



# **Cisco Videoscape Distribution Suite Transparent Caching Application Downgrade Guide**

Release 5.2.1

**February 2015**

**Cisco Systems, Inc.**  
[www.cisco.com](http://www.cisco.com)

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco website at [www.cisco.com/go/offices](http://www.cisco.com/go/offices).

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment causes interference to radio or television reception, which can be determined by turning the equipment off and on, users are encouraged to try to correct the interference by using one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Modifications to this product not authorized by Cisco could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: [www.cisco.com/go/trademarks](http://www.cisco.com/go/trademarks). Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2015 Cisco Systems, Inc. All rights reserved.



**Preface** v

Obtaining Documentation and Submitting a Service Request v

---

**CHAPTER 1**

**Downgrading from VDS TC 5.2.1 to VDS TC 5.2.0** 1-1

Rolling Back the VDS TC Software 1-1

---

**CHAPTER 2**

**Downgrading from VDS TC 5.2.1 to VDS TC 5.1.1** 2-1

Rolling Back the VDS TC Software from VDS TC 5.2.1 to VDS TC 5.2.0 2-1

Rolling Back the VDS TC Software from VDS TC 5.2.0 to VDS TC 5.1.1 2-3

---

**CHAPTER 3**

**Downgrading from VDS TC 5.2.1 to VDS TC 5.0.X** 3-1

Rolling Back the VDS TC Software from VDS TC 5.2.1 to VDS TC 5.2.0 3-1

Rolling Back the VDS TC Software from VDS TC 5.2.0 to VDS TC 5.0.X 3-3





## Preface

---

**Created: February 2015**

The *Cisco Videoscape Distribution Suite Transparent Caching Application Downgrade Guide* provides information on how to downgrade the VDS TC software and license from VDS TC version 5.2.1 to a previous version of VDS TC.

This guide contains the following chapters:

- [Downgrading from VDS TC 5.2.1 to VDS TC 5.2.0](#)
- [Downgrading from VDS TC 5.2.1 to VDS TC 5.1.1](#)
- [Downgrading from VDS TC 5.2.1 to VDS TC 5.0.X](#)

## Obtaining Documentation and Submitting a Service Request

For information on obtaining documentation, submitting a service request, and gathering additional information, see the monthly *What's New in Cisco Product Documentation*, which also lists all new and revised Cisco technical documentation, at:

<http://www.cisco.com/en/US/docs/general/whatsnew/whatsnew.html>

Subscribe to the *What's New in Cisco Product Documentation* as an RSS feed and set content to be delivered directly to your desktop using a reader application. The RSS feeds are a free service. Cisco currently supports RSS Version 2.0.





## Downgrading from VDS TC 5.2.1 to VDS TC 5.2.0

This chapter describes how to downgrade from VDS TC 5.2.1 to VDS TC 5.2.0 if necessary. Only use these steps if you are downgrading to VDS TC 5.2.0. To downgrade a VDS TC 5.2.1 installation to VDS TC 5.1.1, please see [Chapter 2, “Downgrading from VDS TC 5.2.1 to VDS TC 5.1.1”](#). To downgrade a VDS TC 5.2.1 installation to VDS TC 5.0.X, please see [Chapter 3, “Downgrading from VDS TC 5.2.1 to VDS TC 5.0.X”](#).



### Note

Because you will need to stop traffic redirection to the VDS TC system during the downgrade process, you should perform the downgrade during a maintenance window.

## Rolling Back the VDS TC Software

Follow these steps to roll back the VDS TC software to the version that was installed before you performed the upgrade.

- Step 1** On the PBR routers, stop redirecting traffic to the VDS TC solution.
- Step 2** Immediately after stopping the traffic redirection to the VDS TC solution, you must stop the VDS TC caching service. Follow these steps to stop the VDS TC caching service:
- Using SSH software, such as Putty, open an SSH connection to the management IP address of the VDS TC appliance.
  - Log into the system using the username **admin**. The default password is the serial number of the VDS TC Integrated Appliance, which can be found either by accessing the CIMC or by accessing the Status > Hardware View page from VDS TC Manager. The serial number is displayed in the Support Tag ID field in VDS TC Manager.
  - From the VDS TC CLI prompt, enter the command **enable**. When prompted, enter the Enable mode password and press **Enter**. You are now logged into Enable mode and the Enable prompt, console#, should appear.



### Note

By default, your system serial number is the password for the Enable mode, but this password may have been changed.

- From the Enable mode prompt, enter the command **oper service stop** to stop the caching service.
- Wait a few minutes and then enter the command **show status**. Check to see if the Device State shows “stopped.” For example:

```
console# show status
Operational state Device state Administrative state
disabled           stopped           unlocked
```

**Caution**

Do not proceed to the next step until the Device State shows “stopped.” You may need to repeat the **show status** command several times before you see this status. Wait several minutes between executions of the **show status** command.

- Step 3** Close any open VDS TC Manager windows and ensure that no other administrators are connected to the VDS TC Manager before proceeding.
- Step 4** Obtain the kernel load file used for VDS TC 5.2.0 from Cisco. This file is published on cisco.com in the same location as the VDS TC 5.2.0 image file and the file name is `linux-2.6.27.19-5-llpf_10--KERNEL_LOAD_1406831120_rev41398.tar`.
- Step 5** Using SFTP software, such as WinSCP, connect to the management IP address that was assigned to the VDS TC management server. Log in using the user name **padmin** and the password that was provided by Cisco.
- Step 6** Copy the VDS TC 5.2.0 kernel load file that you obtained in Step 4 to the **/tmp** folder.
- Step 7** Log into the VDS TC management server as the **root** user with the password provided by Cisco.
- Step 8** From the VDS TC management server, to copy the VDS TC 5.2.0 kernel installation package file to each of the cache engines enter the command **scp** `linux-2.6.27.19-5-llpf_10--KERNEL_LOAD_1406831120_rev41398.tar root@ce-#:/tmp`, where # is the number of the cache engine to which you are copying the file. For example:

```
scp linux-2.6.27.19-5-llpf_10--KERNEL_LOAD_1406831120_rev41398.tar root@ce-1:/tmp
```

**Note**

Repeat this step for each cache engine.

- Step 9** Perform the following steps for each cache engine:
- Enter the command `ssh ce-#`, where # is the number of the cache engine to which you want to connect. When prompted, enter the password for the padmin account that was provided by Cisco.
  - On the cache engine, enter the command `cd /tmp`.
  - Enter the command `tar -xvf` `linux-2.6.27.19-5-llpf_10--KERNEL_LOAD_1406831120_rev41398.tar` to extract the kernel files.
  - Enter the command `cd linux-2.6.27.19-5-llpf_10--KERNEL_LOAD_1406831120` to change to the new folder that was created when extracting the files in Step c.
  - Enter the command `./linux-2.6.27.19-5-llpf_10--INSTALL_PHASE-1.sh` to run the first phase of the kernel installation.
  - Each time you see the following prompt, press **Enter**:  
Press [Enter] key...

**Note**

You will this prompt several times.

- When you see the following prompt, press **Enter**. This will cause the system to reboot for the first time. When the system reboots, your SSH connection to the cache engine will close.



Going to REBOOT, Press [Enter] key...

- h. After the cache engine reboots, from the VDS TC management server enter the command **ssh ce-X** to reconnect to the cache engine, where *X* is the number of the cache engine to which are reconnecting.
- i. Enter the command **cd /tmp**.
- j. Enter the command **cd linux-2.6.27.19-5-llpf\_10--KERNEL\_LOAD\_1406831120**.
- k. Enter the command **./linux-2.6.27.19-5-llpf\_10--INSTALL\_PHASE-2\_Cisco.sh** to run the second phase of the kernel installation.
- l. Each time you see the following prompt, press **Enter**:

Press [Enter] key...

- m. When you see the following prompt, press **Enter**. This will cause the system to reboot. When the system reboots, your SSH connection to the cache engine will close.

Going to REBOOT, Press [Enter] key...

- n. After the cache engine reboots, from the VDS TC management server enter the command **ssh ce-X** to reconnect to the cache engine, where *X* is the number of the cache engine to which are reconnecting.
- o. To confirm that the kernel version has been rolled back, enter the command **uname -a** and confirm that date **Thu Jul 31 17:18:28 GMT 2014** appears in the output, as shown in the following example:

```
Linux ce-1 2.6.27.19-11pf_10-5-default #20 SMP Thu Jul 31 17:18:28 GMT 2014 x86_64
x86_64 x86_64 GNU/Linux
```

- p. Enter **logout** to close the SSH connection to the cache engine.



**Note** Repeat Step 9 for each cache engine.

- Step 10** From the VDS TC CLI prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**. You are now logged into Enable mode and the Enable prompt, console#, should appear.



**Note** By default, your system serial number is the password for the Enable mode, but this password may have been changed.

- Step 11** Enter the **config** command to enter Configuration mode.
- Step 12** To recover the previous configuration file, from the VDS TC Configuration mode, enter the command **import tftp\_server filename**. In this command *tftp\_server* is the IP address or the hostname of the TFTP server that contains the configuration file that you backed up during the upgrade and *filename* is the name of the file that you backed up. For example, **import localhost cluster\_conf\_5.2.0b124\_bkp.xml**.
- Step 13** Enter the command **apply** to apply the changes.
- Step 14** Enter **exit** to return to Enable mode.
- Step 15** From the VDS TC CLI in Enable mode, enter one of the following commands, depending on whether you are downgrading a VDS TC 1S Integrated Appliance installation or a VDS TC Cluster installation:
  - **For a VDS TC Cluster installation:** Enter the command **upgrade all 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:
 

```
upgrade all 127.0.0.1 VDS-TC_GA_5.2.0b124_Server_Cluster.tar.gz
```

- **For a VDS TC 1S Integrated Appliance installation:** Enter the command **upgrade 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:

```
upgrade 127.0.0.1 VDS-TC_GA_5.2.0b123_Integrated_Appliance.tar.gz
```

- Step 16** After upgrading the system, exit completely from the VDS TC CLI and log back into the CLI to access the new software version.




---

**Note** If you do not log out of the VDS TC CLI and log back in, you will not see the current version.

---

- Step 17** From the VDS TC prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**.

- Step 18** Enter the command **show version** to confirm that the correct version is now installed.

- Step 19** At the Enable mode prompt, enter the command **oper service start** to start the caching service.

- Step 20** Wait a few minutes and then enter the command **show status**. Do *not* proceed to the next step until you see a Device Status of “Started.” For example:

```
console# show status
Operational state Device state Administrative state
enabled           started           unlocked
```

- Step 21** On the PBR routers, start redirecting traffic to the VDS TC solution.



## Downgrading from VDS TC 5.2.1 to VDS TC 5.1.1

This chapter describes how to downgrade from VDS TC 5.2.1 to VDS TC 5.1.1 if necessary. Only use these steps if you are downgrading to VDS TC 5.1.1. To downgrade a VDS TC 5.2.1 installation to VDS TC 5.2.0, please see [Chapter 1, “Downgrading from VDS TC 5.2.1 to VDS TC 5.2.0”](#). To downgrade a VDS TC 5.2.1 installation to VDS TC 5.0.x, please see [Chapter 3, “Downgrading from VDS TC 5.2.1 to VDS TC 5.0.X”](#).



**Note**

To downgrade from VDS TC 5.2.1 to VDS TC 5.1.1, you must first downgrade to VDS TC 5.2.0 and then downgrade from VDS TC 5.2.0 to VDS TC 5.1.1.



**Note**

Because you will need to stop traffic redirection to the VDS TC system during the downgrade process, you should perform the downgrade during a maintenance window.

## Rolling Back the VDS TC Software from VDS TC 5.2.1 to VDS TC 5.2.0

Follow these steps to roll back the VDS TC software to the version that was installed before you performed the upgrade.

- Step 1** On the PBR routers, stop redirecting traffic to the VDS TC solution.
- Step 2** Immediately after stopping the traffic redirection to the VDS TC solution, you must stop the VDS TC caching service. Follow these steps to stop the VDS TC caching service:
- Using SSH software, such as Putty, open an SSH connection to the management IP address of the VDS TC appliance.
  - Log into the system using the username **admin**. The default password is the serial number of the VDS TC Integrated Appliance, which can be found either by accessing the CIMC or by accessing the Status > Hardware View page from VDS TC Manager. The serial number is displayed in the Support Tag ID field in VDS TC Manager.
  - From the VDS TC CLI prompt, enter the command **enable**. When prompted, enter the Enable mode password and press **Enter**. You are now logged into Enable mode and the Enable prompt, console#, should appear.

**Note**

By default, your system serial number is the password for the Enable mode, but this password may have been changed.

- d. From the Enable mode prompt, enter the command **oper service stop** to stop the caching service.
- e. Wait a few minutes and then enter the command **show status**. Check to see if the Device State shows “stopped.” For example:

```
console# show status
Operational state Device state Administrative state
disabled           stopped           unlocked
```

**Caution**

Do not proceed to the next step until the Device State shows “stopped.” You may need to repeat the **show status** command several times before you see this status. Wait several minutes between executions of the **show status** command.

**Step 3** Close any open VDS TC Manager windows and ensure that no other administrators are connected to the VDS TC Manager before proceeding.

**Step 4** From the VDS TC CLI prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**. You are now logged into Enable mode and the Enable prompt, console#, should appear.

**Note**

By default, your system serial number is the password for the Enable mode, but this password may have been changed.

**Step 5** Enter the **config** command to enter Configuration mode.

**Step 6** To recover the previous configuration file, from the VDS TC Configuration mode, enter the command **import tftp\_server filename**. In this command *tftp\_server* is the IP address or the hostname of the TFTP server that contains the configuration file that you backed up during the upgrade and *filename* is the name of the file that you backed up. For example, **import localhost cluster\_conf\_5.2.0b124\_bkp.xml**.

**Step 7** Enter the command **apply** to apply the changes.

**Step 8** Enter **exit** to return to Enable mode.

**Step 9** From the VDS TC CLI in Enable mode, enter one of the following commands, depending on whether you are downgrading a VDS TC 1S Integrated Appliance installation or a VDS TC Cluster installation:

- **For a VDS TC Cluster installation:** Enter the command **upgrade all 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:

```
upgrade all 127.0.0.1 VDS-TC_GA_5.2.0b124_Server_Cluster.tar.gz
```

- **For a VDS TC 1S Integrated Appliance installation:** Enter the command **upgrade 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:

```
upgrade 127.0.0.1 VDS-TC_GA_5.2.0b123_Integrated_Appliance.tar.gz
```

**Step 10** After upgrading the system, exit completely from the VDS TC CLI and log back into the CLI to access the new software version.



**Note** If you do not log out of the VDS TC CLI and log back in, you will not see the current version.

**Step 11** From the VDS TC prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**.

**Step 12** Enter the command **show version** to confirm that the correct version is now installed.

## Rolling Back the VDS TC Software from VDS TC 5.2.0 to VDS TC 5.1.1



**Note** Do not proceed with these steps until you have performed the steps in the [Rolling Back the VDS TC Software from VDS TC 5.2.1 to VDS TC 5.2.0](#) section.

**Step 1** Close any open VDS TC Manager windows and ensure that no other administrators are connected to the VDS TC Manager before proceeding.

**Step 2** Log into the VDS TC management server as the root user with the password provided by Cisco.

**Step 3** Perform the following steps for each cache engine:

- a. Enter the command **ssh ce-#**, where # is the number of the cache engine to which you want to connect. When prompted, enter the password for the padmin account that was provided by Cisco.
- b. Enter the command **vi /boot/grub/menu.lst** to edit the menu.lst file.
- c. Change the second line to **default 3**.
- d. Enter **:wq** to exit the vi editor and save your changes.
- e. After you have saved the changes to the menu.lst file, enter **reboot** to reboot the cache engine.
- f. After the cache engine reboots, to confirm that the kernel version has been rolled back, enter the command **uname -a** and confirm that date **Thu Nov 19 11:42:07 GMT 2009** appears in the output, as shown in the following example:

```
Linux ce-4 2.6.27.19-11pf-5-default #4 SMP Thu Nov 19 11:42:07 GMT 2009 x86_64 x86_64
x86_64 GNU/Linux
```



**Note** Repeat Step 3 for each cache engine.

**Step 4** From the VDS TC CLI prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**. You are now logged into Enable mode and the Enable prompt, console#, should appear.



**Note** By default, your system serial number is the password for the Enable mode, but this password may have been changed.

**Step 5** Enter the **config** command to enter Configuration mode.

- Step 6** To recover the previous configuration file, from the VDS TC Configuration mode, enter the command **import** *tftp\_server filename*. In this command *tftp\_server* is the IP address or the hostname of the TFTP server that contains the configuration file that you backed up during the upgrade and *filename* is the name of the file that you backed up. For example, **import localhost cluster\_conf\_5.1.1b28\_bkp.xml**.
- Step 7** Enter the command **apply** to apply the changes.
- Step 8** Enter **exit** to return to Enable mode.
- Step 9** From the VDS TC CLI in Enable mode, enter one of the following commands, depending on whether you are downgrading a VDS TC 1S Integrated Appliance installation or a VDS TC Cluster installation:
- **For a VDS TC Cluster installation:** Enter the command **upgrade all 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:  

```
upgrade all 127.0.0.1 VDS-TC_GA_5.1.1b28_Server_Cluster.tar.gz
```
  - **For a VDS TC 1S Integrated Appliance installation:** Enter the command **upgrade 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:  

```
upgrade 127.0.0.1 VDS-TC_GA_5.1.1b27_Integrated_Appliance.tar.gz
```
- Step 10** If you had installed the 5.1.1b28\_patch2 on the VDS-TC installation, reinstall this patch using the patch installation guide, available from Cisco.
- Step 11** After upgrading the system, exit completely from the VDS TC CLI and log back into the CLI to access the new software version.




---

**Note** *If you do not log out of the VDS TC CLI and log back in, you will not see the current version.*

---

- Step 12** From the VDS TC prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**.
- Step 13** Enter the command **show version** to confirm that the correct version is now installed.
- Step 14** At the Enable mode prompt, enter the command **oper service start** to start the caching service.
- Step 15** Wait a few minutes and then enter the command **show status**. Do *not* proceed to the next step until you see a Device Status of “Started.” For example:
- ```
console# show status
Operational state Device state Administrative state
enabled           started           unlocked
```
- Step 16** On the PBR routers, start redirecting traffic to the VDS TC solution.



## Downgrading from VDS TC 5.2.1 to VDS TC 5.0.X

This chapter describes how to downgrade from VDS TC 5.2.1 to VDS TC 5.0.X if necessary. Only use these steps if you are downgrading to VDS TC 5.0.X. To downgrade a VDS TC 5.2.1 installation to VDS TC 5.2.0, please see [Chapter 1, “Downgrading from VDS TC 5.2.1 to VDS TC 5.2.0”](#). To downgrade a VDS TC 5.2.1 installation to VDS TC 5.1.1, please see [Chapter 2, “Downgrading from VDS TC 5.2.1 to VDS TC 5.1.1”](#).



**Note**

To downgrade from VDS TC 5.2.1 to VDS TC 5.0.X, you must first downgrade to VDS TC 5.2.0 and then downgrade from VDS TC 5.2.0 to VDS TC 5.0.X.



**Note**

Because you will need to stop traffic redirection to the VDS TC system during the downgrade process, you should perform the downgrade during a maintenance window.

## Rolling Back the VDS TC Software from VDS TC 5.2.1 to VDS TC 5.2.0

Follow these steps to roll back the VDS TC software to the version that was installed before you performed the upgrade.

- Step 1** On the PBR routers, stop redirecting traffic to the VDS TC solution.
- Step 2** Immediately after stopping the traffic redirection to the VDS TC solution, you must stop the VDS TC caching service. Follow these steps to stop the VDS TC caching service:
- Using SSH software, such as Putty, open an SSH connection to the management IP address of the VDS TC appliance.
  - Log into the system using the username **admin**. The default password is the serial number of the VDS TC Integrated Appliance, which can be found either by accessing the CIMC or by accessing the Status > Hardware View page from VDS TC Manager. The serial number is displayed in the Support Tag ID field in VDS TC Manager.
  - From the VDS TC CLI prompt, enter the command **enable**. When prompted, enter the Enable mode password and press **Enter**. You are now logged into Enable mode and the Enable prompt, console#, should appear.

**Note**

By default, your system serial number is the password for the Enable mode, but this password may have been changed.

- d. From the Enable mode prompt, enter the command **oper service stop** to stop the caching service.
- e. Wait a few minutes and then enter the command **show status**. Check to see if the Device State shows “stopped.” For example:

```
console# show status
Operational state Device state Administrative state
disabled           stopped           unlocked
```

**Caution**

Do not proceed to the next step until the Device State shows “stopped.” You may need to repeat the **show status** command several times before you see this status. Wait several minutes between executions of the **show status** command.

**Step 3** Close any open VDS TC Manager windows and ensure that no other administrators are connected to the VDS TC Manager before proceeding.

**Step 4** Obtain the kernel load file used for VDS TC 5.2.0 from Cisco. This file is published on cisco.com in the same location as the VDS TC 5.2.0 image file and the file name is `linux-2.6.27.19-5-llpf_10--KERNEL_LOAD_1406831120_rev41398.tar`.

**Step 5** Using SFTP software, such as WinSCP, connect to the management IP address that was assigned to the VDS TC management server. Log in using the user name **padmin** and the password that was provided by Cisco.

**Step 6** Copy the VDS TC 5.2.0 kernel load file that you obtained in Step 4 to the **/tmp** folder.

**Step 7** Log into the VDS TC management server as the root user with the password provided by Cisco.

**Step 8** From the VDS TC management server, to copy the VDS TC 5.2.0 kernel installation package file to each of the cache engines enter the command **scp linux-2.6.27.19-5-llpf\_10--KERNEL\_LOAD\_1406831120\_rev41398.tar root@ce-#:/tmp**, where # is the number of the cache engine to which you are copying the file. For example:

```
scp linux-2.6.27.19-5-llpf_10--KERNEL_LOAD_1406831120_rev41398.tar root@ce-1:/tmp
```

**Note**

Repeat this step for each cache engine.

**Step 9** Perform the following steps for each cache engine:

- a. Enter the command **ssh ce-#**, where # is the number of the cache engine to which you want to connect. When prompted, enter the password for the padmin account that was provided by Cisco.
- b. On the cache engine, enter the command **cd /tmp**.
- c. Enter the command **tar -xvf linux-2.6.27.19-5-llpf\_10--KERNEL\_LOAD\_1406831120\_rev41398.tar** to extract the kernel files.
- d. Enter the command **cd linux-2.6.27.19-5-llpf\_10--KERNEL\_LOAD\_1406831120** to change to the new folder that was created when extracting the files in Step c.
- e. Enter the command **./linux-2.6.27.19-5-llpf\_10--INSTALL\_PHASE-1.sh** to run the first phase of the kernel installation.



- f. Each time you see the following prompt, press **Enter**:

Press [Enter] key...

**Note**

You will this prompt several times.

- g. When you see the following prompt, press **Enter**. This will cause the system to reboot for the first time. When the system reboots, your SSH connection to the cache engine will close.

Going to REBOOT, Press [Enter] key...

- h. After the cache engine reboots, from the VDS TC management server enter the command **ssh ce-X** to reconnect to the cache engine, where *X* is the number of the cache engine to which are reconnecting.

- i. Enter the command **cd /tmp**.

- j. Enter the command **cd linux-2.6.27.19-5-llpf\_10--KERNEL\_LOAD\_1406831120**.

- k. Enter the command **./linux-2.6.27.19-5-llpf\_10--INSTALL\_PHASE-2\_Cisco.sh** to run the second phase of the kernel installation.

- l. Each time you see the following prompt, press **Enter**:

Press [Enter] key...

- m. When you see the following prompt, press **Enter**. This will cause the system to reboot. When the system reboots, your SSH connection to the cache engine will close.

Going to REBOOT, Press [Enter] key...

- n. After the cache engine reboots, from the VDS TC management server enter the command **ssh ce-X** to reconnect to the cache engine, where *X* is the number of the cache engine to which are reconnecting.

- o. To confirm that the kernel version has been rolled back, enter the command **uname -a** and confirm that date **Thu Jul 31 17:18:28 GMT 2014** appears in the output, as shown in the following example:

```
Linux ce-1 2.6.27.19-11pf_10-5-default #20 SMP Thu Jul 31 17:18:28 GMT 2014 x86_64
x86_64 x86_64 GNU/Linux
```

- p. Enter **logout** to close the SSH connection to the cache engine.

**Note**

Repeat Step 9 for each cache engine.

- Step 10** From the VDS TC CLI prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**. You are now logged into Enable mode and the Enable prompt, console#, should appear.

**Note**


By default, your system serial number is the password for the Enable mode, but this password may have been changed.

- Step 11** Enter the **config** command to enter Configuration mode.

- Step 12** To recover the previous configuration file, from the VDS TC Configuration mode, enter the command **import tftp\_server filename**. In this command *tftp\_server* is the IP address or the hostname of the TFTP server that contains the configuration file that you backed up during the upgrade and *filename* is the name of the file that you backed up. For example, **import localhost cluster\_conf\_5.2.0b124\_bkp.xml**.

- Step 13** Enter the command **apply** to apply the changes.
- Step 14** Enter **exit** to return to Enable mode.
- Step 15** From the VDS TC CLI in Enable mode, enter one of the following commands, depending on whether you are downgrading a VDS TC 1S Integrated Appliance installation or a VDS TC Cluster installation:
- **For a VDS TC Cluster installation:** Enter the command **upgrade all 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:  

```
upgrade all 127.0.0.1 VDS-TC_GA_5.2.0b124_Server_Cluster.tar.gz
```
  - **For a VDS TC 1S Integrated Appliance installation:** Enter the command **upgrade 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:  

```
upgrade 127.0.0.1 VDS-TC_GA_5.2.0b123_Integrated_Appliance.tar.gz
```
- Step 16** After upgrading the system, exit completely from the VDS TC CLI and log back into the CLI to access the new software version.
-  **Note** If you do not log out of the VDS TC CLI and log back in, you will not see the current version.
- Step 17** From the VDS TC prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**.
- Step 18** Enter the command **show version** to confirm that the correct version is now installed.

## Rolling Back the VDS TC Software from VDS TC 5.2.0 to VDS TC 5.0.X



**Note**

Do not proceed with these steps until you have performed the steps in the [Rolling Back the VDS TC Software from VDS TC 5.2.1 to VDS TC 5.2.0](#) section.

- Step 1** Close any open VDS TC Manager windows and ensure that no other administrators are connected to the VDS TC Manager before proceeding.
- Step 2** Log into the VDS TC management server as the root user with the password provided by Cisco.
- Step 3** Perform the following steps for each cache engine:
- a. Enter the command **ssh ce-#**, where # is the number of the cache engine to which you want to connect. When prompted, enter the password for the padmin account that was provided by Cisco.
  - b. Enter the command **vi /boot/grub/menu.lst** to edit the menu.lst file.
  - c. Change the second line to **default 3**.
  - d. Enter **:wq** to exit the vi editor and save your changes.
  - e. After you have saved the changes to the menu.lst file, enter the command **reboot** to reboot the cache engine.

- f. After the cache engine reboots, to confirm that the kernel version has been rolled back, enter the command **uname -a** and confirm that date **Thu Nov 19 11:42:07 GMT 2009** appears in the output, as shown in the following example:

```
Linux ce-4 2.6.27.19-1lpf-5-default #4 SMP Thu Nov 19 11:42:07 GMT 2009 x86_64 x86_64
x86_64 GNU/Linux
```

**Note**

Repeat Step 3 for each cache engine.

**Step 4**

If you have configured an external NTP server on the VDS TC 5.2 installation follow these steps to change the configuration file:

- a. From the VDS TC CLI prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**. You are now logged into Enable mode and the Enable prompt, **console#**, should appear.

**Note**

By default, your system serial number is the password for the Enable mode, but this password may have been changed.

- b. Enter the **config** command to enter Configuration mode.
- c. Enter the command **export localhost filename** to export the configuration file.
- d. Open the configuration file in a text editor or an XML editor and make the following changes in the file:

```
<ntp>
  <server-ip>127.127.1.0</server-ip>
  <timezone>GMT</timezone>
</ntp>
```

- e. From the VDS TC Configuration mode, enter the command **import localhost filename** to import the updated configuration file to the VDS TC management server.
- f. Enter the command **apply** to apply the changes.
- g. Enter **exit** to return to Enable mode.

**Step 5**

From the SSH connection to the VDS TC management server, enter the command **/opt/pang/mgmt/config/downgrade\_proc.sh**. This command will do the following:

- Restore the Policy Manager configuration
- Restore configuration files
- Restore the CMDB files

**Step 6**

From the VDS TC CLI in Enable mode, enter one of the following commands, depending on whether you are downgrading a VDS TC 1S Integrated Appliance installation or a VDS TC Cluster installation:

- **For a VDS TC Cluster installation:** Enter the command **upgrade all 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:
 

```
upgrade all 127.0.0.1 VDS-TC_GA_5.0.3b276_Server_Cluster.tar.gz
```
- **For a VDS TC 1S Integrated Appliance installation:** Enter the command **upgrade 127.0.0.1 filename**, where *filename* is the filename of the upgrade package for the *previous* version of VDS TC. For example:

```
upgrade 127.0.0.1 VDS-TC_GA_5.0.3b275_Integrated_Appliance.tar.gz
```

**Step 7** After upgrading the system, exit completely from the VDS TC CLI and log back into the CLI to access the new software version.

**Note**

If you do not log out of the VDS TC CLI and log back in, you will not see the current version and when you try to activate the new license, you will receive a “License activation failed” error message.

**Step 8** From the VDS TC prompt, enter the **enable** command. When prompted, enter the Enable mode password and press **Enter**.

**Step 9** Enter the command **show version** to confirm that the correct version is now installed.

**Step 10** When you logged back into the CLI, if you received a compatibility configuration error, follow these steps to restore the VDS TC 5.0.x configuration file that you backed up during the upgrade process:

- a. Enter the **config** command to enter Configuration mode.
- b. To recover the previous configuration file, from the VDS TC Configuration mode, enter the command **import tftp\_server filename**. In this command *tftp\_server* is the IP address or the hostname of the TFTP server that contains the configuration file that you backed up during the upgrade and *filename* is the name of the file that you backed up. For example, **import localhost cluster\_conf\_5.0.2b28\_bkp.xml**.
- c. Enter the command **apply** to apply the changes.
- d. Enter **exit** to return to Enable mode.

**Step 11** From Enable mode, enter the command **license import 127.0.0.1 filename**, where *filename* is the name of the license file of the *previous* version.

**Step 12** Enter **license activate** to apply the license. When prompted with “Are you sure you want to activate this license?” enter **Y**.

**Step 13** After the license activation is complete, at the Enable mode prompt enter the command **oper service start** to start the caching service.

**Step 14** Wait a few minutes and then enter the command **show status**. Do *not* proceed to the next step until you see a Device Status of “Started.” For example:

```
console# show status
Operational state Device state Administrative state
enabled           started           unlocked
```

**Step 15** On the PBR routers, start redirecting traffic to the VDS TC solution.