



Signaling Delivery Controller

Upgrade Guide

4.4

Catalog Number: RG-015-44-36 Ver. 3

Publication Date: June 2015



Legal Information

Copyright

© 2005-2015 F5 Networks, Inc. All rights reserved.

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

Trademarks

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

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

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 Upgrade Guide

Catalog Number: RG-015-44-36 Ver. 3

Publication Date: June 2015

Document Objectives

This document introduces and describes the In-Service Software Upgrade (ISSU) process. This document provides a high level description of the ISSU of both a single SDC site, as well as the ISSU of a deployment of multiple SDC sites managed by a central EMS site. This document describes the generic ISSU procedure. Some F5 SDC installations may require additional procedures to successfully complete the upgrade. For more information, contact *F5 Support*.

Document History

Revision Number	Change Description	Change Location
May 2015 – 2	Updates were made throughout the document.	
June 2015 – 3	The order of prerequisites was changed, the post-upgrade procedures were updated, and the upgrade rollback was updated.	See <i>Upgrading an EMS Site</i> , <i>Upgrading an SDC Site</i> , <i>Performing an Upgrade Rollback</i> , <i>Post-Upgrade Procedures</i>

Conventions

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

Table 1: Conventions

Convention	Use
Normal Text	Regular text; style: F5_Normal





Convention	Use
Normal Text Bold	Names of menus, commands, buttons, and other elements of the user interface; style: F5_Normal_Bold
<i>Normal Text Italic</i>	Links to figures, tables, and sections in the document, as well as references to other documents; style: <i>F5_Normal_CrossRef</i>
Script	Language scripts; style: F5_Scripts
Calibri	File names; F5_Normal_FileName
Table Heading	Table Headings; style: F5_Table Header Text
Table Text	Table Text; style: F5_Table_Text
 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. Document Prerequisites	1
2. About the In-Service Software Upgrade	2
2.1 What Happens During an ISSU of Multiple SDC Sites Managed by an EMS Site?	2
2.1.1 How is Data Collection per Site and Communication between Sites Affected?	5
2.2 What Happens During an ISSU of a single site?	5
2.2.1 How is Traffic Processing Affected?	7
2.2.2 How Can You Minimize the Impact Caused by an ISSU?	7
2.2.2.1 Planning the Site Server Groups that the Site Will Be Split Into	8
2.2.2.2 Planning the Correct Time to Perform the Upgrade	8
2.2.3 Can Changes Made by the ISSU be Reverted?	8
2.2.4 Which SDC Versions Can be Upgraded?	9
3. Performing In-Service Software Upgrades	10
3.1 Upgrading Multiple SDC Sites Managed by an EMS Site	10
3.2 Upgrading an EMS Site	11
3.2.1 Prerequisites	12
3.2.1.1 Plan the Two Server Groups	13
3.2.1.2 Define Which Server Group will be Upgraded First	13
3.2.1.3 Plan the Upgrade	13
3.2.1.4 Upgrade the F5 Traffix Menu	13
3.2.1.5 Upgrade the Installer	14
3.2.1.6 Copy the New Build Package	15
3.2.1.7 Verify the Current Site Status	15
3.2.1.8 Back Up Site Data	16
3.2.1.9 Validate System Resources	16
3.2.1.10 Verify Both Sets of Ports are Available	17
3.2.1.11 Verify OS Upgrade Viability	18
3.2.1.12 Validate the System RPMs	19
3.2.1.13 Delete Existing Snapshots	20
3.2.1.14 Update the EMS Site Configuration File	21
3.2.2 Performing the ISSU on an EMS Site	23
3.2.2.1 Performing Phase 1: Upgrading the First Server Group	23
3.2.2.2 Performing Phase 2: Activating Server Group 1 as Primary Server Group	31
3.2.2.3 Performing Phase 3: Upgrading Server Group 2	36
3.3 Upgrading an SDC Site	41
3.3.1 Prerequisites	41
3.3.1.1 Plan the Two Server Groups	42
3.3.1.2 Define Which Server Group will be Upgraded First	42
3.3.1.3 Plan the Upgrade When Traffic is Reduced	42
3.3.1.4 Upgrade the F5 Traffix Menu	43
3.3.1.5 Upgrade the Installer	43



3.3.1.6	Copy the New Build Package	44
3.3.1.7	Verify the Current Site Status	44
3.3.1.8	Validate System Resources	45
3.3.1.9	Verify Both Sets of Ports are Available	46
3.3.1.10	Verify OS Upgrade Viability.....	47
3.3.1.11	Validate the System RPMs	48
3.3.1.12	Delete Existing Snapshots.....	50
3.3.1.13	Update the SDC Site Configuration File	50
3.3.2	Performing the ISSU on an SDC Site	55
3.3.2.1	Performing Phase 1: Upgrading the First Server Group	55
3.3.2.2	Performing Phase 2: Activating Server Group 1 as Primary Server Group	64
3.3.2.3	Performing Phase 3: Upgrading Server Group 2.....	69
3.4	Performing an Upgrade Rollback.....	74
4.	Post-Upgrade Procedures	80
4.1	Validate the System RPMs.....	80
4.2	Enabling Tripo Site Replication	81
4.3	Enabling SS7 Driver Redundancy.....	84
5.	Glossary.....	89

List of Figures

Figure 1: Deployment Containing Multiple Sites Managed by EMS.....	2
Figure 2: Phase 1 – Upgrade EMS Site	3
Figure 3: Phase 2 – Upgrade One SDC Site	4
Figure 4: Phase 3 – Upgrade Second SDC Site	5
Figure 5: Phase 1 of an ISSU.....	6
Figure 6: Phase 2 of an ISSU.....	6
Figure 7: Phase 3 of an ISSU.....	7
Figure 8: F5 Traffix Service Menu	14
Figure 9: Installer Replacement Message	15
Figure 10: Select Configuration Screen.....	24
Figure 11: Verify Version Screen.....	25
Figure 12: Choose Servers Screen.....	26
Figure 13: Select Steps Screen	27
Figure 14: Define OS Screen	29
Figure 15: Phase 1 Progress Screen	30
Figure 16: Phase 1 Verification Screen	31
Figure 17: Migration Service Phase 2 Screen.....	32
Figure 18: Select Steps Phase 2 Screen.....	33
Figure 19: Migration Progress Screen.....	34



Figure 20: Phase 2 Verification Screen	35
Figure 21: Choose Servers Phase 3 Screen	36
Figure 22: Select Steps Phase 3 Screen.....	37
Figure 23: Define OS Phase 3 Screen	39
Figure 24: Phase 3 Progress screen	39
Figure 25: F5 Traffix Service Menu	43
Figure 26: Installer Replacement Message.....	44
Figure 27: Select Configuration Screen.....	56
Figure 28: Verify Version Screen.....	57
Figure 29: Choose Servers Screen.....	58
Figure 30: Select Steps Screen	59
Figure 31: Define OS Screen	61
Figure 32: Phase 1 Progress Screen	62
Figure 33: Phase 1 Verification Screen	64
Figure 34: Migration Service Phase 2 Screen.....	65
Figure 35: Select Steps Phase 2 Screen.....	66
Figure 36: Migration Progress Screen.....	67
Figure 37: Phase 2 Verification Screen	68
Figure 38: Choose Servers Phase 3 Screen	69
Figure 39: Select Steps Phase 3 Screen.....	70
Figure 40: Define OS Phase 3 Screen	72
Figure 41: Phase 3 Progress screen	72
Figure 42: Rollback Commands and Snapshot List with “Original” and “Snapshot”	78
Figure 43: Tripo Inter-site Connection Verification (Versions and IP Addresses)	81
Figure 44: Connection Verification of Inter-site Tripo Instances.....	82
Figure 45: SiteReplication Parameter Verification	83

List of Tables

Table 1: Conventions	II
Table 2: Port Configuration.....	18
Table 3: Phase 1 Upgrade Steps.....	27
Table 4: Phase 2 Upgrade Steps.....	33
Table 5: Phase 3 Upgrade Steps.....	37
Table 6: Port Configuration.....	47
Table 7: Phase 1 Upgrade Steps.....	59
Table 8: Phase 2 Upgrade Steps.....	66
Table 9: Phase 3 Upgrade Steps.....	70
Table 10: Terms and Abbreviations	89



1. Document Prerequisites

This document assumes that you have read the *F5 SDC Product Description* and the *F5 SDC Installation Guide*, and have a comprehensive understanding of:

1. Positioning of the SDC in and/or between networks
2. SDC and EMS deployments
3. SDC architecture
4. SDC site configuration files
5. SDC Installation Utility

This document describes the generic ISSU procedure. This procedure successfully upgrades F5 SDC deployments that were installed using an ISO package. While some F5 SDC installations may require additional procedures to successfully complete the upgrade, this document assumes that you have verified that your F5 SDC Installation can be successfully upgraded using the generic ISSU procedure. For more information, contact *F5 Support*.

2. About the In-Service Software Upgrade

The In-Service Software Upgrade (ISSU) is a granular upgrade process, where site servers are upgraded in stages. Using the ISSU, you can upgrade your active SDC and EMS sites without experiencing significant system downtime.

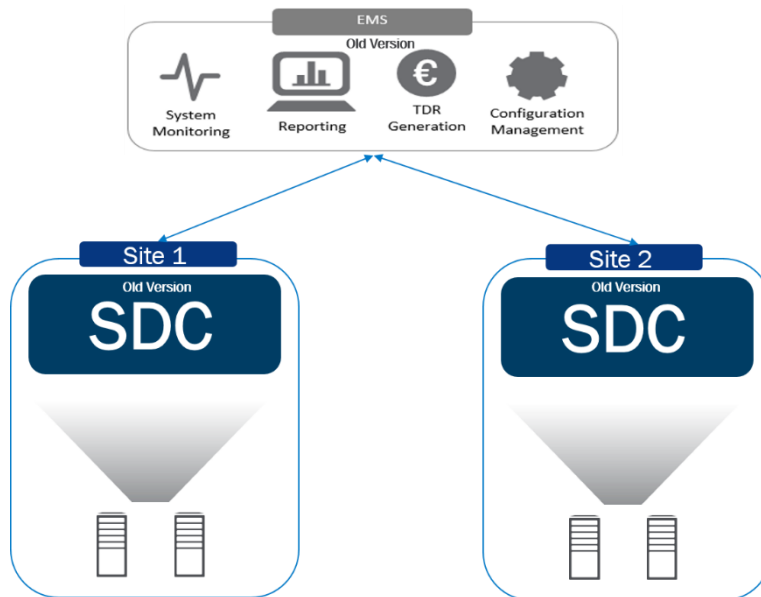
This section answers the following questions:

- *What Happens During an ISSU of Multiple SDC Sites Managed by an EMS Site?*
- *What Happens During an ISSU of a single site?*

2.1 What Happens During an ISSU of Multiple SDC Sites Managed by an EMS Site?

The ISSU of a deployment containing multiple sites managed by a central EMS site (*Figure 1*) includes the successive upgrade of each individual site.

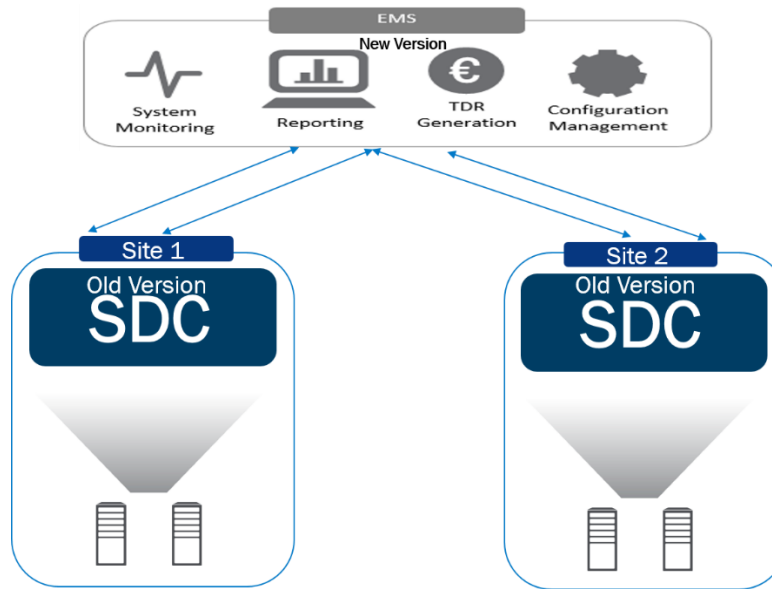
Figure 1: Deployment Containing Multiple Sites Managed by EMS



The first site that is upgraded is the EMS site managing the SDC sites (*Figure 2*).

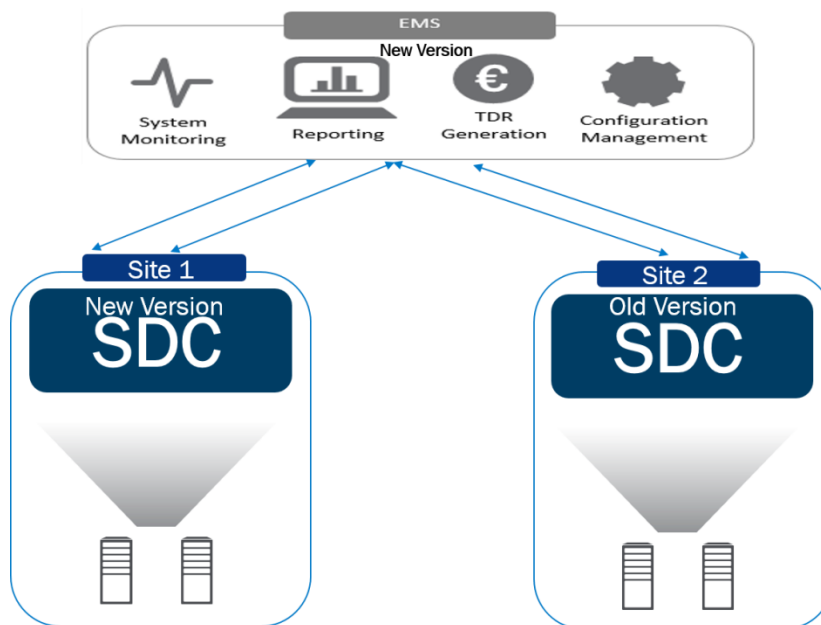


Figure 2: Phase 1 – Upgrade EMS Site



Once the EMS site is upgraded and successfully running with the new software, each SDC site is – in turn – upgraded with the new software. *Figure 3* shows the upgrade of the SDC site “Site 1”, following the successful upgrade of the EMS site.

Figure 3: Phase 2 – Upgrade One SDC Site

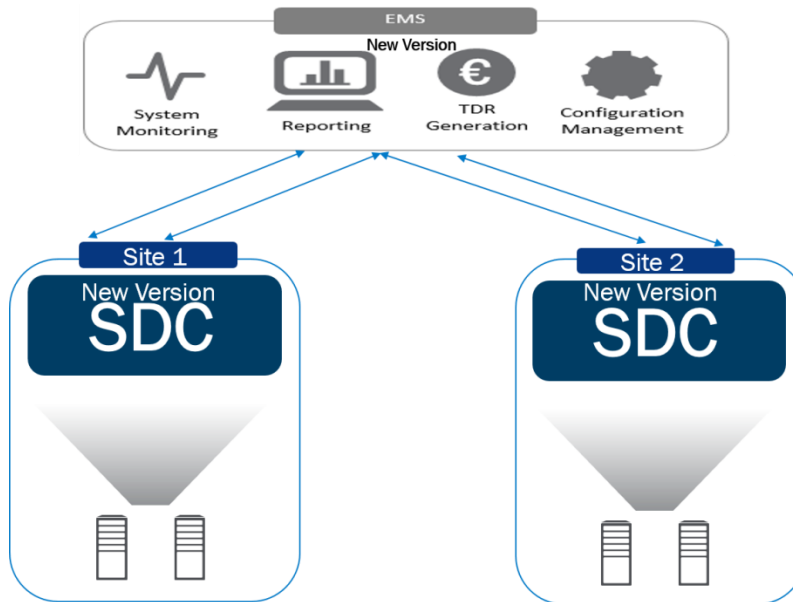


Only once “Site 1” is successfully upgraded and running with the new software is the next SDC site – “Site 2” – upgraded (*Figure 4*).



Note: Since performing an ISSU of SDC sites managed by an EMS site entails performing a separate ISSU for each site, make sure you have read and understand the ISSU and the impact it has on each single site. For more information, see the *What Happens During an ISSU of a single site?* section.

Figure 4: Phase 3 – Upgrade Second SDC Site



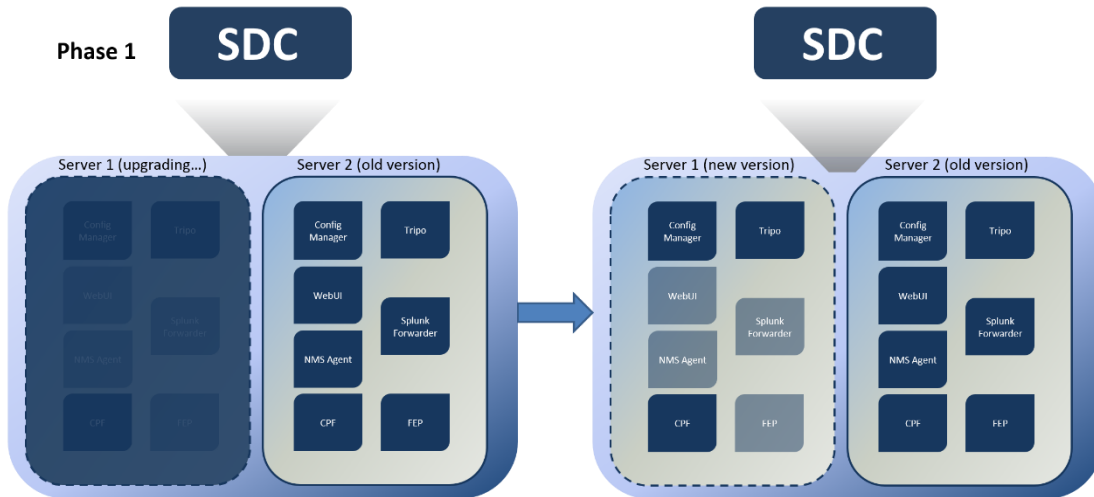
2.1.1 How is Data Collection per Site and Communication between Sites Affected?

Data Collection per site and communication between the SDC and EMS sites is not impacted by the ISSU.

2.2 What Happens During an ISSU of a single site?

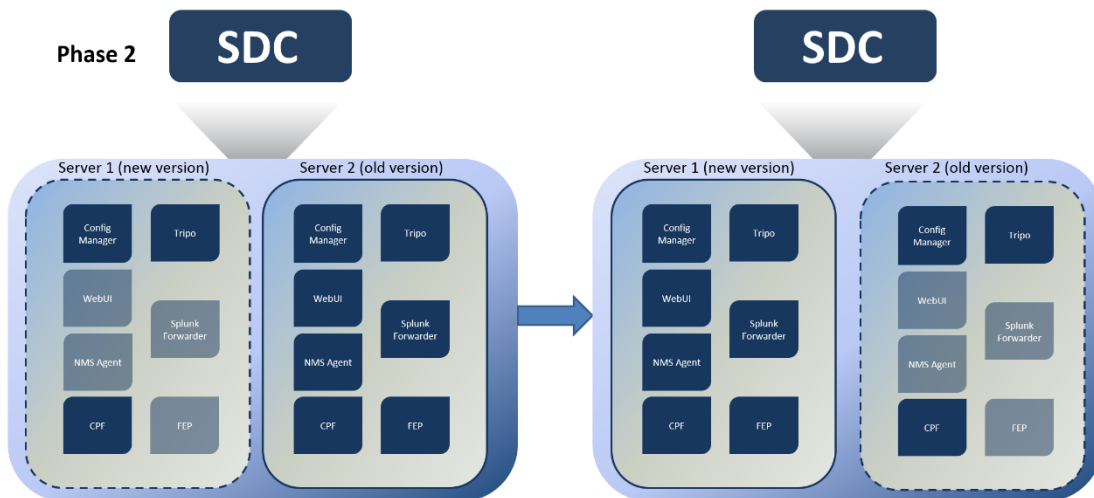
The ISSU includes three phases, illustrated in *Figure 5*, *Figure 6*, and *Figure 7*. As illustrated, the site servers are divided into two groups of servers (known as the “first server group” and the “second server group”). In the first phase (*Figure 5*), the first server group is disconnected from the site and upgraded.

Figure 5: Phase 1 of an ISSU



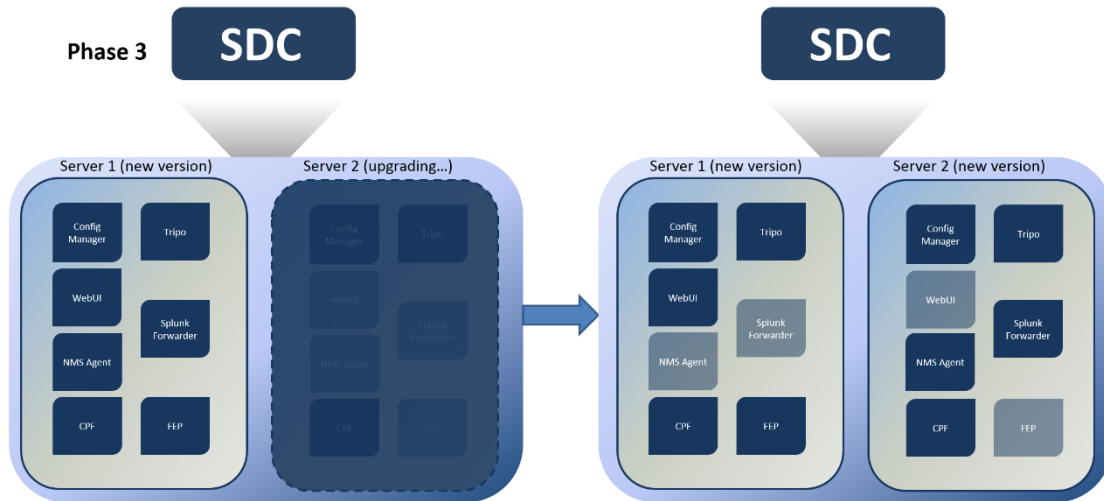
In the second phase (*Figure 6*), this group of upgraded servers is reconnected to the site and starts processing traffic, while the remaining servers – the second server group – that were not upgraded are disconnected from the site.

Figure 6: Phase 2 of an ISSU



In the third and final phase (*Figure 7*), the servers in the second server group are upgraded and are reconnected to the site.

Figure 7: Phase 3 of an ISSU



2.2.1 How is Traffic Processing Affected?

The ISSU ensures that traffic processing continues throughout the upgrade process and that site data is not lost as a result of the upgrade.

Site performance is, however, impacted as a result of the servers being disconnected from the site. For the duration of the upgrade, the site capacity decreases to approximately 30% of the usual maximum capacity, and there is no local high-availability. In addition, in each phase of the upgrade a system disruption of no more than thirty seconds each may be experienced. This system disruption is caused by the FEP failover. More information about this disruption is mentioned where it may occur in the *Performing the ISSU on an SDC Site* section.

The site upgrade (successfully completing all three phases of the ISSU) may take up to two hours.

2.2.2 How Can You Minimize the Impact Caused by an ISSU?

Proper preparation for an ISSU will ensure that the impact on the site is minimal.

Two important preparations include:

- *Planning the Site Server Groups that the Site Will Be Split Into*



- *Planning the Correct Time to Perform the Upgrade*

2.2.2.1 Planning the Site Server Groups that the Site Will Be Split Into

The main reason that performing an ISSU only minimally impacts performance is the site's ability to continue processing traffic throughout the upgrade. In each of the upgrade phases, as the site servers are upgraded, only one group of site servers ("server groups") is connected to the site and is processing traffic. The site can only continue to process traffic if each group that the site servers are split into contains at least one occurrence of each SDC component running on the site.

Correctly splitting the site servers into two groups is a prerequisite of the ISSU. For examples about how to correctly split your site servers into two groups, see the *Plan the Two Server Groups* section.

2.2.2.2 Planning the Correct Time to Perform the Upgrade

During each phase of the ISSU, only about half of the site servers will be connected to the site and processing traffic. As a result, while traffic will continuously be processed, the site capacity will be reduced to process up to 30% of the typical maximum capacity.

Therefore, correctly planning the maintenance window in which to perform the upgrade can greatly influence the impact felt on site performance. Try to perform the upgrade during the site's off-peak hours, when the expected traffic doesn't exceed 30% of the site's maximum capacity. Alternatively, for the duration of the upgrade, limit the traffic sent to the site to up to 30% of the site's maximum capacity.

2.2.3 Can Changes Made by the ISSU be Reverted?

The ISSU includes three phases. Each phase of the ISSU is supported by the upgrade rollback procedure. The rollback procedure reverts changes made on the site servers, and returns them to their original state.

For more information about the upgrade rollback procedure, see *Performing an Upgrade Rollback*.



2.2.4 Which SDC Versions Can be Upgraded?

The ISSU is supported by all SDC systems running release versions later than and including release 4.0.2, provided they were installed from the installation ISO package. Specifically, the ISSU can be used to upgrade to SDC release 4.4 from all SDC release versions later than (and including) 4.0.2. The ISSU can also be used to upgrade from one build to a later build of SDC release 4.4.



3. Performing In-Service Software Upgrades

This section includes the following topics:

- *Upgrading Multiple SDC Sites Managed by an EMS Site*
- *Upgrading an EMS Site*
- *Upgrading an SDC Site*

3.1 Upgrading Multiple SDC Sites Managed by an EMS Site

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.



Note: This section describes the ISSU procedure necessary to upgrade multiple SDC sites managed by an EMS site. To upgrade a single SDC site that is not managed by an EMS site, see the *Upgrading an SDC Site* section.

To upgrade multiple SDC sites managed by an EMS site, perform the following steps. Verify that you have successfully completed each step before advancing to the next step:

1. Upgrade the EMS site, following the instructions in the *Upgrading an EMS Site* section.
2. Upgrade the first local SDC site, following the instructions in the *Upgrading an SDC Site* section.
3. If needed, wait the agreed upon “freeze period” between upgrading local SDC sites.
4. Upgrade the next local SDC site, following the instructions in the *Upgrading an SDC Site* section.
5. Repeat steps 3-4 until all local SDC sites are upgraded.



6. Perform the following steps on the EMS servers:



Note: This step is only necessary when upgrading from SDC 4.0.2 or 4.0.5. When upgrading from an earlier build of SDC 4.4, this step is not necessary.



Warning: Verify that all preceding steps have been successfully completed, and all EMS and SDC sites have been upgraded, before performing this step.

- a. Run the following command:

```
vi /opt/traffix/sdc/config/sysconfig/traffix_config_mgr
```

- b. Locate and delete the following two text blocks:

```
CONFIG_MGR_REMOTE_NETWORK_URI="static:(failover:(tcp://  
<SDCSite1Server1_Management_IP>:61617?wireFormat.maxInacti  
vityDuration=30000&keepAlive=true,tcp://
```

```
://<SDCSite1Server2_Management_IP>:61617?wireFormat.maxInacti  
vityDuration=30000&keepAlive=true)?randomize=false&maxReconne  
ct
```

```
Attempts=0,failover:(tcp://
```

```
://<SDCSite2Server1_Management_IP>:61617?wireFormat.maxInacti  
vityDuration=30000&keepAlive=true,tcp://
```

```
://<SDCSite2Server2_Management_IP>:61617?wireFormat.maxInacti  
vityDuration=30000&keepAlive=true)?randomize=false&maxReconne  
ctAttempts=0)"
```

and

```
USE_MIXED_MODE=true
```

- c. Restart the Config Manager resource.

3.2 Upgrading an EMS Site

This section includes the following topics:



- *Prerequisites*
- *Performing the ISSU on an EMS Site*



Note: This section describes the ISSU procedure necessary to upgrade an individual EMS site. This procedure is performed as part of the ISSU of a deployment with multiple SDC sites managed by an EMS site. Therefore, make sure that you have read and understood the procedure described in the *Upgrading Multiple SDC Sites Managed by an EMS Site* section before proceeding with this section.

3.2.1 Prerequisites

The following prerequisites must be completed before beginning the upgrade procedure:

- *Plan the Two Server Groups*
- *Define Which Server Group will be Upgraded First*
- *Plan the Upgrade*
- *Upgrade the F5 Traffic Menu*
- *Upgrade the Installer*
- *Copy the New Build Package*
- *Verify the Current Site Status*
- *Back Up Site Data*
- *Validate System Resources*
- *Verify Both Sets of Ports are Available*
- *Verify OS Upgrade Viability*
- *Validate the System RPMs*
- *Delete Existing Snapshots*
- *Update the EMS Site Configuration File*



3.2.1.1 Plan the Two Server Groups



Note: When a site only has two servers, each server is a “server group”. Refer to the first server that is upgraded as the “first server group” or “server group 1”, and the second server that is upgraded as the “second server group” or “server group 2”.

As previously described, the In-Service Software Upgrade (ISSU) is a granular process, upgrading the site in three phases. In the first phase, one group of servers is disconnected and upgraded, while the remaining servers continue to process traffic. In the following phases the upgraded servers are connected to the site to process traffic, as the remaining servers are disconnected and upgraded.

The two groups of servers are referred to in the guide as server groups. Before beginning the upgrade process, check the servers in your site and divide them into two server groups.



Note: Each server group should include half (“ $n/2$ ”) of the site servers (“ n ”). If you have an odd number of servers, one server group will include one more server.

3.2.1.2 Define Which Server Group will be Upgraded First

To optimize the ISSU process, it is recommended to first upgrade the server group that is not actively running the Splunk Master component, and that does not include the installer server.

3.2.1.3 Plan the Upgrade

During each phase of the ISSU, only one of the site’s servers is going to be connected to the site. To minimize the impact felt during the upgrade – that takes approximately two hours in total – perform the upgrade during off-peak hours.

3.2.1.4 Upgrade the F5 Traffix Menu

Before performing the upgrade, verify that the F5 Traffix Menu version installed on the site servers is the version included in the upgrade package.



To upgrade the F5 Traffix service menu, perform the following steps:

1. Run the following command on each site server:

`rpm -Uvh <full path to the menu RPM file.rpm>`

3.2.1.5 Upgrade the Installer

Before performing the upgrade, verify that the Installer version installed on the site is the version included in the upgrade package.

To upgrade the Installer, perform the following steps:

1. Access the F5 Traffix menu by typing **menu**.

Figure 8: F5 Traffix Service Menu

```
| F5 Traffix service menu 1.1.0 |
-----
1) Return to shell          4) Corosync Management    7) Generate Reports
2) Network Management      5) Installer Management
3) Snapshot Management     6) System Management
Select your choice:
```

2. Select **5) Installer Management**.
3. In the next menu screen, the Installer Management, select **3) Upgrade Installer via tar.gz**.
4. Enter the **tar.gz full path** of the new Installer and click **ENTER**.

For example:

`/root/sdc-installer-4.1-87.tar.gz`

The following message appears:



Figure 9: Installer Replacement Message

```
Installer replacement is over, it is recommended to select
4) "Print Installer version" option from the menu to verify current version.
Select your choice: 4
Version: 4.1
Build: 87
```

5. In the **Select your choice** prompt, enter **4** for the Print installer version option.

The Installer upgrade is confirmed with the relevant version and build information.

3.2.1.6 Copy the New Build Package

The new build package must be copied to the Installer server.



Note: The duration of this step varies as a result of a number of factors, including server location and speed.

To copy the new build package:

1. On the Installer server, go to
`/var/lib/tomcat/webapps/new_versions/`.
2. Verify that the folder is empty.
3. Copy the new upgrade `.tar.gz` file to this folder.

3.2.1.7 Verify the Current Site Status

Before performing the upgrade, verify that there are no pre-existing performance issues on any of the servers in the site.

To verify the current site status, perform the following tests:

1. On each server in the site, run the following command, and verify that each server is successfully running the SDC components as defined in the site configuration file.

crm_mon -n



2. Using the Web UI, verify that there are no SNMP alerts raised regarding system performance and connectivity.
3. Using the Web UI, check the statistics graphs to ensure that traffic is being processed as expected.

3.2.1.8 Back Up Site Data

Before performing the upgrade, create a snapshot of the site data.

To create a snapshot of the site data:

1. Using the Web UI, go to **Administration > Backup & Restore**.
2. Click **Backup**.

A snapshot of the site data is created, and can be applied using the Audit option in the Web UI.

3.2.1.9 Validate System Resources

Before performing the upgrade, verify the following items regarding system resources:

1. Verify all system components and log files. Back up the log files if needed.
2. Verify that there are no SDC components running on the site servers that are marked as migrated, and that no SDC component is configured to run only on one of the site servers.

To verify that the SDC components are running correctly, perform the following steps on each server:

- a. Access the F5 Traffic service menu by typing **menu**.
- b. Select **7) Generate Reports**.
- c. Select **2) Generate TTA Report**.
- d. Select **2) Normal Mode**.

The `tta-ng*.tar.gz` file is generated in the `/tmp` folder.

- e. Exit the menu and run the following commands to locate and open the `tta-ng*.tar.gz` file:



Note: When running the commands, replace `<tta-ng*>` with the specific file/folder name.

```
cd /tmp
```

```
tar xzvf <tta-ng*>.tar.gz
```

```
cd <tta-ng*>
```

- f. Locate and open the `cluster_errors.txt` file.
 - g. If any errors appear in the `cluster_errors.txt` file, contact *F5 Support* before beginning the ISSU.
3. Verify that at least 10% of the disk space, and a minimum of 4GB, in the partitions is free.
 4. Verify that at least 24GB (20GB for Splunk services and 4GB for the remaining site services) is free, by running the following command on each site server:

```
vgdisplay
```

The Free PE / Size value shows the amount of free disk space.

3.2.1.10 Verify Both Sets of Ports are Available

During installation, 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.

During the ISSU, each server group will be running a different version of the SDC software. To ensure that each group of servers continues to function as expected during the ISSU, a second set of ports must be enabled. This second set of network ports will be used by the upgraded servers. At the end of the upgrade, all the servers will be using the second set of ports. At this point, the ports that the servers were using prior to the upgrade will not be in use. If, in the future, the site will be upgraded again, the first set of ports will act as the second set of ports, and will be used for the upgraded servers.

Both sets of ports will only be used simultaneously during the ISSU.



Table 2 details the ports that may need to be enabled. Of this list, the necessary ports can differ per deployment. For a list of the specific ports, contact *F5 Support*.



Note: The `<Instance_UID>` value in the table below should be retrieved from the `/opt/traffix/sdc/config/sysconfig/traffix_+instancename` file.

Table 2: Port Configuration

Port Type	First Set of Ports	Second Set of Ports
JMX	D_JMX_PORT_1=1400 + <Instance_UID>	D_JMX_PORT_1=1500 + <Instance_UID>
Communication	D_INTER_COMMUNICATION_P ORT_1=4545 + <Instance_UID>	D_INTER_COMMUNICATION_PORT _2=5545 + <Instance_UID>
Corosync	<Corosync Port Number>	<Corosync Port Number> + 2

3.2.1.11 Verify OS Upgrade Viability

Before performing the upgrade, verify that the Operating System currently installed on the site servers can be upgraded.

To verify that the installed OS can be upgraded, perform the following steps on each site server:

1. Access the F5 Traffix service menu by typing **menu**.
2. Select **6) System Management**.
3. Select **3) Try to Upgrade OS**.
4. Select **2) Normal Mode**.
5. Enter the full path to the upgrade `.tar.gz` file.

If the returned value contains errors, contact *F5 Support* before beginning the ISSU.



3.2.1.12 Validate the System RPMs

The SDC software is installed on each site server with a specific set of RPMs. When upgrading the Operating System during the ISSU, RPMs that are relevant for the target SDC version are also upgraded. Existing RPMs on the site server that are not relevant for the target SDC version are not upgraded, and may not function as expected after the upgrade. To avoid this potential impact, the SDC can scan the RPMs installed on the site servers and identify RPMs that are not part of the currently installed SDC version's required RPMs. It is recommended to use the SDC to identify these RPMs, and to then manually delete these RPMs from **each site server** before performing the ISSU.



Note: In the event that the target version of the SDC requires additional RPMs, these RPMs are automatically added during the upgrade.

To identify the RPMs that must be deleted, upgrade the F5 Traffix service menu and generate a TTA Report. This report contains a .txt file with the list of RPMs that must be manually deleted before the ISSU, as well as a list of the RPMs that will be added automatically during the ISSU.

To verify the RPM files that are installed in your system, perform the following steps on each site server:



Note: The following procedure must be performed on all servers in the site.



Note: If you generated a TTA Report when validating system resources, skip to step 5.

1. Access the F5 Traffix service menu by typing **menu**.
2. Select **7) Generate Reports**.
3. Select **2) Generate TTA Report**.
4. Select **2) Normal Mode**.

The `tta-ng*.tar.gz` file is generated in the `/tmp` folder.



- h. Exit the menu and run the following commands to locate and open the `tta-ng*.tar.gz` file:

Note: When running the commands, replace `<tta-ng*>` with the specific file/folder name.


```
cd /tmp
```

```
tar xzvf <tta-ng*>.tar.gz
```

5. Run the following command:

```
cat /tmp/<tta-ng*>/os/OSReq/OSReq_rpm_check_report.txt
```

6. Manually delete the RPMs in the “RPM need to be deleted” list.

 Warning: RPMs in the list that are not manually deleted may not function as expected after upgrade.

3.2.1.13 Delete Existing Snapshots

The ISSU includes a rollback option. During the upgrade process, snapshots are created of the servers in their pre-upgrade state. If, for any reason, the upgrade cannot be completed, these snapshots are used to revert servers back to their pre-upgrade state.

To ensure successful rollbacks, verify that there are no pre-existing F5 snapshots (F5_Snapshot) on the site servers.

To verify that there are no pre-existing snapshots on the site servers:

1. Run the following command on each server in the site:

```
lvscan
```

Any existing snapshots existing on the server will appear.

2. Delete existing F5 snapshots by running the following command on each server with snapshots:

```
lvremove <snapshot_name>
```



Note: This command only deletes the specific snapshot. To delete all available snapshots, enter the common pathname for all snapshots as the `F5_Snapshot_name` appended with an `*`. All F5 snapshots in that location will be deleted.

3.2.1.14 Update the EMS Site Configuration File

The EMS site configuration file that the EMS site was installed with must be updated to reflect the changes included in the upgrade. Since this upgrade is going to install a different version of SDC software, the site configuration file must be updated accordingly.

To update the SDC site configuration file with the new SDC software information:

1. In the Installation Utility home page, click **Edit Existing Configuration**.
The **Select Configuration** screen appears.
2. Select the updated site configuration file by choosing the one of the following options:
 - a. **Load the site configuration file from the installation Server** by performing the following steps:



Note: Choose this option if the file you want to work is already uploaded to the Installer server.

- i. Select the updated file from the drop-down list.
- b. **Upload Site Configuration File** to the installation server.



Note: Choose this option if the file you want to work with is located locally (for example, on a USB or on the desktop) and has not yet been uploaded to the installation server.

- i. Click **Browse** and navigate to the desired file.
 - ii. Click **Open**.



Note: The selected configuration file is now on the installation server, and will appear in the drop-down list of available configuration files.

3. Click **Next**. The **Define Servers** screen appears.
 4. Update the OS definition for each server in the table by selecting the relevant “rhel66” OS option from the drop-down list.
 5. Add the “installer” role to the server that the installation utility is running on.
 6. Add the “installer” role to one other site server.
-



Note: From release 4.4, the installation utility must run on a site server. In addition, from release 4.4 each site must contain two servers that are defined as installer servers.

7. Click **Next** until the **Configure Properties** screen appears.
8. Verify and update (if needed) the following site properties:
 - a. In the System section:
 - **SDCVersion** – enter the file name of the SDC software version and build you are updating the site with. For example, 4.4.2-4.
 - **Installerip** – enter the IP address of the Installer server that the EMS connects to.
 - b. In the config_mgr section:
 - **CM_MGT_VIP** – enter the VIP address of the EMS Configuration Manager.
 - **CM_IC_VIP** – enter an IP address in the EMS site interconnect network.
 - **EMS_MGT_VIP** – enter the VIP address of the EMS Configuration Manager.
 - c. In the installer section:



- **Network** – enter the network IP address that is used for communication between the installation server and the site servers.
- **startDHCP** – enter the lower end of the range of IP addresses that can be installed using PXE.
- **endDHCP** – enter the upper end of the range of IP addresses that can be installed using PXE.

9. Click **Save**.

3.2.2 Performing the ISSU on an EMS Site

The following section describes the three phases of the ISSU.

3.2.2.1 Performing Phase 1: Upgrading the First Server Group

In this phase, one server group is selected, disconnected from the site, and upgraded, while the second server group continues to process traffic.



Note: First upgrade the server group that is not actively running the Splunk Master component or the installation utility.



Note: During this phase, the second server group processes traffic without a local high availability option.

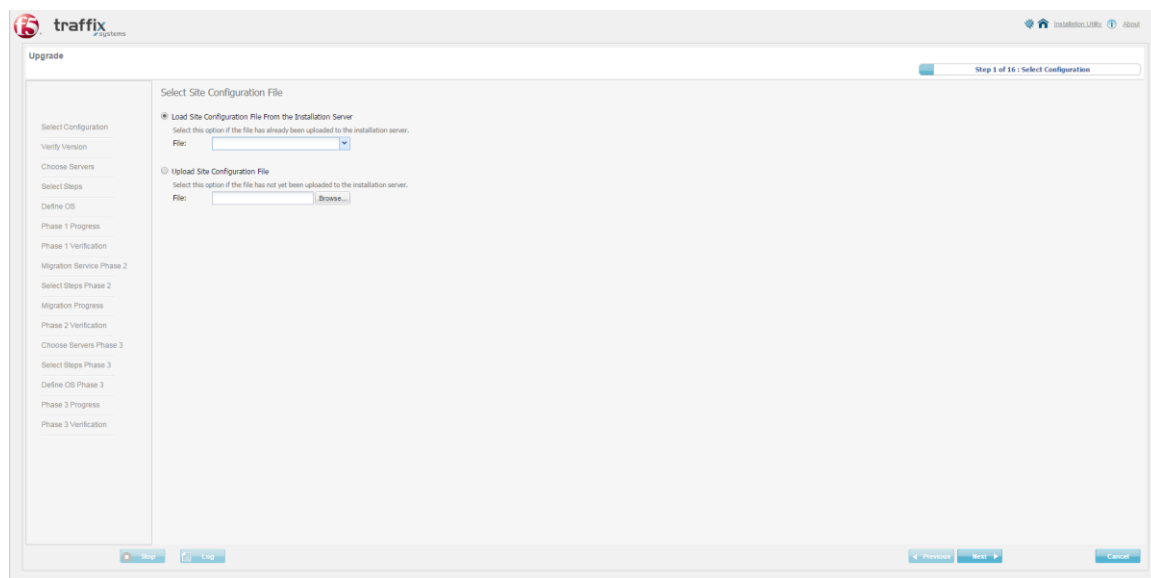
To perform phase 1:

1. In the Installation Utility home page, click **Upgrade**.

The **Select Configuration** screen appears.



Figure 10: Select Configuration Screen



2. Select the updated site configuration file by choosing the one of the following options:
 - a. **Load the site configuration file from the installation Server** by performing the following steps:



Note: Choose this option if the file you want to work is already uploaded to the Installer server.

- i. Select the updated file from the drop-down list.



Warning: Even though the site configuration file may appear in the list of Installer server configuration files, remember that you have just updated this file (based on the instructions in the *Update the EMS Site Configuration File* section). Verify that the updated version of the configuration file is defined in this step.

- b. **Upload Site Configuration File** to the installation server.



Note: Choose this option if the file you want to work with is located locally (for example, on a USB or on the desktop) and has not yet been uploaded to the installation server.

- i. Click **Browse** and navigate to the desired file.
- ii. Click **Open**.

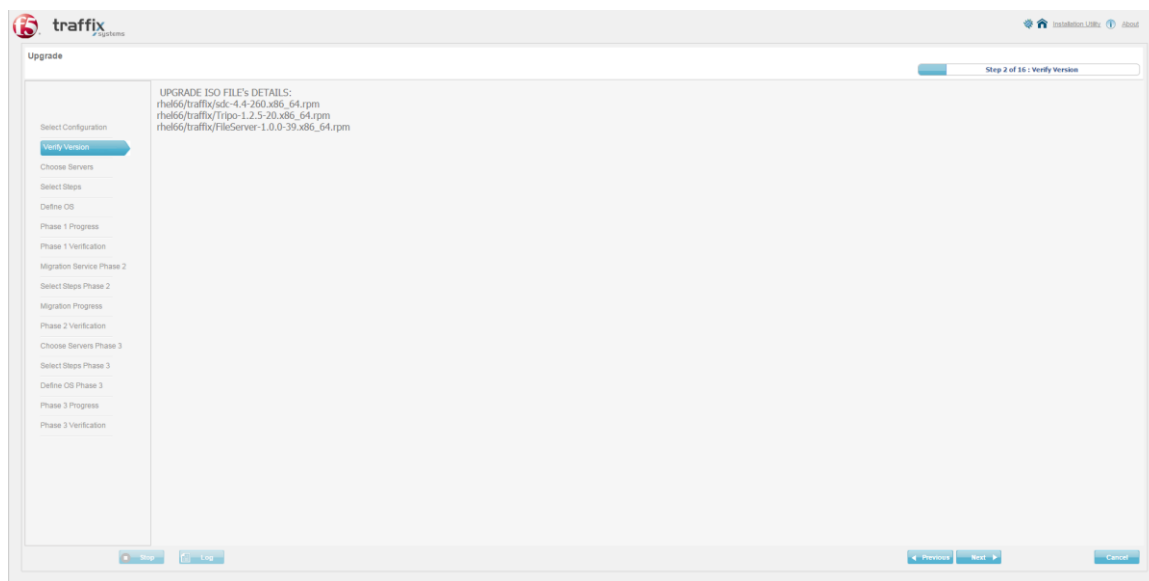


Note: The selected configuration file is now on the installation server, and will appear in the drop-down list of available configuration files.

3. Click **Next**.

The **Verify Version** screen appears.

Figure 11: Verify Version Screen



4. The Verify Version screen displays the release and build information of the target SDC version for the upgrade. Verify that these details are correct.

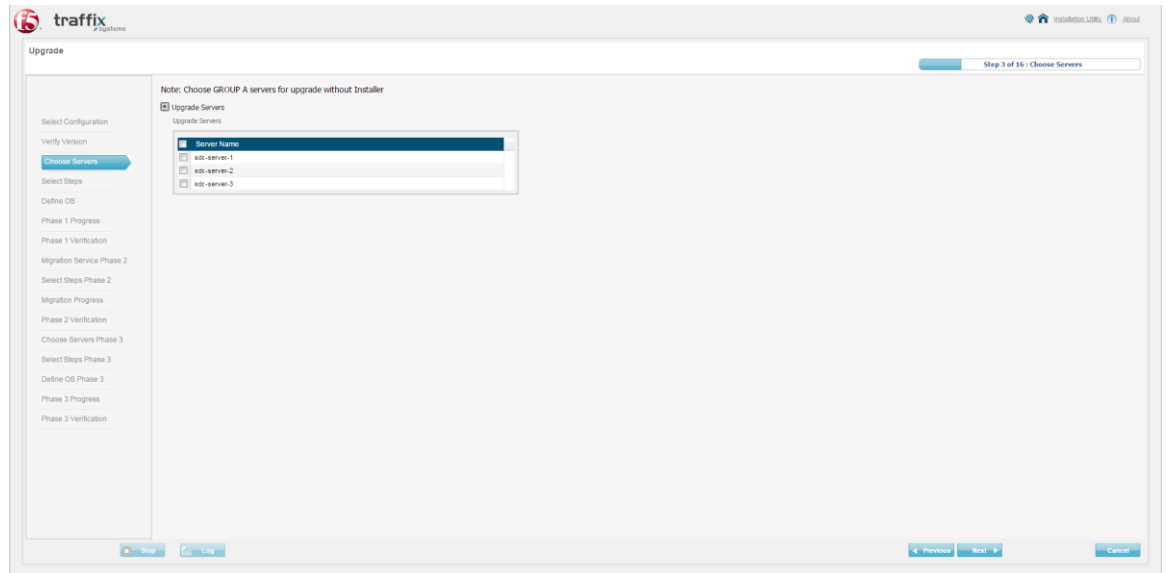
If the details are incorrect, verify that the prerequisites were completed correctly and the site configuration file was correctly updated, saved and uploaded. For more information, see the *Update the EMS Site Configuration File* section.



5. Click **Next**.

The **Choose Servers** screen appears.

Figure 12: Choose Servers Screen



6. Select the servers that are to be included in the first server group and click **Next**.

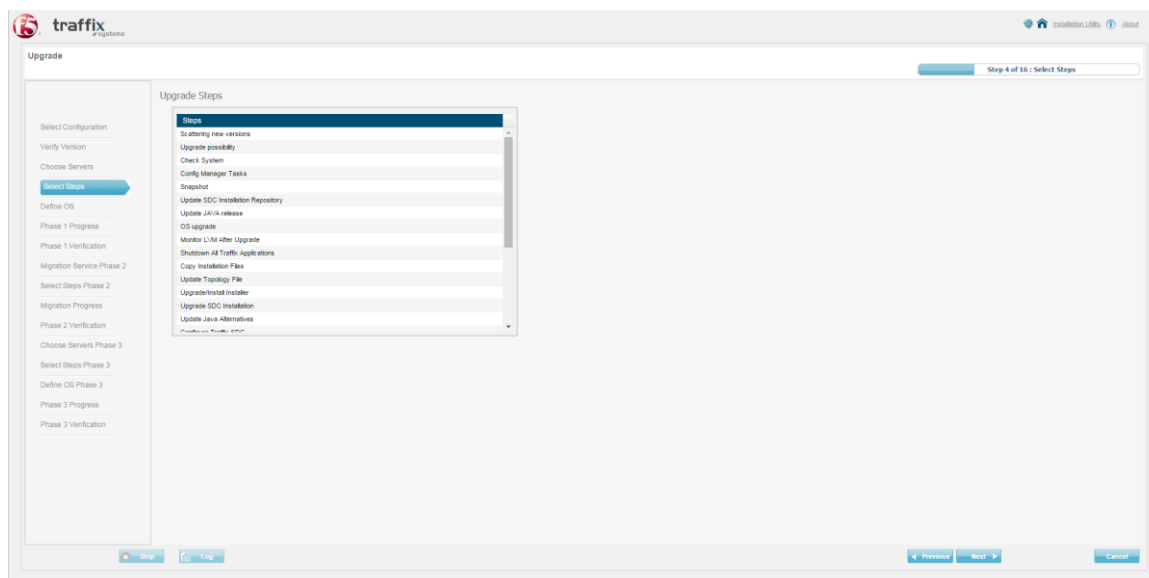


Note: This server group should **not** include the server that the installation utility is actively running on.

The **Select Steps** screen appears.



Figure 13: Select Steps Screen



Phase 1 of the ISSU procedure includes the following steps:

Table 3: Phase 1 Upgrade Steps

Step	Description
Scattering new versions	Copy files from the upgrade ISO file to the relevant repositories.
Upgrade possibility	Verify that each of the two server groups have the SDC components necessary to independently process site traffic.
Check System	Verify disk space, interfaces, etc.
Config Manager Task	Shuts down the Config Manager
Snapshot	Create a snapshot of the servers in the first server group, as they appear at the beginning of phase 1.
Update SDC Installation Repository	Update the SDC Installation Repository.
Update Java release	Upgrade Java version (if required).
OS Upgrade	Upgrade OS (if required).
Monitor LVM After Upgrade	Check the validity of the created snapshot.



Step	Description
Shutdown All Traffix Applications	Shut down all Traffix application.
Copy Installation Files	Copy the new installation files to the servers in the first server group.
Update Topology File	Copy the updated site configuration file to the servers in the first server group.
Upgrade/Install Installer	Upgrades the version of the installation utility installed on the secondary installer server.
Upgrade SDC Installation	Upgrade the SDC installation.
Update Java Alternatives	Updates Java links.
Configure Traffix SDC	Configure Traffix SDC.
Configure SDC Cluster	Configure the SDC cluster according to the site configuration file.
Upgrade NMSAgent	Upgrade the NMS Agent component (if different than current version)
Upgrade SS7	Upgrade the SS7 component (if different than current version)
Upgrade Splunk	Upgrade the Splunk component (if different than current version)
Migrate SDC Configuration	Migrate the SDC configuration onto the servers in the first server group.
Upgrade Tripo	Upgrade the Tripo component (if different than current version)
Upgrade FileServer	Upgrade the Fileserver component (if different than current version)
Split the system	Change the configured listener ports of all SDC components in order to sever communication between the server groups for the duration of the upgrade.
Configure Corosync Cluster	Change the configured Corosync ports to allow two clusters in the system.

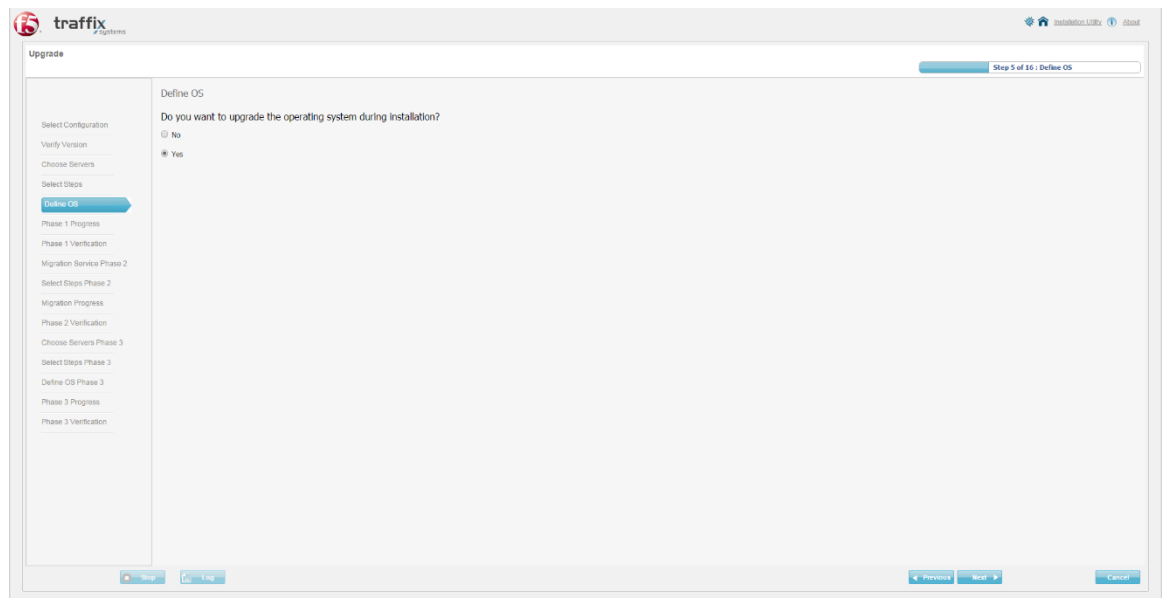


Step	Description
Reboot	Reboots the servers.

7. Click **Next**.

The **Define OS** screen appears.

Figure 14: Define OS Screen

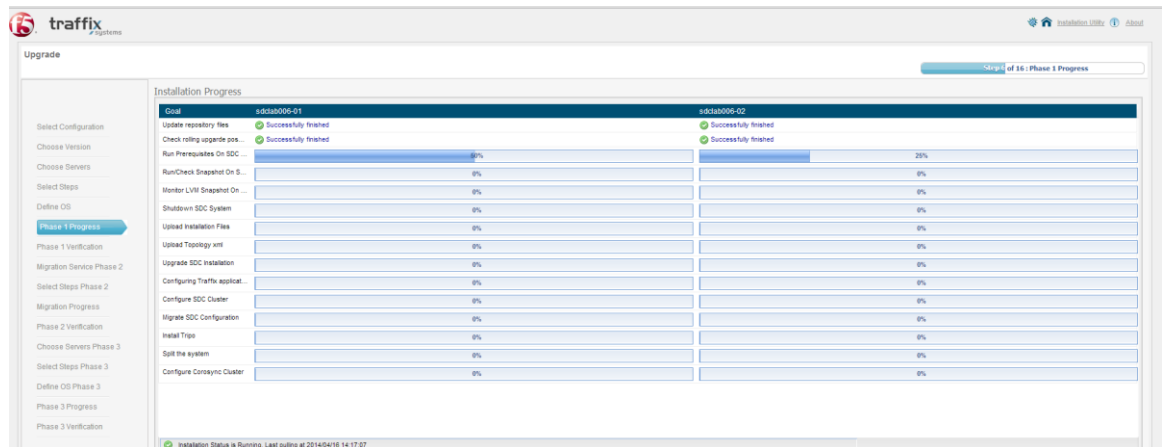


8. Select **Yes** in response to the question: **Do you want to upgrade the operating system during the upgrade.**
9. Click **Next** to start the phase 1 upgrade process.

The **Phase 1 Progress** screen appears.



Figure 15: Phase 1 Progress Screen



The **Phase 1 Progress** screen displays the upgrade progression for each upgrade step for each server. This way, if the upgrade fails on specific steps for a specific server, you can effectively troubleshoot the cause of the failure.



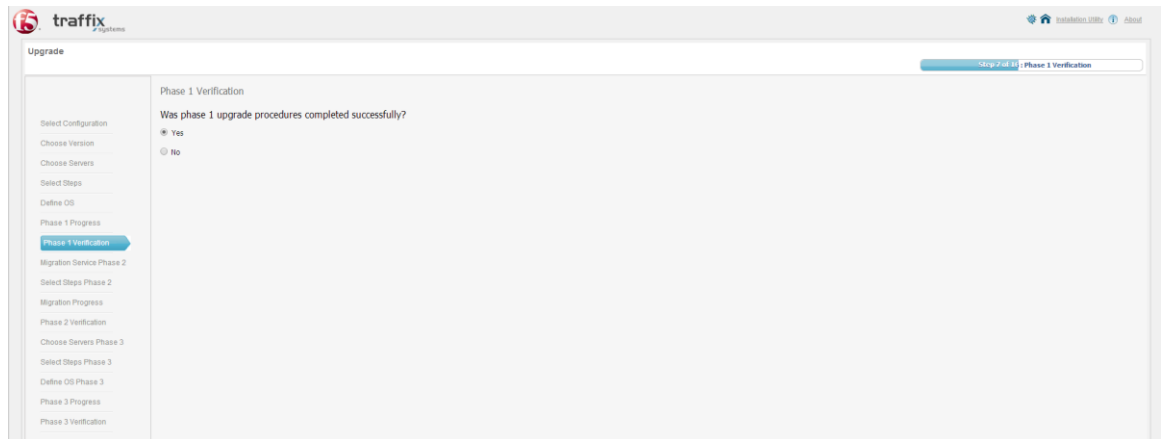
Note: If you encounter browser issues during the phase 1 upgrade process, this phase must be rolled back before retrying.

10. The following message is displayed: **“Upgrade has been successfully finished.”** Click **OK**.
11. Run the following command on each server in the group to switch the servers to online mode.
crm node online
12. Click **Next**.

The **Phase 1 Verification** screen appears.



Figure 16: Phase 1 Verification Screen



13. Run the following command on each server in the first server group to check that each server is successfully online. Each server is successfully online if the EMS clone components configured to run on the server are up.

crm_mon -n

14. If the servers in the first server group are up and running, select **Yes** in the **Phase 1 Verification** screen.


If the servers in the first server group are not up and running properly, select **No**. This means that this phase failed and the servers need to be reverted to their pre-phase 1 state. The following message appears: **Please perform manual rollback**. For information about the rollback, see *Performing an Upgrade Rollback*.

3.2.2.2 Performing Phase 2: Activating Server Group 1 as Primary Server Group

At this point, phase 1 is complete. The servers that were selected to be upgraded in phase 1 are successfully upgraded, but are still disconnected from the site. Site traffic is being processed by the second server group.

In phase 2, site traffic will be processed by the servers in the first server group that will be reconnected to the site, while the remaining servers will be disconnected from the site and will not process site traffic.



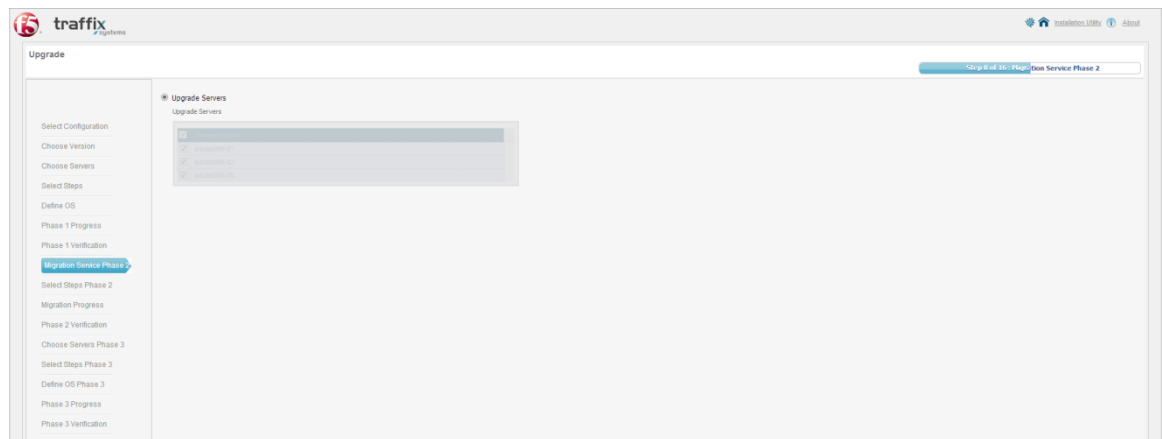
 Note: During this phase, the first server group processes traffic without a local high availability option.

To perform phase 2:

1. After selecting **Yes** in the Phase 1 Verification screen, click **Next**.

The **Migration Service Phase 2** screen appears.

Figure 17: Migration Service Phase 2 Screen



2. In the **Migration Service Phase 2** screen, the server selection option is grayed out.

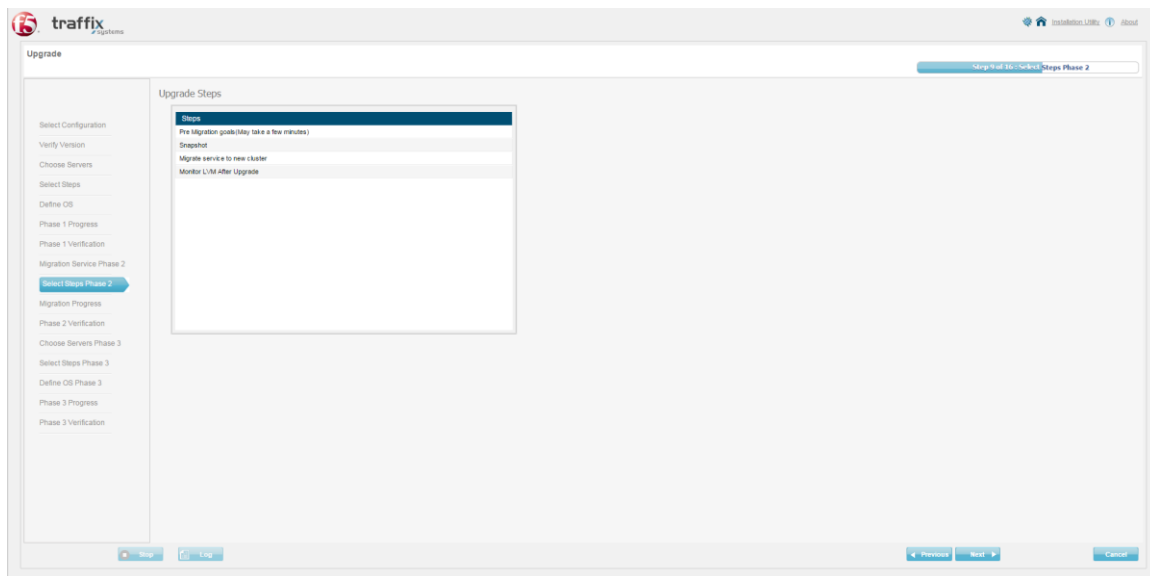
All servers are selected in this phase.

3. Click **Next**.

The **Select Steps Phase 2** screen appears.



Figure 18: Select Steps Phase 2 Screen



Phase 2 of the ISSU procedure includes the following steps:

Table 4: Phase 2 Upgrade Steps

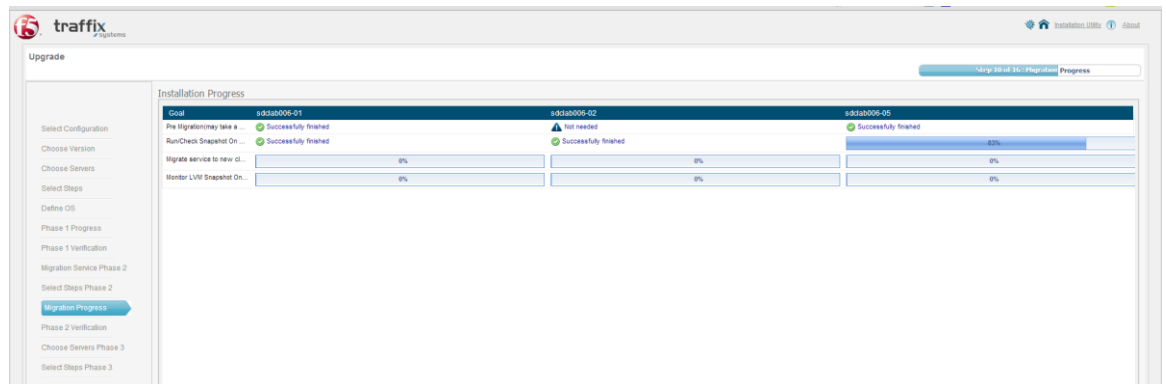
Step	Description
Pre Migration goals (Make take a few minutes)	Perform the prerequisites steps necessary before service migration (for example, syncing Tripo entries).
Snapshot	Create a snapshot of the second server group.
Migrate service to new cluster	Switch site traffic to be processed by servers in the first server group.
Monitor LVM After Upgrade	Verify the validity of the created snapshots.

4. Click **Next** to start the phase 2 upgrade process.

The **Migration Progress** screen appears.



Figure 19: Migration Progress Screen



The **Migration Progress** screen displays the upgrade progression for each upgrade step for each server. This way, if the migration fails on specific steps for a specific server, you can effectively troubleshoot the cause of the failure.



Note: If you encounter browser issues during the phase 2 migration process, this phase must be rolled back before retrying.



Note: The first goal, **Pre Migration goals** that is displayed is not relevant for EMS sites and will result in a “Not Needed” status.

5. The following message is displayed: “**Upgrade has been successfully finished.**” Click **OK**.
6. Click **Next**.

The **Phase 2 Verification** screen appears.



Figure 20: Phase 2 Verification Screen

The screenshot shows the 'Upgrade' utility window. On the left is a sidebar with a list of steps: Select Configuration, Verify Version, Choose Servers, Select Steps, Define OS, Phase 1 Progress, Phase 1 Verification, Migration Service Phase 2, Select Steps Phase 2, Migration Progress, **Phase 2 Verification** (highlighted with a blue arrow), Choose Servers Phase 3, Select Steps Phase 3, Define OS Phase 3, Phase 3 Progress, and Phase 3 Verification. The main panel is titled 'Phase 2 Verification' and contains the question 'Was phase 2 upgrade procedures completed successfully?'. Below this are two radio buttons: 'Yes' (which is selected) and 'No'. At the bottom of the window are buttons for 'Step', 'Log', 'Previous', 'Next', and 'Cancel'. A status bar at the top right indicates 'Step 11 of 16 - Phase 2 Verification'.

7. After all upgrade steps are successfully completed for each server in the first server group, perform the following steps:
 - a. Run the following command on each server in the site, and check the servers as follows:
crm_mon -n
 - i. Check that servers in the first server group are all online and running all the EMS components configured on them.
 - ii. Check that servers in the second server group are all online and running only the EMS “ClusterMon” clone component configured on them.
8. If the servers in the first server group are up and running, select **Yes** in the **Phase 2 Verification** screen, and click **Next**.

If the servers in the second server group are not up and running properly, select **No**. This means that this phase failed and the servers need to be reverted to their pre-phase 2 state. The following message appears: **Please perform manual rollback**. For information about the rollback, see *Performing an Upgrade Rollback*.



3.2.2.3 Performing Phase 3: Upgrading Server Group 2

At this point, phase 2 is successfully finished. Traffic is being processed by the upgraded servers in the first server group. The servers in the second server group are online, but are disconnected from the site and are not processing site traffic.

In this phase, the second server group is selected, shut down, and upgraded, while the first server group processes traffic.



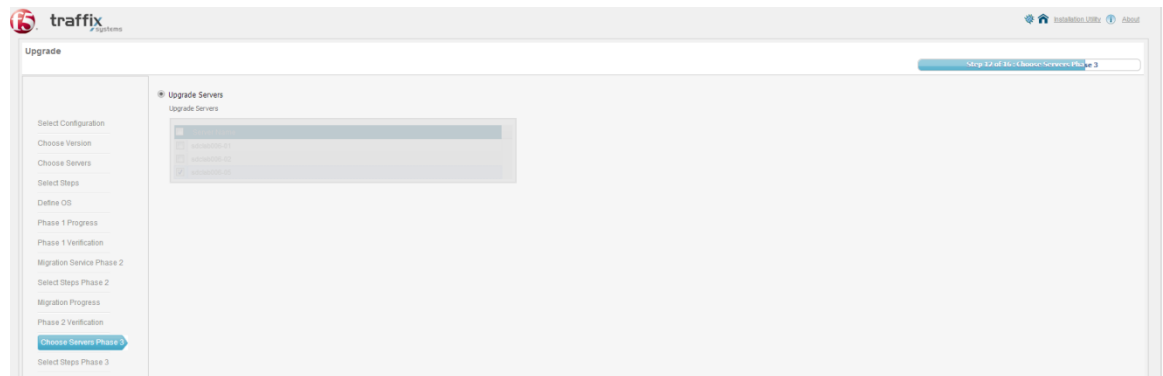
Note: During this phase, the first server group continues to process traffic without a local high availability option.

To perform phase 3:

1. After selecting **Yes** in the Phase 2 Verification screen, click **Next**.

The **Choose Servers Phase 3** screen appears.

Figure 21: Choose Servers Phase 3 Screen

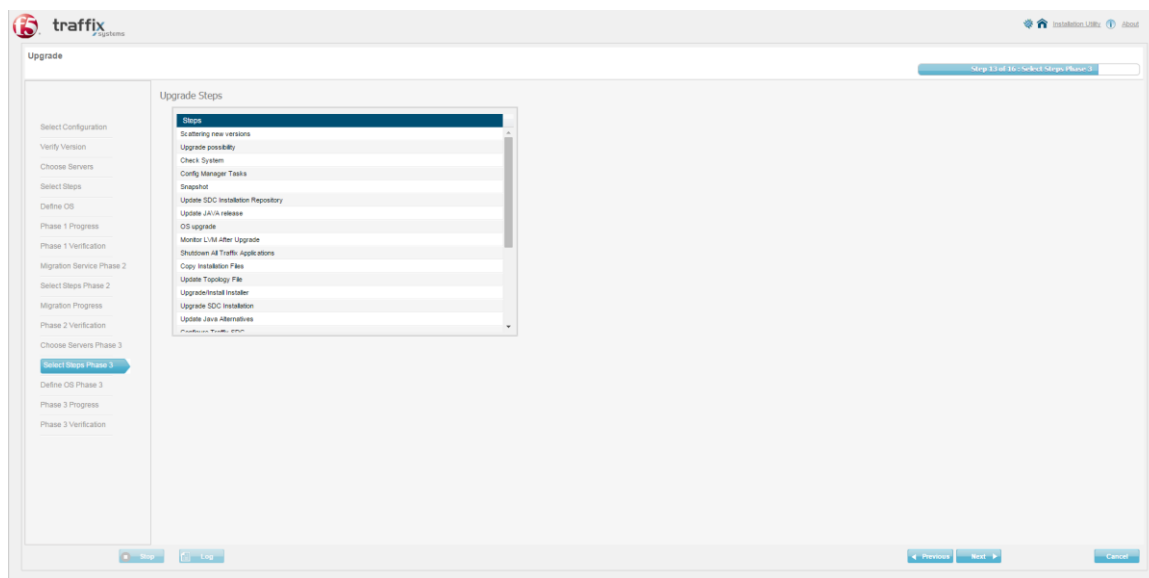


2. In the **Choose Servers Phase 3** screen, select the servers in the second server group and click **Next**.

The **Select Steps Phase 3** screen appears.



Figure 22: Select Steps Phase 3 Screen



Phase 3 of the ISSU procedure includes the following steps:

Table 5: Phase 3 Upgrade Steps

Step	Description
Scattering new versions	Copy files from the upgrade ISO file to the relevant repositories.
Upgrade possibility	Verify that each of the two server groups have the SDC components necessary to independently process site traffic.
Check System	Verify disk space, interfaces, etc.
Config Manager Task	Shuts down the Config Manager
Snapshot	Create a snapshot of the servers in the first server group, as they appear at the beginning of phase 1.
Update SDC Installation Repository	Update the SDC Installation Repository.
Update Java release	Upgrade Java version (if required).
OS Upgrade	Upgrade OS (if required).



Step	Description
Monitor LVM After Upgrade	Check the validity of the created snapshot.
Shutdown All Traffix Applications	Shut down all Traffix application.
Copy Installation Files	Copy the new installation files to the servers in the first server group.
Update Topology File	Copy the updated site configuration file to the servers in the first server group.
Upgrade/Install Installer	Upgrades the version of the installation utility installed on the secondary installer server.
Upgrade SDC Installation	Upgrade the SDC installation.
Update Java Alternatives	Updates Java links.
Configure Traffix SDC	Configure Traffix SDC.
Configure SDC Cluster	Configure the SDC cluster according to the site configuration file.
Upgrade NMSAgent	Upgrade the NMS Agent component (if different than current version)
Upgrade SS7	Upgrade the SS7 component (if different than current version)
Upgrade Splunk	Upgrade the Splunk component (if different than current version)
Migrate SDC Configuration	Migrate the SDC configuration onto the servers in the first server group.
Upgrade Tripo	Upgrade the Tripo component (if different than current version)
Upgrade FileServer	Upgrade the Fileserver component (if different than current version)
Split the system	Change the configured listener ports of all SDC components in order to sever communication between the server groups for the duration of the upgrade.

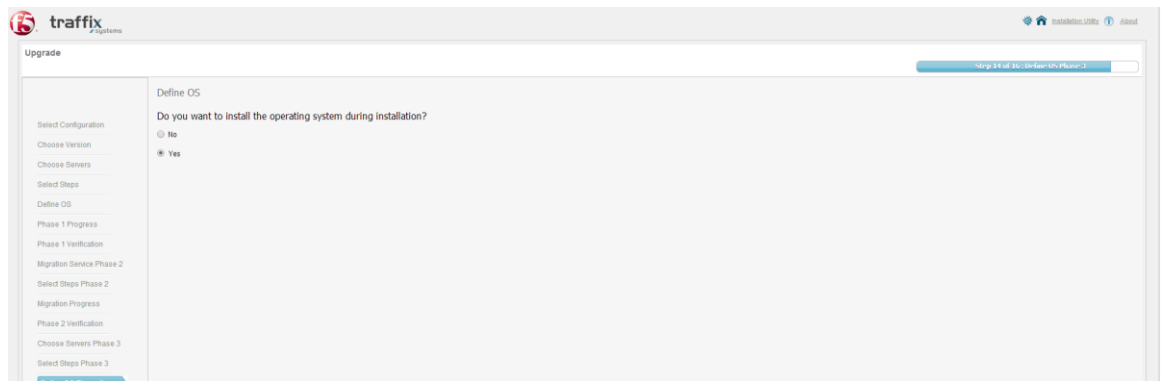


Step	Description
Configure Corosync Cluster	Change the configured Corosync ports to allow two clusters in the system.
Reboot	Reboots the servers.

3. Click **Next**.

The **Define OS Phase 3** screen appears.

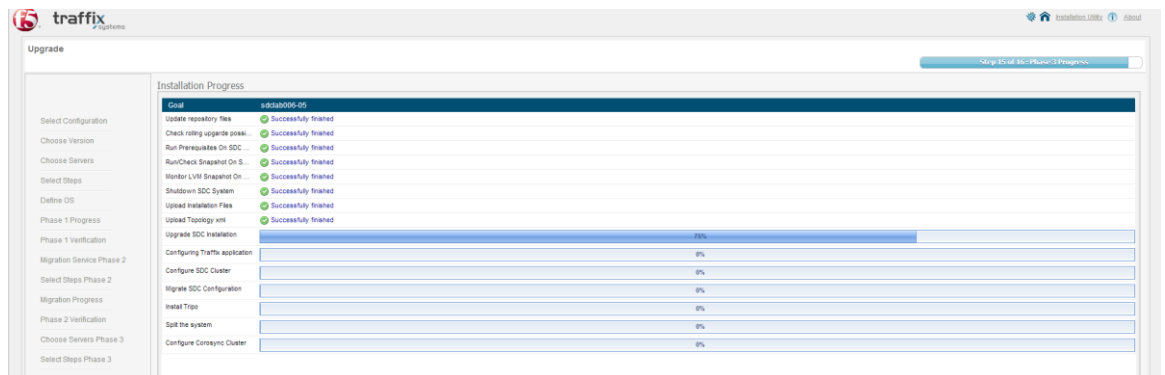
Figure 23: Define OS Phase 3 Screen



4. Select **Yes** in response to the question: **Do you want to upgrade the operating system during the upgrade.**
5. Click **Next** to start the phase 3 upgrade process.

The **Phase 3 Progress** screen appears.

Figure 24: Phase 3 Progress screen





The **Phase 3 Progress** screen displays the upgrade progression for each upgrade step for each server. This way, if the upgrade fails on specific steps for a specific server, you can effectively troubleshoot the cause of the failure.



Note: If you encounter browser issues during the phase 3 upgrade process, this phase must be rolled back before retrying.

6. The following message is displayed: “**Upgrade has been successfully finished.**” Click **OK**.
7. In the **Phase 3 Verification** screen, select **Next > Yes > Finish**.
8. Reboot the server(s) in the group that the installer is installed on.
9. Run the following command on each server in that group to switch the servers to online mode:

crm node online

10. Run the following command on each server in the second server group and verify that each server has the SDC components configured for it in the site configuration file, and that all SDC clone components are running:

crm_mon -n

If the servers are not up and running properly, this means that this phase failed and the servers need to be reverted to their pre-phase 3 state. For information about the rollback, see *Performing an Upgrade Rollback*.

If the server are up and running properly, this means that phase 3 is complete, and the site has been successfully upgraded. Traffic is processed by all servers in the site.

To continue with the ISSU of a deployment with multiple SDC sites managed by an EMS site, return to the *Upgrading Multiple SDC Sites Managed by an EMS Site* section.



3.3 Upgrading an SDC Site

This section includes the following topics:

- *Prerequisites*
- *Performing the ISSU on an SDC Site*



Note: This section describes the ISSU procedure necessary to upgrade an individual SDC site. If you are upgrading an SDC site that is managed by an EMS site, make sure to follow the procedure described in the *Upgrading Multiple SDC Sites Managed by an EMS Site* section.

3.3.1 Prerequisites

The following prerequisites must be completed before beginning the upgrade procedure:

- *Plan the Two Server Groups*
- *Define Which Server Group will be Upgraded First*
- *Plan the Upgrade When Traffic is Reduced*
- *Upgrade the F5 Traffic Menu*
- *Upgrade the Installer*
- *Copy the New Build Package*
- *Verify the Current Site Status*
- *Validate System Resources*
- *Verify Both Sets of Ports are Available*
- *Verify OS Upgrade Viability*
- *Validate the System RPMs*
- *Delete Existing Snapshots*
- *Update the SDC Site Configuration File*



3.3.1.1 Plan the Two Server Groups



Note: When a site only has two servers, each server is a “server group”. Refer to the first server that is upgraded as the “first server group” or “server group 1”, and the second server that is upgraded as the “second server group” or “server group 2”.

As previously described, the In-Service Software Upgrade (ISSU) is a granular process, upgrading the site in three phases. In the first phase, one group of servers is disconnected and upgraded, while the remaining servers continue to process traffic. In the following phases the upgraded servers are connected to the site to process traffic, as the remaining servers are disconnected and upgraded.

The two groups of servers are referred to in the guide as server groups. Before beginning the upgrade process, check the servers in your site and divide them into two server groups.



Note: Each server group should include half (“ $n/2$ ”) of the site servers (“ n ”). If you have an odd number of servers, one server group will include one more server.

3.3.1.2 Define Which Server Group will be Upgraded First

To optimize the ISSU process, it is recommended to first upgrade the server group that is running the least amount of active FEP resources, and that does not include the installer server.

3.3.1.3 Plan the Upgrade When Traffic is Reduced

During each phase of the ISSU, only one of the site’s servers is going to be connected to the site and processing traffic. This impacts the site’s traffic processing capacity and reduces it to about 30% of the usual maximum load. To minimize the impact felt during the upgrade – that takes approximately two hours in total – perform the upgrade during off-peak hours, or reduce the traffic forwarded to the site to 30% of its usual maximum load for the duration of the upgrade.



Note: When planning the upgrade, remember that each site upgrade takes approximately two hours.

3.3.1.4 Upgrade the F5 Traffic Menu

Before performing the upgrade, verify that the F5 Traffic Menu version installed on the site servers is the version included in the upgrade package.

To upgrade the F5 Traffic service menu, perform the following steps:

11. Run the following command on each site server:

```
rpm -Uvh <full path to the menu RPM file.rpm>
```

3.3.1.5 Upgrade the Installer

Before performing the upgrade, verify that the Installer version installed on the site is the version included in the upgrade package.

To upgrade the Installer, perform the following steps:

12. Access the F5 Traffic menu by typing **menu**.

Figure 25: F5 Traffic Service Menu

```
| F5 Traffic service menu 1.1.0 |
-----
1) Return to shell      4) Corosync Management  7) Generate Reports
2) Network Management  5) Installer Management
3) Snapshot Management 6) System Management
Select your choice:
```

13. Select **5) Installer Management**.

14. In the next menu screen, the Installer Management, select **3) Upgrade Installer via tar.gz**.



15. Enter the **tar.gz full path** of the new Installer and click **ENTER**.

For example:

/root/sdc-installer-4.1-87.tar.gz

The following message appears:

Figure 26: Installer Replacement Message

```
Installer replacement is over, it is recommended to select
4) "Print Installer version" option from the menu to verify current version.
Select your choice: 4
Version: 4.1
Build: 87
```

16. In the **Select your choice** prompt, enter **4** for the Print installer version option.

The Installer upgrade is confirmed with the relevant version and build information.

3.3.1.6 Copy the New Build Package

The new build package must be copied to the Installer server.



Note: The duration of this step varies as a result of a number of factors, including server location and speed.

To copy the new build package:

17. On the Installer server, go to

/var/lib/tomcat/webapps/new_versions/.

18. Verify that the folder is empty.

19. Copy the new upgrade **.tar.gz** file to this folder.

3.3.1.7 Verify the Current Site Status

Before performing the upgrade, verify that there are no pre-existing performance issues on any of the servers in the site.



To verify the current site status, perform the following tests:

1. On each server in the site, run the following command, and verify that each server is successfully running the SDC components as defined in the site configuration file.

crm_mon -n

2. Using the Web UI, verify that there are no SNMP alerts raised regarding system performance and connectivity
3. Using the Web UI, check the statistics graphs to ensure that traffic is being processed as expected.

3.3.1.8 Validate System Resources

Before performing the upgrade, verify the following items regarding system resources:

1. Verify all system components and log files. Back up the log files if needed.
2. Verify that there are no SDC components running on the site servers that are marked as migrated, and that no SDC component is configured to run only on one of the site servers.
3. Verify that there are no SDC components running on the site servers that are marked as migrated, and that no SDC component is configured to run only on one of the site servers.

To verify that the SDC components are running correctly, perform the following steps on each server:

- a. Access the F5 Traffic service menu by typing **menu**.
- b. Select **7) Generate Reports**.
- c. Select **2) Generate TTA Report**.
- d. Select **2) Normal Mode**.

The `tta-ng*.tar.gz` file is generated in the `/tmp` folder.



- e. Exit the menu and run the following commands to locate and open the `tta-ng*.tar.gz` file:

Note: When running the commands, replace `<tta-ng*>` with the specific file/folder name.

```
cd /tmp
```

```
tar xzvf <tta-ng*>.tar.gz
```

```
cd <tta-ng*>
```

- f. Locate and open the `cluster_errors.txt` file.
 - g. If any errors appear in the `cluster_errors.txt` file, contact *F5 Support* before beginning the ISSU.
4. Verify that at least 10% of the partitions space, and a minimum of 4GB, in each partition is free.
 5. Verify that at least 20% of the disk space, or a minimum of 1GB, is free, by running the following command on each site server:

```
vgdisplay
```

The Free PE / Size value shows the amount of free disk space.

3.3.1.9 Verify Both Sets of Ports are Available

During installation, a set of ports was defined and configured to ensure communication both between the different SDC components within the deployment, and between the SDC components and the necessary network elements.

During the ISSU, each server group will be running a different version of the SDC software. To ensure that each group of servers continues to function as expected during the ISSU, a second set of ports must be defined and configured. This second set of network ports will be used by the upgraded servers. At the end of the upgrade, all the servers will be using the second set of ports. At this point, the ports that the servers were using prior to



the upgrade will not be in use. If, in the future, the site will be upgraded again, the first set of ports will act as the second set of ports, and will be used for the upgraded servers.

Both sets of ports will only be used simultaneously during the ISSU.

Table 6 details the ports that may need to be enabled. Of this list, the necessary ports can differ per deployment. For a list of the specific ports, contact *F5 Support*.



Note: The <Instance_UID> value in the table below should be retrieved from the /opt/traffix/sdc/config/sysconfig/traffix_+instancename file.

Table 6: Port Configuration

Port Type	First Set of Ports	Second Set of Ports
General	D_CPF_BIND_PORT_1=61637	D_CPF_BIND_PORT_2=62637
General	D_CPF_DIAMETER_PORT=13868	D_CPF_DIAMETER_PORT_UPGRADE D=23868
General	D_CPF_RADIUS_PORT=11812	D_CPF_RADIUS_PORT_UPGRADED= 21812
General	D_CPF_HTTP_PORT=18080	D_CPF_HTTP_PORT_UPGRADED=280 80
JMX	D_JMX_PORT_1=1400 + <Instance_UID>	D_JMX_PORT_1=1500 + <Instance_UID>
FEP	D_FEP_BIND_PORT_1=61627 + <Instance_UID>	D_FEP_BIND_PORT_2=62627 + <Instance_UID>
Communication	D_INTER_COMMUNICATION_PORT _1=4545 + <Instance_UID>	D_INTER_COMMUNICATION_PORT _2=5545 + <Instance_UID>
Corosync	<Corosync Port Number>	<Corosync Port Number> + 2

3.3.1.10 Verify OS Upgrade Viability

Before performing the upgrade, verify that the Operating System currently installed on the site servers can be upgraded.



To verify that the installed OS can be upgraded, perform the following steps on each site server:

6. Access the F5 Traffix service menu by typing **menu**.
7. Select **6) System Management**.
8. Select **3) Try to Upgrade OS**.
9. Select **2) Normal Mode**.
10. Enter the full path to the upgrade `.tar.gz` file.

If the returned value contains errors, contact *F5 Support* before beginning the ISSU.

3.3.1.11 Validate the System RPMs

The SDC software is installed on each site server with a specific set of RPMs. When upgrading the Operating System during the ISSU, RPMs that are relevant for the target SDC version are also upgraded. Existing RPMs on the site server that are not relevant for the target SDC version are not upgraded, and may not function as expected after the upgrade. To avoid this potential impact, the SDC can scan the RPMs installed on the site servers and identify RPMs that are not part of the currently installed SDC version's required RPMs. It is recommended to use the SDC to identify these RPMs, and to then manually delete these RPMs from **each site server** before performing the ISSU.



Note: In the event that the target version of the SDC requires additional RPMs, these RPMs are automatically added during the upgrade.

To identify the RPMs that must be deleted, upgrade the F5 Traffix service menu and generate a TTA Report. This report contains a `.txt` file with the list of RPMs that must be manually deleted before the ISSU, as well as a list of the RPMs that will be added automatically during the ISSU.



To verify the RPM files that are installed in your system, perform the following steps on each site server:



Note: The following procedure must be performed on all servers in the site.



Note: If you generated a TTA Report when validating system resources, skip to step 5.

11. Access the F5 Traffix service menu by typing **menu**.

12. Select **7) Generate Reports**.

13. Select **2) Generate TTA Report**.

14. Select **2) Normal Mode**.

The `tta-ng*.tar.gz` file is generated in the `/tmp` folder.

- h. Exit the menu and run the following commands to locate and open the `tta-ng*.tar.gz` file:

Note: When running the commands, replace `<tta-ng*>` with the specific file/folder name.

```
cd /tmp
```

```
tar xzvf <tta-ng*>.tar.gz
```

15. Run the following command:

```
cat /tmp/<tta-ng*>/os/OSReq/OSReq_rpm_check_report.txt
```

16. Manually delete the RPMs in the “RPM need to be deleted” list.



Warning: RPMs in the list that are not manually deleted may not function as expected after upgrade.



3.3.1.12 Delete Existing Snapshots

The ISSU includes a rollback option. During the upgrade process, snapshots are created of the servers in their pre-upgrade state. If, for any reason, the upgrade cannot be completed, these snapshots are used to revert servers back to their pre-upgrade state.

To ensure successful rollbacks, verify that there are no pre-existing F5 snapshots (F5_Snapshot) on the site servers.

To verify that there are no pre-existing snapshots on the site servers:

1. Run the following command on each server in the site:

lvscan

Any existing snapshots existing on the server will appear.

2. Delete existing F5 snapshots by running the following command on each server with snapshots:

lvremove <snapshot_name>



Note: This command only deletes the specific snapshot. To delete all available snapshots, enter the common pathname for all snapshots as the F5_Snapshot_name appended with an *. All F5 snapshots in that location will be deleted.

3.3.1.13 Update the SDC Site Configuration File

The SDC site configuration file that the SDC site was installed with must be updated to reflect the changes included in the upgrade. Since this upgrade is going to install a different version of SDC software, the site configuration file must be updated accordingly.

To update the SDC site configuration:

1. In the Installation Utility home page, click **Edit Existing Configuration**.

The **Select Configuration** screen appears.



2. Select the updated site configuration file by choosing the one of the following options:

- a. **Load the site configuration file from the installation Server** by performing the following steps:



Note: Choose this option if the file you want to work is already uploaded to the Installer server.

- i. Select the updated file from the drop-down list.

- b. **Upload Site Configuration File** to the installation server.



Note: Choose this option if the file you want to work with is located locally (for example, on a USB or on the desktop) and has not yet been uploaded to the installation server.

- i. Click **Browse** and navigate to the desired file.
- ii. Click **Open**.



Note: The selected configuration file is now on the installation server, and will appear in the drop-down list of available configuration files.

3. Click **Next**. The **Define Servers** screen appears.
4. Update the OS definition for each server in the table by selecting the relevant “rhel66” OS option from the drop-down list.
5. Add the “installer” role to the server that the installation utility is running on.
6. Add the “installer” role to one other site server.



Note: From release 4.4, the installation utility must run on a site server. In addition, from release 4.4 each site must contain two servers that are defined as installer servers.



7. Click **Next** until the **Configure Cluster** screen appears.



Note: This step is only applicable for SDC sites installed with SS7.

8. Remove the SS7 Cluster Group that was previously configured for prior SDC versions.



Note: This step is only applicable for SDC sites installed with SS7.

9. Verify that a CPF Cluster Clone is defined as part of the cluster. In version 4.4, the SS7 Cluster Group is automatically generated when the SS7 role is defined for the site and a CPF Cluster Clone is defined for the site.



Note: This step is only applicable for SDC sites installed with SS7.

10. Click **Next** until the **Configure Properties** screen appears.

11. Verify and update (if needed) the following site properties:

- a. In the System section:
 - **SDCVersion** – enter the file name of the SDC software version and build you are updating the site with. For example, 4.4.2-4.
 - **Installerip** – enter the IP address of the Installer server that the SDC connects to.
- b. In the config_mgr section:
 - **CM_MGT_VIP** – enter an IP address in the SDC site management network.
 - **CM_IC_VIP** – enter an IP address in the SDC site interconnect network.
 - **EMS_MGT_VIP** – enter the VIP address of the EMS Configuration Manager.
- c. In the Installer section:



- **Network** – enter the network IP address that is used for communication between the installation server and the site servers.
 - **startDHCP** – enter the lower end of the range of IP addresses that can be installed using PXE.
 - **endDHCP** – enter the upper end of the range of IP addresses that can be installed using PXE.
- d. In the SS7 section, verify and update (if needed) the IP addresses of the SS7 Signal Transfer Points (STPs) that the SDC will communicate with. Each SS7 deployment contains two STPs, and each STP can be accessed with up to two IP addresses in the signaling network.



Note: This step is optional, and must only be performed when enabling SS7 for the first time.

- **IsSccpMode** - enter True to enable the SCCP mode.
- **STP1IP1** - enter the primary IP address (on the signaling network) that is defined for the first STP (STP1). This address will be used by the CPF to communicate with the STP.
- **STP1IP2** - enter the secondary IP address (on the signaling network) that is defined for the first STP (STP1). This address will be used by the CPF to communicate with the STP.
- **STP1Port** - enter the STP1 port used by the SS7 driver.
- **STP1PC** - enter the point code for the STP1.
- **STP2IP1** - enter the primary IP address (on the signaling network) that is defined for the second STP (STP2). This address will be used by the CPF to communicate with the STP.



- **STP2IP2** - enter the secondary IP address (on the signaling network) that is defined for the second STP (STP2). This address will be used by the CPF to communicate with the STP.
- **STP2Port** - enter the STP2 port used by the SS7 driver.
- **STP2PC** - enter the point code for the STP2.
- **CPF1PC** - enter the point code for the SS7 driver that is used on CPF1.
- **CPF2PC** - enter the point code for the SS7 driver that is used on CPF2.



Note: When using RSI, the CPFPC value is the Originating Point Code, and must be configured with the same value for both CPF1 and CPF2.

- **RoutingContext1** - enter a unique value (i.e.1) for a routing context that defines a routing key of defined SS7 parameters.
 - **RoutingContext2** - enter a unique value (i.e.2) for a routing context that defines a routing key of defined SS7 parameters.
 - **NA** - enter a value in the Network Appearance field that identifies the SS7 network context (i.e. SS7 Point Code) for a routing key.
 - **NI** - enter a value in the Network Indicator field that identifies using a national (2) or international (o) network.
 - **iwfSgsnVirtualGtBase** - enter the IWF Virtual GT prefix of a pool for the MME node (TCAP mode only).
- e. In the Tripo section:
- **TripoVersion** – The default value is the “latest”. It is recommended to enter the version saved in the topology file.
 - **SecondSiteIP1** – The IP address of the first Tripo instance on the second SDC server.



- **SecondSiteIP2** – The IP address of the second Tripo instance on the second SDC server.

12. Click **Save**.

3.3.2 Performing the ISSU on an SDC Site

The following section describes the three phases of the ISSU.

3.3.2.1 Performing Phase 1: Upgrading the First Server Group

In this phase, one server group is selected, disconnected from the site, and upgraded, while the second server group continues to process traffic.



Note: First upgrade the server group that is not actively running the installation utility.



Note: During this phase, the second server group processes traffic without a local high availability option.



Warning: When upgrading SDC sites, if the active FEP component is running on a server in the first server group, a service disruption of up to 30 seconds may be experienced during this phase. To minimize the total downtime incurred throughout the ISSU, it is recommended to first upgrade the server group that is not actively running the FEP component.

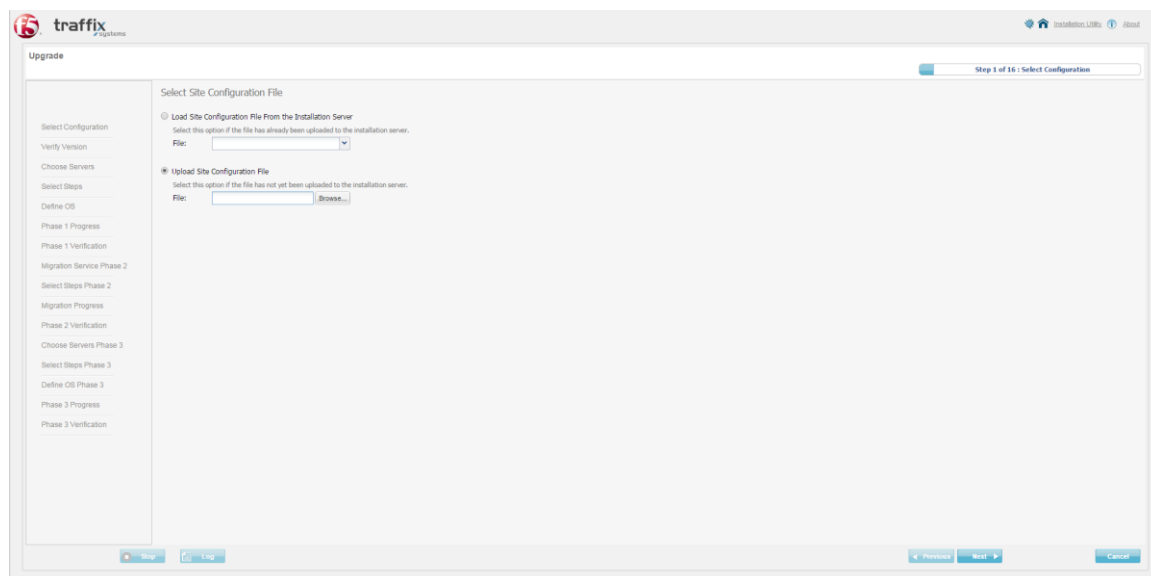
To perform phase 1:

1. In the Installation Utility home page, click **Upgrade**.

The **Select Configuration** screen appears.



Figure 27: Select Configuration Screen



2. Select the updated site configuration file by choosing the one of the following options:
 - a. **Load the site configuration file from the installation Server** by performing the following steps:



Note: Choose this option if the file you want to work is already uploaded to the Installer server.

- i. Select the updated file from the drop-down list.



Warning: Even though the site configuration file may appear in the list of Installer server configuration files, remember that you have just updated this file (based on the instructions in the *Update the SDC Site Configuration File* section). Verify that the updated version of the configuration file is defined in this step.

- b. **Upload Site Configuration File** to the installation server.



Note: Choose this option if the file you want to work with is located locally (for example, on a USB or on the desktop) and has not yet been uploaded to the installation server.

- i. Click **Browse** and navigate to the desired file.
- ii. Click **Open**.

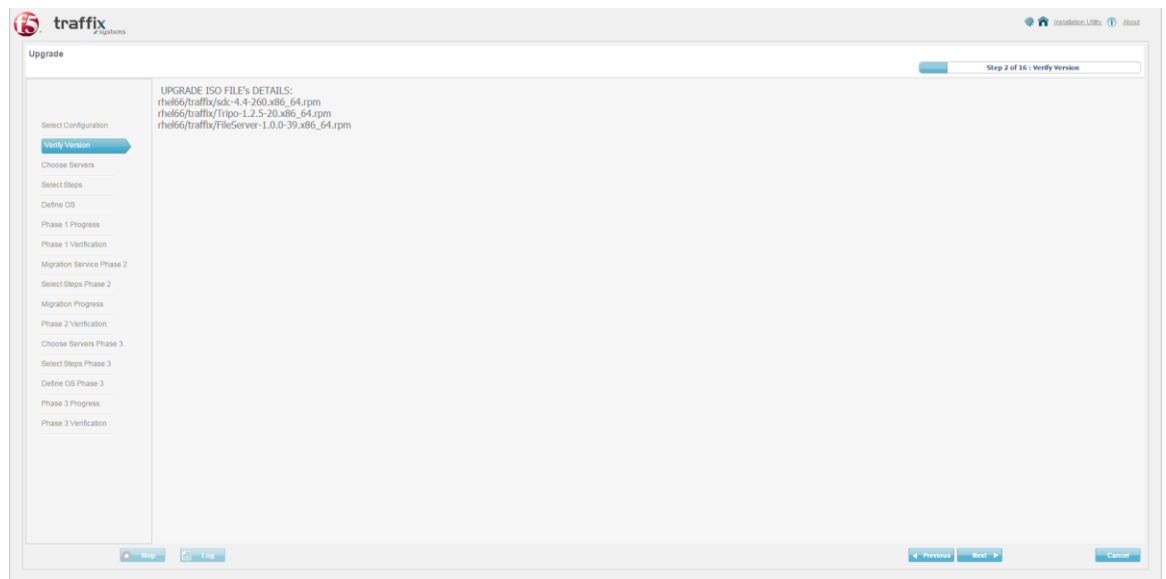


Note: The selected configuration file is now on the installation server, and will appear in the drop-down list of available configuration files.

3. Click **Next**.

The **Verify Version** screen appears.

Figure 28: Verify Version Screen



4. The **Verify Version** screen displays the release and build information of the target SDC version for the upgrade. Verify that these details are correct.

If the details are incorrect, verify that the prerequisites were completed correctly and the site configuration file was correctly updated, saved and uploaded.

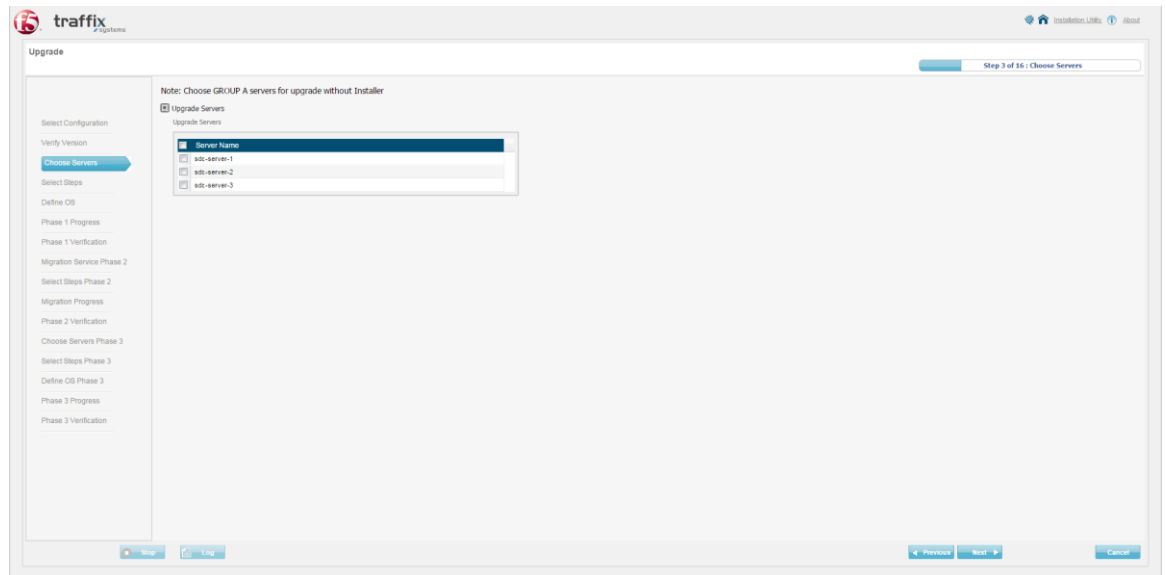


For more information, see *Update the SDC Site Configuration File*.

5. Click **Next**.

The **Choose Servers** screen appears.

Figure 29: Choose Servers Screen



6. Select the servers that are to be included in the first server group and click **Next**.

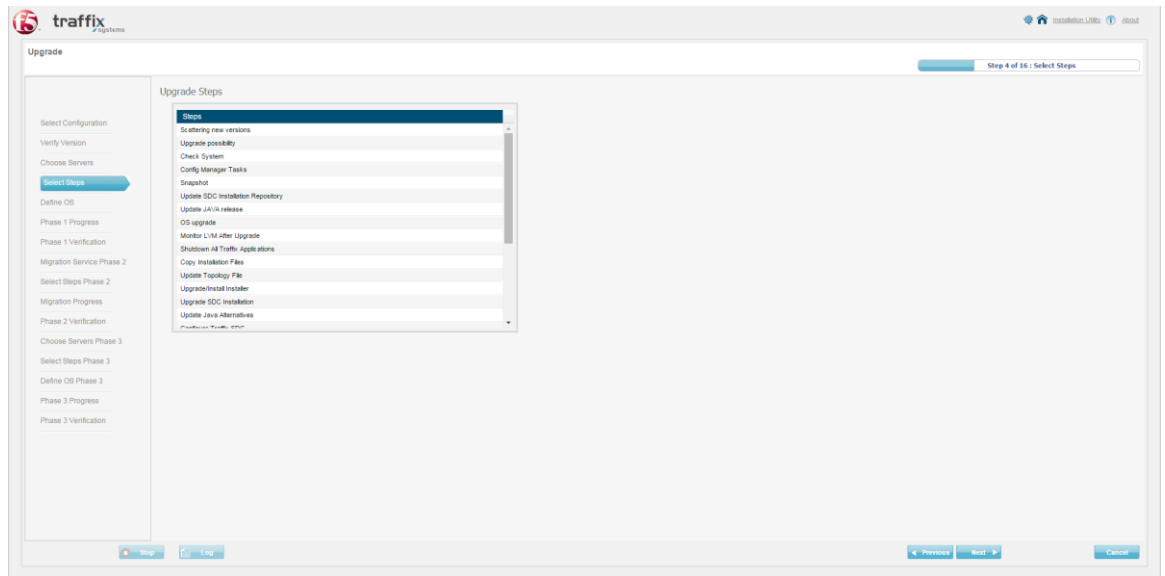


Note: This server group should **not** include the server that the installation utility is actively running on.

The **Select Steps** screen appears.



Figure 30: Select Steps Screen



Phase 1 of the ISSU procedure includes the following steps:

Table 7: Phase 1 Upgrade Steps

Step	Description
Scattering new versions	Copy files from the upgrade ISO file to the relevant repositories.
Upgrade possibility	Verify that each of the two server groups have the SDC components necessary to independently process site traffic.
Check System	Verify disk space, interfaces, etc.
Config Manager Task	Shuts down the Config Manager
Snapshot	Create a snapshot of the servers in the first server group, as they appear at the beginning of phase 1.
Update SDC Installation Repository	Update the SDC Installation Repository.
Update Java release	Upgrade Java version (if required).
OS Upgrade	Upgrade OS (if required).
Monitor LVM After Upgrade	Check the validity of the created snapshot.



Step	Description
Shutdown All Traffic Applications	Shut down all Traffic application.
Copy Installation Files	Copy the new installation files to the servers in the first server group.
Update Topology File	Copy the updated site configuration file to the servers in the first server group.
Upgrade/Install Installer	Upgrades the version of the installation utility installed on the secondary installer server.
Upgrade SDC Installation	Upgrade the SDC installation.
Update Java Alternatives	Updates Java links.
Configure Traffic SDC	Configure Traffic SDC.
Configure SDC Cluster	Configure the SDC cluster according to the site configuration file.
Upgrade NMSAgent	Upgrade the NMS Agent component (if different than current version)
Upgrade SS7	Upgrade the SS7 component (if different than current version)
Upgrade Splunk	Upgrade the Splunk component (if different than current version)
Migrate SDC Configuration	Migrate the SDC configuration onto the servers in the first server group.
Upgrade Tripo	Upgrade the Tripo component (if different than current version)
Upgrade FileServer	Upgrade the Fileserver component (if different than current version)
Split the system	Change the configured listener ports of all SDC components in order to sever communication between the server groups for the duration of the upgrade.
Configure Corosync Cluster	Change the configured Corosync ports to allow two clusters in the system.

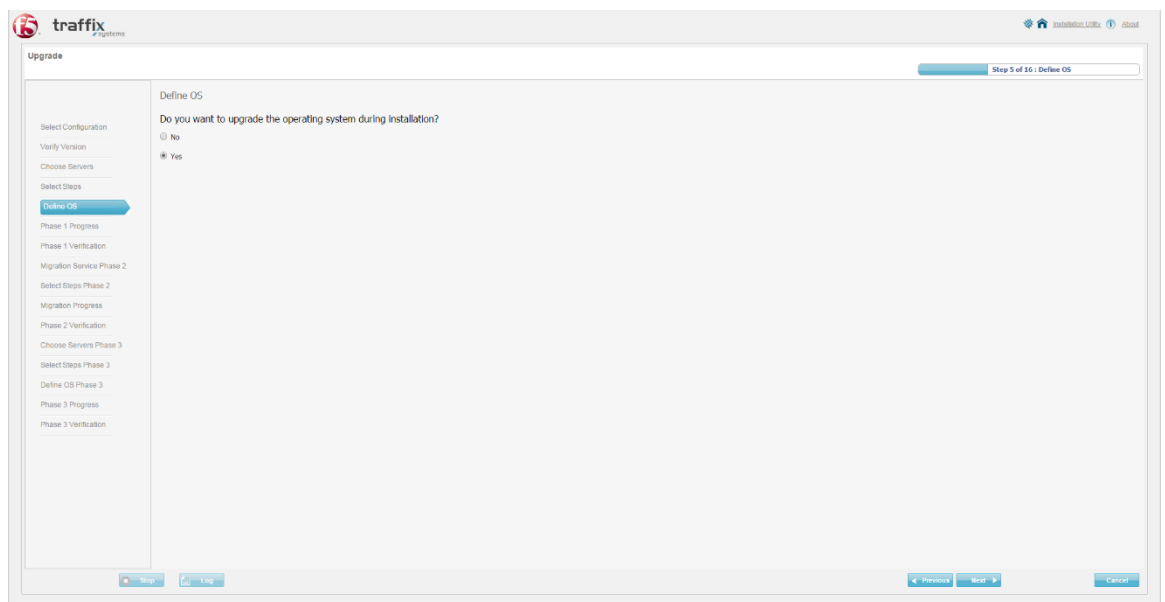


Step	Description
Reboot	Reboots the servers.

7. Click **Next**.

The **Define OS** screen appears.

Figure 31: Define OS Screen

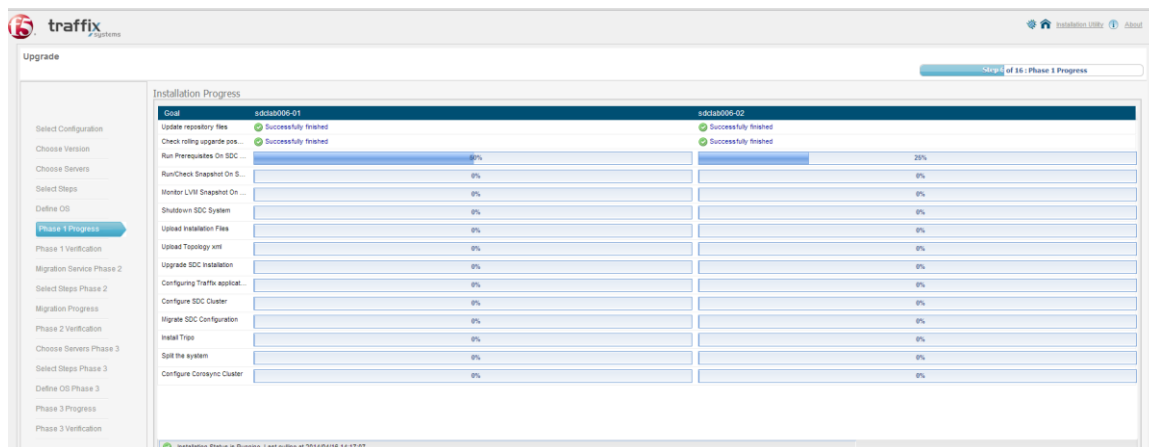


8. Select **Yes** in response to the question: **Do you want to upgrade the operating system during the upgrade.**
9. Click **Next** to start the phase 1 upgrade process.

The **Phase 1 Progress** screen appears.



Figure 32: Phase 1 Progress Screen



The **Phase 1 Progress** screen displays the upgrade progression for each upgrade step for each server. This way, if the upgrade fails on specific steps for a specific server, you can effectively troubleshoot the cause of the failure.



Note: If you encounter browser issues during the phase 1 upgrade process, this phase must be rolled back before retrying.

10. The following message is displayed: **“Upgrade has been successfully finished.”** Click **OK**.
11. Activate the SS7 license by performing the following steps:



Note: This step is only applicable when enabling SS7 for the first time, and must be repeated for every server that will run SS7.

- a. In your web browser, go to
<http://membersresource.dialogic.com/ss7/license/license.asp>.
- b. In the License Activation screen, follow the instructions to complete the form.
- i. Run the following command on the server to retrieve the Host ID # (Licensing Host ID):



cd /opt/DSI

./HSTBIN/m3ua -v

- ii. Run the following command on the server to retrieve the Machine Name:

Echo \$HOSTNAME

- c. Click **Submit**. The license file will be sent to the email address in the form.
- d. Copy the license file to /opt/DSI.
- e. Repeat for each server that will run SS7.

12. Install the activated SS7 license, by performing the following steps on each server in the first server group:

- a. Copy the activated SS7 license file to the following directory:
/opt/DSI
- b. Restart the SS7 driver by running the following command at /opt/DSI:
gctload -x

13. Run the following command on each server in that group to switch the servers to online mode.

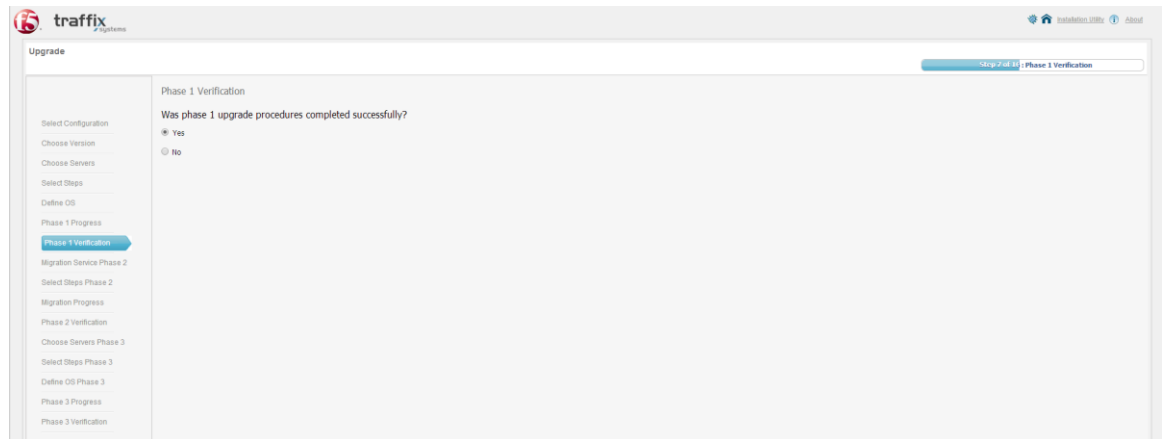
crm node online

14. Click **Next**.

The **Phase 1 Verification** screen appears.



Figure 33: Phase 1 Verification Screen



15. Run the following command on each server in the first server group to check that each server is successfully online. Each server is successfully online if the SDC clone components configured to run on the server are up.

crm_mon -n

16. If the servers in the first server group are up and running, select **Yes** in the **Phase 1 Verification** screen.

If the servers in the first server group are not up and running properly, select **No**. This means that this phase failed and the servers need to be reverted to their pre-phase 1 state. The following message appears: **Please perform manual rollback**. For information about the rollback, see *Performing an Upgrade Rollback*.

3.3.2.2 Performing Phase 2: Activating Server Group 1 as Primary Server Group

At this point, phase 1 is complete. The servers that were selected to be upgraded in phase 1 are successfully upgraded, but are still disconnected from the site. Site traffic is being processed by the second server group.



In phase 2, site traffic will be processed by the servers in the first server group that will be reconnected to the site, while the remaining servers will be disconnected from the site and will not process site traffic.



Note: During this phase, the first server group processes traffic without a local high availability option.



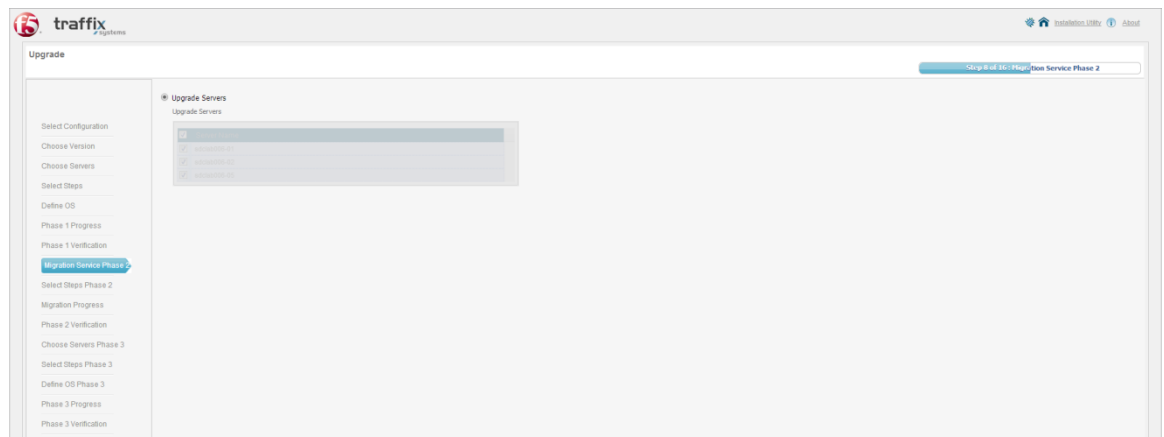
Warning: In this phase, a service disruption of up to 30 seconds will be experienced, as a result of the FEP component in the first server group being activated from standby mode.

To perform phase 2:

1. After selecting **Yes** in the Phase 1 Verification screen, click **Next**.

The **Migration Service Phase 2** screen appears.

Figure 34: Migration Service Phase 2 Screen

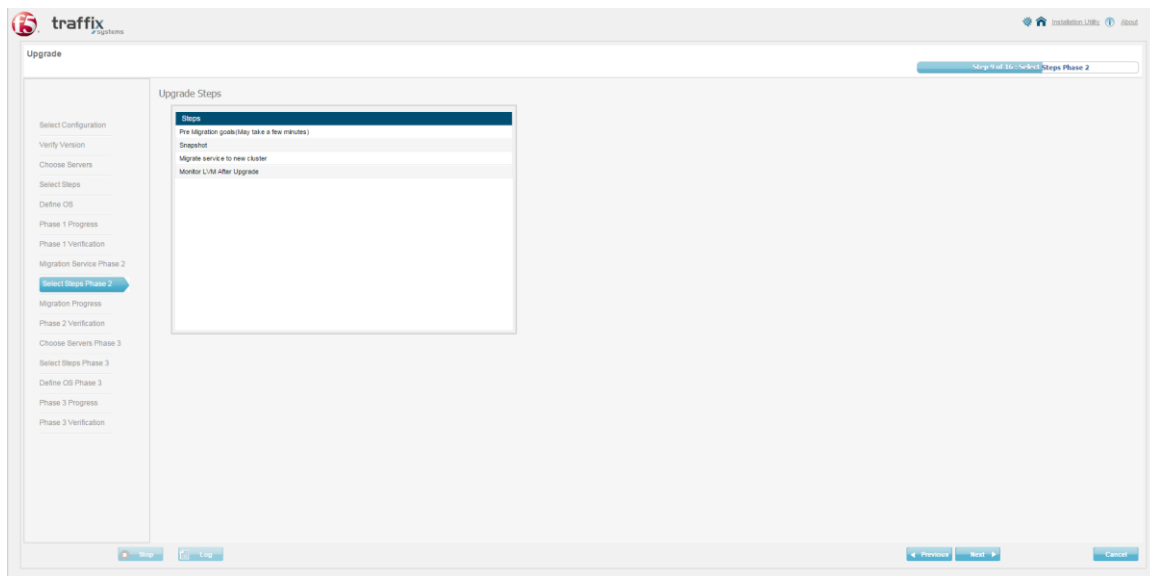


2. In the **Migration Service Phase 2** screen, the server selection option is grayed out. All servers are selected in this phase.
3. Click **Next**.

The **Select Steps Phase 2** screen appears.



Figure 35: Select Steps Phase 2 Screen



Phase 2 of the ISSU procedure includes the following steps:

Table 8: Phase 2 Upgrade Steps

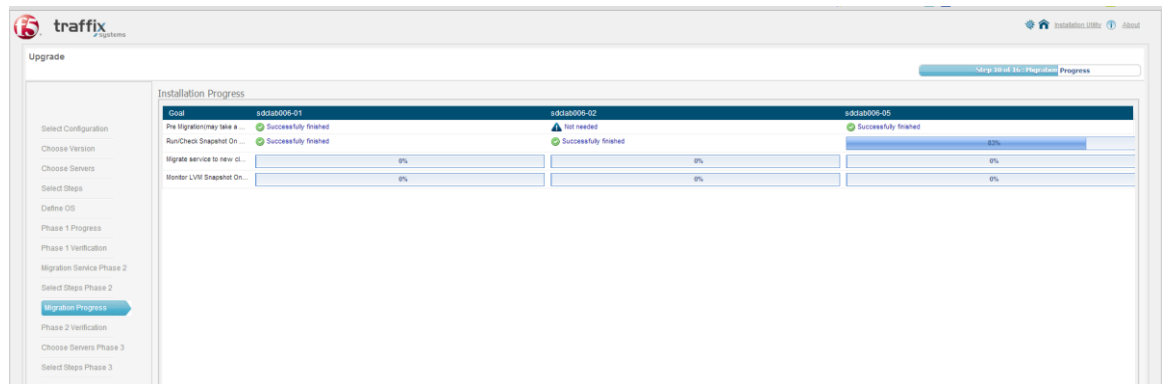
Step	Description
Pre Migration goals (Make take a few minutes)	Perform the prerequisites steps necessary before service migration (for example, syncing Tripo entries).
Snapshot	Create a snapshot of the second server group.
Migrate service to new cluster	Switch site traffic to be processed by servers in the first server group.
Monitor LVM After Upgrade	Verify the validity of the created snapshots.

4. Click **Next** to start the phase 2 upgrade process.

The **Migration Progress** screen appears.



Figure 36: Migration Progress Screen



The **Migration Progress** screen displays the upgrade progression for each upgrade step for each server. This way, if the migration fails on specific steps for a specific server, you can effectively troubleshoot the cause of the failure.



Note: If you encounter browser issues during the phase 2 migration process, this phase must be rolled back before retrying.



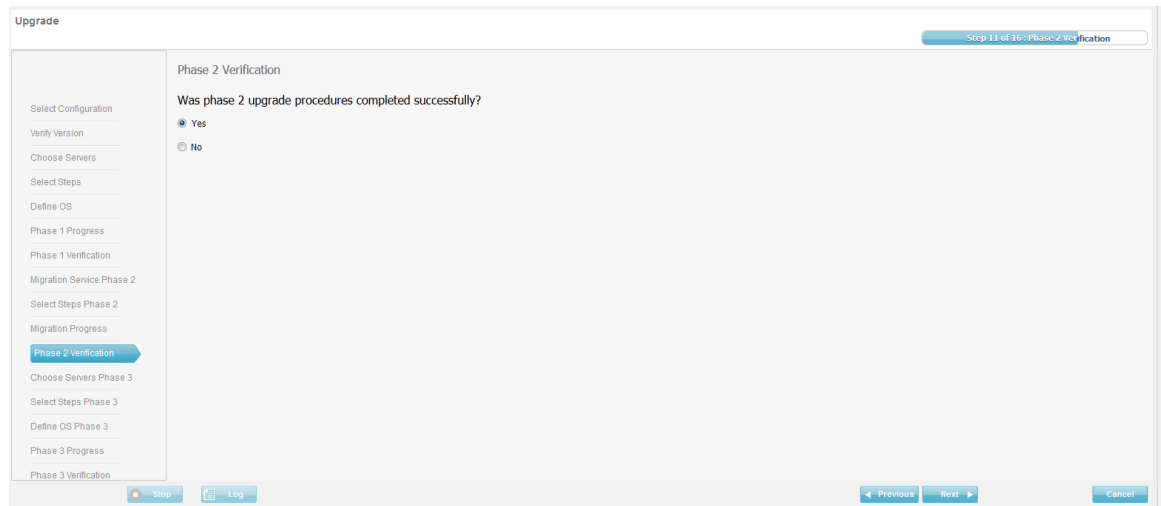
Note: The first goal, **Pre Migration goals** that is displayed is only relevant when your system is also upgrading the Tripo version.

5. The following message is displayed: “**Upgrade has been successfully finished.**” Click **OK**.
6. Click **Next**.

The **Phase 2 Verification** screen appears.



Figure 37: Phase 2 Verification Screen



7. Run the following command on each server in the site, and check the servers as follows:

crm_mon -n

- a. Check that servers in the first server group are all online and running all the SDC components configured on them.
- b. Check that servers in the second server group are all online and running only the SDC “ClusterMon” and “Tripo” clone components configured on them.
- c. Using the Web UI, check that the FEP and CPF components running on servers in the first server group are shown as active.



Note: You may need to refresh the Web UI by pressing **F5**.

8. If the servers in the first server group are up and running, select **Yes** in the **Phase 2 Verification** screen, and click **Next**.

If the servers are not up and running properly, select **No**. This means that this phase failed and the servers need to be reverted to their pre-phase 2 state. The following message appears: **Please perform manual rollback**. For information about the rollback, see *Performing an Upgrade Rollback*.



3.3.2.3 Performing Phase 3: Upgrading Server Group 2

At this point, phase 2 is successfully finished. Traffic is being processed by the upgraded servers in the first server group. The servers in the second server group are online, but are disconnected from the site and are not processing site traffic.

In this phase, the second server group is selected, shut down, and upgraded, while the first server group processes traffic.



Note: During this phase, the first server group continues to process traffic without a local high availability option.



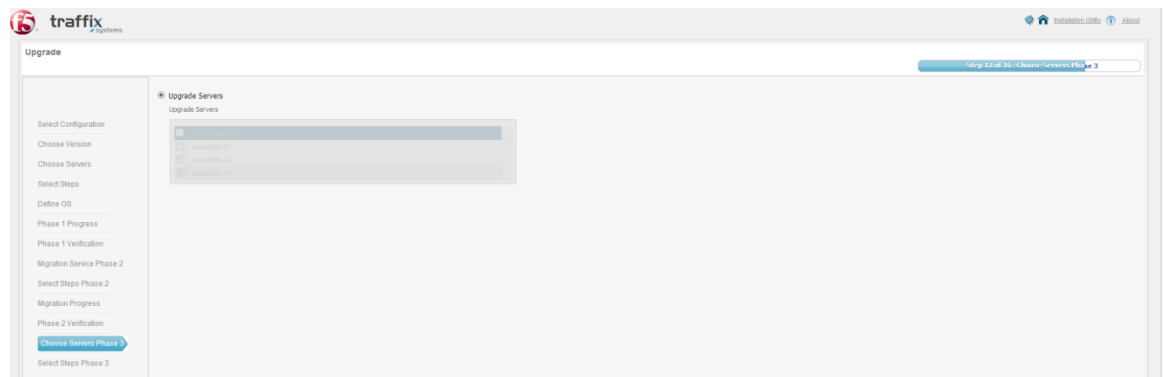
Warning: If the active FEP component is configured to actively run on one of the servers in the second server group, a service disruption of up to 30 seconds may be experienced during this phase.

To perform phase 3:

1. After selecting **Yes** in the Phase 2 Verification screen, click **Next**.

The **Choose Servers Phase 3** screen appears.

Figure 38: Choose Servers Phase 3 Screen

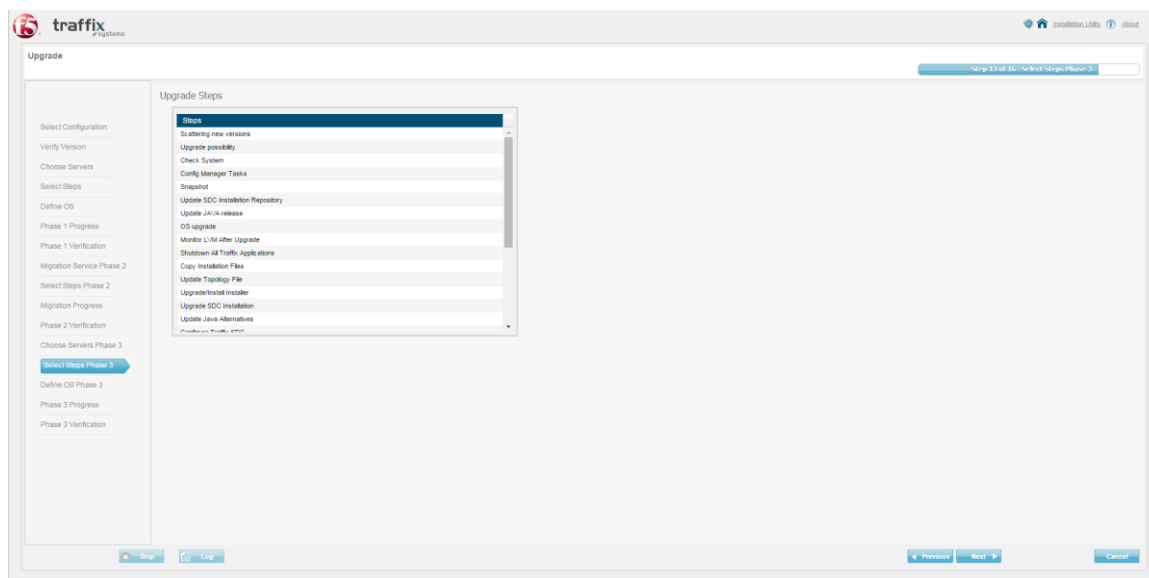


2. In the **Choose Servers Phase 3** screen, select the servers in the second server group and click **Next**.

The **Select Steps Phase 3** screen appears.



Figure 39: Select Steps Phase 3 Screen



Phase 3 of the ISSU procedure includes the following steps:

Table 9: Phase 3 Upgrade Steps

Step	Description
Scattering new versions	Copy files from the upgrade ISO file to the relevant repositories.
Upgrade possibility	Verify that each of the two server groups have the SDC components necessary to independently process site traffic.
Check System	Verify disk space, interfaces, etc.
Config Manager Task	Shuts down the Config Manager
Snapshot	Create a snapshot of the servers in the first server group, as they appear at the beginning of phase 1.
Update SDC Installation Repository	Update the SDC Installation Repository.
Update Java release	Upgrade Java version (if required).
OS Upgrade	Upgrade OS (if required).
Monitor LVM After Upgrade	Check the validity of the created snapshot.



Step	Description
Shutdown All Traffic Applications	Shut down all Traffic application.
Copy Installation Files	Copy the new installation files to the servers in the first server group.
Update Topology File	Copy the updated site configuration file to the servers in the first server group.
Upgrade/Install Installer	Upgrades the version of the installation utility installed on the secondary installer server.
Upgrade SDC Installation	Upgrade the SDC installation.
Update Java Alternatives	Updates Java links.
Configure Traffic SDC	Configure Traffic SDC.
Configure SDC Cluster	Configure the SDC cluster according to the site configuration file.
Upgrade NMSAgent	Upgrade the NMS Agent component (if different than current version)
Upgrade SS7	Upgrade the SS7 component (if different than current version)
Upgrade Splunk	Upgrade the Splunk component (if different than current version)
Migrate SDC Configuration	Migrate the SDC configuration onto the servers in the first server group.
Upgrade Tripo	Upgrade the Tripo component (if different than current version)
Upgrade FileServer	Upgrade the Fileserver component (if different than current version)
Split the system	Change the configured listener ports of all SDC components in order to sever communication between the server groups for the duration of the upgrade.
Configure Corosync Cluster	Change the configured Corosync ports to allow two clusters in the system.

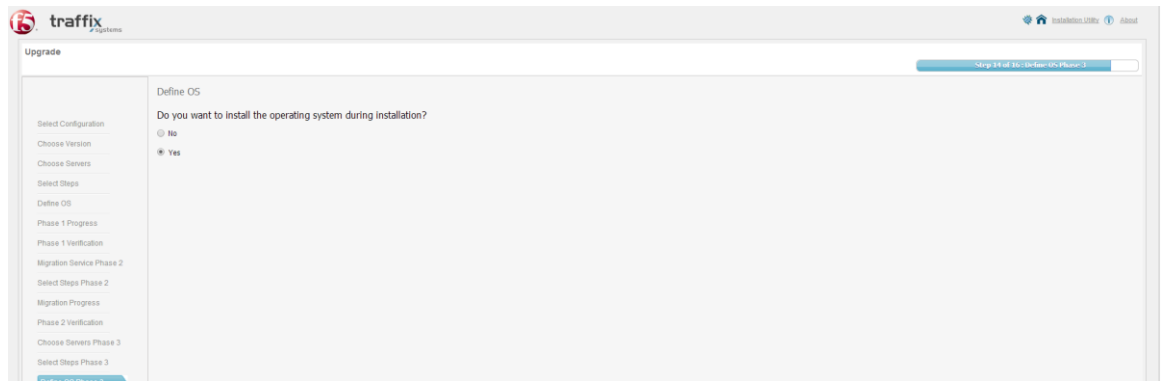


Step	Description
Reboot	Reboots the servers.

3. Click **Next**.

The **Define OS Phase 3** screen appears.

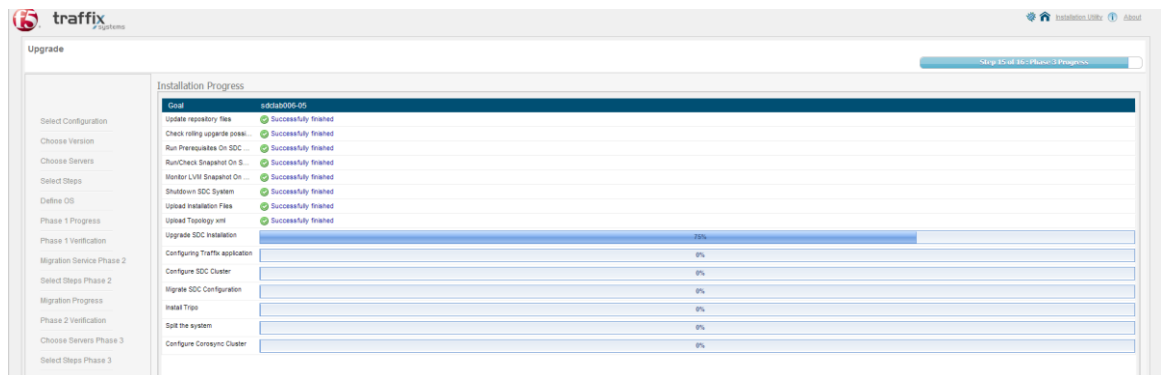
Figure 40: Define OS Phase 3 Screen



4. Select **Yes** in response to the question: **Do you want to upgrade the operating system during the upgrade.**
5. Click **Next** to start the phase 3 upgrade process.

The **Phase 3 Progress** screen appears.

Figure 41: Phase 3 Progress screen





The **Phase 3 Progress** screen displays the upgrade progression for each upgrade step for each server. This way, if the upgrade fails on specific steps for a specific server, you can effectively troubleshoot the cause of the failure.



Note: If you encounter browser issues during the phase 3 upgrade process, this phase must be rolled back before retrying.

6. The following message is displayed: “**Upgrade has been successfully finished.**” Click **OK**.
7. Install the activated SS7 license, by performing the following steps on each server in the first server group:
 - a. Copy the activated SS7 license file to the following directory:
`/opt/DSI`
 - b. Restart the SS7 driver by running the following command at `/opt/DSI`:
gctload -x
8. In the **Phase 3 Verification** screen, select **Next > Yes > Finish**.
9. Reboot the server(s) in the group that the installer is installed on.
10. Run the following command on each server in that group to switch the servers to online mode:
crm node online
11. Run the following command on each server in the second server group and verify that each server has the SDC components configured for it in the site configuration file, and that all SDC clone components are running:

crm_mon -n

If the servers are not up and running properly, this means that this phase failed and the servers need to be reverted to their pre-phase 3 state. For information about the rollback, see *Performing an Upgrade Rollback*.



If the server are up and running properly, this means that phase 3 is complete, and the site has been successfully upgraded. Traffic is processed by all servers in the site.

At this point, phase 3 is complete, and the site has been successfully upgraded. Traffic is processed by all servers in the site.

If your SDC site includes SS7, perform the *Enabling SS7 Driver Redundancy* post-upgrade procedure.

To continue with the ISSU of a deployment with multiple SDC sites managed by an EMS site, return to the *Upgrading Multiple SDC Sites Managed by an EMS Site* section.

3.4 Performing an Upgrade Rollback

Each phase in the F5 In-Service Software Upgrade (ISSU) includes the option to revert the changes made on your SDC site servers to their original state prior to that phase. In the initial stages of each upgrade phase, snapshots are created of each of the servers selected for that phase. Using these snapshots, the servers can be returned to their original state.



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.

Performing an upgrade rollback after phase 1 of a site upgrade only affects servers in the first server group, as only they are selected in phase 1. Performing an upgrade after phase 2 of a site upgrade, however, affects all site servers, as they are all selected in phase 2.

For more information about the ISSU phases, see *What Happens During an ISSU of a single site?* section.



Note: All servers in the affected server group must be rolled back and rebooted at the same time.



Note: The option to roll back the upgrade is only available while the snapshot is active.

To perform an upgrade rollback:

To return a server to its original, pre-upgrade state, perform the following steps:



Note: The following commands must be performed on each server that was selected as part of the upgrade phase that you want to revert.

1. When rolling back an SDC site that is managed by the EMS that previously ran an SDC 4.0.2 or 4.0.5 version, perform the following step:



Warning: This step must only be performed on SDC sites that are managed by an EMS site, and **only** when the EMS site is **not** going to be rolled back.

- a. Back up the `/opt/traffic/sdc/config/sysconfig/traffic_config_mgr` file.
- b. Run the following command on the EMS server:
`vi /opt/traffic/sdc/config/sysconfig/traffic_config_mgr`
- c. This file contains a text block that we have divided into the following two sections (in the two bullets below). Search for the “CONFIG_MGR_REMOTE_NETWORK_URI” parameter in the file to locate the text block. Delete the section that includes the Management IP addresses of the servers in the SDC site you wish to roll back, as follows:
 - If the Management IP addresses of the servers in the site that you wish to roll back appear in the following section, delete this section:

```
failover:(tcp://
://<SDCSite1Server1_Management_IP>:61617?wireFormat.maxInacti
vityDuration=30000&keepAlive=true,tcp://
://<SDCSite1Server2_Management_IP>:61617?wireFormat.maxInacti
vityDuration=30000&keepAlive=true)?randomize=false&maxReconne
ct
Attempts=0,
```



- If the Management IP addresses of the servers in the site that you wish to roll back appear in the following section, delete this section:

```
failover:(tcp://  
://<SDCSite2Server1_Management_IP>:61617?wireFormat.maxInacti  
vityDuration=30000&keepAlive=true,tcp://  
://<SDCSite2Server2_Management_IP>:61617?wireFormat.maxInacti  
vityDuration=30000&keepAlive=true)?randomize=false&maxReconne  
ctAttempts=0
```

- d. Restart the Config Manager clone resource on the EMS servers.
2. Print a list of the snapshots available for the server, by running the following command:

```
lvscan
```

A list of the available snapshots will be printed.

3. Apply an available snapshot and revert to it, by running the following command:
lvconvert --merge <snapshot_name>



Note: This command only applies the specific snapshot. To apply all available snapshots, enter the common pathname for all snapshots as the `snapshot_name` appended with an F5*. All snapshots in that location will be applied.

4. Run the following commands to roll back to the original OS kernel:

```
cd /  
  
tar zxvf /var/tmp/boot-backup.tgz  
  
/sbin/grub-install /dev/sda
```

5. Reboot the server by running the following command:

```
reboot
```



Note: After reboot the snapshot is automatically deleted.

6. Print a list of the snapshots available for the server, by running the following command:

lvscan

A list of the available snapshots will be printed.

7. Check the list of available snapshots. If the word “original” or “snapshot” initially appears, run the following command until a list of available snapshots appears without the word “original” or “snapshot”:

lvscan

8. Reboot the server by running the following command:



Note: All servers in the affected server group must be rebooted at the same time.

reboot

The rollback commands are illustrated in the following screenshot:



Figure 42: Rollback Commands and Snapshot List with “Original” and “Snapshot”

```
[root@sdclab005-16 ~]# lvscan
ACTIVE      Original   '/dev/vg1/lv_root' [19.53 GiB] inherit
ACTIVE      Original   '/dev/vg1/lv_swap' [14.11 GiB] inherit
ACTIVE      Original   '/dev/vg1/lv_opt' [19.53 GiB] inherit
ACTIVE      Original   '/dev/vg1/lv_var' [19.53 GiB] inherit
ACTIVE      Original   '/dev/vg1/lv_data' [19.53 GiB] inherit
ACTIVE      Snapshot   '/dev/vg1/F5_Snapshot-lv_data' [37.29 GiB] inherit
ACTIVE      Snapshot   '/dev/vg1/F5_Snapshot-lv_opt' [29.83 GiB] inherit
ACTIVE      Snapshot   '/dev/vg1/F5_Snapshot-lv_root' [23.86 GiB] inherit
ACTIVE      Snapshot   '/dev/vg1/F5_Snapshot-lv_var' [19.09 GiB] inherit
[root@sdclab005-16 ~]# lvconvert --merge /dev/vg1/F5*
Can't merge over open origin volume
Merging of snapshot F5_Snapshot-lv_data will start next activation.
Can't merge over open origin volume
Merging of snapshot F5_Snapshot-lv_opt will start next activation.
Can't merge over open origin volume
Merging of snapshot F5_Snapshot-lv_root will start next activation.
Can't merge over open origin volume
Merging of snapshot F5_Snapshot-lv_var will start next activation.
[root@sdclab005-16 ~]# reboot

Broadcast message from root@sdclab005-16
(/dev/pts/0) at 14:20 ...

The system is going down for reboot NOW!
[root@sdclab005-16 ~]#
```

9. Switch the configuration manager component to online mode by running the following script on **one server** from the **first server group** according to the instructions below.

```
cd /var/tmp/installation
```


```
./resource_mgmt.sh      myip=172.29.55.210      resource=config_mgr  
command=start
```

- myip – enter the management IP of the server that you are running the script on.
- resource – verify that the value is “config_mgr”.
- command – verify that the value is “start”

10. When rolling back an SDC site that is managed by the EMS that previously ran an SDC 4.0.2 or 4.0.5 version, perform the following step to connect the SDC site to the EMS site:



- a. Run the following command on the EMS server:
`vi /opt/traffix/sdc/config/sysconfig/traffix_config_mgr`
- b. Add the text block that was removed at the beginning of the rollback procedure.
- c. Restart the Config Manager resource on the EMS servers.

 Warning: This step must only be performed when rolling back an SDC site managed by the EMS to its original SDC 4.0.2 or 4.0.5 version.



4. Post-Upgrade Procedures

The following procedures are performed after the upgrade process is successfully completed.

4.1 Validate the System RPMs

During the upgrade, RPM files were installed on the upgraded servers. Verify that all necessary RPM files are installed in your system with the following procedure.

To verify the RPM files that are installed in your system, perform the following steps on each site server:



Note: The following procedure must be performed on all servers in the site.

1. Access the F5 Traffic service menu by typing **menu**.
2. Select **7) Generate Reports**.
3. Select **2) Generate TTA Report**.
4. Select **2) Normal Mode**.

The `tta-ng*.tar.gz` file is generated in the `/tmp` folder.

5. Exit the menu and run the following commands to locate and open the `tta-ng*.tar.gz` file:

Note: When running the commands, replace `<tta-ng*>` with the specific file/folder name.

```
cd /tmp
```

```
tar xzvf <tta-ng*>.tar.gz
```

6. Run the following command:

```
cat /tmp/<tta-ng*>/os/OSReq/OSReq_rpm_check_report.txt
```



7. Verify that there are no RPMs in the “RPM need to be added” list. If the list is not empty, contact *F5 Support*.

4.2 Enabling Tripo Site Replication

This feature enables the replication of sessions between Tripo instances on mated SDC sites. Enabling the Tripo Site Replication feature is a post-installation step that is performed only after the Tripo site replication on Tripo instances (resources) on both SDC sites has been enabled

To enable Tripo site replication on each server that has a Tripo resource:

1. Verify the Tripo inter-site connection between the mated SDC sites:
 - a. Run the following commands:
 - i. **su - traffix**
 - ii. **cd /home/traffix/Tripo/env/linux-x86_64/**
 - iii. **. DefEnv Tripo**
 - iv. **UI_ViewServers -p**
 - b. Verify that the version of both Tripo resources on the SDC site are the same by comparing the **Local version** to a **Local Mate version**.
 - c. Verify that the IP addresses of the Tripo instances on the remote SDC site are displayed in the **Site IP** column. These IP addresses are configured during the installation.

Figure 43: Tripo Inter-site Connection Verification (Versions and IP Addresses)

```
[root@sdclab008-03 ~]# su - traffix
[traffix@sdclab008-03 ~]$ cd /home/traffix/Tripo/env/linux-x86_64/
[traffix@sdclab008-03 linux-x86_64]$ . DefEnv Tripo

Environment:    Tripo
Version:        svn head revision
Build no:       Not supported yet.
ICORE version:  svn head revision
OCORE version:  svn head revision

[traffix@sdclab008-03 Tripo]$ UI_ViewServers -p
11:19:58
Local version = 21000
Local mate version = 21000
Site IP      | Site Port | Status    | Version
-----+-----+-----+-----
10.1.57.11   | 43211     | Secondary | 21000
10.1.57.12   | 43211     | Primary   | 21000
```



2. Verify that the connection between each Tripo instance and the Tripo instances on the mated SDC site are established. The verification is done by:
 - a. Checking that each Tripo instance has two established connections to both Tripo instances on the mated SDC site.
 - b. Checking that each Tripo instance is listening on the Tripo SRR port defined during the installation.

The following screenshot is an example for a deployment which has two Tripo instances on the local SDC and on the mated SDC site.

Figure 44: Connection Verification of Inter-site Tripo Instances

```
[traffix@sdclab008-03 Tripo]$ netstat -na | grep 43211
tcp        0      0 0.0.0.0:43211          0.0.0.0:*              LISTEN
tcp        0      0 10.1.57.7:50965        10.1.57.11:43211       ESTABLISHED
tcp        0      0 10.1.57.7:50963        10.1.57.11:43211       ESTABLISHED
tcp        0      0 10.1.57.7:43211        10.1.57.12:39722       ESTABLISHED
tcp        0      0 10.1.57.7:43211        10.1.57.11:34557       ESTABLISHED
tcp        0      0 10.1.57.7:43211        10.1.57.12:39721       ESTABLISHED
tcp        0      0 10.1.57.7:48315        10.1.57.12:43211       ESTABLISHED
tcp        0      0 10.1.57.7:43211        10.1.57.11:34558       ESTABLISHED
tcp        0      0 10.1.57.7:48316        10.1.57.12:43211       ESTABLISHED
[traffix@sdclab008-03 Tripo]$
```

3. Enable Tripo Site Replication by running the following commands on each server running Tripo Resource:
 - a. **su - traffix**
 - b. **cd /home/traffix/Tripo/env/linux-x86_64/**
 - c. **. DefEnv Tripo**
 - d. **UI_Config**
 - e. **set SiteReplication true**
 - f. **CTRL-C** to exit from UI_config
 - g. **UI_Config -w ConfigParams.cfg**
4. Verify that the Tripo Site Replication was enabled, by running the following commands:
 - a. Run **UI_config**
 - b. **==>dump**
 - c. Review the *ConfigParams.cfg* file (located in the */home/traffix/Tripo/cfg/* folder) and check that **SiteReplication = true**



Figure 45: SiteReplication Parameter Verification

```
[traffix@VM-1 ~]$ cd /home/traffix/Tripo/env/linux-x86_64/
[traffix@VM-1 linux-x86_64]$ . DefEnv Tripo

Environment:      Tripo
Version:          svn head revision
Build no:         Not supported yet.
ICORE version:    svn head revision
OCORE version:    svn head revision

[traffix@VM-1 Tripo]$ UI_Config

==>set SiteReplication true

==>dump

[Storage]
RetransTimerInterval = 6000
SiteRetransTimerInterval = 2000
DeleteTimerInterval = 1500
NumOfMateRetrans = 3
NumOfSiteRetrans = 1
DeleteNotification = true
SiteReplication = true
UpdateOnExpireTimerInterval = 1000
[Replication]
MaxTransToProcess = 500
MaxTransToSend = 40
MaxTransToSendSite = 40
SleepInterval = 1
RecoveryRequestWaitTime = 10000
RecoveryMonitorInterval = 1000
RecoveryMatePendingCnt = 180
RecoveryMatesCompleteCnt = 30
[ComSrv]
NumOfTCPMsgsToSend = 200
NumOfMsgsToSend = 200
==>
```

5. Enable Tripo replication on each server that has a CPF resource on both SDC sites:
 - a. Go to the following folder: `/opt/traffix/sdc/config/sysconfig/`
 - b. Within the folder, open the “traffix” file.
 - c. Add the parameter `USE_TREPO_REPLICATION=true`. If the parameter exists, change the setting from false to true.
 - d. Save the file and restart each CPF and FEP resource one by one.



Note: After changing the SiteReplication parameter to true, verify that a “tripoEnableSRR” trap is generated from each Tripo instance.



4.3 Enabling SS7 Driver Redundancy

Configuring RSI & RMM between two drivers of two CPF instances (A and B) can:

- Enable rerouting of SS7 traffic from CPF A to the driver serving CPF B when the links of the driver serving CPF A are down.
- Ensures that SS7 responses are sent to the CPF driver that initiated the corresponding SS7 request.

Before enabling SS7 driver redundancy, verify the following prerequisites:

- The SDC should be installed and configured with the required SS7 drivers.
- The SDC should have two CPF instances. Each CPF instance should be on a separate server and have a dedicated Dialogic driver which serves it.

To enable SS7 Driver Redundancy:

1. Modify the system.txt file in the /opt/DSI directory by adding the following three modules:
 - RMM module – identified by module id 0x32 for both drivers.
 - RSI module – identified by module id 0xb0 for both drivers.
 - rsicmd module – identified by module id 0xfd for both drivers.



Note: These modules should be added to both SS7 drivers.

- a. Add the following lines to the system.txt file:

```
LOCAL 0x32 *RMM module
LOCAL 0xb0 *RSI module
LOCAL 0xfd *rsicmd module
```

- b. Each driver requires a different redirection configuration.
 - i. For driver A's redirection configuration, add the following lines to driver A's system.txt file:

```
*
* Definitions for Unit A:
```



```
*
REDIRECT 0x52 0xb0 * RMM to unit B
REDIRECT 0x12 0xb0 * M3UA to unit B
REDIRECT 0x53 0xb0 * SCCP to unit B
REDIRECT 0x34 0xb0 * TCAP to unit B
*
REDIRECT 0x42 0x32 * RMM from unit B
REDIRECT 0x02 0xd2 * M3UA from unit B
REDIRECT 0x43 0x33 * SCCP from unit B
REDIRECT 0x24 0x14 * TCAP from unit B
*
```

The first segment redirects traffic from driver A (“Unit A”) modules to driver B (“Unit B”) via the RSI module. The second segment redirects traffic from driver B (“Unit B”) to driver A (“Unit A”) local modules.

- ii. For driver B’s redirection configuration, add the following lines to driver B’s system.txt file:

```
*
* Definitions for Unit B:
*
REDIRECT 0x42 0xb0 * RMM to unit A
REDIRECT 0x02 0xb0 * M3UA to unit A
REDIRECT 0x43 0xb0 * SCCP to unit A
REDIRECT 0x24 0xb0 * TCAP to unit A
*
REDIRECT 0x52 0x32 * RMM from unit A
REDIRECT 0x12 0xd2 * M3UA from unit A
REDIRECT 0x53 0x33 * SCCP from unit A
REDIRECT 0x34 0x14 * TCAP from unit A
*
```

The first segment redirects traffic from driver B (“Unit B”) modules to driver A (“Unit A”) via the RSI module. The second segment redirects traffic from driver B (“Unit B”) to driver A (“Unit A”) local modules.



- c. Use the FORK_PROCESS command to configure and start the modules:
 - i. Add the following lines to driver A's system.txt file:

```
FORK_PROCESS ./rmm -m0x32 -d  
FORK_PROCESS ./rsi -m0xb0 -r./rsi_lnk -l1  
FORK_PROCESS ./rsicmd 0 0x32 0 <rem_addr> <rem_port> 0xb0
```

- ii. Add the following lines to driver B's system.txt file:

```
FORK_PROCESS ./rmm -m0x32 -d  
FORK_PROCESS ./rsi -m0xb0 -r./rsi_lnk -l1  
FORK_PROCESS ./rsicmd 0 0x32 1 <rem_addr> <rem_port> 0xb0
```



Note: The syntax for rsicmd is:

rsicmd <link_id> <conc_id> <link_type> <rem_addr> <rem_port> [<rsi_id>]

<link_id> should be set to '0' – represents one link with id '0'.

<conc_id> should be set to "0x32" - identifies the local module which will receive a message when the RSI link fails.

<link_type> should be set to '0' for driver A (represents Client connection type) and should be set to '1' for driver B (represents Server connection type).

<rem_addr> should be configured to the server driver IP address.

<rem_port> should be configured to the server driver TCP/IP socket port. Each RSI link should have a unique port value, starting from 9000.

<rsi_id> should be set to "0xb0" – identifies the RSI module.

2. Modify the config.txt file in the /opt/DSI directory by performing the following steps:



Note: These modules should be added to both SS7 drivers.

- a. To enable RMM transport over RSI, add the <DUAL> parameter to the CNSYS command:



- i. For driver A, set the <DUAL> parameter value to 'A':

```
CNSYS:IPADDR=10.2.9.7,IPADDR2=10.2.9.9,DUAL=A;
```

- ii. For driver B, set the <DUAL> parameter value to 'B':

```
CNSYS:IPADDR=10.2.9.8,IPADDR2=10.2.9.10,DUAL=B;
```

- b. To configure dual-resiliency, edit the SCCP_CONFIG command:

- i. Add the SCCP partner module id (<partner id>) for each driver. The <partner id> value should be set to '0x53' on driver A and '0x43' on driver B.
- ii. Set the <sccp_instance> parameter to a unique number (between 0 and 15) for each SCCP instance. The <sccp_instance> value should be set to '0' on driver A and '1' on driver B.

Driver A:

```
SCCP_CONFIG 704 0 0x108c0100 1 0x53 0
```

Driver B:

```
SCCP_CONFIG 704 0 0x108c0100 1 0x43 1
```

- c. To configure dual-resiliency, edit the TCAP_CONFIG command:

- i. Add the TCAP partner module id (<partner id>) for each driver. The <partner id> value should be set to '0x34' on driver A and '0x24' on driver B.
- ii. Set the <tcap_instance> parameter to a unique number (between 0 and 15) for each TCAP instance. The <tcap_instance> value should be set to '0' on driver A and '1' on driver B:

Unit A:

```
TCAP_CONFIG 0x8000 32767 0x0 32768 0x0100 0 0 0x34 0
```

Unit B:



```
TCAP_CONFIG 0x8000 32767 0x0 32768 0x0100 0 0 0x24 1
```

- d. Verify that the OPC (Originating Point Code) defined in the SNAPI command is the same for both drivers:

Driver A:

```
SNAPI:LAS=1,OPC=704,TRMD=LS;
```

Driver B:

```
SNAPI:LAS=1,OPC=704,TRMD=LS;
```



5. Glossary

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

Table 10: Terms and Abbreviations

Term	Definition
AAA	Authentication, Authorization and Accounting.
AF	Application Function
Cluster	Group of nodes used to provide services as a single unit.
Cluster Node	A node in the Cluster.
CPF	Control Plane Function
Data Dictionary	Defines the format of a protocol's message and its validation parameters: structure, number of fields, data format, etc.
DRA	Diameter Routing Agent
DRT	Data Transfer Request (GTP term)
EMS	Element Management System
FEP	Front End Proxy
HTTP	Hypertext Transfer Protocol
HSS	Home Subscriber Server
IMS	IP Multimedia Subsystem
JMS	Java Message Service
LDAP	Lightweight Directory Access Protocol
Link	The connection joint between the Cluster and Remote Nodes.
LTE	Long Term Evolution
MME	Mobile Management Entity
NGN	Next Generation Networking.
Node	Physical or virtual addressable entity
PCEF	Policy and Charging Enforcement Function
PCRF	Policy and Charging Rules Function, acts as decision point and enforces policy usage for a subscribers



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