



Avaya Call Management System

Base Load Upgrade

Release 18
August 2017

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published by Avaya in varying mediums which may include product information, operating instructions and performance specifications that Avaya may generally make available to users of its products and Hosted Services. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of documentation unless such modifications, additions, or deletions were performed by Avaya. End User agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End User.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website:

<https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010> under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if You acquired the product(s) from an authorized Avaya Channel Partner outside of the United States and Canada, the warranty is provided to You by said Avaya Channel Partner and not by Avaya.

"Hosted Service" means a hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES IF YOU PURCHASE A HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo) UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE. YOUR USE OF THE HOSTED SERVICE SHALL BE LIMITED BY THE NUMBER AND TYPE OF LICENSES PURCHASED UNDER YOUR CONTRACT FOR THE HOSTED SERVICE, PROVIDED, HOWEVER, THAT FOR CERTAIN HOSTED SERVICES IF APPLICABLE, YOU MAY HAVE THE OPPORTUNITY TO USE FLEX LICENSES, WHICH WILL BE INVOICED ACCORDING TO ACTUAL USAGE ABOVE THE CONTRACT LICENSE LEVEL. CONTACT AVAYA OR AVAYA'S CHANNEL PARTNER FOR MORE INFORMATION ABOUT THE LICENSES FOR THE APPLICABLE HOSTED SERVICE, THE AVAILABILITY OF ANY FLEX LICENSES (IF APPLICABLE), PRICING AND BILLING INFORMATION, AND OTHER IMPORTANT INFORMATION REGARDING THE HOSTED SERVICE.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, [HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO](https://support.avaya.com/licenseinfo), UNDER THE LINK "AVAYA SOFTWARE LICENSE TERMS (Avaya Products)" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AVAYA CHANNEL PARTNER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA CHANNEL PARTNER; AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Avaya grants You a license within the scope of the license types described below, with the exception of Heritage Nortel Software, for which the scope of the license is detailed below. Where the order documentation does not expressly identify a license type, the applicable license will be a Designated System License. The applicable number of licenses and units of capacity for which the license is granted will be one (1), unless a different number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a Designated Processor that hosts a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License type(s)

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only on a number of Designated Processors up to the number indicated in the order. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named User," means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

Shrinkwrap License (SR). You may install and use the Software in accordance with the terms and conditions of the applicable license agreements, such as "shrinkwrap" or "clickthrough" license accompanying or applicable to the Software ("Shrinkwrap License").

Heritage Nortel Software

"Heritage Nortel Software" means the software that was acquired by Avaya as part of its purchase of the Nortel Enterprise Solutions Business in December 2009. The Heritage Nortel Software is the software contained within the list of Heritage Nortel Products located at <https://support.avaya.com/LicenseInfo/> under the link "Heritage Nortel Products," or such successor site as designated by Avaya. For Heritage Nortel Software, Avaya grants Customer a license to use Heritage Nortel Software provided hereunder solely to the extent of the authorized activation or authorized usage level, solely for the purpose specified in the Documentation, and solely as embedded in, for execution on, or for

communication with Avaya equipment. Charges for Heritage Nortel Software may be based on extent of activation or use authorized as specified in an order or invoice.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Note that each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third party components

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at:

<https://support.avaya.com/Copyright> or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components, to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

The following applies if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE <HTTP://WWW.MPEGLA.COM>.

Service Provider

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, H.264 CODEC, OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE <WWW.SIPRO.COM/CONTACT.HTML>. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (I) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (II) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS

GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE <HTTP://WWW.MPEGLA.COM>.

Compliance with Laws

Customer acknowledges and agrees that it is responsible for complying with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of <https://support.avaya.com/security>. Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (<https://support.avaya.com/css/P8/documents/100161515>).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya Inc.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: <https://support.avaya.com>, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: <https://support.avaya.com> for product or Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: <https://support.avaya.com> (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Chapter 1: Introduction	7
When and how to use this document	8
Impacts to CMS service	8
Contacting Avaya for assistance with your upgrade	9
Possible customization impacts	9
Upgrade kit contents	9
Contacting Avaya technical support during the upgrade.	9
Chapter 2: Preparing for a base load upgrade on RHEL (Linux®)	11
Prerequisites	11
Verifying the current CMS version and load	12
Verifying that your previous backups completed successfully	12
Verifying the backup of your CMS system data	12
Verifying that your last CMSADM backup completed successfully	13
Verifying that your last LAN backup of the system data completed successfully	13
Verifying the backup of your CMS data	14
Verifying that your previous full or incremental backup completed successfully	14
Verifying that your last LAN backup of CMS data completed successfully	15
Verifying that the nightly archiver is functioning	15
Checking the status of the disk drives	16
Checking for memory errors and system panics	17
Verifying free space in the root file system	18
Rebooting your CMS system	18
Backing up the CMS system	19
Backing up your system data	19
Performing a CMSADM backup to tape	19
Performing a full system backup with Tivoli Storage Manager.	21
Performing a full system backup with Netbackup.	21
Backing up your CMS data	21
Performing a full data backup with a tape device	22
Performing a full data backup with Tivoli Storage Manager	23
Performing a full data backup with Netbackup	23
Backing up any new CMS data	23
Chapter 3: Updating the RHEL (Linux®) operating system.	25
Prerequisites	25
Stopping CMS Supervisor Web.	25
Stopping Avaya OA data forwarders	26
Installing RHEL (Linux®) rpms	26

Contents

Installing the Avaya CMS security script.	29
Chapter 4: Upgrading the CMS base load on RHEL (Linux®)	33
Prerequisites	33
Removing the current CMS load	34
Installing the new CMS base load	35
Installing the new CMS base load on a Linux®-based platform	36
Installing the new CMS base load on a Virtual CMS.	38
Installing CMS patches	40
Upgrading Avaya CMS Supervisor Web	41
Turning on CMS	42
Starting CMS Supervisor Web	43
Starting Avaya OA data forwarders.	43
Installing Access Security Gateway and the CMS Authentication File	43
Chapter 5: Completing the base load upgrade process	47
Prerequisites	47
Performing a backup of the system files.	48
Performing a backup of the CMS data	48

Chapter 1: Introduction

Purpose

The purpose of this document is to describe the Avaya CMS base load upgrade process for R18. This Avaya CMS base load upgrade is designed to be installed by Avaya CMS customers who either have had problems with an earlier version of the product or would like access to any new features added in the maintenance release. This upgrade provides known software fixes from previous versions. The software is acquired by ordering the latest PCN. The PCN provides a list of all fixes and features added in the maintenance release.

Important:

All customers must use Customer Upgrade Express (CUE) to upgrade to Call Management System (CMS) R18 from an earlier release.

You must install this upgrade as soon as possible as Technical Support Organization only troubleshoots products that have the latest release installed.

This section includes the following topics:

- [When and how to use this document](#) on page 8
- [Impacts to CMS service](#) on page 8
- [Contacting Avaya for assistance with your upgrade](#) on page 9
- [Possible customization impacts](#) on page 9
- [Upgrade kit contents](#) on page 9
- [Contacting Avaya technical support during the upgrade](#) on page 9
- [If you encounter problems or have questions during the upgrade and are unable to resolve them by following the upgrade instructions, call technical support at 1-800-242-2121. Be ready to provide the number of the Quality Protection Plan you are using.](#) on page 9

Important:

Before installing a base load upgrade, verify that the software discs you received when ordering the PCN are a newer version of the software than your current version of the software. Verify that you are using the proper base load upgrade document for your release of CMS.

For a complete list of bug fixes and new features available in the latest CMS load, see the CMS R18 release notes on <https://support.avaya.com>.

When and how to use this document

 **Important:**

All customers must use Customer Upgrade Express (CUE) to upgrade to Call Management System (CMS) R18 from an earlier release.

Use this document to upgrade CMS from an older CMS Release 18 base load to a newer CMS R18 load. Unless indicated otherwise, all procedures in the Avaya CMS Base Load Upgrade document are required.

Avaya recommends that:

- Before performing the upgrade, read through this entire document so that you are familiar with what tasks you will need to perform. If you decide you would like to have Avaya assist you performing the upgrade, see [Contacting Avaya for assistance with your upgrade](#) on page 9.
- Have a pen or pencil during the upgrade so that you can record any required information.
- During the upgrade, mark each step as it is completed.
- You will be required to enter UNIX commands during the upgrade process. You must enter the command from the UNIX prompt in a terminal window. Press the **Enter** key after you have typed in the command. Use the same capitalization and spacing shown in this document.
- If you encounter problems or have questions during the upgrade, contact Avaya technical support.

Impacts to CMS service

 **CAUTION:**

This software upgrade is service affecting.

During the Operating System patch installation using `rpm_updates` for Linux®, your system displays an estimate of the amount of time needed to install the Operating System updates. The Operating System update installation is the part of the base load upgrade that usually requires the longest amount of time to complete."

Contacting Avaya for assistance with your upgrade

You can make arrangements to have Avaya provide remote assistance for this upgrade. This remote assistance must be scheduled at least two weeks before your upgrade. Charges, which will be quoted, vary for this service. Contact the Technical Support Organization at 1-800-242-2121.

Possible customization impacts

The software upgrade that you are installing could potentially impact system customization that was performed before this upgrade. For example:

- Custom reports
- LAN printer customization
- Work-force management interfaces
- Operational Analyst

You can schedule an evaluation of your system to determine whether any of your system customizations might be impacted by this upgrade. Schedule this evaluation at least two weeks before your upgrade. Charges, which will be quoted, vary for this service. Contact Avaya CRM at 1-866-282-9266.

Upgrade kit contents

All the software you need for the upgrade should be included with your upgrade kit.

Contacting Avaya technical support during the upgrade

If you encounter problems or have questions during the upgrade and are unable to resolve them by following the upgrade instructions, call technical support at 1-800-242-2121. Be ready to provide the number of the Quality Protection Plan you are using.

Chapter 2: Preparing for a base load upgrade on RHEL (Linux®)

This section describes the tasks you must perform before you upgrade your CMS base load. These procedures will help you verify that your CMS system has no existing hardware or software problems before the upgrade. If you do not perform these procedures, your base load upgrade could fail, and your CMS system could be put in a non-functioning state for some time.

This section includes the following topics:

- [Prerequisites](#) on page 11
- [Verifying the current CMS version and load](#) on page 12
- [Verifying that your previous backups completed successfully](#) on page 12
- [Verifying that the nightly archiver is functioning](#) on page 15
- [Checking the status of the disk drives](#) on page 16
- [Checking for memory errors and system panics](#) on page 17
- [Verifying free space in the root file system](#) on page 18
- [Rebooting your CMS system](#) on page 18
- [Backing up the CMS system](#) on page 19

Prerequisites

Before you perform the procedures in this section, you must:

- Read the information in [Introduction](#) on page 7.
- The Avaya CMS software disc will include a readme file called **cms.readme**. Avaya recommends you review this file for any changes that might impact the procedures in this document.
- Log in to the system as **root**.



Important:

You will not be able to log into the system remotely as **root**. If you are logging into the system remotely, log in as a user and then enter: **su - root**

Verifying the current CMS version and load

To verify the version and load of CMS currently on the machine:

1. Log in to the system as **root**.
2. Enter:

```
rpm -q cms
```

The system displays the currently installed CMS package, including the load number, for example:

```
cms-R18.0.0.0-ca.b.x86_64
```

3. Record the displayed CMS version information for reference later, during the upgrade process.

CMS version: _____

Verifying that your previous backups completed successfully

Approximately two days before the CMS base load upgrade, verify that your backups have been completing successfully.

This section includes the following topics:

- [Verifying the backup of your CMS system data](#) on page 12
- [Verifying the backup of your CMS data](#) on page 14

Verifying the backup of your CMS system data

To verify that your previous system backup completed successfully, choose one of the following procedures:

- If you backup your data directly to tape, a USB storage device or a network mount point, go to [Verifying that your last CMSADM backup completed successfully](#) on page 13.

You are responsible for backing up your CMS system unless you engage Avaya to perform the backups in conjunction with this base load upgrade.

- If you use the CMS LAN backup feature, go to [Verifying that your last LAN backup of the system data completed successfully](#) on page 13

You are responsible for backing up your CMS system. Avaya is not responsible for performing LAN backups. For more information about the CMS LAN backup feature, see *Avaya Call Management System LAN Backup User Guide*. This document provides: information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

Verifying that your last CMSADM backup completed successfully

To verify that your last CMSADM backup completed successfully:

1. Enter:

```
tail /cms/install/logdir/backup.log
```

2. Verify that the previous CMSADM backup completed successfully.

An example of a successful CMSADM backup message is:

```
==== Begin backup <timestamp>

Converter started <timestamp>
Converter completed successfully <timestamp>

Testing tape on /dev/rmt/0...

Tape test on /dev/rmt/0 is okay...

2873600 blocks

==== Finished backup <timestamp>
```

3. Choose one of the following actions:
 - If your previous backup was successful, go to [Verifying the backup of your CMS data](#) on page 14.
 - If your previous backup was *not* successful, contact your Avaya CMS support representative.

Verifying that your last LAN backup of the system data completed successfully

If you use the CMS LAN backup feature, perform the following procedure:

1. Enter:

```
cat /cms/install/logdir/backup.log | more
```

2. Press **Enter** to continue the display. It might be necessary to repeat this step several times.

3. Verify that the previous system backup completed successfully.

An example of a successful system backup message is:

```
===== LAN SYSTEM BACKUP SUCCESSFULLY FINISHED Date and time
```

4. Choose one of the following actions:
 - If your previous backup was successful, go to [Verifying the backup of your CMS data](#) on page 14.
 - If your previous backup was *not* successful, contact your Avaya CMS support representative.

Verifying the backup of your CMS data

To verify that your previous system backup completed successfully, choose one of the following procedures:

- If you backup your data directly to a tape device, go to [Verifying that your previous full or incremental backup completed successfully](#) on page 14.
- If you use the CMS LAN backup feature, go to [Verifying that your last LAN backup of CMS data completed successfully](#) on page 15.

For more information about the CMS LAN backup feature, see *Avaya Call Management System LAN Backup User Guide*. This document provides: information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

Verifying that your previous full or incremental backup completed successfully

To verify that your previous full or incremental backup completed successfully:

1. Verify that you are logged in as **root**.



Important:

If at anytime during the upgrade process you need to verify that you are logged in as the root user, you can enter the command: **id**

2. Enter:

```
tail /cms/maint/backup/back.log
```

3. Verify that the previous full or incremental backup completed successfully.

An example of a successful full or incremental backup message is:

```
1711 <timestamp> 2 1 INFO
      BACKUP INFO: The backup has completed successfully.
      Please label the volume CMS-030415-01-LSAC-00-F-01-r3milcms
```

4. Choose one of the following actions:
 - If your previous backup was successful go to [Verifying that the nightly archiver is functioning](#) on page 15.
 - If your previous backup was *not* successful, contact your Avaya CMS support representative.

Verifying that your last LAN backup of CMS data completed successfully

To verify that your last LAN backup of CMS data completed successfully:

1. Enter:

```
cat /cms/install/logdir/backup.log | more
```
2. Press **Enter** to continue the display. It might be necessary to repeat this step several times.
3. Verify that the previous data backup completed successfully.

An example of a successful data backup message is:

```
+++++ ON-Bar BACKUP SUCCESSFULLY FINISHED Date and time
```

4. Choose one of the following actions:
 - If your previous backup was successful, go to [Verifying that the nightly archiver is functioning](#) on page 15.
 - If your previous backup was *not* successful, contact your Avaya CMS support representative.

Verifying that the nightly archiver is functioning

To verify that nightly archiver is functioning correctly:

1. Verify that you are logged in to the system as **root**.

2. Enter:

```
su cms cms
```

The system displays the CMS main menu.

3. Press **Enter** to accept the default terminal type.
4. Select `Maintenance > Error Log Report`.
5. Enter **2600** in the `Error codes` field.
6. Leave all of the other fields blank.
7. Press **Enter** to select the `Run` option.
8. Press **Enter**.

The system displays an archive history report.

9. Verify that the nightly archiver is functioning correctly for all ACDs administered on the system.

An example of a successful nightly archiver message is:

```
2600 <timestamp> 2 1 INFO
      ARCHIVER status: Daily Archive for (Mon)
      <timestamp> Successful
```

10. Select `Exit` to return to the previous menu.
11. Choose one of the following actions:
 - If the nightly archiver is functioning correctly, go to [Checking the status of the disk drives](#) on page 16.
 - If the nightly archiver is *not* functioning correctly, contact your Avaya CMS support representative.

Checking the status of the disk drives

1. To verify the disk or disk volume, run the following command:

```
# /olds/chkDisks
```

- If this command returns to the prompt without generating any output, there are no errors and you can continue with the upgrade.

- If this command returns the following output:

```
SEVERE ERROR: Enclosure 32, RAID Drive Slot X is in state Failed (where X is  
the slot number)  
Possible Disk Errors! Please check /olds/log/err.log for details
```

then you must contact Avaya Services and resolve the issue before continuing with the upgrade.

Checking for memory errors and system panics

1. Check for memory errors and system panics. Enter:

```
egrep -i "panic | memory error" /var/log/messages* | more
```

Note:

It might be necessary to press **Enter** to continue the display.

An example of a panic error message is:

```
messages-20121223:<timestamp> trex Kernel panic - not syncing: : Port x halting  
system due to client process failure
```

2. Choose one of the following actions, depending on the message that is displayed:
 - If the system displays no memory error or panic messages, go to [Verifying free space in the root file system](#) on page 18.
 - If the system displays any memory error or panic messages, your system requires maintenance. Contact your Avaya CMS support representative.

Verifying free space in the root file system

To verify that sufficient free space is available in your root file system to accomplish the base load upgrade:

1. Enter:

```
df -k /
```

The system displays a message similar to the following:

Filesystem	1K-blocks	Used	Available	Use%	Mounted on
/dev/sda2	9842412	2709148	6633288	29%	/

2. Check the disk capacity.
3. Choose one of the following actions:
 - If the disk Use% is less than 85%, go to [Rebooting your CMS system](#) on page 18.
 - If the disk Use% is 85% or greater, contact your Avaya CMS support representative.

Rebooting your CMS system

You must reboot your CMS system and verify that the system is functioning properly. Reboot the CMS system before you backup your data.

To reboot your CMS system:

1. Enter the following command from the pound (#) prompt:

```
shutdown -r now
```

The system reboots.

2. Log in to the system as **root**.
3. Choose one of the following actions:
 - If the system does not boot correctly or if any error messages are displayed, contact your Avaya CMS support representative.
 - If the system boots correctly, go to [Backing up the CMS system](#) on page 19.

Backing up the CMS system

Before beginning a CMS base load upgrade, you must backup your CMS system data and CMS data.

This section includes the following topics:

- [Backing up your system data](#) on page 19
- [Backing up your CMS data](#) on page 21
- [Backing up any new CMS data](#) on page 23

Backing up your system data

A backup of the system data must be performed approximately one day before the CMS base load upgrade.

To take a back up of your current system files, choose one of the following procedures:

- If you backup your data directly to a tape device, go to [Performing a CMSADM backup to tape](#) on page 19.
- If you backup your data to a USB storage device, refer to the section *Performing a CMSADM backup to a USB storage device* of the *Avaya CMS Software Installation, Maintenance, and Troubleshooting for Linux®* document for information on how to perform CMSADM backups to a USB storage device.
- If you backup your data to a network mount point, refer to the section *Performing a CMSADM backup to a network mount point* of the *Avaya CMS Software Installation, Maintenance, and Troubleshooting for Linux®* document for information on how to perform CMSADM backups to a network mount point.
- If you use the CMS LAN backup feature, go to [Performing a full system backup with Tivoli Storage Manager](#) on page 21.

For more information about the CMS LAN backup feature, see *Avaya Call Management System LAN Backup User Guide*. This document provides information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

Performing a CMSADM backup to tape

To take a back up of your current system files, perform the following procedure:

1. Verify that you are using the correct tape for the tape drive for your system. Many of the tape cartridges look alike, and using the wrong tape can damage the tape drive mechanism and tape heads.

Chapter 2: Preparing for a base load upgrade on RHEL (Linux®)

2. Log in as **root**.
3. Enter:

cmsadm

The Avaya Call Management System Administration Menu (CMSADM Menu) is displayed.

4. Enter the number associated with the `backup` option.

Depending on the number of tape drives connected to your system, one of the following messages will be displayed by your system.

- If only one tape drive is available, the system displays the following message:

```
Please insert the first cartridge tape into device name.
Press ENTER when ready or Del to quit:
```

- If more than one tape drive is available for use, the system displays a list of tape devices. Enter a tape drive selection from the displayed list.

An example of a tape device list is:

```
Select the tape drive:
 1) SCSI 2 tape drive: /dev/st0
 2) SCSI 2 tape drive: /dev/st1
Enter choice (1-2):
```

Note:

If the system fails to identify the tapes by manufacturer name, tape devices are displayed according to their system device names, such as “/dev/st0”.

5. Press **Enter**.

The backup process is initiated.

When the backup is complete, the system displays the following message:

```
xxxxxxx blocks
Tape Verification
xxxxxxx blocks
WARNING: A CMS Full Maintenance Backup in addition to this cmsadm
backup must be done to have a complete backup of the system. . .
. .

Please label the backup tape(s) with the date and the current CMS
version (rXXXXXX.X)
```

6. Write protect the tape and store the tape in a secure location until the next backup is performed.
7. Go to [Backing up your CMS data](#) on page 21.

Performing a full system backup with Tivoli Storage Manager

If you use the Tivoli Storage Manager backup feature, perform the following procedure:

1. Log in as **root**.
2. Enter:

```
/cms/LANbkup/bin/backup.tivoli 0
```
3. Verify that the backup has completed successfully by entering:

```
cat /cms/install/logdir/backup.log
```
4. Go to [Backing up your CMS data](#) on page 21.

Performing a full system backup with Netbackup

If you use the CMS Netbackup feature, perform the following procedure:

1. Log in as **root**.
2. Enter:

```
/cms/LANbkup/bin/backup.netbackup 0
```
3. Verify that the backup has completed successfully by entering:

```
cat /cms/install/logdir/backup.log
```
4. Continue with [Backing up your CMS data](#) on page 21.

Backing up your CMS data

Your CMS data must be backed up approximately one day before the CMS base load upgrade is performed.

To backup your CMS data, choose one of the following procedures:

- If you backup your data directly to a tape device, go to [Performing a full data backup with a tape device](#) on page 22.
- If you backup your data to a USB storage device, refer to the section *Performing a CMS Maintenance Back Up of data to a USB storage device* of the *Avaya CMS Software Installation, Maintenance, and Troubleshooting for Linux®* document for information on how to perform CMSADM backups to a USB storage device.
- If you backup your data to a network mount point, refer to the section *Performing a CMS Maintenance Back Up of data to a network mount point* of the *Avaya CMS Software Installation, Maintenance, and Troubleshooting for Linux®* document for information on how to perform CMSADM backups to a network mount point.

Chapter 2: Preparing for a base load upgrade on RHEL (Linux®)

- If you use the CMS LAN backup feature, go to [Performing a full data backup with Tivoli Storage Manager](#) on page 23.

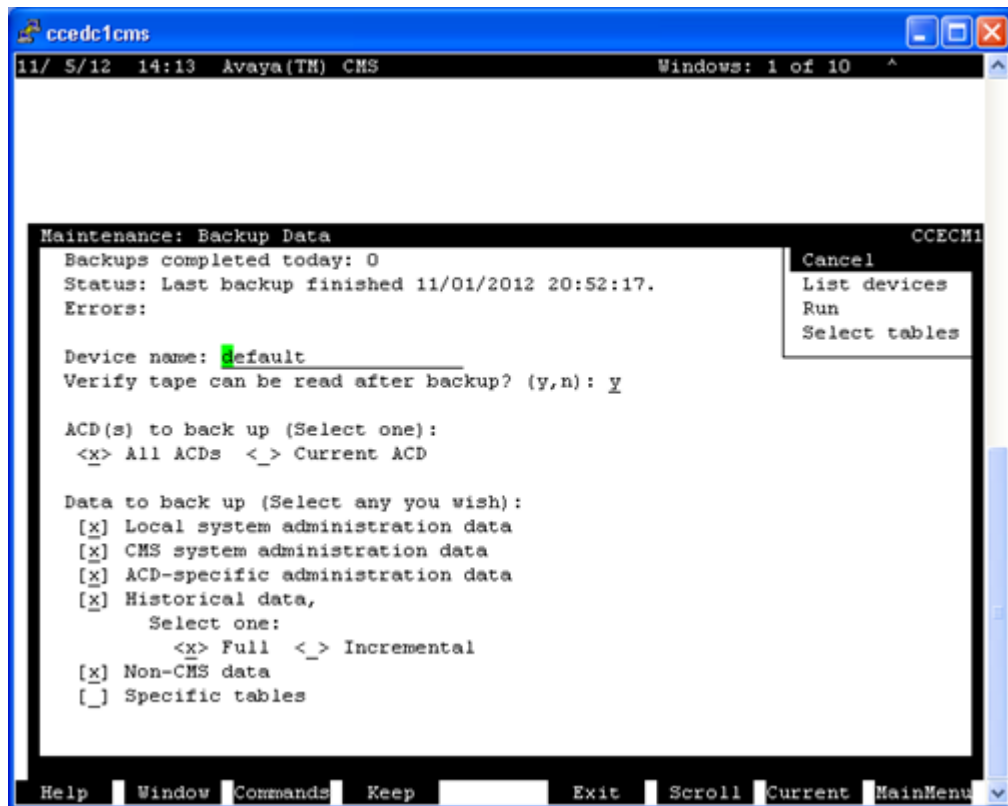
For more information about the CMS LAN backup feature, see *Avaya Call Management System LAN Backup User Guide*. This document provides: information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

Performing a full data backup with a tape device

To perform a full backup of CMS data:

1. Verify that you are using the correct tape for the tape drive for your system. Many of the tape cartridges look alike, and using the wrong tape can damage the tape drive mechanism and tape heads.
2. Verify that you are logged in as **cms**.
3. Enter **cms**.
4. From the main menu, select Maintenance > Back Up Data.

The system displays the Back Up Data window, as shown below. Do not change any of the default selections.



5. Press **Enter** to access the action list in the upper right corner of the window.

6. Select `Run` and press **Enter**.
7. Wait for the backup to complete. If the backup does not complete successfully, contact your Avaya CMS support representative.
8. Write protect the tape and store the tape in a secure location until the next backup is performed.
9. Go to [Backing up any new CMS data](#) on page 23.

Performing a full data backup with Tivoli Storage Manager

If you use the Tivoli Storage Manager backup feature, perform the following procedure:

1. Verify that you are logged in as **root**.
2. Enter:

```
/cms/LANbkup/bin/onbar_backup.tivoli 0
```
3. Verify that the backup has completed successfully by entering the following commands:

```
cat /cms/install/logdir/backup.log  
cat /cms/install/logdir/bar_act.log
```
4. Go to [Backing up any new CMS data](#) on page 23.

Performing a full data backup with Netbackup

If you use the CMS Netbackup feature, perform the following procedure:

1. Verify that you are logged in as **root**.
2. Enter:

```
/cms/LANbkup/bin/onbar_backup.netbackup 0
```
3. Verify that the backup has completed successfully by entering the following commands:

```
cat /cms/install/logdir/backup.log  
cat /cms/install/logdir/bar_act.log
```
4. Continue with [Backing up any new CMS data](#) on page 23.

Backing up any new CMS data

You must back up any CMS data that has been generated since your last CMS data backup. Choose one of the following options:

- If no new CMS data has been generated since your last CMS data backup, continue with [Updating the RHEL \(Linux®\) operating system](#) on page 25.

Chapter 2: Preparing for a base load upgrade on RHEL (Linux®)

- If new CMS data has been generated since your last CMS data backup, perform one of the following procedures immediately before the upgrade:
 - [Performing a full data backup with a tape device](#) on page 22
 - [Performing a full data backup with Tivoli Storage Manager](#) on page 23

Once the new CMS data has been backed up, continue with [Updating the RHEL \(Linux®\) operating system](#) on page 25.

For more information about the CMS LAN backup feature, see *Avaya Call Management System LAN Backup User Guide*. This document provides information about using the CMS LAN backup feature, hardware requirements, software requirements, and support guidelines.

Chapter 3: Updating the RHEL (Linux®) operating system

This section contains procedures for updating your operating system. You must complete the procedures in this section before upgrading your CMS base load.

This section includes the following topics:

- [Prerequisites](#) on page 25
- [Stopping Avaya OA data forwarders](#) on page 26
- [Installing RHEL \(Linux®\) rpms](#) on page 26
- [Installing the Avaya CMS security script](#) on page 29

Prerequisites

Before you perform the procedures in this section, you must:

- Read the information in [Introduction](#) on page 7.
- Perform all of the required procedures in [Preparing for a base load upgrade on RHEL \(Linux®\)](#) on page 11.
- Verify that you are logged in to the system as `root`.

Stopping CMS Supervisor Web

To stop the CMS Supervisor Web, enter:

```
cmsweb stop
```

Stopping Avaya OA data forwarders

If the CMS configuration includes data collection by Avaya OA, turn off all Avaya OA forwarders on the CMS server using the **pa stop all** command. For more information about Avaya OA forwarders, see *Avaya OA Maintenance and Troubleshooting*.

Installing RHEL (Linux®) rpms

1. Load the Avaya Call Management System software disc into the disk drive.
2. Change to the root directory, enter:

```
cd /
```

3. Mount the DVD drive. Enter:

```
mount /dev/dvd /mnt
```

The system displays the following message:

```
mount: block device /dev/sr0 is write-protected, mounting read-only
```



CAUTION:

You must turn off CMS in order to install the RHEL Linux® rpms.

4. Enter:

```
cmssvc
```

The system displays the Avaya Call Management System Services Menu or **CMSSVC** Menu.

5. Enter the number associated with the **run_cms** option.
6. Enter the number associated with the **Turn off both CMS and IDS** option.

The system returns to the command prompt.

7. Run the rpm update script. Enter:

```
/mnt/rpm_update
```

The system displays one of the following messages:

- If there are Linux® rpms to install, the system displays the following messages:

```

RPM updates started: <timestamp>
RPM Updates for CMS R18 created <date>

Loaded plugins: security
cms_approved | 1.3 kB 00:00 ...
cms_approved/primary | 718 kB 00:00 ...
cms_approved 1102/1102

NetworkManager.x86_64 1:0.8.1-34.el6_3 cms_approved
NetworkManager-glib.x86_64 1:0.8.1-34.el6_3 cms_approved
NetworkManager-gnome.x86_64 1:0.8.1-34.el6_3 cms_approved
.
.
.
yum-rhn-plugin.noarch 0.9.1-49.el6 cms_approved 79 k
There are XXX rpm packages to update.
Update process will take approximately YY Minutes to complete

The above shows the rpms that will be updated. This process will
apply the updates then reboot the system to assure sanity.
WARNING: Not applying these updates could cause issues with
running the newer CMS load.
Do you want to continue? [y/n]

```

Note:

This message contains an estimate of the amount of time needed to install the RHEL (Linux®) rpms. Ignore messages associated with the `/var/cms/spatches/yum.log` file as this file is created during the initial rpm installation.

⚠ Important:

You need to monitor the system during the rpm installation process to ensure that the installation of the rpms does not halt. When the rpm installation process completes, the system automatically reboots into multiuser mode and displays the graphical login screen.

- If there are no RHEL (Linux®) rpms to install, the system displays the following message:

```

RPM updates started: <timestamp>
RPM Updates for CMS R18 created <date>

Loaded plugins: security
cms_approved | 1.3 kB 00:00 ...
No rpm updates are required. Quitting rpm_update.

```

8. If there are no Linux® rpms to install, continue with Step [12](#).



CAUTION:

If you cancel the installation of RHEL (Linux®) rpms, you must install them before upgrading CMS. To cancel installation of the RHEL (Linux®) rpms, enter n.

9. To install the RHEL (Linux®) rpms, enter `y`.

The system displays the following messages:

```
Loaded plugins: security
Setting up Update Process
Resolving Dependencies
--> Running transaction check
----> Package NetworkManager.x86_64 1:0.8.1-33.el6 will be updated
----> Package NetworkManager.x86_64 1:0.8.1-34.el6_3 will be an update
.
.
.
Transaction Summary
=====
Install      1 Package(s)
Upgrade     129 Package(s)

Total download size: 166 M
Downloading Packages:
.
.
.
Complete!
  All RPM updates applied successfully
Stopping sshd:           [ OK ]
Starting sshd:          [ OK ]
  post-update changes for SAL/ASG support completed.
  Rebooting the system now.
```

Note:

The rpm installation takes at least the amount of time that was estimated earlier in the procedure. After the rpms are installed, the system reboots into multi-user mode and displays a login prompt.



Important:

Do not halt the system.

10. Log in to the system as **root**.
11. Verify that all the Linux® rpms are installed. Enter:

tail -10 /var/cms/spatches/yum.log

Verify that the system displays the following message:

```
All RPM updates applied successfully
```

Note:

If the installation procedure fails for any of the rpms, the system displays the following message:

```
- Customers in the US should call the CMS Technical Services Organization at
1-800-242-2121
- Customers outside the US should contact your Avaya representative or distributor.
```

If the system displays this message, continue with this procedure and the remaining CMS base load upgrade procedures. When the upgrade is complete, notify your Avaya CMS support organization as prompted by the system.

12. Verify that IDS is running. Enter:

cmssvc

The system displays the **CMSSVC** menu. If the system first displays the following text, then IDS is not running:

```
cmssvc: Warning IDS off-line. It will take approx 45 seconds to
start cmssvc. IDS can be turned on with the run_ids command on the
cmssvc menu
```

13. Select the **run_ids** option.

- If IDS is running, the system displays the following:

```
IDS is already up and running
```

Continue with Step [14](#).

- If IDS is not running, select the **Turn IDS on** option.

The system starts IDS and returns to the command prompt.

14. Continue with [Installing the Avaya CMS security script](#) on page 29.

Installing the Avaya CMS security script

Important:

You can log in to the console only as **root** after you run the Avaya CMS security script. If you are logging into the system remotely, log in as another user and then use `su` to log in as root.

1. Verify that you are logged in to the system as **root**.
2. Verify the current services running on the system and save the list for comparison with the listing after the security script run.

Note:

It is necessary to find out which services in the list of differences are used by the customer.

3. To capture the current services and preserve the output to a file, enter:

```
chkconfig --list > /tmp/current_chkconfig.txt
```

4. If the system has mounted the Avaya Call Management System software disc, continue with Step [8](#).

5. Insert the Avaya Call Management System software disc into the disk drive.

6. Change to the root directory. Enter:

```
cd /
```

7. Mount the Avaya Call Management System software disc. Enter:

```
mount /dev/dvd /mnt
```

8. Enter:

```
/mnt/security/cms_sec
```

The system configures your security settings and displays the following message when the process is complete:

```
Avaya CMS security configuration completed: date
```

Note:

If the system displays a configuration failed message, contact your Avaya services representative.

9. To capture the new services and preserve the output to a different file, enter:

```
chkconfig --list > /tmp/new_chkconfig.txt
```

10. Run the `diff` command against the two listings files and search for services that need to be re-enabled.

```
diff /tmp/current_chkconfig.txt /tmp/new_chkconfig.txt
```

11. View the output from the `diff` command and re-enable the services that are displayed.

To re-enable any customer used services, enter:

```
chkconfig [--level levels] <Service name> <on|off|reset>
```

Service name is the first column of the output from the `chkconfig --list` command.

Example:

```
chkconfig --level 2345 rpcbind on
```

Note:

The files in `/tmp` directory are not saved during the reboot process. If you need to keep a copy of the files, move them to a directory whose contents are not erased during a reboot.

12. Reboot the system. Enter:

```
shutdown -r now
```

Log in to the system as **root**.

13. Continue with [Upgrading the CMS base load on RHEL \(Linux®\)](#) on page 33.

Chapter 4: Upgrading the CMS base load on RHEL (Linux®)

Use this procedure only if the operating system is RHEL (Linux®).

You must complete the procedures in the previous sections before upgrading your CMS base load. Use the procedures in this section to upgrade an older CMS base load to a newer CMS base load.

This section includes the following topics:

- [Prerequisites](#) on page 33
- [Removing the current CMS load](#) on page 34
- [Removing the current CMS load](#) on page 34
- [Installing the new CMS base load on a Linux®-based platform](#) on page 36
- [Installing the new CMS base load on a Virtual CMS](#) on page 38
- [Installing CMS patches](#) on page 40
- [Upgrading Avaya CMS Supervisor Web](#) on page 41
- [Turning on CMS](#) on page 42
- [Starting CMS Supervisor Web](#) on page 43
- [Starting Avaya OA data forwarders](#) on page 43
- [Installing Access Security Gateway and the CMS Authentication File](#) on page 43

Prerequisites

Before you perform the procedures in this section, you must:

- Read the information in [Introduction](#) on page 7.
- Perform all of the required procedures in [Preparing for a base load upgrade on RHEL \(Linux®\)](#) on page 11.
- Perform all of the required procedures in [Updating the RHEL \(Linux®\) operating system](#) on page 25.
- Verify that you are logged in to the system as `root`.

Removing the current CMS load

1. Load the Avaya Call Management System software disc into the disk drive.
2. Enter:

cmssvc

The system displays the following message:

```
Avaya(TM) Call Management System Services Menu

Select a command from the list below.
 1) auth_display Display feature authorizations
 2) auth_set     Authorize capabilities/capacities
 3) run_ids      Turn Informix Database on or off
 4) run_cms     Turn Avaya CMS on or off
 5) setup       Set up the initial configuration
 6) swinfo     Display switch information
 7) swsetup    Change switch information
 8) uninstall  Remove the CMS rpm from the machine
 9) patch_rmv  Backout an installed CMS patch
10) back_all   Backout all installed CMS patches from machine
Enter choice (1-10) or q to quit: 8
```

3. Select the **uninstall** option.

The system displays the following message:

```
The following package is currently installed

Avaya(TM) Call Management System R18.0.0.0
  cms-R18.0.0.0-ca.b.x86_64

Do you want to remove this package? [y,n,?] ?
```

4. Enter **y**.

The system displays the following message:

```
Proceeding with the removal of CMS...
Do you want to preserve CMS data? [y,n,?] ?
```

**WARNING:**

If you select **n** in response to this question, *all* your CMS data is deleted from the system, so you should answer **y** to preserve the data.

5. Enter **y**.

The system displays the following message:

```
CMS will be removed from this machine; the data will be preserved
Are you sure this is correct? [y,n,?] ?
```

6. Enter **y**.

The system displays the following message:

```
All file systems should be backed up before continuing.
See the Maintenance chapter in the CMS
Installation and Maintenance Manual for instructions.

Have you backed up the file systems? [y,n,?] ?
```

7. Enter **y**.

The system displays the following message:

```
Proceeding with removal of CMS...

warning: /var/elog/elog_if saved as /var/elog/elog_if.rpmsave
warning: /var/elog/elog saved as /var/elog/elog.rpmsave
warning: /usr/lib/cms/Sname saved as /usr/lib/cms/Sname.rpmsave
warning: /usr/lib/cms/Pname saved as /usr/lib/cms/Pname.rpmsave
warning: /usr/lib/cms/Aname saved as /usr/lib/cms/Aname.rpmsave
warning: /cms/pbx/master saved as /cms/pbx/master.rpmsave
warning: /cms/pbx/acd1/xln.log saved as /cms/pbx/acd1/xln.log.rpmsave
.
.
.
Removal of Avaya(TM) Call Management System (cms) is complete
```

8. Continue with [Installing the new CMS base load](#) on page 35.

Installing the new CMS base load

- If the system is a Dell R620/R720 or a HP DL380P platform, continue with [Installing the new CMS base load on a Linux®-based platform](#) on page 36.

- If the system is a Virtual CMS, continue with [Installing the new CMS base load on a Virtual CMS](#) on page 38.

Installing the new CMS base load on a Linux®-based platform

1. Verify the Avaya Call Management System software disc is in the disk drive.
2. Mount the Avaya Call Management System software disc by running the following command:

```
mount /dev/dvd /mnt
```

3. Enter the following command to update the CMS related Informix files:

```
/mnt/update_ids
```

The system displays the following message when IDS updates are applied:

```
/mnt/update_ids successfully finished
```

4. Install CMS. Enter:

```
/mnt/cms.bin
```

The system displays the following message:

```
Unpacking files please wait...
Extracting the tar....

Installing Avaya(TM) Call Management System R18.0.0.0 (cms) version r18ca.b
This is an upgrade

CMS must be turned off in order to perform the upgrade.
Do you want to turn off CMS now? [y,n,?] ?
```

- If CMS is turned on and you want to continue with the installation of the new CMS base load, enter **y**.
- If CMS is turned on and you want to cancel the installation of the new CMS base load, enter **n**.
- If CMS is not running, the installation process continues without prompting the user for an input.

5. When CMS is installed, the system displays the following message:

```

Proceeding with install...

Preparing...          ##### [100%]
  1:cms              ##### [100%]
CMS is installed.

```

Note:

If the installation procedure fails for any reason, the system displays the following message:

```

- Customers in the US should call the CMS Technical Services
Organization at 1-800-242-2121
- Customers outside the US should contact your Avaya representative or
distributor.

```

If the system displays the message shown in this example, notify your Avaya CMS support organization as prompted by the system.

6. Enter:

```
cat /cms/install/logdir/admin.log | more
```

The system displays part of the CMS administration log.

7. Verify that there were no errors during the installation.
8. Press **Enter** to continue the display. It might be necessary to repeat this step several times.
9. Reboot the system. Enter:

```
shutdown -r now
```

The system reboots.

10. Log in to the system as **root**.

11. Verify that IDS is running. Enter:

```
cmssvc
```

The system displays the **CMSSVC** menu. If the system first displays the following text, then IDS is not running:

```

cmssvc: Warning IDS off-line. It will take approx 45 seconds to
start cmssvc. IDS can be turned on with the run_ids command on the
cmssvc menu

```

12. Select the **run_ids** option.

- If IDS is running, the system displays the following:

```
IDS is already up and running
```

Continue with Step [13](#).

- If IDS is not running, select the **Turn IDS on** option.

The system starts IDS and returns to the command prompt.

13. Continue with [Installing CMS patches](#) on page 40.

Installing the new CMS base load on a Virtual CMS

1. Copy the Avaya Call Management System software iso image for the new CMS load that has been downloaded to the PC where the vSphere client is installed.
2. Establish a CD/DVD connection to the directory where the Avaya Call Management System software iso image is located.
3. Run the following command to mount the Avaya Call Management System software disc:

```
mount /dev/dvd /mnt
```

The system displays the following message:

```
mount: block device /dev/sr0 is write-protected, mounting read-only
```

4. Enter the following command to update the CMS related Informix files:

```
/mnt/update_ids
```

The system displays the following message:

```
<timestamp> Updating dbinit.sh and env files
```

5. Install CMS. Enter:

```
/mnt/cms.bin
```

The system displays the following message:

```
Unpacking files please wait...
Extracting the tar....

Installing Avaya(TM) Call Management System R18.0.0.0 (cms) version r18ca.b
This is an upgrade

In order to install CMS, the existing version must be removed.
The following package is currently installed:

    Avaya(TM) Call Management System R18.0.0.0
    cms-R18.0.0.0-bb.e.x86_64

Do you want to remove this package? [y,n,?] ?
...
```

- If CMS is turned on and you want to continue with the installation of the new CMS base load, enter **y**.
- If CMS is turned on and you want to cancel the installation of the new CMS base load, enter **n**.
- If CMS is not running, the installation process continues without prompting the user for an input.

When CMS is installed, the system displays the following message:

```
Customer CMS data successfully upgraded.
CMS is installed.
```

Note:

If the installation procedure fails for any reason, the system displays the following message:

```
- Customers in the US should call the CMS Technical Services
Organization at 1-800-242-2121
- Customers outside the US should contact your Avaya representative or
distributor.
```

If the system displays the message shown in this example, notify your Avaya CMS support organization as prompted by the system.

6. Enter:

```
cat /cms/install/logdir/admin.log | more
```

The system displays part of the CMS administration log.

7. Verify that there were no errors during the installation.
8. Press **Enter** to continue the display. It might be necessary to repeat this step several times.

9. Reboot the system. Enter:

```
shutdown -r now
```

The system reboots.

10. Log in to the system as **root**.
11. Verify that IDS is running. Enter:

```
cmssvc
```

The system displays the **CMSSVC** menu. If the system first displays the following text, then IDS is not running:

```
cmssvc: Warning IDS off-line. It will take approx 45 seconds to
start cmssvc. IDS can be turned on with the run_ids command on the
cmssvc menu
```

12. Select the **run_ids** option.

- If IDS is running, the system displays the following:

```
IDS is already up and running
```

Continue with Step [13](#).

- If IDS is not running, select the **Turn IDS on** option.

The system starts IDS and returns to the command prompt.

13. Continue with [Installing CMS patches](#) on page 40.

Installing CMS patches

The initial release of CMS R18 running on RHEL (Linux®) will not require any CMS patches. This section will be updated when CMS patches are available for installation.

For a complete list of bug fixes and new features available in the latest CMS load, see the CMS R18 release notes on <https://support.avaya.com>.

Upgrading Avaya CMS Supervisor Web

Perform this procedure to upgrade CMS Supervisor Web.

1. Verify the Avaya Call Management System software disc for your specific platform architecture (Linux®), is loaded in the disk drive.
2. Mount the DVD drive, enter:

```
mount /dev/dvd /mnt
```

The system displays the following message:

```
mount: block device /dev/sr0 is write-protected, mounting read-only
```

3. Determine if CMS Supervisor Web is installed on the system. Enter:

```
rpm -q cmsweb
```

The system displays the following output:

```
cmsweb-R18.0.0.0-ca.b.x86_64
```

4. Determine the CMS Supervisor Web version on the Avaya Call Management System software disc. Enter:

```
strings /mnt/cmsweb.bin | grep MINOR=
```

The system displays the following output:

```
MINOR=web18ca.j
```

Compare the version portion of CMS Supervisor Web on the cdrom, web18ca.j, to the version portion of CMS Supervisor Web currently installed on the CMS system, cmsweb-R18.0.0.0-ca.b.x86_64.

Since ca.j of web18ca.j is a later version than ca.b of cmsweb-R18.0.0.0-ca.b.x86_64, an update is needed.

- If the CMS Supervisor Web version on the Avaya Call Management System disc is newer than the CMS Supervisor Web version on the CMS system, then you need to upgrade CMS Supervisor Web. Continue with [Step 5](#).
- If the CMS Supervisor Web version on the Avaya Call Management System disc is same or older than the CMS Supervisor Web version on the CMS system, then you do not need to upgrade CMS Supervisor Web, continue with [Turning on CMS](#) on page 42.

5. Remove the current CMS Supervisor Web package. Enter:

```
rpm -e cmsweb
```

The system removes the CMS Supervisor Web package.

6. To install the CMS Supervisor Web package, enter:

```
/mnt/cmsweb.bin
```

The system displays the following messages:

```
Unpacking files please wait...
Extracting the rpm...

Installing (cmsweb) version
Proceeding with install...

Preparing...          ##### [100%]
 1:cmsweb             ##### [100%]
```

The system installs the new CMS Supervisor Web package.

7. Continue with [Turning on CMS](#) on page 42.

Turning on CMS

To turn on CMS:

1. Enter:

```
cmsadm
```

The system displays the CMSADM Menu.

2. Enter the number associated with the `run_cms` option.

The system displays the following message:

```
Select one of the following
 1) Turn on CMS
 2) Turn off CMS but leave IDS Running
 3) Turn off CMS
Enter choice (1-3):
```

3. Enter: **1**

The system starts CMS and returns to the command prompt.

4. Restart CMS data collection if data collection was turned off at the beginning of the upgrade.

5. Manually run the appropriate Archiver from System Setup if CMS was off during the time your Archiver normally runs.

Starting CMS Supervisor Web

To start the CMS Supervisor Web, enter:

```
cmsweb start
```



Important:

Do not start CMS Supervisor Web if the customer does not plan on using CMS Supervisor Web to access CMS reports. Starting CMS Supervisor Web opens ports that the customer may not want opened.

Starting Avaya OA data forwarders

If the CMS configuration includes data collection by Avaya OA, turn on all Avaya OA forwarders on the CMS server using the **pa start all** command. For more information about Avaya OA forwarders, see *Avaya OA Maintenance and Troubleshooting*.

Installing Access Security Gateway and the CMS Authentication File

Access Security Gateway (ASG) is an authentication interface used to protect the system logins associated with Avaya CMS. ASG uses a challenge and response protocol to validate the user and reduce unauthorized access.

To install ASG on your CMS server, perform the following steps:

Note:

System in the following steps refers to the CMS server.

1. Log in as `root`.

Chapter 4: Upgrading the CMS base load on RHEL (Linux®)

2. Verify that CMS is installed on the system. Enter:

```
rpm -q cms
```

If CMS is installed, the system displays the following:

```
cms-R18.0.0.0-ca.b.x86_64
```

3. Insert the Avaya Call Management System disc into the disk drive.
4. To install the ASG package, enter:

```
mount /dev/dvd /mnt
```

```
/mnt/cmslxsag.bin
```

The system displays a list of status messages at the time of installation. It takes less than a minute to install the ASG package.

- If the system successfully installs the ASG package, the system displays the following message at the end of the installation process:

```
INFO:Install ASG on CMS complete.  
Review output on screen above
```

- If the system does not install the ASG package successfully, the system displays the error on the screen and at the end of the installation, the installer displays a message to review the output on the screen.
5. From your PC, go to the following URL:
<https://rfa.avaya.com/rfa-docs/index.jsp>
 6. Click on the **Start the AFS Application** button to access the Authentication File System (AFS) application.
 7. Select **Avaya CMS** as the product and then select the appropriate release from the drop down list.
 8. Navigate to the download page by following the instructions in the intermediate pages and pressing **Next**.
 9. Download the CMS Authentication File (AF) file to your PC.

Note:

You can download the AF file to your PC prior to CMS installation.

10. Transfer the AF file from your PC to the CMS server.

11. Install the AF file. If you transferred the AF file from your PC to the `/tmp` directory of the CMS server, run the following command to install the AF file:

```
/opt/cmsasg/usr/local/bin/loadauth -af -l /tmp/  
AF-7000009669-11.xml
```

Replace `/tmp` in this example with the actual location of the AF file. Replace the AF file name in this example with the name that corresponds to the AF file that was transferred to the CMS server. Each AF file has a unique name. The `-l` option in the `loadauth` command is a lower case L.

Chapter 5: Completing the base load upgrade process

You must perform the procedures in this section to complete the CMS base load upgrade process.

This section includes the following procedures:

- [Prerequisites](#) on page 47
- [Performing a backup of the system files](#) on page 48
- [Performing a backup of the CMS data](#) on page 48

Prerequisites

Before you perform the procedures in this section, you must:

- Read the information in [Introduction](#) on page 7.
- If your operating system is Solaris, you must:
 - Perform all of the required procedures in [Preparing for a base load upgrade on Solaris](#) on page 13.
 - Perform all of the required procedures in [Updating the Solaris operating system](#) on page 41.
 - Perform all of the required procedures in [Upgrading the CMS base load on Solaris](#) on page 57.
- If your operating system is RHEL (Linux®), you must:
 - Perform all of the required procedures in [Preparing for a base load upgrade on RHEL \(Linux®\)](#) on page 11.
 - Perform all of the required procedures in [Updating the RHEL \(Linux®\) operating system](#) on page 25.
 - Perform all of the required procedures in [Upgrading the CMS base load on RHEL \(Linux®\)](#) on page 33.

Performing a backup of the system files

After the base load upgrade has completed successfully, perform a backup to create a reliable copy of the computer system files. For instructions on how to backup the system files, see [Backing up your system data](#) on page 21 if your operating system is Solaris or [Backing up your system data](#) on page 19 if your operating system is RHEL (Linux®).

Performing a backup of the CMS data

After the base load upgrade has completed successfully, perform a backup to create a reliable copy of the computer CMS data files. For instructions on how to backup the CMS data, see [Backing up your CMS data](#) on page 23 if your operating system is Solaris or [Backing up your CMS data](#) on page 21 if your operating system is RHEL (Linux®).