Signaling Delivery Controller

Bare Metal System Upgrade Guide

5.2

Catalog Number: RG-024-52-1 Ver. 7

Publication Date: January 2024

Legal Information

Copyright

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

Trademarks

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

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

Patents

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

Confidential and Proprietary

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

About F5 Networks

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

About this Document

Document Name: F5 Signaling Delivery Controller Bare Metal System Upgrade Guide

Catalog Number: RG-024-52-1 Ver. 7

Publication Date: January 2024

Document Objectives

This document describes the necessary procedures to set up and install bare metal deployments of SDC and EMS sites.


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

Document History

Revision Number	Change Description	Change Location
Ver.2 – June 2022	1. Update Cassandra commands. 2. Update interfaces name from eth to eno/ens. 3. Update Map the Network Interfaces between Releases section	*3. Map the Network Interfaces between Releases*
Ver.3 – November 2022	Update Salt Master network ID to IC and moved from external ports to internal ports table	*Table 6: EMS Internal Ports* *Table 8: SDC Internal Ports*
Ver.4 – March 2023	Added a prerequisite in case of upgrade from CF 3 (or lower) to CF 4 (or higher)	*Upgrade from CF-5 or lower to CF-6 or higher*
Ver.4 – May 2023	Add IC Network note	*Map the Network Interfaces between Releases*

Revision Number	Change Description	Change Location
Ver.6 – May 2023	Update master0 and mater1 and ip1 networks and IP address of ip1 in the example.	*Defining Master and Minion Servers*
Ver.7 – January 2024	Modified the prerequisite in case of upgrade from CF 5 (or lower) to CF 6 (or higher)	*Upgrade from CF-5 or lower to CF-6 or higher*

Conventions

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

Table 1: Conventions

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

Table of Contents

List of Figures

List of Tables

1. Introduction

The F5® Traffix® Signaling Delivery Controller™ (SDC) 5.2 release can be upgraded from any SDC 5.1 release.

In addition, SDC sites installed with an early build of SDC release 5.2 can be upgraded to a later build of this SDC release, as part of a Rolling Upgrade.

The following procedures are described in this document:

- *Upgrading an EMS Deployment from 5.1 to 5.2*
- *Upgrading a Standalone SDC Site*
- *Performing a Rolling Upgrade*
- *Performing a Rollback to 5.1*
- *Performing a Rollback to a Previous 5.2 CF*

2. Upgrading an EMS Deployment from 5.1 to 5.2

In a deployment with multiple SDC sites managed by a central EMS site, the EMS site must be upgraded first. Once the EMS site is upgraded, the SDC sites in the deployment should each be upgraded, in succession.

2.1 EMS Upgrade Prerequisites

The following prerequisites must be completed before starting the upgrade:

2.1.1 Back Up Site Data

It is recommended to create an external backup of the EMS site data folder before beginning the upgrade in /data/backup.

 Note: TDR generated data is not automatically saved in the backup site data and therefore is not included as part of the upgrade.

2.1.2 Map the Network Interfaces between Releases

SDC 5.2 release is running on Linux RedHat 8 in which the interfaces names are eno/ens (depends on the NIC type).

The networking definitions previously defined in the SDC 5.1 release need to be modified for the SDC 5.2 release. These modifications must be reflected in the definitions configured in the site topology file for any EMS and/or SDC site before upgrading.

This section describes how to create a table of the networking changes. For more information about how to update the site topology file, see *Update the Site Topology File with exportRoutes.py Script.*

Note: The IC Network interfaces must be connected to a switch and not directly between the servers/nodes.

2.1.2.1 Map the Network Interfaces in SDC 5.1

1. Extract the 5.2 release ISO image to a local folder and go to:

   traffix/repositories/traffix folder.

2. Locate the salt-srv.rpm package, and extract the data to a local folder.

3. Go to the scripts folder located at the following path:

```
..\<customer_defined_local_folder>\salt-
srv<latest_version>.noarch\salt-
srv<latest_version>.noarch.cpio\.\opt\traffix\salt-
srv\<latest_version>\archive.tar\salt\system\scripts
```

4. Copy this folder to each site server, and run the following commands:

   # dos2unix showNetMap.sh

   # chmod +x showNetMap.sh

5. Run the following script:

   # ./ showNetMap.sh

As shown in the following example output, a table is displayed with the current network interfaces.

Note: The below output will be saved as **/tmp/5.1_network_interfaces.txt**.

You must download it from the server – it will be used during the 5.2 OS installation.

```
You are running SDC 5.1 - Redhat 6

The list of 5.1 network interfaces mapping:

CURRENT HWADDR
-------- -----------------
eth0  ec:b1:d7:a3:d5:f0
eth1  ec:b1:d7:a3:d5:f8
eth2  ec:b1:d7:a3:d5:f1
eth3  ec:b1:d7:a3:d5:f9
eth4  ec:b1:d7:a3:d5:f2
eth5  ec:b1:d7:a3:d5:fa
eth6  ec:b1:d7:a3:d5:f3
eth7  ec:b1:d7:a3:d5:fb
```

 Note: You can also disable network interfaces by running the disabledInterfaces.sh script. The script will rename and disable the NICs that are not brought up while the boot (BOOT=no), and the naming convention is “disabled<interface-name>”.

```
..\<customer_defined_local_folder>\salt-
srv<latest_version>.noarch\salt-
srv<latest_version>.noarch.cpio\.\opt\traffix\salt-
srv\<latest_version>\archive.tar\salt\network\disabledInterfaces.sh
```

Execution example:

```
Shutting down interface bond3.555: [ OK ]
Shutting down interface bond0: [ OK ]
Shutting down interface bond1: [ OK ]
Shutting down interface bond3: [ OK ]
Shutting down loopback interface: [ OK ]
Bringing up loopback interface: [ OK ]
```

```
Bringing up interface bond0: Determining if ip address 172.29.55.201 is
already in use for device bond0...
                                                           [ OK ]
Bringing up interface bond1: Determining if ip address 10.1.54.9 is
already in use for device bond1...
                                                           [ OK ]
Bringing up interface bond3: [ OK ]
Bringing up interface bond3.555: Determining if ip address 10.1.55.9 is
already in use for device bond3.555...
                                                           [ OK ]
```

6. Run showNetMap script:

```
The list of 5.1 network interfaces mapping:

CURRENT HWADDR
-------- -----------------
eth0  ec:b1:d7:a3:d5:f0
eth1  ec:b1:d7:a3:d5:f8
eth2  ec:b1:d7:a3:d5:f1
eth3  ec:b1:d7:a3:d5:f9
disabledeth4  ec:b1:d7:a3:d5:f2
disabledeth5  ec:b1:d7:a3:d5:fa
eth6  ec:b1:d7:a3:d5:f3
eth7  ec:b1:d7:a3:d5:fb
```

2.1.2.2 Map the Network Interfaces between Releases


Note: This section need be performed after the new Redhat 8 OS installation is completed and before updating the Topology.

1. Extract the 5.2 release ISO image to a local folder and go to:

   traffix/repositories/traffix folder.

2. Locate the salt-srv.rpm package, and extract the data to a local folder.

3. Go to the scripts folder located at the following path:

```
..\<customer_defined_local_folder>\salt-
srv<latest_version>.noarch\salt-
srv<latest_version>.noarch.cpio\.\opt\traffix\salt-
srv\<latest_version>\archive.tar\salt\system\scripts
```

4. Copy this folder to each site server, and run the following commands:

   # dos2unix showNetMap.sh

   # chmod +x showNetMap.sh

5. Run the following script:

   # ./ showNetMap.sh

```
You are running SDC 5.2 - Redhat 8

The list of 5.1 to 5.2 network interfaces mapping:

OLD       NEW       HWADDR
--------  --------  -----------------
eth0      eno49     ec:b1:d7:a3:d5:f0
eth1      eno50     ec:b1:d7:a3:d5:f8
eth2      eno51     ec:b1:d7:a3:d5:f1
eth3      eno52     ec:b1:d7:a3:d5:f9
eth4      eno53     ec:b1:d7:a3:d5:f2
eth5      eno54     ec:b1:d7:a3:d5:fa
eth6      eno55     ec:b1:d7:a3:d5:f3
eth7      eno56     ec:b1:d7:a3:d5:fb
```

Now you can use the above interfaces name in the new Topology file.

2.1.3 Update the Site Topology File with exportRoutes.py Script

For overall information about the site topology file, refer to *The F5 SDC 5.2 Bare Metal Installation Guide Appendix A: Site Topology File Structure*.

The exportRoutes.py (IP Route) script allows you to export the IP routes from the Cassandra DB and print them in the correct Topology xml format.

The output will contain the name of the site > node and interface > existing routes, for example:

```
Site:   SDC_Site008-07-08
-------------------------------
sdclab008-08    fep-sctp-a-out-vip
<route name="turing-08-sig2" net4="10.1.72.18" ip4sub="32"
gateway="10.1.56.1"/>
sdclab008-08    fep-sctp-b-out-vip
<route name="turing-08-sig3" net4="10.1.73.18" ip4sub="32"
gateway="10.1.57.1"/>
```

To extract the production IP routes prior to an upgrade to push the most updated routes to the topology file.

1. Access the script in: */srv/traffix/utils/.*
2. Run the following script only once on one of the Cassandra/oam db nodes (EMS / SDC master - the table is duplicated across all Cassandra copies).

 # python /srv/traffix/utils/exportRoutes.py <Cassandra MGMT IP>

 Note: Running the script without the Cassandra MGMT IP will result with the below error:

[root@sdclab008-05 ~]# python /srv/traffix/utils/exportRoutes.py

ERROR

Script is missing a variable!

Script is expecting the MGMT IP argument

Syntax example:

/srv/traffix/utils/exportRoutes.py 1.1.1.1.

An example of valid output:

```
root@sdclab008-05 ~]# python2 /srv/traffix/utils/exportRoutes.py
172.29.55.201
Site:   SDC_Site008-07-08
------------------------------
sdclab008-08    fep-sctp-a-out-vip
<route name="turing-08-sig2" net4="10.1.72.18" ip4sub="32"
gateway="10.1.56.1"/>
<route name="turing-08-sig2" net4="10.1.72.18" ip4sub="32"
gateway="10.1.56.1"/>
sdclab008-08    fep-sctp-b-out-vip
<route name="turing-08-sig3" net4="10.1.73.18" ip4sub="32"
gateway="10.1.57.1"/>
<route name="turing-08-sig3" net4="10.1.73.18" ip4sub="32"
gateway="10.1.57.1"/>
sdclab008-08    fep-sctp-b-in-vip
<route name="turing-07-sig3" net4="10.1.73.11" ip4sub="32"
gateway="10.1.57.1"/>
<route name="turing-07-sig3" net4="10.1.73.11" ip4sub="32"
gateway="10.1.57.1"/>
sdclab008-08    fep-sctp-a-in-vip
<route name="turing-07-sig2" net4="10.1.72.11" ip4sub="32"
gateway="10.1.56.1"/>
```

```
<route name="turing-07-sig2" net4="10.1.72.11" ip4sub="32"
gateway="10.1.56.1"/>
sdclab008-08    fep-tcp-in-vip
<route name="Turing-sig1" net4="10.1.71.0" ip4sub="24"
gateway="10.1.55.1"/>
<route name="Turing-sig1" net4="10.1.71.0" ip4sub="24"
gateway="10.1.55.1"/>
sdclab008-07    fep-sctp-a-out-vip
<route name="turing-08-sig2" net4="10.1.72.18" ip4sub="32"
gateway="10.1.56.1"/>
<route name="turing-08-sig2" net4="10.1.72.18" ip4sub="32"
gateway="10.1.56.1"/>
sdclab008-07    fep-sctp-b-out-vip
<route name="turing-08-sig3" net4="10.1.73.18" ip4sub="32"
gateway="10.1.57.1"/>
<route name="turing-08-sig3" net4="10.1.73.18" ip4sub="32"
gateway="10.1.57.1"/>
sdclab008-07    fep-sctp-b-in-vip
<route name="turing-07-sig3" net4="10.1.73.11" ip4sub="32"
gateway="10.1.57.1"/>
<route name="turing-07-sig3" net4="10.1.73.11" ip4sub="32"
gateway="10.1.57.1"/>
sdclab008-07    fep-sctp-a-in-vip
<route name="turing-07-sig2" net4="10.1.72.11" ip4sub="32"
gateway="10.1.56.1"/>
<route name="turing-07-sig2" net4="10.1.72.11" ip4sub="32"
gateway="10.1.56.1"/>
sdclab008-07    fep-tcp-in-vip
<route name="Turing-sig1" net4="10.1.71.0" ip4sub="24"
gateway="10.1.55.1"/>
<route name="Turing-sig1" net4="10.1.71.0" ip4sub="24"
gateway="10.1.55.1"/>
```

2.1.4 Install the HP SSA CLI Utility – in case needed

The HP SSA CLI Utility is used throughout the upgrade. For the Split and Merge Disk mirror procedures.

To install the HP SSA CLI Utility RPM file (hpssacli.rpm):

1. Download and install the HP SSA CLI Utility RPM file (hpssacli.rpm) from the following link per which RHEL you are using in 5.1:

- For RHEL 6: http://downloads.linux.hpe.com/repo/spp/redhat/6/x86_64/current/
- For RHEL 7: http://downloads.linux.hpe.com/repo/spp/redhat/7/x86_64/current/

2.1.5 Validate System Resources

An integral part of the upgrade process is the site mirror process. This process designates one of the HP Arrays as a backup array, ensuring support for upgrade rollbacks. The split mirror process is supported by a specific HP configuration.

Just before beginning the upgrade, perform the following steps to validate that your HP configuration is supported:

 Note: Perform this prerequisite as close as possible to performing the upgrade. The supported controller types are those listed in the most recent CF Release Notes (Supported Firmware Versions):

---

1. Validate the RAID Controller type by running the following command:

   # hpssacli ctrl all show

2. Validate the RAID Controller cache size by running the following command:

   # hpssacli ctrl all show detail |grep -i "Total Cache Size"

   The minimum supported cache size is:

512MB (Blade)

1GB FBWC Cache (DL380)

3. Verify that the RAID Controller has battery backup by running the following command and getting an OK response:

   # hpssacli ctrl all show detail |grep -i Battery |grep -i Status

4. Validate the RAID Controller firmware version by running the following command:

   # hpssacli ctrl all show detail |grep -i Firmware

2.2 Performing an EMS Upgrade

Warning: All configuration changes performed locally on SDC sites while the EMS site is being upgraded will be overridden by the configuration data distributed by the upgraded EMS site. It is therefore recommended to not perform any configuration changes on the SDC site(s) while the EMS site is being upgraded.

2.2.1 Performing a Split Mirror on All Sites (EMS + SDC)

During this phase, a backup array is created to enable upgrade rollbacks.

To create a backup array:

1. Perform the Split Mirror procedure to designate one of the HP Arrays as a backup array:
   a. Run the following command to verify that the logical drive is in an "OK" state:

      # hpssacli controller slot=0 ld all show

   b. Run the following command to create a backup array:

      # hpssacli controller slot=0 array A splitmirror action=splitwithbackup

   c. Enter "y" to confirm that you want to continue after being prompted with the warning message.

   d. Run the following command to verify that there are two arrays, each with a logical drive, and that backup logical drive was created.

      # hpssacli controller slot=0 ld all show

Note: To ensure successful rollbacks, be sure to clearly mark which array and logical disk are the backup.

   e. Run the following command to create a visual marker for the mirrored array:

 # hpssacli controller slot=0 ld <active_logicaldrive_ID> modify led=on

2.2.2 Decommission the current Cassandra site

Decommission the EMS Cassandra site before performing an upgrade.

1. Connect to each EMS node (using SSH)
2. Run the decommission command – one by one:

   # /usr/bin/nodetool decommission

3. Connect to each SDC Salt Master node (using SSH) - all sites
4. Clear the EMS MGMT IPs information from the cassandra.yaml on each SDC Salt Master node:

   # cp /srv/salt/<salt version>/oamDB/cassandra.yaml /var/tmp

   # sed -i 's/if emsIps/ if emsIps2/g' /srv/salt/<salt version>/oamDB/cassandra.yaml

5. After all **cassandra.yaml** files are updated run state.apply on **one** of the SDC Salt Master on each site:

   # salt '*' state.apply oamDB

6. Stop the Cassandra on all SDC Cassandra nodes:

   # monit stop <node name>_oamDB

7. Start one Cassandra on one SDC Cassandra node:

   # monit start <node name>_oamDB

8. Verify that the decommissioned EMS nodes no longer exist:

   # /usr/bin/nodetool gossipinfo

9. After verifying that decommissioned nodes are gone, start all other SDC Cassandra nodes.

2.2.3 Installing the Operating System

You need to install the operating system on each site machine. The operating system is installed from the ISO image. You can load the ISO image using the ILO Integrated Remote Console, any other available console or directly from your system.

 Note: The ISO image must be loaded for each server in the site. Always set up the master Installer servers and upload the site topology file to them before setting up the other site machines.

To load the ISO image:

 Note: For an EMS deployment, the following steps can be run in parallel on each EMS site.

---

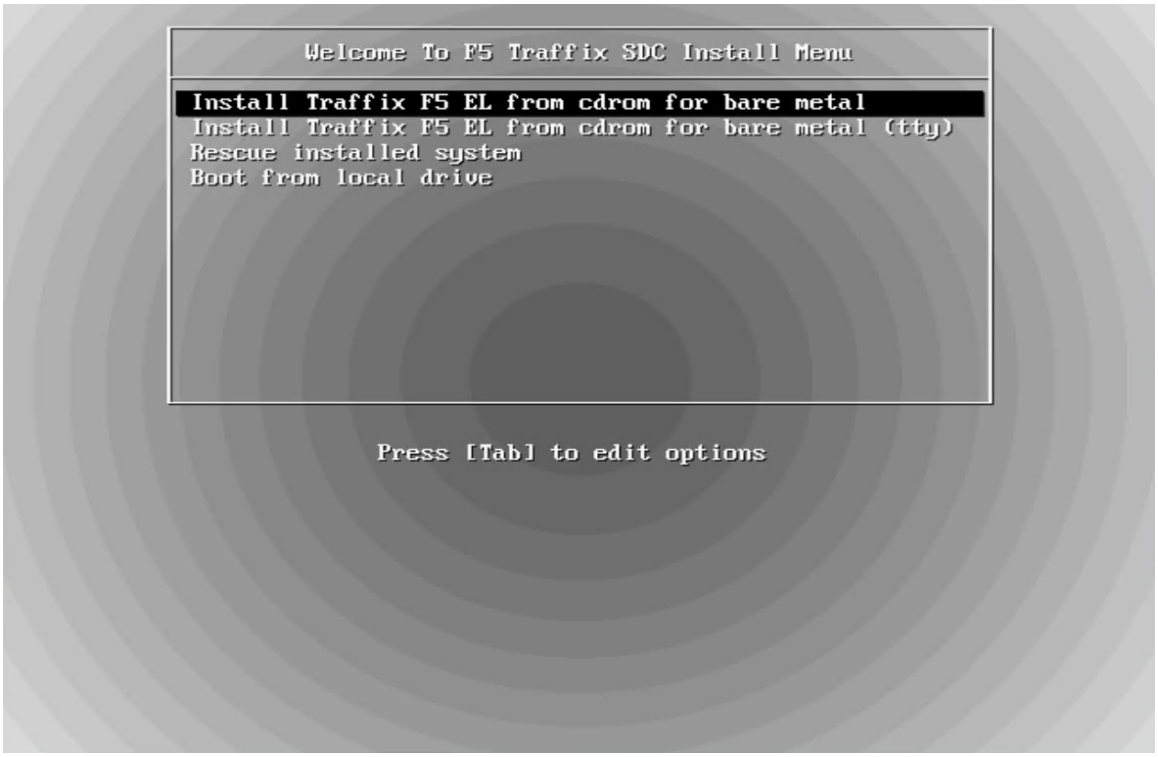
1. Select the ISO image from where it is saved on your computer.
2. Start the installed site machine from the ISO image.

   The **Welcome To F5 Traffix SDC Install Menu** is displayed.
3. Under the **Welcome To F5 Traffix SDC Install Menu**, select **Install Traffix F5 EL from cdrom for bare metal**.
4. You have two options to enter the GRUB parameters:

   - Press on the **TAB** key and enter them in a row – with spaces between each other
   - Press on the **Enter** key and after the ISO is installed to modify the */var/tmp/salt-install/paramas* file

   The GRUB boot loader page displays.

Figure 1: GRUB Boot Loader Page



2.2.4 Defining Master and Minion Servers

The GRUB boot parameters define a server's role as either a master Installer server or as a minion server that will host the SDC components. Configuring the parameters is done from the GRUB boot loader page. There are mandatory parameters and optional parameters that are only required if relevant for the deployment.

Table 2: Mandatory Parameters

Name	Value Description
server	master/minion
hostname	the server's hostname Note: The hostname must be identical (case sensitive) to the value defined under the name attribute for the vm element in the Site Topology file

Name	Value Description
master0	The IP address on the IC network that the first vInstaller uses.
master1	The IP address on the IC network that the second vInstaller uses.
ip0	The IP address is from the management network interface for minion and master Installer servers
ip1	The IP address is from the management network interface for minion and master Installer servers
netmask0	netmask for the IP0 address defined above
netmask1	netmask for the IP1 address defined above
device0	The ethernet interface used by the IP0 address defined above
device1	The ethernet interface used by the IP1 address defined above

Table 3: Optional Parameters

Name	Value Description
vlan0	vlan number for interface (if vlan defined) used by the IP0 address defined above
vlan1	vlan number for interface (if vlan defined) used by the IP1 address defined above
gw	default gateway (need to be mandatory if server = master)
debug	debug=yes enable salt log with debug
dns	DNS

The following is an example of inputted GRUB parameters:

```
server=master
ip0=172.29.55.203
ip1=172.29.55.204
netmask0=255.255.255.192
netmask1=255.255.255.224
```

```
gw=172.29.55.193
hostname=sdclab008-07
device0=eno0
device1=eno2
master0=10.1.54.11
master1=10.1.54.12
debug=yes
```

To configure the GRUB boot parameters:

1. Configure the GRUB boot parameters and then click **ENTER** when done.
2. Repeat these steps for each site machine.

   Each site server is now installed with an Operating System and has a defined role (master or minion). You can verify which servers in a site are defined as a master or minion with the siteStatus API Request.

2.2.4.1 Modifying the GRUB Boot Parameters

The GRUB boot parameters are saved in the params file. If you want to change any of the parameters or add a parameter, you can do so by editing the params file.


Note: You can only edit the parameters at this stage in the installation process, prior to uploading the Site Topology file. After editing any GRUB boot parameters in params File, you must run an installation script.

You can reconfigure a master server as a minion server, but you cannot reconfigure a minion server as a master server.

To edit the GRUB boot parameters:

1. Go to the directory where the params file is saved: *cd /var/tmp/salt-install/*
2. Execute the following command to edit the relevant parameters:

 # vi params

Note: If when entering the GRUB parameters from the GRUB boot screen, you clicked **ENTER**, but you still want to edit the parameters, you need to use the example params file to edit by executing the following command:

 # cp params.example params

3. Add/Edit a parameter according to the list of mandatory or optional parameters (see *Table 2* and *Table 3*).
4. Execute the following command to run the installation script:

 # ./salt-install.sh

Each installed site server is now updated with the edited parameters. You can verify which servers in a site are defined as a master or minion with the siteStatus API Request.

Note: If you changed the IP address of the master Installer or any of the GRUB parameters in the params file, then you need to run the installation script on all of the minion servers. If the master Installer IP address has not been changed, then you need to restart the Salt minion service.

2.2.5 Loading the Backed-Up Site Data

Note: This step is only relevant for EMS site upgrades. Once the SDC site is upgraded, the EMS site will distribute this data to the SDC site.

Note: This should be performed on each EMS site server.

Once the EMS site servers are successfully created, the backed-up site data is loaded from the logical drive previously defined as the backup logical drive

1. Install the HP SSA CLI Utility RPM file (hpssacli.rpm) by running the following command:

   # yum install ssacli

2. Migrate the backed-up site data saved in the Config Manager:

   a. Enable access to the backup disk created with the Split Mirror mechanism:

      i. Run the following command on the active array on each EMS machine:

 # ssacli controller slot=0 Array A splitmirror action=activatebackup

---

Warning: Potential loss of site data! Once this step has been performed, the logical drive is no longer defined as a backup drive, and its data is no longer protected from being overwritten. Any ISO installation performed after this point will result in the data on both logical drives being overwritten. To ensure that the data on the backed up logical drive will not be lost, follow the rollback procedure in the ***Error! Reference source not found.*** (running SDC 5.1) before starting the upgrade from the beginning.

---

   b. Run the following commands to ensure that the logical drive that is used is the logical drive that is being upgraded and is running with SDC release 5.2

   # ssacli controller slot=0 ld <active_array_logical_drive_number> modify bootvolume=primary

   # ssacli controller slot=0 ld <backup_array_logical_drive_number> modify bootvolume=secondary

   c. Run the following commands on both EMS nodes to identify the activated disk that was previously backed up:

   # grep device /etc/lvm/backup/vg1 -B1 | grep id

 # pvs -o pv_name,vg_name,pv_uuid

The output of the first command includes the disk that the system recognizes, while the output of the second command includes a list of all the disks that are installed in the system.

d. Identify the disk in the output of the second command that did not appear in the list of recognized disks (in the output of the first command), and run the following command using the disk name of the disk that did not appear in the list of recognized disks:

 # vgimportclone --basevgname vg2_clone /dev/sd<name of disk>

e. Run the following commands to mount and activate the volume that you want to restore data from:

 # lvchange -a y vg2_clone/vol_data

 # mount -t ext4 -o ro /dev/mapper/vg2_clone-vol_data /mnt

 Note: If the site must be re-installed after this stage, perform a rollback. For more information, see *Performing a Rollback to 5.1*.

---

f. Verify that the /data folder (or its subdirectories) is available for data migration:

ii. Locate the /data folder (or its subdirectories) in the site topology file and verify that it has been defined as a “mountPoint” value, meaning, to be used as a volume. Once this has been verified:

iii. Copy the updated site topology file to each site nodes

iv. On each EMS server, run the emsMigration.sh script using the –m argument, followed by the full path to the topology file:

 # /srv/salt/<current version>/system/scripts/emsMigration.sh -m

<path_to_topology_file.xml>

Note: In case the topology validation fails, the script will exit with an error.

Fix the topology.xml file and run the **emsMigration** again.

---

g. Copy the previous backup folder from the backup disk to the verified data folder:

h. On each EMS server, run the following command:

 # mkdir -p /data/backup

 # cd /mnt/

 # cp -rp backup /data/backup

2.2.6 Uploading the Site Topology File

In this phase, the site topology file is uploaded to the master Installer servers using an API request. Once the Site Topology file is uploaded successfully to the master Installer servers, the Site Topology parameters are saved in the Cassandra database in both master Installers.

Note: Upload the Site Topology file only after the below steps are completed:

1. The master Installer servers are up and running

2. The Network mapping is completed, and new interfaces names are updated (see *Map the Network Interfaces between Releases*)

To upload the Site Topology file to the Installer Machines:

1. Upload the Site Topology file to a master Installer server.
2. Authenticate the Installer REST interface by sending the following request to the master Installer to generate an authentication token:

Note: An authentication token expires after ten hours.

```
curl -ksi https://<master_IP_address>:8000/login -H "Accept:
application/json" -d username='saltuser' -d password='traffix' -d
eauth='pam'
```

Note: For all API requests, you need to use the minus sign, for example "-d" and not the N-dash "-". If you copy–paste the API request, you may have to type in the "- d" again with the minus sign to avoid syntax conversion errors.

The success return code for this request is ‘200’.

3. After validating the Site Topology file and generating an authentication token, run the following API command to upload the topology file:

```
curl -ksi https://<master_IP_address>:8000 -H "Accept: application/x-
yaml" -H "X-Auth-Token: <Token>" -d client="runner" -d
fun="traffix.uploadTopology" -X POST --data-urlencode "topology=$(cat
<Full path>/topology.xml)"
```

The response indicates if the Site Topology file has been successfully uploaded. The following is an example of the API request with a successful response:

```
# curl -ksi https://localhost:8000 -H "Accept: application/x-yaml" -H
"X-Auth-Token:fc2e8dcc1fed67dbd182b42609642b5ffcf27ed9" -d
client="runner" -d fun="traffix.uploadTopology" -X POST --data-
urlencode "topology=$(cat /tmp/topology.xml)"
@topology.xml
HTTP/1.1 100 Continue
HTTP/1.1 200 OK
Content-Length: 63
Access-Control-Expose-Headers: GET, POST
Access-Control-Allow-Credentials: true
```

```
Vary: Accept-Encoding
Server: CherryPy/3.2.2
Allow: GET, HEAD, POST
Cache-Control: private
Date: Wed, 10 Aug 2016 10:45:22 GMT
Access-Control-Allow-Origin: *
Content-Type: application/x-yaml
Set-Cookie: session_id=fc2e8dcc1fed67dbd182b42609642b5ffcf27ed9;
expires=Wed, 10 Aug 2016 20:45:22 GMT; Path=/
return:
- - 0
- topology uploaded to the server successfully
```

The Site Topology parameters are now saved in the Cassandra database in both of the master Installers. Once the Site Topology file has been uploaded successfully to the master Installer servers, set up the remaining site machines by following the Setting up the Site Machines procedure.

 Note: Once the Site Topology file has been uploaded successfully, the only way to modify the site configurations (in the params file or in the Site Topology file) is to perform a new installation by reinstalling the ISO.

2.2.7 Installing the SDC Components

The minion servers communicate with the master Installer servers and the master Installer servers then reply to the minion servers, based on the Site Topology definitions, to know where to install the different SDC components (FEP, CPF, etc.).

2.2.8 Verifying the SDC Installation Status

This verification is done by invoking the “appStatus” REST API. This REST APIs queries the master Installer about the status of the SDC applications running on a specific server

or on all the servers. This API is based on a standard Salt API interface and the body of the REST API message contains CLI Salt functions.

The site is only successfully installed once the “12000” result code is returned for the appStatus API request.

2.2.8.1 Generating an Authentication Token

Before any REST API request can be sent, you must have a valid authentication token. You need to send a request to the master Installer to generate an authentication token.

Note: An authentication token expires after ten hours.

```
curl -ksi https://<master_IP_address>:8000/login -H "Accept:
application/json" -d username='saltuser' -d password='traffix' -d
eauth='pam'
```

Note: For all API requests, you need to use the minus sign, for example "-d" and not the N-dash "-". If you copy–paste the API request, you may have to type in the "- d" again with the minus sign to avoid syntax conversion errors.

2.2.8.2 Authentication Request Status Codes

The following are the possible return codes for the authentication API request:

Return Code	Description
200	success
401	authentication required
406	requested Content-Type not available

2.2.8.3 Application Status per Server

This API request checks the status of a specific server. The response includes the relevant status codes for successfully installed applications. In addition, as with all other API requests, there are related command execution codes.

2.2.8.4 appStatus API Request

```
curl -ksi https://<master_IP_address>:8000 -H "Accept: application/x-yaml" -H "X-Auth-Token:<Token>" -d client="runner" -d fun="traffix.appStatus" -d tgt="*" -d apps=True (optional for apps list)
```

2.2.8.5 Command Execution Codes for appStatus API Request

Table 4: appStatus Command Error Codes

Exit Code	Description
-50	Failed to validate site topology file - check site topology file
-51	Installation not started yet
-52	Could not get information from DB

2.2.8.6 Return Codes for appStatus API Request

Table 5: appStatus Return Codes

Exit Code	Description
14002	Pending Machine Start
14003	Pending SDC Installation
14004	Pending SDC Start
14006	Pending SDC Stop
15002	Fail VM Start
15003	Fail To Install SDC

Exit Code	Description
15004	Fail To Start SDC
15006	Failed To Stop SDC
13000	Suspended
12000	Successfully installed

2.2.9 Verifying Site Component Status

To verify the site component status:

1. Verify that all the EMS site components are up and running according to the site topology file by running the following command:

   # monit summary

Note: If the site components are not installed, up, and running, as expected, perform an upgrade rollback. For more information, see *Performing* a Rollback to 5.1

2.3 Post-EMS Upgrade Tasks

2.3.1 Check Cassandra connection

When upgrade is done make sure that the EMS is **not** connected to any other Cassandra:

 # /usr/bin/nodetool status

 # /usr/bin/nodetool gossipinfo

2.3.2 Perform a Site Health Check

Verify that the site is running as expected by performing a health check:

1. Run the following command:

   # /srv/traffix/upgrade/upgrade-cli

2. Log in to the upgrade CLI, using traffix as your username and password.

Note: If you have changed your Web UI password since the upgrade, use the new password to log in to the upgrade CLI.

---

3. Run the following command in the upgrade CLI:

 # healthcheck

Note: If site components are up and running as expected, the EMS site has been successfully upgraded. If not, perform an upgrade rollback. For more information, see *Performing a Rollback to 5.1*.

2.3.3 Reinstalling Data Center/Customer Environment RPMs

As part of the upgrade process, previously installed Data Center/Customer environment RPMs were removed. After performing the upgrade, reinstall any relevant Data Center/Customer environment RPMs. The Data Center/Customer environment specific RPMs should match the OS version.

2.4 Upgrading SDC Sites (within an EMS deployment) from 5.1 to 5.2

When upgrading multiple SDC sites managed by an EMS site:

1. Create an upgrade schedule, defining the order that the SDC sites will be upgraded in **after** upgrading the EMS site.
2. Upgrade each of the managed SDC sites in succession, according to the order that was defined. Make sure that each SDC site is successfully upgraded before beginning the upgrade of the next SDC site. You will need to repeat the upgrade procedure for each site

Warning: The EMS site upgrade cannot be rolled back once the SDC site upgrade has begun.

2.4.1 SDC Site (within an EMS deployment) Upgrade Prerequisites

2.4.1.1 Copy the SS7 License and Configuration Files

 Note: This is only relevant for SDC sites that are configured to work with SS7.

After the upgrade, the SS7 license must be installed on the upgraded site servers. Before beginning the upgrade, copy the SS7 license for easy access after the upgrade. In addition, the SS7 configuration files must be copied to each upgraded SDC site that has an SS7 driver with a CPF.

To copy the SS7 license:

3. Go to the */opt/DSI/* directory.
4. Copy the SS7 licenses file - <filename>.lic to a local directory.

To copy the SS7 configuration files:

1. Copy the following files to a local directory:
    - /opt/DSI/config.txt and /opt/DSI/system.
    - /opt/traffix/sdc/config/ss7/routing/e212Toe214-v2.csv
    - /opt/traffix/sdc/config/ss7/routing/mmeToHlr.csv
    - /opt/traffix/sdc/config/ss7/routing/hss.csv
    - /opt/traffix/sdc/config/ss7/routing/hlr.csv

Note: If a new version of the SS7 driver is installed during the upgrade, compare the original configuration files to the new version files. If configuration file sets are not identical, ensure that the relevant SS7 driver version files are later restored during the upgrade.

2.4.2 Decommission the Current Cassandra site

Decommission the SDC Cassandra site before performing an upgrade.

1. Connect to each SDC node (using SSH)
2. Run the decommission command – one by one:

   # /usr/bin/nodetool decommission

3. Stop the Cassandra on **all** SDC Cassandra nodes:

   # monit stop <sdc node name>_oamDB

   Note: Do not start the Cassandra service on the local decommissioned SDC site after this step, it will reconnect to other SDC sites as a cluster.

4. Start the Cassandra on all the other SDC Cassandra nodes except the decommissioned SDC site:

   # monit start <sdc node name>_oamDB

5. Verify that the decommissioned SDC nodes no longer exists:

   # /usr/bin/nodetool gossipinfo

2.4.3 Performing an SDC Site (within an EMS deployment) Upgrade

The SDC Site upgrade procedures are the same as for the EMS Upgrade. Refer to

Performing an EMS Upgrade for the following:

- *Installing the Operating System*
- *Defining Master and Minion Servers*
- *Modifying the GRUB Boot Parameters*
- *Uploading the Site Topology File*
- *Installing the SDC Components*
- *Verifying the SDC Installation Status*
- *Verifying Site Component Status*

2.4.4 Post-SDC Site (within an EMS deployment) Upgrade Tasks

2.4.4.1 Check Cassandra connection

When upgrade is done make sure that the EMS is only connected to the Cassandra on the upgraded site:

 # /usr/bin/nodetool status

 # /usr/bin/nodetool gossipinfo

2.4.4.2 Perform a Site Health Check

See *Perform a Site Health Check*.

2.4.4.3 Install the SS7 License

 Note: This is only relevant for SDC sites that are configured to work with SS7.

Each server running SS7 must have a license installed.

To install the SS7 license, perform the following step on every server that will run SS7:

1. Copy the saved SS7 license file to `/opt/DSI`
2. Stop and start the CPF component by running the following:

   monit stop <server_name><cpf_name>

   monit start <server_name><cpf_name>

2.4.4.4 Add Licenses to New FEP IP Addresses

Each FEP IP address must have a license. During the upgrade, additional IP addresses may have been added to the FEP instances. If additional FEP IP addresses were added, these IP addresses much each have their own license. For more information about obtaining the

license, contact *F5 Support* and refer to the *F5 SDC User Guide* on how to add a new license key.

2.4.4.5 Reinstalling Data Center/Customer Environment RPMs

See *Reinstalling Data Center/Customer Environment RPMs*

2.5 Post Network Upgrade

After successfully upgrading all the sites (EMS + SDC) re-mirror the disks across all nodes.

ssacli controller slot=0 array <active_array> splitmirror action=remirror

3. Upgrading a Standalone SDC Site

You can upgrade a standalone 5.1 SDC site to 5.2 standalone site.

Note: Since this is a standalone site, this upgrade causes downtime. The expected downtime is approximately 2 hours.

3.1 Standalone SDC Site Upgrade Prerequisites

See the following prerequisites:

- *Back Up Site Data*
- *Map the Network Interfaces between Releases*
- *eth0 ec:b1:d7:a3:d5:f0*
- *eth1 ec*:b1:d7:a3:d5:f8

```
eth2  ec:b1:d7:a3:d5:f1
eth3  ec:b1:d7:a3:d5:f9
disabledeth4  ec:b1:d7:a3:d5:f2
disabledeth5  ec:b1:d7:a3:d5:fa
eth6  ec:b1:d7:a3:d5:f3
eth7  ec:b1:d7:a3:d5:fb
```

3.1.1.1 Map the Network Interfaces between Releases

Note: This section need be performed after the new Redhat 8 OS installation is completed and before updating the Topology.

---

3. Extract the 5.2 release ISO image to a local folder and go to:

   traffix/repositories/traffix folder.

4. Locate the salt-srv.rpm package, and extract the data to a local folder.

5. Go to the scripts folder located at the following path:

```
..\<customer_defined_local_folder>\salt-
srv<latest_version>.noarch\salt-
srv<latest_version>.noarch.cpio\.\opt\traffix\salt-
srv\<latest_version>\archive.tar\salt\system\scripts
```

6. Copy this folder to each site server, and run the following commands:

 # dos2unix showNetMap.sh

 # chmod +x showNetMap.sh

7. Run the following script:

 # ./ showNetMap.sh

```
You are running SDC 5.2 - Redhat 8

The list of 5.1 to 5.2 network interfaces mapping:

OLD       NEW       HWADDR
--------  --------  -----------------
eth0      eno49     ec:b1:d7:a3:d5:f0
eth1      eno50     ec:b1:d7:a3:d5:f8
eth2      eno51     ec:b1:d7:a3:d5:f1
eth3      eno52     ec:b1:d7:a3:d5:f9
eth4      eno53     ec:b1:d7:a3:d5:f2
eth5      eno54     ec:b1:d7:a3:d5:fa
eth6      eno55     ec:b1:d7:a3:d5:f3
eth7      eno56     ec:b1:d7:a3:d5:fb
```

Now you can use the above interfaces name in the new Topology file.

- Update the Site Topology File with exportRoutes.py Script
- *Install the HP SSA CLI Utility*

- *Validate System Resources*
- *Copy the SS7 License and Configuration Files*

3.2 Performing a Standalone SDC Site Upgrade

See the following procedures:

- *Performing a Split Mirror*
- *Installing the Operating System*
- *Defining Master and Minion Servers*
- *Modifying the GRUB Boot Parameters*
- *Loading the Backed-Up Site Data*
- *Uploading the Site Topology File*
- *Installing the SDC Components*
- *Verifying the SDC Installation Status*
- *Verifying Site Component Status*

3.3 Post-Standalone SDC Site Upgrade Tasks

3.3.1 Perform a Site Health Check

See *Perform a Site Health Check*.

3.3.2 Re-Mirror the Drives

See ***Error! Reference source not found.***

3.3.3 Install the SS7 License

 Note: This is only relevant for SDC sites that are configured to work with SS7.

Each server running SS7 must have a license installed.

To install the SS7 license, perform the following step on every server that will run SS7:

1. Copy the saved SS7 license file to `/opt/DSI`
2. Stop and start the CPF component by running the following:

   # monit stop <server_name><cpf_name>

   # monit start <server_name><cpf_name>

3.3.4 Add Licenses to New FEP IP Addresses

Each FEP IP address must have a license. During the upgrade, additional IP addresses may have been added to the FEP instances. If additional FEP IP addresses were added, these IP addresses much each have their own license. For more information about obtaining the license, contact *F5 Support* and refer to the *F5 SDC User Guide* on how to add a new license key.

3.3.5 Reinstalling Data Center/Customer Environment RPMs

See *Reinstalling Data Center/Customer Environment RPMs*

4. Performing a Rolling Upgrade

You can perform a rolling upgrade from a 5.2 release to a new 5.2 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. If 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 60 minutes per site, with minimal downtime. After completing the upgrade of all the components (applications), you need to upgrade the operating system.

4.1 Prerequisites

This section describes the prerequisites of a rolling upgrade.

4.1.1 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/traffix/upgrade/upgrade-cli

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

Figure 2: Upgrade CLI Application Login

```
[root@sdclab008-05 ~]# /srv/traffix/upgrade/upgrade-cli
webui Username: traffix
webui Password:
[upgrade-cli: 5.2_1-2]#
```

4.1.2 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 load it.

4.1.3 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: 5.2_1-2]# healthcheck
sdclab008-08_tripo1           : SUCCESS
sdclab008-08_keepalived       : SUCCESS
sdclab008-08_webui            : SUCCESS
sdclab008-07_tripo1           : SUCCESS
sdclab008-08_cpf1             : SUCCESS
sdclab008-07_fep-tcp-in       : SUCCESS
sdclab008-07_fep-sctp-out     : SUCCESS
sdclab008-07_nmsagent         : SUCCESS
sdclab008-07_vnf              : SUCCESS
sdclab008-07                  : SUCCESS
sdclab008-07_cm               : SUCCESS
sdclab008-07_oamDB            : SUCCESS
sdclab008-08                  : SUCCESS
sdclab008-07_cpf1             : SUCCESS
sdclab008-07_webui            : SUCCESS
sdclab008-08_oamDB            : SUCCESS
sdclab008-08_vnf              : SUCCESS
sdclab008-07_fep-sctp-in      : SUCCESS
sdclab008-08_fep-tcp-out      : SUCCESS
sdclab008-08_tomcat           : SUCCESS
sdclab008-07_keepalived       : SUCCESS
sdclab008-07_fep-tcp-out      : SUCCESS
sdclab008-08_fep-sctp-in      : SUCCESS
sdclab008-08_nmsagent         : SUCCESS
sdclab008-07_tomcat           : SUCCESS
sdclab008-08_fep-sctp-out     : SUCCESS
sdclab008-07_fluent           : SUCCESS
sdclab008-08_fep-tcp-in       : SUCCESS
sdclab008-08_cm               : SUCCESS
sdclab008-08_fluent           : SUCCESS
```

4.1.4 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.

4.1.5 Split Mirror for Rollback

During this phase, a backup array is created to enable upgrade rollbacks.

To create a backup array:

3. Perform the Split Mirror procedure to designate one of the HP Arrays as a backup array:

   i. Run the following command to verify that the logical drive is in an "OK" state:

   # ssacli controller slot=0 ld all show

   j. Run the following command to create a backup array:

   # ssacli controller slot=0 array A splitmirror action=splitwithbackup

   k. Enter "y" to confirm that you want to continue after being prompted with the warning message.

   l. Run the following command to verify that there are two arrays, each with a logical drive, and that backup logical drive was created.

   # ssacli controller slot=0 ld all show

4.1.6 Upgrade from CF-5 or lower to CF-6 or higher

If you are upgrading from version 5.2 CF 5 or lower to version 5.2 CF 6 or higher, you will need to copy the Salt "**upgrade-cli**" file from the new CF ISO in order to carry out the upgrade.

4.1.6.1 Extracting and Replacing the Salt File

1. Login using SSH to the EMS master Installer server
   (In case there is no EMS, login to the SDC master Installer server)
2. Backup existing file

   # cp /srv/traffix/upgrade/upgrade-cli /srv/traffix/upgrade/upgrade-cli_orig
3. Create temporary directories

   # mkdir -p /tmp/patch

   # mkdir -p /mnt/tmp_mount
4. Upload the new CF ISO file to the server to **/tmp/patch/**
5. Mount the new ISO

   # mount -o loop /tmp/patch/iso-5.2_<CF version>.iso /mnt/tmp_mount/
6. Copy the new Salt rpm file from the mounted ISO

   # cp /mnt/tmp_mount/traffix/Packages/salt-srv5.2_<CF version>.noarch.rpm /tmp/patch/
7. Unmount the new ISO

   # umount /mnt/tmp_mount
8. Extract the rpm contents

 # cd /tmp/patch/

 # rpm2cpio salt-srv5.2_<CF version>.noarch.rpm | cpio -idmv

 # cd /tmp/patch/opt/traffix/salt-srv/5.2_<CF version>/

 # tar xvf archive.tar

 # \cp traffix/upgrade/upgrade-cli /srv/traffix/upgrade/

9. Transfer the new Salt file (to all master Installer server that are about to be upgraded (Using SCP or any other tool)
10. Delete the temporary directories.

 # rm -rf /tmp/patch/

 # rm -rf /mnt/tmp_mount/

4.2 Update Files from the ISO image for the Component Upgrade

You need to update files from the following three repositories: BaseOS, AppStream, traffix , This is done with the copyfromISO command.

To update the files:

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/traffix/upgrade/upgrade-cli

iii. Log in with the Web UI username (traffix) and password.

iv. Run the following command to copy the RPM files from the ISO image to the */opt/repo/*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"

4.3 Upgrading the Master Installer

During this phase, the Master Installers are upgraded with the operating system included in the new ISO image (After running this command, you will be logged out of the CLI Application).

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 apply the patch file to the new state files in */srv/salt/<5.2-new rpm salt srv version>* on each Master Installer.

Once the file has been applied, and only in the case the saltupgrade was interrupted because of changes in the state file, 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:

   # /usr/bin/cqlsh <IP address>

   SELECT * FROM statusflow.appflow;

4.4 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.

To upgrade the OAM database:

1. Run the following command:

   # upgradeOamDB

4.5 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.

To upgrade the Tomcat version:

1. Run the following command:

tomcatUpgrade

4.6 Upgrading the SDC Components

During this phase, each SDC component is upgraded. 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: If HealthCheck does not show success, you cannot perform an upgrade.

4.6.1 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

4.7 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

4.8 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.

4.8.1 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.

4.8.1.1 New ISO Image

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

4.8.1.2 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.

4.8.1.3 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.*
2. Run the following command:

   # healthcheck
3. Exit the cli application:

   # exit

4.8.2 Uploading the New ISO Image

In this step, you will load the ISO and save the RPM packages in the relevant BaseOS and AppStream 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 for each repo folder:

Log in to each master Installer server.

Delete the relevant file from */opt/repo/update-BaseOS*

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

Delete the relevant file from */opt/repo/update-AppStream*

Run the commands:

createrepo_c /opt/repo/updates-AppStream

modifyrepo_c --mdtype=modules /opt/repo/updates-AppStream/<modules.yaml.gz file> /opt/repo/updates-AppStream/repodata

---

4.8.3 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/traffix/scripts/osRollingUpgrade.sh -u"

2. Run the following command for local servers:

   # /opt/traffix/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.

4.9 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 a Rollback to 5.1*

4.9.1 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 components: (Fluentd, Elasticsearch and Kibana)

To check the processes:

1. Run the following command:

   salt '*' monit.summary

4.9.2 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.

4.9.3 Monitoring SDC Release Versions

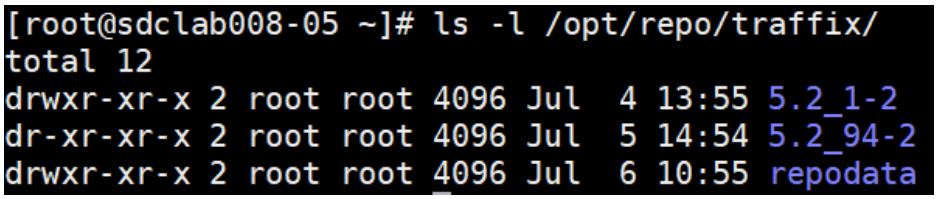
You can check which SDC release versions are available to support your deployment. Upon completing the upgrade, the previous version and the new version should be displayed.

To view the SDC release versions:

1. Run the following command:

   ls -l /opt/repo/traffix/

Figure 3: Example of Monitoring SDC Release Versions



4.9.4 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.

4.9.5 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

4.10 Post Network Upgrade

After successfully upgrading all the sites (EMS + SDC) re-mirror the disks across all nodes.

ssacli controller slot=0 array <active_array> splitmirror action=remirror

5. Performing a Rollback to 5.1

The 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 *Rolling Back an SDC Site Upgrade to Release 5.1* procedure.
- To roll back an upgrade of an EMS site before activating the backup array, following the *Rolling Back an EMS Site Upgrade to Release 5.1 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 Release 5.1 after Activating the Backup Array or a Standalone SDC Site Upgrade* procedure.

5.1 Rolling Back an SDC Site Upgrade to Release 5.1

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.


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.

To perform the upgrade rollback:

1. Stop all traffic on the SDC site.
2. Stop the applications running on the SDC site and the EMS site by running the following command on the relevant servers:

   # monit stop all

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

   # cd /data/backup

   # mv <site name> /var/tmp/

4. From the EMS mount folder, copy the 5.1 site data to the EMS /data/backup/ folder:

   # cp -rp /mnt/backup/<Site Name> data/backup/

5. Start the EMS site:

   # **monit start all**

6. While the SDC site is still down, on the EMS site, run the following command to generate the Cassandra class status:

   # /usr/bin/nodetool status

   The following is an example of the Cassandra class status for EMS Datacenter:

```
Status=Up/Down
State=Normal/Leaving/Joining/Moving
Address            Host ID
Rack
UN10.240.13.67     d126cb8a-b3e0-4a8c-a4aa-453d88316f1e RAC1
UN10.240.13.68     33eeb22a-edf0-4a52-89c7-54367b3f55a2 RAC1:
```

The following is an example of the Cassandra class status for SDC site Datacenter:

```
Status=Up/Down
State=Normal/Leaving/Joining/Moving
Address            Host ID
Rack
UN 10.240.13.69    7e5a6a30-2c2e-4a7c-bfb1-1b8508125916 RAC1
UN10.240.13.70     b9c50a48-c046-4383-a759-5ec1ae3f6ecb RAC1
```

7. From the Cassandra class status output, remove the SDC Site's host IDs, by selecting them and then running the following command:

 # /usr/bin/nodetool removenode <host ID>

For example, based on the generated SDC site datacenter output, the commands would be the following:

```
/usr/bin/nodetool removenode 7e5a6a30-2c2e-4a7c-bfb1- 1b8508125916
/usr/bin/nodetool removenode b9c50a48-c046-4383-a759- 5ec1ae3f6ecb
```

8. Clear the Cassandra data base keyspace of the rollback SDC site, by running the following script:

 # Python3 /opt/traffix/scripts/clearSdcSiteFromEms.py <SDC rollback Site name>

9. 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. Press **F5** (for Gen8) 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.

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

 # stopsh

 # cleansh

 # start.sh

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

 # monit start all

5.2 Rolling Back an EMS Site Upgrade to Release 5.1 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. Stop the applications running on the EMS site by running the following command on the relevant servers:

   # monit stop all

2. Reboot the SDC site server.

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. Press **F5** (for Gen8) 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. Restore the cassandra.yaml file:

   # cp /var/tmp/cassandra.yaml /srv/salt/<salt version>/oamDB/

6. Run state.apply:

   # salt '*' state.apply oamDB

7. Restart the Cassandra on all SDC nodes by running the following command on the relevant servers:

   # monit restart <sdc node name>_oamDB

8. Make sure that the EMS and sites are connected to the Cassandra:

   # /usr/bin/nodetool status

   # /usr/bin/nodetool gossipinfo

5.3 Rolling Back an EMS Site Upgrade to Release 5.1 after Activating the Backup Array or a Standalone SDC Site Upgrade

This procedure is used to roll back two types of upgrades:

- An EMS site upgrade, after the backup array was activated.
- A standalone SDC site upgrade, after the backup array was activated.

This procedure uses the backup array as the master copy.

To perform the upgrade rollback:

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

   # monit stop all

2. Rename volume groups:

   # **vgrename vg1 vg_temp**

   # **vgrename vg2_clone vg1**

3. Reboot the SDC site server.

4. 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. Press **F5** (for Gen8) to start the **HP Storage Controller Administrator**.

5. Define and activate the active array as the master array by performing the following steps:

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

    b. From Actions list - Click "Configure"

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

    d. Under "Arrays", select the "Active Array".

    e. Under "Actions" select "Re-Mirror Array" and select **Backup array as a source**.

    f. Define the rollback procedure:

    iii. 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.

    iv. Confirm the selection.

    g. Click “X” at the top right corner of the SSA Menu screen and confirm the exit.

    h. Click the Power Icon at the top right corner of the screen and confirm the reboot action.

6. Start the EMS site by running the following command on the relevant servers:

    # monit start all

7. Restore the cassandra.yaml file:

    # cp /var/tmp/cassandra.yaml /srv/salt/<salt version>/oamDB/

8. Run state.apply:

   # salt '*' state.apply oamDB

9. Restart the Cassandra on all SDC nodes by running the following command on the relevant servers:

   # monit restart <sdc node name>_oamDB

10. Make sure that the EMS and sites are connected to the Cassandra:

    # /usr/bin/nodetool status

    # /usr/bin/nodetool gossipinfo

6. Performing a Rollback to a Previous 5.2 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* procedure.
- To roll back an upgrade of an EMS site after activating the backup array, follow the ***Error! Reference source not found.*** procedure.

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

   # monit stop all

3. 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/

4. Start the EMS site.

5. 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) 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.

6. 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 - traffix

cd /home/traffix/Tripo/env/linux-x86_64/

. DefEnv Tripo

 # stopsh

 # cleansh

 # start.sh

7. 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.

---

8. 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.

6.2 Rolling Back an EMS Site Upgrade to a Previous CF

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

To perform the upgrade rollback:

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

   # monit stop all

2. 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) 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.

3. Start the EMS site by running the following command on the relevant servers:

 # monit start all

4. 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 "currentVersion" = '<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.

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 6: EMS Internal Ports

Transport Protocol	Port	Network	Description
TCP	4505/6	IC	Salt Master
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

Transport Protocol	Port	Network	Description
UDP	162	IC	SNMP traps listener
UDP	1162		OS trap daemon listener
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 7: 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

Transport Protocol	Port	In/Out	Network	Description
UDP	User-defined Ports (and IPs)	Out	MGMT	Trap Forwarding: For External EMS Trap listeners
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	8000	In/Out	MGMT	Salt API

Transport Protocol	Port	In/Out	Network	Description
TCP	8080/8443	In	MGMT	SDC web console (Web UI)
TCP	10040	Out	MGMT	NMS Agent to NMS Manager 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 8: SDC Internal Ports

Transport Protocol	Port	Network	Description
TCP	4505/6	IC	Salt Master
TCP	2812	IC	Monit
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

Transport Protocol	Port	Network	Description
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
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 9: SDC External Ports

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

Transport Protocol	Port	In/Out	Network	Description
				servers for new configuration propagation (internal and external data)
\TCP	22/80/443/623/17990/17988	In	MGMT	HP iLO4 management 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.

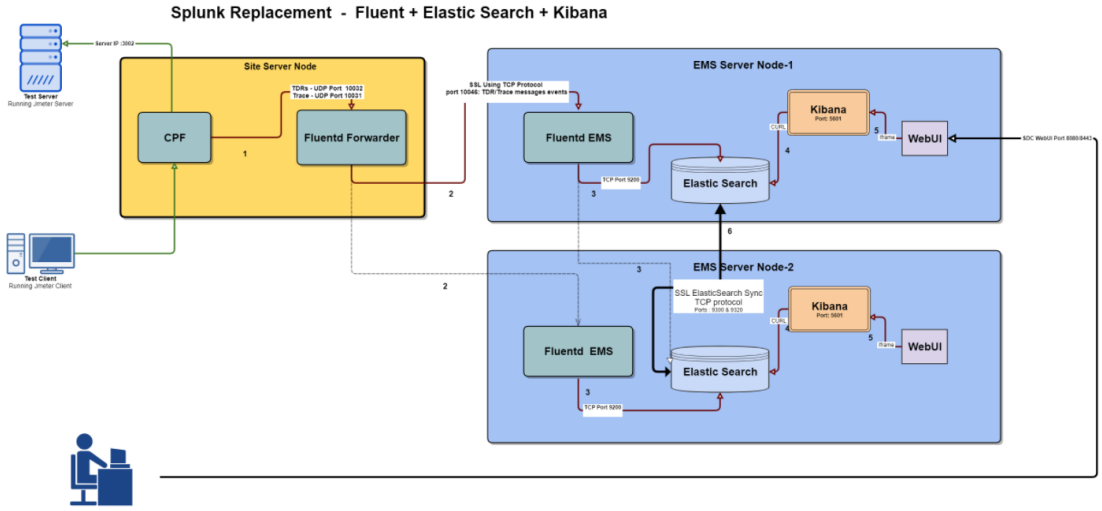
Table 10: HP iLO Ports

Transport Protocol	Port	iLO Function
CP	22	Secure Shell (SSH)
TCP	80	Web Server Non-SSL
TCP	443	Web Server SSL
TCP	3389	Terminal Services
TCP	17988	Virtual Media
TCP	9300	Shared Remote Console
TCP	17990	Console Replay

Appendix B: ELK Components

In SDC 5.2, for EMS deployments, Splunk is replaced with ELK. There are three ELK components on the EMS (Fluentd, Elasticsearch and Kibana) and one component on the SDC (Fluentd Forwarder). These components receive and forward information to create an overview of the deployment's performance and support shared configuration across multiple sites.

The following diagram shows the full flow of how information is forwarded and collected between an SDC site and EMS sites.



All of the ELK components are managed by monit and their status (up/down) is easily viewed, as all other components, on the WebUI SDC components page.

Glossary

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

Table 11: Common Terms

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

Term	Definition
Salt-API	Manages and communicates between a network of 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 12: 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