to EMS UDP for Hearbeats)
UDP	4545	IC	Port prefix is 4545 and the postfix is the UID of the CPF or FEP (4545 + UID)
TCP	5555	MGMT	Tripo Web statistics
TCP	7000	MGMT	Cassandra Database inter-site communication
TCP	7001	MGMT	Cassandra Database inter-site communication
TCP	7199	MGMT	Cassandra JMX monitoring inter-site communication
TCP	9042	MGMT	Cassandra client

A.4 SDC Site External Ports

Table 5: SDC External Ports

Transport Protocol	Port	In/Out	Network	Description
TCP	4505/6	In/Out	MGMT	Salt Master
TCP	8000	In/Out	MGMT	Salt API

Transport Protocol	Port	In/Out	Network	Description
TCP	8080 8443	In	MGMT	SDC web console (Web UI)
TCP	80	In	MGMT	HP Blade System web consoles
UDP	162	Out	MGMT	SNMP traps toward the EMS or third party NMS servers
TCP	3868	In/Out	H-TCP	Inter-site communication link for geo-redundancy
SCTP	3868	In/Out	H-SCTP-A	Primary SCTP path for domestic traffic
SCTP	3868	In/Out	H-SCTP-B	Secondary SCTP path for domestic traffic
TCP	61617	In	MGMT	Communication between the EMS and the SDC servers for new configuration propagation (internal and external data)
\TCP	22/80/443/623/17990/17988	In	MGMT	HP iLO4 management

Transport Protocol	Port	In/Out	Network	Description
				consoles and virtual media
TCP	10030	Out	OAM	NMS Agent
UDP	123	Out	OAM	NTP Process
UDP	514	Out	OAM	Syslog Process
TCP	7000	In/Out	MGMT	Cassandra Database inter-site communication
TCP	7001	In/Out	MGMT	Cassandra Database inter-site communication
TCP	7199	In/Out	MGMT	Cassandra JMX monitoring inter-site communication
TCP	9042	In/Out	MGMT	Cassandra client

A.5 HP Integrated Lights-Out (iLO) Port Settings

The following information is not specific to SDC, but relates to relevant ports configured on different servers.

Table 6: HP iLO Ports

Transport Protocol	Port	iLO Function
CP	22	Secure Shell (SSH)
TCP	80	Web Server Non-SSL

Transport Protocol	Port	iLO Function
TCP	443	Web Server SSL
TCP	3389	Terminal Services
TCP	17988	Virtual Media
TCP	9300	Shared Remote Console
TCP	17990	Console Replay

Glossary

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

Table 7: 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 (Representational State Transfer)
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
vCenter	Vmware Virtual Infrastructure tool for centralized management of multiple hypervisors and enabling functionalities
Virtual Server	A binding point used by SDC to communicate with the Remote Peers (Clients and Servers)

Table 8: 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

Term	Definition
EMS Site	Element Management System Site
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
OVF	Open Virtualization Format
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

Term	Definition
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
UE	User Equipment
URI	Universal Resource Identification.
VIP	Virtual IP
VM	Virtual Machine
VNFC	Virtualized Network Function Component
VPLMN	Visited Public Land Mobile Network
Web UI	Web User Interface
WS	Web Service